



Cisco Identity Services Engine リリース 2.2 管理者ガイド

シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスコ コンタクトセンター

0120-092-255（フリーコール、携帯・PHS含む）

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>



目次

第 I 部 :

はじめに 57

第 1 章

Cisco ISE の機能 1

Cisco ISE の概要 2

主要な機能 2

ID ベースのネットワーク アクセス 3

複数の展開シナリオのサポート 3

UCS ハードウェアのサポート 4

基本的なユーザ認証および許可 4

ポリシー セット 5

FIPS 140-2 の実装 5

Common Access Card 機能のサポート 6

クライアント ポスチャ評価 7

ゲストのネットワーク アクセス 8

パーソナル デバイスのサポート 8

Mobile Device Manager と Cisco ISE との相互運用性 8

ネットワークのプロファイリングされたエンドポイント 8

pxGrid ペルソナ 9

TrustSec ワーク センター 9

TACACS+ デバイス管理 9

SXP のサポート 10

サードパーティ デバイスのサポート 10

テレメトリ 11

IPv6 のサポート	11
ロケーションに基づく認証	12
Cisco ISE 認証局	12
証明書プロビジョニング ポータル	12
証明書テンプレートの拡張子	12
Cisco ISE 内部 CA は ASA VPN ユーザに証明書を発行します	13
Active Directory マルチドメイン フォレストのサポート	13
SAnet デバイスのサポート	13
複数のハードウェアおよび VMware プラットフォームへのインストールのサポート	14
外部 ID ソースとしての ID プロバイダ	14
管理ノードの自動フェールオーバーのサポート	14
GUI ベースのアップグレード	15
高度なトラブルシューティングのテクニカル サポートのトンネル	15

第 2 章

管理者ポータルでの移動	17
管理者ポータル	17
ISE ホーム ダッシュボード	19
ホーム ダッシュボードの設定	20
[コンテキストの可視性 (Context Visibility)] のビュー	21
ダッシュレット	23
ビューに表示するデータのフィルタリング	24
ビューのリストでのエンドポイント アクション	26
コンテキストの可視性の属性	26
Cisco ISE 国際化およびローカリゼーション	27
サポートされる言語	27
エンドユーザ Web ポータルのローカリゼーション	28
UTF-8 文字データ エントリのサポート	28
UTF-8 クレデンシャル認証	29
UTF-8 ポリシーおよびポスチャ評価	29
Cisco NAC および MAC エージェントの UTF-8 サポート	29
サブリカントに送信されるメッセージの UTF-8 サポート	30

レポートおよびアラートの UTF-8 サポート	30
ポータルでの UTF-8 文字のサポート	30
ユーザ インターフェイス外での UTF-8 サポート	34
UTF-8 の値のインポートおよびエクスポートのサポート	35
REST での UTF-8 サポート	35
ID ストアの許可データの UTF-8 サポート	35
MAC アドレスの正規化	35
ロールベース アクセス コントロール ポリシーによって制限されている管理者機能	36

 第 3 章

Wireless Setup について 37

ワイヤレス ネットワークの WLC の設定	41
Active Directory と Wireless Setup	43
Wireless Setup でのゲスト ポータル	43
ワイヤレス ネットワーク アカウント登録ポータル	44
ワイヤレス ネットワーク Sponsored Guest フロー	45
Wireless Setup BYOD フロー：ネイティブ サプリカントおよび証明書のプロビジョニング	45
セキュア アクセス フロー	47
Wireless Setup による ISE と WLC の変更	49

 第 II 部：

Cisco ISE ノードの展開 53

 第 4 章

分散環境での Cisco ISE の設定 55

Cisco ISE 展開の用語	55
分散 Cisco ISE 展開のペルソナ	56
Cisco ISE 分散展開	56
Cisco ISE 展開の設定	56
プライマリ ISE ノードからセカンダリ ISE ノードへのデータ レプリケーション	57
Cisco ISE ノードの登録解除	57
分散展開を設定する場合のガイドライン	58
プライマリ ノードおよびセカンダリ ノードで使用可能なメニュー オプション	58

Cisco ISE ノードの設定	60
プライマリ PAN の設定	60
セカンダリ Cisco ISE ノードの登録	61
管理ノード	63
管理ノードのハイ アベイラビリティ	63
ハイ アベイラビリティのヘルス チェック ノード	65
ヘルス チェック ノード	66
セカンダリ PAN への自動フェールオーバー	66
自動フェールオーバーが回避された場合のシナリオ例	67
PAN 自動フェールオーバー機能の影響を受ける機能	68
自動フェールオーバー用のプライマリ PAN の設定	70
セカンダリ PAN のプライマリへの手動昇格	71
プライマリ PAN にサービスを復元する	71
ポリシー サービス ノード	72
ポリシー サービス ノードのハイ アベイラビリティ	72
PSN 間で均等に要求を分散するためのロード バランサ	72
ポリシー サービス ノードでのセッション フェールオーバー	73
ポリシー サービス ノード グループ内のノード数	73
モニタリング ノード	73
モニタリング ノードでの自動フェールオーバー	74
pxGrid ノード	76
pxGrid クライアントおよび機能の管理	77
pxGrid クライアントの有効化	78
pxGrid 機能の有効化	78
Cisco pxGrid ライブ ログ	79
pxGrid の設定	79
pxGrid 証明書の生成	80
展開内のノードの表示	81
プライマリおよびセカンダリの Cisco ISE ノードの同期	81
ノード ペルソナとサービスの変更	82
Cisco ISE でのノードの変更による影響	82

ポリシー サービス ノード グループの作成	83
ISE pxGrid ノードの展開	84
自動フェールオーバー用のモニタリング ノードの設定	85
展開からのノードの削除	86
スタンドアロン Cisco ISE ノードのホスト名または IP アドレスの変更	87
Cisco ISE アプライアンス ハードウェアの交換	88

 第 III 部 :

Cisco ISE 管理アクセスの設定 89

 第 5 章

Cisco ISE の管理 91

Cisco ISE へのログイン	91
管理者ログインブラウザのサポート	92
ログインの試行に失敗した後の管理者のロックアウト	92
Cisco ISE でのプロキシ設定の指定	93
管理者ポータルで使用されるポート	93
外部 RESTful サービス API の有効化	94
外部 RESTful サービス SDK	95
システム時刻と NTP サーバ設定の指定	95
システムの時間帯の変更	96
通知をサポートするための SMTP サーバの設定	97
Cisco ISE 展開のアップグレード	97
さまざまなタイプの展開	98
分散展開のアップグレード	98
ソフトウェア パッチのインストール	102
Cisco ISE ソフトウェア パッチ	103
ソフトウェア パッチ インストールのガイドライン	104
ソフトウェア パッチのロールバック	104
ソフトウェア パッチ ロールバックのガイドライン	105
パッチのインストールおよびロールバックの変更の表示	106
FIPS モードのサポート	106
Cisco ISE での FIPS モードの有効化	107

FIPS モードの動作パラメータ	107
FIPS モードが有効のときの Cisco NAC Agent の要件	108
管理者 CAC 認証のための Cisco ISE の設定	108
サポートされる Common Access Card 標準	110
Cisco ISE での共通アクセス カードの動作	111
Diffie-Hellman アルゴリズムを使用した SSH キー交換の保護	111
セキュア syslog 送信のための Cisco ISE の設定	111
セキュア syslog リモート ロギング ターゲットの設定	112
セキュア syslog ターゲットに監査可能なイベントを送信するためのロギング カテゴリの有効化	113
TCP syslog および UDP syslog コレクタの無効化	113
デフォルトのセキュア syslog コレクタ	114
オフライン メンテナンス	115

第 6 章

管理者および管理者アクセス ポリシーの管理	117
ロールベース アクセス コントロール	117
Cisco ISE 管理者	117
CLI 管理者と Web ベースの管理者の権限の比較	118
新しい Cisco ISE 管理者の作成	118
Cisco ISE 管理者グループ	119
管理者グループの作成	129
Cisco ISE への管理アクセス	130
Cisco ISE のロールベース アクセス コントロール	130
ロールベースの権限	130
RBAC ポリシー	130
デフォルトのメニュー アクセス権限	131
メニュー アクセス権限の設定	131
データ アクセス権限を付与するための前提条件	132
デフォルトのデータ アクセス権限	132
データ アクセス権限の設定	135
管理者のアクセス ポリシーの設定	135

管理者アクセスの設定	136
同時管理セッションとログイン バナーの最大数の設定	137
IP アドレスの選択からの Cisco ISE への管理アクセスの許可	137
管理者アカウントのパスワード ポリシーの設定	138
管理者アカウントのアカウント無効化ポリシーの設定	139
管理者のセッション タイムアウトの設定	139
アクティブな管理セッションの終了	140
管理者の名前の変更	140
外部 ID ストアを使用した Cisco ISE への管理アクセス	141
外部認証および許可	141
外部認証のプロセス フロー	142
外部 ID ストアを使用したパスワード ベースの認証の設定	142
外部管理者グループの作成	142
外部管理者グループのメニュー アクセス権限とデータ アクセス権限の設定	143
外部管理者認証の RBAC ポリシーの作成	144
内部許可を伴う認証に対する外部 ID ストアを使用した管理アクセスの設定	144

第 7 章	Cisco ISE ライセンス	147
	Cisco ISE ライセンス	147
	従来のライセンス ファイルの管理	148
	Cisco ISE ライセンス モデル	149
	従来のライセンスの使用	152
	ライセンスの使用の表示	153
	登録解除されたライセンスの使用	154
	ライセンス ファイルの管理	155
	ライセンスの登録	155
	ライセンスの再ホスト	156
	ライセンスの更新	156
	ライセンスの移行およびアップグレード	156
	ライセンスの削除	157

第 8 章

証明書管理 159

Cisco ISE での証明書の管理 159

Cisco ISE によるセキュアなアクセスの提供を可能にする証明書 159

証明書の使用 160

Cisco ISE での証明書の一致 161

X.509 証明書の有効性 162

Cisco ISE での PKI の有効化 163

ワイルドカード証明書 164

Cisco ISE のワイルドカード証明書のサポート 165

HTTPS および EAP 通信用のワイルドカード証明書 165

URL リダイレクションの完全修飾ドメイン名 165

ワイルドカード証明書を使用する利点 166

ワイルドカード証明書を使用することの欠点 167

ワイルドカード証明書の互換性 168

証明書階層 168

システム証明書 169

システム証明書の表示 170

システム証明書のインポート 171

自己署名証明書の生成 172

システム証明書の編集 172

システム証明書の削除 173

システム証明書のエクスポート 174

信頼できる証明書ストア 175

信頼できる証明書ストアの証明書 176

信頼できる証明書の命名の制約 176

信頼できるストア証明書の表示 177

信頼できる証明書ストアの証明書のステータス変更 178

信頼できる証明書ストアへの証明書の追加 178

信頼できる証明書の編集 179

信頼できる証明書の削除 179

信頼できる証明書ストアからの証明書のエクスポート	180
信頼できる証明書ストアへのルート証明書のインポート	180
証明書チェーンのインポート	181
証明書署名要求	181
証明書署名要求の作成と認証局への CSR の送信	181
CSR への CA 署名付き証明書のバインド	182
証明書署名要求のエクスポート	183
Cisco ISE ノード間通信の信頼できる証明書のインストール	184
ポータルで使用する証明書のセットアップ	184
CA 署名付き証明書へのデフォルトのポータル証明書グループ タグの再割り当て	185
ノードの登録前のポータル証明書タグの関連付け	186
ユーザおよびエンドポイントの証明書の更新	187
ポリシー条件で証明書更新に使用されるディクショナリ属性	187
証明書更新用の許可ポリシー条件	188
証明書を更新するための CWA リダイレクト	188
ユーザによる証明書の更新を許可する Cisco ISE の設定	188
許可されるプロトコルの設定の更新	188
CWA リダイレクションの許可ポリシー プロファイルの作成	189
証明書を更新する許可ポリシー ルールの作成	190
ゲスト ポータルでの BYOD 設定の有効化	191
Apple iOS デバイスの証明書更新の失敗	191
Cisco ISE CA サービス	191
管理ノードとポリシー サービス ノードでプロビジョニングされる ISE CA 証明書	192
ISE CA チェーンの再生成	193
楕円曲線暗号化証明書のサポート	193
Cisco ISE 認証局証明書	195
Cisco ISE CA 証明書の編集	196
Cisco ISE CA 証明書のエクスポート	196
Cisco ISE CA 証明書のインポート	196
証明書テンプレート	197
証明書テンプレート名の拡張子	198

許可ポリシー条件での証明書テンプレート名の使用	198
pxGrid コントローラ用の Cisco ISE CA 証明書の展開	198
Simple Certificate Enrollment Protocol プロファイル	199
発行された証明書	200
Cisco ISE CA 証明書およびキーのバックアップと復元	200
Cisco ISE CA 証明書およびキーのエクスポート	201
Cisco ISE CA 証明書およびキーのインポート	202
プライマリ PAN および PSN でのルート CA および下位 CA の生成	203
外部 PKI の下位 CA としての Cisco ISE ルート CA の設定	203
証明書を使用してパーソナル デバイスを許可するための Cisco ISE の設定	204
Employee ユーザ グループへのユーザの追加	205
TLS ベース認証の証明書認証プロファイルの作成	206
TLS ベース認証の ID ソース順序の作成	206
認証局の設定	207
CA テンプレートの作成	208
クライアント プロビジョニング ポリシーで使用されるネイティブ サプリカント プロファイルの作成	210
Cisco サイトからの Windows および Mac OS X オペレーティング システムのエージェント リソースのダウンロード	211
Apple iOS、Android および MACOSX デバイスのクライアント プロビジョニング ポリシー ルールの作成	212
TLS ベース認証の Dot1X 認証ポリシー ルールの設定	213
中央 Web 認証とサプリカント プロビジョニング フローの許可プロファイルの作成	213
許可ポリシー ルールの作成	214
CA サービス ポリシーのリファレンス	215
証明書サービスのクライアント プロビジョニング ポリシー ルール	215
証明書サービスの許可プロファイル	216
証明書サービスの許可ポリシー ルール	217
ISE CA による ASA VPN ユーザへの証明書の発行	218
VPN 接続の証明書プロビジョニング フロー	219
ASA VPN ユーザに証明書を発行する Cisco ISE CA の設定	220
エンドポイント証明書の失効	223

OCSP サービス	224
Cisco ISE CA サービスの Online Certificate Status Protocol レスポнда	224
OCSP 証明書のステータスの値	225
OCSP ハイ アベイラビリティ	225
OCSP の障害	225
OCSP クライアント プロファイルの追加	226
OCSP 統計情報カウンタ	227

第 9 章

TACACS+ を使用したデバイス管理の制御	229
デバイス管理	229
イネーブル パスワードを変更するためのコマンドライン インターフェイスへのアクセス	230
デバイス管理ワーク センター	231
Cisco Secure ACS から Cisco ISE へのデータ移行	232
デバイス管理の展開設定	232
デバイス管理ポリシー セット	233
TACACS+ 認証設定と共有秘密	233
デバイス管理：許可ポリシーの結果	235
TACACS+ デバイス管理を許可された FIPS および非 FIPS モードの Protokol	236
TACACS+ コマンドセット	236
コマンドセットのワイルドカードと正規表現	236
コマンドラインおよびコマンドセットのリストの一致	236
複数のコマンドセットを持つルールの処理	238
TACACS+ プロファイル	238
共通タスク設定	239
TACACS+ コマンドセットの作成	242
TACACS+ プロファイルの作成	242
デバイス管理ポリシー セットの作成	243
デバイス管理アクティビティのモニタ	244
TACACS+ のグローバル設定	245

第 10 章

ネットワーク デバイスの管理 247

Cisco ISE のネットワーク デバイス定義	247
Cisco ISE でのデフォルトのネットワーク デバイス定義	248
Cisco ISE でのネットワーク デバイス定義の作成	249
Cisco ISE へのネットワーク デバイスのインポート	250
Cisco ISE からのネットワーク デバイスのエクスポート	250
Cisco ISE でのサードパーティ ネットワーク デバイスのサポート	251
ネットワーク デバイス プロファイル	254
Cisco ISE でのサードパーティ製ネットワーク デバイスの設定	256
ネットワーク デバイス プロファイルの作成	257
Cisco ISE からのネットワーク デバイス プロファイルのエクスポート	258
Cisco ISE へのネットワーク デバイス プロファイルのインポート	258
ネットワーク デバイス グループ (Network Device Groups)	259
ポリシー評価で Cisco ISE が使用するネットワーク デバイスの属性	260
Cisco ISE へのネットワーク デバイス グループのインポート	260
Cisco ISE からのネットワーク デバイス グループのエクスポート	261
Cisco ISE でのテンプレートのインポート	262
ネットワーク デバイスのインポート テンプレート形式	262
ネットワーク デバイス グループのインポート テンプレート形式	266
Cisco ISE-NAD 通信を保護する IPSec セキュリティ	267
Cisco ISE での RADIUS IPSec の設定	268
ESR-5921 での X.509 証明書の設定とインストール	271
例 : Cisco Catalyst 3850 での事前共有キー設定の出力	277
Mobile Device Manager と Cisco ISE との相互運用性	278
サポートされる MDM の使用例	280
サポートされる MDM サーバ	281
MDM サーバにより使用されるポート	282
MDM ディクショナリ属性	282
MDM 統合プロセス フロー	282
Cisco ISE による MDM サーバの設定	284

Cisco ISE への MDM サーバ証明書のインポート	285
ISE でのモバイル デバイス管理サーバの定義	285
Microsoft Intune および SCCM のための ISE MDM サポート	287
MDM サーバとしての Microsoft Intune の設定	289
Microsoft SCCM のポリシー設定の例	291
ISE 用の Microsoft SCCM サーバの設定	293
AD ユーザがドメイン管理グループに属しているときの権限の設定	293
AD ユーザがドメイン管理グループの一部ではない場合に必要な権限	293
ドメイン コントローラで DCOM を使用するための権限	295
WMI ルート/CIMv2 名前空間にアクセスするための権限の設定	296
AD ユーザがドメイン管理グループに属しているときの権限の設定	297
AD ユーザがドメイン管理グループの一部ではない場合に必要な権限	298
ドメイン コントローラで DCOM を使用するための権限	299
WMI ルート/CIMv2 名前空間にアクセスするための権限の設定	301
WMI アクセス用にファイアウォール ポートを開く	302
未登録のデバイスのリダイレクトのための許可プロファイルの設定	303
MDM 使用例の許可ポリシー ルールの設定	304
デバイスのワイプまたはロック	304
Mobile Device Manager のレポートの表示	305
Mobile Device Manager のログの表示	305

 第 11 章

リソースの管理 307

ディクショナリおよびディクショナリ属性	307
システム定義のディクショナリとディクショナリ属性	307
システム ディクショナリおよびディクショナリ属性の表示	308
ユーザ定義のディクショナリとディクショナリ属性	308
ユーザ定義のディクショナリの作成	309
ユーザ定義のディクショナリ属性の作成	309
RADIUS ベンダー ディクショナリ	310
RADIUS ベンダー ディクショナリの作成	310
RADIUS ベンダー ディクショナリ属性の作成	311

HP RADIUS IETF サービス タイプ属性 311

第 12 章

ロギング メカニズム 313

Cisco ISE ロギング メカニズム 313

ローカル ログの消去の設定 314

Cisco ISE システム ログ 314

ローカル ストア syslog メッセージの形式 315

リモート syslog メッセージの形式 316

リモート syslog 収集場所の設定 319

Cisco ISE メッセージ コード 320

メッセージ コードの重大度レベルの設定 320

Cisco ISE メッセージ カタログ 321

デバッグ ログ 321

ノードのロギング コンポーネントの表示 321

デバッグ ログの重大度レベルの設定 322

エンドポイントのデバッグ ログ コレクタ 322

特定のエンドポイントのデバッグ ログのダウンロード 323

収集フィルタ 323

収集フィルタの設定 324

イベント抑制バイパス フィルタ 324

第 13 章

バックアップ/復元操作 327

バックアップ データのタイプ 327

バックアップ/復元リポジトリ 328

リポジトリの作成 329

SFTP リポジトリでの RSA 公開キー認証の有効化 330

オンデマンドおよびスケジュール バックアップ 331

オンデマンド バックアップの実行 332

バックアップのスケジュール 334

CLI を使用したバックアップ 336

バックアップ履歴 336

バックアップの失敗	336
Cisco ISE 復元操作	337
データの復元に関するガイドライン	337
CLI からの設定またはモニタリング（操作）バックアップの復元	338
GUI からの設定バックアップの復元	341
モニタリング データベースの復元	341
スタンドアロン環境でのモニタリング（運用）バックアップの復元	342
管理およびモニタリングペルソナによるモニタリング バックアップの復元	342
モニタリング ペルソナによるモニタリング バックアップの復元	343
復元履歴	344
認証および許可ポリシー設定のエクスポート	344
分散環境でのプライマリ ノードとセカンダリ ノードの同期	345
スタンドアロンおよび分散展開での失われたノードの復元	345
分散展開での既存 IP アドレスとホスト名を使用しての失われたノードの復元	345
分散展開の新 IP アドレスとホスト名を使用しての失われたノードの復元	346
スタンドアロン展開の既存 IP アドレスとホスト名によるノードの復元	347
スタンドアロン展開の新 IP アドレスとホスト名によるノードの復元	347
設定のロールバック	348
分散展開での障害発生時のプライマリ ノードの復元	348
分散展開での障害発生時のセカンダリ ノードの復元	349
<hr/>	
第 14 章	適応型ネットワーク制御のセットアップ 351
Cisco ISE での適応型ネットワーク制御の有効化	351
ネットワーク アクセスの設定	351
隔離済みエンドポイントがポリシー変更の後に認証を更新しない	352
適応型ネットワーク制御	353
ANC によるネットワーク アクセスの許可プロファイルの作成	354
ANC によるネットワーク アクセスの例外ポリシーの作成	354
ANC 操作は IP アドレスまたは MAC アドレスが見つからない場合に失敗する	355
外部認証された管理者が ANC 操作を実行できない	355
ANC 隔離と隔離解除フロー	356

ANC NAS ポートのシャットダウン フロー 357

エンドポイントの消去の設定 357

第 IV 部 :

ユーザおよびエンドユーザ ポータルの管理 359

第 15 章

ユーザおよび外部 ID ソースの管理 361

Cisco ISE ユーザ 361

ユーザ ID 362

ユーザ グループ 362

ユーザ ID グループ 362

ユーザ ロール 362

ユーザ アカウントのカスタム属性およびパスワード ポリシー 363

ユーザおよび管理者用の自動パスワードの生成 367

ユーザの追加 367

Cisco ISE ユーザ データのエクスポート 368

Cisco ISE 内部ユーザのインポート 368

ユーザ ID グループの作成 369

ユーザ ID グループのエクスポート 369

ユーザ ID グループのインポート 370

外部 ID ソースを使用した許可ポリシーの作成 370

最大同時セッション数の設定 371

アカウント無効化ポリシー 373

個別のユーザ アカウントの無効化 373

グローバルにユーザ アカウントを無効にする 374

内部 ID ソースと外部 ID ソース 374

外部 ID ソースの作成 376

外部 ID ストア パスワードに対する内部ユーザの認証 377

証明書認証プロファイル 378

証明書認証プロファイルの追加 378

外部 ID ソースとしての Active Directory 379

Active Directory でサポートされる認証プロトコルおよび機能 379

許可ポリシーで使用する Active Directory 属性およびグループの取得	380
ブール属性のサポート	381
証明書ベース認証の Active Directory 証明書の取得	381
Active Directory ユーザ認証プロセス フロー	382
Active Directory マルチドメイン フォレストのサポート	382
Active Directory と Cisco ISE の統合の前提条件	382
さまざまな操作の実行に必要な Active Directory アカウント権限	383
通信用に開放するネットワーク ポート	384
DNS サーバ	384
外部 ID ソースとしての Active Directory の設定	385
Active Directory 参加ポイントの追加および参加ポイントへの Cisco ISE ノードの参加	386
ドメイン コントローラの追加	388
WMI の設定	388
Active Directory ドメインの脱退	389
認証ドメインの設定	390
Active Directory ユーザ グループの設定	390
Active Directory ユーザとマシンの属性の設定	391
パスワード変更、マシン認証、およびマシン アクセス制限の設定の変更	392
マシン アクセス制限 (MAR) キャッシュの維持	393
カスタム スキーマの設定	393
Active Directory の複数参加設定のサポート	393
Active Directory 参加ポイントを追加する新しい範囲の作成	394
ID 書き換え	395
ID 書き換えの有効化	396
ID 解決の設定	396
ID 解決問題の回避	397
ID 解決の設定	397
Active Directory 認証のためのユーザのテスト	398
Active Directory の設定の削除	399
ノードの Active Directory の参加の表示	399

Active Directory の問題の診断	400
Active Directory デバッグ ログの有効化	401
トラブルシューティング用の Active Directory ログ ファイルの入手	401
Active Directory のアラームおよびレポート	401
Active Directory の高度な調整	402
Active Directory アイデンティティ検索属性	402
Active Directory が構成された Cisco ISE をセットアップするための補足情報	403
Active Directory のグループ ポリシーの設定	404
Active Directory に対する EAP-TLS マシン認証のための Odyssey 5.X サブリカントの設定	405
マシン認証のための AnyConnect エージェント	405
Active Directory で Easy Connect および パッシブ ID サービス をサポートするための要件	406
パッシブ ID サービス の Active Directory の設定	406
Windows 監査ポリシーの設定	410
AD ユーザがドメイン管理グループに属しているときの権限の設定	411
AD ユーザがドメイン管理グループの一部ではない場合に必要な権限	411
ドメイン コントローラで DCOM を使用するための権限	412
WMI ルート/CIMv2 名前空間にアクセスするための権限の設定	414
AD ドメイン コントローラのセキュリティ イベント ログへのアクセス権の付与	415
Easy Connect	417
Easy Connect 適用モードの設定	421
Easy Connect 表示モードの設定	422
PassiveID ワーク センター	423
初期セットアップと設定	424
PassiveID ワーク センター ダッシュボード	425
プローブおよびプロバイダーとしての Active Directory	426
PassiveID セットアップの使用を開始する	427
Active Directory プロバイダーの管理	429
Active Directory の設定	429
その他のパッシブ ID サービスプロバイダー	433
Active Directory エージェント	436

Active Directory (AD) エージェントの自動インストールおよび展開	437
Active Directory (AD) エージェントの手動インストールおよび展開	438
エージェントのアンインストール	440
Active Directory (AD) エージェントの設定	440
API プロバイダー	441
パッシブ ID サービス の ISE REST サービスへのブリッジの設定	443
パッシブ ID REST サービスへの API コールの送信	444
API プロバイダーの設定	444
API コール	445
SPAN	447
SPAN の使用	447
SPAN 設定	448
syslog プロバイダー	449
syslog クライアントの設定	450
syslog メッセージ構造のカスタマイズ (テンプレート)	456
syslog 事前定義メッセージテンプレートの使用	462
パッシブ ID サービスのフィルタリング	474
エンドポイントプローブ	474
エンドポイントプローブの使用	476
エンドポイントプローブ設定	476
サブスクライバ	477
サブスクライバの pxGrid 証明書の生成	479
サブスクライバの有効化	480
ライブ ログからのサブスクライバ イベントの表示	481
サブスクライバの設定	481
PassiveID ワーク センター でのサービスのモニタリングとトラブルシューティング	481
LDAP	482
LDAP ディレクトリ サービス	482
複数の LDAP インスタンス	482
LDAP フェールオーバー	483
LDAP 接続管理	483

LDAP ユーザ認証	483
許可ポリシーで使用する LDAP グループおよび属性の取得	484
LDAP グループ メンバーシップ情報の取得	484
LDAP 属性の取得	485
LDAP 証明書の取得	486
LDAP サーバによって返されるエラー	486
LDAP ユーザ ルックアップ	487
LDAP MAC アドレス ルックアップ	487
LDAP ID ソースの追加	487
LDAP スキーマの設定	488
プライマリおよびセカンダリ LDAP サーバの設定	488
LDAP サーバからの属性を取得するための Cisco ISE の有効化	489
LDAP サーバからのグループ メンバーシップ詳細の取得	489
LDAP サーバからのユーザ属性の取得	490
LDAP ID ソースによるセキュア認証の有効化	490
ODBC ID ソース	491
ODBC データベースのクレデンシャル チェック	492
ODBC ID ソースの追加	497
RADIUS トークン ID ソース	499
RADIUS トークン サーバでサポートされる認証プロトコル	499
通信に RADIUS トークン サーバで使用するポート	499
RADIUS 共有秘密	499
RADIUS トークン サーバでのフェールオーバー	500
RADIUS トークン サーバの設定可能なパスワードプロンプト	500
RADIUS トークン サーバのユーザ認証	500
RADIUS トークン サーバのユーザ属性キャッシュ	500
ID 順序での RADIUS ID ソース	500
RADIUS サーバがすべてのエラーに対して同じメッセージを返す	501
Safeword サーバでサポートされる特別なユーザ名の形式	501
RADIUS トークン サーバでの認証要求と応答	502
RADIUS トークン サーバの追加	502

RADIUS トークン サーバの削除	504
RSA ID ソース	504
Cisco ISE と RSA SecurID サーバの統合	505
Cisco ISE の RSA 設定	505
RSA SecurID サーバに対する RSA エージェント認証	505
分散 Cisco ISE 環境の RSA ID ソース	505
Cisco ISE 展開の RSA サーバの更新	506
自動 RSA ルーティングの上書き	506
RSA ノード秘密リセット	506
RSA の自動可用性のリセット	506
RSA ID ソースの追加	507
RSA コンフィギュレーション ファイルのインポート	507
Cisco ISE サーバのオプション ファイルの設定および SecurID ファイルと sdstatus.12 ファイルのリセット	508
RSA ID ソースの認証制御オプションの設定	509
RSA プロンプトの設定	510
RSA メッセージの設定	510
外部 ID ソースとしての SAMLv2 ID プロバイダ	511
SAML ID プロバイダーの追加	512
ID プロバイダの削除	516
認証失敗ログ	516
ID ソース順序	517
ID ソース順序の作成	517
ID ソース順序の削除	518
レポートでの ID ソースの詳細	518
[認証 (Authentications)] ダッシュレット	519
ID ソース レポート	519

第 16 章

ゲスト アクセスの設定 521

Cisco ISE ゲスト サービス 521

分散環境のエンドユーザのゲスト ポータルとスポンサー ポータル 522

ゲスト アカウントとスポンサー アカウント	522
ゲスト タイプおよびユーザ ID グループ	523
ゲスト タイプの作成または編集	523
ゲスト タイプの無効化	527
ゲスト アカウント属性の変更	527
エンドポイント ユーザの最大同時ログイン数の設定	527
期限切れのゲスト アカウントを消去するスケジューリング設定	529
ゲスト アカウント作成用のカスタム フィールドの追加	530
電子メールでの通知用の電子メール アドレスおよび SMTP サーバの指定	531
ゲストのロケーションおよび SSID の割り当て	532
ゲスト パスワード ポリシーのルール	533
ゲスト パスワード ポリシーと有効期限の設定	534
ゲスト ユーザ名ポリシーのルール	535
ゲスト ユーザ名ポリシーの設定	535
SMS プロバイダーおよびサービス	536
ゲストに SMS 通知を送信するための SMS ゲートウェイの設定	537
ゲスト ポータル	538
ゲスト ポータルのクレデンシャル	539
ホットスポット ゲスト ポータルを使用したゲスト アクセス	540
クレデンシャルを持つゲスト ポータルを使用したゲスト アクセス	540
クレデンシャルを持つゲスト ポータルを使用した従業員アクセス	541
ゲスト デバイスのコンプライアンス	541
ゲスト ポータルの設定タスク	541
ポリシー サービスの有効化	543
ゲスト ポータルの証明書の追加	543
外部 ID ソースの作成	543
ID ソース順序の作成	545
エンドポイント ID グループの作成	545
ホットスポット ゲスト ポータルの作成	546
Sponsored-Guest ポータルの作成	547
アカウント登録ゲスト ポータルの作成	549

ポータル	許可	554
ゲスト	ポータルのカスタマイズ	556
	定期的な AUP 受け入れの設定	556
スポンサー	ポータル	556
	スポンサー ポータルでのゲスト アカウントの管理	557
	スポンサー アカウントの管理	558
	スポンサー アカウント作成のためのアカウント コンテンツの設定	564
スポンサー	ポータル フローの設定	565
	ポリシー サービスの有効化	566
	ゲスト サービスの証明書の追加	566
	外部 ID ソースの作成	566
	ID ソース順序の作成	567
	スポンサー ポータルの作成	568
	スポンサー ポータルのカスタマイズ	569
	スポンサー アカウント作成のためのアカウント コンテンツの設定	569
	スポンサーに対して使用可能な時間設定項目の設定	570
	スポンサーがスポンサー ポータルにログインできない	571
ゲストとスポンサー	のアクティビティのモニタ	572
	メトリック ダッシュボード	572
	AUP 受け入れステータス レポート	573
	ゲスト アカウンティング レポート	573
	マスター ゲスト レポート	573
	スポンサーのログインおよび監査レポート	574
	ゲストおよびスポンサー ポータルの監査ロギング	574
ゲスト	アクセス Web 認証オプション	574
	中央 WebAuth プロセス対応の NAD	575
	ローカル WebAuth プロセス対応のワイヤレス LAN コントローラ	577
	ローカル WebAuth プロセス対応の有線 NAD	578
	Login.html ページに必要な IP アドレスおよびポートの値	579
	NAD での HTTPS サーバの有効化	579
	NAD 上でのカスタマイズされた認証プロキシ Web ページのサポート	579

第 17 章

デバイス アクセスのサポート 583

NAD の Web 認証の設定	580
デバイス登録 WebAuth プロセス	581
企業ネットワークのパーソナル デバイス (BYOD)	583
分散環境のエンドユーザのデバイス ポータル	584
デバイス ポータルのグローバル設定	584
パーソナル デバイス ポータル	585
デバイス ポータルへのアクセス	585
ブラックリスト ポータル	586
証明書プロビジョニング ポータル	586
個人所有デバイスの持ち込みポータル	586
クライアント プロビジョニング ポータル	587
モバイル デバイス管理ポータル	587
デバイス ポータル	588
BYOD の展開オプションとステータス ワークフロー	588
ネイティブ サプリカントを使用したデバイス登録のサポート	592
ネイティブ サプリカントがサポートするオペレーティング システム	592
クレデンシャルを持つゲスト ポータルを使用したパーソナル デバイスの登録を従業員に許可	592
BYOD 登録に再接続する URL の提供	593
デバイス ポータルの設定タスク	593
ポリシー サービスの有効化	595
証明書の追加	595
外部 ID ソースの作成	596
ID ソース順序の作成	596
エンドポイント ID グループの作成	597
ブラックリスト ポータルの編集	598
BYOD ポータルの作成	600
クライアント プロビジョニング ポータルの作成	602
クライアント プロビジョニング ポータルの作成	603

MDM ポータルの作成	605
デバイス ポータルの作成	607
許可プロファイルの作成	608
許可プロファイルの作成	609
許可ポリシー ルールの作成	609
デバイス ポータルのカスタマイズ	610
従業員が追加するパーソナル デバイスの管理	610
従業員が追加したデバイスの表示	610
デバイスをデバイス ポータルに追加するときのエラー	611
デバイス ポータルから削除されたデバイスはエンドポイント データベースに残っている	611
デバイス ポータルおよびエンドポイント アクティビティのモニタ	611
デバイス ログインおよび監査レポート	612
登録済みエンドポイント レポート	612

第 18 章

エンドユーザ Web ポータルのカスタマイズ	613
エンドユーザ ポータル	613
エンドユーザ Web ポータルのカスタマイズ	613
ポータル コンテンツのタイプ	616
ポータルの基本的なカスタマイズ	617
ポータルのテーマ カラーの変更	618
ポータルの表示言語の変更	619
ポータルのアイコン、イメージ、およびロゴの変更	619
ポータルのバナーおよびフッター要素の更新	620
タイトル、手順、ボタン、およびラベル テキストの変更	621
テキスト ボックスの内容のフォーマットおよびスタイル	621
ポータル ページのカスタマイズ用の変数	622
カスタマイズの参照	626
カスタム ポータル ファイル	626
ポータルの高度なカスタマイズ	627
ポータルのカスタマイズの設定	628

ポータルテーマと構造 CSS ファイル	628
jQuery Mobile によるテーマ カラーの変更について	629
jQuery Mobile によるテーマ カラーの変更	631
ロケーションに基づくカスタマイズ	632
ユーザ デバイス タイプに基づくカスタマイズ	633
ポータルのデフォルト テーマ CSS ファイルのエクスポート	633
カスタム ポータルテーマ CSS ファイルの作成	634
ポータル コンテンツに組み込まれたリンク	634
動的なテキスト更新の変数の挿入	635
テキストをフォーマットし、リンクを含めるソース コードの使用	636
アドバタイズメントとしてのイメージの追加	638
カルーセル アドバタイジングの設定	639
ゲスト ロケーションに基づいたグリーティングのカスタマイズ	641
ユーザ デバイス タイプに基づいたグリーティングのカスタマイズ	642
ポータル ページのレイアウトの変更	643
カスタム ポータルテーマ CSS ファイルのインポート	646
カスタム ポータルテーマの削除	646
カスタマイズの参照	647
ポータル言語のカスタマイズ	648
言語ファイルのエクスポート	649
言語ファイルでの言語の追加または削除	650
更新された言語ファイルのインポート	650
ゲスト通知、承認、およびエラー メッセージのカスタマイズ	651
電子メールでの通知のカスタマイズ	652
SMS テキスト メッセージ通知のカスタマイズ	653
印刷通知のカスタマイズ	653
承認要求の電子メールでの通知のカスタマイズ	654
エラー メッセージの編集	655

第 19 章

ポリシー条件の設定 659

ポリシー条件 659

単純条件と複合条件 659

ポリシー評価 660

単純条件の作成 661

複合条件の作成 661

プロファイラ条件 662

プロファイラ条件の作成 663

ポスチャ条件 663

単純ポスチャ条件 664

単純ポスチャ条件の作成 664

複合ポスチャ条件 665

Windows クライアントでの自動アップデートを有効にするためのシスコ事前定義の条件
665

シスコ事前設定済みアンチウイルスおよびアンチスパイウェア条件 665

アンチウイルスとアンチスパイウェア サポート表 666

コンプライアンス モジュール 666

複合ポスチャ条件の作成 667

パッチ管理条件の作成 668

ディスク暗号化条件の作成 669

ネットワーク条件 669

エンドステーション ネットワーク条件の設定 671

デバイス ネットワーク条件の設定 671

デバイス ポート ネットワーク条件の設定 672

時刻と日付の条件の作成 672

第 20 章

認証ポリシーの管理 675

Cisco ISE 認証ポリシー 675

ポリシー条件の評価 676

サポートされている認証 プロトコル 676

サポートされる認証タイプおよびデータベース	677
認証失敗のタイプ：フェイルオーバー	677
認証ポリシーの用語	678
簡易認証ポリシー	678
簡易認証ポリシーのフロー	680
簡易認証ポリシー設定のガイドライン	681
ルールベースの認証ポリシー	681
ルールベースの認証ポリシー	682
ルールベースの認証ポリシーのサポート ディクショナリ	683
ディクショナリによってサポートされる属性	683
認証用の プロトコルの設定	686
認証プロトコルとして EAP-FAST を使用するためのガイドライン	686
EAP-FAST の設定	687
EAP-FAST の PAC の生成	687
認証プロトコルとしての EAP-TTLS の使用	688
EAP-TLS の設定	688
EAP-TLS の設定	689
PEAP の設定	689
RADIUS の設定	689
セキュリティ設定の構成	690
ネットワーク アクセス サービス	691
ネットワーク アクセスの許可されるプロトコルの定義	691
シスコ以外のデバイスからの MAB の有効化	693
シスコ デバイスからの MAB の有効化	694
ネットワーク アクセス ワーク センター	695
RADIUS プロキシ サーバとして機能する Cisco ISE	696
外部 RADIUS サーバの設定	697
RADIUS サーバ順序の定義	697
TACACS+ プロキシ クライアントとして機能する Cisco ISE	698
TACACS+ 外部サーバの設定	698
外部 TACACS+ サーバの設定	700

TACACS+ サーバ順序の設定	700
TACACS+ サーバ順序の定義	702
ロケーションに基づく認証	702
MSE サーバの追加	703
ロケーション ツリー	704
ポリシー モード	704
ポリシー モードの変更	705
簡易認証ポリシーの設定	706
ルールベースの認証ポリシーの設定	707
デフォルトの認証ポリシー	708
ポリシー セット	708
ポリシー セットの評価フロー	709
ポリシー セットの作成のガイドライン	710
グローバル許可例外ポリシー	710
ポリシー セットの設定	710
認証ポリシーの組み込み設定	711
認証結果の表示	714
認証ダッシュレット	715
認証レポートおよびトラブルシューティング ツール	715

第 21 章

許可ポリシーおよびプロファイルの管理	717
Cisco ISE の許可ポリシー	717
Cisco ISE の許可プロファイル	717
許可ポリシーの用語	718
ネットワーク許可	718
ポリシー要素	718
許可プロファイル	719
許可ポリシー	719
アクセス コントロール リスト	720
許可ポリシーとサポートされているディクショナリ	720
許可ポリシーおよびプロファイルの設定のガイドライン	721

デフォルトの許可ポリシー、ルール、プロファイルの設定	722
デフォルトの許可ルール	727
許可ポリシーの設定	728
許可ポリシーの属性および条件	729
時刻と日付の条件	730
許可ポリシーでの IPv6 属性の使用	730
許可プロファイルの権限	732
新しい標準許可プロファイルの権限の設定	733
ダウンロード可能 ACL (Downloadable ACLs)	733
ダウンロード可能 ACL に対する権限の設定	734
Active Directory ユーザ許可のためのマシン アクセス制限	734

第 22 章

脅威中心型 NAC サービスの設定	737
脅威中心型 NAC サービス	737
脅威中心型 NAC サービスの有効化	741
SourceFire FireAMP アダプタの追加	741
Cognitive Threat Analytics アダプタの追加	742
CTA アダプタの許可プロファイルの設定	744
Course of Action 属性を使用した許可ポリシーの設定	745
Cisco ISE での脆弱性アセスメントのサポート	746
脆弱性アセスメント サービスの有効化と設定	747
脅威中心型 NAC サービスの有効化	747
Qualys アダプタの設定	747
Nexpose アダプタの設定	751
Tenable アダプタの設定	754
認可プロファイルの設定	758
脆弱なエンドポイントを隔離する例外ルールの設定	759
脆弱性アセスメント ログ	759

第 23 章

スマート ライセンス サービスおよび Smart Call Home サービスの設定	761
Cisco ISE スマート ライセンス	761

ISE でのスマート ライセンスの有効化および登録	762
ISE のスマート ライセンスの管理	764
Smart Call Home	766
Smart Call Home プロファイル	766
Anonymous Reporting	766
Smart Call Home サービスの登録	767

第 24 章

Cisco ISE エンドポイント プロファイリング ポリシー	769
Cisco ISE プロファイリング サービス	770
プロファイラ ワーク センター	770
[プロファイラ (Profiler)] ダッシュボード	770
プロファイリング サービスを使用したエンドポイント インベントリ	771
Cisco ISE プロファイラ キュー制限の設定	771
Cisco ISE ノードでのプロファイリング サービスの設定	772
プロファイリング サービスによって使用されるネットワーク プローブ	773
IP アドレスと MAC アドレスのバインディング	773
NetFlow プローブ	774
DHCP プローブ	774
DHCP ブリッジ モードのワイヤレス LAN コントローラ設定	775
DHCP SPAN プローブ	775
HTTP プローブ	776
HTTP SPAN プローブ	776
VMware で実行中の Cisco ISE の HTTP 属性の収集の無効化	776
RADIUS プローブ	777
ネットワーク スキャン (NMAP) プローブ	777
NMAP の手動サブネット スキャンの SNMP 読み取り専用コミュニティ スtring	778
手動 NMAP スキャンの結果	778
DNS プローブ	779
DNS FQDN ルックアップ	779
WLC Web インターフェイスでの呼出端末 ID タイプの設定	780
SNMP クエリ プローブ	780

SNMP クエリに関する Cisco Discovery Protocol のサポート	781
SNMP クエリに関する Link Layer Discovery Protocol のサポート	781
SNMP トラップ プローブ	782
Active Directory プローブ	783
Cisco ISE ノードごとのプローブの設定	784
CoA、SNMP RO コミュニティおよびエンドポイント属性フィルタの設定	784
認証されたエンドポイントに対する許可変更のグローバル設定	785
許可変更の発行の使用例	786
許可変更の発行の免除	787
CoA 設定の各タイプに発行される許可変更	788
ISE データベースの持続性とパフォーマンスの属性フィルタ	788
ホワイトリストを使用してエンドポイント属性をフィルタリングするグローバル設定	789
IOS センサー組み込みスイッチからの属性の収集	791
IOS センサー組み込みネットワーク アクセス デバイス	791
IOS センサー組み込みネットワーク アクセス デバイスの設定チェックリスト	792
プロファイラ条件	793
Cisco NAC アプライアンスとの Cisco ISE 統合	794
管理ノードでの Cisco Clean Access Manager の設定	794
Cisco ISE プロファイラと Cisco Clean Access Manager の通信	794
Cisco Clean Access Manager の追加	795
プロファイラ条件の作成	796
エンドポイント プロファイリング ポリシー ルール	796
エンドポイント プロファイリング ポリシーの作成	797
エンドポイント プロファイリング ポリシーごとの許可変更の設定	799
エンドポイント プロファイリング ポリシーのインポート	800
エンドポイント プロファイリング ポリシーのエクスポート	800
事前定義されたエンドポイント プロファイリング ポリシー	801
アップグレード中に上書きされる事前定義されたエンドポイント プロファイリング ポリシー	802
エンドポイント プロファイリング ポリシーを削除できない	802
Draeger 医療機器用の事前定義済みプロファイリング ポリシー	803

不明なエンドポイントのエンドポイント プロファイリング ポリシー	803
静的に追加されたエンドポイントのエンドポイント プロファイリング ポリシー	804
スタティック IP デバイスのエンドポイント プロファイリング ポリシー	804
エンドポイント プロファイリング ポリシーの一致	804
許可に使用するエンドポイント プロファイリング ポリシー	805
エンドポイント プロファイリング ポリシーの論理プロファイルによるグループ化	805
論理プロファイルの作成	806
プロファイリング例外アクション	806
例外アクションの作成	807
ポリシーおよび ID グループのスタティック割り当てによるエンドポイントの作成	807
CSV ファイルからのエンドポイントのインポート	808
エンドポイントで使用可能なデフォルトのインポート テンプレート	810
インポート中の不明なエンドポイントの再プロファイリング	810
インポートされない無効な属性を持つエンドポイント	811
LDAP サーバからのエンドポイントのインポート	812
カンマ区切り形式ファイルを使用したエンドポイントのエクスポート	812
識別されたエンドポイント	813
識別されたエンドポイントの、ポリシー サービス ノード データベースへのローカル保存	814
クラスタのポリシー サービス ノード	814
エンドポイント ID グループの作成	815
プロファイラ フィード サービス	818
OUI フィード サービス	819
プロファイラ フィード サービスの設定	819
オフラインでのプロファイラ フィード サービスの設定	821
フィード更新の取り消し	823
プロファイラ レポート	823
エンドポイントの異常な動作の検出	824
異常な動作が発生しているエンドポイントに関する許可ポリシー ルールの設定	825
異常な動作が発生しているエンドポイントの表示	825
プロファイラ フィード サービス	826

OUI フィード サービス	827
プロファイラ フィード サービスの設定	827
オフラインでのプロファイラ フィード サービスの設定	829
オフライン更新プログラム パッケージのダウンロード	829
オフライン フィード更新の適用	830
プロファイルと OUI の更新に関する電子メール通知の設定	831
フィード更新の取り消し	831
プロファイラ レポート	831
エンドポイントの異常な動作の検出	832
異常な動作が発生しているエンドポイントに関する許可ポリシー ルールの設定	833
異常な動作が発生しているエンドポイントの表示	833
Cisco NAC アプライアンスとの Cisco ISE 統合	834
管理ノードでの Cisco Clean Access Manager の設定	834
Cisco ISE プロファイラと Cisco Clean Access Manager の通信	835
Cisco Clean Access Manager の追加	836
ポリシーおよび ID グループのスタティック割り当てによるエンドポイントの作成	836
CSV ファイルからのエンドポイントのインポート	837
エンドポイントで使用可能なデフォルトのインポート テンプレート	839
インポート中の不明なエンドポイントの再プロファイリング	839
インポートされない無効な属性を持つエンドポイント	840
LDAP サーバからのエンドポイントのインポート	841
カンマ区切り形式ファイルを使用したエンドポイントのエクスポート	841
識別されたエンドポイント	842
識別されたエンドポイントの、ポリシー サービス ノード データベースへのローカル保存	843
クラスタのポリシー サービス ノード	843
エンドポイント ID グループの作成	844
プロファイラ フィード サービス	847
OUI フィード サービス	848
プロファイラ フィード サービスの設定	848
オフラインでのプロファイラ フィード サービスの設定	850

フィード更新の取り消し	852
プロファイラ レポート	852
エンドポイントの異常な動作の検出	853
異常な動作が発生しているエンドポイントに関する許可ポリシー ルールの設定	854
異常な動作が発生しているエンドポイントの表示	854

第 25 章

クライアント プロビジョニングの設定 857

Cisco ISE でのクライアント プロビジョニングの設定	858
クライアント プロビジョニン リソース	859
シスコからのクライアント プロビジョニング リソースの追加	860
ローカル マシンからのシスコ提供のクライアント プロビジョニング リソースの追加	861
ローカル マシンからの AnyConnect 用の顧客作成リソースの追加	862
ネイティブ サプリカント プロファイルの作成	863
ネイティブ サプリカント プロファイルの設定	863
各種ネットワークでの URL リダイレクトなしでのクライアント プロビジョニング	865
AMP イネーブラ プロファイルの設定	867
組み込みプロファイル エディタを使用した AMP イネーブラ プロファイルの作成	869
スタンドアロン エディタを使用した AMP イネーブラ プロファイルの作成	870
一般的な AMP イネーブラ インストール エラーのトラブルシューティング	871
Cisco ISE の Chromebook デバイスのオンボーディングのサポート	872
共有環境での Chromebook デバイスの使用のベスト プラクティス	874
Chromebook オンボーディング プロセス	874
Google 管理コンソールでのネットワークの設定と拡張機能の強制	875
Chromebook オンボーディングのための ISE の設定	876
Chromebook デバイスのワイプ	877
Google 管理コンソールへの Chromebook の登録	878
BYOD オンボーディング用の Cisco ISE ネットワークへの Chromebook の接続	878
Google 管理コンソール : Wi-Fi ネットワーク設定	879
Cisco ISE での Chromebook デバイス アクティビティのモニタ	884
オンボーディング中の Chromebook デバイスのトラブルシューティング	884
AnyConnect 設定の作成	885

AnyConnect と Cisco NAC のエージェント プロファイルの作成	887
エージェント プロファイル設定のガイドライン	887
エージェントの動作の設定	888
サポートされる言語	893
クライアント IP アドレスのリフレッシュ設定	894
ポスチャ プロトコル設定	897
クライアント ログインセッションの基準	902
クライアント マシン上のエージェントのダウンロードの問題	902
Cisco NAC Agent MSI インストーラを使用したクライアント マシンのプロビジョニング	903
Cisco ISE ポスチャ エージェント	904
ポスチャ エージェントの検出要求と Cisco ISE 応答	904
Web Agent ポスチャの検出要求と Cisco ISE 応答	905
エージェントが「一時的なアクセス」を表示する	905
エージェントがポスチャ評価の開始に失敗する	906
AnyConnect	906
Cisco NAC Agent XML ファイルのインストール ディレクトリ	907
Windows クライアント用 Cisco NAC Agent	908
Windows 7 以前のクライアントからの Cisco NAC Agent のアンインストール	908
Windows 8 クライアントの Cisco NAC Agent のアンインストール	908
Windows 8 メトロおよびメトロ アプリケーションのサポート : Toast 通知	909
Macintosh クライアント用 Cisco NAC Agent	910
Macintosh クライアントからの Cisco NAC Agent のアンインストール	910
Cisco Web Agent	910
Cisco NAC Agent ログ	911
Cisco NAC Agent のエージェント カスタマイズ ファイルの作成	911
カスタム nac_login.xml ファイルのテンプレート	912
カスタム nacStrings_xx.xml ファイルのテンプレート	913
拡張 nacStrings_xx.xml ファイルのサンプル	922
UpdateFeed.xml ディスクリプタ ファイルのテンプレート	923
プロファイル作成機能を使用して生成された XML ファイルの例	924
クライアント プロビジョニング リソース ポリシーの設定	925

クライアントプロビジョニングポリシーの Cisco ISE ポスチャ エージェントの設定	927
パーソナルデバイスのネイティブ サプリカントの設定	927
クライアントプロビジョニング レポート	928
クライアントプロビジョニング イベント ログ	929

第 26 章

クライアント ポスチャ ポリシーの設定 931

ポスチャ サービス	932
ポスチャ サービスのコンポーネント	932
ポスチャおよびクライアントプロビジョニング ポリシー ワークフロー	934
ポスチャ サービス ライセンス	934
ポスチャ サービス展開	934
Cisco ISE でのポスチャ セッション サービスの有効化	935
ポスチャ評価レポートの実行	935
ポスチャ管理の設定	936
クライアントのタイマー設定	936
指定した時間内で修復するためのクライアントの修復タイマーの設定	937
クライアントの遷移のためのネットワーク遷移遅延タイマーの設定	937
ログイン成功ウィンドウを自動的に閉じる設定	937
非エージェント デバイスへのポスチャ ステータスの設定	938
ポスチャのリース	938
定期的再評価	939
定期的再評価の設定	939
Cisco ISE へのポスチャ更新のダウンロード	940
ポスチャ更新の自動ダウンロード	941
ポスチャ評価の利用規定の設定	941
ポスチャ条件	942
単純ポスチャ条件	942
単純ポスチャ条件の作成	943
複合ポスチャ条件	943
Windows クライアントでの自動アップデートを有効にするためのシスコ事前定義の条件	944
シスコ事前設定済みアンチウイルスおよびアンチスパイウェア条件	944

アンチウイルスとアンチスパイウェア サポート表	944
コンプライアンス モジュール	945
複合ポスチャ条件の作成	946
パッチ管理条件の作成	947
ディスク暗号化条件の作成	948
ポスチャ ポリシーの設定	948
ポスチャ評価オプション	949
ポスチャ修復オプション	950
ポスチャのカスタム条件	951
カスタム ポスチャ修復アクション	952
ファイル修復の追加	952
リンク修復の追加	952
パッチ管理修復の追加	953
アンチウイルス修復の追加	953
アンチスパイウェア修復の追加	954
プログラム修復起動の追加	954
プログラム修復起動のトラブルシューティング	955
Windows Update 修復	955
Windows Update 修復の追加	956
Windows Server Update Services 修復の追加	956
ポスチャ評価要件	957
非準拠状態でスタックしたクライアント システム	958
クライアントのポスチャ要件の作成	959
ポスチャのカスタム権限	959
標準許可ポリシーの設定	960
ステルス モードの展開	961
ポスチャ ポリシーと要件タイプへのステルス モードの影響	962
ポスチャとネットワーク ドライブ マッピングのベスト プラクティス	965
AnyConnect クライアントレス モード ワークフロー	965
AnyConnect エージェント プロファイルの作成	966
AnyConnect パッケージの AnyConnect 設定の作成	966

Cisco ISE へのオープン DNS プロファイルのアップロード	967
クライアント プロビジョニング ポリシーの作成	967
ポスチャ条件の作成	968
ポスチャ修復の作成	968
クライアントレス モードでのポスチャ要件の作成	968
ポスチャ ポリシーの作成	969

第 27 章

Cisco TrustSec ポリシーの設定 971

TrustSec アーキテクチャ	971
TrustSec のコンポーネント	972
TrustSec の用語	974
TrustSec のサポートされるスイッチと必要なコンポーネント	975
TrustSec ダッシュボード	975
メトリック	976
現在のネットワーク ステータス	976
アクティブな SGT セッション	976
アラーム	977
クイック ビュー	977
ライブ ログ	978
TrustSec のグローバル設定	978
TrustSec マトリックスの設定	979
TrustSec デバイスの設定	980
OOB TrustSec PAC	980
[設定 (Settings)] 画面からの TrustSec PAC の生成	980
[ネットワーク デバイス (Network Devices)] 画面からの TrustSec PAC の生成	981
[ネットワーク デバイス リスト (Network Devices List)] 画面からの TrustSec PAC の生成	982
[プッシュ (Push)] ボタン	982
TrustSec AAA サーバの設定	982
セキュリティ グループの設定	983
セキュリティ グループの追加	984

Cisco ISE へのセキュリティ グループのインポート	984
Cisco ISE からのセキュリティ グループのエクスポート	985
IP SGT スタティック マッピングの追加	985
Cisco ISE への IP SGT スタティック マッピングのインポート	986
Cisco ISE からの IP SGT スタティック マッピングのエクスポート	987
SGT マッピング グループの追加	987
セキュリティ グループ アクセス コントロール リストの追加	988
出力ポリシー (Egress Policy)	989
送信元ツリー ビュー	990
宛先ツリー ビュー	990
マトリクス ビュー	991
マトリクスの次元	992
マトリクスのインポート/エクスポート	992
カスタム ビューの作成	992
マトリクス操作	993
ワーク プロセスの設定	993
[マトリックス登録 (Matrices Listing)] ページ	995
TrustSec マトリックス ワークフロー プロセス	996
出力ポリシー テーブル セルの設定	1005
出力ポリシー セルのマッピングの追加	1005
出力ポリシーのエクスポート	1006
出力ポリシーのインポート	1006
出力ポリシーの SGT の設定	1007
モニタ モード	1008
モニタ モードの機能	1008
不明セキュリティ グループ	1008
デフォルト ポリシー	1009
[プッシュ (Push)] ボタン	1009
SGT の割り当て	1009
NDAC 許可	1010
NDAC 許可の設定	1010

エンドユーザの許可の設定	1011
TrustSec の設定およびポリシー プッシュ	1012
CoA でサポートされるネットワーク デバイス	1012
非 CoA サポート デバイスへの設定変更のプッシュ	1013
SSH キーの検証	1013
環境 CoA 通知のフロー	1014
環境 CoA トリガー	1015
SGACL コンテンツ更新のフロー	1017
SGACL 名前付きリストの更新 CoA の開始	1018
ポリシーの更新 CoA 通知のフロー	1019
SGT マトリクスの更新 CoA のフロー	1019
出力ポリシーからの、SGT マトリクスの更新 CoA の開始	1020
TrustSec CoA の概要	1021
セキュリティ グループ タグの交換プロトコル	1022
SXP デバイスの追加	1023
SXP ドメイン フィルタの追加	1024
SXP の設定	1025
TrustSec-ACI 統合	1026
ACI の設定	1027
ユーザ レポート別上位 N 個の RBACL ドロップの実行	1028

第 VI 部 : Cisco ISE のモニタリングおよびトラブルシューティング 1031

第 28 章	モニタリングおよびトラブルシューティング	1033
	Cisco ISE のモニタリングとトラブルシューティング サービス	1033
	Cisco ISE ダッシュボード	1034
	NPF イベント フロー プロセス	1038
	モニタリングおよびトラブルシューティング機能のユーザ ロールと権限	1038
	モニタリング データベースに格納されているデータ	1038
	モニタリングのためのデバイス設定	1039
	プロファイラ フィードのトラブルシューティング	1039

ポスチャ コンプライアンス	1039
ポスチャ コンプライアンスのチェック	1040
Cisco ISE プロセスをモニタする SNMP トラップ	1040
Cisco ISE アラーム	1042
アラーム設定	1064
カスタム アラームの追加	1065
Cisco ISE アラーム通知およびしきい値	1066
アラームの有効化および設定	1066
モニタリング用の Cisco ISE アラーム	1066
モニタリング アラームの表示	1067
ログ収集 (Log Collection)	1067
アラーム syslog 収集場所	1067
ライブ認証	1068
ライブ認証のモニタ	1068
[ライブ認証 (Live Authentications)] ページでのデータのフィルタリング	1069
エンドポイントのグローバル検索	1070
エンドポイントのセッションのトレース	1071
ディレクトリからのセッションの削除	1073
認証概要レポート	1073
ネットワーク アクセスの問題のトラブルシューティング	1074
診断トラブルシューティング ツール	1074
RADIUS 認証のトラブルシューティング ツール	1074
予期せぬ RADIUS 認証結果のトラブルシューティング	1075
ネットワーク デバイス ツールの実行	1075
設定を確認する IOS show コマンドの実行	1075
設定バリデータ ツールの評価	1076
ネットワーク デバイス設定の問題のトラブルシューティング	1076
ポスチャのトラブルシューティング ツール	1076
エンドポイント ポスチャの障害のトラブルシューティング	1076
セッション トレース テスト ケース	1077
セッション トレース テスト ケースの設定	1077

高度なトラブルシューティングのテクニカル サポートのトンネル	1078
テクニカル サポート トンネルの確立	1079
着信トラフィックを検証する TCP ダンプ ユーティリティ	1080
ネットワーク トラフィックのモニタリングでの TCP ダンプの使用	1080
TCP ダンプ ファイルの保存	1081
エンドポイントまたはユーザの予期しない SGACL の比較	1082
出力ポリシー診断フロー	1082
SXP-IP マッピングを持つ TrustSec 対応ネットワークの接続問題のトラブルシューティング	1083
IP-SGT マッピングを持つ TrustSec 対応ネットワークの接続問題のトラブルシューティング	1083
デバイス SGT ツール	1084
デバイス SGT マッピングの比較による TrustSec 対応ネットワークの接続問題のトラブルシューティング	1084
モニタリング ノードからのエンドポイント統計データのダウンロード	1084
その他のトラブルシューティング情報の入手	1085
Cisco ISE のサポート バンドル	1085
サポート バンドル	1086
Cisco ISE ログ ファイルのダウンロード	1086
Cisco ISE デバッグ ログ	1088
デバッグ ログの入手	1088
Cisco ISE コンポーネントおよび対応するデバッグ ログ	1088
デバッグ ログのダウンロード	1090
モニタリング データベース	1091
モニタリング データベースのバックアップと復元	1091
モニタリング データベースの消去	1091
モニタリング データベースの消去に関するガイドライン	1092
運用データの消去	1092
古い運用データの消去	1093
第 29 章 レポート	1095
Cisco ISE レポート	1095

レポート フィルタ	1096
クイック フィルタ条件の作成	1096
拡張フィルタ条件の作成	1097
レポートの実行および表示	1098
レポートのナビゲーション	1098
レポートのエクスポート	1098
レポートのスケジュールと保存	1100
Cisco ISE のアクティブな RADIUS セッション	1100
RADIUS セッションの許可の変更	1101
使用可能なレポート	1103

第 VII 部 :

参照 1129

第 30 章

管理のユーザ インターフェイスのリファレンス 1131

システム管理	1131
展開設定	1131
展開のノード リスト ページ	1131
ノードの一般設定	1133
プロファイリング ノードの設定	1142
証明書ストアの設定	1146
自己署名証明書の設定	1147
証明書署名要求の設定	1148
発行および失効した証明書	1154
証明書定期チェックの設定	1155
システム証明書のインポート設定	1156
[信頼できる証明書ストア (Trusted Certificate Store)] ページ	1157
証明書設定の編集	1158
信頼できる証明書のインポート設定	1161
OCSP クライアント プロファイル設定	1162
内部 CA の設定	1165
証明書テンプレートの設定	1166

ログgingsの設定	1167
リモート ログgings ターゲツツの設定	1168
ログgings カテゴリの設定	1169
メンテナンスの設定	1171
リポジトリの設定	1171
オンデマンド バックアップの設定	1172
スケジュール バックアップの設定	1173
管理者アクセスの設定	1174
管理者パスワード ポリシーの設定	1175
セッション タイムアウトおよびセッション情報の設定	1179
設定	1179
ポストチャの全般設定	1180
ポストチャ再評価の構成設定	1181
ポストチャの利用規定の構成設定	1183
EAP-FAST 設定	1186
EAP-FAST の PAC の生成の設定	1186
EAP-TTLS 設定	1188
EAP-TLS 設定	1189
PEAP 設定	1189
RADIUS 設定	1190
一般 TrustSec の設定	1193
TrustSec マトリックスの設定	1196
SMS ゲートウェイ設定 (SMS Gateway Settings)	1198
DHCP および DNS サービス	1201
ID の管理	1205
エンドポイント	1205
エンドポイント設定	1205
エンドポイントの、LDAP からのインポートの設定	1208
グループ (Groups)	1211
エンドポイント ID グループの設定	1211
外部 ID ソース	1211

LDAP ID ソースの設定	1211
RADIUS トークン ID ソースの設定	1221
RSA SecurID ID ソースの設定	1223
ID の管理の設定	1225
ユーザ認証ポリシーの設定	1225
ネットワーク リソース	1227
ネットワーク デバイス	1227
ネットワーク デバイス定義の設定	1227
デフォルトのネットワーク デバイス定義の設定	1240
デバイス セキュリティ設定	1244
ネットワーク デバイスのインポート設定	1244
ネットワーク デバイス グループ (Network Device Groups)	1245
ネットワーク デバイス グループの設定	1245
ネットワーク デバイス グループのインポート設定	1246
ネットワーク デバイス プロファイル設定	1248
外部 RADIUS サーバの設定	1256
RADIUS サーバ順序	1258
NAC マネージャの設定	1260
デバイス ポータルの管理	1261
デバイス ポータルの設定	1261
デバイス ポータルのグローバル設定	1261
デバイス ポータルのポータル ID 設定	1262
ブラックリスト ポータルのポータル設定	1263
BYOD と MDM ポータルのポータル設定	1266
BYOD ポータルの BYOD 設定	1268
証明書プロビジョニング ポータルのポータル設定	1270
クライアント プロビジョニング ポータルのポータル設定	1274
MDM ポータルの従業員のモバイル デバイス管理設定	1277
デバイス ポータルのポータル設定	1278
デバイス ポータルのログイン ページ設定	1281
デバイス ポータルの利用規定 (AUP) ページ設定	1282

デバイス ポータルのポストログイン バナー ページ設定	1283
デバイス ポータルの従業員によるパスワード変更の設定	1283
デバイス ポータルのデバイス管理設定	1284
デバイス ポータルのデバイス カスタマイズの追加、編集、および検索	1286
デバイス ポータルのサポート情報ページの設定	1287
脅威中心型 NAC サービス	1288
新しいベンダー インスタンスの追加	1288

第 31 章

ゲスト アクセスのユーザ インターフェイスのリファレンス 1291

ゲスト ポータル設定	1291
ポータル ID 設定	1291
ホットスポット ゲスト ポータルのポータル設定	1292
ホットスポット ゲスト ポータルの利用規定 (AUP) ページ設定	1295
ホットスポット ポータルのポストアクセス バナー ページ設定	1296
クレデンシャルを持つゲスト ポータルのポータル設定	1296
クレデンシャルを持つゲスト ポータルのログイン ページ設定	1299
アカウント登録ページの設定 (Self-Registration Page Settings)	1300
アカウント登録成功ページの設定	1304
クレデンシャルを持つゲスト ポータルの利用規定 (AUP) ページ設定	1305
クレデンシャルを持つゲスト ポータルのゲストによるパスワード変更の設定	1306
クレデンシャルを持つゲスト ポータルのゲスト デバイス登録の設定	1306
クレデンシャルを持つゲスト ポータルの BYOD 設定	1307
クレデンシャルを持つゲスト ポータルのポストログイン バナー ページ設定	1309
クレデンシャルを持つゲスト ポータルのゲスト デバイスのコンプライアンス設定	1309
ゲスト ポータルの VLAN DHCP リリース ページ設定	1310
ゲスト ポータルの認証成功の設定	1311
ゲスト ポータルのサポート情報ページの設定	1311
スポンサー ポータル アプリケーションの設定	1313
ポータル ID 設定	1313
スポンサー ポータルのポータル設定	1314
スポンサー ポータルのログイン設定	1318

スポンサー ポータルの利用規定（AUP）設定	1318
スポンサー ポータルのスポンサーのパスワード変更設定	1319
スポンサー ポータルのポストログイン バナー設定	1319
スポンサー ポータルのサポート情報ページの設定	1320
スポンサー ポータルのゲストへの通知のカスタマイズ	1321
スポンサー ポータルのカスタマイズの管理と承認	1322
グローバル設定（Global Settings）	1322
ゲストおよびスポンサー ポータルのグローバル設定	1322
ゲスト タイプの設定	1323
スポンサー グループ設定	1326

第 32 章

Web ポータルのカスタマイズのリファレンス 1331

ポータル ページのタイトル、コンテンツおよびラベルの文字数制限	1331
ポータル ページのタイトル、コンテンツおよびラベルの文字数制限	1331
ポータルのカスタマイズ	1333
エンドユーザ ポータルのページ レイアウトの CSS クラスと説明	1334
ポータル言語ファイルの HTML サポート	1335
ブラックリスト ポータルの言語ファイルの HTML サポート	1336
個人所有デバイスの持ち込みポータルの言語ファイルの HTML サポート	1336
証明書プロビジョニング ポータルの言語ファイルの HTML サポート	1337
クライアント プロビジョニング ポータルの言語ファイルの HTML サポート	1338
クレデンシャル ゲスト ポータルの言語ファイルの HTML サポート	1339
ホットスポット ゲスト ポータルの言語ファイルの HTML サポート	1342
モバイル デバイス管理ポータルの言語ファイルの HTML サポート	1343
デバイス ポータルの言語ファイルの HTML サポート	1344
スポンサー ポータルの言語ファイルの HTML サポート	1345

第 33 章

ポリシーのユーザ インターフェイスのリファレンス 1349

認証	1349
簡易認証ポリシーの構成設定	1349
ルールベースの認証ポリシーの構成設定	1350

許可ポリシーの設定	1356
エンドポイント プロファイリング ポリシーの設定	1358
UDID 属性を使用するエンドポイント コンテキストの可視性	1365
Dictionaries	1366
条件	1368
プロファイラ条件の設定	1368
ポスチャ条件の設定	1369
ファイル条件の設定	1369
ファイアウォール条件の設定	1376
レジストリ条件の設定	1377
継続的なエンドポイント属性モニタリング	1378
アプリケーション条件の設定	1379
サービス条件の設定	1381
ポスチャ複合条件の設定	1383
ウイルス対策条件の設定	1384
アンチスパイウェア複合条件の設定	1387
マルウェア対策条件の設定	1389
ディクショナリ単純条件の設定	1393
ディクショナリ複合条件の設定	1393
パッチ管理条件の設定	1395
ディスク暗号化条件の設定	1397
USB 条件の設定	1399
時刻と日付の条件の設定	1399
結果	1400
許可されるプロトコル	1400
PAC オプション	1417
許可プロファイルの設定	1421
プロファイリング例外アクションの設定	1427
ファイル修復	1428
ファイアウォール修復	1428
リンク修復	1430

アプリケーション修復	1431
マルウェア対策修復	1435
アンチウイルス修復	1436
アンチスパイウェア修復	1437
プログラム修復起動	1438
Windows Update 修復	1440
Windows Server Update Services 修復	1442
パッチ管理修復	1445
USB 大容量ストレージのチェックのワークフロー	1448
USB 大容量ストレージ修復	1448
クライアントのポスチャ要件	1449

第 34 章

操作のユーザ インターフェイスのリファレンス 1451

RADIUS ライブ ログ	1451
RADIUS ライブ セッション	1454
TACACS ライブ ログ	1459
診断ツール	1461
RADIUS 認証のトラブルシューティングの設定	1461
ネットワーク デバイス コマンドの実行の設定	1463
設定バリデータの評価の設定	1463
ポスチャのトラブルシューティングの設定	1464
TCP ダンプの設定	1465
SXP-IP マッピング	1467
IP ユーザ SGT	1469
デバイス SGT の設定	1469
進行状況の詳細の設定	1471
結果概要 (Results Summary)	1472

第 35 章

ネットワーク アクセス フロー 1475

パスワード ベースの認証	1475
暗号化されたパスワードと暗号化技術を使用したセキュアな認証	1475

認証方式と許可特権	1476
Cisco ISE の RADIUS プロトコルのサポート	1476
ユーザのネットワーク アクセス	1476
EAP を使用しない RADIUS ベースのプロトコル	1477
RADIUS-Based Non-EAP 認証フロー	1477
パスワード認証プロトコル	1477
Cisco ISE の RADIUS-Based PAP 認証	1478
チャレンジ ハンドシェイク 認証プロトコル	1478
Microsoft Challenge Handshake Authentication Protocol Version 1	1478
Microsoft Challenge Handshake Authentication Protocol Version 2	1479
RADIUS ベースの EAP プロトコル	1479
RADIUS-Based EAP 認証フロー	1479
Extensible Authentication Protocol-Message Digest 5	1480
Lightweight Extensible Authentication Protocol	1480
保護拡張認証プロトコル	1481
PEAP の使用の利点	1481
PEAP プロトコルでサポートされているサブリカント	1481
PEAP プロトコルのフロー	1481
Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling	1482
EAP-FAST の利点	1483
EAP-FAST フロー	1483

第 36 章

Cisco ISE の機能をサポートするために必要なスイッチとワイヤレス LAN コントローラの設定
1485

スイッチでの標準 Web 認証のサポートの有効化	1486
代理 RADIUS トランザクション用のローカル ユーザ名とパスワードの定義	1486
ログとアカウントिंगのタイムスタンプの正確性を保証するための NTP サーバ設定	1486
AAA 機能を有効にするコマンド	1486
スイッチ上の RADIUS サーバの設定	1487
RADIUS 許可変更 (CoA) を有効にするコマンド	1488
デバイス トラッキングと DHCP スヌーピングを有効にするコマンド	1488
802.1X ポートベースの認証を有効にするコマンド	1489

クリティカルな認証の EAP を有効にするコマンド	1489
リカバリ遅延を使用して AAA 要求をスロットリングするコマンド	1489
適用状態に基づく VLAN の定義	1489
スイッチのローカル（デフォルト）ACL 定義	1490
802.1X および MAB のスイッチ ポートを有効にする	1492
EPM ログイングを有効にするコマンド	1494
SNMP トラップを有効にするコマンド	1494
プロファイリング用の SNMP v3 クエリーを有効にするコマンド	1494
プロファイラによる収集を可能にするための MAC 通知トラップを有効にするコマンド	1495
スイッチ上での RADIUS Idle-timeout の設定	1495
iOS サプリカント プロビジョニングのためのワイヤレス LAN コントローラ設定	1496
MDM Interoperability のためのワイヤレス LAN コントローラでの ACL の設定	1496

第 37 章

Cisco ISE でサポートされる管理情報ベース 1499

IF-MIB	1499
SNMPv2-MIB	1500
IP-MIB	1500
CISCO-CDP-MIB	1501
CISCO-VTP-MIB	1502
CISCO-STACK-MIB	1502
BRIDGE-MIB	1502
OLD-CISCO-INTERFACE-MIB	1502
CISCO-LWAPP-AP-MIB	1503
CISCO-LWAPP-DOT11-CLIENT-MIB	1504
CISCO-AUTH-FRAMEWORK-MIB	1505
EEE8021-PAE-MIB: RFC IEEE 802.1X	1505
HOST-RESOURCES-MIB	1506
LLDP-MIB	1506

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2017–2021 Cisco Systems, Inc. All rights reserved.



第 Ⅰ 部

はじめに

- [Cisco ISE の機能](#) (1 ページ)
- [管理者ポータルでの移動](#) (17 ページ)
- [Wireless Setup について](#) (37 ページ)



第 1 章

Cisco ISE の機能

- Cisco ISE の概要 (2 ページ)
- 主要な機能 (2 ページ)
- ID ベースのネットワーク アクセス (3 ページ)
- 複数の展開シナリオのサポート (3 ページ)
- UCS ハードウェアのサポート (4 ページ)
- 基本的なユーザ認証および許可 (4 ページ)
- ポリシー セット (5 ページ)
- FIPS 140-2 の実装 (5 ページ)
- Common Access Card 機能のサポート (6 ページ)
- クライアント ポスチャ評価 (7 ページ)
- ゲストのネットワーク アクセス (8 ページ)
- パーソナル デバイスのサポート (8 ページ)
- Mobile Device Manager と Cisco ISE との相互運用性 (8 ページ)
- ネットワークのプロファイリングされたエンドポイント (8 ページ)
- pxGrid ペルソナ (9 ページ)
- TrustSec ワーク センター (9 ページ)
- TACACS+ デバイス管理 (9 ページ)
- SXP のサポート (10 ページ)
- サードパーティ デバイスのサポート (10 ページ)
- テレメトリ (11 ページ)
- IPv6 のサポート (11 ページ)
- ロケーションに基づく認証 (12 ページ)
- Cisco ISE 認証局 (12 ページ)
- Active Directory マルチドメイン フォレストのサポート (13 ページ)
- SAnet デバイスのサポート (13 ページ)
- 複数のハードウェアおよび VMware プラットフォームへのインストールのサポート (14 ページ)
- 外部 ID ソースとしての ID プロバイダ (14 ページ)
- 管理ノードの自動フェールオーバーのサポート (14 ページ)

- [GUI ベースのアップグレード \(15 ページ\)](#)
- [高度なトラブルシューティングのテクニカル サポートのトンネル \(15 ページ\)](#)

Cisco ISE の概要

Cisco ISE はネットワーク リソースへのセキュアなアクセスを提供するセキュリティ ポリシー 管理プラットフォームです。Cisco ISE はポリシー デシジョン ポイントとして動作し、企業におけるコンプライアンスの遵守、インフラストラクチャのセキュリティの向上、およびサービス オペレーションの合理化を可能にします。企業は、Cisco ISE を使用して、ネットワーク、ユーザ、およびデバイスから状況情報をリアルタイムで収集できます。その後、管理者はその情報を使用して、ガバナンス上の決定を下すことができます。これを行うには、ID をアクセス スイッチ、ワイヤレス LAN コントローラ (WLC)、バーチャル プライベート ネットワーク (VPN) ゲートウェイ、データセンタースイッチなどのさまざまなネットワーク要素に結び付けます。Cisco ISE は、Cisco TrustSec ソリューションのポリシー マネージャとして機能し、TrustSec ソフトウェアによって定義されたセグメンテーションをサポートします。

ISE コミュニティ リソース

ISE コミュニティに[参加](#)して、リソースを参照し、質問を投稿し、ディスカッションに参加しましょう。[ISE 製品マニュアル](#)、[ISE の概要](#)、[YouTube ビデオ](#)、[デモ](#)、[機能と統合のデモ](#)、[トレーニング リソース](#)を参照してください。

(注) ISE コミュニティ リソースで提供される例やスクリーンショットは、旧リリースの Cisco ISE のものである可能性があります。新しい機能、追加の機能、更新については、GUI を確認してください。

主要な機能

Cisco ISE は、既存の Cisco ポリシー プラットフォームで利用できる機能のスーパーセットを組み込む、統合されたポリシーベースのアクセス制御システムです。Cisco ISE では次の機能が実行されます。

- 認証、許可、アカウンティング (AAA)、ポスチャ、およびプロファイラを1つのアプリケーションに結合します。
- Cisco ISE 管理者、認可されたスポンサー管理者、またはその両方向けの、包括的なゲスト アクセス管理を提供します。
- 包括的なクライアントプロビジョニングの方法を提供し、802.1X 環境など、ネットワークにアクセスするすべてのエンドポイントのデバイスポスチャを評価することによって、エンドポイントのコンプライアンスを強化します。
- ネットワーク上のエンドポイントデバイスの検出、プロファイリング、ポリシーベースの配置、モニタリングのサポートを提供します。

- 集中型展開および分散型展開においてポリシーの一貫性が維持され、サービスを必要な場所に配信できるようになります。
- セキュリティ グループ タグ (SGT) およびセキュリティ グループ アクセス コントロール リスト (SGACL) を使用した TrustSec などの高度な適用機能を利用します。
- 小さな事務所から大企業まで様々な環境の展開シナリオに対応するスケーラビリティをサポートします。
- ワーク センターを介して TACACS 対応デバイスの管理を容易にします。[ワークセンター (Work Center)] メニューには、すべてのデバイス管理ページが含まれており、ISE 管理者の単一の始点として機能します。ただし、[ユーザ (Users)]、[ユーザIDグループ (User Identity Groups)]、[ネットワークデバイス (Network Devices)]、[デフォルトのネットワークデバイス (Default Network Devices)]、[ネットワークデバイスグループ (Network Device Groups)]、[認証 (Authentication)] および [許可条件 (Authorization Conditions)] などのページは、他のメニュー オプションと共有されます。

ID ベースのネットワーク アクセス

Cisco ISE ソリューションでは、次の領域で、コンテキストに対応した ID 管理が提供されます。

- Cisco ISE は、許可され、ポリシーに準拠したデバイスからユーザがネットワークにアクセスしているかどうかを確認します。
- Cisco ISE は、コンプライアンスとレポーティングに使用できる、ユーザの ID、ロケーション、およびアクセス履歴を確認します。
- Cisco ISE は、割り当て済みのユーザ ロール、グループ、関連付けられたポリシー（ジョブ ロール、ロケーション、デバイス タイプなど）に基づいてサービスを割り当てます。
- Cisco ISE は、認証結果に基づいて、ネットワークの特定のセグメントへのアクセスと、特定のアプリケーションおよびサービスへのアクセスのいずれかまたは両方を、認証されたユーザに許可します。

複数の展開シナリオのサポート

Cisco ISE は企業インフラストラクチャ全体に展開することが可能で、802.1X 有線、無線、およびバーチャルプライベート ネットワーク (VPN) がサポートされます。

Cisco ISE アーキテクチャでは、1 台のマシンがプライマリ ロール、もう 1 台の「バックアップ」マシンがセカンダリ ロールとなる環境において、スタンドアロン展開と分散（別名「ハイアベイラビリティ」または「冗長」）展開の両方がサポートされます。Cisco ISE は、個別の設定可能なペルソナ、サービス、およびロールを特徴としており、これらを使用して、Cisco ISE サービスを作成し、ネットワーク内の必要な箇所に適用できます。これにより、フル機能を備え統合されたシステムとして動作する包括的な Cisco ISE 展開が実現します。

Cisco ISE ノードは、1 つ以上の管理ペルソナ、モニタリング ペルソナ、およびポリシー サービス ペルソナとして展開できます。各ペルソナは、ネットワーク ポリシー管理トポロジ内の異なる部分で重要な役割を担います。Cisco ISE を管理ペルソナとしてインストールすると、集中型ポータルからネットワークを設定および管理することによって、効率と使いやすさを向上させることができます。

UCS ハードウェアのサポート

Cisco ISE 2.0 は、次のハードウェア プラットフォームをサポートしています。

- SNS-3415 (小)
- SNS-3495 (大)

ハードウェアの仕様については、『[Cisco Identity Services Engine Data Sheet](#)』の表 3 を参照してください。

基本的なユーザ認証および許可

Cisco ISE のユーザ認証ポリシーを使用すると、パスワード認証プロトコル (PAP)、チャレンジ ハンドシェイク認証プロトコル (CHAP)、保護拡張認証プロトコル (PEAP)、拡張認証プロトコル (EAP) などのさまざまな標準認証プロトコルを使用して、多くのユーザログインセッションタイプに対応した認証を提供できます。Cisco ISE では、ユーザが認証を試みるネットワーク デバイスで使用するプロトコル、およびユーザ認証の検証元となる ID ソースが指定されます。

Cisco ISE では、許可ポリシーの範囲内で広範な可変要素が許可されるため、許可されたユーザのみが、ネットワークにアクセスしたときに目的のリソースにアクセスできます。Cisco ISE の最初のリリースでは、RADIUS によって管理された、内部ネットワークとそのリソースへのアクセスのみがサポートされます。

最も基本的なレベルにおいて、Cisco ISE では、802.1X、MAC 認証バイパス (MAB)、およびブラウザベースの Web 認証ログインが、有線ネットワークと無線ネットワークの両方を介した基本的なユーザ認証およびアクセスに対してサポートされます。認証要求を受信すると、認証ポリシーの「外側部分」を使用して、要求の処理に使用できる一連のプロトコルが選択されます。その後、認証ポリシーの「内側部分」を使用して、要求の認証に使用する ID ソースが選択されます。ID ソースは、特定の ID ストア、またはユーザが最終的な許可応答を受信するまでアクセス可能な一連の ID を一覧表示する ID ストア順序で構成できます。

認証が成功すると、セッションフローは許可ポリシーに進みます。(認証が成功しなかった場合でも Cisco ISE に許可ポリシーの処理を許可するオプションも提供されます)。Cisco ISE を使用すると、「認証失敗」、「ユーザが見つからない」、および「プロセスの失敗」に対する動作を設定できます。また、要求を拒否またはドロップ (応答は発行されません) するか、許可ポリシーに進むかを判断することもできます。Cisco ISE が許可の実行に進む場合、

「NetworkAccess」ディクショナリの「AuthenticationStatus」属性を使用して、認証結果を許可ポリシーの一部として組み込むことができます。

許可ポリシーの結果として、Cisco ISE によって割り当てられる許可プロファイルには、ネットワーク ポリシー適用デバイス上のトラフィック管理を指定する、ダウンロード可能な ACL が含まれる場合があります。このダウンロード可能な ACL では、認証中に返される RADIUS 属性が指定され、この属性により、Cisco ISE で認証されると付与されるユーザアクセス権限が定義されます。



(注) Cisco ISE は、着信アカウントリング パケットの認証セッションを識別しながら、次の順序で属性を処理します。

- シスコ デバイスの場合：
 1. クラス/状態
 2. audit-session-id
- サード パーティ製のデバイスの場合：
 1. クラス/状態
 2. Calling-Station-ID
 3. 認証セッションを識別できない場合、Cisco ISE は Calling-Station-ID、NAS-Port、および NAS-IP-Address に基づいて新しいセッション ID を作成します。

ポリシー セット

Cisco ISE では、認証ポリシーおよび許可ポリシーのセットをグループ化できるポリシー セットがサポートされます。認証および許可ルールフラットなリストである基本的な認証および許可ポリシーモデルとは対照的に、ポリシーセットでは、設定、展開、およびトラブルシューティングがより簡単になるように、組織の IT ビジネス事例をポリシー グループまたはサービス (VPN や 802.1x など) に論理的に定義できます。

ポリシー セットを [ポリシー (Policy)] メニューでできるようにするには、[管理 (Administration)] > [システム (System)] > [設定 (Settings)] > [ポリシー設定 (Policy Settings)] でポリシー セットを有効にする必要があります。

FIPS 140-2 の実装

Cisco ISE では、連邦情報処理標準 (FIPS) 140-2 共通基準 EAL2 へのコンプライアンスがサポートされます。FIPS 140-2 は暗号モジュールとして使用されている米国政府のコンピュータセキュリティ標準です。Cisco ISE は、FIPS 140-2 実装ガイダンスのセクション G.5 ガイドラインに従って認可済みの C3M および Cisco ACS NSS モジュールを使用した組み込み FIPS 140-2 実装を使用しています。

また、FIPS 標準では、特定のアルゴリズムの使用が制限されます。この標準を適用するには、Cisco ISE で FIPS の動作を有効にする必要があります。Cisco ISE では、RADIUS 共有秘密およびキー管理手法を経由した FIPS 140-2 へのコンプライアンスが有効になり、証明書の SHA-256 暗号化および復号化機能が提供されます。FIPS モードでは、非 FIPS 準拠のアルゴリズムを使用した機能の試行がすべて失敗するほか、このような特定の認証機能が無効になります。

ISE にインストールされている証明書で使用されている暗号化方式が FIPS でサポートされていない場合には、証明書を再発行する必要があります。Cisco ISE で FIPS モードを有効にすると、次の機能が影響を受けます。

- IEEE 802.1X 環境
 - EAP-Flexible Authentication via Secure Tunneling (EAP-FAST)
 - EAP-Transport Layer Security (EAP-TLS)
 - PEAP
 - RADIUS



(注) EAP-Message Digest 5 (EAP-MD5)、Lightweight Extensible Authentication Protocol (LEAP)、PAP など、その他のプロトコルは FIPS 140-2 に準拠したシステムと互換性がなく、Cisco ISE が FIPS モードのときは無効になります。ゲスト アクセスの従来の方法である、ローカル Web 認証 (LWA) は PAP を使用し、Cisco ISE が FIPS モードのときには動作しません。しかし、FIPS モードが有効な Cisco ISE 展開は、MAC 認証バイパス (MAB) の許可されているプロトコルの「ホスト参照」を使用することがあり、したがって中央 Web 認証 (CWA) でアクセスできるようになると推測されます。

- Secure Shell (SSH) クライアントは SSHv2 のみを使用できる
- Lightweight Directory Access Protocol (LDAP) over Secure Sockets Layer (SSL)

Common Access Card 機能のサポート

Cisco ISE は、Common Access Card (CAC) 認証デバイスを使用して自身を認証する米国政府ユーザをサポートします。CAC とは、内蔵の電子チップに X.509 クライアント証明書が記録された身分証明バッジであり、この証明書によって、米国国防総省 (DoD) などの特定の 1 人の職員が識別されます。CAC によるアクセスには、カードを挿入し PIN を入力するカードリーダーが必要です。カードからの証明書が Windows の証明書ストアに転送されます。Windows の証明書ストアは、Cisco ISE などのローカル ブラウザで実行されているアプリケーションで使用可能です。

CAC カードを使用して認証を行うことの利点は、次のとおりです。

- Common Access Card X.509 証明書は、802.1X EAP-TLS 認証の ID ソースです。
- Common Access Card X.509 証明書は、Cisco ISE 管理に対する認証および許可用の ID ソースでもあります。

Cisco ISE は、管理者ポータルへのログインのみをサポートします。次のアクセス方法では、CAC 認証はサポートされません。

- Cisco ISE コマンドライン インターフェイスの管理に CAC 認証ログインは使用できません。
- 外部の REST API（モニタリングおよびトラブルシューティング）とエンドポイント保護 サービス適応型ネットワーク制御 API では、CAC 認証はサポートされません。
- ゲスト サービスとゲスト スポンサー管理からのアクセスでは、Cisco ISE 内での CAC 認証はサポートされません。

クライアント ポスチャ評価

Cisco ISE を使用すると、適用されたネットワーク セキュリティ対策の適切さと効果を維持するために、保護されたネットワークにアクセスする任意のクライアントマシンに対してセキュリティ機能を検証し、そのメンテナンスを行うことができます。Cisco ISE 管理者は、クライアントマシンで最新のセキュリティ設定またはアプリケーションを使用できるように設計されたポスチャ ポリシーを使用することによって、どのクライアント マシンでも、企業ネットワークへのアクセスについて定義されたセキュリティ標準を満たし、その状態を継続することを保証できます。ポスチャ コンプライアンス レポートによって、ユーザがログインしたとき、および定期的再評価が行われるたびに、クライアントマシンのコンプライアンス レベルのスナップショットが Cisco ISE に提供されます。

ポスチャ評価およびコンプライアンスは、Cisco ISE で提供される次のいずれかのエージェント タイプを使用して行われます。

- Cisco NAC Web Agent : ログイン時にユーザがシステムにインストールする一時的なエージェントであり、ログインセッションが終了すると、クライアント マシンには表示されなくなります。
- Cisco NAC Agent : 一度インストールすると、Windows または Mac OS X クライアント マシン上で維持される永続的なエージェントであり、セキュリティ コンプライアンスに関するすべての機能を実行できます。
- AnyConnect ISE Agent : Windows または Mac OS X クライアントにインストールできる永続的なエージェントであり、ポスチャ コンプライアンス機能を実行します。

ゲストのネットワーク アクセス

ゲスト スポンサーとして Cisco ISE ゲスト登録ポータルへの適切なアクセスが付与されている Cisco ISE 管理者および従業員は、一時的なゲスト ログイン アカウントを作成し、使用可能なネットワーク リソースを指定して、ゲスト、訪問者、請負業者、コンサルタント、顧客に、指定されたネットワーク リソースおよびインターネットへの制限付きアクセスを許可することができます。ゲスト アクセス セッションには有効期限タイマーが関連付けられるため、ゲスト アクセスを特定の日付や期間に制限できます。

ゲスト ユーザーセッションのすべての側面（アカウントの作成と停止を含む）は追跡され、Cisco ISE に記録されるため、必要に応じて監査情報を提供したり、セッションアクセスのトラブルシューティングを行うことができます。

パーソナル デバイスのサポート

Cisco ISE では、従業員はラップトップ コンピュータ、携帯電話、タブレット、プリンタ、およびその他のネットワーク デバイスなど、自分のパーソナル デバイスを企業ネットワークに接続することができます。

これらのデバイスをサポートするとネットワーク サービスおよびエンタープライズ データの保護が難しくなるため、従業員とそれらのデバイスの両方をネットワーク アクセスに対して認証および許可できるようにする必要があります。Plus ライセンスの場合、Cisco ISE では、従業員が自分のパーソナル デバイスを企業ネットワーク上でセキュアに使用するために必要なツールを提供します。

Mobile Device Manager と Cisco ISE との相互運用性

モバイルデバイス管理 (MDM) サーバはモバイル事業者、サービスプロバイダー、企業にわたって展開されたモバイルデバイスの保護、モニタ、管理、およびサポートを行います。MDM はエンドポイントにポリシーを適用しますが、ユーザにデバイスの登録や、修復を強制することはできません。ISE は MDM サーバからポリシーを取得し、ユーザが自分のデバイスを登録したときにそれらのポリシーを適用します。ISE デバイス ポリシーで MDM を必要とし、デバイスが MDM に準拠していない場合、ISE はユーザを MDM オンボーディング ポータルにリダイレクトし、ネットワークにアクセスするためにデバイスを更新するようユーザに求めます。ISE では、MDM コンプライアンスに従っていないユーザに対してインターネット アクセスのみを許可することもできます。

ネットワークのプロファイリングされたエンドポイント

プロファイラ サービスは、ネットワーク上にあるすべてのエンドポイントの機能（Cisco ISE では ID とも呼ばれる）を、デバイス タイプにかかわらず識別、検索、および特定して、企業

ネットワークへの適切なアクセスを保証および維持するのに役立ちます。Cisco ISE プロファイラ機能では、さまざまなプローブを使用して、ネットワーク上にあるすべてのエンドポイントの属性を収集し、それらを既知のエンドポイントが関連ポリシーおよび ID グループに従って分類されるプロファイラ アナライザに渡します。

プロファイラ フィード サービスによって、管理者は、新規および更新されたエンドポイント プロファイリング ポリシーや更新された OUI データベースを、指定された Cisco フィード サーバからの、サブスクリプションを介した Cisco ISE へのフィードとして取得できます。

pxGrid ペルソナ

Cisco pxGrid は、Cisco ISE セッションディレクトリから Cisco Adaptive Security Appliance (ASA) などの他のポリシー ネットワーク システムへのコンテキスト ベースの情報の共有を有効にするために使用されます。pxGrid フレームワークは、ポリシー データや設定データをノード間で交換するためにも使用できます (たとえば、ISE とサードパーティベンダー間でのタグやポリシーオブジェクトの共有)。また、脅威情報など、非 ISE 関連情報の交換用にも使用できます。

TrustSec ワーク センター

すべての TrustSec 関連のオプションは、[TrustSec ワークセンター (TrustSec Work Center)] メニュー ([ワークセンター (Work Centers)] > [TrustSec]) の下に統合されており、管理者は 1 つの場所ですべての TrustSec オプションに簡単にアクセスできます。

TrustSec ダッシュボードは、TrustSec ネットワークの一元化されたモニタリング ツールです。[メトリック (Metrics)] ダッシュレットには、TrustSec ネットワークの動作に関する統計情報が表示されます。[アクティブな SGT セッション (Active SGT Sessions)] ダッシュレットには、ネットワークで現在アクティブな SGT セッションが表示されます。[アラーム (Alarms)] ダッシュレットには、TrustSec セッション関連のアラームが表示されます。[クイックビュー (Quick View)] ダッシュレットには、NAD および SGT の TrustSec 関連情報が表示されます。

アクティブな TrustSec セッションを表示するには、[ライブログ (Live Log)] ダッシュレットの [TrustSec セッション (TrustSec Sessions)] リンクをクリックします。また、NAD から Cisco ISE への TrustSec プロトコル データ要求と応答に関する情報を表示することもできます。

TACACS+ デバイス管理

Cisco ISE は、ネットワーク デバイスの設定を制御および監査するための Terminal Access Controller Access-Control System (TACACS+) のセキュリティ プロトコルを使用したデバイス管理をサポートしています。ネットワーク デバイスは、デバイス管理者の操作の認証および認可のために ISE にクエリを行うために設定され、ISE のアカウンティング メッセージを送信して操作をログに記録します。これによって、どのネットワーク デバイスに誰がアクセスできて関連するネットワーク設定を変更できるかについて、きめ細かい制御が容易になります。ISE

管理者は、コマンドセットやシェルプロファイルなどの TACACS 結果をデバイス管理アクセス サービスの許可ポリシー ルールで選択できるようにするポリシー セットを作成できます。ISE モニタリング ノードでは、デバイス管理に関する高度なレポートが提供されます。[ワークセンター (Work Center)] メニューには、すべてのデバイス管理ページが含まれており、ISE 管理者の単一の始点として機能します。

ISE には、TACACS+ を使用するためのデバイス管理ライセンスが必要です。

SXP のサポート

リソース グループ タグ (SGT) の交換プロトコル (SXP) は、TrustSec のハードウェア サポートがないネットワーク デバイスに SGT を伝播するために使用されます。SXP は、ある SGT 対応ネットワーク デバイスから別のデバイスに IP アドレスとともにエンドポイントの SGT を転送するために使用されます。

ノードで SXP サービスをイネーブルにするには、[ノードの一般設定 (General Node Settings)] ページで [SXP サービスの有効化 (Enable SXP Service)] チェックボックスをオンにします。また、SXP サービスに使用するインターフェイスを指定する必要があります。

各 SXP 接続には、SXP スピーカーとして指定されたピアと、SXP リスナーとして指定されたピアがあります。ピアは双方向モードで設定することもでき、そのモードでは、それぞれがスピーカーとリスナーの両方として機能します。接続はいずれかのピアによって開始できますが、マッピング情報は常にスピーカーからリスナーに伝播されます。

サードパーティ デバイスのサポート

Cisco ISE は、ネットワーク デバイス プロファイルを使用して、一部のサードパーティ製ネットワーク アクセス デバイス (NAD) をサポートします。これらのプロファイルによって、ゲスト、BYOD、MAB、ポスチャなどのフローを有効にするために Cisco ISE が使用する機能が定義されます。

Cisco ISE には、次のベンダーからのネットワーク デバイスの定義済みプロファイルが含まれています。

- シスコ：有線および無線
- Aruba：無線
- HP：有線および無線
- Motorola：無線
- Brocade：有線
- Alcatel：有線
- Ruckus：無線

また、定義済みプロファイルがないその他のサードパーティ製ネットワークデバイス用のプロファイルを作成することもできます。AnyConnect クライアントのプロビジョニングとポスチャ検出では、CoA と URL のリダイレクションは必須ではありません。

リリース 2.0 以前のシスコ以外の NAD を展開し、それらを使用するようにポリシー ルール/RADIUSディクショナリを作成した場合、これらはアップグレード後に通常どおりに機能し続けます。

テレメトリ

インストール後、管理者ポータルに初めてログインすると、Cisco ISE テレメトリ バナーが画面に表示されます。この機能を使用して、Cisco ISE は、ユーザの展開、ネットワーク アクセスデバイス、プロファイラ、およびユーザが使用している他のサービスに関する非機密情報を安全に収集します。収集されたデータは、今後のリリースでよりよいサービスと追加機能を提供するために使用されます。デフォルトでは、テレメトリ機能は有効になっています。管理者ポータルからディセーブルにすることができます。

IPv6 のサポート

Cisco ISE リリース 2.0 は、次の IPv6 機能をサポートしています。

- IPv6 対応エンドポイントのサポート：Cisco ISE は、エンドポイントからの IPv6 トラフィックを検出、管理、保護できます。IPv6 属性を使用して、IPv6 対応エンドポイントからの要求を処理し、エンドポイントが準拠していることを保証するための、許可プロファイルおよびポリシーを Cisco ISE で設定できます。
- レポートでの IPv6 サポート：リリース 2.0 のレポートは IPv6 の値をサポートしています。ライブ セッションおよびライブ認証ページもまた IPv6 の値をサポートしています。
- CLI での IPv6 サポート：リリース 2.0 は次の CLI コマンドで IPv6 をサポートしています。
 - `ipv6 address`：ネットワーク インターフェイスごとにスタティック IPv6 アドレス設定を許可する場合
 - `ipv6 enable`：すべてのネットワーク インターフェイスで IPv6 を有効化または無効化する場合
 - `ipv6 route`：IPv6 スタティック ルートを設定する場合
 - `ip host`：ホストのローカル テーブルでの IPv6 アドレスの追加を許可する場合
 - `show IPv6 route`：IPv6 ルートを表示する場合

これらのコマンドの詳細については、『[Cisco Identity Services Engine CLI Reference Guide](#)』を参照してください。

ロケーションに基づく認証

Cisco ISE は、Cisco モビリティ サービス エンジン (MSE) と統合し、物理ロケーション ベースの認証を導入します。Cisco ISE は、MSE からの情報を使用して、MSE によって報告される ユーザの実際の位置に基づいて差別化されたネットワーク アクセスを提供します。

この機能を使用すると、エンドポイントのロケーション情報を使用して、ユーザが適切なゾーンにいる場合にネットワーク アクセスを提供できます。また、エンドポイントのロケーションをポリシーの追加属性として追加して、デバイスのロケーションに基づいてより詳細なポリシー許可のセットを定義することもできます。次のように、ロケーションベースの属性を使用する許可ルール内で条件を設定できます。

MSE.Location Equals LND_Campus1:Building1:Floor2:SecureZone

ロケーション階層 (キャンパス/ビルディング/フロア構造) を定義して、Cisco Prime Infrastructure のアプリケーションを使用してセキュアおよび非セキュアのゾーンを設定できます。ロケーション階層を定義した後、ロケーション階層データを MSE サーバと同期する必要があります。

ロケーション ツリーは、MSE インスタンスから取得されたロケーション データを使用して作成されます。ロケーション ツリーを使用して、許可ポリシーに公開するロケーション エントリを選択できます。

Cisco ISE 認証局

Cisco ISE は、一元的なコンソールからエンドポイントのデジタル証明書を発行および管理して、従業員が自分のパーソナルデバイスを使用して企業のネットワークに接続できるようにするネイティブの認証局 (CA) を提供します。Cisco ISE CA は、スタンドアロンおよび下位の展開をサポートします。

証明書プロビジョニング ポータル

Cisco ISE では証明書プロビジョニング ポータルが提供され、そこで従業員はオンボーディングフローを通過できないデバイスについて証明書を要求することができます。たとえば、販売時点管理端末などのデバイスは、BYOD フローを通過できず、証明書を手動で発行する必要があります。証明書プロビジョニングポータルで、権限のある一連のユーザは、そのようなデバイスに対する証明書要求をアップロードし、キーペアを生成し (必要に応じて)、証明書をダウンロードできます。従業員は、このポータルにアクセスして、1 つの証明書について要求を行うか、または CSV ファイルを使用して一括証明書要求を行うことができます。

証明書テンプレートの拡張子

Cisco ISE の内部 CA には、エンドポイント証明書を作成するために使用された証明書テンプレートを表す拡張子が含まれています。内部 CA によって発行されたすべてのエンドポイント証明書には、証明書テンプレート名の拡張子が含まれています。この拡張子は、そのエンドポ

イント証明書を作成するために使用された証明書テンプレートを表します。CERTIFICATE: テンプレート名属性を許可ポリシーの条件に使用して、評価の結果に基づいて適切なアクセス権限を割り当てることができます。

Cisco ISE 内部 CA は ASA VPN ユーザに証明書を発行します

内部 ISE CA は、ASA VPN 経由で接続するクライアントマシンに証明書を発行できます。ISE は、Simple Certificate Enrollment Protocol (SCEP) を使用して登録を行い、証明書を Cisco ISE からクライアントマシンにプロビジョニングします。

Active Directory マルチドメイン フォレストのサポート

Cisco ISE では、マルチドメイン フォレストの Active Directory がサポートされます。Cisco ISE は単一のドメインに接続しますが、Cisco ISE が接続されているドメインと他のドメイン間に信頼関係が確立されている場合は、Active Directory フォレストの他のドメインからリソースにアクセスできます。

SAnet デバイスのサポート

Cisco ISE は、セッション認識型ネットワーク (SAnet) が限定的にサポートされます。SAnet は、可視性、認証、許可などのアクセスセッションの管理における一貫性と柔軟性を高める、スイッチのセッション管理フレームワークです。SAnet は、デバイスだけでなく、ISE の両方によって受け入れられる許可オブジェクトであるサービステンプレートの概念を定義します。このことは、デバイスに送信される前に属性のリストにマージされ、フラット化される RADIUS 許可属性のコンテナである Cisco ISE 許可プロファイルと矛盾します。同様に、SAnet サービス テンプレートも RADIUS 許可属性のコンテナですが、デバイスに送信する前にリストにフラット化されません。代わりに、Cisco ISE はサービス テンプレートの名前を送信し、デバイスはキャッシュされたか、または静的に定義されたバージョンがまだない場合コンテンツ (RADIUS 属性) をダウンロードします。さらに、サービス テンプレートの定義が変更された、つまり、RADIUS 属性が追加、削除、または変更された場合、Cisco ISE はデバイスに CoA 通知を送信します。

Cisco ISE は、許可プロファイルを「サービス テンプレート」互換としてマークする特別なフラグを含む許可プロファイルとして、サービステンプレートを実装します。このように、許可プロファイルでもあるサービステンプレートは、SAnet 対応デバイスと同時にレガシーデバイスから接続するセッションをサポートする単一のポリシーステートメントで 사용할 ことができます。

複数のハードウェアおよび VMware プラットフォームへのインストールのサポート

Cisco ISE は、さまざまなパフォーマンス上の特徴を備えた広い範囲の物理アプライアンスにあらかじめインストールされた状態で提供されます。Cisco Application Deployment Engine (ADE) と Cisco ISE ソフトウェアは、専用の SNS-3400 シリーズ アプライアンスまたは仮想マシン (Cisco ISE VM) のいずれかで実行されます。Cisco ISE ソフトウェア イメージでは、この専用プラットフォームにその他のパッケージまたはアプリケーションをインストールできません。Cisco ISE が本来備えている拡張性によってアプライアンスを展開に追加し、必要に応じてパフォーマンスと復元力を向上させることができます。

外部 ID ソースとしての ID プロバイダ

Cisco ISE は、次のポータルで SAML シングルサインオン (SSO) をサポートしています。

- ゲスト ポータル (スポンサー付きおよびアカウント登録)
- スポンサー ポータル
- デバイス ポータル
- 証明書プロビジョニング ポータル

Oracle Access Manager や Oracle Identity Federation などの ID プロバイダをポータルの外部 ID ソースとして追加できます。ID プロバイダは、ユーザ クレデンシャルを保管、検証し、ユーザがポータルにアクセスできる SAML 応答を生成します。異なるユーザ名とパスワードの組み合わせを入力する必要がなくなるため、パスワードの劣化が軽減します。

管理ノードの自動フェールオーバーのサポート

Cisco ISE は、管理ペルソナの自動フェールオーバーをサポートしています。自動フェールオーバー機能をイネーブルにするには、分散セットアップで少なくとも 2 つのノードが管理ペルソナを引き継ぎ、1 つのノードが非管理ペルソナを引き継ぐ必要があります。プライマリ管理ノード (PAN) がダウンした場合は、セカンダリ管理ノードの自動プロモーションが開始されます。この場合、非管理セカンダリ ノードが各管理ノードのヘルス チェック ノードとして指定されます。ヘルス チェック ノードは、設定された間隔で PAN の正常性を確認します。PAN の正常性について受信されたヘルス チェック 応答がダウンまたは到達不能により良好でない場合、ヘルス チェック ノードは、設定されたしきい値まで待機した後、プライマリ ロールを引き継ぐようにセカンダリ管理ノードのプロモーションを開始します。セカンダリ管理ノードの自動フェールオーバー後に使用できなくなる機能がいくつかあります。Cisco ISE は、元の PAN へのフォールバックをサポートしていません。詳細については、「Cisco ISE ノードの展開」の章の「管理ノードのハイ アベイラビリティ」の項を参照してください。

GUI ベースのアップグレード

Cisco ISE では、管理者ポータルから GUI ベースの一元化されたアップグレードが提供されます。アップグレードプロセスはさらに簡素化され、アップグレードの進行状況およびノードのステータスが画面に表示されます。



-
- (注) GUI ベースのアップグレードは、リリース 2.0 からそれ以降のリリースにアップグレードする場合、または Cisco ISE 2.0 の限定提供リリースを一般提供リリースにアップグレードする場合にのみ適用できます。
-

高度なトラブルシューティングのテクニカルサポートのトンネル

Cisco ISE は、Cisco IronPort トンネル インフラストラクチャを使用して、展開内の ISE サーバに接続してシステムの問題をトラブルシューティングするための、シスコ テクニカル サポート エンジニア用のセキュア トンネルを作成します。Cisco ISE は SSH を使用して、トンネル経由のセキュアな接続を作成します。管理者として、トンネルアクセスを制御できます。サポート エンジニアにアクセス権を付与する時期と期間を選択できます。シスコ カスタマー サポートは、ユーザの介入なしにトンネルを確立できません。サービスログインに関する通知を受信します。任意の時点でトンネル接続をディセーブルにできます。



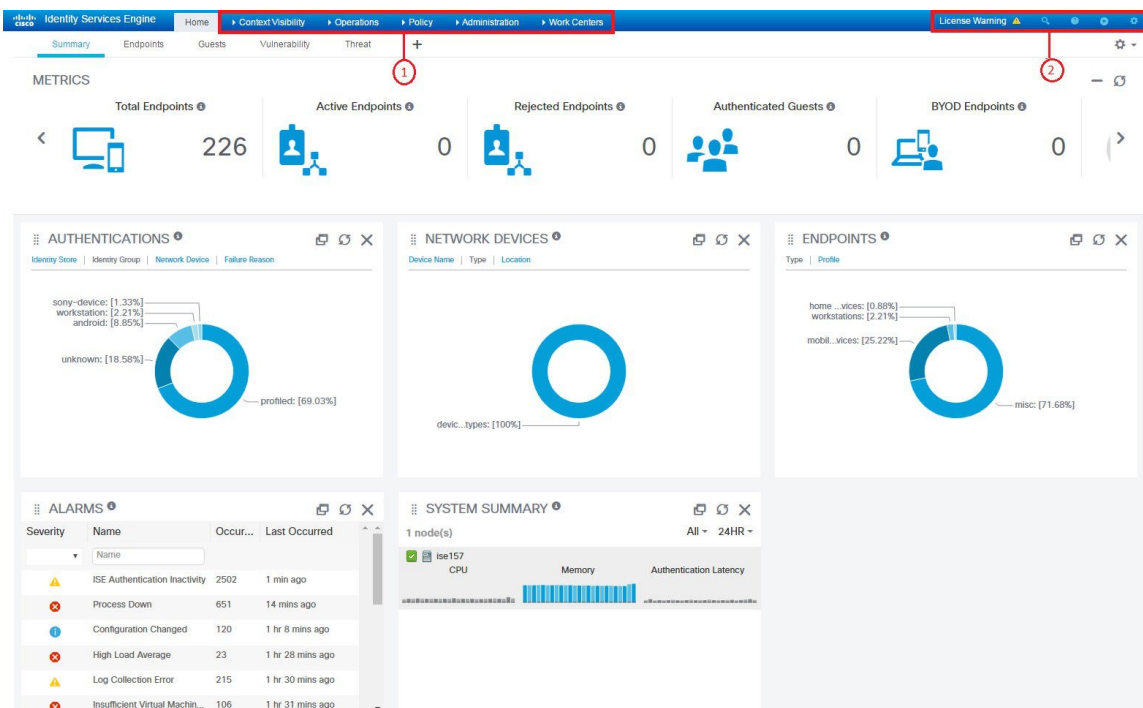
第 2 章

管理者ポータルでの移動





- 管理者ポータル (17 ページ)
- Cisco ISE 国際化およびローカリゼーション (27 ページ)
- MAC アドレスの正規化 (35 ページ)
- ロールベース アクセス コントロール ポリシーによって制限されている管理者機能 (36 ページ)

管理者ポータル

管理者ポータルでは、ISE の設定およびレポートにアクセスできます。次の図に、このポータルのメニュー バーの主要要素を示します。



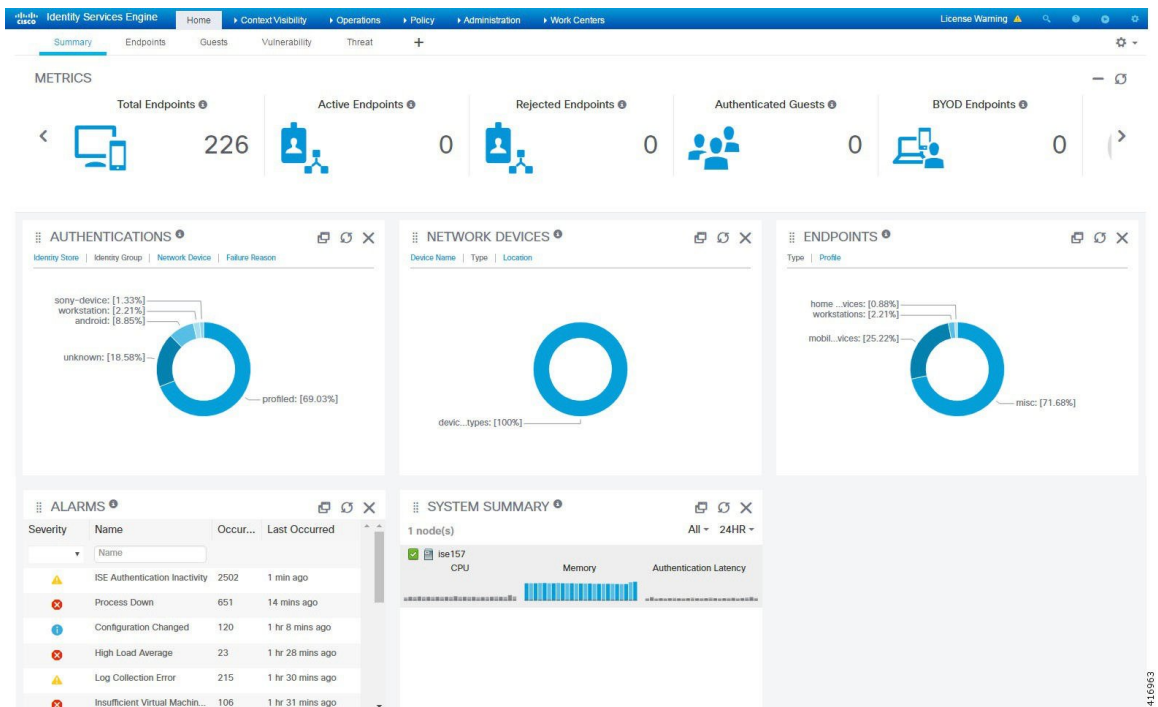
1	メニューのドロップダウン	<ul style="list-style-type: none">• [コンテキストの可視性 (Context Visibility)] : これらのメニューでは、エンドポイント、ユーザ、NAD に関する情報が表示されます。情報は、ライセンスに応じて、機能、アプリケーション、BYOD、その他のカテゴリ別にセグメント化できます。コンテキストメニューは中央データベースを使用して、データベーステーブル、キャッシュ、およびバッファから情報を収集し、それにより、コンテキストダッシュレットおよびリストの内容が非常に高速に更新されます。コンテキストメニューは上部のダッシュレットおよび下部の情報のリストから構成されます。リストのカラム属性を変更することによってデータをフィルタすると、変更したコンテンツを示すためにダッシュレットが更新されます。• [ポリシー (Policy)] : 認証、許可、プロファイリング、ポスチャ、クライアントプロビジョニングの領域でネットワークセキュリティを管理するためのツールにアクセスします。• [管理 (Administration)] : Cisco ISE ノード、ライセンス、証明書、ネットワーク デバイス、ユーザ、エンドポイント、およびゲスト サービスを管理するためのツールにアクセスします。
---	--------------	--

2	右上のメニュー	<ul style="list-style-type: none">  <p>エンドポイントを検索し、プロフィール、障害、IDストア、ロケーション、デバイス タイプ別にそれらの分布を表示します。</p>  <p>現在表示されているページのヘルプにアクセスします。</p>  <p>次のオプションにアクセスします。</p> <ul style="list-style-type: none"> • [PassiveIDセットアップ (PassiveID Setup)] : [PassiveID セットアップ (PassiveID Setup)] オプションでは、Active Directory を使用してパッシブ ID をセットアップする [PassiveIDセットアップ (PassiveID Setup)] ウィザードが起動されます。外部認証サーバからユーザ ID と IP アドレスを収集し、認証済み IP アドレスを対応するサブスクライバに配信するように、サーバを設定することができます。 • [可視性セットアップ (Visibility Setup)] : [可視性セットアップ (Visibility Setup)] オプションでは、ISE の [可視性セットアップ (Visibility Setup)] ウィザードが起動し、エンドポイント検出のための一連の IP アドレス範囲を追加できます。 • [ワイヤレスのセットアップ (ベータ) (Wireless Setup (BETA))] : [ワイヤレスのセットアップ (ベータ) (Wireless Setup (BETA))] オプションでは、802.1x、ゲスト、および個人所有デバイス持ち込み (BYOD) のワイヤレス フローを容易にセットアップできます。また、このオプションには、ゲストおよび BYOD 向けの各ポータルを設定してカスタマイズするためのワークフローも用意されています。  <p>システム アクティビティ。</p>
---	---------	---

ISE ホーム ダッシュボード

Cisco ISE ダッシュボードには、効果的なモニタリングおよびトラブルシューティングに必要な、統合された相関性のあるライブ統計データが表示されます。特に指定がない限り、ダッシュボード要素によってアクティビティは 24 時間表示されます。次の図に、Cisco ISE

ダッシュボードで利用できる情報の一部を示します。Cisco ISE ダッシュボード データはプライマリ管理ノード（PAN）でのみ表示されます。



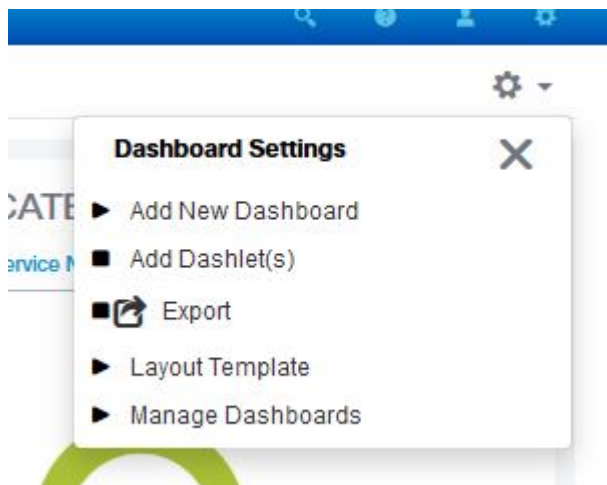
[ホーム (Home)] ページには、ISE データのビューを表示する 5 つのデフォルト ダッシュボードがあります。

- [概要 (Summary)] : このビューには、線形の [メトリック (Metrics)] ダッシュレット、円グラフ ダッシュレット、およびリスト ダッシュレットが表示されます。[メトリック (Metrics)] ダッシュレットは設定できません。
- [エンドポイント (Endpoints)] : ステータス、エンドポイント、エンドポイント カテゴリ、ネットワーク デバイス。
- [ゲスト (Guests)] : ゲスト ユーザ タイプ、ログイン失敗、ロケーション。
- [脆弱性 (Vulnerability)] : 脆弱性サーバにより ISE に報告される情報。
- [脅威 (Threat)] : 脅威サーバにより ISE に報告される情報。

これらの各ダッシュボードには、複数の事前定義ダッシュレットがあります。たとえば [概要 (Summary)] ダッシュボードには [ステータス (Status)]、[エンドポイント (Endpoints)]、[エンドポイント カテゴリ (Endpoint Categories)]、および [ネットワーク デバイス (Network Devices)] があります。

ホーム ダッシュボードの設定

ホーム ページ ダッシュボードをカスタマイズするには、ページの右上隅にある歯車アイコンをクリックします。



- [エクスポート (Export)] は、現在選択されているホーム ビューを PDF に保存します。
- [レイアウト テンプレート (Layout Template)] は、このビューに表示される列の数を設定します。
- [ダッシュボードの管理 (Manage Dashboards)] では、現在のダッシュボードをデフォルト ([ホーム (Home)]) を選択すると表示されるダッシュボード) に設定するか、またはすべてのダッシュボードをリセットする (すべてのホーム ダッシュボードの設定を削除する) ことができます。

[コンテキストの可視性 (Context Visibility)] のビュー

[コンテキストの可視性 (Context Visibility)] ページの構造はホーム ページに似ていますが、[コンテキストの可視性 (Context Visibility)] ページでは次の点が異なります。

- 表示データをフィルタリングするときに、現在のコンテキストを維持する (ブラウザウィンドウ)。
- より細かなカスタマイズが可能である
- エンドポイント データを中心としている

コンテキストの可視性データはプライマリ管理ノード (PAN) にのみ表示されます。

[コンテキスト (Context)] ページのダッシュレットには、エンドポイントと、エンドポイントから NAD への接続に関する情報が表示されます。現在表示されている情報は、各ページのダッシュレットの下にあるデータリストの内容に基づいています。各ページには、タブの名前に基づいてエンドポイントデータのビューが表示されます。データをフィルタリングすると、リストとダッシュレットの両方が更新されます。データをフィルタリングするには、1 つ以上の円グラフの特定部分をクリックするか、表で行をフィルタリングするか、またはこれらの操作を組み合わせるで実行します。複数のフィルタを選択した場合、フィルタ結果は加算的になります。これはカスケードフィルタと呼ばれます。これにより、ドリルダウンして特定のデータを

見つけることができます。また、リストでエンドポイントをクリックして、そのエンドポイントの詳細ビューを表示することもできます。

[コンテキストの可視性 (Context Visibility)] には 3 つのメイン ビューがあります。

- [エンドポイント (Endpoints)] : デバイスタイプ、コンプライアンスステータス、認証タイプ、などに基づいて表示するエンドポイントを選択できます。



- (注) アカウンティングの開始および更新情報が Cisco ISE に確実に送信されるように、NADでアカウンティングの設定を有効にすることを推奨します。

Cisco ISE では、アカウンティングが有効な場合にのみ、最新の IP アドレス、セッションのステータス (接続 [Connected]、切断 [Disconnected]、または拒否 [Rejected])、エンドポイントの非アクティブな日数などのアカウンティング情報を収集できます。この情報は、[ライブログ (Live Logs)]、[ライブセッション (Live Sessions)] および [コンテキストの可視性 (Context Visibility)] ページに表示されます。NADでアカウンティングが無効にされている場合、[ライブセッション (Live Sessions)]、[ライブログ (Live Logs)] および [コンテキストの可視性 (Context Visibility)] ページ間でアカウンティング情報が欠落しているか、間違っているか、一致していない可能性があります。



- (注) [可視性セットアップ (Visibility Setup)] ウィザードでは、エンドポイントを検出するため IP アドレス範囲のリストを追加できます。このウィザードの設定後に、Cisco ISE はエンドポイントを認証しますが、設定された IP アドレス範囲に含まれないエンドポイントは、[コンテキストの可視性 (Context Visibility)] > [エンドポイント (Endpoints)] タブと、[エンドポイント (Endpoints)] リスト ページ ([ワーク センター (Work Centers)] > [ネットワーク アクセス (Network Access)] > [ID (Identities)] > [エンドポイント (Endpoints)] の下) には表示されません。

- [ユーザベース (User-Based)] : ユーザ ID ソースからのユーザ情報を表示します。

このビューを使用する際には次の点に注意してください。

1. ユーザ名属性またはパスワード属性が変更されると、認証ステータスが変更された時点でこのページに変更が即時に反映されます。
2. Active Directory でユーザ名以外の属性が変更されると、再認証から 24 時間後に、更新された属性が表示されます。

3. Active Directory でユーザ名とその他の属性が変更されると、再認証後即時に最新の変更が表示されます。

- [ネットワーク デバイス (Network Devices)] : エンドポイントに接続している NAD のリスト。NAD のエンドポイント数 (右端の列) をクリックすると、その NAD に基づいてフィルタリングされたすべてのデバイスが [コンテキストの可視性 (Context Visibility)] 画面にリストされます。

フィルタリング処理を追加する目的で、[コンテキストの可視性 (Context Visibility)] の下に新しいビューを作成し、カスタム リストを作成できます。このリリースでは、カスタム ビューでダッシュレットがサポートされていません。

ダッシュレットの円グラフの特定部分をクリックすると、新しいページが開き、そのダッシュレットからフィルタリングされたデータが [コンテキストの可視性 (Context Visibility)] モードで表示されます。この新しいページから、表示されているデータをさらにフィルタリングできます。これについては [ビューに表示するデータのフィルタリング \(24 ページ\)](#) で説明します。

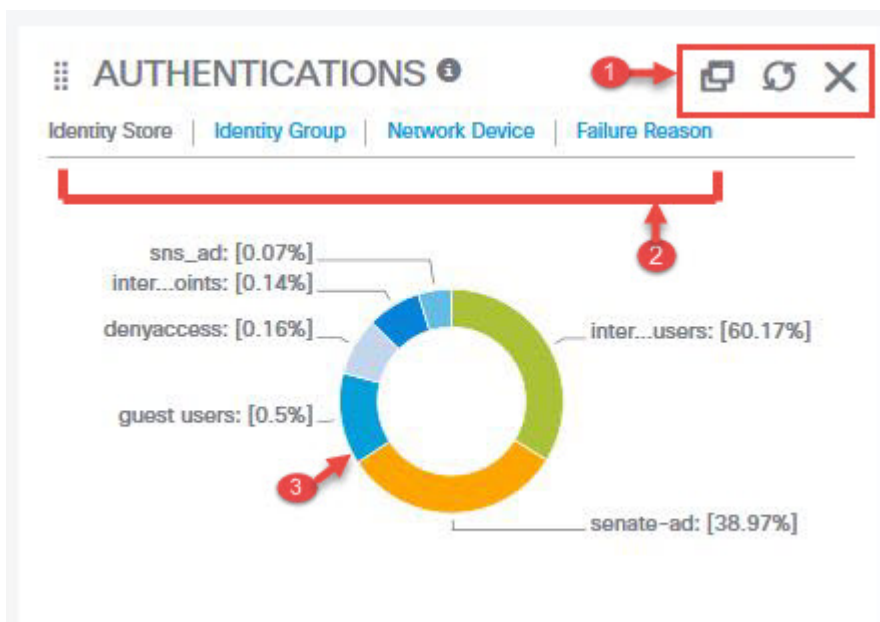
[コンテキストの可視性 (Context Visibility)] を使用してエンドポイント データを検索する方法の詳細については、Cisco YouTube ビデオを参照してください。このビデオでは ISE 2.1 <https://www.youtube.com/watch?v=HvonGhrydfg> を使用しています。

関連トピック

[ハードウェア ダッシュボード](#)

ダッシュレット

次に、ダッシュレットの例を示します。



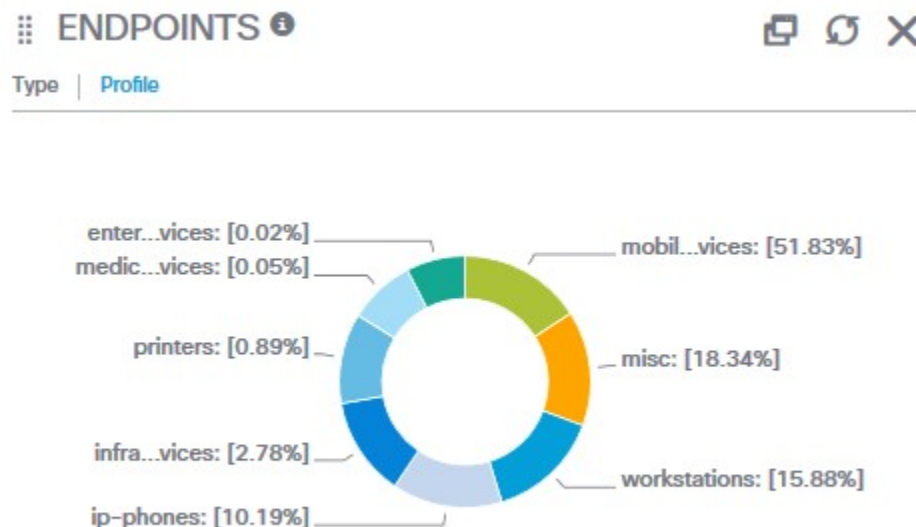
1. ウィンドウが重なり合ったシンボルは、このダッシュレットを「切り離し」ます。つまり、新しいブラウザウィンドウでこのダッシュレットを開きます。円形のシンボルは更新を実行します。Xはこのダッシュレットを削除します。このシンボルはホームページでのみ使用可能です。[コンテキストの可視性 (Context Visibility)] でダッシュレットを削除するには、画面右上隅にある歯車のシンボルを使用します。
2. 一部のダッシュレットには異なるカテゴリのデータが表示されます。リンクをクリックすると、そのデータセットの円グラフが表示されます。
3. 円グラフには、選択したデータが表示されます。円グラフの1つのセグメントをクリックすると、[コンテキストの可視性 (Context Visibility)] で新しいタブが開き、円グラフセグメントに基づいてフィルタリングされたデータが表示されます。

ホーム ダッシュボードで円グラフのセクションをクリックすると、新しいブラウザ ウィンドウが開き、円グラフでクリックしたセクションに基づいてフィルタリングされたデータが表示されます。

[コンテキスト (Context)] ビューで円グラフのセクションをクリックすると、表示されているデータがフィルタリングされますが、コンテキストは変更されず、フィルタリングされたデータは同じブラウザ ウィンドウに表示されます。

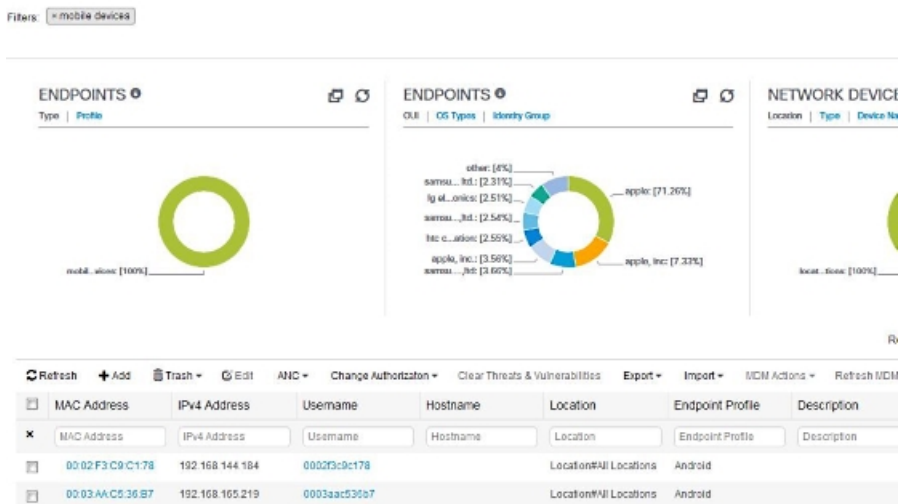
ビューに表示するデータのフィルタリング

[コンテキストの可視性 (Context Visibility)] ページでいずれかのダッシュレットをクリックすると、クリックしたアイテムに基づいて表示されるデータ (円グラフの一部分など) がフィルタリングされます。



[エンドポイント (Endpoints)] ダッシュレットで [mobil...vices] をクリックすると、ページが再表示され、2つの [エンドポイント (Endpoints)] ダッシュレット、[ネットワーク デバイス

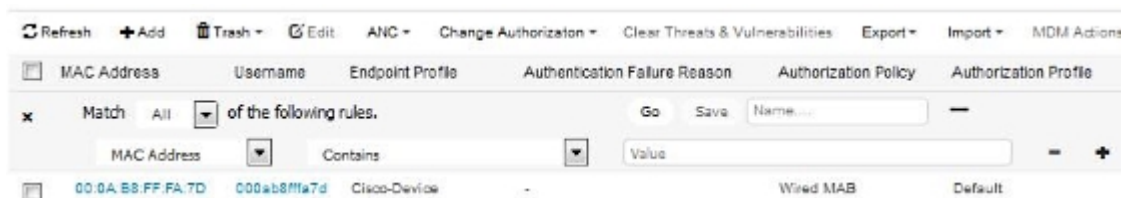
(Network Devices)] ダッシュレット、およびデータのリストが表示されます。次の例に示すように、ダッシュレットとリストにはモバイル デバイスのデータが表示されます。



さらにデータをフィルタリングするには、円グラフの他のセクションをクリックするか、またはデータ リストのコントロールを使用します。



1. 歯車アイコンにより、表示列がフィルタリングされます。ドロップダウンでは、このダッシュボードのリストに表示する列を選択できます。
2. デフォルトではクイック フィルタが表示されます。ボックス（ラベル番号 3）に文字を入力すると、結果に基づいてリストがフィルタリングされます。カスタムフィルタでは、次に示すようにより細かく設定できるフィルタが表示されます。

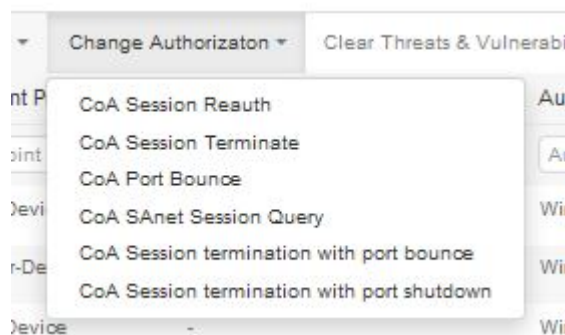


カスタム フィルタは保存できます。

ビューのリストでのエンドポイント アクション

リスト上部にあるツールバーから、リストで選択したエンドポイントに対してアクションを実行できます。すべてのリストですべてのアクションが有効になっているわけではありません。一部のアクションは、使用可能な機能に基づいています。次のリストに、使用する前に ISE で有効にする必要がある 2 つのエンドポイント アクションを示します。

- 適応型ネットワーク制御（ANC）が有効な場合、リストでエンドポイントを選択して、ネットワークアクセスを割り当てるかまたは取り消すことができます。認可変更（CoA）も発行できます。



ANC（エンドポイント保護サービス）は、ISE の [管理（Administration）] > [システム（System）] > [設定（Settings）] > [エンドポイント保護サービス（Endpoint Protection Service）] > [適応型ネットワーク制御（Adaptive Network Control）] で有効にします。詳細については、[Cisco ISE での適応型ネットワーク制御の有効化（351 ページ）](#) を参照してください。

- MDM がインストールされている場合は、選択したエンドポイントに対して MDM アクションを実行できます。

コンテキストの可視性の属性

コンテキストの可視性の属性を提供するシステムとサービスでは、同じ属性名に異なる値を使用していることがよくあります。次にいくつかの例を示します。

オペレーティング システム

- *OperatingSystem* : ポスチャ オペレーティング システム
- *operating-system* : NMAP オペレーティング システム
- *operating-system-result* : プロファイラ統合オペレーティング システム

ポータル名

- *Portal.Name* : デバイス登録が有効な場合のゲスト ポータル名。
- *PortalName* : デバイス登録が無効な場合のゲスト ポータル名。

ポータル ユーザ

- *User-Name* : RADIUS 認証のユーザ名
- *GuestUserName* : ゲスト ユーザ
- *PortalUser* : ポータル ユーザ

Cisco ISE 国際化およびローカリゼーション

Cisco ISE 国際化では、サポートされる言語にユーザ インターフェイスを合わせます。ユーザ インターフェイスのローカリゼーションでは、ロケール固有のコンポーネントおよび翻訳されたテキストが組み込まれます。Windows、MAC OSX、および Android デバイスの場合、ネイティブ サプリカント プロビジョニング ウィザードは、次のサポートされている言語のいずれかで使用できます。

Cisco ISE の国際化およびローカリゼーションのサポートでは、ポータルに接するエンドユーザに対して UTF-8 符号化で英語以外のテキストをサポートすること、および管理者ポータルの選択的フィールドに重点を置いています。

サポートされる言語

Cisco ISE では、次の言語とブラウザ ロケールのローカリゼーションおよび国際化がサポートされます。

[言語 (Language)]	ブラウザ ロケール
中国語 (繁体字)	zh-tw
中国語 (簡体字)	zh-cn
チェコ語	cs-cz
Dutch	nl-nl
英語	en
フランス語	fr-fr
ドイツ語	de-de
ハンガリー語	hu-hu
イタリア語	it-it

[言語 (Language)]	ブラウザ ロケール
日本語	ja-jp
Korean	ko-kr
ポーランド語	pl-pl
ポルトガル語 (ブラジル)	pt-br
ロシア語	ru-ru
スペイン語	es-es

エンドユーザ Web ポータルのローカリゼーション

ゲスト、スポンサー、デバイスおよびクライアントプロビジョニングの各ポータルは、サポートされているすべての言語およびロケールにローカライズされています。ローカライズには、テキスト ラベル、メッセージ、フィールド名およびボタン ラベルが含まれます。クライアント ブラウザが Cisco ISE テンプレートにマッピングされていないロケールを要求した場合、ポータルは英語のテンプレートを使用して内容を表示します。

管理者ポータルを使用して、各言語のゲスト、スポンサー、デバイスの各ポータルで使用されるフィールドを個別に変更できます。また、言語を追加することも可能です。現在、クライアントプロビジョニングポータルについては、これらのフィールドはカスタマイズできません。

HTML ページを Cisco ISE にアップロードすることによって、ゲスト ポータルを詳細にカスタマイズできます。カスタマイズしたページをアップロードする場合は、展開に対する適切なローカリゼーションサポートに責任を負います。Cisco ISE では、サンプル HTML ページを含むローカリゼーションサポート例が提供されており、これをガイドとして使用できます。Cisco ISE には、国際化されたカスタム HTML ページをアップロード、格納、および表示する機能があります。



(注) NAC および MAC エージェントのインストーラおよび WebAgent ページはローカライズされていません。

UTF-8 文字データ エントリのサポート

エンドユーザに (Cisco NAC Agent またはサブリカント、あるいはスポンサー、ゲスト、デバイス、クライアントプロビジョニングの各ポータルを介して) 公開される Cisco ISE フィールドは、すべての言語の UTF-8 文字セットをサポートします。UTF-8 は、Unicode 文字セット用のマルチバイト文字エンコーディングであり、ヘブライ語、サンスクリット語、アラビア語など、多数の異なる言語文字セットがあります。

文字の値は、管理設定データベースに UTF-8 で格納され、UTF-8 文字はレポートおよびユーザーインターフェイス コンポーネントで正しく表示されます。

UTF-8 クレデンシャル認証

ネットワークアクセス認証では、UTF-8 ユーザー名およびパスワードのクレデンシャルがサポートされます。これには、RADIUS、EAP、RADIUS プロキシ、RADIUS トークン、ゲストおよび管理ポータルログイン認証からの Web 認証が含まれます。ユーザー名とパスワードの UTF-8 サポートは、ローカル ID ストアおよび外部 ID ストアに対する認証に適用されます。

UTF-8 認証は、ネットワークログインに使用されるクライアントサブリカントに依存します。一部の Windows ネイティブサブリカントでは、UTF-8 クレデンシャルはサポートされません。



(注) RSA では UTF-8 ユーザーはサポートされないため、RSA を使用した UTF-8 認証はサポートされません。同様に、Cisco ISE と互換性がある RSA サーバでも UTF-8 がサポートされません。

UTF-8 ポリシーおよびポスチャ評価

属性値に基づいて決定される Cisco ISE のポリシー ルールに、UTF-8 テキストが含まれている場合があります。UTF-8 属性値はルール評価でサポートされます。また、管理ポータルで UTF-8 の値を使用して条件を設定できます。

ポスチャ要件を、UTF-8 文字セットに基づくファイル、アプリケーション、およびサービス条件として変更できます。これには、UTF-8 要件の値を NAC エージェントに送信することが含まれます。NAC エージェントはそれに応じてエンドポイントを評価し、UTF-8 の値を報告します（該当する場合）。

Cisco NAC および MAC エージェントの UTF-8 サポート

Cisco NAC エージェントでは、テキスト、メッセージ、および Cisco ISE と交換される任意の UTF-8 データの国際化がサポートされます。これには、要件メッセージ、要件名、および条件で使用されるファイル名およびプロセス名が含まれます。

次の制限が適用されます。

- UTF-8 サポートは、Windows ベースの NAC エージェントにのみ適用されます。
- Cisco NAC および MAC エージェントのインターフェイスでは、現在、ローカリゼーションはサポートされていません。
- WebAgent では、UTF-8 ベースのルールおよび要件はサポートされません。
- 利用規定 (AUP) が設定されている場合は、ブラウザ ロケールと設定で指定された言語セットに基づいて、ポリシーのページがクライアント側で提供されます。ローカライズされた AUP バンドルまたはサイト URL の提供は、ユーザーの責任です。

サブリカントに送信されるメッセージの UTF-8 サポート

RSA プロンプトおよびメッセージは、RADIUS 属性 REPLY-MESSAGE を使用して、または EAP データ内で、サブリカントに転送されます。テキストに UTF-8 データが含まれている場合は、サブリカントによって、クライアントのローカル オペレーティング システムの言語サポートに基づいて表示されます。一部の Windows ネイティブ サブリカントでは、UTF-8 クレデンシャルはサポートされません。

Cisco ISE プロンプトおよびメッセージは、サブリカントが実行されているクライアントのオペレーティング システムのロケールと同期していない場合があります。エンドユーザのサブリカントのロケールを Cisco ISE によってサポートされている言語に合わせる必要があります。

レポートおよびアラートの UTF-8 サポート

モニタリングおよびトラブルシューティングのレポートおよびアラートでは、Cisco ISE でサポートされる言語について、次のように関連属性の UTF-8 の値がサポートされます。

- ライブ認証の表示
- レポート レコードの詳細ページの表示
- レポートのエクスポートと保存
- Cisco ISE ダッシュボードの表示
- アラート情報の表示
- tcpdump データの表示

ポータルでの UTF-8 文字のサポート

Cisco ISE フィールド (UTF-8) では、ポータルおよびエンドユーザメッセージでローカリゼーション用に現在サポートされているよりも、多くの文字セットがサポートされます。たとえば、Cisco ISE では、ヘブライ語やアラビア語などの右から左へ記述する言語はサポートされていません (文字セット自体はサポートされています)。

次の表に、データの入力および表示に UTF-8 文字をサポートする管理者ポータルおよびエンドユーザ ポータルのフィールドを示します。次の制限があります。

- Cisco ISE では、UTF-8 文字を使用したゲスト パスワードはサポートされません。
- Cisco ISE では、証明書で UTF-8 文字を使用することはできません。

表 1: 管理者ポータルの UTF-8 文字フィールド

管理者ポータル要素	UTF-8 フィールド
ネットワーク アクセスのユーザ設定	<ul style="list-style-type: none"> • ユーザ名 (User name) • 名 (First name) • 姓 (Last name) • 電子メール (e-mail)
ユーザ リスト	<ul style="list-style-type: none"> • すべてのフィルタ フィールド • [ユーザ リスト (User List)] ページに表示される値 • 左側のナビゲーションクイック ビューに表示される値
ユーザ パスワード ポリシー	<p>パスワードには、大文字と小文字、数字、特殊文字 (「!」、「@」、「#」、「\$」、「%」、「^」、「&」、「*」、「(」、「)」) など) を自由に組み合わせて使用できます。[パスワード (Password)] フィールドでは、UTF-8 文字を含むあらゆる文字を使用できますが、制御文字は使用できません。</p> <p>言語の中には大文字または小文字のアルファベットがないものがあります。ユーザパスワードポリシーでユーザに大文字または小文字でパスワードを入力することを求め、ユーザの言語がこれらの文字をサポートしていない場合、ユーザはパスワードを設定できません。ユーザパスワードフィールドで UTF-8 文字をサポートするには、ユーザパスワードポリシー ページ ([管理 (Administration)] > [ID の管理 (Identity Management)] > [設定 (Settings)] > [ユーザ パスワード ポリシー (User Password Policy)]) で次のオプションをオフにする必要があります。</p> <ul style="list-style-type: none"> • 小文字の英文字 (Lowercase alphabetic characters) • 大文字の英文字 (Uppercase alphabetic characters)

管理者ポータル要素	UTF-8 フィールド
管理者リスト	<ul style="list-style-type: none"> • すべてのフィルタ フィールド • [管理者リスト (Administrator List)] ページに表示される値 • 左側のナビゲーションクイック ビューに表示される値
管理者ログイン ページ	<ul style="list-style-type: none"> • ユーザ名 (User name)
RSA	<ul style="list-style-type: none"> • メッセージ • プロンプト
RADIUS トークン	<ul style="list-style-type: none"> • [認証 (Authentication)] タブ > [プロンプト (Prompt)]
ポスチャ要件	<ul style="list-style-type: none"> • [名前 (Name)] • [修復アクション (Remediation action)] > エージェント ユーザに表示されるメッセージ • 要件リスト表示
ポスチャ条件	<ul style="list-style-type: none"> • [ファイル条件 (File condition)] > [ファイルパス (File path)] • [アプリケーション条件 (Application condition)] > [プロセス名 (Process name)] • [サービス条件 (Service condition)] > [サービス名 (Service name)] • 条件リスト表示

管理者ポータル要素	UTF-8 フィールド
ゲストおよびデバイスの設定	<ul style="list-style-type: none"> • [スポンサー (Sponsor)] > [言語テンプレート (Language Template)] : サポートされているすべての言語、すべてのフィールド • [ゲスト (Guest)] > [言語テンプレート (Language Template)] : サポートされているすべての言語、すべてのフィールド • [デバイス (My Devices)] > [言語テンプレート (Language Template)] : サポートされているすべての言語、すべてのフィールド
システム設定	<ul style="list-style-type: none"> • [SMTP サーバ (SMTP Server)] > [デフォルトの電子メールアドレス (Default e-mail address)]
[操作 (Operations)] > [アラーム (Alarms)] > [ルール (Rule)]	<ul style="list-style-type: none"> • [基準 (Criteria)] > [ユーザ (User)] • [通知 (Notification)] > [電子メール通知ユーザリスト (e-mail Notification user list)]
[操作 (Operations)] > [レポート (Reports)]	<ul style="list-style-type: none"> • [操作 (Operations)] > [ライブ認証 (Live Authentications)] > フィルタ フィールド • [操作 (Operations)] > [レポート (Reports)] > [カタログ (Catalog)] > レポート フィルタ フィールド
[操作 (Operations)] > [トラブルシューティング (Troubleshoot)]	<ul style="list-style-type: none"> • [一般ツール (General Tools)] > [RADIUS 認証トラブルシューティング (RADIUS Authentication Troubleshooting)] > [ユーザ名 (Username)]
ポリシー	<ul style="list-style-type: none"> • [認証 (Authentication)] > ポリシー条件内での av 式の値 • [許可 (Authorization)]/[ポストチャ (Posture)]/[クライアントプロビジョニング (Client Provisioning)] > [その他の条件 (Other Conditions)] > ポリシー条件内での av 式の値

管理者ポータル要素	UTF-8 フィールド
ポリシー ライブラリ 条件の属性値	<ul style="list-style-type: none"> • [認証 (Authentication)] > [単純条件/複合条件 (Simple Condition/Compound Condition)] > av 式の値 • [認証 (Authentication)] > 単純条件リスト表示 • [認証 (Authentication)] > 単純条件リスト > 左のナビゲーション クイック ビュー表示 • [許可 (Authorization)] > [単純条件/複合条件 (Simple Condition/Compound Condition)] > av 式の値 • [許可 (Authorization)] > 単純条件リスト > 左のナビゲーション クイック ビュー表示 • [ポスチャ (Posture)] > [ディクショナリ 単純条件/ディクショナリ 複合条件 (Dictionary Simple Condition/Dictionary Compound Condition)] > av 式の値 • [ゲスト (Guest)] > [単純条件/複合条件 (Simple Condition/Compound Condition)] > av 式の値

ユーザ インターフェイス外での UTF-8 サポート

この項では、Cisco ISE ユーザ インターフェイス外で UTF-8 がサポートされる領域について説明します。

デバッグ ログおよび CLI 関連の UTF-8 サポート

一部のデバッグ ログには、属性値およびポスチャ条件の詳細が表示されます。そのため、すべてのデバッグ ログで UTF-8 の値が受け入れられます。raw UTF-8 データを含むデバッグ ログをダウンロードして、UTF-8 対応ビューアで表示できます。

ACS 移行の UTF-8 サポート

Cisco ISE では、ACS UTF-8 設定オブジェクトおよび値の移行が可能です。一部の UTF-8 オブジェクトの移行は、Cisco ISE UTF-8 言語でサポートされない場合があります。そのため、移行中に提供される UTF-8 データの一部は、管理ポータルまたはレポート方式を使用して読み取れない表示になる場合があります。（ACS から移行された）読み取り不可能な UTF-8 値は ASCII テキストに変換する必要があります。ACE から ISE への移行の詳細については、『ISE Migration

Guide』 (http://www.cisco.com/c/en/us/td/docs/security/ise/2-1/migration_guide/b_ise_MigrationGuide21.html) を参照してください。

UTF-8 の値のインポートおよびエクスポートのサポート

管理者ポータルおよびスポンサー ポータルは、ユーザ アカウントの詳細をインポートするときに使用される UTF-8 値のプレーンテキストおよび .csv ファイルをサポートします。エクスポートされたファイルは csv ファイルとして提供されます。

REST での UTF-8 サポート

UTF-8 の値は、外部 REST 通信でサポートされます。これは、admin 認証を除き、Cisco ISE ユーザーインターフェイスの UTF-8 がサポートされる設定可能項目に適用されます。REST での admin 認証には、ログインのために ASCII テキスト クレデンシャルが必要です。

ID ストアの許可データの UTF-8 サポート

Cisco ISE では、Active Directory および LDAP がポリシー処理のために許可ポリシーで UTF-8 データを使用できます。

MAC アドレスの正規化

ISE は次のいずれかの形式で入力された MAC アドレスの正規化をサポートします。

- 00-11-22-33-44-55
- 0011.2233.4455
- 00:11:22:33:44:55
- 001122334455
- 001122-334455

次の ISE ウィンドウでは、完全または部分的な MAC アドレスを指定できます。

- [ポリシー (Policy)] > [許可 (Authorization)]
- [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [条件 (Conditions)] > [許可 (Authorization)]
- [認証 (Authentications)] > [フィルタ (Filters)] (エンドポイント カラムおよび ID カラム)
- [グローバル検索 (Global Search)]
- [操作 (Operations)] > [レポート (Reports)] > [レポート フィルタ (Reports Filters)]
- [操作 (Operations)] > [診断ツール (Diagnostic Tools)] > [一般ツール (General Tools)] > [エンドポイントのデバッグ (Endpoint Debug)]

次の ISE ウィンドウでは、完全な MAC アドレスを指定する必要があります（「:」または「-」または「.」で区切られた 6 オクテット）。

- [操作 (Operations)] > [エンドポイント保護サービス (Endpoint Protection Services) 適応型ネットワーク制御 (Adaptive Network Control)]
- [操作 (Operations)] > [トラブルシューティング (Troubleshooting)] > [診断ツール (Diagnostic Tools)] > [一般ツール (General Tools)] > [RADIUS 認証トラブルシューティング (RADIUS Authentication Troubleshooting)]
- [操作 (Operations)] > [トラブルシューティング (Troubleshooting)] > [診断ツール (Diagnostic Tools)] > [一般ツール (General Tools)] > [ポスチャのトラブルシューティング (Posture Troubleshooting)]
- [管理 (Administration)] > [ID (Identities)] > [エンドポイント (Endpoints)]
- [管理 (Administration)] > [システム (System)] > [展開 (Deployment)]
- [管理 (Administration)] > [ロギング (Logging)] > [収集フィルタ (Collection Filter)]

REST API でも、完全な MAC アドレスの正規化がサポートされます。

有効なオクテットには 0 ～ 9、a ～ f、または A ～ F のみ含めることができます。

ロールベース アクセス コントロール ポリシーによって制限されている管理者機能

Cisco ISE では、管理権限を制限することでセキュリティを確保するロールベース アクセス コントロール (RBAC) ポリシーが提供されます。RBAC ポリシーは、ロールおよび権限を定義するためにデフォルトの管理者グループに関連付けられています。標準的な権限セット（メニューおよびデータアクセス）が、事前定義された管理者グループそれぞれとペアになっており、それによって、関連付けられたロールおよび職務機能と整合性がとられています。

ユーザインターフェイスにある一部の機能には、使用するために特定の権限が必要です。ある機能が使用できない場合、または特定のタスクの実行が許可されない場合、その機能を利用するタスクを実行するのに必要な権限が自分の管理者グループにない場合があります。

アクセスレベルに関係なく、すべての管理者アカウントは、管理者がアクセスできるすべてのページの、権限を持つオブジェクトを変更または削除できます。読み取り専用機能は、いずれの管理者アクセスにも使用できません。



第 3 章

Wireless Setup について

Wireless Setup では、802.1x、ゲスト、および BYOD のワイヤレス フローを容易にセットアップできます。また、適切な場合にはゲスト向けのポータルと BYOD 向けのポータルを設定およびカスタマイズするためのワークフローも提供されます。これらのワークフローでは、最も一般的な推奨設定が提供されるため、ISE で関連ポータルフローを設定するよりもシンプルです。Wireless Setup では、ISE と WLC でユーザが実行する必要があるステップの多くが自動的に処理されるため、迅速に作業環境を構築できます。

フローのテストと開発に、Wireless Setup により作成された環境を使用できます。Wireless Setup 環境が稼働したら、ISE に切り替えることができます。これにより、より多くの拡張設定に対応できるようになります。ISE でのゲストの設定についての詳細は、『ISE Administrators Guide』の [Cisco ISE ゲスト サービス \(521 ページ\)](#) と Cisco コミュニティ サイト

(<https://communities.cisco.com/docs/DOC-64018>) を参照してください。Wireless Setup の設定と使用の詳細については、<https://communities.cisco.com/docs/DOC-71189> を参照してください。



(注) ISE Wireless Setup はベータ ソフトウェアです。実稼働ネットワークでは ISE Wireless Setup を使用しないでください。

- Wireless Setup は、Cisco ISE の新規インストール後はデフォルトで無効になっています。Wireless Setup は、ISE CLI から **application configure ise** コマンド (オプション 17 を選択) を使用するか、または ISE GUI の [ホーム (Home)] ページで [ワイヤレスのセットアップ (Wireless Setup)] オプションを使用して有効にすることができます。
- Wireless Setup インスタンスは一度に 1 つだけ実行してください。また、Wireless Setup を実行できるユーザは一度に 1 人だけです。
- ISE を以前のバージョンからアップグレードすると、Wireless Setup メニューが表示されなくなります。これは、新しい ISE インストールでのみ Wireless Setup がサポートされているためです。ISE CLI で **application configure ise** コマンドを使用して Wireless Setup を有効にするオプションを選択して、Wireless Setup を有効にできます。
- Wireless Setup を使用するには、ポート 9103 と 9104 が開いている必要があります。これらのポートを閉じるには、CLI を使用して Wireless Setup を無効にします。

- 一部のフローの実行後に **Wireless Setup** の新規インストールを開始する場合には、CLI コマンド **application reset-config ise** を使用できます。このコマンドは ISE 設定をリセットして ISE データベースをクリアしますが、ネットワーク定義を維持します。したがって、ISE と **Wireless Setup** をリセットするときに、ISE を再インストールしてセットアップを実行する必要はありません。

Wireless Setup を再び使用開始するには、次の手順に従って ISE と **Wireless Setup** の両方の設定をリセットできます。

- CLI で **application reset-config** を実行し、ISE 設定をすべてリセットします。新規インストールで **Wireless Setup** をテストしていた場合、このコマンドを実行すると、ISE で **Wireless Setup** によって行われた設定が削除されます。
- CLI で **application configure ise** を実行し、**[18]Reset Config Wi-Fi Setup** を選択します。これにより、**Wireless Setup** 設定データベースの内容が消去されます。
- WLC で、**Wireless Setup** により WLC に追加された設定を削除します。WLC での **Wireless Setup** の設定内容については、[Wireless Setup による ISE と WLC の変更 \(49 ページ\)](#) を参照してください。

ISE の新規インストール完了後に VM のスナップショットを取得しておく、この手順を行わずに済みます。

CLI の詳細については、『[Cisco Identity Services Engine CLI Reference Guide](#)』を参照してください。

- Wireless Setup** を使用するには、ISE スーパー管理者ユーザである必要があります。
- Wireless Setup** を使用するには、少なくとも 2 つの CPU コアと 8GB のメモリが必要です。
- Active Directory グループとユーザだけがサポートされています。**Wireless Configuration** で 1 つ以上のフローを作成すると、**Wireless Setup** でその他のタイプのユーザ、グループ、認証を使用できますが、これらを ISE で設定する必要があります。
- ISE で Active Directory をすでに定義しており、この AD を **Wireless Setup** に使用する予定の場合は、次の要件を満たしている必要があります。
 - 参加名とドメイン名が同一である必要があります。これらの名前が同一でない場合は、**Wireless Setup** でその AD を使用する前に、ISE で名前を同一にしてください。
 - ISE で WLC がすでに設定されている場合、その WLC には共有秘密が設定されている必要があります。WLC 定義に共有秘密がない場合は、**Wireless Setup** でその WLC を設定する前に、共有秘密を追加するか、または ISE から WLC を削除してください。
- Wireless Setup** では ISE コンポーネントを設定できますが、フローの開始後に ISE コンポーネントを削除または変更することはできません。**Wireless Setup** が ISE で設定するすべての内容のリストについては、次を参照してください。[Wireless Setup による ISE と WLC の変更 \(49 ページ\)](#)
- 開始したフローは完了する必要があります。フローでトピックパスをクリックすると、フローが停止します。フローをステップに従って進むと、ISE 設定が動的に変更されます。

Wireless Setup では設定変更のリストが表示されるので、手動で変更を元に戻すことができます。1 つの例外を除いて、フローで前に戻って追加の変更を行うことはできません。例外として、ゲスト ポータルまたは BYOD ポータルのカスタマイズ内容を変更する場合には戻ることができます。

- 複数の WLC と Active Directory ドメインがサポートされていますが、各フローでは 1 つの WLC と 1 つの Active Directory だけがサポートされています。
- Wireless Setup が動作するためには、ISE Basic ライセンスが必要です。BYOD には Plus ライセンスが必要です。
- Wireless Setup をスタンドアロンセットアップで実行することが推奨されます（必要に応じて 2 番目のノードを使用します）。スタンドアロンセットアップの定義の詳細については、http://www.cisco.com/c/en/us/td/docs/security/ise/2-1/install_guide/b_ise_InstallationGuide21/b_ise_InstallationGuide21_chapter_00.html#ID-1413-0000009d を参照してください。
- Wireless Setup の設定前に ISE 2.2 リソースを設定している場合、Wireless Setup が既存のポリシーと矛盾することがあります。この状況では、Wireless Setup から、ツールの実行後に認証ポリシーをレビューするよう指示されます。Wireless Setup の実行時には、正常にセットアップされた ISE を使用して開始することが推奨されます。Wireless Setup と ISE の混合設定のサポートは限定されています。
- Wireless Setup は英語でのみ提供されており、他の言語では提供されていません。ポータルで他の言語を使用する場合には、Wireless Setup の実行後に ISE でその言語を設定してください。
- BYOD ではデュアル SSID がサポートされています。この設定で使用するオープン SSID では、競合のためゲスト アクセスはサポートされません。ゲストと BYOD の両方に対応したポータルが必要な場合、Wireless Setup は使用できません。これについてはこのマニュアルでは説明しません。
- SSID 名にはスペースを使用してください。
- 電子メール通知と SMS 通知
 - アカウント登録ゲストの場合、SMS 通知と電子メール通知がサポートされています。これらの通知は、ポータル カスタマイズ通知セクションで設定します。SMS 通知と電子メール通知をサポートするように SMTP サーバを設定する必要があります。ISE に組み込まれているセルラープロバイダー（AT&T、T Mobile、Sprint、Orange、Verizon など）は、事前に設定されている無料の電子メール/SMS ゲートウェイです。
 - ゲストはポータルで各自のセルラープロバイダーを選択します。プロバイダーがリストにない場合は、メッセージを受信できません。グローバルプロバイダーも設定できますが、これについてはこのマニュアルでは説明しません。ゲスト ポータルで SMS 通知と電子メール通知が設定されている場合、ゲストは両方のサービスの値を入力する必要があります。
 - Sponsored Guest フローでは、Wireless Setup での SMS 通知または電子メール通知の設定は行いません。このフローについては、ISE で通知サービスを設定する必要があります。

- 通知の設定の詳細については、『**Configure SMTP Server to Support Notifications**』
(http://www.cisco.com/c/en/us/td/docs/security/ise/2-1/admin_guide/b_ise_admin_guide_21/b_ise_admin_guide_20_chapter_0100.html#ID166) および『**SMS Gateway Settings**』
(http://www.cisco.com/c/en/us/td/docs/security/ise/2-1/admin_guide/b_ise_admin_guide_21/b_ise_admin_guide_20_chapter_011010.html#reference_637B4FC473F247249AD42888125FA5D0) を参照してください。
- ポータルで通知を設定するときには、SMS プロバイダー *Global Default* を選択しないでください。（デフォルトでは）このプロバイダーは設定されていません。
- **Wireless Setup** では、HA を使用しないスタンドアロンセットアップだけがサポートされています。認証のために追加の PSN を使用する場合は、それらの PSN の ISE IP アドレスを WLC の RADIUS 設定に追加してください。

Wireless Setup での Apple ミニブラウザ（Captive Network Assistant）のサポート

- **ゲストフロー**：Apple 擬似ブラウザの自動ポップアップは、すべてのゲストフローで機能します。ゲストは Apple の Captive Network Assistant ブラウザを使用してフローを通過することができます。Apple ユーザが OPEN ネットワークに接続すると、ミニブラウザが自動的に表示されます。これにより、ユーザは AUP（ホットスポット）を受け入れるか、または各自のクレデンシャルを使用してアカウント登録またはログインを実行できます。
- **BYOD**
 - **シングル SSID**：ISE 2.2 では Apple ミニブラウザのサポートが追加されました。ただし Apple デバイスで SSID フローの問題が発生する可能性を抑えるため、リダイレクション ACL に captive.apple.com を追加してミニブラウザが表示されないようにしました。これにより、Apple デバイスはインターネットにアクセスできると想定します。ユーザは、Web 認証またはデバイス オンボーディングのためにポータルにリダイレクトされるように、Safari を手動で起動する必要があります。
 - **デュアル SSID**：ゲスト アクセスを開始するか、または従業員がデバイス オンボーディング（BYOD）を実行できるようにするために、最初の OPEN ネットワーク WLAN で開始し、セキュア SSID にリダイレクトされるデュアル SSID フローの場合にも、ミニブラウザが表示されなくなります。

Apple CAN ミニブラウザの詳細については、<https://communities.cisco.com/docs/DOC-71122> を参照してください。

- [ワイヤレス ネットワークの WLC の設定](#)（41 ページ）
- [Active Directory と Wireless Setup](#)（43 ページ）
- [Wireless Setup でのゲスト ポータル](#)（43 ページ）
- [ワイヤレス ネットワーク アカウント登録ポータル](#)（44 ページ）
- [ワイヤレス ネットワーク Sponsored Guest フロー](#)（45 ページ）
- [Wireless Setup BYOD フロー：ネイティブ サプリカントおよび証明書のプロビジョニング](#)（45 ページ）
- [セキュア アクセス フロー](#)（47 ページ）

- [Wireless Setup](#) による ISE と WLC の変更 (49 ページ)

ワイヤレス ネットワークの WLC の設定

Wireless Setup に初めてログインしてフローを選択すると、ワイヤレス コントローラを設定するように促されます。Wireless Setup は設定するフローのタイプに対応するため、必要な設定を WLC にプッシュします。

- WLC は、AireOS 8.x 以降が稼働する Cisco WLC でなければなりません。
- vWLC は ACL ベースの DNS をサポートしません
- Wireless Setup 展開で使用する予定のインターフェイス VLANs (ネットワーク) 用に WLC を設定します。デフォルトでは、WLC には管理インターフェイスがありますが、ゲストおよびセキュアアクセス (従業員) ネットワーク用に別のインターフェイスを設定することが推奨されます。
- ゲスト フローの場合、AUP の受け入れ (ホットスポット)、ログイン、またはクレデンシャルの作成のために、ACL_WEBAUTH_REDIRECT ACL を使用して、ゲスト デバイスがホットスポットまたはクレデンシャルを持つゲストポータルのいずれかにリダイレクトされます。承認されたゲストには、アクセスが許可されます (ACCESS-ACCEPT)。WLC で ACL を使用してゲストの権限を制限することができます。WLC で ACL を作成し、その ACL をゲスト権限 authz プロファイルで使用します。ISE 成功ページへのアクセスを許可するには、この ACL を WLC に追加します。限定的な ACL の作成の詳細については、<https://communities.cisco.com/docs/DOC-68169>を参照してください。

- Wireless Setup ではフローごとに WLAN が設定されます。フローに WLAN を設定したら、その WLAN は他のフローには使用できません。唯一の例外は、アカウント登録フロー用に WLAN を設定しており、後でこの WLAN を Sponsored Guest フロー (ゲストのアカウント登録とスポンサー処理の両方を扱うフロー) に使用することに決定した場合です。

実稼働環境で Wireless Setup を実行する場合、設定によって一部の既存ユーザの接続が切断されることがあります。

- Wireless Setup で WLC を使用してフローを設定したら、ISE ではその WLC を削除しないでください。
- ISE ですでに WLC を設定しているが、RADIUS オプションで共有秘密を設定していない場合、Wireless Setup で WLC を使用する前に共有秘密を追加する必要があります。
- ISE で WLC をすでに設定しており、共有秘密を設定している場合は、Wireless Setup で異なる共有秘密を設定しないでください。Wireless Setup と ISE のシークレットパスワードが一致している必要があります。選択する WLAN はフローで無効にされますが、フローの終わりで [本番稼働 (Go Live)] ボタンをクリックすると再度有効にできます。
- リモート LAN: ネットワークにリモート LAN が含まれている場合、Wireless Setup はリモート LAN にすでに割り当てられている VLAN ID を使用しようとする失敗します。この回避策として、リモート LAN を削除するか、または Wireless Setup を使用する前に WLC

で使用する予定の VLAN を作成しておきます。Wireless Setup では、フローに対してこれらの既存の VLAN を有効にできます。

- **FlexConnect** : Flexconnect ローカル スイッチおよび Flexconnect ACL は、Wireless Setup によって設定されますが、使用されず、サポートされていません。Wireless Setup は、Flexconnect 集中型またはローカル モード Ap および SSID でのみ動作します。

Cisco ワイヤレス LAN の設定の詳細については、<http://www.cisco.com/c/en/us/td/docs/wireless/technology/wlc/82463-wlc-config-best-practice.html>を参照してください。

ワイヤレス設定の例

次に示す WLC ログの一部には、フローの設定時に Wireless Setup により行われる設定の例が示されています。

```
"config radius auth add 1 192.168.201.228 1812 ascii cisco"
"config radius auth disable 1"
"config radius auth rfc3576 enable 1"
"config radius auth management 1 disable"
"config radius auth enable 1"
"config radius acct add 1 192.168.201.228 1813 ascii cisco"
"config radius acct enable 1"
"config acl create ACL_WEBAUTH_REDIRECT"
"config acl rule add ACL_WEBAUTH_REDIRECT 1"
"config acl rule action ACL_WEBAUTH_REDIRECT 1 permit"
"config acl rule source port range ACL_WEBAUTH_REDIRECT 1 53 53"
"config acl rule protocol ACL_WEBAUTH_REDIRECT 1 17"
"config acl rule add ACL_WEBAUTH_REDIRECT 1"
"config acl rule action ACL_WEBAUTH_REDIRECT 1 permit"
"config acl rule destination port range ACL_WEBAUTH_REDIRECT 1 53 53"
"config acl rule protocol ACL_WEBAUTH_REDIRECT 1 17"
"config acl rule add ACL_WEBAUTH_REDIRECT 1"
"config acl rule action ACL_WEBAUTH_REDIRECT 1 permit"
"config acl rule source address ACL_WEBAUTH_REDIRECT 1 192.168.201.228 255.255.255.255"
"config acl rule add ACL_WEBAUTH_REDIRECT 1"
"config acl rule action ACL_WEBAUTH_REDIRECT 1 permit"
"config acl rule destination address ACL_WEBAUTH_REDIRECT 1 192.168.201.228 255.255.255.255"
"config acl apply ACL_WEBAUTH_REDIRECT"
"show flexconnect acl summary"
"config flexconnect acl create ACL_WEBAUTH_REDIRECT"
"config flexconnect acl rule add ACL_WEBAUTH_REDIRECT 1"
"config flexconnect acl rule action ACL_WEBAUTH_REDIRECT 1 permit"
"config flexconnect acl rule source port range ACL_WEBAUTH_REDIRECT 1 53 53"
"config flexconnect acl rule protocol ACL_WEBAUTH_REDIRECT 1 17"
"config flexconnect acl rule add ACL_WEBAUTH_REDIRECT 1"
"config flexconnect acl rule action ACL_WEBAUTH_REDIRECT 1 permit"
"config flexconnect acl rule destination port range ACL_WEBAUTH_REDIRECT 1 53 53"
"config flexconnect acl rule protocol ACL_WEBAUTH_REDIRECT 1 17"
"config flexconnect acl rule add ACL_WEBAUTH_REDIRECT 1"
"config flexconnect acl rule action ACL_WEBAUTH_REDIRECT 1 permit"
"config flexconnect acl rule source address ACL_WEBAUTH_REDIRECT 1 192.168.201.228 255.255.255.255"
"config flexconnect acl rule add ACL_WEBAUTH_REDIRECT 1"
"config flexconnect acl rule action ACL_WEBAUTH_REDIRECT 1 permit"
"config flexconnect acl rule destination address ACL_WEBAUTH_REDIRECT 1 192.168.201.228 255.255.255.255"
"config flexconnect acl apply ACL_WEBAUTH_REDIRECT"
```


Active Directory と Wireless Setup

Sponsored Guest、802.1x、および BYOD のフローを作成するには、Active Directory ドメインが必要です。Active Directory は、スポンサー ポータル、802.1x セキュア アクセスおよび関連 VLAN、BYOD およびデバイス オンボーディングにアクセスできるスポンサー グループのユーザを指定します。Wireless Setup でいずれかのフローを設定したら、必要に応じて [ISE ID (ISE Identities)] に移動して次の項目を追加できます。

- スポンサーグループにマッピングされている内部スポンサーアカウント (ALL_ACCOUNTS など)。Active Directory を使用している場合は、これは不要です。
- ISE 内部従業員グループに含まれている従業員。内部従業員グループが許可ポリシーと ISE 内部従業員グループに追加されていることを確認してください。

Wireless Setup でのゲスト ポータル

企業の訪問者が企業のネットワークを使用してインターネットまたはネットワーク上のリソースおよびサービスにアクセスしようとしている場合、ゲストポータルを使用してネットワークアクセスを提供することができます。設定すると、従業員はゲストポータルを使用して会社のネットワークにアクセスできます。

3 つのデフォルトのゲスト ポータルがあります。

- ホットスポット ゲスト ポータル：ネットワーク アクセスはクレデンシアルを必要とせずに許可されます。通常、ネットワーク アクセスを許可する前にユーザ ポリシーの認可 (AUP) が承認される必要があります。
- Sponsored-Guest ポータル：ゲストのアカウントを作成したスポンサーによりネットワークアクセスが許可され、ゲストにログイン クレデンシアルが提供されます。
- アカウント登録ゲスト ポータル：ゲストは各自のアカウント クレデンシアルを作成できます。ネットワークアクセスが付与される前に、スポンサー承認が必要となることがあります。

Cisco ISE は、事前に定義されたデフォルト ポータルなど、複数のゲスト ポータルをホストすることができます。

デフォルトのポータルテーマには、管理者ポータルからカスタマイズできる標準のシスコブランドが適用されています。

Wireless Setup には独自のデフォルト テーマ (CSS) があります。ロゴ、バナー、背景画像、色、フォントなどの基本的な設定の一部を変更できます。ISE では、他の設定を変更することでポータルをさらにカスタマイズでき、高度なカスタマイズを行うこともできます。

ゲスト ポータル ワークフロー

1. ポータルのタイプを選択すると、使用するコントローラを選択するよう求められます。フローごとに新しいワイヤレス ネットワークを設定します。Wireless Setup でまだ使用していない既存の WLAN を選択するか、または新しい WLAN を作成することができます。

リダイレクトが必要なフローには、元の URL、正常完了ページ、または特定の URL（例：www.cisco.com）にユーザをリダイレクトするオプションがあります。元の URL を使用する場合は、WLC からのサポートが必要です。



(注) WLC バージョン 8.4 のリリースまでは、元の URL はサポートされていません。

2. ポータルの外観をカスタマイズし、基本設定を変更します。
3. カスタマイズが完了したら、テスト ポータルへの URL リンクをたどります。テスト ポータルに、ポータルのテストバージョンのプレビューが表示されます。フローを通過し、必要に応じてさらに変更を行うことができます。プレビュー ポータルで機能する正常完了時のリダイレクトは、[成功 (Success)] ページへのリダイレクトだけです。元の URL とステティック URL は、リダイレクトをサポートするためにワイヤレス セッションが必要であるため、機能しません。
4. 設定が完了しました。ワークフローにおいて Wireless Setup により ISE と WLC で実行されたステップをダウンロードして確認できます。



(注) Wireless Setup では基本ゲスト アクセスにはロケーションは使用されません。ローカル時刻に基づいてアクセスを制御する場合に、ロケーションが必要となります。ISEでのタイムゾーンの設定については、[SMS プロバイダーおよびサービス \(536 ページ\)](#) を参照してください。

ワイヤレス ネットワーク アカウント登録ポータル

アカウント登録ゲストポータルでは、ゲストが自分自身を登録し、自分のアカウントを作成して、ネットワークにアクセスできるようにすることができます。

ログオン成功ページではユーザに対して画面にログオンクレデンシャルが表示されるため、ログオン成功ページを選択しないことが推奨されます。ベストプラクティスは、ユーザにクレデンシャルを電子メールまたは SMS で受信することを要求することです。これにより、クレデンシャルが監査目的に特有の内容に関連付けられます。

ワイヤレス ネットワーク Sponsored Guest フロー

スポンサーはスポンサー ポータルを使用して、承認ユーザ用の一時アカウントを作成および管理し、企業ネットワークまたはインターネットにセキュアにアクセスできるようにします。ゲスト アカウントを作成した後、スポンサーは、スポンサー ポータルを使用して、印刷、電子メール送信、または携帯電話による送信を行ってゲストにアカウントの詳細を提供することもできます。アカウント登録ゲストに企業ネットワークへのアクセス権を提供する前に、スポンサーはゲスト アカウントを承認するように電子メールで要求されることがあります。

スポンサー フローで、Wireless Setup がスポンサー ポータルと Sponsored Guest ポータルを設定します。

承認フローは Wireless Setup ではサポートされていません。

ワークフローで Active Directory をスポンサー グループにマッピングします。ワークフローにより、選択された AD グループが ALL_ACCOUNTS スポンサー グループにマッピングされます。GROUP または OWN アカウント スポンサー グループは設定されません。必要に応じて、他の ID ソース（内部設定やLDAP 設定など）を追加するには、ISE 管理 UI を使用して追加します。ISE でのスポンサー グループの詳細については、http://www.cisco.com/c/en/us/td/docs/security/ise/2-1/admin_guide/b_ise_admin_guide_21/b_ise_admin_guide_20_chapter_01110.html#concept_0C4E9B15B81B4FE0ACD61178815E4272を参照してください。

Wireless Setup BYOD フロー：ネイティブ サプリカントおよび証明書のプロビジョニング

個人所有デバイスの持ち込み（BYOD）ポータルでは、従業員が各自のパーソナルデバイスを登録できます。ネイティブ サプリカント、証明書プロビジョニングはネットワークへのアクセスを許可する前にすることができます。従業員はBYODポータルに直接アクセスできません。パーソナルデバイスを登録するときにこのポータルにリダイレクトされます。従業員がパーソナルデバイスを使用してネットワークへ初めてアクセスしようとする、（iOS以外のデバイスの場合）手動で Network Setup Assistant（NSA）ウィザードをダウンロードして起動するように促されることがあります。NSA では、ネイティブ サプリカントの登録とインストールを順を追って実行できます。デバイスを登録すると、デバイスポータルを使用して、それを管理できます。

Wireless Setup は ISE とコントローラでネイティブ サプリカントと証明書のプロビジョニングを設定します。ユーザはコントローラにPEAP接続し、証明書を提供します。接続がEAP-TLS（証明書）に切り替わります。

Wireless Setup でサポートされるデバイスは、Apple デバイス（MAC および iOS）、Windows デスクトップ OS（モバイル以外）、および Android です。Chrome OS オンボーディングは、Wireless Setup ではサポートされていません。



- (注) デュアル SSID フローは、オンボーディング用のオープン ネットワークと、認証済みアクセス用の TLS 証明書ベースのセキュア ネットワークで構成されます。デバイスはオンボーディングなしでセキュア ネットワークに接続できます。これは、`basic_authenticated_access` デフォルト ルールにより、有効な認証はすべて通過できるためです。デバイスがセキュア ネットワークに接続する際に、BYOD セキュア 許可ルールに一致しないと、`basic_authenticated_access` のリストの下部に一致が移動します。

この対策として、許可ポリシーで `Basic_Authenticated_Access` ルールを無効にするか、特定の SSID (WLAN) に一致するようにこのルールを編集します。いずれの変更でも、許可しないデバイスへの PEAP 接続がブロックされます。



- (注) Wireless Setup には、ロストとマークされたデバイスをリダイレクトする許可ルールはありません。これはブラックリストと呼ばれ、ブラックリストポータルによって管理されます。ロストしたデバイスや盗まれたデバイスの管理については、http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/BYOD_Design_Guide/Managing_Lost_or_Stolen_Device.pdf を参照してください。

Wireless Setup での BYOD フロー

Wireless Setup での BYOD 設定は次のステップで構成されます。

1. ワイヤレス LAN コントローラを選択または登録
2. ワイヤレス ネットワークの追加：デュアル SSID の場合、この手順が 2 回実行されます。



- (注) 新しい ISE インストールには、デフォルトのワイヤレス ネットワークが含まれます。デュアル SSID BYOD では、ユーザが 2 番目の SSID にリダイレクトされると、ユーザのネットワーク プロファイルにデフォルトのネットワーク SSID が示されます。デフォルト SSID を削除するか、またはユーザにこの SSID を無視するように通知できます。

3. Active Directory (AD) の選択または AD への参加：オンボーディング VLAN と最終アクセス VLAN の両方のデフォルト VLAN 設定を上書きできます。最終アクセス VLAN は Active Directory グループにマッピングされます。
4. BYOD ポータルのカスタマイズ：BYOD ポータルとデバイス ポータルをここでカスタマイズできます。このステップでは、ISE がサポートするすべてのページをカスタマイズできます。このステップでは、すべてのポータルカスタマイズ内容が送信され、ポリシーが作成され、プロファイルが関連するポリシーにリンクされます。



(注) デバイス ポータルでは、BYOD ポータルのカスタマイズの基本カスタマイズが使用されます。Wireless Setup ではデバイス ポータルをカスタマイズできません。

5. 行った設定変更をプレビューして [完了 (Done)] を選択します。

デュアル SSID BYOD の場合

デュアル SSID BYOD をサポートするには、Fast SSID が有効になっている必要があります。ワイヤレス コントローラで Fast SSID Change が有効になっている場合、クライアントは SSID 間を高速で移動できます。高速 SSID が有効になっている場合、クライアントエントリがクリアされず、遅延は適用されません。Fast SSID の詳細と、Cisco WLC での Fast SSID の設定の詳細については、http://www.cisco.com/c/en/us/td/docs/wireless/controller/8-3/config-guide/b_cg83/b_cg83_chapter_0100001.htmlを参照してください。

推奨される WLC タイマー設定

Wireless Setup で使用する予定の WLC で、次のタイマーを設定しておくことが推奨されます。この設定は CLI に表示されます。

```
config radius auth retransmit-timeout {SERVER_INDEX} 5
config radius aggressive-failover disable
config radius fallback-test mode passive
config wlan exclusionlist {WLAN ID} 180
config wlan exclusionlist {WLAN ID} enabled
```

セキュア アクセス フロー

Wireless Setup フローにより、802.1x ワイヤレス LAN コントローラが PEAP (ユーザ名とパスワードのクレデンシャル) に対して設定されます。

このフローの一部で、Active Directory (AD) を指定するように求められます。従業員 AD グループを VLAN にマッピングできます。VLAN によってグループを分ける場合は、異なる従業員グループを異なる VLAN に設定することができます。[アクセス (access)] の横のドロップダウンをクリックすると、設定した AD で使用可能な AD グループが表示されます。

Active Directory でセキュアなアクセスを使用すると、AD グループを VLAN にマッピングしていない場合には、有効な AD ユーザに対してログインを許可する基本アクセスポリシーにユーザが一致します。Wireless Setup で AD グループを選択すると、各グループが VLAN にマッピングされます。

従業員がネットワークに接続する

1. 従業員のクレデンシャルが認証される : Cisco ISE は、社内 Active Directory と照合して従業員を認証し、許可ポリシーを提供します。

2. **デバイスが BYOD ポータルにリダイレクトされる**：デバイスが BYOD ポータルにリダイレクトされます。デバイスの MAC アドレスは自動的に事前設定されます。ユーザはデバイス名と説明を追加できます。
3. **ネイティブ サプリカントが設定される (MacOS、Windows、iOS、Android)**：ネイティブ サプリカントが設定されます。ただしこのプロセスはデバイスに応じて異なります。
 - **MacOS および Windows デバイス**：従業員が BYOD ポータルで [登録 (Register)] をクリックし、サプリカントプロビジョニングウィザードをダウンロードしてインストールします。このウィザードではサプリカントが設定され、EAP-TLS 証明書ベース認証に使用する証明書がインストールされます。デバイスの MAC アドレスと従業員のユーザ名が発行済み証明書に組み込まれます。
 - **iOS デバイス**：Cisco ISE ポリシー サーバは Apple の iOS ワイヤレス機能を使用して新しいプロファイルを iOS デバイスに送信します。このプロファイルには次の情報が含まれます。
 - 発行された証明書が、IOS デバイスの MAC アドレスおよび従業員のユーザ名と共に埋め込まれます。
 - 802.1X 認証の MSCHAPv2 または EAP-TLS の使用を強制できる Wi-Fi サプリカント プロファイル。
 - **Android デバイス**：Cisco ISE は、従業員に Google Play ストアから Cisco Network Setup Assistant (NSA) をダウンロードするように要求し、ルーティングします。アプリのインストール後に、従業員は NSA を開いてセットアップウィザードを開始できます。このウィザードでは、サプリカントの設定と、デバイスの設定に使用される発行済み証明書が生成されます。
 - **認可変更が発行される**：ユーザがオンボーディング フローを通過すると、Cisco ISE は認可変更 (CoA) を開始します。これにより、MacOS X、Windows、および Android デバイスは EAP-TLS を使用してセキュアな 802.1X ネットワークに再接続します。シングル SSID の場合、iOS デバイスも自動的に接続されますが、デュアル SSID の場合、ウィザードは iOS ユーザに手動で新しいネットワークに接続するように要求します。

ネイティブ サプリカントは、次のオペレーティング システムでサポートされます。

- Android (Amazon Kindle、B&N Nook を除く)
- Mac OS X (Apple Mac コンピュータの場合)
- Apple iOS デバイス (Apple iPod、iPhone、および iPad)
- Microsoft Windows 7、8 (RT を除く)、Vista、および 10

Wireless Setup による ISE と WLC の変更

Wireless Setup では、フローをステップに従って進むことで ISE とコントローラが設定されます。Wireless Setup は、行った変更のリストを各フローの終わりで表示します。各フローの変更内容がここで参考のために表示されます。これにより、Wireless Setup が ISE に対して行ったすべての変更を確認し、変更内容をレビューまたは変更できます。

• ホットスポット

- [ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [ゲスト ポータル (Guest Portals)] > [ホットスポット ポータル (Hotspot Portal)]
- [ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] > [許可プロファイル (Authorization Profiles)]
- [ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [許可ポリシー (Authorization Policy)]

• アカウント登録

- [ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [ゲスト ポータル (Guest Portals)] > [アカウント登録ポータル (Self-reg Portal)]
- [ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [ゲスト タイプ (Guest Types)] > [ゲスト タイプ (Guest Types)]
- [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [許可 (Authorization)] > [許可プロファイル (Authorization Profiles)]
- [ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [許可ポリシー (Authorization Policy)]
- [管理 (Administration)] > [システム (System)] > [設定 (Settings)] > [SMTP サーバ (SMTP Server)]
- [管理 (Administration)] > [システム (System)] > [設定 (Settings)] > [SMTP ゲートウェイ (SMTP Gateway)]

• スポンサー

- [ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [ゲスト ポータル (Guest Portals)] > [Sponsored Guest ポータル (Sponsored Guest Portal)] >
- [ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [スポンサー ポータル (Sponsor Portals)] > > [スポンサー ポータル (Sponsor Portal)] >

- [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [許可 (Authorization)] > [許可プロファイル (Authorization Profiles)]
- [ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [許可ポリシー (Authorization Policy)]
- [ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [スポンサー (Sponsor)] > [スポンサーグループ (Sponsor Groups)]
- [ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [ゲスト タイプ (Guest Types)] > [ゲスト タイプ (Guest Types)]
- [ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [外部 ID ソース (Ext ID Sources)] > [Active Directory]
- **BYOD**
 - [ワーク センター (Work Centers)] > **BYOD** > [ポータルとコンポーネント (Portals & Components)] > [BYOD ポータル (BYOD Portals)] > [BYOD ポータル (BYOD Portal)]
 - [ワーク センター (Work Centers)] > **BYOD** > [ポータルとコンポーネント (Portals & Components)] > [デバイス ポータル (My Devices Portals)] > [デバイス ポータル (My Devices Portal)]
 - [ワーク センター (Work Centers)] > [BYOD] > [ポリシー要素 (Policy Elements)] > [許可 (Authorization)] > [許可プロファイル (Authorization Profiles)]
 - [ワーク センター (Work Centers)] > [BYOD] > [許可ポリシー (Authorization Policy)]
 - [ワーク センター (Work Centers)] > [BYOD] > [外部 ID ソース (Ext ID Sources)] > [Active Directory]
 - [ワーク センター (Work Centers)] > [BYOD] > [外部 ID ソース (Ext ID Sources)] > [Active Directory] を選択し、AD を選択し、[グループ (Groups)] タブを選択します。
- **セキュアなアクセス**
 - [ポリシー (Policy)] > [許可 (Authorization)] > [許可ポリシー (Authorization Policy)]
 - [ポリシー (Policy)] > [ポリシー セット (Policy Sets)]
 - [ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [外部 ID ソース (Ext ID Sources)] > [Active Directory] を選択し、AD を選択し、[グループ (Groups)] タブを選択します。
- **ワイヤレス LAN コントローラ**
 - **WLAN**

- **[セキュリティ (Security)] > [アクセス制御リスト (Access Control Lists)]** : Wireless Setup では次の ACL が作成されます。
 - ゲストと BYOD 用のリダイレクト ACL
- Wireless Setup により、**[セキュリティ (Security)] > [AAA] > [認証およびアカウントिंग (Authentication and Accounting)]** にもエントリが作成されます。



第 II 部

Cisco ISE ノードの展開

- [分散環境での Cisco ISE の設定 \(55 ページ\)](#)



第 4 章

分散環境での Cisco ISE の設定

- [Cisco ISE 展開の用語](#) (55 ページ)
- [分散 Cisco ISE 展開のペルソナ](#) (56 ページ)
- [Cisco ISE 分散展開](#) (56 ページ)
- [Cisco ISE ノードの設定](#) (60 ページ)
- [管理ノード](#) (63 ページ)
- [ポリシー サービス ノード](#) (72 ページ)
- [モニタリング ノード](#) (73 ページ)
- [pxGrid ノード](#) (76 ページ)
- [展開内のノードの表示](#) (81 ページ)
- [プライマリおよびセカンダリの Cisco ISE ノードの同期](#) (81 ページ)
- [ノード ペルソナとサービスの変更](#) (82 ページ)
- [Cisco ISE でのノードの変更による影響](#) (82 ページ)
- [ポリシー サービス ノード グループの作成](#) (83 ページ)
- [ISE pxGrid ノードの展開](#) (84 ページ)
- [自動フェールオーバー用のモニタリング ノードの設定](#) (85 ページ)
- [展開からのノードの削除](#) (86 ページ)
- [スタンドアロン Cisco ISE ノードのホスト名または IP アドレスの変更](#) (87 ページ)
- [Cisco ISE アプライアンス ハードウェアの交換](#) (88 ページ)

Cisco ISE 展開の用語

次の用語は Cisco ISE 展開シナリオの説明に一般に使用されるものです。

- サービス：サービスは、ネットワークアクセス、プロファイラ、ポスチャ、セキュリティグループアクセス、モニタリング、トラブルシューティングなどの、ペルソナが提供する固有の機能です。
- ノード：Cisco ISE ソフトウェアを実行する個別インスタンスです。Cisco ISE はアプライアンスとして使用でき、VMware で実行できるソフトウェアとしても使用できます。Cisco ISE ソフトウェアを実行する各インスタンス、アプライアンス、または VMware はノードと呼ばれます。

- ペルソナ：ノードのペルソナによって、そのノードが提供するサービスが決まります。Cisco ISE ノードは、管理、ポリシー サービス、モニタリング、および pxGrid のペルソナのいずれかを担うことができます。管理者ポータルで使用できるメニューオプションは、Cisco ISE ノードが担当するロールおよびペルソナによって異なります。
- 展開モデル：展開が分散か、スタンドアロンか、スタンドアロンのハイ アベイラビリティ（基本的な 2 ノード構成）かを決定します。

分散 Cisco ISE 展開のペルソナ

Cisco ISE ノードは、管理、ポリシー サービス、またはモニタリングのペルソナを担当できます。

Cisco ISE ノードは担当するペルソナに基づき、各種のサービスを提供できます。導入の各ノードは、管理、ポリシー サービス、およびモニタリングのペルソナのいずれかを担当することができます。分散展開では、ネットワーク上で次の組み合わせのノードを使用できます。

- ハイ アベイラビリティ用のプライマリ管理ノードとセカンダリ管理ノード
- 自動フェールオーバー用の管理ノードのヘルス チェック用の非管理ノードの 1 つまたはペア
- PAN 自動フェールオーバー用のヘルス チェック ノードのペアまたは単一のヘルス チェック ノード
- セッション フェールオーバー用の 1 つ以上のポリシー サービス ノード

Cisco ISE 分散展開

複数の Cisco ISE ノードがある展開は、分散展開と呼ばれます。フェールオーバーをサポートし、パフォーマンスを改善するために、展開に複数の Cisco ISE ノードを分散方式でセットアップできます。Cisco ISE の分散展開では、管理およびモニタリング アクティビティは一元化され、処理はポリシー サービス ノード間で分配されます。パフォーマンスのニーズに応じて、導入環境の規模を変更できます。展開の各 Cisco ISE ノードは、管理、ポリシー サービス、およびモニタリングのペルソナのいずれかを担当することができます。

Cisco ISE 展開の設定

『Cisco Identity Services Engine Hardware Installation Guide』で説明されているように Cisco ISE をすべてのノードにインストールした後、ノードはスタンドアロン状態で稼働します。次に、1 つのノードをプライマリ PAN として定義する必要があります。プライマリ PAN の定義時に、そのノードで管理ペルソナおよびモニタリング ペルソナを有効にする必要があります。任意で、プライマリ PAN でポリシー サービス ペルソナを有効にできます。プライマリ PAN のペ

ルソナ定義のタスクの完了後に、他のセカンダリ ノードをプライマリ PAN に登録し、セカンダリ ノードのペルソナを定義できます。

すべての Cisco ISE システムおよび機能に関連する設定は、プライマリ PAN でだけ実行する必要があります。プライマリ PAN で行った設定の変更は、展開内のすべてのセカンダリ ノードに複製されます。

分散展開内にモニタリングノードが少なくとも1つ存在する必要があります。プライマリ PAN の設定時に、モニタリングペルソナを有効にする必要があります。展開内のモニタリングノードを登録した後、必要に応じてプライマリ PAN を編集したり、モニタリングペルソナを無効にしたりできます。

プライマリ ISE ノードからセカンダリ ISE ノードへのデータ レプリケーション

1 つの Cisco ISE ノードをセカンダリ ノードとして登録すると、Cisco ISE はプライマリ ノードからセカンダリ ノードへのデータ レプリケーションチャンネルをすぐに作成し、複製のプロセスを開始します。複製は、プライマリ ノードからセカンダリ ノードに Cisco ISE 設定データを共有するプロセスです。複製によって、展開を構成するすべての Cisco ISE ノードの設定データの整合性を確実に維持できます。

通常、最初に ISE ノードをセカンダリ ノードとして登録したときに、完全な複製が実行されます。完全な複製の実行後は差分複製が実行され、PAN での設定データに対する新しい変更（追加、変更、削除など）がセカンダリ ノードに反映されます。複製のプロセスでは、展開内のすべての Cisco ISE ノードが同期されます。Cisco ISE 管理者ポータルでの展開のページから [ノードステータス (Node Status)] 列で複製のステータスを表示できます。セカンダリ ノードとして Cisco ISE ノードを登録するか、または PAN との手動同期を実行すると、要求されたアクションが進行中であることを示すオレンジのアイコンがノードステータスに表示されます。これが完了すると、ノードステータスは、セカンダリ ノードが PAN と同期されたことを示す緑に変わります。

Cisco ISE ノードの登録解除

展開からノードを削除するには、ノードの登録を解除する必要があります。プライマリ PAN からセカンダリ ノードの登録を解除すると、登録解除されたノードのステータスがスタンダアロンに変わり、プライマリ ノードとセカンダリ ノード間の接続が失われます。複製の更新は、登録解除されたスタンダアロン ノードに送信されなくなります。

PSN の登録が取り消されると、エンドポイント データは失われます。スタンダアロン ノードになった後も PSN にエンドポイント データを残すには、以下のいずれかを実行します。

- プライマリ PAN からバックアップを取得し、PSN がスタンダアロン ノードになったときに、このデータ バックアップを復元します。
- PSN のペルソナを管理者（セカンダリ PAN）に変更し、管理者ポータルでの展開ページからデータを同期してから、ノードを登録解除します。この時点で、このノードに、すべてのデータがあります。この後、既存の展開にセカンダリ管理ノードを追加できます。



(注) プライマリ PAN は登録解除できません。

分散展開を設定する場合のガイドライン

分散環境で Cisco ISE を設定する前に、次の内容をよく読んでください。

- ノードタイプ、ISE ノード、を選択します。管理、ポリシーサービス、およびモニタリング機能の場合は、ISE ノードを選択する必要があります。
- すべてのノードで、同じ Network Time Protocol (NTP) サーバを選択します。ノード間のタイムゾーンの問題を回避するには、各ノードのセットアップ中に同じ NTP サーバ名を指定する必要があります。この設定で、展開内にあるさまざまなノードからのレポートとログが常にタイムスタンプで同期されるようになります。
- Cisco ISE のインストール時に Cisco ISE 管理パスワードを設定します。以前の Cisco ISE 管理のデフォルトのログインクレデンシャル (admin/cisco) は無効になっています。初期セットアップ中に作成したユーザ名とパスワードを使用するか、または後でパスワードを変更した場合はそのパスワードを使用します。
- ドメイン ネーム システム (DNS) サーバを設定します。DNS サーバに、分散展開に含まれるすべての Cisco ISE ノードの IP アドレスと完全修飾ドメイン名 (FQDN) を入力します。解決できない場合は、ノード登録が失敗します。
- DNS サーバに、分散展開のすべての Cisco ISE ノードの逆引き DNS ルックアップを設定します。設定しなかった場合、Cisco ISE ノードの登録時および再起動時に、展開に関する問題が発生することがあります。すべてのノードで逆引き DNS ルックアップが設定されていない場合、パフォーマンスが低下する可能性があります。
- (任意) プライマリ PAN からセカンダリ Cisco ISE ノードを登録解除して、Cisco ISE をアンインストールします。
- プライマリ モニタリング ノードをバックアップし、新しいセカンダリ モニタリング ノードにデータを復元します。これにより、新しい変更内容が複製されるため、プライマリ モニタリング ノードの履歴が新しいセカンダリ ノードと同期状態となります。
- プライマリ PAN と、セカンダリ ノードとして登録しようとしているスタンドアロン ノードで、同じバージョンの Cisco ISE が実行されていることを確認します。

プライマリ ノードおよびセカンダリ ノードで使用可能なメニュー オプション

分散展開を構成する Cisco ISE ノードで使用可能なメニュー オプションは、ノードで有効なペルソナによって異なります。すべての管理およびモニタリングアクティビティは、プライマリ PAN を介して実行する必要があります。その他のタスクについては、セカンダリ ノードを使

用する必要があります。このため、セカンダリ ノードのユーザ インターフェイスでは、ノードで有効なペルソナに基づく限定されたメニュー オプションが提供されます。

1 つのノードが、ポリシー サービス ペルソナとアクティブ ロールのモニタリング ペルソナを担当するなど、複数のペルソナを担当する場合、ポリシー サービス ノードおよびアクティブ モニタリング ノードにリストされているメニュー オプションがそのノードで使用可能となります。

次の表に、さまざまなペルソナとなる Cisco ISE ノードで使用可能なメニュー オプションを示します。

表 2: Cisco ISE ノードおよび使用可能なメニュー オプション

Cisco ISE ノード	使用可能なメニュー オプション
すべてのノード	<ul style="list-style-type: none"> システム時刻と NTP サーバ設定の表示および設定。 サーバ証明書のインストール、証明書署名要求の管理。すべてのサーバ証明書を一元的に管理するプライマリ PAN 経由で、展開内のすべてのノードに対し、サーバ証明書の操作を実行できます。 <p>(注) 秘密キーは、ローカル データベースに格納されず、関連ノードからコピーされません。秘密キーは、ローカル ファイル システムに格納されます。</p>
プライマリ PAN	すべてのメニューおよびサブメニュー。
アクティブ モニタリング ノード	<ul style="list-style-type: none"> ホームおよび操作メニュー。 プライマリ モニタリング ノードおよびアクティブ モニタリング ノードの両方からモニタリング データにアクセスできることで、冗長アクセスが提供されます。
ポリシー サービス ノード	Active Directory 接続への参加、脱退、およびテストを行うオプション。各ポリシー サービス ノードが別個に Active Directory ドメインに参加している必要があります。最初にドメイン情報を定義し、PAN を Active Directory ドメインに参加させる必要があります。次に、他のポリシー サービス ノードを Active Directory ドメインに個別に参加させます。

Cisco ISE ノード	使用可能なメニュー オプション
セカンダリ PAN	<p>セカンダリ PAN をプライマリ PAN に昇格させるオプション。</p> <p>(注) プライマリ PAN にセカンダリ ノードを登録した後は、いずれのセカンダリ ノードの管理者ポータルにログインする場合にも、プライマリ PAN のログインクレデンシャルを使用する必要があります。</p>

Cisco ISE ノードの設定

Cisco ISE ノードをインストールすると、管理ペルソナ、ポリシー サービス ペルソナ、およびモニタリング ペルソナによって提供されるすべてのデフォルト サービスがそのノードで実行されます。このノードはスタンドアロン状態となります。Cisco ISE ノードの管理者ポータルにログインして設定する必要があります。スタンドアロン Cisco ISE ノードのペルソナまたはサービスは編集できません。ただし、プライマリおよびセカンダリ Cisco ISE ノードのペルソナおよびサービスは編集できます。最初にプライマリ ISE ノードを設定し、その後、セカンダリ ISE ノードをプライマリ ISE ノードに登録する必要があります。

ノードに初めてログインする場合は、デフォルトの管理パスワードを変更し、有効なライセンスをインストールする必要があります。

設定済みの Cisco ISE または本番環境では、ホスト名とドメイン名を変更しないことを推奨します。これが必要な場合は、初期展開時にアプライアンスのイメージを再作成し、変更を加え、詳細を設定します。

始める前に

Cisco ISE での分散展開の設定方法に関する基礎を理解しておく必要があります。分散展開を設定する場合のガイドラインを参照してください。

ステップ 1 [管理 (Administration)] > [システム (System)] > [展開 (Deployment)] を選択します。

ステップ 2 設定する Cisco ISE ノードの隣にあるチェックボックスをオンにし、[編集 (Edit)] をクリックします。

ステップ 3 必要に応じて値を入力し、[保存 (Save)] をクリックします。

プライマリ PAN の設定

分散展開を設定するには、最初に Cisco ISE ノードをプライマリ PAN として設定する必要があります。

ステップ 1 [管理 (Administration)] > [システム (System)] > [展開 (Deployment)] を選択します。

当初は [登録 (Register)] ボタンが無効になっています。このボタンを有効にするには、プライマリ PAN を設定する必要があります。

ステップ 2 現在のノードの隣にあるチェックボックスをオンにして [編集 (Edit)] をクリックします。

ステップ 3 [プライマリにする (Make Primary)] をクリックして、プライマリ PAN を設定します。

ステップ 4 [全般設定 (General Settings)] タブでデータを入力します。

ステップ 5 [保存 (Save)] をクリックしてノード設定を保存します。

次のタスク

1. 展開にセカンダリ ノードを追加します。
2. 必要に応じて、プロファイラ サービスを有効にし、プローブを設定します。

関連トピック

[管理ノード \(63 ページ\)](#)

[Cisco ISE 分散展開 \(56 ページ\)](#)

[分散展開を設定する場合のガイドライン \(58 ページ\)](#)

[管理ノードのハイ アベイラビリティ \(63 ページ\)](#)

[セカンダリ PAN のプライマリへの手動昇格 \(71 ページ\)](#)

[セカンダリ Cisco ISE ノードの登録 \(61 ページ\)](#)

セカンダリ Cisco ISE ノードの登録

セカンダリ ノードを登録した後、プライマリ ノードのデータベースにセカンダリ ノードの設定が追加され、セカンダリ ノードのアプリケーション サーバが再起動します。再起動が完了した後、セカンダリ ノードでは、そのノードに対して有効にしたペルソナおよびサービスが実行されます。プライマリ PAN の [展開 (Deployment)] ページで、行ったすべての設定変更を表示できます。ただし、変更が反映され、[展開 (Deployment)] ページに表示されるには 5 分間の遅延が生じます。

始める前に

プライマリ ノードの信頼できる証明書ストアに、登録するセカンダリ ノードの HTTPS 証明書を検証するための適切な認証局 (CA) 証明書があることを確認します。信頼できる証明書ストアにセカンダリ ノードの証明書をインポートする場合は、セカンダリ ノードの証明書を検証するようにプライマリ PAN の [ISE 内の認証用に信頼する (Trust for authentication within ISE)] チェックボックスをオンにします。

セカンダリ ノードをプライマリ ノードに登録した後、セカンダリ ノードで HTTPS 証明書を変更する場合は、プライマリ ノードの信頼できる証明書ストアに適切な CA 証明書をインポートする必要があります。

プライマリ PAN の信頼できる証明書ストアにインポートする証明書はセカンダリ ノードに複製されます。

ハイアベイラビリティを実現するために2つの管理ノードを展開する場合は、セカンダリ PAN を登録してから、その他のセカンダリ ノードを登録します。この順序でノードを登録する場合は、セカンダリ PAN をプライマリに昇格させた後にセカンダリ ISE ノードを再起動する必要はありません。

セッション サービスを実行する複数のポリシー サービス ノードを、ノード間の相互フェールオーバーを設定して展開する場合は、ノード グループにポリシー サービス ノードを配置します。ノードを登録する前にノード グループを作成する必要があります。

ステップ 1 プライマリ PAN にログインします。

ステップ 2 [管理 (Administration)] > [システム (System)] > [展開 (Deployment)] を選択します。

ステップ 3 [登録 (Register)] > [ISE ノードの登録 (Register an Cisco ISE Node)] を選択して、セカンダリ ノードを登録します。

ステップ 4 セカンダリ ノードの DNS 解決可能なホスト名を入力します。

Cisco ISE ノードの登録時にホスト名を使用する場合、登録するスタンドアロンノードの完全修飾ドメイン名 (FQDN) (たとえば、*abc.xyz.com*) は、プライマリ PAN から DNS を使用して解決できる必要があります。解決できない場合は、ノード登録が失敗します。DNS サーバでセカンダリ ノードの IP アドレスおよび FQDN を事前に定義しておく必要があります。

ステップ 5 [ユーザー名 (Username)] フィールドおよび [パスワード (Password)] フィールドに、セカンダリ ノードの UI ベースの管理者クレデンシャルを入力します。

ステップ 6 [Next] をクリックします。

Cisco ISE はセカンダリ ノードに接続し、ホスト名、デフォルトゲートウェイなどの基本情報を取得して、表示します。

セカンダリ ノードを登録するよう選択している場合は、セカンダリ ノードの設定を編集できます。

ステップ 7 [保存 (Save)] をクリックします。

セカンダリ ノードが正常に登録されると、プライマリ PAN で、ノードの正常な登録を確認するアラームを受信します。セカンダリ ノードのプライマリ PAN への登録が失敗した場合は、このアラームは生成されません。ノードが登録されると、そのノードのアプリケーションサーバが再起動します。登録およびデータベース同期が正常に完了した後、セカンダリ ノードのユーザインターフェイスにログインするにはプライマリ PAN のクレデンシャルを入力します。



(注) 展開の既存のプライマリ ノードに加えて、新しいノードの登録に成功した場合は、新しく登録されたノードに対応するアラームは表示されません。設定変更アラームは、新しく登録されたノードに対応する情報を反映します。新しいノードが正常に登録されたことを確認するためにこの情報を使用できます。

次のタスク

- ゲストユーザのアクセスと許可、ロギングなどの時間依存タスクの場合は、ノード間のシステム時刻が同期されていることを確認します。
- セカンダリ PAN を登録し、内部 Cisco ISE CA サービスを使用する場合は、プライマリ PAN から Cisco ISE CA 証明書およびキーをバックアップし、セカンダリ PAN に復元する必要があります。

関連トピック

[プライマリ ISE ノードからセカンダリ ISE ノードへのデータ レプリケーション](#) (57 ページ)

[管理ノード](#) (63 ページ)

[ポリシー サービス ノード](#) (72 ページ)

[モニタリング ノード](#) (73 ページ)

[管理ノードのハイ アベイラビリティ](#) (63 ページ)

[ポリシー サービス ノードのハイ アベイラビリティ](#) (72 ページ)

[モニタリング ノードでの自動フェールオーバー](#) (74 ページ)

[セカンダリ PAN のプライマリへの手動昇格](#) (71 ページ)

[ポリシー サービス ノード グループの作成](#) (83 ページ)

[自動フェールオーバー用のモニタリング ノードの設定](#) (85 ページ)

管理ノード

管理ペルソナの Cisco ISE ノードは、Cisco ISE のすべての管理操作を実行することができます。認証、許可、監査などの機能に関連したすべてのシステム関連設定を処理します。分散環境では、最大2つの管理ペルソナを実行するノードを実行できます。管理ペルソナは、スタンダード、プライマリ、またはセカンダリのロールのいずれかを担当できます。

管理ノードのハイ アベイラビリティ

ハイアベイラビリティ構成では、プライマリ管理ノード (PAN) がアクティブな状態です。セカンダリ PAN (バックアップ PAN) はスタンバイ状態です。これは、セカンダリ PAN がプライマリ PAN からすべての設定更新を受信するものの、ISE ネットワークではアクティブではないことを意味します。

Cisco ISE は、手動および自動フェールオーバーをサポートします。自動フェールオーバーでは、プライマリ PAN がダウンした場合にセカンダリ PAN の自動プロモーションが開始されます。自動フェールオーバーでは、ヘルス チェック ノードと呼ばれる非管理セカンダリ ノードが必要です。ヘルス チェック ノードは、プライマリ PAN の正常性を確認します。プライマリ PAN がダウンまたは到達不能であることが検出された場合、ヘルス チェック ノードがセカンダリ PAN のプロモーションを開始して、プライマリ ロールが引き継がれます。

自動フェールオーバー機能を展開するには、少なくとも 3 つのノードが必要です。このうち 2 つのノードが管理ペルソナとなり、1 つのノードはヘルスチェックノードとして機能します。ヘルスチェックノードは非管理ノードで、ポリシーサービスノード、モニタリングノード、または pxGrid ノード、あるいはそれらの組み合わせにできます。これらの PAN が異なるデータセンターにある場合、それぞれの PAN にヘルスチェックノードが必要です。

次の表に、プライマリ PAN がダウンし、セカンダリ PAN がまだ引き継がれていない場合に影響を受ける機能を示します。

機能	プライマリ PAN のダウン時に使用できるかどうか（はい/いいえ）
既存の内部ユーザの RADIUS 認証	○
既存または新しい AD ユーザの RADIUS 認証	○
プロファイル変更がない既存のエンドポイント	○
プロファイル変更がある既存のエンドポイント	なし
プロファイリングで学習した新しいエンドポイント。	なし
既存のゲスト：LWA	○
既存のゲスト：CWA	はい（自動デバイス登録機能を持つホットスポット、BYOD、CWA などのデバイス登録に有効なフローを除く）
ゲストのパスワード変更	なし
ゲスト：AUP	なし
ゲスト：ログイン失敗の最大回数の適用	なし
新しいゲスト（Sponsored-Guest またはアカウント登録）	なし
ポスチャ（Posture）	○
内部 CA による BYOD	なし
登録済みの既存のデバイス	○
MDM オンボーディング	なし
pxGrid サービス	なし

内部認証局による証明書のプロビジョニングをサポートするには、プロモーションの後に、元のプライマリ PAN のルート証明書とそのキーを新しいプライマリ ノードにインポートする必要があります。セカンダリ ノードからプライマリ PAN へのプロモーションの後に追加された PSN ノードでは、自動フェールオーバー後に証明書のプロビジョニングが機能しません。

関連トピック

[自動フェールオーバー用のモニタリング ノードの設定](#) (85 ページ)

ハイ アベイラビリティのヘルス チェック ノード

プライマリ PAN のヘルス チェック ノードをアクティブ ヘルス チェック ノードと呼びます。セカンダリ PAN のヘルス チェック ノードをパッシブ ヘルス チェック ノードと呼びます。アクティブ ヘルス チェック ノードは、プライマリ PAN のステータスを検査し、管理ノードの自動フェールオーバーを管理します。ヘルス チェック ノードとして 2 つの非管理 ISE ノードを使用することをお勧めします。1 つはプライマリ PAN、もう 1 つはセカンダリ PAN です。1 つだけヘルス チェック ノードを使用する場合、そのノードがダウンすると、自動フェールオーバーは発生しません。

両方の PAN が同じデータセンターにある場合、1 つの非管理 ISE ノードをプライマリ PAN とセカンダリ PAN の両方のヘルス チェック ノードとして使用できます。単一のヘルス チェック ノードがプライマリ PAN とセカンダリ PAN の両方の状態を検査する場合、そのノードはアクティブ/パッシブ両方の役割を担います。

ヘルス チェック ノードは非管理ノードです。つまり、ポリシー サービス ノード、モニタリング ノード、または pxGrid ノード、あるいはそれらの組み合わせにできます。管理ノードと同じデータセンター内の PSN ノードをヘルス チェック ノードとして指定することをお勧めします。ただし、2 つの管理ノードが同じ場所（LAN またはデータセンター）にない小規模または一元化された展開では、管理ペルソナを持っていないノード（PSN/pxGrid/MnT）をヘルス チェック ノードとして使用できます。

自動フェールオーバーを無効にし、プライマリ PAN の障害発生時に手動でセカンダリ ノードを昇格させることを選択した場合には、チェック ノードは不要です。

セカンダリ PAN のヘルス チェック ノード

セカンダリ PAN のヘルス チェック ノードはパッシブ モニタです。セカンダリ PAN がプライマリ PAN として昇格するまで、このノードはアクションを実行しません。セカンダリ PAN がプライマリ ロールを引き継ぐと、関連するヘルス チェック ノードは管理ノードの自動フェールオーバーを管理するアクティブ ロールを担います。以前のプライマリ PAN のヘルス チェック ノードはセカンダリ PAN のヘルス チェック ノードになり、受動的にモニタリングを行います。

ヘルス チェックの無効化と再起動

ノードがヘルス チェック ロールから削除された場合、または自動フェールオーバー設定が無効な場合、ヘルス チェック サービスはそのノードで停止します。自動フェールオーバー設定が指定されたハイアベイラビリティヘルス チェック ノードでイネーブルになると、ノードは管理ノードの正常性のチェックを再度開始します。ノードでハイアベイラビリティヘルス

チェック ロールを指定または削除しても、そのノードのいずれのアプリケーションが再起動されることはありません。ヘルス チェック アクティビティのみが開始または停止します。

ハイアベイラビリティのヘルス チェック ノードを再起動すると、プライマリ PAN の以前のダウンタイムが無視され、再びヘルス ステータスのチェックが開始されます。

ヘルス チェック ノード

アクティブなヘルス チェック ノードは、設定したポーリング間隔でプライマリ PAN のヘルス ステータスをチェックします。ヘルス チェック ノードはプライマリ PAN に要求を送信し、それに対する応答が設定内容に一致する場合は、プライマリ PAN が良好な状態であると見なします。そうでなければ、ヘルス チェック ノードはプライマリ PAN が不良な状態であると見なします。プライマリ PAN の状態が設定済みフェールオーバー期間を超えて継続的に不良である場合、ヘルス チェック ノードはセカンダリ PAN へのフェールオーバーを開始します。

ヘルス チェックの任意の時点で、フェールオーバー期間中に不良と報告されたヘルス ステータスがその後で良好になったことが検出されると、ヘルス チェック ノードはプライマリ PAN のステータスを良好としてマークし、ヘルス チェック サイクルをリセットします。

プライマリ PAN ヘルス チェックからの応答は、そのヘルス チェック ノードで使用可能な設定値に照らして検証されます。応答が一致しない場合、アラームが発生します。ただし、プロモーション要求はセカンダリ PAN に行われます。

ヘルス ノードの変更

ヘルス チェックに使用している ISE ノードを変更できますが、考慮すべき点があります。

たとえば、ヘルス チェック ノード (H1) が非同期になり、他のノード (H2) がプライマリ PAN のヘルス チェック ノードになったとします。この場合、プライマリ PAN がダウンした時点で、同じプライマリ PAN を検査している別のノード (H2) があることを N1 が認識する方法はありません。その後、H2 がダウンしたりネットワークから切断されたりした場合に、実際のフェールオーバーが必要になります。しかし、セカンダリ PAN はプロモーション要求を拒否する権限を保持します。したがって、セカンダリ PAN がプライマリ ロールに昇格すると、H2 からのプロモーション要求が拒否されてエラーが発生します。プライマリ PAN のヘルス チェック ノードは、非同期になった場合でもプライマリ PAN の状態を引き続き検査します。

セカンダリ PAN への自動フェールオーバー

プライマリ PAN が使用できなくなったときにセカンダリ PAN を自動的に昇格させるように ISE を設定できます。この設定は、**[管理 (Administration)] > [システム (System)] > [展開 (Deployment)]** ページのプライマリ管理ノード (プライマリ PAN) で行うことができます。フェールオーバー時間は、「**フェールオーバーの前に障害が発生したポーリング数 (Number of Failure Polls before Failover)**」で設定された回数と「**ポーリング間隔 (Polling Interval)**」で設定された秒数をかけて得られる値として定義されます。デフォルト設定では、この時間は 10 分です。セカンダリ PAN からプライマリへの昇格には、さらに 10 分かかります。つまりデ

フォルトでは、プライマリ PAN の障害発生からセカンダリ PAN の動作開始までの時間は 20 分です。

セカンダリ PAN がフェールオーバー コールを受信すると、実際のフェールオーバーに進む前に、次の検証が行われます。

- ネットワークでプライマリ PAN が使用不能になっている。
- 有効なヘルス チェック ノードからフェールオーバー要求が受信された。
- この PAN に関するフェールオーバー要求である。

すべての検証に合格すると、セカンダリ PAN はプライマリ ロールに自身を昇格させます。

次に、セカンダリ PAN の自動フェールオーバーが試行されるシナリオのサンプルを示します（ただしこれに限定されません）。

- ポーリング期間中に、プライマリ PAN の正常性が「フェールオーバーの前に障害が発生したポーリング数（Number of failure polls before failover）」の値に対して一貫して良好でない。
- プライマリ PAN 上の Cisco ISE サービスが手動で停止され、フェールオーバー時間にわたって停止状態のままである。
- ソフト停止またはリブート オプションを使ってプライマリ PAN がシャットダウンされ、設定済みのフェールオーバー時間にわたってシャットダウン状態のままである。
- プライマリ PAN が突然ダウン（電源オフ）し、フェールオーバー時間にわたってダウン状態のままである。
- プライマリ PAN のネットワーク インターフェイスがダウンした（ネットワーク ポートが閉じた、またはネットワーク サービスがダウンした）、あるいは他の理由でヘルス チェック ノードから到達不能になり、設定済みのフェールオーバー時間にわたってダウン状態のままである。

ヘルス チェック ノードの再起動

ハイアベイラビリティのヘルス チェック ノードを再起動すると、プライマリ PAN の以前のダウンタイムが無視され、再びヘルス ステータスのチェックが開始されます。

自動フェールオーバーが回避された場合のシナリオ例

次に、ヘルス チェック ノードによる自動フェールオーバーが回避された場合、またはセカンダリ ノードへのプロモーション要求が拒否された場合を表すシナリオの例を示します。

- プロモーション要求を受信するノードがセカンダリ ノードでない。
- プロモーション要求に正しいプライマリ PAN の情報がない。
- プロモーション要求が不正なヘルス チェック ノードから受信された。
- プロモーション要求が受信されたが、プライマリ PAN が起動していて良好な状態である。

- プロモーション要求を受信するノードが同期していない。

PAN 自動フェールオーバー機能の影響を受ける機能

次の表に、PANの自動フェールオーバーの設定が展開でイネーブルの場合にブロックされる機能、または追加の設定変更を必要とする機能を示します。

機能	影響の詳細
ブロックされる操作	
アップグレード	<p>CLI によるアップグレードがブロックされます。</p> <p>PAN の自動フェールオーバー機能は、Cisco ISE の以前のバージョンからリリース 1.4 にアップグレードした後の構成で使用できます。デフォルトでは、この機能は無効になっています。</p> <p>自動フェールオーバー機能を展開するには、少なくとも 3 つのノードが必要です。このうち 2 つのノードが管理ペルソナとなり、1 つのノードはヘルスチェック ノードとして機能します。ヘルスチェック ノードは非管理ノードで、ポリシーサービス ノード、モニタリング ノード、または pxGrid ノード、あるいはそれらの組み合わせにできます。これらの PAN が異なるデータセンターにある場合、それぞれの PAN にヘルスチェック ノードが必要です。</p>
バックアップの復元	<p>CLI による復元およびユーザ インターフェイスがブロックされます。</p> <p>PAN の自動フェールオーバーの設定が復元前にイネーブルであった場合は、正常に復元した後には再設定する必要があります。</p>
ノード ペルソナの変更	<p>ユーザ インターフェイスによる次のノード ペルソナの変更がブロックされます。</p> <ul style="list-style-type: none"> • 両方の管理ノード内の管理ペルソナ。 • PAN のペルソナ。 • PAN の自動フェールオーバー機能をイネーブルにした後の、ヘルスチェック ノードの登録解除。

機能	影響の詳細
その他の CLI 操作	<p>CLIによる次の管理操作がブロックされます。</p> <ul style="list-style-type: none"> • パッチのインストールおよびロールバック • DNS サーバの変更 • eth1、eth2、およびeth3 インターフェイスの IP アドレスの変更 • eth1、eth2、およびeth3 インターフェイスのホスト エイリアスの変更 • タイムゾーンの変更
他の管理ポータル操作	<p>ユーザ インターフェイスによる次の管理操作がブロックされます。</p> <ul style="list-style-type: none"> • パッチのインストールおよびロールバック • HTTPS 証明書の変更。 • 管理者認証タイプの変更（パスワードベースの認証から証明書ベースの認証へ、およびその逆）。
すでに最大数のデバイスに接続しているユーザは接続できません。	<p>障害の発生した PAN に一部のセッションデータが格納されていたため、PSN によってこれを更新できません。</p>
PAN の自動フェールオーバーをディセーブルにする必要がある操作	
CLI の操作	<p>PAN の自動フェールオーバーの設定がイネーブルの場合、CLI による次の管理操作では警告メッセージが表示されます。サービス/システムがフェールオーバー ウィンドウ内で再起動されない場合、これらの操作によって自動フェールオーバーが起動する場合があります。そのため、以下の操作の実行時には、PAN の自動フェールオーバーの設定を無効にすることを推奨します。</p> <ul style="list-style-type: none"> • 手動による ISE サービスの停止 • 管理 CLI を使用したソフト リロード（リブート）

関連トピック

[ノード ペルソナとサービスの変更](#) (82 ページ)

自動フェールオーバー用のプライマリ PAN の設定

始める前に

自動フェールオーバー機能を展開するには、少なくとも 3 つのノードが必要です。このうち 2 つのノードが管理ペルソナとなり、1 つのノードはヘルスチェックノードとして機能します。ヘルスチェックノードは非管理ノードで、ポリシーサービスノード、モニタリングノード、または pxGrid ノード、あるいはそれらの組み合わせにできます。これらの PAN が異なるデータセンターにある場合、それぞれの PAN にヘルスチェックノードが必要です。

ステップ 1 プライマリ PAN のユーザ インターフェイスにログインします。

ステップ 2 [管理 (Administration)] > [システム (System)] > [展開 (Deployment)] > [PAN のフェールオーバー (PAN Failover)] の順に選択します。

ステップ 3 プライマリ PAN の自動フェールオーバーをイネーブルにするには、[PAN の自動フェールオーバーを有効にする (Enable PAN Auto Failover)] チェックボックスをオンにします。

セカンダリ PAN をプライマリ PAN に昇格させることはできません。ポリシー サービス ペルソナ、モニタリング ペルソナ、または pxGrid ペルソナ、あるいはそれらの組み合わせのみを担当する Cisco ISE ノードはプライマリ PAN に昇格できません。

ステップ 4 使用可能なすべてのセカンダリ ノードを含む [プライマリ ヘルス チェック ノード (Primary Health Check Node)] ドロップダウン リストから、プライマリ PAN のヘルス チェック ノードを選択します。

このノードは、プライマリ PAN と同じロケーションまたはデータセンターに置くことを推奨します。

ステップ 5 使用可能なすべてのセカンダリ ノードを含む [セカンダリ ヘルス チェック ノード (Secondary Health Check Node)] ドロップダウン リストから、セカンダリ PAN のヘルス チェック ノードを選択します。

このノードは、セカンダリ PAN と同じロケーションまたはデータセンターに置くことを推奨します。

ステップ 6 管理ノードのステータスがチェックされるまでの [ポーリング間隔 (Polling Interval)] 時間を指定します。有効な範囲は 30 ～ 300 秒です。

ステップ 7 [フェールオーバーの前に障害が発生したポーリング数 (Number of Failure Polls before Failover)] の数を指定します。

フェールオーバーは、管理ノードのステータスが障害が発生したポーリング数として指定された数に対して良好でない場合に発生します。有効な範囲は 2 ～ 60 です。

ステップ 8 [保存 (Save)] をクリックします。

次のタスク

セカンダリ PAN のプライマリ PAN へのプロモーション後に、次の操作を実行します。

- 手動で古いプライマリ PAN を同期して、展開内に戻します。
- 手動で同期されていない他のセカンダリ ノードを同期して、展開内に戻します。

セカンダリ PAN のプライマリへの手動昇格

プライマリ PAN が失敗し、PAN の自動フェールオーバーを設定していない場合は、セカンダリ PAN を新しいプライマリ PAN に手動で昇格させる必要があります。

始める前に

プライマリ PAN に昇格するように管理ペルソナで設定された 2 番目の Cisco ISE ノードがあることを確認します。

ステップ 1 セカンダリ PAN のユーザ インターフェイスにログインします。

ステップ 2 [管理 (Administration)] > [システム (System)] > [展開 (Deployment)] を選択します。

ステップ 3 [ノードの編集 (Edit Node)] ページで、[プライマリに昇格 (Promote to Primary)] をクリックします。

セカンダリ PAN をプライマリ PAN に昇格させることしかできません。ポリシー サービス ペルソナまたはモニタリング ペルソナ、あるいはその両方のみを担当する Cisco ISE ノードはプライマリ PAN に昇格できません。

ステップ 4 [保存 (Save)] をクリックします。

次のタスク

元はプライマリ PAN であったノードが復帰した場合は、自動的にレベル下げされ、セカンダリ PAN になります。このノード (元のプライマリ PAN) で手動で同期を実行し、ノードを展開に戻す必要があります。

セカンダリ ノードの [ノードの編集 (Edit Node)] ページでは、オプションが無効なためペルソナまたはサービスを変更できません。変更を加えるには、管理者ポータルにログインする必要があります。

プライマリ PAN にサービスを復元する

Cisco ISE は、元のプライマリ PAN への自動フォールバックをサポートしていません。セカンダリ PAN への自動フェールオーバーが開始された後、元のプライマリ PAN をネットワークに戻す場合には、それをセカンダリ PAN として設定する必要があります。

ポリシー サービス ノード

ポリシー サービス ペルソナの Cisco ISE ノードは、ネットワーク アクセス、ポスチャ、ゲスト アクセス、クライアント プロビジョニング、およびプロファイリング サービスを提供します。このペルソナはポリシーを評価し、すべての決定を行います。複数のノードがこのペルソナを担当できます。通常、1つの分散展開に複数のポリシー サービス ノードが存在します。同じ高速ローカル エリア ネットワーク (LAN) またはロード バランサの背後に存在するポリシー サービス ノードはすべて、グループ化してノード グループを形成することができます。ノード グループのいずれかのノードで障害が発生した場合、その他のノードは障害を検出し、URL にリダイレクトされたセッションをリセットします。

分散セットアップでは、少なくとも 1 つのノードがポリシー サービス ペルソナを担当する必要があります。

ポリシー サービス ノードのハイ アベイラビリティ

ノード障害を検出し、障害が発生したノードで URL がリダイレクトされたすべてのセッションをリセットするために、2 つ以上のポリシー サービス ノードを同じノード グループに配置できます。ノード グループに属しているノードがダウンすると、同じノード グループの別のノードが、障害が発生したノードで URL がリダイレクトされたすべてのセッションに関する許可変更 (CoA) を発行します。

同じノード グループ内のすべてのノードが、ネットワーク アクセス デバイス (NAD) で RADIUS クライアントとして設定され、CoA の許可を得る必要があります。これは、それらすべてのノードで、ノード グループ内の任意のノードを介して確立されたセッションに関する CoA 要求を発行できるためです。ロード バランサを使用していない場合、ノード グループ内のノードは、NAD で設定されている RADIUS サーバおよびクライアントと同じであるか、またはこれらのサブセットである必要があります。これらのノードは RADIUS サーバとしても設定できます。

多数の ISE ノード (RADIUS サーバおよび動的許可クライアントとして) を持つ単一の NAD を設定できますが、すべてのノードが同じノード グループに属している必要はありません。

ノード グループのメンバーは、ギガビットイーサネットなどの高速 LAN 接続を使用して相互に接続する必要があります。ノード グループのメンバーは L2 隣接関係である必要はありませんが、十分な帯域幅と到達可能性を確保するには L2 隣接関係が強く推奨されます。詳細については、[ポリシー サービス ノード グループの作成 \(83 ページ\)](#) の項を参照してください。

PSN 間で均等に要求を分散するためのロード バランサ

展開内に複数のポリシー サービス ノードがある場合、ロード バランサを使用して要求を均等に分散できます。ロード バランサは、その背後にある機能ノードに要求を分散します。ロード バランサの背後に PSN を展開する詳細とベスト プラクティスについては、『[Cisco and F5 Deployment Guide: ISE Load Balancing using BIG-IP](#)』を参照してください。

ポリシー サービス ノードでのセッション フェールオーバー

アクティブな URL にリダイレクトされたセッションがあるポリシー サービス ノードがダウンすると、エンドポイントが中間状態となります。リダイレクトエンドポイントが通信していたポリシー サービス ノードのダウンを検出した場合でも、許可を再開することはできません。

ポリシー サービス ノードがノードグループに属している場合は、ノードグループ内のノード間でハートビートメッセージが交換され、ノードの障害が検出されます。ノードに障害が発生した場合、ノードグループのピアの1つによって、障害が発生したノードのアクティブな URL にリダイレクトされたセッションが学習され、それらのセッションへの接続を解除するための CoA が発行されます。

その結果、同じノードグループで使用可能な別のポリシー サービス ノードによって、セッションが処理されます。セッション フェールオーバーでは、ダウンしたポリシー サービス ノードから使用可能なポリシー サービス ノードにセッションが自動的に移動しませんが、セッションを移動するための CoA が発行されます。

分散展開のポリシー サービス ノードは、マシンアクセス制限 (MAR) キャッシュを相互に共有しません。Cisco ISE で MAR 機能を有効にしている、クライアント マシンが障害が発生したポリシー サービス ノードによって認証される場合は、展開内の別のポリシー サービス ノードがユーザ認証を処理します。ただし、2 番目のポリシー サービス ノードでは、その MAR キャッシュにホスト認証情報がないため、ユーザ認証が失敗します。

ポリシー サービス ノードグループ内のノード数

ノードグループに含めることができるノードの数は、展開要件によって異なります。ノードグループを使用すると、確実に、ノードの障害が検出され、許可されたがポスチャされていないセッションに関する CoA がピアによって発行されます。ノードグループのサイズはあまり大きくする必要はありません。

ノードグループのサイズが増加すると、ノード間で交換されるメッセージおよびハートビートの数が大幅に増加します。その結果、トラフィックも増加します。ノードグループ内のノードの数を少なくすることで、トラフィックを削減でき、同時にポリシー サービス ノードの障害を検出するのに十分な冗長性が提供されます。

ノードグループ クラスタに含めることができるポリシー サービス ノードの数にはハード制限はありません。

モニタリング ノード

モニタリング ペルソナの機能を持つ Cisco ISE ノードがログ コレクタとして動作し、ネットワーク内のすべての管理およびポリシー サービス ノードからのログメッセージを保存します。このペルソナは、ネットワークとリソースを効果的に管理するために使用できる高度な監視およびトラブルシューティングツールを提供します。このペルソナのノードは、収集するデータを集約して関連付けて、意味のある情報をレポートの形で提供します。

Cisco ISE では、プライマリ ロールまたはセカンダリ ロールを担うことができるこのペルソナを持つノードを最大 2 つ使用してハイ アベイラビリティを実現できます。プライマリ モニタリング ノードおよびセカンダリ モニタリング ノードの両方で、ログ メッセージを収集します。プライマリ モニタリング ノードがダウンした場合は、セカンダリ モニタリング ノードが自動的にプライマリ モニタリング ノードになります。

分散セットアップでは、少なくとも 1 つのノードが監視ペルソナを担当する必要があります。同じ Cisco ISE ノードで、モニタリング ペルソナとポリシー サービス ペルソナを有効にしないことを推奨します。最適なパフォーマンスを実現するために、ノードをモニタリング専用とすることを推奨します。

展開内の PAN から [モニタリング (Monitoring)] メニューにアクセスできます。

モニタリング ノードでの自動フェールオーバー

モニタリング ノードでは真の意味でハイ アベイラビリティがサポートされていないため、自動フェールオーバーという用語が使用されます。モニタリング ノードの場合、操作監査データはポリシー サービス ノードによって複製されます。ポリシー サービス ノードは、コピーをプライマリ モニタリング ノードとセカンダリ モニタリング ノードの両方に送信します。



- (注) モニタリングは、プライマリ (アクティブ) モニタリング ノードで行われます。アクティブ ノードがダウンした場合、モニタリング データは、セカンダリ (スタンバイ) モニタリング ノードからのみ提供されます。セカンダリ モニタリング ノードは読み取り専用です。

自動フェールオーバー プロセス

プライマリ モニタリング ノードがダウンした場合は、セカンダリ モニタリング ノードがすべてのモニタリング情報およびトラブルシューティング情報を引き継ぎます。セカンダリ ノードは、読み取り専用機能を提供します。

既存のセカンダリ ノードをアクティブなプライマリ ノードに変換するには、管理者は初めに手動でセカンダリ ノードをプライマリ ロールに昇格する必要があります。セカンダリ ノードが昇格された後にプライマリ ノードが復旧した場合、プライマリ ノードはセカンダリ ロールを担当します。セカンダリ ノードが昇格されなかった場合、プライマリ モニタリング ノードは、復旧後にそのロールを再開します。



- 注意** プライマリ ノードがフェールオーバー後に復旧すると、バックアップを取得してデータを復元し、プライマリ ノードを最新の状態にします。

モニタリング ノードのアクティブ/スタンバイ ペアを設定するためのガイドライン

ISE ネットワークでは 2 つのモニタリング ノードを指定して、アクティブ/スタンバイ ペアを作成できます。セカンダリ モニタリング ノードを登録する場合は、プライマリ モニタリング ノードをバックアップしてから、新しいセカンダリ モニタリング ノードにデータを復元する

ことを推奨します。これにより、新しい変更内容が複製されるため、プライマリ モニタリング ノードの履歴が新しいセカンダリ ノードと同期状態となります。アクティブ-スタンバイ ペアを定義すると、次のルールが適用されます。

- すべての変更は、プライマリ モニタリング ノードで行う必要があります。セカンダリ ノードは読み取り専用です。
- プライマリ ノードで行った変更は、セカンダリ ノードに自動的に複製されます。
- プライマリ ノードとセカンダリ ノードは両方とも、他のノードがログを送信するログ コレクタとしてリストされます。
- Cisco ISE ダッシュボードは、モニタリングおよびトラブルシューティングの主要なエントリ ポイントとなります。PAN からのモニタリング情報は、ダッシュボードに表示されます。プライマリ ノードがダウンすると、セカンダリ ノードから情報が提供されます。
- モニタリング データのバックアップおよび消去は、標準 Cisco ISE ノードのバックアップ プロセスでは行われません。プライマリ モニタリング ノードとセカンダリ モニタリング ノードの両方でバックアップとデータ消去用のリポジトリを設定し、それぞれに同じリポジトリを使用する必要があります。

モニタリング ノードのフェールオーバー シナリオ

次のシナリオは、モニタリング ノード数に応じてアクティブ/スタンバイまたは単一ノード構成に適用されます。

- モニタリング ノードのアクティブ/スタンバイ構成では、プライマリ管理ノード (PAN) は、常にアクティブ モニタリング ノードに接続してモニタリング データを収集します。アクティブなモニタリング ノードに障害が発生した後に、PAN はスタンバイ モニタリング スタンバイ ノードに接続します。アクティブなモニタリング ノードからスタンバイ モニタリング ノードへのフェールオーバーは、アクティブなモニタリング ノードのダウンから 5 分以上経過した後に行われます。

ただし、アクティブ ノードに障害が発生した後に、スタンバイ ノードはアクティブ ノードになりません。アクティブ ノードが復旧すると、管理ノードは再開されたアクティブ ノードからのモニタリング データの収集を再び開始します。
- アクティブなモニタリング ノードがダウンしている間に、スタンバイ モニタリング ノードをアクティブ ステータスに昇格する場合は、既存のアクティブ モニタリング ノードを登録解除する必要があります。既存のアクティブモニタリングノードを登録解除すると、スタンバイ ノードがアクティブなモニタリング ノードになり、PAN は新しく昇格されたアクティブ ノードに自動的に接続を開始します。
- アクティブ/スタンバイ ペアでは、展開からスタンバイ モニタリング ノードの登録解除を選択するか、スタンバイ モニタリング ノードがダウンすると、既存のアクティブ モニタリング ノードは、アクティブ ノードの状態を保持します。PAN は、既存のアクティブ ノードに接続してデータを収集します。
- ISE 展開内にモニタリング ノードが 1 つだけ存在する場合、そのノードは PAN にモニタリング データを提供するアクティブ モニタリング ノードとして機能します。ただし、新

しいモニタリングノードを登録して展開内でアクティブノードにすると、既存のアクティブモニタリングノードは自動的にスタンバイノードになります。PANは、新しく登録されたアクティブモニタリングノードへの接続を開始し、モニタリングデータを収集します。

pxGrid ノード

Cisco pxGrid を使用すると、Cisco ISE セッションディレクトリからの状況依存情報を、ISE エコシステムのパートナー システムなどの他のネットワーク システムや他のシスコ プラットフォームと共有できます。また、pxGrid フレームワークは、Cisco ISE とサードパーティのベンダー間でのタグおよびポリシーオブジェクトの共有のように、ノード間でのポリシーおよび設定データの交換に使用でき、その他の情報交換にも使用できます。また、pxGrid では、サードパーティシステムが適応型ネットワーク制御アクション (EPS) を起動して、ネットワークイベントまたはセキュリティイベントに応答してユーザ/デバイスを隔離できます。タグ定義、値、および説明のような TrustSec 情報は、TrustSec トピックを通して Cisco ISE から別のネットワークに渡すことができます。完全修飾名 (FQN) を持つエンドポイントプロファイルは、エンドポイントプロファイル メタ トピックを通して Cisco ISE から他のネットワークに渡すことができます。Cisco pxGrid は、タグおよびエンドポイントプロファイルの一括ダウンロードもサポートしています。

pxGrid 経由で SXP バインディング (IP-SGT マッピング) を発行および受信登録できます。SXP バインディングの詳細については、[セキュリティ グループ タグの交換プロトコル \(1022 ページ\)](#) を参照してください。

ハイアベイラビリティ設定で、Cisco pxGrid サーバは、PAN を通してノード間で情報を複製します。PAN がダウンすると、pxGrid サーバは、クライアントの登録およびサブスクリプション処理を停止します。pxGrid サーバの PAN をアクティブにするには、手動で昇格する必要があります。[pxGrid サービス (pxGrid Services)] ページ ([管理 (Administration)] > [pxGrid サービス (pxGrid Services)]) を調べ、pxGrid ノードが現在アクティブであるか、スタンバイ状態であるかを確認できます。

XMPP (Extensible Messaging and Presence Protocol) クライアントの場合、pxGrid ノードはアクティブ/スタンバイの高可用性モードで動作します。つまり、pxGrid サービスはアクティブノード上では「実行中」状態で、スタンバイノードでは「無効」状態です。

セカンダリ pxGrid ノードへの自動フェールオーバーが開始された後、元のプライマリ pxGrid ノードがネットワークに戻された場合、元のプライマリ pxGrid ノードは引き続きセカンダリロールを持ち、現在のプライマリ ノードがダウンしない限り、プライマリ ロールに昇格されません。



(注) 時々、元のプライマリ pxGrid ノードがプライマリ ロールに自動的に昇格されることがあります。

ハイアベイラビリティ展開では、プライマリ pxGrid ノードがダウンすると、セカンダリ pxGrid ノードに切り替えるのに約 3 ～ 5 分かかることがあります。プライマリ pxGrid ノードに障害が発生した場合は、キャッシュデータを消去する前に、クライアントはスイッチオーバーが完了するまで待機することを推奨します。

pxGrid ノードでは、次のログを使用できます。

- pxgrid.log : 状態変更通知。
- pxgrid-cm.log : パブリッシャ/サブスクライバおよびクライアントとサーバ間のデータ交換アクティビティの更新。
- pxgrid-controller.log : クライアント機能、グループ、およびクライアント許可の詳細を表示します。
- pxgrid-jabberd.log : システムの状態と認証に関連するすべてのログ。
- pxgrid-pubsub.log : パブリッシャとサブスクライバのイベントに関する情報。



- (注) Base ライセンスを使用して pxGrid を有効にできますが、pxGrid ペルソナを有効にするには Plus ライセンスが必要です。また、 のアップグレードライセンスを最近インストールしている場合には、Base インストールで特定の拡張 pxGrid サービスが使用可能である可能性があります。



- (注) パッシブ ID ワークセンターを使用するには pxGrid を定義する必要があります。詳細については、 [PassiveID ワークセンター \(423 ページ\)](#) を参照してください。

関連トピック

- [pxGrid クライアントおよび機能の管理 \(77 ページ\)](#)
- [pxGrid クライアントの有効化 \(78 ページ\)](#)
- [ISE pxGrid ノードの展開 \(84 ページ\)](#)

pxGrid クライアントおよび機能の管理

Cisco ISE に接続するクライアントは、pxGrid サービスを使用するには登録が必要です。pxGrid クライアントは、クライアントになるために pxGrid SDK を介してシスコから使用可能な pxGrid クライアント ライブラリを採用する必要があります。Cisco pxGrid クライアントには、pxGrid サービスに参加するための承認済みアカウントが必要です。Cisco ISE は、自動および手動承認の両方をサポートします。クライアントは、一意の名前と証明書ベースの相互認証を使用して pxGrid にログインできます。スイッチの AAA 設定と同様に、クライアントは設定された pxGrid サーバのホスト名または IP アドレスに接続できます。

公開および登録するためにクライアントの pxGrid で作成される、情報トピックまたはチャネル機能があります。Cisco ISE では、ID、適応型ネットワーク制御、SGA などの機能のみがサポートされます。クライアントが新しい機能を作成すると、その機能は **[管理]**

(Administration)] > [pxGrid サービス (pxGrid Services)] > [機能別に表示 (View by Capabilities)] に表示されます。機能は個別に有効または無効にできます。機能情報は、発行、ダイレクト クエリー、または一括ダウンロード クエリーでパブリッシャーから入手してください。



(注) pxGrid セッション グループが EPS グループの一部であるため、EPS ユーザ グループに割り当てられたユーザはセッション グループで操作を実行できます。ユーザが EPS グループに割り当てられると、ユーザは pxGrid クライアントのセッションのグループに加入できます。

関連トピック

[pxGrid クライアントの有効化](#) (78 ページ)

[pxGrid 証明書の生成](#) (80 ページ)

pxGrid クライアントの有効化

始める前に

- Cisco pxGrid クライアントからの要求を表示するには、少なくとも 1 つのノードで pxGrid ペルソナを有効にします。
- パッシブ ID サービスを有効にします。[管理 (Administration)] > [展開 (Deployment)] を選択し、必要なノードにチェックマークを付け、[編集 (Edit)] をクリックします。設定画面で [パッシブ ID サービスを有効にする (Enable Passive Identity Service)] をオンにします。

ステップ 1 [管理 (Administration)] > [pxGrid サービス (pxGrid Services)] を選択します。

ステップ 2 クライアントの隣にあるチェックボックスをオンにして [承認 (Approve)] をクリックします。

ステップ 3 [リフレッシュ (Refresh)] をクリックすると、最新のステータスが表示されます。

pxGrid 機能の有効化

始める前に

- Cisco pxGrid クライアントからの要求を表示するには、少なくとも 1 つのノードで pxGrid ペルソナを有効にします。
- pxGrid クライアントをイネーブルにします。

ステップ 1 [管理 (Administration)] > [pxGrid サービス (pxGrid Services)] を選択します。

ステップ 2 右上の [機能別に表示 (View by Capabilities)] をクリックします。

ステップ 3 有効にする機能を選択し、[有効 (Enable)] をクリックします。

ステップ 4 [リフレッシュ (Refresh)] をクリックすると、最新のステータスが表示されます。

Cisco pxGrid ライブ ログ

[ライブ ログ (Live Logs)] ページには、すべての pxGrid 管理イベントが表示されます。イベント情報には、クライアント名と機能名、およびイベントタイプとタイムスタンプが含まれています。

[管理 (Administration)] > [pxGrid サービス (pxGrid Services)] > [ライブ ログ (Live Log)] の順に移動して、イベントリストを表示します。ログを消去して、リストを再同期またはリフレッシュすることもできます。

pxGrid の設定

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 [管理 (Administration)] > [pxGrid サービス (pxGrid Services)] > [設定 (Settings)] を選択します。

ステップ 2 必要に応じて、次のオプションを選択します。

- 新しいアカウントの自動承認 (Automatically Approve New Accounts) : このチェック ボックスにマークを付けると、新しい pxGrid クライアントからの接続要求が自動的に承認されます。
- パスワード ベースのアカウント作成の許可 (Allow Password Based Account Creation) : このチェック ボックスにマークを付けると、pxGrid クライアントのユーザ名/パスワードベースの認証が有効になります。このオプションを有効にした場合、pxGrid クライアントを自動的に承認することはできません。

pxGrid クライアントは、REST API を介してユーザ名を送信することで、pxGrid コントローラに自身を登録できます。pxGrid コントローラは、クライアント登録時に pxGrid クライアントのパスワードを生成します。管理者は接続要求を承認または拒否できます。

ステップ 3 [保存 (Save)] をクリックします。

[pxGrid の設定 (pxGrid Settings)] ページで [テスト (Test)] オプションを使用して、pxGrid ノードでヘルス チェックを実行します。pxgrid/pxgrid-test.log ファイルで詳細を確認できます。

pxGrid 証明書の生成

始める前に

- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。
- pxGrid 証明書はプライマリ PAN から生成する必要があります。
- PxGrid 証明書がサブジェクト代替名 (SAN) の拡張を使用する場合、DNS 名のエントリとしてサブジェクト ID の FQDN が含まれるようにします。

ステップ 1 [管理 (Administration)] > [pxGrid サービス (pxGrid Services)] > [設定 (Settings)] の順に選択します。

ステップ 2 [処理の選択 (I want to)] ドロップダウン リストから、以下のいずれかのオプションを選択します。

- 単一の証明書の生成 (証明書署名要求なし) (Generate a single certificate without a certificate signing request) : このオプションを選択すると、コモン ネーム (CN) を入力する必要があります。
- 単一の証明書の生成 (証明書署名要求あり) (Generate a single certificate with a certificate signing request) : このオプションを選択すると、証明書署名要求の詳細を入力する必要があります。
- 一括証明書の生成 (Generate bulk certificates) : 必要な詳細を含む CSV ファイルをアップロードすることができます。
- ルート証明書チェーンのダウンロード (Download root certificate chain) : ルート証明書をダウンロードして、信頼できる証明書ストアに追加できます。ホスト名と証明書のダウンロード形式を指定する必要があります。

[証明書テンプレート (Certificate Templates)] リンクから証明書テンプレートをダウンロードし、必要に応じて、テンプレートを編集できます。

ステップ 3 ([単一の証明書の生成 (証明書署名要求なし) (Generate a single certificate (without a certificate signing request))] オプションを選択した場合は必須) pxGrid クライアントの FQDN を入力します。

ステップ 4 (オプション) この証明書の説明を入力できます。

ステップ 5 サブジェクト代替名 (SAN) を指定します。複数の SAN を追加できます。次のオプションを使用できます。

- IP アドレス (IP address) : この証明書に関連付ける pxGrid クライアントの IP アドレスを入力します。
- FQDN : pxGrid の完全修飾ドメイン名を入力します。

(注) このフィールドは、[一括証明書の生成 (Generate bulk certificates)] オプションを選択している場合には表示されません。

ステップ 6 [証明書のダウンロード形式 (Certificate Download Format)] ドロップダウン リストから、以下のいずれかのオプションを選択します。

- Private Enhanced Electronic Mail (PEM) 形式の証明書、PKCS8 PEM 形式のキー（証明書チェーンを含む）：ルート証明書、中間 CA 証明書、およびエンドエンティティ証明書は PEM 形式で表されます。PEM 形式の証明書は BASE64 エンコード ASCII ファイルです。各証明書は「-----BEGIN CERTIFICATE-----」タグで始まり、「-----END CERTIFICATE-----」タグで終わります。エンドエンティティの秘密キーは PKCS* PEM を使用して格納されています。「-----BEGIN ENCRYPTED PRIVATE KEY-----」タグで始まり、「-----END ENCRYPTED PRIVATE KEY-----」タグで終わります。
- PKCS12 形式（証明書チェーンを含む。つまり証明書チェーンとキーの両方で 1 ファイル）：1 つの暗号化ファイルにルート CA 証明書、中間 CA 証明書、およびエンドエンティティの証明書と秘密キーを格納するバイナリ形式。

ステップ 7 証明書のパスワードを入力します。

ステップ 8 [作成 (Create)] をクリックします。

作成した証明書は、ISE の [管理 (Administration)] > [システム (System)] > [証明書 (Certificates)] > [認証局 (Certificate Authority)] > [発行された証明書 (Issued Certificates)] に表示され、ブラウザのダウンロードディレクトリにダウンロードされます。

展開内のノードの表示

[展開ノード (Deployment Nodes)] ページで、展開を構成するすべての Cisco ISE ノード、プライマリ ノードおよびセカンダリ ノードを表示できます。

ステップ 1 プライマリ Cisco ISE 管理者ポータルにログインします。

ステップ 2 [管理 (Administration)] > [システム (System)] > [展開 (Deployment)] を選択します。

ステップ 3 左側のナビゲーションペインで、[展開 (Deployment)] をクリックします。

展開を構成するすべての Cisco ISE ノードが表示されます。

プライマリおよびセカンダリの Cisco ISE ノードの同期

Cisco ISE の設定に変更を加えることができるのは、プライマリ PAN からのみです。設定変更はすべてのセカンダリ ノードに複製されます。何らかの理由でこの複製が正しく実行されない場合は、プライマリ PAN に手動でセカンダリ PAN を同期できます。

始める前に

[同期ステータス (Sync Status)] が [同期していない (Out of Sync)] に設定されている場合や [複製ステータス (Replication Status)] が [失敗 (Failed)] または [無効 (Disabled)] の場合は、[同期を更新 (Syncup)] ボタンをクリックして完全複製を強制的に実行する必要があります。

ステップ 1 プライマリ PAN にログインします。

ステップ 2 [管理 (Administration)] > [システム (System)] > [展開 (Deployment)] を選択します。

ステップ 3 プライマリ PAN と同期させるノードの横にあるチェックボックスをオンにし、[同期を更新 (Syncup)] をクリックして完全データベース複製を強制的に実行します。

関連トピック

[プライマリ ISE ノードからセカンダリ ISE ノードへのデータ レプリケーション](#) (57 ページ)

ノード ペルソナとサービスの変更

Cisco ISE ノードの設定を編集して、そのノードで実行されているペルソナおよびサービスを変更できます。

始める前に

- ポリシーサービス ノードで実行されるサービスを有効または無効にしたり、ポリシーサービス ノードを変更したりする場合は、そのサービスが実行されるアプリケーション サーバプロセスを再起動します。これらのサービスが再起動されるまで遅延が発生します。
- このサービスの再起動の遅延により、自動フェールオーバーが開始される場合があります (展開内で有効になっている場合)。これを回避するには、自動フェールオーバー設定がオフになっていることを確認します。

ステップ 1 プライマリ PAN にログインします。

ステップ 2 [管理 (Administration)] > [システム (System)] > [展開 (Deployment)] を選択します。

ステップ 3 ペルソナまたはサービスを変更するノードの隣にあるチェックボックスをオンにし、[編集 (Edit)] をクリックします。

ステップ 4 必要なサービスおよびペルソナを選択します。

ステップ 5 [保存 (Save)] をクリックします。

ステップ 6 プライマリ PAN でアラームの受信を確認して、ペルソナまたはサービスの変更を確認します。ペルソナまたはサービスの変更が正常に保存されなかった場合、アラームは生成されません。

Cisco ISE でのノードの変更による影響

Cisco ISE ISE で次のいずれかの変更を行うと、そのノードが再起動するため、遅延が発生します。

- ノードの登録（スタンドアロンからセカンダリへ）
- ノードの登録解除（セカンダリからスタンドアロンへ）
- プライマリ ノードからスタンドアロンへの変更（他のノードが登録されていない場合は、プライマリからスタンドアロンに変更されます）
- 管理ノードの昇格（セカンダリからプライマリへ）
- ペルソナの変更（ノードからポリシー サービスまたは監視ペルソナを割り当てたり、削除したりする場合）
- ポリシー サービス ノードでのサービスの変更（セッションとプロファイラ サービスを有効または無効にします）
- プライマリでのバックアップの復元（同期操作がトリガーされ、プライマリ ノードからセカンダリ ノードにデータが複製されます）

ポリシー サービス ノード グループの作成

2つ以上のポリシー サービス ノード（PSN）が同じ高速ローカルエリアネットワーク（LAN）に接続されている場合は、同じノードグループに配置することを推奨します。この設計は、グループにローカルの重要度が低い属性を保持し、ネットワークのリモートノードに複製される情報を減らすことによって、エンドポイント プロファイリング データのレプリケーションを最適化します。ノードグループメンバーは、ピアグループメンバーの可用性もチェックします。グループがメンバーに障害が発生したことを検出すると、障害が発生したノードの URL にリダイレクトされたすべてのセッションをリセットし、回復することを試行します。



- (注) すべての PSN を同じノードグループの同じローカル ネットワークの部分に置くことを推奨します。PSN は、同じノードグループに参加するために負荷分散クラスタの一部である必要はありません。ただし、負荷分散クラスタの各ローカル PSN は通常同じノードグループに属している必要があります。

ノードグループにメンバーとして PSN を追加する前に、最初にノードグループを作成する必要があります。管理者ポータル の [展開 (Deployment)] ページで、ポリシー サービス ノードグループを作成、編集、および削除できます。

始める前に

ノードグループメンバーは TCP/7800 および TCP/7802 を使用して通信できます。

ステップ 1 [管理 (Administration)] > [システム (System)] > [展開 (Deployment)] を選択します。

ステップ 2 [アクション (action)] アイコンをクリックし、[ノードグループの作成 (Create Node Group)] をクリックします。

ステップ 3 ノード グループに付ける一意の名前を入力します。

ステップ 4 (任意) ノード グループの説明を入力します。

ステップ 5 [送信 (Submit)] をクリックして、ノード グループを保存します。

ノードグループを保存すると、左側のナビゲーションペインにそのグループが表示されます。左側のペインにノードグループが表示されていない場合、そのグループは非表示になっている可能性があります。非表示オブジェクトを表示するには、ナビゲーション ペインで [展開 (Expand)] ボタンをクリックします。

次のタスク

ノード グループにノードを追加します。ノードを編集するには、[ノード グループのメンバー (Member of Node Group)] ドロップダウン リストからノード グループを選択します。

関連トピック

[ポリシー サービス ノード \(72 ページ\)](#)

[ポリシー サービス ノードのハイ アベイラビリティ \(72 ページ\)](#)

ISE pxGrid ノードの展開

スタンドアロン ノードと分散展開ノードの両方で、Cisco pxGrid ペルソナを有効にできます。

始める前に

- Base ライセンスを使用して pxGrid を有効にできますが、pxGrid ペルソナを有効にするには Plus ライセンスが必要です。
- Cisco pxGrid サービスは、Cisco ISE SNS 3415/3495 アプライアンス上または VMware で実行されます。
- すべてのノードは、pxGrid 用に CA 証明書を使用するように設定されています。アップグレード前にデフォルトの証明書を pxGrid に使用する場合、アップグレード後にこの証明書は内部 CA 証明書に置き換えられます。
- 分散展開を使用しているか、または Cisco ISE 1.2 からアップグレードする場合は、証明書で [pxGrid 使用 (pxGrid Usage)] オプションを有効にする必要があります。[pxGrid 使用 (pxGrid Usage)] オプションを有効にするには、[管理 (Administration)] > [証明書 (Certificates)] > [システム証明書 (Certificates)] に移動します。展開に使用される証明書を選択し、[編集 (Edit)] をクリックします。pxGridを確認します。[pxGrid コントローラ (pxGrid Controller)] チェックボックスの証明書を使用します。
- Cisco ISE 1.2 で FIPS モードを有効にしていた場合、1.4 にアップグレードすると、証明書 (自己署名証明書または CA 署名証明書を含む) の生成時または編集時に pxGrid オプションが無効になります。pxGrid オプションは、FIPS 対応の Cisco ISE アプライアンスでは有効にできません。これは、pxGrid と Cisco ISE の統合に使用される XCP サーバが FIPS に準拠していないためです。FIPS モードが Cisco ISE 1.2 で有効でなかった場合は、1.4 にアップグレードした後、pxGrid オプションが証明書に対して有効になります。

ステップ 1 [管理 (Administration)] > [システム (System)] > [展開 (Deployment)] を選択します。

ステップ 2 [展開ノード (Deployment Nodes)] ページで、pxGrid サービスを有効にするノードの隣にあるチェックボックスをオンにし、[編集 (Edit)] をクリックします。

ステップ 3 [全般設定 (General Settings)] タブをクリックし、[pxGrid] チェックボックスをオンにします。

ステップ 4 [保存 (Save)] をクリックします。

以前のバージョンからアップグレードするとき、[保存 (Save)] オプションが無効になる場合があります。このことは、ブラウザ キャッシュが旧バージョンの Cisco ISE の古いファイルを参照する場合に発生します。[保存 (Save)] オプションを有効にするには、ブラウザ キャッシュを消去します。

自動フェールオーバー用のモニタリングノードの設定

展開に 2 つのモニタリング ISE ノードがある場合は、自動フェールオーバーのプライマリ-セカンダリ ペアを設定して、Cisco ISE モニタリング サービスのダウンタイムを回避します。プライマリ-セカンダリ ペアによって、プライマリ ノードに障害が発生した場合に、セカンダリ モニタリング ノードが自動的にモニタリングを提供します。

始める前に

- 自動フェールオーバー用のモニタリング ノードを設定するには、モニタリング ノードが Cisco ISE ノードとして登録されている必要があります。
- 両方のノードでモニタリングロールおよびサービスを設定し、必要に応じてこれらのノードにプライマリ ロールおよびセカンダリ ロールの名前を付けます。
- プライマリ モニタリング ノードとセカンダリ モニタリング ノードの両方でバックアップとデータ消去用のリポジトリを設定します。バックアップおよび消去を正しく動作させるには、両方のノードに同じリポジトリを使用します。消去は、冗長ペアのプライマリ ノードおよびセカンダリ ノードの両方で行われます。たとえば、プライマリ モニタリング ノードでバックアップおよび消去用に 2 つのリポジトリが使用されている場合、同じリポジトリをセカンダリノードに指定する必要があります。

システム CLI の **repository** コマンドを使用してモニタリング ノードのデータ リポジトリを設定します。



注意 スケジュールバックアップと消去をモニタリング冗長ペアのノードで正しく動作させるには、CLI を使用して、プライマリ ノードとセカンダリ ノードの両方で同じリポジトリを設定します。リポジトリは、2 つのノードの間で自動的に同期されません。

Cisco ISE ダッシュボードで、モニタリング ノードの準備ができていることを確認します。[システム概要 (System Summary)] ダッシュレットに、サービスが準備完了の場合は左側に緑色のチェック マークが付いたモニタリング ノードが表示されます。

ステップ 1 [管理 (Administration)] > [システム (System)] > [展開 (Deployment)] を選択します。

ステップ 2 [展開ノード (Deployment Nodes)] ページで、アクティブとして指定するモニタリング ノードの隣にあるチェックボックスをオンにし、[編集 (Edit)] **Edit** をクリックします。

ステップ 3 [全般設定 (General Settings)] タブをクリックし、[ロール (Role)] ドロップダウン リストから [プライマリ (Primary)] を選択します。

1 つのモニタリング ノードをプライマリとして選択すると、もう 1 つのモニタリング ノードが自動的にセカンダリとなります。スタンドアロン展開の場合、プライマリおよびセカンダリのロール設定は無効になります。

ステップ 4 [保存 (Save)] **Save** をクリックします。アクティブ ノードおよびスタンバイ ノードが再起動します。

展開からのノードの削除

展開からノードを削除するには、ノードの登録を解除する必要があります。登録解除されたノードは、スタンドアロン Cisco ISE ノードになります。

これはプライマリ PAN から受信した最後の設定を保持し、管理、ポリシー サービス、およびモニタリングであるスタンドアロンノードのデフォルトのペルソナを担当します。モニタリングノードを登録解除した場合、このノードは **syslog** ターゲットではなくなります。

プライマリ PSN の登録が取り消されると、エンドポイント データは失われます。スタンドアロンノードになった後も PSN にエンドポイント データを残すには、以下のいずれかを実行します。

- プライマリ PAN からバックアップを取得し、PSN がスタンドアロン ノードになったときに、このデータ バックアップを復元します。
- PSN のペルソナを管理者 (セカンダリ PAN) に変更し、管理者ポータルを展開ページからデータを同期してから、ノードを登録解除します。この時点で、このノードに、すべてのデータがあります。この後、既存の展開にセカンダリ PAN を追加できます。

プライマリ PAN の [展開 (Deployment)] ページからこれらの変更を表示できます。ただし、変更が反映され、[展開 (Deployment)] ページに表示されるには 5 分間の遅延が生じます。

始める前に

展開からセカンダリ ノードを削除する前に、必要に応じて後で復元できる Cisco ISE 設定のバックアップを実行します。

-
- ステップ 1 [管理 (Administration)] > [システム (System)] > [展開 (Deployment)] を選択します。
- ステップ 2 削除するセカンダリ ノードの隣のチェックボックスをオンにして、[登録解除 (Deregister)] をクリックします。
- ステップ 3 [OK] をクリックします。
- ステップ 4 プライマリ PAN のアラームの受信を確認し、セカンダリ ノードが正常に登録解除されたことを確認します。セカンダリ ノードのプライマリ PAN からの登録解除が失敗した場合は、このアラームは生成されません。
-

スタンドアロン Cisco ISE ノードのホスト名または IP アドレスの変更

スタンドアロン Cisco ISE ノードのホスト名、IP アドレス、またはドメイン名を変更できます。ノードのホスト名として「localhost」を使用することはできません。

始める前に

Cisco ISE ノードが分散展開の一部である場合、展開から削除し、スタンドアロン ノードであることを確認する必要があります。

-
- ステップ 1 Cisco ISE CLI から **hostname**、**ip address**、**ip domain-name** の各コマンドを使用して Cisco ISE ノードのホスト名または IP アドレスを変更します。
- ステップ 2 すべてのサービスを再起動するために、Cisco ISE CLI から **application stop ise** コマンドを使用して Cisco ISE アプリケーション設定をリセットします。
- ステップ 3 Cisco ISE ノードは、分散展開の一部である場合、プライマリ PAN に登録します。
- (注) Cisco ISE ノードの登録時にホスト名を使用する場合、登録するスタンドアロンノードの完全修飾ドメイン名 (FQDN) (たとえば、*abc.xyz.com*) は、プライマリ PAN から DNS を使用して解決する必要があります。解決できない場合は、ノード登録が失敗します。DNS サーバに、分散展開の一部である Cisco ISE ノードの IP アドレスと FQDN を入力する必要があります。

セカンダリ ノードとして Cisco ISE ノードを登録した後、プライマリ PAN は IP アドレス、ホスト名、またはドメイン名への変更を展開内の他の Cisco ISE ノードに複製します。

Cisco ISE アプライアンス ハードウェアの交換

Cisco ISE アプライアンス ハードウェアは、ハードウェアに問題がある場合にのみ交換する必要があります。ソフトウェアに問題がある場合は、アプリケーションのイメージを再作成し、Cisco ISE ソフトウェアを再インストールできます。

-
- ステップ 1** 新しいノードで Cisco ISE ソフトウェアを再インストールするか、またはイメージを再作成します。
- ステップ 2** プライマリおよびセカンダリ PAN の UDI を使用してライセンスを取得し、プライマリ PAN にインストールします。
- ステップ 3** 置き換えられたプライマリ PAN でバックアップを復元します。
- 復元スクリプトはセカンダリ PAN でデータの同期を試行しますが、現在セカンダリ PAN はスタンドアロンノードであり、同期は失敗します。データは、プライマリ PAN でバックアップが実行された時刻に設定されます。
- ステップ 4** 新しいノードをセカンダリ サーバとしてプライマリ PAN に登録します。
-



第 III 部

Cisco ISE 管理アクセスの設定

- [Cisco ISE の管理 \(91 ページ\)](#)
- [管理者および管理者アクセス ポリシーの管理 \(117 ページ\)](#)
- [Cisco ISE ライセンス \(147 ページ\)](#)
- [証明書の管理 \(159 ページ\)](#)
- [TACACS+ を使用したデバイス管理の制御 \(229 ページ\)](#)
- [ネットワーク デバイスの管理 \(247 ページ\)](#)
- [リソースの管理 \(307 ページ\)](#)
- [ロギング メカニズム \(313 ページ\)](#)
- [バックアップ/復元操作 \(327 ページ\)](#)
- [適応型ネットワーク制御のセットアップ \(351 ページ\)](#)



第 5 章

Cisco ISE の管理

- [Cisco ISE へのログイン](#) (91 ページ)
- [Cisco ISE でのプロキシ設定の指定](#) (93 ページ)
- [管理者ポータルで使用されるポート](#) (93 ページ)
- [外部 RESTful サービス API の有効化](#) (94 ページ)
- [外部 RESTful サービス SDK](#) (95 ページ)
- [システム時刻と NTP サーバ設定の指定](#) (95 ページ)
- [システムの時間帯の変更](#) (96 ページ)
- [通知をサポートするための SMTP サーバの設定](#) (97 ページ)
- [Cisco ISE 展開のアップグレード](#) (97 ページ)
- [ソフトウェア パッチのインストール](#) (102 ページ)
- [ソフトウェア パッチのロールバック](#) (104 ページ)
- [パッチのインストールおよびロールバックの変更の表示](#) (106 ページ)
- [FIPS モードのサポート](#) (106 ページ)
- [Cisco ISE での FIPS モードの有効化](#) (107 ページ)
- [管理者 CAC 認証のための Cisco ISE の設定](#) (108 ページ)
- [Diffie-Hellman アルゴリズムを使用した SSH キー交換の保護](#) (111 ページ)
- [セキュア syslog 送信のための Cisco ISE の設定](#) (111 ページ)
- [デフォルトのセキュア syslog コレクタ](#) (114 ページ)
- [オフライン メンテナンス](#) (115 ページ)

Cisco ISE へのログイン

管理者のユーザ名とパスワードを使用して Cisco ISE にログインします。

初期設定時に、SSH を有効にしない場合、SSH 経由で ISE 管理コンソールにアクセスできません。SSH を有効にするには、Cisco ISE CLI にアクセスして、グローバルコンフィギュレーション モードで **service sshd enable** コマンドを入力します。グローバル コンフィギュレーション モードで **no service sshd** コマンドを使用して、SSH を無効にできます。

-
- ステップ 1** Cisco ISE URL をブラウザのアドレス バーに入力します（たとえば `https://<ise hostname or ip address>/admin/`）。
- ステップ 2** ユーザ名と、Cisco ISE の初期セットアップで指定して設定した大文字と小文字が区別されるパスワードを入力します。
- ステップ 3** [ログイン (Login)] をクリックするか、Enter を押します。
- ログインに失敗した場合は、[ログイン (Login)] ページの[ログインで問題が発生する場合 (Problem logging in?)] リンクをクリックして、手順に従ってください。
-

関連トピック

[管理者ログイン ブラウザのサポート](#) (92 ページ)

管理者ログイン ブラウザのサポート

Cisco ISE 管理者ポータルは次の HTTPS 対応ブラウザをサポートしています。

- Mozilla Firefox バージョン 45.x ESR および 48.0 以降
- Google Chrome 53.0 以降
- Microsoft Internet Explorer 10.x および 11.x

Internet Explorer 10.x を使用する場合は、TLS 1.1 と TLS 1.2 をイネーブルにし、SSL 3.0 と TLS 1.0 をディセーブルにします ([インターネット オプション (Internet Options)] > [詳細設定 (Advanced)])。

ISE コミュニティ リソース

[ISE Pages Fail to Fully Load When Adblock Plus is Used](#)

ログインの試行に失敗した後の管理者のロックアウト

管理者ユーザ ID に対して誤ったパスワードを入力した回数が所定の数に達すると、ユーザは「ロックアウト」されて管理者ポータルからシステムにアクセスできなくなり、ログエントリが [サーバ管理者ログイン (Server Administrator Logins)] レポートに記録され、その管理者 ID のクレデンシャルは一時停止されます。一時停止を解除するには、その管理者 ID に関連付けられたパスワードをリセットする必要があります。手順については、『*Cisco Identity Services Engine Hardware Installation Guide*』の「Performing Post-Installation Tasks」の章を参照してください。管理者アカウントを無効にするのに必要な試行失敗回数は、「ユーザアカウントのカスタム属性およびパスワード ポリシー」の項で説明しているガイドラインに従って設定できます。管理者ユーザ アカウントがロックアウトされると、関連付けられた管理者ユーザに電子メールが送信されます。

無効になったシステム管理者のステータスは、Active Directory ユーザを含むすべてのスーパー管理者が有効にできます。

Cisco ISE でのプロキシ設定の指定

既存のネットワーク トポロジにおいて、外部リソース（たとえば、クライアント プロビジョニングやポスチャ関連のリソースが存在するリモート ダウンロード サイト）にアクセスするために、Cisco ISE に対してプロキシを使用することが要求されている場合は、管理者ポータルを使用してプロキシのプロパティを指定できます。

プロキシ設定は次の Cisco ISE 機能に影響します。

- パートナー モバイル管理
- エンドポイント プロファイラ フィード サービスの更新
- エンドポイント ポスチャの更新
- エンドポイント ポスチャ エージェント リソースのダウンロード
- CRL（証明書失効リスト）のダウンロード
- ゲスト通知

Cisco ISE プロキシ設定はプロキシ サーバの基本認証をサポートします。NT LAN Manager (NTLM) 認証はサポートされていません。

-
- ステップ 1** [管理 (Administration)] > [システム (System)] > [設定 (Settings)] > [プロキシ (Proxy)] を選択します。
- ステップ 2** プロキシの IP アドレスまたは DNS 解決可能ホスト名を入力し、Cisco ISE との間のプロキシ トラフィックを通過させるポートを [プロキシ ホスト サーバ : ポート (Proxy host server : port)] で指定します。
- ステップ 3** 必要に応じて、[パスワード必須 (Password required)] チェックボックスをオンにします。
- ステップ 4** [ユーザ名 (User Name)] および [パスワード (Password)] フィールドに、プロキシ サーバへの認証に使用するユーザ名とパスワードを入力します。
- ステップ 5** [次のホストとドメインに対するプロキシをバイパス (Bypass proxy for these hosts and domain)] に、バイパスするホストまたはドメインの IP アドレスまたはアドレス範囲を入力します。
- ステップ 6** [保存 (Save)] をクリックします。
-

管理者ポータルで使用されるポート

管理者ポータルは HTTP ポート 80 および HTTPS ポート 443 を使用するように設定され、これらの設定は変更できません。Cisco ISE はまた、あらゆるエンドユーザ ポータルが同じポートを使用することを禁止して、管理者ポータルへのリスクを減らすようになっています。

外部 RESTful サービス API の有効化

外部 RESTful サービス API は HTTPS プロトコルおよび REST 方法論に基づいており、ポート 9060 を使用します。

外部 RESTful サービス API は、基本認証をサポートしています。認証クレデンシャルは、暗号化され、要求ヘッダーの一部となっています。

JAVA、curl Linux コマンド、Python などの REST クライアントやその他のクライアントを使用して、外部 RESTful サービス API コールを呼び出すことができます。

ISE 管理者は、外部 RESTful サービス API を使用して操作を実行するための特権をユーザに割り当てる必要があります。外部 RESTful サービス API（ゲスト API を除く）を使用して操作を実行するには、次の管理者グループのいずれかにユーザを割り当て、Cisco ISE の内部データベース（内部管理者ユーザ）に保存されているクレデンシャルに対して認証する必要があります。

- 外部 RESTful サービス管理者：すべての ERS API へのフルアクセス（GET、POST、DELETE、PUT）。このユーザは、ERS API 要求を作成、読み取り、更新、および削除できます。
- 外部 RESTful サービス オペレータ：読み取り専用アクセス（GET 要求のみ）。

外部 RESTful サービス API は、デフォルトではイネーブルになっていません。それらをイネーブルにする前に外部 RESTful サービス API コールを呼び出そうとすると、エラー応答を受信します。Cisco ISE REST API 用に開発されたアプリケーションから Cisco ISE にアクセスできるようにするには、Cisco ISE REST API をイネーブルにする必要があります。Cisco REST API は HTTPS ポート 9060 を使用します。このポートはデフォルトでは閉じられています。Cisco ISE REST API が Cisco ISE 管理用サーバでイネーブルになっていない場合、クライアントアプリケーションは、サーバから Guest REST API 要求に対するタイムアウトエラーを受信します。

ステップ 1 [管理 (Administration)] > [設定 (Settings)] > [ERS 設定 (ERS Settings)] の順に選択します。

ステップ 2 プライマリ管理ノードの [読み取り/書き込み用に ERS をイネーブル化 (Enable ERS for Read/Write)] を選択します。

ステップ 3 セカンダリ ノードがある場合は、[その他すべてのノードの読み取り用に ERS をイネーブル化 (Enable ERS for Read for All Other Nodes)] を選択します。

すべてのタイプの外部 RESTful サービス要求はプライマリ ISE ノードに限り有効です。セカンダリ ノードは読み取りアクセス（GET 要求）に対応します。

ステップ 4 [送信 (Submit)] をクリックします。

すべての REST 操作が監査され、ログがシステムログに記録されます。外部 RESTful サービス API にはデバッグロギングカテゴリがあります。このカテゴリは、Cisco ISE GUI のデバッグログページからイネーブルにすることができます。

関連トピック

[外部 RESTful サービス SDK](#) (95 ページ)

外部 RESTful サービス SDK

外部 RESTful サービス SDK を使用して、独自ツールの構築を開始できます。次の URL から外部 RESTful サービス SDK にアクセスできます。https://<ISE-ADMIN-NODE>:9060/ers/sdk 外部 RESTful サービス SDK には、外部 RESTful サービス管理ユーザのみがアクセスできます。

SDK は、次のコンポーネントで構成されています。

- クイック リファレンス API マニュアル
- すべての利用可能な API 操作の完全なリスト
- ダウンロード可能なスキーマ ファイル
- ダウンロード可能な Java のサンプル アプリケーション
- cURL スクリプト形式の使用例
- python スクリプト形式の使用例
- Chrome POSTMAN の使用方法

システム時刻と NTP サーバ設定の指定

Cisco ISE では、Network Time Protocol (NTP) サーバを 3 台まで設定することができます。NTP サーバを使用すると、正確な時刻を維持でき、複数のタイムゾーンの間で時刻を同期できます。また、認証済みの NTP サーバのみを Cisco ISE で使用するかどうかを指定することもでき、そのための認証キーを入力できます。

シスコは、すべての Cisco ISE ノードを協定世界時 (UTC) の時間帯に設定することを推奨します (特に Cisco ISE ノードが分散展開されてインストールされている場合)。この手順では、展開内にあるさまざまなノードからのレポートとログのタイムスタンプが常に同期されます。

始める前に

スーパー管理者またはシステム管理者の管理者ロールが割り当てられている必要があります。

プライマリおよびセカンダリの両方の Cisco ISE ノードがある場合は、セカンダリ ノードのユーザインターフェイスにログインし、展開内の各 Cisco ISE ノードのシステム時間と NTP サーバ設定を個別に設定する必要があります。

ステップ 1 [管理 (Administration)] > [システム (System)] > [設定 (Settings)] > [システム時刻 (System Time)] を選択します。

ステップ 2 NTP サーバに一意の IP アドレスを入力します。

- ステップ 3** システムおよびネットワーク時間の維持に認証済みの NTP サーバだけを使用するように Cisco ISE を制限する場合は、[認証済みの NTP サーバのみ可能 (Only allow authenticated NTP servers)] チェックボックスをオンにします。
- ステップ 4** (オプション) 秘密キーを使用して NTP サーバを認証する場合に、指定したサーバのいずれかが認証キーによる認証を必要とする場合は、[NTP 認証キー (NTP Authentication Keys)] タブをクリックし、1 つ以上の認証キーを次のように指定します。
- [追加 (Add)] をクリックします。
 - [キー ID (Key ID)] と [キー値 (Key Value)] に必要な値を入力します。そのキーが信頼できる場合は、[信頼できるキー (Trusted Key)] オプションをオンにし、[OK] をクリックします。[キー ID (Key ID)] フィールドは 1 ～ 65535 の数値をサポートし、[キー値 (Key Value)] フィールドは最大 15 文字の英数字をサポートします。
 - NTP サーバの認証キーの入力が終了したら、[NTP サーバ設定 (NTP Server Configuration)] タブに戻ります。
- ステップ 5** [保存 (Save)] をクリックします。

システムの時間帯の変更

一度設定すると、管理者ポータルからの時間帯の編集はできません。時間帯設定を変更するには、Cisco ISE CLI で次のコマンドを入力します。

clock timezone タイムゾーン



- (注) Cisco ISE は、タイムゾーン名と出力の省略形に POSIX スタイルの記号を使用します。そのため、グリニッジの西にあるゾーンはプラス記号を持ち、グリニッジの東にあるゾーンはマイナス記号を持ちます。たとえば、TZ='Etc/GMT+4' はグリニッジ標準時 (UT) の 4 時間遅れに対応します。



- 注意** インストール後に Cisco ISE アプライアンスでタイムゾーンを変更するには、ISE サービスをその特定のノードで再起動する必要があります。そのため、メンテナンスウィンドウ内でこのような変更を行うことを推奨します。また、単一 ISE 展開内のすべてのノードが同じタイムゾーンに設定されていることが重要です。複数の ISE ノードが異なる地理的な場所やタイムゾーンにある場合は、すべての ISE ノードで UTC などのグローバルなタイムゾーンを使用する必要があります。

clock timezone コマンドの詳細については、『Cisco Identity Services Engine CLI Reference Guide』を参照してください。

通知をサポートするための SMTP サーバの設定

アラームの電子メール通知を送信したり、スポンサーがゲストにログインクレデンシャルやパスワードのリセット指示の電子メール通知を送信できるようにしたり、ゲストがアカウント登録に成功した後、自動的にログインクレデンシャルを受信したり、ゲストアカウントの期限が切れる前に実行するアクションを受信したりできるようにするには、Simple Mail Transfer Protocol (SMTP) サーバを設定する必要があります。

-
- ステップ 1** [管理 (Administration)] > [システム (System)] > [設定 (Settings)] > [SMTP サーバ (SMTP Server)] を選択します。
- ステップ 2** [設定 (Settings)] > [SMTP サーバ (SMTP Server)] を選択します。
- ステップ 3** [SMTP サーバ (SMTP Server)] フィールドにアウトバウンド SMTP サーバのホスト名を入力します。この SMTP ホストサーバは Cisco ISE サーバからアクセス可能である必要があります。このフィールドの最大長は 60 文字です。
- ステップ 4** 次のオプションのいずれかを選択します。
- スポンサーの電子メールアドレスからゲスト通知メールを送信するには、[スポンサーの電子メールアドレスを使用 (Use email address from Sponsor)] を選択して、[通知の有効化 (Enable Notifications)] を選択します。
 - すべてのゲスト通知の送信元となる電子メールアドレスを指定するには、[デフォルトの電子メールアドレスを使用 (Use Default email address)] を選択して、それを [デフォルトの電子メール アドレス (Default email address)] フィールドに入力します。
- ステップ 5** [保存 (Save)] をクリックします。
-

アラーム通知の受信者は、[電子メールにシステム アラームを含む (Include system alarms in emails)] オプションが有効になっている内部管理ユーザです。アラーム通知を送信する送信者の電子メールアドレスは、ise@<hostname> としてハードコードされています。

Cisco ISE 展開のアップグレード

Cisco ISE では、管理者ポータルから GUI ベースの一元化されたアップグレードが提供されます。アップグレードプロセスはさらに簡素化され、アップグレードの進行状況およびノードのステータスが画面に表示されます。アップグレード前およびアップグレード後のタスクのリストについては、『Cisco Identity Services Engine Upgrade Guide』を参照してください。

[アップグレードの概要 (Upgrade Overview)] ページには、展開内のすべてのノード、そのノードで有効なペルソナ、インストールされている ISE のバージョン、およびノードのステータス (ノードがアクティブか非アクティブか) がリストされます。ノードがアクティブな状態である場合にのみアップグレードを開始できます。

さまざまなタイプの展開

- スタンドアロン ノード：管理、ポリシー サービスおよびモニタリングのペルソナを担当する単一の Cisco ISE ノード
- マルチノード展開：複数の ISE ノードによる分散展開。分散展開をアップグレードする手順については、下記で詳しく説明します。

ISE コミュニティ リソース

ネットワークが ISE 展開への準備ができているかどうかを評価する方法については、[ISE Deployment Assistant \(IDA\)](#) を参照してください。

分散展開のアップグレード

管理者ポータルから Cisco ISE 展開のすべてのノードをアップグレードできます。



- (注) GUI ベースのアップグレードは、リリース 2.0 以降からそれよりも新しいリリースにアップグレードする場合、または Cisco ISE 2.0 以降の限定提供リリースを一般提供リリースにアップグレードする場合にのみ適用できます。

始める前に

アップグレードする前に、次の作業が完了していることを確認します。

- ISE の設定および運用データのバックアップを取得します。
- システム ログのバックアップを取得します。
- スケジュールしたバックアップを無効にします。展開のアップグレードが完了したら、バックアップ スケジュールを再設定します。
- 証明書および秘密キーをエクスポートします。
- リポジトリを設定します。アップグレードバンドルをダウンロードし、このリポジトリに格納します。
- Active Directory の参加クレデンシアルと RSA SecurID ノード秘密のメモを取ります（該当する場合）。この情報は、アップグレード後に Active Directory または RSA SecurID サーバに接続するために必要です。
- アップグレードのパフォーマンスを向上させるために、運用データを消去します。

ステップ 1 管理者ポータルの [アップグレード (Upgrade)] タブをクリックします。

ステップ 2 [続行 (Proceed)] をクリックします。

[レビューチェックリスト (Review Checklist)] ウィンドウが表示されます。表示された手順を確認してください。

ステップ 3 [チェックリストを確認済み (I have reviewed the checklist)] チェックボックスをオンにし、[続行 (Continue)] をクリックします。

[バンドルのノードへのダウンロード (Download Bundle to Nodes)] ウィンドウが表示されます。

ステップ 4 リポジトリからノードにアップグレードバンドルをダウンロードします。

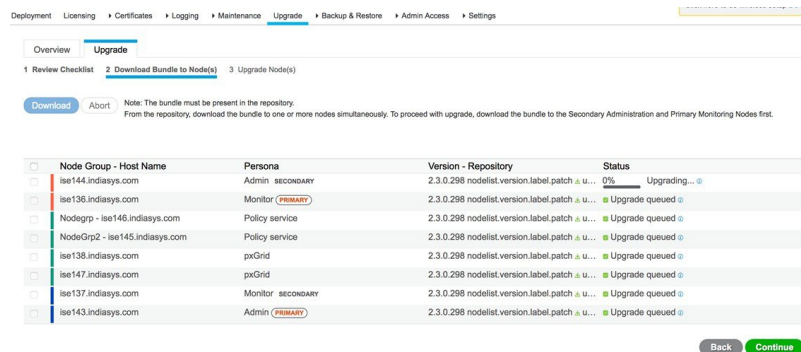
- アップグレードバンドルをダウンロードするノードの隣のチェックボックスをオンにします。
- [ダウンロード (Download)] をクリックします。

[リポジトリおよびバンドルの選択 (Select Repository and Bundle)] ウィンドウが表示されます。

- リポジトリを選択します。

異なるノードで同じリポジトリまたは異なるリポジトリを選択できますが、すべてのノードで同じアップグレードバンドルを選択する必要があります。

図 1: 各ノードの選択したリポジトリを表示するアップグレードウィンドウ



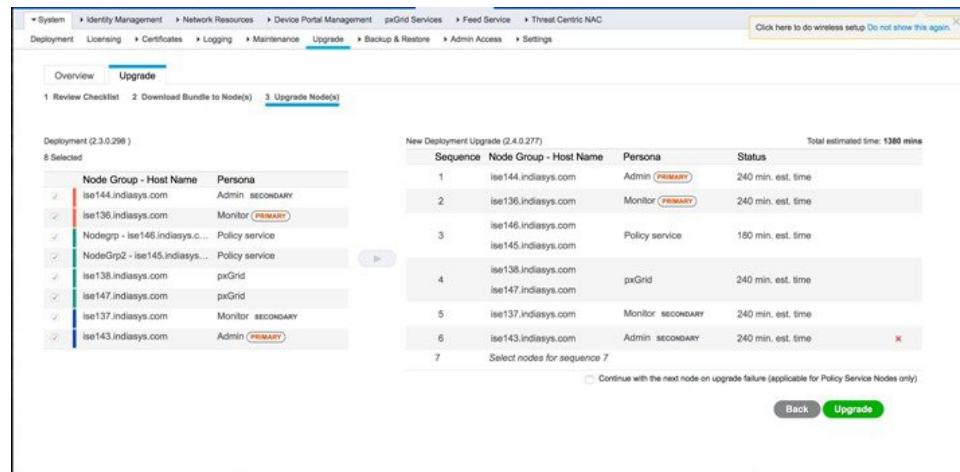
- アップグレードに使用するバンドルの隣にあるチェックボックスをオンにします。
- [確認 (Confirm)] をクリックします。

バンドルがノードにダウンロードされると、ノードステータスが「アップグレードの準備が整いました (Ready for Upgrade)」に変わります。

ステップ 5 [続行 (Continue)] をクリックします。

[ノードのアップグレード (Upgrade Nodes)] ウィンドウが表示されます。

図 2: 現在の展開と新しい展開を表示するアップグレードウィンドウ



ステップ 6 アップグレード順序を選択します。

ノードを新しい展開に移動すると、アップグレードの推定所要時間が [ノードのアップグレード (Upgrade Nodes)] ウィンドウに表示されます。この情報を使用して、アップグレードを計画し、ダウンタイムを最小化できます。管理ノードとモニタリング ノードのペアおよび複数のポリシー サービス ノードがある場合は、以下の手順に従います。

- デフォルトでは、セカンダリ管理ノードは、アップグレード順序の最初にリストされています。アップグレード後に、このノードは新しい展開でプライマリ管理ノードになります。
- プライマリ モニタリング ノードは、次に新しい展開にアップグレードされるノードです。
- ポリシー サービス ノードを選択し、新しい展開に移動します。ポリシー サービス ノードをアップグレードする順序を変更できます。

ポリシーサービスノードは、順番にまたは並行してアップグレードできます。ポリシーサービスノードのセットを選択し、並行してアップグレードできます。

- セカンダリ モニタリング ノードを選択し、新しい展開に移動します。
- 最後に、プライマリ管理ノードを選択し、新しい展開に移動します。

管理ノードがモニタリング ペルソナも担当する場合は、次の表に示す手順に従ってください。

現在の展開内のノード ペルソナ	アップグレードの順序
セカンダリ管理/プライマリ モニタリング ノード、 ポリシー サービス ノード、プライマリ管理/セカン ダリ モニタリング ノード	<ol style="list-style-type: none"> セカンダリ管理/プライマリ モニタリング ノード ポリシー サービス ノード プライマリ管理/セカンダリ モニタリング ノード
セカンダリ管理/セカンダリ モニタリング ノード、 ポリシー サービス ノード、プライマリ管理/プライ マリ モニタリング ノード	<ol style="list-style-type: none"> セカンダリ管理/セカンダリ モニタリング ノード ポリシー サービス ノード

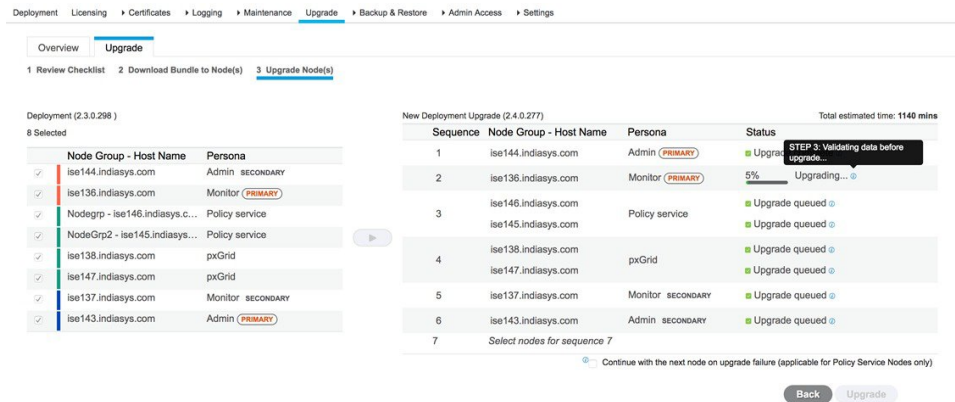
現在の展開内のノード ペルソナ	アップグレードの順序
	3. プライマリ管理/プライマリ モニタリング ノード
セカンダリ管理ノード、プライマリ モニタリング ノード、ポリシー サービス ノード、プライマリ管理/セカンダリ モニタリング ノード	1. セカンダリ管理ノード 2. プライマリ モニタリング ノード 3. ポリシー サービス ノード 4. プライマリ管理/セカンダリ モニタリング ノード
セカンダリ管理ノード、セカンダリ モニタリング ノード、ポリシー サービス ノード、プライマリ管理/プライマリ モニタリング ノード	1. セカンダリ管理ノード 2. セカンダリ モニタリング ノード 3. ポリシー サービス ノード 4. プライマリ管理/プライマリ モニタリング ノード
セカンダリ管理/プライマリ モニタリング ノード、ポリシー サービス ノード、セカンダリ モニタリング ノード、プライマリ管理ノード	1. セカンダリ管理/プライマリ モニタリング ノード 2. ポリシー サービス ノード 3. セカンダリ モニタリング ノード 4. プライマリ管理ノード
セカンダリ管理/セカンダリ モニタリング ノード、ポリシー サービス ノード、プライマリ モニタリング ノード、プライマリ管理ノード	1. セカンダリ管理/セカンダリ モニタリング ノード 2. ポリシー サービス ノード 3. プライマリ モニタリング ノード 4. プライマリ管理ノード

ステップ 7 アップグレードがアップグレード順序のいずれかのポリシーサービスノードで失敗した場合でもアップグレードを続行するには、[失敗時でもアップグレードを続行する (Continue with upgrade on failure)] チェックボックスをオンにします。

このオプションは、セカンダリ管理ノードおよびプライマリモニタリングノードには適用されません。これらのノードのいずれかに障害が発生すると、アップグレードプロセスはロールバックされます。ポリシーサービスノードのいずれかが失敗すると、セカンダリモニタリングノードおよびプライマリ管理ノードはアップグレードされず、古い展開内に残ります。

ステップ 8 [アップグレード (Upgrade)] をクリックして、展開のアップグレードを開始します。

図 3: アップグレードの進行状況を表示するアップグレードウィンドウ



各ノードのアップグレードの進行状況が表示されます。正常に完了すると、ノードのステータスが「アップグレード完了 (Upgrade Complete)」に変わります。

- (注) 管理者ポータルからノードをアップグレードするときに、ステータスが長時間変化しない場合 (80% のままの場合) は、CLI からアップグレードログをチェックするか、コンソールからアップグレードのステータスをチェックできます。アップグレードの進行状況を表示するには、CLI にログインするか、Cisco ISE ノードのコンソールを表示します。 **show logging application** コマンドを使用して、`upgrade-uibackend-cliconsole.log` および `upgrade-postosupgrade-yyyyymmdd-xxxxxx.log` を表示できます。
- (注) 新しい展開のプライマリ管理ノードでポスチャデータの更新処理が実行している場合、プライマリ管理ノードにノードを登録できません。ポスチャ更新プロセスが終了するまで待つ (約 20 分かかることがあります)、またはアップグレードまたはノードの新しい展開への登録中に、[管理 (Administration)] > [システム (System)] > [設定 (Settings)] > [ポスチャ (Posture)] > [更新 (Updates)] ページから、ポスチャの自動更新機能を無効にすることができます。

ソフトウェアパッチのインストール

展開内の Cisco ISE サーバにパッチをインストールする作業は、プライマリ PAN から行うことができます。プライマリ PAN からパッチをインストールするには、Cisco.com からクライアントブラウザを実行しているシステムにパッチをダウンロードします。

GUI からパッチをインストールする場合、パッチは最初にプライマリ PAN に自動的にインストールされます。その後、システムは、GUI にリストされている順序で、展開内の他のノードにパッチをインストールします。ノードが更新される順序を制御することはできません。

CLI からパッチをインストールする場合は、ノードの更新順序を制御できます。ただし、最初にプライマリ PAN にパッチをインストールすることを推奨します。



- (注) Cisco ISE のパッチをインライン ポスチャ ノードにインストールする作業を実行できるのは、CLI からに限られます。

始める前に

- スーパー管理者またはシステム管理者の管理者ロールが割り当てられている必要があります。
- 自動フェールオーバー設定が展開でイネーブルになっている場合はオフにします。ソフトウェア パッチをインストールすると、アプリケーション サーバプロセスが再起動されます。これらのサービスが再起動されるまで遅延が発生する場合があります。このサービスの再起動の遅延により、セカンダリ PAN の自動フェールオーバーが開始される場合があります。

ステップ 1 [管理 (Administration)] > [システム (System)] > [メンテナンス (Maintenance)] > [パッチ管理 (Patch Management)] > [インストール (Install)] を選択します。

ステップ 2 [参照 (Browse)] をクリックし、Cisco.com からダウンロードしたパッチを選択します。

ステップ 3 [インストール (Install)] をクリックしてパッチをインストールします。

PAN でのパッチのインストールが完了すると、Cisco ISE から自動的にログアウトされます。再びログインできるようになるまで数分間待つ必要があります。

- (注) パッチインストールの進行中は、[パッチ管理 (Patch Management)] ページ上の機能のうち、アクセスできるのは [ノードステータスを表示 (Show Node Status)] **Show Node Status**のみです。

ステップ 4 [管理 (Administration)] > [システム (System)] > [メンテナンス (Maintenance)] > [パッチ管理 (Patch Management)] を選択して、[パッチのインストール (Patch Installation)] ページに戻ります。

ステップ 5 セカンダリ ノードにインストールしたパッチの横のオプション ボタンをクリックし、[ノードステータスを表示 (Show Node Status)] をクリックしてインストールが完了したことを確認します。

次のタスク

1つ以上のセカンダリ ノードでパッチをインストールする必要がある場合は、ノードが動作中であることを確認し、プロセスを繰り返して残りのノードにパッチをインストールします。

Cisco ISE ソフトウェア パッチ

Cisco ISE ソフトウェア パッチは通常累積されます。Cisco ISE では、パッチのインストールおよびロールバックを CLI または GUI から実行できます。

関連トピック

[ソフトウェア パッチ インストールのガイドライン](#) (104 ページ)

- [ソフトウェア パッチのインストール \(102 ページ\)](#)
- [ソフトウェア パッチ インストールのガイドライン \(104 ページ\)](#)
- [ソフトウェア パッチ ロールバックのガイドライン \(105 ページ\)](#)
- [ソフトウェア パッチのインストール \(102 ページ\)](#)
- [ソフトウェア パッチのロールバック \(104 ページ\)](#)

ソフトウェア パッチ インストールのガイドライン

パッチのインストールまたはロールバックをスタンドアロンまたはプライマリ PAN から実行したときは、Cisco ISE によってアプリケーションが再起動されます。再びログインできる状態になるまで、数分かかることがあります。

インストールするパッチが、ネットワーク内に展開されている Cisco ISE のバージョンに適用されるものであることを確認してください。Cisco ISE はパッチ ファイルのバージョンの不一致とあらゆるエラーをレポートします。

Cisco ISE に現在インストールされているパッチよりも低いバージョンのパッチをインストールできません。同様に、あるバージョンのパッチの変更をロールバックしようとしたときに、それよりも高いバージョンのパッチがその時点で Cisco ISE にインストール済みの場合は、ロールバックはできません。たとえば、パッチ 3 が Cisco ISE サーバにインストール済みの場合に、パッチ 1 または 2 をインストールしたり、パッチ 1 または 2 にロールバックすることはできません。

分散展開の一部であるプライマリ PAN からパッチのインストールを実行するときは、Cisco ISE によってそのパッチが展開内のプライマリ ノードとすべてのセカンダリ ノードにインストールされます。パッチのインストールがプライマリ PAN で成功すると、Cisco ISE はセカンダリ ノードでパッチのインストールを続行します。プライマリ PAN で失敗した場合は、インストールはセカンダリ ノードに進みません。ただし、何らかの理由でセカンダリ ノードのいずれかでインストールに失敗した場合は、処理が続行され、展開内の次のセカンダリ ノードでインストールが実行されます。パッチがセカンダリ Cisco ISE ノード上にインストールされると、そのノードは続けて再起動されます。パッチをセカンダリ ノードにインストールしている間も、プライマリ PAN の管理タスクの実行を続けることができます。

2 ノード展開の一部であるプライマリ PAN からパッチのインストールを実行するときは、Cisco ISE によってそのパッチが展開内のプライマリ ノードとセカンダリ ノードにインストールされます。パッチのインストールがプライマリ PAN で成功すると、Cisco ISE はセカンダリ ノードでパッチのインストールを続行します。プライマリ PAN で失敗した場合は、インストールはセカンダリ ノードに進みません。パッチをセカンダリ ノードにインストールしている間も、プライマリ PAN の管理タスクの実行を続けることができます。

ソフトウェア パッチのロールバック

分散展開の一部である PAN からパッチのロールバックを実行するときは、Cisco ISE によってそのパッチが展開内のプライマリ ノードとすべてのセカンダリ ノードにロールバックされます。

始める前に

- スーパー管理者またはシステム管理者の管理者ロールが割り当てられている必要があります。
- 自動フェールオーバー設定が展開でイネーブルになっている場合はオフにします。ソフトウェア パッチをロールバックすると、アプリケーション サーバプロセスが再起動されます。これらのサービスが再起動されるまで遅延が発生する場合があります。このサービスの再起動の遅延により、セカンダリ管理ノードの自動フェールオーバーが開始される場合があります。

ステップ 1 [管理 (Administration)] > [システム (System)] > [メンテナンス (Maintenance)] > [パッチ管理 (Patch Management)] を選択します。

ステップ 2 変更をロールバックするパッチ バージョンのオプション ボタンをクリックしてから、[ロールバック (Rollback)] をクリックします。

(注) パッチのロールバックの進行中は、[パッチ管理 (Patch Management)] ページ上の機能のうち、アクセスできるのは [ノードステータスを表示 (Show Node Status)] **Show Node Status**のみです。

PAN からのパッチのロールバックが完了すると、Cisco ISE から自動的にログアウトされます。再びログインできるようになるまで数分間待つ必要があります。

ステップ 3 ログイン後に、ページの一番下にある [アラーム (Alarms)] リンクをクリックしてロールバック操作のステータスを表示します。

ステップ 4 [管理 (Administration)] > [システム (System)] > [メンテナンス (Maintenance)] > [パッチ管理 (Patch Management)] を選択します。

ステップ 5 パッチのロールバックの進行状況を表示するには、[パッチ管理 (Patch Management)] ページでパッチを選択し、[ノードステータスを表示 (Show Node Status)] をクリックします。

ステップ 6 パッチのオプション ボタンをクリックし、セカンダリ ノード上で [ノードステータスを表示 (Show Node Status)] をクリックして、そのパッチが展開内のすべてのノードからロールバックされたことを確認します。

そのパッチがロールバックされていないセカンダリ ノードがある場合は、そのノードが稼働中であることを確認してから、プロセスをもう一度実行して残りのノードから変更をロールバックしてください。Cisco ISE は、このバージョンのパッチがインストールされているノードからのみパッチをロールバックします。

関連トピック

[ソフトウェア パッチ ロールバックのガイドライン](#) (105 ページ)

ソフトウェア パッチ ロールバックのガイドライン

展開の Cisco ISE ノードからパッチをロールバックするには、最初に PAN から変更をロールバックします。これに成功すると、セカンダリ ノードからパッチがロールバックされます。PAN でロールバック プロセスが失敗した場合は、セカンダリ ノードからのパッチ ロールバック

クは行われません。ただし、いずれかのセカンダリ ノードでパッチのロールバックが失敗しても、展開内の次のセカンダリ ノードからのパッチのロールバックは継続されます。

Cisco ISE によるセカンダリ ノードからのパッチ ロールバックが進行中のときも、引き続き PAN GUI から他のタスクを実行できます。セカンダリ ノードは、ロールバック後に再起動されます。

パッチのインストールおよびロールバックの変更の表示

インストールされているパッチに関連するレポートを表示するには、次の手順を実行します。

始める前に

スーパー管理者またはシステム管理者の管理者ロールが割り当てられている必要があります。
[管理 (Administration)] > [システム (System)] > [メンテナンス (Maintenance)] > [パッチ管理 (Patch Management)] ページで、パッチをインストールまたはロールバックできます。展開内の各ノードで特定のパッチのステータス ([インストール済み (installed)]、[処理中 (in-progress)]、[未インストール (not installed)]) を確認できます。このためには、特定のパッチを選択し、[ノードステータスを表示 (Show Node Status)] ボタンをクリックします。

ステップ 1 [操作 (Operations)] > [レポート (Reports)] > [監査 (Audit)] > [操作監査 (Operations Audit)] を選択します。デフォルトでは、過去 7 日間のレコードが表示されます。

ステップ 2 [フィルタ (Filter)] ドロップダウンをクリックして [クイック フィルタ (Quick Filter)] または [拡張フィルタ (Advanced Filter)] を選択し、必要なキーワード (例: patch install initiated) を使用して、インストール済みのパッチを示すレポートを生成します。

FIPS モードのサポート

製品の Cisco Identity Services Engine は、組み込みの FIPS 140-2 検証済み暗号化モジュールのシスコ共通暗号化モジュール (証明書 #1643 および #2100) を使用します。FIPS コンプライアンスの要求の詳細については、『[FIPS Compliance Letter](#)』を参照してください。

FIPS モードを有効にすると、Cisco ISE 管理者インターフェイスのページの右上隅のノード名の左側に FIPS モードアイコンが表示されます。

Cisco ISE は、FIPS 140-2 レベル 1 標準でサポートされないプロトコルまたは証明書の使用を検出すると、準拠していないプロトコルまたは証明書の名前とともに警告を表示し、FIPS モードは有効になりません。必ず FIPS に準拠したプロトコルのみを選択し、FIPS モードを有効にする前に FIPS に非準拠の証明書を交換してください。

FIPS モードを有効にしたら、展開内の他のすべてのノードを再起動する必要があります。ネットワークの中断を最小限にするために、Cisco ISE は自動的にローリング再起動を実行します。

具体的には、最初にプライマリ PAN を再起動し、その後でセカンダリ ノードを 1 つずつ再起動します。



ヒント データベース移行プロセスを行う場合は、移行が完了してから FIPS モードを有効にすることを推奨します。

Cisco ISE リリース 1.3 は FIPS モードをサポートしていません。

Cisco ISE での FIPS モードの有効化

Cisco ISE ネットワークは、Federal Information Processing Standard (FIPS) 140-2 準拠の暗号化と復号化をサポートしています。

ステップ 1 [管理 (Administration)] > [システム (System)] > [設定 (Settings)] > [FIPS モード (FIPS Mode)] を選択します。

ステップ 2 [FIPS モード (FIPS Mode)] ドロップダウン リストで [有効 (Enabled)] オプションを選択します。

ステップ 3 [保存 (Save)] をクリックして、マシンを再起動します。

次のタスク

FIPS モードを有効にしたら、次の FIPS 140-2 準拠機能を有効にして設定します。

- [Cisco ISE へのネットワーク デバイスのインポート \(250 ページ\)](#)
- [自己署名証明書の生成 \(172 ページ\)](#)
- [証明書署名要求の作成と認証局への CSR の送信 \(181 ページ\)](#)
- [ネットワーク デバイス定義の設定 \(1227 ページ\)](#) で RADIUS 認証を設定します。

また、Common Access Card (CAC) 機能を使用して管理者アカウントの許可を有効にすることもできます。許可のために CAC 機能を使用することは、厳密には FIPS 140-2 の要件ではありませんが、セキュアアクセスの手法としてよく知られており、多くの環境で FIPS 140-2 準拠を強化するために使用されています。

FIPS モードの動作パラメータ

FIPS 標準では特定のアルゴリズムの使用について制限が設けられています。この標準を適用するには、Cisco ISE での FIPS 動作を有効にする必要があります。Cisco ISE による FIPS 140-2 準拠の有効化の手段として、RADIUS の共有秘密とキー管理が使用されます。FIPS モードでは、非 FIPS 準拠のアルゴリズムを使用するすべての機能が失敗するほか、特定の認証機能が無効になります。

また FIPS モードを有効にすると、Cisco ISE のゲスト ログイン機能に必要な Password Authentication Protocol (PAP) および Challenge Handshake Authentication Protocol (CHAP) プロトコルが自動的に無効になります。

FIPS モードが有効のときの Cisco NAC Agent の要件

Cisco NAC Agent は、Cisco ISE ネットワークを検出するために、常に Windows Internet Explorer TLS 1.0 の設定を探します。（これらの TLS 1.0 設定が Internet Explorer で有効になっている必要があります。）したがって、ネットワークにアクセスするクライアントマシン上で Cisco ISE のポスチャ評価機能を動作させるには、そのマシンに Windows Internet Explorer バージョン 7、8、または 9 がインストールされて TLS1.0 が有効になっている必要があります。Cisco NAC Agent は、Cisco ISE で FIPS モードが有効になっている場合に、自動的に Windows Internet Explorer の TLS 1.0 設定を有効化することができます。

管理者 CAC 認証のための Cisco ISE の設定

始める前に

設定を始める前に、次の手順を実行してください。

- （任意）FIPS モードを有効にします。FIPS モードは証明書ベースの認証には必要ありませんが、この 2 つのセキュリティ手段は多くの場合、組み合わせて使用されます。Cisco ISE を FIPS 140-2 準拠の環境に展開する予定があり、CAC 証明書ベース許可も使用する場合は、必ず FIPS モードを有効にするとともに、適切な秘密キーと暗号化/復号化設定を最初に指定してください。
- Cisco ISE のドメイン ネーム サーバ (DNS) が Active Directory に設定されていることを確認します。
- Active Directory のユーザとユーザ グループ メンバーシップが、管理者証明書ごとに定義されていることを確認します。

Cisco ISE による管理者の認証と許可を、ブラウザから送信された CAC ベースのクライアント証明書に基づいて実行できるようにするには、次の設定が完了していることを確認してください。

- 外部 ID ソース（次の例では Active Directory）
- 管理者が属する Active Directory のユーザ グループ
- ユーザのアイデンティティを証明書の中で見つける方法
- Active Directory ユーザ グループから Cisco ISE RBAC 権限へのマッピング
- クライアント証明書に署名する認証局（信頼）証明書
- クライアント証明書がすでに CA によって失効させられたかどうかを判断する方法

Cisco ISE にログインする場合、クレデンシャルを認証するために Common Access Card (CAC) を使用できます。

ステップ 1 FIPS モードを有効にします。FIPS モードを有効にすると、システムを再起動するように促されます。CA 証明書もインポートする場合は、再起動を遅らせることができます。

ステップ 2 Cisco ISE の Active Directory ID ソースを設定し、Active Directory にすべての Cisco ISE ノードを追加します。

ステップ 3 ガイドラインに従って証明書認証プロファイルを設定します。

[プリンシパル名 X.509 属性 (Principal Name X.509 Attribute)] フィールドでは、証明書内で管理者ユーザ名が格納されている属性を選択します。(CAC カードの場合は、カード上の署名証明書が通常は Active Directory でのユーザの検索に使用されます。プリンシパル名は、この証明書の「サブジェクトの別名 (Subject Alternative Name)」拡張情報の中にあります。具体的には、この拡張情報の「別の名前 (Other Name)」というフィールドです。したがって、ここで選択する属性は「Subject Alternative Name - Other Name」となります。)

ユーザの AD レコードにユーザの証明書が格納されている場合に、ブラウザから受信した証明書を AD の証明書と比較するには、[証明書のバイナリ比較 (Binary Certificate Comparison)] チェックボックスをオンにして、以前に指定した Active Directory インスタンス名を選択します。

ステップ 4 パスワードベースの admin 認証用の Active Directory を有効にします。Cisco ISE に接続し結合された Active Directory インスタンス名を選択します。

(注) その他の設定が完了するまでは、パスワードベースの認証を使用します。この手順の最後に、認証タイプをクライアント証明書ベースに変更できます。

ステップ 5 外部管理者グループを作成して、Active Directory グループにマッピングします。[管理 (Administration)] > [システム (System)] > [管理者アクセス (Admin Access)] > [管理者 (Administrators)] > [管理グループ (Admin Groups)] を選択します。外部システム管理者グループを作成します。

ステップ 6 外部管理グループに RBAC 権限を割り当てる管理者許可ポリシーを設定します。

注意 外部スーパー管理者グループを作成して Active Directory グループにマッピングし、スーパー管理者権限を持つ管理者許可ポリシー (メニューアクセスおよびデータ アクセス) を設定し、Active Directory グループに少なくとも 1 人のユーザを作成することを強く推奨します。このマッピングにより、クライアント証明書ベースの認証が有効になると、少なくとも 1 人の外部管理者がスーパー管理者権限を持つことが保証されます。これができないと、Cisco ISE 管理者が管理者ポータル重要な機能から締め出される状況になる可能性があります。

ステップ 7 [管理 (Administration)] > [システム (System)] > [証明書 (Certificates)] > [証明書ストア (Certificate Store)] を選択して、認証局証明書を Cisco ISE 証明書信頼ストアにインポートします。

Cisco ISE がクライアント証明書を受け入れるには、そのクライアント証明書の信頼チェーンの CA 証明書が Cisco ISE 証明書ストアの中にあることが条件となります。Cisco ISE 証明書ストアには適切な CA 証明書をインポートする必要があります。

a) [参照 (Browse)] をクリックして証明書を選択します。

b) [クライアント認証を信頼 (Trust for client authentication)] チェックボックスをオンにします。

- c) [送信 (Submit)] をクリックします。

Cisco ISE は、証明書をインポートしたら展開内のすべてのノードを再起動することを促します。すべての証明書をインポートするまで、再起動を遅らせることができます。ただし、すべての証明書をインポートしたら、次に進む前に Cisco ISE を再起動する必要があります。

ステップ 8 失効ステータス確認のための認証局証明書を設定します。

- [管理 (Administration)] > [システム (System)] > [証明書 (Certificates)] > [OSCP サービス (OSCP Services)] を選択します。
- OSCP サーバの名前、説明 (任意)、サーバの URL を入力します。
- [管理 (Administration)] > [システム (System)] > [証明書 (Certificates)] > [証明書ストア (Certificate Store)] を選択します。
- クライアント証明書に署名できる CA 証明書のそれぞれについて、その CA の失効ステータス チェックを行う方法を指定する必要があります。リストから CA 証明書を選択して [編集 (Edit)] をクリックします。編集ページで、OCSP または CRL 検証の一方あるいは両方を選択します。OCSP を選択した場合は、CA に使用する OCSP サービスを選択します。CRL を選択した場合は、CRL Distribution URL などの設定パラメータを指定します。

ステップ 9 クライアント証明書ベースの認証を有効にします。[管理 (Administration)] > [システム (System)] > [管理者アクセス (Admin Access)] > [認証 (Authentication)] を選択します。

- [認証方式 (Authentication Method)] タブの [クライアント証明書ベース (Client Certificate Based)] 認証タイプを選択します。
- 設定済みの証明書認証プロファイルを選択します。
- Active Directory のインスタンス名を選択します。
- [保存 (Save)] をクリックします。

ここで、パスワードベースの認証からクライアント証明書ベースの認証に切り替えます。設定済みの証明書認証プロファイルにより、管理者による証明書の認証方法を指定します。管理者は外部 ID ソースを使用して許可されます。この例では、Active Directory です。

Active Directory での管理者の検索には、証明書認証プロファイルからのプリンシパル名属性が使用されます。

Cisco ISE は、管理者 CAC 認証に設定されています。

関連トピック

[サポートされる Common Access Card 標準](#) (110 ページ)

[Cisco ISE での共通アクセス カードの動作](#) (111 ページ)

サポートされる Common Access Card 標準

Cisco ISE は、Common Access Card (CAC) 認証デバイスを使用して自身を認証する米国政府ユーザをサポートします。CAC は特定の従業員を識別する一連の X.509 クライアント証明書を含む電子チップの認識票です。CAC によるアクセスには、カードを挿入し PIN を入力するカードリーダーが必要です。カードからの証明書が Windows の証明書ストアに転送されます。

Windows の証明書ストアは、Cisco ISE などのローカル ブラウザで実行されているアプリケーションで使用可能です。

Windows Internet Explorer バージョン 8 または 9 を Windows 7 オペレーティング システムで使っている場合は、ActiveIdentity の ActivClient バージョン 6.2.0.133 をインストールする必要があります。このミドルウェアは、Cisco ISE を CAC とともに相互運用するためのサードパーティ製品です。ActiveIdentity セキュリティ クライアント製品の詳細については、[ActivID ActivClient Security Software Datasheet](#) を参照してください。

Cisco ISE での共通アクセス カードの動作

管理者ポータルは、クライアント証明書を使用してのみ Cisco ISE との認証が許可されるように設定できます。ユーザ ID とパスワードなどのクレデンシャル ベースの認証はできません。クライアント証明書認証では、共通アクセス カード (CAC) カードを挿入して PIN を入力してから、ブラウザのアドレス フィールドに Cisco ISE 管理者ポータルの URL を入力します。ブラウザによって証明書が Cisco ISE に転送され、Cisco ISE はログインセッションを証明書の内容に基づいて認証および許可します。このプロセスが完了すると、[Cisco ISE モニタリング およびトラブルシューティング (Cisco ISE Monitoring and Troubleshooting)] ホーム ページに表示され、適切な RBAC 権限が与えられます。

Diffie-Hellman アルゴリズムを使用した SSH キー交換の保護

Diffie-Hellman-Group14-SHA1 SSH キー交換しか許可しないように Cisco ISE を設定することができます。このためには、Cisco ISE コマンドライン インターフェイス (CLI) のコンフィギュレーション モードから次のコマンドを入力します。

```
service sshd key-exchange-algorithm diffie-hellman-group14-sha1
```

次に例を示します。

```
ise/admin#conf t
```

```
ise/admin (config)#service sshd key-exchange-algorithm diffie-hellman-group14-sha1
```

セキュア syslog 送信のための Cisco ISE の設定

Cisco ISE ノード間で、およびモニタリング ノードに対して、TLS 保護されたセキュア syslog のみを送信するように Cisco ISE を設定するには、次の手順を実行します。

始める前に

- 展開内のすべての Cisco ISE ノードに適切なサーバ証明書が設定されていることを確認します。FIPS 140-2 準拠にセットアップする場合は、証明書キーは 2,048 ビット以上のキーサイズが必要です。

- 管理者ポータルでの FIPS モードを有効にします。
- デフォルト ネットワーク アクセス認証ポリシーが、あらゆるバージョンの SSL プロトコルを許可しないことを確認します。FIPS 認定アルゴリズムとともに、FIPS モードで TLS プロトコルを使用します。
- 展開内のすべてのノードがプライマリ PAN に登録されていることを確認します。また、展開の少なくとも 1 つのノードに、セキュア syslog レシーバ (TLS サーバ) としての動作が有効になっているモニタリング ペルソナが含まれることも確認します。

ステップ 1 セキュア syslog リモート ロギング ターゲットを設定します。

ステップ 2 セキュア syslog リモート ロギング ターゲットに監査可能なイベントを送信するロギング カテゴリを有効にします。

ステップ 3 TCP syslog および UDP syslog コレクタを無効にします。TLS 保護された syslog コレクタのみを有効にします。

関連トピック

[セキュア syslog リモート ロギング ターゲットの設定 \(112 ページ\)](#)

[セキュア syslog ターゲットに監査可能なイベントを送信するためのロギング カテゴリの有効化 \(113 ページ\)](#)

[TCP syslog および UDP syslog コレクタの無効化 \(113 ページ\)](#)

セキュア syslog リモート ロギング ターゲットの設定

Cisco ISE システム ログは、さまざまな目的のために、ログ コレクタによって収集され保存されます。セキュア syslog ターゲットを設定するためには、ログ コレクタとして Cisco ISE モニタリング ノードを選択する必要があります。

ステップ 1 管理者ポータルにログインします。

ステップ 2 [管理 (Administration)] > [システム (System)] > [ロギング (Logging)] > [リモート ロギング ターゲット (Remote Logging Targets)] を選択します。

ステップ 3 [追加 (Add)] をクリックします。

ステップ 4 セキュア syslog サーバの名前を入力します。

ステップ 5 [ターゲット タイプ (Target Type)] ドロップダウン リストからセキュア syslog を選択します。

ステップ 6 [ステータス (Status)] ドロップダウン リストで [有効化 (Enabled)] を選択します。

ステップ 7 展開の Cisco ISE モニタリング ノードの IP アドレスを入力します。

ステップ 8 ポート番号として 6514 を入力します。セキュア syslog レシーバは TCP ポート 6514 をリスンします。

ステップ 9 syslog ファシリティ コードを選択します。デフォルトは LOCAL6 です。

ステップ 10 [サーバ ダウンの場合はバッファ メッセージ (Buffer Messages When Server is Down)] チェックボックスをオンにします。このオプションがオンの場合、Cisco ISE は、セキュア syslog レシーバが到達不能な場

合にはログを格納し、セキュア syslog レシーバを定期的に検査し、セキュア syslog レシーバが起動すると転送します。

- a) バッファ サイズを入力します。
- b) 定期的にセキュア syslog レシーバを検査するように、Cisco ISE の再接続タイムアウトを秒単位で入力します。

ステップ 11 Cisco ISE がセキュア syslog サーバに提示する CA 証明書を選択します。

ステップ 12 [サーバ証明書有効性を無視 (Ignore Server Certificate validation)] チェックボックスをオフにします。このオプションをオンにしてはいけません。

ステップ 13 [送信 (Submit)] をクリックします。

セキュア syslog ターゲットに監査可能なイベントを送信するためのロギング カテゴリの有効化

Cisco ISE によってセキュア syslog ターゲットに監査可能なイベントが送信されるようにするには、ロギング カテゴリを有効にする必要があります。

ステップ 1 管理者ポータルにログインします。

ステップ 2 [管理 (Administration)] > [システム (System)] > [ロギング (Logging)] > [ロギングカテゴリ (Logging Categories)] を選択します。

ステップ 3 AAA 監査ロギング カテゴリの横にあるオプション ボタンをクリックし、次に [編集 (Edit)] をクリックします。

ステップ 4 [ログ重大度レベル (Log Severity Level)] ドロップダウン リストから [警告 (WARN)] を選択します。

ステップ 5 作成済みのセキュア syslog リモート ロギング ターゲットを、選択したボックスに移動します。

ステップ 6 [保存 (Save)] をクリックします。

ステップ 7 次のロギング カテゴリを有効にする場合は、この手順を繰り返し行います。

- 管理および操作の監査 (Administrative and Operational Audit)
- ポスチャおよびクライアント プロビジョニングの監査 (Posture and Client Provisioning Audit)

TCP syslog および UDP syslog コレクタの無効化

Cisco ISE が ISE ノード間でセキュアな syslog のみを送信するには、TCP および UDP syslog コレクタを無効にして、セキュアな syslog コレクタのみを有効にする必要があります。

ステップ 1 管理者ポータルにログインします。

ステップ 2 [管理 (Administration)] > [システム (System)] > [ロギング (Logging)] > [リモート ロギング ターゲット (Remote Logging Targets)] を選択します。

ステップ 3 TCP または UDP syslog コレクタの横にあるオプション ボタンをクリックします。

ステップ 4 [編集 (Edit)] をクリックします。

ステップ 5 [ステータス (Status)] ドロップダウン リストから [無効化 (Disabled)] を選択します。

ステップ 6 [保存 (Save)] をクリックします。

ステップ 7 すべての TCP または UDP syslog コレクタが無効になるまで、このプロセスを繰り返します。

デフォルトのセキュア syslog コレクタ

Cisco ISE には、MnT ノード用のデフォルトのセキュア syslog コレクタがあります。デフォルトでは、これらのデフォルトセキュア syslog コレクタにはロギング カテゴリはマッピングされません。デフォルトセキュア syslog コレクタの名前は次のとおりです。

- プライマリ MnT ノード : SecureSyslogCollector
- セカンダリ MnT ノード : SecureSyslogCollector2

[リモート ロギング ターゲット (Remote Logging Targets)] ページ ([管理 (Administration)] > [システム (System)] > [ロギング (Logging)]) でこの情報を確認できます。デフォルトの syslog コレクタは削除できません。また、デフォルト syslog コレクタの [名前 (Name)]、[ターゲット タイプ (Target Type)]、[IP/ホスト アドレス (IP/Host address)]、および [ポート (Port)] フィールドは更新できません。

Cisco ISE の新規インストール中に、システムから「デフォルトの自己署名サーバ証明書 (Default Self-signed Server Certificate)」が信頼ストアに追加され、「クライアント認証および syslog 用の信頼 (Trust for Client authentication and Syslog)」目的で使用されるものとしてマークされます。これにより、この証明書はセキュア syslog に使用できるようになります。展開を設定する場合または証明書を更新する場合には、関連する証明書をセキュア syslog ターゲットに割り当てる必要があります。

アップグレード中に、ポート 6514 で MnT ノードを指し示している既存のセキュア syslog ターゲットがある場合、同じ名前と設定が維持されますが、アップグレード完了後にこれらの syslog ターゲットを削除すること、および [名前 (Name)]、[ターゲット タイプ (Target Type)]、[IP/ホスト アドレス (IP/Host address)]、および [ポート (Port)] フィールドを編集することはできません。アップグレードの時点でこのようなターゲットが存在しない場合、新規インストールの場合と同様にデフォルトセキュア syslog ターゲットが作成されますが、証明書のマッピングは行われません。これらの syslog ターゲットに関連証明書を割り当てることができます。どの証明書にもマッピングされていないセキュア syslog ターゲットをロギング カテゴリにマッピングしようとすると、次のメッセージが表示されます。

log_target_name □□□□□□□□□□□□□□ Please configure the certificate for log_target_name□

オフライン メンテナンス

メンテナンス時間が 1 時間未満の場合、ISE ノードをオフラインにしてメンテナンス作業を行います。ノードをオンラインに戻すと、メンテナンス時間内に行われたすべての変更が PAN により自動的に同期されます。変更が自動的に同期されない場合は、PAN を使用して手動で同期できます。

メンテナンス時間が 1 時間を超える場合は、メンテナンスの時点でノードを登録解除し、ノードを展開に再び追加するときにノードを再登録します。

処理があまり行われていない時間帯にメンテナンスをスケジュールすることが推奨されます。



-
- (注)
1. キューに格納されているメッセージの数が 1,000,000 を超える場合、または ISE ノードが 6 時間を超えてオフラインになっている場合には、データの複製の問題が発生している可能性があります。
 2. プライマリ MnT ノードでメンテナンスを行う予定の場合は、メンテナンスアクティビティを実行する前に、MnT ノードの操作バックアップを作成しておくことを推奨します。
-



第 6 章

管理者および管理者アクセス ポリシーの管理

- [ロールベース アクセス コントロール \(117 ページ\)](#)
- [Cisco ISE 管理者 \(117 ページ\)](#)
- [Cisco ISE 管理者グループ \(119 ページ\)](#)
- [Cisco ISE への管理アクセス \(130 ページ\)](#)

ロールベース アクセス コントロール

Cisco ISE では、管理者に対して特定のシステム動作の権限を許可または拒否するロールベース アクセス コントロール (RBAC) ポリシーを定義することができます。これらの RBAC ポリシーは、個々の管理者の ID、または管理者が属する管理者グループの ID に基づいて定義されます。

さらにセキュリティを強化し、管理者ポータルにアクセスできる者を制御するために、次を実行します。

- リモート クライアントの IP アドレスに基づいて管理アクセスを設定します。
- 管理アカウントの強力なパスワード ポリシーを定義します。
- 管理 GUI セッションのセッション タイムアウトを設定します。

Cisco ISE 管理者

Cisco ISE 管理者は管理者ポータルを使用して次の操作を行います。

- 展開、ヘルプ デスク操作、ネットワーク デバイス、および ノードのモニタリングとトラブルシューティングの管理。
- Cisco ISE のサービス、ポリシー、管理者アカウント、およびシステム設定と操作の管理
- 管理者パスワードおよびユーザ パスワードを変更します。

管理者は、コマンドラインインターフェイス (CLI) または Web ベースのインターフェイスから Cisco ISE にアクセスできます。Cisco ISE のセットアップ中に設定したユーザ名とパスワードは、CLI への管理アクセスにのみ使用されます。このロールは、CLI 管理者ユーザ (CLI 管理者) と見なされます。デフォルトでは、CLI 管理ユーザのユーザ名は `admin`、パスワードはセットアップで定義したパスワードです。デフォルトのパスワードはありません。この CLI 管理ユーザはデフォルトの `admin` ユーザと呼ばれます。このデフォルトの `admin` ユーザアカウントは削除できませんが、他の管理者が編集できます (このアカウントのパスワードを有効、無効、または変更するオプションを含む)。

管理者を作成するか、または既存のユーザを管理者ロールに昇格できます。管理者は、対応する管理者権限を無効にすることで、単純なネットワーク ユーザ ステータスに降格することもできます。

管理者は、Cisco ISE システムを設定および操作するローカル権限を持つユーザと見なすことができます。

管理者は、1 つ以上の管理者グループに割り当てられます。これらの管理者グループはシステムで事前に定義されています。これについては、次の項で説明します。

関連トピック

[Cisco ISE 管理者グループ](#) (119 ページ)

CLI 管理者と Web ベースの管理者の権限の比較

CLI 管理者は Cisco ISE アプリケーションの開始と停止、ソフトウェア パッチとアップグレードの適用、Cisco ISE アプライアンスのリロードとシャットダウン、およびすべてのシステムログとアプリケーションログの表示を行うことができます。CLI 管理者には特別な権限が付与されているため、CLI 管理者クレデンシャルを保護し、Cisco ISE の展開を設定および管理する Web ベースの管理者を作成することが推奨されます。

新しい Cisco ISE 管理者の作成

Cisco ISE 管理者は、特定の管理タスクを実行するために、特定のロールが割り当てられたアカウントが必要です。管理者アカウントを作成して、管理者が実行する必要がある管理タスクに基づいて 1 つ以上のロールの割り当てることができます。

[管理者ユーザ (Admin Users)] ページを使用して、Cisco ISE 管理者の属性の表示、作成、変更、削除、ステータスの変更、複製、または検索を実行できます。

ステップ 1 [管理 (Administration)] > [システム (System)] > [管理者アクセス (Admin Access)] > [管理者 (Administrators)] > [管理者ユーザ (Admin Users)] > [追加 (Add)] を選択します。

ステップ 2 次のいずれかを実行します。

- 新しいユーザの作成 (Create New User)

[新しいユーザの作成 (Create New User)] を選択すると、空白の [管理者ユーザ (Admin User)] ページが表示され、設定する必要があります。

- ネットワーク アクセス ユーザからの選択 (Select from Network Access Users)

[ネットワーク アクセス ユーザからの選択 (Select from Network Access Users)] を選択した場合、現在のユーザのリストが表示され、このリストでクリックしてユーザを選択することができ、対応する [管理者ユーザ (Admin User)] ページが表示されます。

ステップ 3 [管理者 (Administrator)] フィールドに値を入力します。[名前 (name)] フィールドでサポートされる文字は次のとおりです: # \$ ' () * + - . / @ _。

ステップ 4 [送信 (Submit)] をクリックして、新しい管理者を Cisco ISE 内部データベースに作成します。

関連トピック

[Cisco ISE 管理者 \(117 ページ\)](#)

[CLI 管理者と Web ベースの管理者の権限の比較 \(118 ページ\)](#)

[Cisco ISE 管理者グループ \(119 ページ\)](#)

[管理者アクセスの設定 \(136 ページ\)](#)

[読み取り専用管理ポリシー](#)

[内部読み取り専用管理者の作成](#)

[読み取り専用管理者のメニュー アクセスのカスタマイズ](#)

[外部グループを読み取り専用管理者グループにマッピング](#)

Cisco ISE 管理者グループ

管理者グループは、Cisco ISE でロールベース アクセス コントロール (RBAC) グループとも呼ばれ、同じ管理者グループに属する多数の管理者が含まれます。同じグループに属するすべての管理者は、共通の ID を共有し、同じ権限を持ちます。特定の管理者グループのメンバーとしての管理者の ID は、許可ポリシーの条件として使用できます。管理者は、複数の管理者グループに属することができます。

アクセス レベルに関係なく、すべての管理者アカウントは、管理者がアクセスできるすべてのページの、権限を持つオブジェクトを変更または削除できます。

Cisco ISE セキュリティ モデルでは、管理者が、その管理者が持っている同じ権限セット (Cisco ISE データベースで定義されているユーザの管理ロールに基づく) が含まれる管理者グループを作成することが制限されます。このようにして、管理者グループは、Cisco ISE システムにアクセスするための権限を定義する基礎を形成します。

次の表に、Cisco ISE で事前定義された管理者グループ、およびこれらのグループのメンバーが実行できるタスクを示します。

表 3: Cisco ISE 管理者グループ、アクセス レベル、権限、および制約事項

管理者グループロール	アクセス レベル	権限 (Permissions)	制約事項
カスタマイズ管理者	スポンサー、ゲスト、およびパーソナルデバイス ポータルの管理	<ul style="list-style-type: none"> • ゲストおよびスポンサー アクセスの設定。 • ゲスト アクセス設定の管理。 • エンドユーザ Web ポータルの管理。 	<ul style="list-style-type: none"> • Cisco ISE のすべてのポリシー管理、ID 管理、またはシステムレベルの設定タスクを実行できません • レポートを表示できません
ヘルプデスク管理者	クエリのモニタリングおよびトラブルシューティング操作	<ul style="list-style-type: none"> • すべてのレポートの実行 • すべてのトラブルシューティングフローの実行 • Cisco ISE ダッシュボードと livelogs の表示 • アラームの表示 	レポート、トラブルシューティングフロー、ライブ認証、またはアラームの作成、更新、または削除は実行できません

管理者グループロール	アクセス レベル	権限 (Permissions)	制約事項
ID 管理者	<ul style="list-style-type: none"> • ユーザ アカウントおよびエンドポイントの管理 • ID ソースの管理 	<ul style="list-style-type: none"> • ユーザ アカウントおよびエンドポイントの追加、編集、および削除 • ID ソースの追加、編集、および削除 • ID ソース順序の追加、編集、および削除 • ユーザ アカウントの一般的な設定 (属性およびパスワード ポリシー) • Cisco ISE ダッシュボード、livelogs、アラーム、およびレポートの表示。 • すべてのトラブルシューティングフローの実行。 	Cisco ISE のすべてのポリシー管理またはシステムレベルの設定タスクを実行できません
MnT 管理者	すべてのモニタリングおよびトラブルシューティング操作の実行。	<ul style="list-style-type: none"> • すべてのレポートの管理 (実行、作成、および削除) • すべてのトラブルシューティングフローの実行 • Cisco ISE ダッシュボードとlivelogsの表示 • アラームの管理 (作成、更新、表示、および削除) 	Cisco ISE のすべてのポリシー管理、ID管理、またはシステムレベルの設定タスクを実行できません

管理者グループロール	アクセス レベル	権限 (Permissions)	制約事項
ネットワークデバイス 管理者	Cisco ISE ネットワーク デバイスとネットワー ク デバイス リポジト リを管理します。	<ul style="list-style-type: none"> • ネットワーク デ バイスに対する読 み取りおよび書き 込み権限 • NDG およびすべ てのネットワーク リソース オブ ジェクト タイプ に対する読み取り および書き込み権 限 • Cisco ISE ダッ シュボード、 livelogs、アラ ーム、およびレポー トの表示 • すべてのトラブル シューティング フローの実行 	Cisco ISE のすべてのポ リシー管理、ID 管理、 またはシステム レベル の設定タスクを実行で きません

管理者グループロール	アクセス レベル	権限 (Permissions)	制約事項
ポリシー管理者	認証、許可、ポスチャ、プロファイラ、クライアントプロビジョニング、およびワークセンターに関連する、ネットワーク上のすべての Cisco ISE サービスのポリシーを作成および管理します。	<ul style="list-style-type: none"> • ポリシーで使用されるすべての要素（許可プロファイル、NDG、条件など）に対する読み取りおよび書き込み権限 • ID、エンドポイント、および ID グループ（ユーザー ID グループおよびエンドポイント ID グループ）に対する読み取りおよび書き込み権限 • サービス ポリシーおよび設定に対する読み取りおよび書き込み権限 • Cisco ISE ダッシュボード、livelogs、アラーム、およびレポートの表示 • すべてのトラブルシューティングフローの実行 • デバイス管理：デバイス管理ワークセンターにアクセスします。TACACS ポリシーの条件および結果に関する権限。TACACS プロキシおよびプロキシケンスのネットワーク デバイス権限。 	<p>Cisco ISE のすべての ID 管理またはシステムレベルの設定タスクを実行できません</p> <p>デバイス管理：ワークセンターへのアクセスは下位リンクへのアクセスを保証していません。</p>

管理者グループロール	アクセス レベル	権限 (Permissions)	制約事項
RBAC 管理者	エンドポイント保護 サービス適応型ネット ワーク制御を除く、 [操作 (Operations)] メ ニューの下すべての タスク、および [管理 (Administration)] の 下のいくつかのメ ニュー項目への部分的 なアクセス	<ul style="list-style-type: none"> • 認証の詳細の表示 • エンドポイント保護サービス適応型ネットワーク制御の有効化/無効化 • アラームの作成、編集、および削除、レポートの生成と表示、Cisco ISE を使用したネットワーク内の問題のトラブルシューティング • 管理者アカウント設定および管理者グループ設定に対する読み取り権限 • RBAC ポリシーページに加えて、管理者アクセスおよびデータ アクセス権限に対する表示権限 • Cisco ISE ダッシュボード、livelogs、アラーム、およびレポートの表示 • すべてのトラブルシューティングフローの実行 	Cisco ISE のすべての ID 管理またはシステムレベルの設定タスクを実行できません

管理者グループロール	アクセス レベル	権限 (Permissions)	制約事項
スーパー管理者	すべての Cisco ISE 管理機能。デフォルトの管理者アカウントは、このグループに属します。	<p>すべての Cisco ISE リソースに対する作成、読み取り、更新、削除、および実行 (CRUDX) 権限。</p> <p>(注) スーパー管理者ユーザは、デフォルトのシステム生成 RBAC ポリシーおよび権限は変更できません。これを行うには、ニーズに基づいた必要な権限が含まれた新しい RBAC ポリシーを作成し、これらのポリシーを任意の管理者グループにマッピングする必要があります。</p> <p>デバイス管理：デバイス管理ワークセンターにアクセスします。TACACS ポリシーの条件および結果に関する権限。TACACS プロキシおよびプロキシシークエンスのネットワークデバイス権限。さらに、TACACS グローバルプロトコル設定をイネーブルにする権限。</p>	デバイス管理：ワークセンターへのアクセスは下位リンクへのアクセスを保証していません。

管理者グループロール	アクセス レベル	権限 (Permissions)	制約事項
システム管理者	すべての Cisco ISE 設定およびメンテナンスのタスク。		Cisco ISE のすべてのポリシー管理またはシステムレベルの設定タスクを実行できません

管理者グループロール	アクセス レベル	権限 (Permissions)	制約事項
		<p>[操作 (Operations)] タブの下すべてのアクティビティを実行するためのフル アクセス (読み取りおよび書き込み権限) 、および [管理 (Administration)] タブの下いくつかのメニュー項目への部分的なアクセス。</p> <ul style="list-style-type: none"> • 管理者アカウント設定および管理者グループ設定に対する読み取り権限 • RBAC ポリシーページに加えて、管理者アクセスおよびデータ アクセス権限に対する読み取り権限 • [管理 (Administration)] > [システム (System)] メニューのすべてのオプションに対する読み取りおよび書き込み権限 • 認証の詳細の表示 • エンドポイント保護サービス適応型ネットワーク制御の有効化/無効化 • アラームの作成、編集、および削除、レポートの生成と表示、Cisco ISE を使用したネットワーク内の 	

管理者グループロール	アクセス レベル	権限 (Permissions)	制約事項
		<p>問題のトラブルシューティング</p> <ul style="list-style-type: none"> デバイス管理 : TACACS グローバル プロトコル設定をイネーブルにする権限。 	
外部 RESTful サービス (ERS) 管理者	GET、POST、DELETE、PUT など、すべての ERS API 要求へのフル アクセス	<ul style="list-style-type: none"> ERS API 要求の作成、読み取り、更新、および削除 	ロールは、内部ユーザ、ID グループ、エンドポイント、エンドポイントグループ、および SGT をサポートする ERS 許可のみを対象としています
外部 RESTful サービス (ERS) オペレータ	ERS API への読み取り専用アクセス、GET のみ	<ul style="list-style-type: none"> ERS API 要求の読み取りのみ可能 	ロールは、内部ユーザ、ID グループ、エンドポイント、エンドポイントグループ、および SGT をサポートする ERS 許可のみを対象としています
TACACS+ Admin	フル アクセス	<p>次へのアクセス :</p> <ul style="list-style-type: none"> デバイス管理ワークセンター。 展開 (Deployment) : TACACS+ サービスを有効にします。 外部 ID ストア。 [操作 (Operations)] > [TACACS ライブ ログ (TACACS Live Logs)] ページ。 	—

関連トピック

[Cisco ISE 管理者](#) (117 ページ)

管理者グループの作成

[管理者グループ (Admin Groups)] ページでは、Cisco ISE ネットワーク管理者グループを表示、作成、変更、削除、複製、またはフィルタリングできます。

始める前に

外部管理者グループ タイプを設定するには、1 つ以上の外部 ID ストアが指定されている必要があります。

ステップ 1 [管理 (Administration)] > [システム (System)] > [管理者アクセス (Admin Access)] > [管理者 (Administrators)] > [管理者グループ (Admin Groups)] を選択します。

ステップ 2 [追加 (Add)] をクリックし、[名前 (Name)] および [説明 (Description)] を入力します。[名前 (name)] フィールドでサポートされる特殊文字は次のとおりです：スペース、# \$ & ' () * + - . / @ _。

ステップ 3 設定する管理者グループのタイプを次のように指定します。

- [内部 (Internal)] : このグループタイプに割り当てられた管理者は、Cisco ISE 内部データベースに保存されたクレデンシャルに対して認証を行います。
- [外部 (External)] : このグループに割り当てられた管理者は、属性セクタで指定した外部 ID ストアに含まれているクレデンシャルに対して認証を行います。[外部 (External)] を選択した後、Cisco ISE による外部グループ情報のインポート元になる ID ストアを指定します。

ステップ 4 [追加 (Add)] をクリックして、ユーザを [管理者グループ ユーザ (Admin Group Users)] テーブルに追加します。[ユーザ (Users)] リストで、管理者グループに追加するユーザを選択します。

ステップ 5 ユーザを [管理者グループ ユーザ (Admin Group Users)] テーブルから削除するには、削除するユーザに対応するチェックボックスをオンにして、[削除 (Remove)] をクリックします。

ステップ 6 [送信 (Submit)] をクリックして、作成した管理者グループに対して行った変更を Cisco ISE データベースに保存します。



(注) 内部ユーザに認証用の外部 ID ストアが設定されている場合、内部ユーザは ISE 管理者用ポータルにログインするときに、その外部 ID ストアを ID ソースとして選択する必要があります。内部 ID ストアを選択すると認証が失敗します。

関連トピック

[Cisco ISE 管理者グループ](#) (119 ページ)

Cisco ISE への管理アクセス

Cisco ISE 管理者は、自分が属する管理者グループに基づいてさまざまな管理タスクを実行できます。これらの管理タスクは重大であり、管理アクセスがネットワークでの Cisco ISE の管理を許可されたユーザに制限されるようにする必要があります。

Cisco ISE では、次のオプションによって Web インターフェイスへの管理アクセスを制御することができます。

Cisco ISE のロールベース アクセス コントロール

ロールベース アクセス コントロール ポリシー（管理者アクセスと呼ばれる）は自分で定義するアクセス コントロール ポリシーで、Cisco ISE 管理インターフェイスへのアクセスを制限できます。これらの管理者アクセスポリシーによって、個々の管理者ユーザまたは管理者グループに適用する指定のロールベース アクセス権限設定を使用し、管理者単位または管理者グループ単位でアクセスの量とタイプをカスタマイズすることができます。

ロールベース アクセスにより、各エンティティがアクセスできる対象が決まり、アクセス コントロール ポリシーにより制御されます。また、ロールベース アクセスにより、使用中の管理ロール、エンティティが属している管理者グループ、およびエンティティのロールに基づいて適用される対応する権限と設定も決まります。

ロールベースの権限

Cisco ISE は、メニュー アクセス権限およびデータ アクセス権限と呼ばれる、メニューおよびデータ レベルの権限を設定することができます。

メニューアクセス権限により、Cisco ISE 管理インターフェイスのメニューおよびサブメニュー項目を表示または非表示にすることができます。この機能によって、メニューレベルのアクセスを制限または有効にすることができるように権限を作成することができます。

データ アクセス権限により、Cisco ISE インターフェイスの次のデータへの読み取り/書き込みアクセス権、読み取り専用アクセス権、またはアクセス権なしを付与できます。管理者グループ、ユーザ ID グループ、エンドポイント ID グループ、ロケーション、およびデバイス タイプ。

RBAC ポリシー

RBAC ポリシーにより、管理者にメニュー項目やその他の ID グループ データ要素への特定のタイプのアクセスを付与できるかどうかが決まります。RBAC ポリシーを使用して、管理グループに基づく管理者に、メニュー項目または ID グループ データ要素へのアクセスを許可または拒否できます。管理者は、管理者ポータルにログインすると、関連付けられている管理者グループに定義されているポリシーおよび権限に基づいて、メニューおよびデータにアクセスできます。

RBAC ポリシーは、管理者グループをメニュー アクセス権限とデータ アクセス権限にマッピングします。たとえば、ネットワーク管理者に [管理者アクセス (Admin Access)] 操作メニュー

およびポリシーデータ要素を表示しないようにすることができます。これは、ネットワーク管理者が関連付けられるカスタム RBAC ポリシーを作成することで実現できます。

デフォルトのメニュー アクセス権限

Cisco ISE では、事前定義された一連の管理者グループに関連付けられた、すぐに使用できる権限セットが用意されています。事前定義済みの管理者グループ権限により、任意の管理者グループのメンバーが、管理インターフェイス内のメニュー項目へのフルアクセス権または制限されたアクセス権（メニューアクセスと呼ばれます）を持つように権限を設定したり、その他の管理者グループのデータ アクセス要素の使用（データ アクセスと呼ばれます）を管理者グループに委任するように権限を設定したりできます。これらの権限は、さまざまな管理者グループ用の RBAC ポリシーの策定にさらに使用できる再利用可能なエンティティです。Cisco ISE では、デフォルトの RBAC ポリシーですでに使用されている一連のシステム定義メニューアクセス権限が用意されています。定義済みのメニュー アクセス権限とは別に、Cisco ISE では RBAC ポリシーで使用できるカスタム メニュー アクセス権限を作成することができます。キー アイコンはメニューとサブメニューのメニュー アクセス権限を表し、クロス付きのキー アイコンは異なる RBAC グループのアクセス権限がないことを表します。



- (注) スーパー管理者ユーザの場合、すべてのメニュー項目が使用可能です。その他の管理ユーザの場合、このカラムのすべてのメニュー項目はスタンドアロン展開、および分散展開におけるプライマリ ノードで使用可能です。分散展開のセカンダリ ノードの場合、[管理 (Administration)] タブの下メニュー項目は使用不可です。

メニュー アクセス権限の設定

Cisco ISE では、RBAC ポリシーにマッピングできるカスタム メニュー アクセス権限を作成することができます。管理者のロールに応じて、管理者の特定のメニュー オプションのみへのアクセスを許可できます。

ステップ 1 [管理 (Administration)] > [システム (System)] > [管理者アクセス (Admin Access)] > [認証 (Authorization)] > [権限 (Permissions)] > [メニュー アクセス (Menu Access)] を選択します。

ステップ 2 [追加 (Add)] をクリックし、[名前 (Name)] フィールドおよび[説明 (Description)] フィールドに値を入力します。

- 目的のレベルまでメニュー項目をクリックして展開し、権限を作成するメニュー項目をクリックします。
- [メニュー アクセス (Menu Access)] 領域の[権限 (Permissions)] で、[表示 (Show)] をクリックします。

ステップ 3 [送信 (Submit)] をクリックします。

データ アクセス権限を付与するための前提条件

RBAC 管理者がオブジェクト（たとえば「ユーザ ID グループ」データ型の「従業員」）へのフルアクセス権限を持っている場合、管理者はそのグループに属するユーザの表示、追加、更新、削除を行うことができます。管理者に [ユーザ (Users)] ページのメニューのアクセス権限が付与されていることを確認します ([管理 (Administration)] > [ID の管理 (Identity Management)] > [ID (Identities)] > [ユーザ (Users)])。これは、ネットワーク デバイスとエンドポイント オブジェクトに当てはまります (ネットワーク デバイス グループおよびエンドポイント ID グループのデータ型に付与されたアクセス権限に基づく)。

デフォルトのネットワーク デバイス グループ オブジェクト (すべてのデバイスタイプおよびすべてのロケーション) に属するネットワーク デバイスのデータ アクセスを有効にしたり、制限したりすることはできません。これらのデフォルト ネットワーク デバイス グループ オブジェクトの下に作成されたオブジェクトに対するフルアクセスデータ権限が付与される場合、すべてのネットワーク デバイスが表示されます。このため、デフォルト ネットワーク デバイス グループ オブジェクトに依存しない、ネットワーク デバイス グループのデータ型の階層を別個に作成することをお勧めします。制限付きアクセスを作成するには、新たに作成された ネットワーク デバイス グループに、ネットワーク デバイス オブジェクトを割り当てる必要があります。



(注) ユーザ ID グループ、ネットワーク デバイス グループ、およびエンドポイント ID グループに関してのみ、データ アクセス権限を有効にしたり制限したりできます。管理グループには当てはまりません。

デフォルトのデータ アクセス権限

Cisco ISE では、事前定義されたデータ アクセス権限のセットが付属しています。データ アクセス権限により、複数の管理者が、同じユーザ母集団内でデータ アクセス権限を持つことができます。データ アクセス権限の使用を1つ以上の管理者グループに対して有効化または制限することができます。このプロセスにより、1つの管理者グループの管理者に対する自律委任制御が可能となり、選択的関連付けを介して選択済みの管理者グループのデータ アクセス権限を再利用できます。データ アクセス権限の範囲は、フルアクセス権から、選択された管理者グループまたはネットワーク デバイス グループを表示するためのアクセス権なしまでとなります。RBAC ポリシーは、管理者 (RBAC) グループ、メニューアクセス、データアクセス権限に基づいて定義されます。最初に、メニューアクセス権限とデータ アクセス権限を作成し、次に、対応するメニューアクセス権限とデータ アクセス権限に管理者グループを関連付ける RBAC ポリシーを作成します。RBAC ポリシーには、次の形式を使用します。admin_group=Super Admin の場合、スーパー管理者メニュー アクセス権限とスーパー管理者データ アクセス権限を割り当てます。定義済みのデータ アクセス権限とは別に、Cisco ISE では RBAC ポリシーと関連付けることができるカスタム データ アクセス権限を作成することができます。

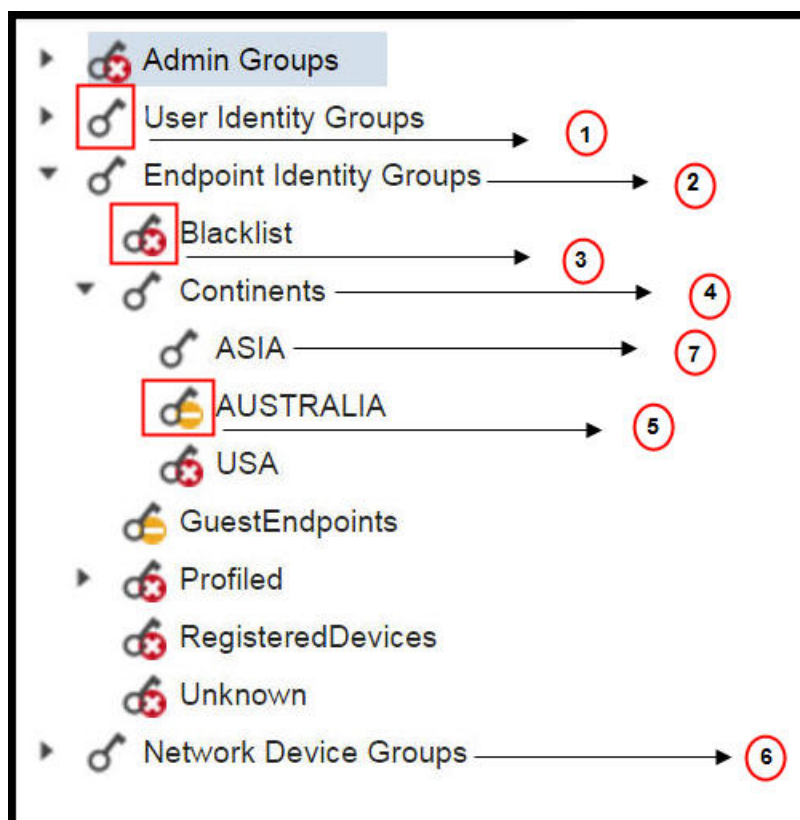
管理者グループに付与することができる、フルアクセス、アクセスなし、読み取り専用という名前の3つのデータ アクセス権限があります。

読み取り専用権限は次の管理者グループに付与できます。

- [管理 (Administration)] > [管理者アクセス (Admin Access)] > [管理者 (Administrators)] > [管理者グループ (Admin Groups)]
- [管理 (Administration)] > [グループ (Groups)] > [ユーザ ID グループ (User Identity Group)]
- [管理 (Administration)] > [グループ (Groups)] > [エンドポイント ID グループ (Endpoint Identity Groups)]
- [ネットワーク可視性 (Network Visibility)] > [エンドポイント (Endpoints)]
- [管理 (Administration)] > [ネットワーク リソース (Network Resources)] > [ネットワーク デバイス グループ (Network Device Groups)]
- [管理 (Administration)] > [ネットワーク リソース (Network Resources)] > [ネットワーク デバイス (Network Devices)]
- [管理 (Administration)] > [ID の管理 (Identity Management)] > [ID (Identities)]
- [管理 (Administration)] > [ID の管理 (Identity Management)] > [グループ (Groups)] > [ユーザ ID グループ (User Identity Groups)]
- [管理 (Administration)] > [ID の管理 (Identity Management)] > [グループ (Groups)] > [エンドポイント ID グループ (Endpoint Identity Groups)]

データ タイプ ([エンドポイント ID グループ (Endpoint Identity Groups)] など) に対して読み取り専用権限を持つ場合は、そのデータ タイプに CRUD 操作を実行することはできません。オブジェクト (GuestEndpoints など) に対して読み取り専用権限を持つ場合には、そのオブジェクトに編集/削除操作を実行することはできません。

以下の図に、さまざまな RBAC グループのための追加のサブメニューまたはオプションを含む 2 番目または 3 番目のレベルのメニューに、データ アクセス権限がどのように適用されるかを示します。



ラベル (Label)	説明
1	[ユーザ ID グループ (User Identity Groups)] データ タイプのフルアクセスが示されています。
2	[エンドポイント ID グループ (Endpoint Identity Groups)] が、その子 (Asia) に付与されている最大の権限 (フル アクセス) を得ていることが示されています。
3	オブジェクト (Blacklist) のアクセス権限がないことが示されています。
4	親 (Continents) が、その子 (Asia) に付与されている最大のアクセス権限を得ていることが示されています。
5	オブジェクト (Australia) の読み取り専用アクセスが示されています。

ラベル (Label)	説明
[6]	親 ([ネットワーク デバイス グループ (Network Device Groups)]) にフル アクセスが付与されている場合、子が自動的に権限を継承することが示されています。
7	親 (Asia) にフル アクセスが付与されている場合、オブジェクトに権限が明示的に付与されていない限り、オブジェクトがフル アクセス権限を継承することが示されています。

データ アクセス権限の設定

Cisco ISE では、RBAC ポリシーにマッピングできるカスタム データ アクセス権限を作成することができます。管理者のロールに基づいて、データを選択するのみのアクセス権を管理者に提供することができます。

ステップ 1 [管理 (Administration)] > [システム (System)] > [管理者アクセス (Admin Access)] > [許可 (Authorization)] > [権限 (Permissions)] を選択します。

ステップ 2 [権限 (Permissions)] > [データ アクセス (Data Access)] を選択します。

ステップ 3 [追加 (Add)] をクリックし、[名前 (Name)] フィールドおよび [説明 (Description)] フィールドに値を入力します。

- 管理者グループをクリックして展開し、目的の管理者グループを選択します。
- [フル アクセス (Full Access)]、[読み取り専用アクセス (Read Only Access)]、または [アクセスなし (No Access)] をクリックします。

ステップ 4 [保存 (Save)] をクリックします。

管理者のアクセス ポリシーの設定

管理者アクセス (RBAC) ポリシーは if-then 形式で表され、ここで if は RBAC 管理者グループの値、および then は RBAC 権限の値になります。

[RBAC ポリシー (RBAC policies)] ページ ([管理 (Administration)] > [システム (System)] > [管理者アクセス (Admin Access)] > [認証 (Authorization)] > [ポリシー (Policy)]) には、デフォルト ポリシーのリストが含まれています。これらのデフォルト ポリシーは編集または削除できません。[RBAC ポリシー (RBAC policies)] ページでは、特に職場の管理者グループ用にカスタム RBAC ポリシーを作成し、パーソナライズされた管理者グループに適用できます。

制限付きメニュー アクセスを割り当てるときには、データ アクセス権限により、指定されているメニューを使用するために必要なデータに管理者がアクセスできることを確認してください。

い。たとえばデバイス ポータルへのメニュー アクセスを付与するが、エンドポイント ID グループへのデータ アクセスを許可しないと、管理者はポータルを変更できません。

始める前に

- RBAC ポリシーを定義するすべての管理者グループを作成していることを確認します。
- これらの管理者グループが、個々の管理者ユーザにマッピングされていることを確認します。
- メニュー アクセス権限やデータ アクセス権限など、RBAC 権限を設定していることを確認します。

ステップ 1 [管理 (Administration)] > [システム (System)] > [管理者アクセス (Admin Access)] > [許可 (Authorization)] > [ポリシー (Policy)] を選択します。

[RBAC ポリシー (RBAC Policies)] ページには、デフォルトの管理者グループ用にすぐに使用できる定義済みの一連のポリシーが含まれています。これらのデフォルト ポリシーは編集または削除できません。

ステップ 2 デフォルト RBAC ポリシー ルールのいずれかの隣にある [操作 (Action)] をクリックします。

ここでは、新しい RBAC ポリシーを挿入し、既存の RBAC ポリシーを複製し、既存の RBAC ポリシーを削除できます。

ステップ 3 [新しいポリシーの挿入 (Insert New Policy)] をクリックします。

ステップ 4 [ルール名 (Rule Name)]、[RBAC グループ (RBAC Group(s))]、および [権限 (Permissions)] フィールドに値を入力します。

RBAC ポリシーの作成時に、複数のメニュー アクセス権限とデータ アクセス権限を選択することはできません。

ステップ 5 [保存 (Save)] をクリックします。

関連トピック

[RBAC ポリシー \(130 ページ\)](#)

[デフォルトのメニュー アクセス権限 \(131 ページ\)](#)

[メニュー アクセス権限の設定 \(131 ページ\)](#)

[デフォルトのデータ アクセス権限 \(132 ページ\)](#)

[データ アクセス権限の設定 \(135 ページ\)](#)

管理者アクセスの設定

Cisco ISE では、セキュリティ強化のために管理者アカウントにルールを定義できます。管理インターフェイスへのアクセスを制限したり、強力なパスワードの使用やパスワードの定期的な変更を管理者に強制することができます。Cisco ISE の [管理者アカウントの設定 (Administrator

Account Settings)] で定義するパスワード ポリシーは、すべての管理者アカウントに適用されます。

Cisco ISE では、管理者パスワードでの UTF-8 文字の使用はサポートされていません。

同時管理セッションとログインバナーの最大数の設定

同時管理 GUI または CLI (SSH) セッションの最大数、および管理 Web または CLI インターフェイスにアクセスする管理者を手助け、ガイドするログインバナーを設定できます。管理者のログイン前後に表示されるログインバナーを設定できます。デフォルトでは、これらのログインバナーは無効になっています。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

-
- ステップ 1 [管理 (Administration)]>[システム (System)]>[管理者アクセス (Admin Access)]>[設定 (Settings)]>[アクセス (Access)]>[セッション (Session)] を選択します。
 - ステップ 2 GUI および CLI インターフェイスを介した同時管理セッションの、許可する最大数を入力します。同時管理 GUI セッションの有効範囲は 1 ～ 20 です。同時管理 CLI セッションの有効範囲は 1 ～ 10 です。
 - ステップ 3 Cisco ISE で管理者がログインする前にメッセージを表示する場合は、[プリログインバナー (Pre-login banner)] チェックボックスをオンにして、テキストボックスにメッセージを入力します。
 - ステップ 4 Cisco ISE で管理者がログインした後にメッセージを表示する場合は、[ポストログインバナー (Post-login banner)] チェックボックスをオンにして、テキストボックスにメッセージを入力します。
 - ステップ 5 [保存 (Save)] をクリックします。
-

関連トピック

[IP アドレスの選択からの Cisco ISE への管理アクセスの許可](#) (137 ページ)

IP アドレスの選択からの Cisco ISE への管理アクセスの許可

Cisco ISE では、管理者が Cisco ISE 管理インターフェイスにアクセスできる IP アドレスのリストを設定することができます。

管理者アクセス コントロール設定は、管理ペルソナ、ポリシー サービス ペルソナ、またはモニタリング ペルソナを担う Cisco ISE ノードに対してのみ適用できます。これらの制限はプライマリ ノードからセカンダリ ノードに複製されます。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

-
- ステップ 1 [管理 (Administration)]>[システム (System)]>[管理者アクセス (Admin Access)]>[設定 (Settings)]>[アクセス (Access)]>[IP アクセス (IP Access)] を選択します。
 - ステップ 2 [リストにある IP アドレスだけに接続を許可 (Allow only listed IP addresses to connect)] を選択します。

- ステップ 3** [アクセス制限の IP リストの設定 (Configure IP List for Access Restriction)] 領域で、[追加 (Add)] をクリックします。
- ステップ 4** [IP アドレス (IP Address)] フィールドに IP アドレスをクラスレス ドメイン間ルーティング (CIDR) 形式で入力します。
- ステップ 5** [CIDR 形式のネットマスク (Netmask in CIDR format)] フィールドにサブネット マスクを入力します。
- ステップ 6** [OK] をクリックします。このプロセスを繰り返して、他の IP アドレス範囲をこのリストに追加します。
- ステップ 7** [保存 (Save)] をクリックして、変更内容を保存します。

関連トピック

[管理者アクセスの設定](#) (136 ページ)

管理者アカウントのパスワードポリシーの設定

Cisco ISE では、セキュリティ向上のために管理者アカウントにパスワードポリシーを作成することもできます。必要な管理者認証がパスワードベースか、クライアント証明書ベースかを定義できます。ここで定義したパスワードポリシーは、Cisco ISE のすべての管理者アカウントに適用されます。



(注) Cisco ISE では、管理者パスワードでの UTF-8 文字の使用はサポートされていません。

始める前に

- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。
- 自動フェールオーバー設定が展開でイネーブルになっている場合はオフにします。認証方式を変更すると、アプリケーション サーバプロセスが再起動されます。これらのサービスが再起動されるまで遅延が発生する場合があります。このサービスの再起動の遅延により、セカンダリ管理ノードの自動フェールオーバーが開始される場合があります。

ステップ 1 [管理 (Administration)] > [システム (System)] > [管理者アクセス (Admin Access)] > [認証 (Authentication)] を選択します。

ステップ 2 次の認証方式のいずれかを選択します。

- パスワードベース：管理者ログインで標準のユーザ ID およびパスワード クレデンシャルを使用する場合は、[パスワードベース (Password Based)] オプションを選択し、[内部 (Internal)] または [外部 (External)] のいずれかの認証タイプを指定します。
- (注) LDAP などの外部 ID ストアを設定しており、それを認証ソースとして使用して管理者ユーザにアクセス権を付与する場合は、その ID ソースを [ID ソース (Identity Source)] リストボックスから選択する必要があります。

- [クライアント証明書ベース (Client Certificate Based)] : 証明書ベースのポリシーを指定する場合は、[クライアント証明書ベース (Client Certificate Based)] オプションを選択し、既存の証明書認証プロファイルを選択します。

ステップ 3 [パスワードポリシー (Password Policy)] タブをクリックし、値を入力します。

ステップ 4 [保存 (Save)] をクリックして、管理者パスワードポリシーを保存します。

(注) 外部 ID ストアを使用してログイン時に管理者を認証する場合は、管理者プロファイルに適用されるパスワードポリシーにこの設定値が設定されている場合でも、外部 ID ストアが依然として管理者のユーザ名とパスワードを認証することに留意してください。

関連トピック

[管理者アクセスの設定](#) (136 ページ)

[管理者パスワードポリシーの設定](#) (1175 ページ)

[管理者アカウントのアカウント無効化ポリシーの設定](#) (139 ページ)

管理者アカウントのアカウント無効化ポリシーの設定

Cisco ISE では、設定した連続日数の間に管理者アカウントが認証されなかった場合は、管理者アカウントを無効にすることができます。

ステップ 1 [管理 (Administration)] > [システム (System)] > [管理者アクセス (Admin Access)] > [認証 (Authentication)] > [アカウント無効化ポリシー (Account Disable Policy)] の順に選択します。

ステップ 2 [非アクティブになってから n 日後にアカウントを無効にする (Disable account after n days of inactivity)] チェックボックスをオンにして、日数を入力します。

このオプションでは、管理者アカウントが連続する日数非アクティブだった場合に管理者アカウントを無効にすることができます。ただし、[管理 (Administration)] > [システム (System)] > [管理者アクセス (Admin Access)] > [管理者 (Administrators)] > [管理ユーザ (Admin Users)] の [非アクティブ アカウントを無効化しない (Inactive Account Never Disabled)] オプションを使用して、このアカウント無効化ポリシーから個々の管理者アカウントを除外することができます。

ステップ 3 [保存 (Save)] をクリックして、管理者のグローバルアカウント無効化ポリシーを設定します。

管理者のセッションタイムアウトの設定

Cisco ISE を使用すると、管理 GUI セッションが非アクティブであっても依然として接続状態である時間を決定できます。分単位の時間を指定することができ、その時間が経過すると Cisco ISE は管理者をログアウトします。セッションのタイムアウト後、管理者は、Cisco ISE 管理者ポータルにアクセスするには再びログインする必要があります。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

-
- ステップ 1** [管理 (Administration)] > [システム (System)] > [管理者アクセス (Admin Access)] > [設定 (Settings)] > [セッション (Session)] > [セッションのタイムアウト (Session Timeout)] を選択します。
- ステップ 2** アクティビティがない場合に管理者をログアウトするまでに Cisco ISE が待機する時間 (分) を入力します。デフォルト値は 60 分です。有効な範囲は 6 ~ 100 分です。
- ステップ 3** [保存 (Save)] をクリックします。
-

関連トピック

[管理者アクセスの設定](#) (136 ページ)

アクティブな管理セッションの終了

Cisco ISE では、すべてのアクティブな管理セッションが表示され、そこからセッションを選択し、必要が生じた場合はいつでも終了できます。同時管理 GUI セッションの最大数は 20 です。GUI セッションの最大数に達した場合、スーパー管理者グループに属する管理者がログインして一部のセッションを終了できます。

始める前に

次のタスクを実行するには、スーパー管理者である必要があります。

-
- ステップ 1** [管理 (Administration)] > [システム (System)] > [管理者アクセス (Admin Access)] > [設定 (Settings)] > [セッション (Session)] > [セッション情報 (Session Info)] を選択します。
- ステップ 2** 終了するセッション ID の隣にあるチェックボックスをオンにし、[無効化 (Invalidate)] をクリックします。
-

管理者の名前の変更

Cisco ISE では GUI からユーザ名を変更できます。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

-
- ステップ 1** 管理者ポータルにログインします。
- ステップ 2** Cisco ISE UI の右上にリンクとして表示されるユーザ名をクリックします。
- ステップ 3** 表示される [管理者ユーザ (Admin User)] ページに新しいユーザ名を入力します。
- ステップ 4** 変更するアカウントに関するその他の詳細を編集します。
-

ステップ 5 [保存 (Save)] をクリックします。

外部 ID ストアを使用した Cisco ISE への管理アクセス

Cisco ISE では、Active Directory、LDAP、RSA SecureID などの外部 ID ストアを介して管理者を認証できます。外部 ID ストアを介した認証の提供に使用できる次の 2 つのモデルがあります。

- 外部認証および許可：管理者に関してローカル Cisco ISE データベースで指定されたクレデンシアルはなく、許可は、外部 ID ストア グループ メンバーシップのみに基づきます。このモデルは、Active Directory および LDAP 認証で使用されます。
- 外部認証および内部許可：管理者の認証クレデンシアルは外部 ID ソースから取得され、許可および管理者ロール割り当てはローカル Cisco ISE データベースを使用して行われます。このモデルは、RSA SecurID 認証で使用されます。この方法では、外部 ID ストアとローカル Cisco ISE データベースの両方で同じユーザ名を設定する必要があります。

認証プロセス時、Cisco ISE は、外部 ID ストアとの通信が確立されなかった場合や失敗した場合はフォールバックし、内部 ID データベースから認証の実行を試行するように設計されています。また、外部認証が設定されている管理者には、ブラウザを起動してログインセッションを開始すると必ず、ログイン ダイアログの [ID ストア (Identity Store)] ドロップダウン セレクタから [内部 (Internal)] を選択して Cisco ISE ローカル データベースを介した認証を要求するオプションが依然として表示されます。



(注) 外部管理者認証を提供する方法は、管理者ポータルを介してのみ設定できます。Cisco ISE コマンドライン インターフェイス (CLI) では、これらの機能は設定されません。

ネットワークに既存の外部 ID ストアがまだない場合は、必要な外部 ID ストアをインストールし、これらの ID ストアにアクセスするように Cisco ISE が設定されていることを確認します。

外部認証および許可

デフォルトでは、Cisco ISE によって内部管理者認証が提供されます。外部認証を設定するには、外部 ID ストアで定義している外部管理者アカウントのパスワードポリシーを作成する必要があります。次に、結果的に外部管理者 RBAC ポリシーの一部となるこのポリシーを外部管理者グループに適用できます。

ネットワークでは、外部 ID ストア経由の認証を提供するほかに、Common Access Card (CAC) 認証デバイスを使用する必要もある場合があります。

外部認証を設定するには、次の手順を実行する必要があります。

- 外部 ID ストアを使用してパスワードベースの認証を設定します。
- 外部管理者グループを作成します。

- 外部管理者グループ用のメニュー アクセスとデータ アクセスの権限を設定します。
- 外部管理者認証の RBAC ポリシーを作成します。

外部認証のプロセスフロー

管理者がログインすると、ログインセッションはそのプロセスにおいて次の手順で処理されます。

1. 管理者が RSA SecurID チャレンジを送信します。
2. RSA SecurID は、チャレンジ応答を返します。
3. 管理者は、ユーザ ID とパスワードを入力する場合と同様に、ユーザ名および RSA SecurID チャレンジ応答を Cisco ISE ログイン ダイアログに入力します。
4. 管理者は、指定した ID ストアが外部 RSA SecurID リソースであることを確認します。
5. 管理者は、[ログイン (Login)] をクリックします。

ログイン時、管理者には、RBAC ポリシーで指定されたメニュー アクセス項目とデータ アクセス項目のみが表示されます。

外部 ID ストアを使用したパスワードベースの認証の設定

最初に、Active Directory や LDAP などの外部 ID ストアを使用して認証を行う管理者のためのパスワードベースの認証を設定する必要があります。

ステップ 1 [管理 (Administration)] > [システム (System)] > [管理者アクセス (Admin Access)] > [認証 (Authentication)] を選択します。

ステップ 2 [認証方式 (Authentication Method)] タブで、[パスワードベース (Password Based)] を選択し、すでに設定されている外部 ID ソースの 1 つを選択します。たとえば、作成した Active Directory インスタンスを選択します。

ステップ 3 外部 ID ストアを使用して認証を行う管理者のためのその他の特定のパスワードポリシーを設定します。

ステップ 4 [保存 (Save)] をクリックします。

関連トピック

[外部 ID ストアを使用した Cisco ISE への管理アクセス](#) (141 ページ)

[外部認証および許可](#) (141 ページ)

[外部認証のプロセスフロー](#) (142 ページ)

外部管理者グループの作成

外部 Active Directory または LDAP 管理者グループを作成する必要があります。これにより、Cisco ISE は外部 Active Directory または LDAP ID ストアで定義されているユーザ名を使用して、ログイン時に入力した管理者ユーザ名とパスワードを検証します。

Cisco ISE は、外部リソースから Active Directory または LDAP グループ情報をインポートし、それをディクショナリ属性として保存します。次に、この属性を、外部管理者認証方式用の RBAC ポリシーを設定するときのポリシー要素の 1 つとして指定できます。

ステップ 1 [管理 (Administration)] > [システム (System)] > [管理者アクセス (Admin Access)] > [管理者 (Administrators)] > [管理者グループ (Admin Groups)] を選択します。

ステップ 2 [追加 (Add)] をクリックします。

ステップ 3 名前とオプションの説明を入力します。

ステップ 4 [外部 (External)] オプション ボタンを選択します。

Active Directory ドメインに接続し、参加している場合は、Active Directory インスタンス名が [名前 (Name)] フィールドに表示されます。

ステップ 5 [外部グループ (External Groups)] ドロップダウン リスト ボックスから、この外部管理者グループにマッピングする Active Directory グループを選択します。

追加の Active Directory グループをこの外部管理者グループにマッピングするために「+」記号をクリックします。

ステップ 6 [保存 (Save)] をクリックします。

関連トピック

[Cisco ISE 管理者グループ](#) (119 ページ)

外部管理者グループのメニュー アクセス権限とデータ アクセス権限の設定

外部管理者グループに割り当てることができるメニュー アクセス権限とデータ アクセス権限を設定する必要があります。

ステップ 1 [管理 (Administration)] > [システム (System)] > [管理者アクセス (Admin Access)] > [権限 (Permissions)] を選択します。

ステップ 2 次のいずれかをクリックします。

- [メニューアクセス (Menu Access)] : 外部管理者グループに属するすべての管理者に、メニューまたはサブメニューレベルでの権限を付与することができます。メニューアクセス権限によって、アクセスできるサブメニューまたはメニューが決定されます。
- [データアクセス (Data Access)] : 外部管理者グループに属するすべての管理者に、データ レベルでの権限を付与することができます。データアクセス権限によって、アクセスできるデータが決定されます。

ステップ 3 外部管理者グループのメニュー アクセス権限とデータ アクセス権限を指定します。

ステップ 4 [保存 (Save)] をクリックします。

外部管理者認証の RBAC ポリシーの作成

外部 ID ストアを使用して管理者を認証するように Cisco ISE を設定し、同時にカスタム メニュー アクセス権限とデータ アクセス権限を指定するには、新しい RBAC ポリシーを設定する必要があります。このポリシーには、認証用の外部管理者グループ、および外部認証と許可を管理するための Cisco ISE メニュー アクセス権限とデータ アクセス権限が存在している必要があります。



(注) これらの新しい外部属性を指定するように既存（システムプリセット）の RBAC ポリシーを変更することはできません。「テンプレート」として使用する必要がある既存のポリシーがある場合は、そのポリシーを複製し、名前を変更してから、新しい属性を割り当てます。

ステップ 1 [管理 (Administration)] > [システム (System)] > [管理者アクセス (Admin Access)] > [許可 (Authorization)] > [ポリシー (Policy)] を選択します。

ステップ 2 ルール名、外部管理者グループ、および権限を指定します。

適切な外部管理者グループが正しい管理者ユーザ ID に割り当てられている必要があることに注意してください。問題の管理者が正しい外部管理者グループに関連付けられていることを確認します。

ステップ 3 [保存 (Save)] をクリックします。

管理者としてログインした場合、Cisco ISE RBAC ポリシーが管理者 ID を認証できないと、Cisco ISE では、「認証されていない」ことを示すメッセージが表示され、管理者ポータルにアクセスできません。

関連トピック

[RBAC ポリシー](#) (130 ページ)

内部許可を伴う認証に対する外部 ID ストアを使用した管理アクセスの設定

この方法では、外部 ID ストアとローカル Cisco ISE データベースの両方で同じユーザ名を設定する必要があります。外部 RSA SecurID ID ストアを使用して管理者認証を提供するように Cisco ISE を設定している場合、管理者のクレデンシャル認証が RSA ID ストアによって実行されます。ただし、許可（ポリシー アプリケーション）は、依然として Cisco ISE 内部データベースに従って行われます。また、外部認証と許可とは異なる、留意する必要がある次の 2 つの重要な要素があります。

- 管理者の特定の外部管理者グループを指定する必要はありません。
- 外部 ID ストアとローカル Cisco ISE データベースの両方で同じユーザ名を設定する必要があります。

ステップ 1 [管理 (Administration)] > [システム (System)] > [管理者アクセス (Admin Access)] > [管理者 (Administrators)] > [管理者ユーザ (Admin Users)] を選択します。

ステップ 2 外部 RSA ID ストアの管理者ユーザ名が Cisco ISE にも存在することを確認します。[パスワード (Password)] の下の [外部 (External)] オプションをクリックします。

(注) 外部管理者ユーザ ID のパスワードを指定する必要はなく、特別に設定されている外部管理者グループを関連付けられている RBAC ポリシーに適用する必要もありません。

ステップ 3 [保存 (Save)] をクリックします。



第 7 章

Cisco ISE ライセンス

この章では、Cisco ISE で使用できるライセンスのメカニズムとスキーム、およびライセンスの追加やアップグレードを行う方法について説明します。

- [Cisco ISE ライセンス \(147 ページ\)](#)
- [従来のライセンス ファイルの管理 \(148 ページ\)](#)

Cisco ISE ライセンス

Cisco ISE ライセンスでは、ライセンスを管理する次の 2 つのオプションがあります。

- **スマート ライセンス**：単一のトークン登録で ISE ソフトウェア ライセンスとエンドポイント ライセンスの消費を簡単かつ効率的にモニタします。購入したライセンスは、Cisco Smart Software Manager (CSSM) と呼ばれる集中型データベースに保持されます。スマート ライセンスの詳細については、[Cisco ISE スマート ライセンス \(761 ページ\)](#) を参照してください。
- **従来のライセンス**：実際のニーズに基づいて個々のライセンスを購入およびインポートした後、アプリケーション機能とアクセス（たとえば Cisco ISE のネットワーク リソースを使用できる同時接続可能なエンドポイント数）を管理します。従来のライセンスの詳細については、[従来のライセンス ファイルの管理 \(148 ページ\)](#) を参照してください。

お客様が最大限に節約できるように、Cisco ISE のライセンスは、従来のライセンスおよびスマート ライセンスのオプションの両方に対し、Base、Plus、Apex、Device Administration のようなさまざまなパッケージで提供されます。従来の Cisco ライセンス モデルの詳細は、[Cisco ISE ライセンス モデル \(149 ページ\)](#) を参照してください。

ISE ボックスをインストールまたはアップグレードすると、従来のライセンスはデフォルトで使用中になり、すべてのライセンス コンポーネントは 90 日間の試用期間の間アクティブになります。スマートライセンスに切り替えると、トークンを登録する前は、この評価期間は、スマートライセンスについてはアクティブなままで、評価期間には、評価期間の一部として ISE ライセンスが含まれます。評価期間中、CSSM に使用は報告されません。

次の場合、インストールされたライセンス（従来のライセンス）またはライセンス契約（スマート ライセンス）は更新する必要があります。

- トライアル期間が終了し、まだライセンスをインストールしていない、または登録されていない。
- ライセンスの有効期限が切れている。
- エンドポイントの使用がライセンス契約を超える場合。

ISE は、ライセンスの有効期限日、または使用の問題の 90 日、60 日、および 30 日前に通知します。システムがライセンスに準拠しなくなった場合、管理者は Plus と Apex の機能を編集/設定できなくなります。画面上部にある [ライセンス警告 (License Warning)] アイコンを使用して、ライセンスの詳細情報を表示、追跡できます。

1 つのライセンス パッケージをより複雑な別のパッケージにアップグレードすると、アップグレード前に古いパッケージで使用可能だったすべての機能を Cisco ISE で引き続き使用できます。以前に行った設定を再設定する必要はありません。

ISE コミュニティ リソース

Cisco Identity Services Engine Ordering Guide

評価版ライセンスを入手する方法については、「[How to Get ISE Evaluation Licenses](#)」を参照してください。

従来のライセンス ファイルの管理

90 日間の評価期間の終了後に Cisco ISE サービスの使用を継続し、ネットワークで 100 を超える数の同時エンドポイントをサポートするには、システム上の現在のユーザの数の Base ライセンスを取得して登録する必要があります。追加機能が必要な場合は、該当の機能を有効にする Plus か Apex、またはその両方のライセンスが必要です。

ライセンスはプライマリ管理ノード (PAN) にアップロードされ、クラスタ内の他の Cisco ISE ノードにその情報がコピーされます。ライセンスは管理ノードによって一元的に管理され、他のノードに別個のライセンスは必要ありません。ハイアベイラビリティペアで 2 つの管理ノードを展開している場合、それらのいずれにも同じライセンス機能があることを確実にする必要があります。両方の UDI でライセンスを生成してから、それぞれのノードがスタンドアロンまたはプライマリ状態になっているときに、ライセンスを追加します。

Cisco ISE ソフトウェアをインストールし、最初にそのアプライアンスを PAN として設定したら、Cisco ISE のライセンスを取得して PAN に登録する必要があります。プライマリおよびセカンダリ管理ノードのハードウェア UDI を使用して、PAN にすべてのライセンスを登録します。これにより、その展開に登録されているすべてのライセンスが PAN で集中管理されるようになります。



(注) ノードが PAN から登録解除されると、スタンドアロン ノードになり、そのライセンスは評価ライセンスにリセットされます。

ここでは、従来のISEライセンスの登録、再ホスティング、更新、移行、アップグレード、および削除を行う方法について説明します。

Cisco ISE ライセンス モデル

Cisco ISE ライセンス モデルでは、企業のニーズに適したライセンスを購入できます。従来のライセンスを使用するときは、すべての個別ライセンスをインポートし、ISE から個別に管理し続けます。スマートライセンスを使用するときは、購入したさまざまなエンドポイントのライセンスに関するすべての情報を含むシスコの一元化されたアカウントを管理します。

以下のライセンス オプションが用意されています。

- ISE Base のみ
- ISE Base および Plus
- ISE Base および Apex
- ISE Base および Device Administration
- ISE Base、Plus、Apex、および Device Administration
- ISE Base、Plus、Apex および AnyConnect Apex

Plus ライセンス セッションの数は、展開における Base ライセンス セッションの数以下となります。同じことが Apex ライセンス セッションにも適用されます。Apex ライセンスと Plus ライセンスとの間にこのような数の制限はなく、これらのライセンスを個別にインストールできます。Cisco ISE ライセンスはアクティブなネットワーク接続を持つ同時エンドポイントの数に基づいて計算され、AnyConnect Apex ライセンスは1 ユーザごとに計算されます。AnyConnect Apex ライセンスの数は、Cisco ISE Base ライセンスの総数以下である必要はありません。



(注) Plus ライセンスに含まれるプロファイリングなどのサービスは、展開全体で頻繁に使用されます。展開に Plus ライセンスを追加する場合は、Plus ライセンスの数を Base ライセンスの数と等しくすることを推奨します。ただし、Plus ライセンスのサービスを展開全体で使用する必要がなくなることも考えられます。Cisco ISE で Plus ライセンスの数を Base ライセンスの数より少なくできるのはそのためです。

(従来のライセンスに対しては) Base、Plus、および Apex ライセンスをインストールすると同時に、(スマート ライセンスに対しては) Base、Plus、および Apex ライセンスを購入することをお勧めします。

- Base ライセンスは、Plus や Apex ライセンスで有効になるサービスを使用するためにも必要です。ただし、Apex ライセンスを使用するために Plus ライセンスが必要ということではなく、その逆もありません。これらのライセンスの機能は重複していません。
- Base または Mobility Upgrade ライセンスをインストールすると、Cisco ISE はその期間の残りの部分に対する別個のライセンスとしてデフォルトの評価ライセンスを使用し続けます。

- Mobility Upgrade ライセンスをインストールすると、Cisco ISE ではすべての有線、無線、および VPN サービスが有効になります。
- Base または Mobility ライセンスは、Device Administration ライセンスをインストールするときに必要です。
- Base ライセンスをインストールせずに、評価ライセンスを Plus ライセンスにアップグレードすることはできません。

表 4: Cisco ISE ライセンス パッケージ

ISE ライセンス パッケージ	永続/サブスクリプション（使用可能期間）	カバーされる ISE 機能	注記
基本	永続	<ul style="list-style-type: none"> • 基本的なネットワーク アクセス（AAA、IEEE-802.1X） • ゲスト サービス • リンク暗号化（MACSec） • TrustSec • ISE アプリケーションプログラミングインターフェイス 	ISE-PIC から Base ライセンスへのアップグレードの一環として使用できるパッシブ ID サービスには、シスコサブスクライバだけが使用可能な限定的な pxGrid 機能が含まれます。
プラス記号	サブスクリプション（1、3、または 5 年）	<ul style="list-style-type: none"> • 個人所有デバイス持ち込み（BYOD）：組み込み証明機関または外部証明機関のいずれかを消費する場合 • ロケーションサービスのための MSE 統合 • プロファイリングサービスとフィードサービス • 適応型ネットワーク制御（ANC） • Cisco pxGrid 	<p>Base のサービスは含まれません。Base ライセンスは Plus ライセンスをインストールするために必要です。</p> <p>BYOD フローでエンドポイントをオンボードすると、関連する BYOD 属性が使用されていなくても、アクティブなセッションで Plus サービスが使用されます。</p>

Apex	サブスクリプション (1、3、または 5 年)	<ul style="list-style-type: none"> サードパーティ モバイル デバイス管理 (MDM) 統合 ポスチャ コンプライアンス TC NAC 	<p>Base のサービスは含まれません。Base ライセンスは Apex ライセンスをインストールするために必要です。</p> <p>(注) 有線、ワイヤレス、および VPN 展開でユニファイド ポスチャ エージェントとして Cisco AnyConnect を使用する場合は、Cisco ISE Apex ライセンスに加えて Cisco AnyConnect Apex ユーザ ライセンスが必要です。</p>
モビリティ (Mobility)	サブスクリプション (1、3、または 5 年)	無線および VPN エンドポイント用の Base、Plus、および Apex の組み合わせ	Cisco 管理ノードで Base、Plus、および Apex ライセンスを共存させることはできません。
Mobility Upgrade	サブスクリプション (1、3、または 5 年)	Mobility ライセンスに対する有線サポートの提供	Mobility Upgrade ライセンスは既存の Mobility ライセンスが存在する場合にのみインストールできます。
Device Administration	永続	TACACS+	<p>Base または Mobility ライセンスは、Device Administration ライセンスをインストールするときに必要です。</p> <p>展開あたりの必要なライセンスは (複数ノードである場合も含め) 1 つだけです。</p>
ISE-PIC	永続	パッシブ ID サービス	ノードごとに 1 つのライセンス。各ライセンスでは、最大 3,000 の並列セッションをサポートしています。

ISE-PIC のアップグレード	永続	<p>このライセンスでは、次のオプションを使用できます。</p> <ul style="list-style-type: none"> • 追加の並列セッションの有効化 (300,000 まで) • 完全な ISE インスタンスへのアップグレード 	<p>ノードごとに 1 つのライセンス。各ライセンスでは、最大 300,000 の並列セッションをサポートしています。</p> <p>このライセンスをインストールすると、アップグレードされたノードが既存の ISE 展開に参加できます。あるいは、Base ライセンスをノードにインストールして PAN として機能させることもできます。</p> <p>Base ライセンスへのアップグレードの一環として使用できるパッシブ ID サービスには、シスコサブスクライバだけが使用可能な限定的な pxGrid 機能が含まれます。</p>
評価 (Evaluation)	一時 (90 日)	完全な Cisco ISE 機能が、100 台のエンドポイントに対して提供されます。	すべての Cisco ISE アプライアンスには、評価ライセンスが付属しています。

従来のライセンスの使用

従来のライセンスではシステムの同時ユーザ数に合わせてライセンスを購入します。Cisco ISE ユーザは、アクティブセッション中にライセンスを使用します（常に Base ライセンスか、Plus ライセンスと APex ライセンス（これらのライセンスで適用される機能を使用する場合））。セッションが終了すると、ライセンスは他のユーザが再利用できるように解放されます。



制約事項

Cisco ISE ライセンス アーキテクチャの使用ロジックは、許可ポリシーの構造に依存しています。Cisco ISE は、許可ルール内のディクショナリと属性を使用して、使用するライセンスを決定します。

Cisco ISE ライセンスは次のようにカウントされます。

- Base ライセンスは、アクティブセッションごとに使用されます。同じエンドポイントで、使用している機能に応じて、Plus および Apex ライセンスも使用します。



(注) TACACS+ セッションは、基本ライセンスを使用しませんが、RADIUS セッションは、基本ライセンスを使用します。

- エンドポイントは、Plus および APex ライセンスを使用する前に、Base ライセンスを使用します。
- エンドポイントは、APex ライセンスを使用する前に、Plus ライセンスを使用します。
- 1 Plus ライセンスは、ライセンス機能の組み合わせに対してエンドポイントごとに使用されます。同様に、1 Apex ライセンスは、その機能の組み合わせに対してエンドポイントごとに使用されます。
- ライセンスは、同時のアクティブ セッションに対してカウントされます。
- ライセンスは、エンドポイントのセッションが終了すると、すべての機能について解放されます。
- pxGrid は、ISE によって収集されたコンテキストを他の製品と共有するために使用されます。pxGrid 機能を有効にするには、Plus ライセンスが必要です。セッションのコンテキストが共有されている場合、セッション数の減少はありません。ただし、pxGrid を使用するには、ライセンスされた Plus セッションの数が、ライセンスされた Base セッションの数と等しくなければなりません。詳細については、『[Cisco Identity Services Engine Ordering Guide](#)』の「Cisco ISE Licenses and Services」の項を参照してください。
- 1 つの AnyConnect Apex ユーザ ライセンスは、ユーザが所有するデバイスの数に関係なく、またユーザにネットワークへのアクティブな接続があるかどうかにかかわらず、AnyConnect を使用する各ユーザによって使用されます。
- 既存の Base または Mobility ライセンスの上にデバイス管理ライセンスを追加して TACACS+ サービスを有効にすることができます。この機能はライセンスを使用しません。

サービスの中断を回避するために、Cisco ISE はライセンスの権限付与を超えたエンドポイントにサービスを提供し続けます。代わりに、Cisco ISE は RADIUS アカウンティング機能に依存して、ネットワーク上の同時エンドポイントを追跡し、前日のエンドポイントカウントがライセンス数を超えていた場合にアラームを生成します。ライセンス使用量は、[ライセンス (Licensing)] 画面の [ライセンス使用状況 (License Usage)] 領域で明確に確認できます。この領域の折れ線グラフには、使用量が許容されている数量を上回るライセンスが赤色で表示されます。

また、画面上部にある [ライセンス警告 (License Warning)] アイコンを使用して、ライセンスパッケージの詳細情報を確認、追跡できます。

ライセンスの使用の表示

[管理 (Administration)] > [システム (System)] > [ライセンシング (Licensing)] の順に選択して、ライセンスダッシュボードからシステムの現在のライセンスの使用を表示できます。使用状況は次の画像に示すように表示されます。

図 4: 従来のライセンスの使用



[ライセンスの使用状況 (License Usage)] エリアのライセンス消費グラフは、30 分ごとに更新されます。このウィンドウには、購入したライセンスの種類、システムで許可される同時ユーザの総数、およびサブスクリプションサービスの有効期限も表示されます。

複数の週にわたってシステムのライセンスの使用を確認する場合は、[長期間の使用 (Usage Over Time)] をクリックします。グラフの各バーは、1 週間に使用される最大ライセンス数を示します。

登録解除されたライセンスの使用

問題

ライセンスの使用は、エンドポイントが一致する許可ポリシーにおいて使用される属性に依存します。

システムに Base ライセンスのみが登録されているとします (90 日間の評価ライセンスは削除しました)。対応する基本的なメニュー項目と機能を表示および設定できます。

Apex ライセンスを必要とする機能 (例: Session:PostureStatus) を使用するための許可ポリシーを (誤って) 設定した場合、およびエンドポイントがこの許可ポリシーに一致した場合は、次のようになります。

- エンドポイントは、Apex ライセンスがシステムに登録されていないにもかかわらず、Apex ライセンスを使用します。
- ログインするたびに、このことに対する通知が表示されます。
- Cisco ISE は、通知とアラーム「許可を超えたライセンスの使用 (Exceeded license usage than allowed)」を示します (技術的に、これはシステムに登録済みの Apex ライセンスがないにもかかわらず、エンドポイントが Apex ライセンスを消費していると想定されます)。

考えられる原因

許可ポリシーの設定ミスが原因で、ライセンスのダッシュボードに、Cisco ISE がまだ購入および登録されていないライセンスを消費していることが示される場合があります。Plus および

Apex ライセンスを購入する前は、ISE ユーザ インターフェイスにライセンスが適用される機能が表示されません。ただし、これらのライセンスを購入した場合、ユーザ インターフェイスには、ライセンスの期限が切れた場合、またはエンドポイントの消費を超えた後も、引き続き機能が表示されます。そのため、有効なライセンスがない場合でも、これらを設定できます。

ソリューション

[ポリシー (Policy)] > [認証 (Authorization)] を選択し、登録済みライセンスがない機能を使用している許可ルールを特定し、そのルールを再設定します。

ライセンス ファイルの管理

ここでは、ISE ライセンスの登録、再ホスティング、更新、移行、アップグレード、および削除を行う方法について説明します。

- [ライセンスの登録 \(155 ページ\)](#)
- [ライセンスの再ホスト \(156 ページ\)](#)
- [ライセンスの更新 \(156 ページ\)](#)
- [ライセンスの移行およびアップグレード \(156 ページ\)](#)
- [ライセンスの削除 \(157 ページ\)](#)

ライセンスの登録

始める前に

インストールに必要なライセンスの種類と同時ユーザ数、および購入して費用効率を最大化できるさまざまなパッケージについて、シスコ パートナー/アカウント チームに問い合わせてください。

-
- ステップ 1** シスコの Web サイト (www.cisco.com) の注文システム (Cisco Commerce Workspace (CCW)) から、必要なライセンスを注文します。
- 約 1 時間後、製品認証キー (PAK) を含む電子メール確認が送信されます。
- ステップ 2** Cisco ISE の管理者ポータルから、[管理 (Administration)] [システム (System)] [ライセンシング (Licensing)] を選択します。[ライセンスの詳細 (Licensing Details)] セクションのノード情報 (製品 ID (PID)、バージョン ID (VID)、およびシリアル番号 (SN)) を書き留めます。
- ステップ 3** www.cisco.com/go/licensing に移動し、要求されたら、受け取ったライセンスの PAK、ノード情報、および会社に関する詳細を入力します。
- 1 日後に、シスコからライセンス ファイルが送信されます。
- ステップ 4** システムの既知の場所にこのライセンス ファイルを保存します。

- ステップ 5** Cisco ISE の管理者ポータルから、**[管理 (Administration)] > [システム (System)] > [ライセンシング (Licensing)]** を選択します。[ライセンス ファイル (License Files)] セクションで、[ライセンスのインポート (Import License)] ボタンをクリックします。
- ステップ 6** [Choose File (ファイルの選択)] をクリックし、システムで以前に保存したライセンス ファイルを選択します。
- ステップ 7** [インポート (Import)] をクリックします。

新しいライセンスがシステムにインストールされました。

次のタスク

ライセンシング ダッシュボード (**[管理 (Administration)] > [システム (System)] > [ライセンシング (Licensing)]**) を選択し、新たに入力したライセンスが正しい詳細とともに表示されることを確認します。

ライセンスの再ホスト

再ホストとは、1 つの Cisco ISE ノードから別のノードにライセンスを移動することを意味します。ライセンシング ポータルから、移動するライセンスの PAK を選択し、再ホストの手順に従います。1 日後、新しい PAK が電子メールで送信されます。この新しい PAK を新しいノードに登録し、元の Cisco ISE ノードから古いライセンスを削除します。

ライセンスの更新

Plus ライセンスや Apex ライセンスなどのサブスクリプション ライセンスの期限は、1 年間、3 年間、または 5 年間です。Cisco ISE は、ライセンスの有効期限日が近づくとアラームを送信し、ライセンスが期限切れになると再度アラームを送信します。

ライセンスの有効期限が過ぎたら、更新する必要があります。このプロセスは、シスコパートナーまたはアカウント チームによってのみ実行されます。

ライセンスの移行およびアップグレード

シスコのライセンス ポリシーでは、以前の Cisco ISE バージョンからの移行、無線および VPN 専用から有線を含む展開へのアップグレード、および同時ユーザと機能の追加がサポートされています。また、ライセンスバンドルを購入して、運用コストを最小化することもできます。これらのシナリオは、すべて [ライセンス サイト](#) で説明されています。詳細については、シスコパートナーまたはアカウント チームにお問い合わせください。



(注) Cisco ISE バージョン 1.3 または 1.4 からのアップグレード後、デフォルトの評価ライセンスは、アップグレード前にシステムに存在していた場合にのみ表示されます。



- (注) Mobility/Mobility Upgrade ライセンスは、エンドポイントの対応する番号とともにユーザ インターフェイスに Base/Plus/Apex として常に表示されます。

Cisco ISE ノードで次の内容をサポートしている必要がある場合：

- 所有しているライセンスを上回る数の大量の同時ユーザ
- 有線 (LAN) アクセス (システムに Mobility ライセンスしかない)

そのノードのライセンスをアップグレードする必要があります。このプロセスは、シスコパートナーまたはアカウント チームによってのみ実行されます。

ライセンスの削除

始める前に

ライセンスを削除する前に、次の点に注意してください。

- Mobility ライセンスの後に Mobility アップグレード ライセンスをインストールした場合は、Mobility アップグレード ライセンスを削除してから基盤となる Mobility ライセンスを削除する必要があります。
- 組み合わされたライセンスをインストールした場合は、Base、Plus および Apex パッケージの関連インストールがすべて削除されます。

ステップ 1 [管理 (Administration)] > [システム (System)] > [ライセンシング (Licensing)] を選択します。

ステップ 2 [ライセンスファイル (License Files)] セクションで、関連するファイル名の隣にあるチェックボックスをクリックし、[ライセンスの削除 (Delete License)] をクリックします。

ステップ 3 [OK] をクリックします。



第 8 章

証明書の管理

- [Cisco ISE での証明書の管理 \(159 ページ\)](#)
- [Cisco ISE CA サービス \(191 ページ\)](#)
- [OCSP サービス \(224 ページ\)](#)

Cisco ISE での証明書の管理

証明書は、個人、サーバ、会社、またはその他のエンティティを識別し、そのエンティティを公開キーに関連付ける電子文書です。自己署名証明書は、独自の作成者によって署名されます。証明書は、自己署名したり、外部の認証局（CA）がデジタルで署名したりできます。CA 署名付きデジタル証明書は、業界標準であり、よりセキュアです。

証明書は、ネットワークに対するセキュアなアクセスを提供するために使用されます。Cisco ISE は、ノード間通信、および syslog サーバ、フィード サーバ、すべてのエンドユーザ ポータル（ゲスト、スポンサーおよびパーソナル デバイス ポータル）などの外部サーバとの通信に証明書を使用します。証明書は、エンドポイントに対して Cisco ISE ノードを識別し、そのエンドポイントと Cisco ISE ノード間の通信を保護します。

展開内のすべてのノードの証明書を管理するには、管理者ポータルを使用できます。

Cisco ISE によるセキュアなアクセスの提供を可能にする証明書

Cisco Identity Services Engine (ISE) は、公開キー インフラストラクチャ (PKI) に依存して、エンドポイントおよび管理者の両方とのセキュアな通信、そしてマルチノード展開内の複数の Cisco ISE ノード間のセキュアな通信を実現しています。PKI は X.509 デジタル証明書に依存して、メッセージの暗号化と復号化のための公開キーの転送、およびユーザとデバイスを表す他の証明書の信頼性の検証を行います。Cisco ISE には、次の 2 つの X.509 証明書のカテゴリを管理する、管理者ポータルが用意されています。

- システム証明書：これらはクライアント アプリケーションに対して Cisco ISE ノードを識別するサーバ証明書です。各 Cisco ISE ノードには独自のシステム証明書があり、それぞれの証明書は対応する秘密キーとともにノードに格納されています。

- 信頼できる証明書：この証明書は、ユーザおよびデバイスから受信した公開キーの信頼を確立するために使用される認証局（CA）証明書です。信頼できる証明書ストアには、Simple Certificate Enrollment Protocol（SCEP）から配信された証明書も含まれます。これにより、モバイルデバイスを企業ネットワークに登録できるようになります。信頼できる証明書ストア内の証明書はプライマリ管理ノード（PAN）で管理され、Cisco ISE 展開内の他のすべてのノードに自動的に複製されます。

分散展開では、証明書を PAN の証明書信頼リスト（CTL）のみにインポートする必要があります。この証明書はセカンダリ ノードに複製されます。

一般に、Cisco ISE での証明書認証が、証明書による認証機能のわずかな違いの影響を受けないようにするために、ネットワークに展開されているすべての Cisco ISE ノードには小文字のホスト名を使用してください。

証明書の使用

Cisco ISE に証明書を追加またはインポートする場合、証明書の使用目的を指定する必要があります。

- 管理者：ノード間通信および管理者ポータル認証
- EAP：TLS ベースの EAP 認証
- RADIUS DTLS：RADIUS DTLS サーバ認証用
- ポータル：すべての Cisco ISE エンドユーザ ポータルとの通信
- xGrid：pxGrid コントローラとの通信

管理者ポータル（管理者）、pxGrid コントローラ（xGrid）との通信および TLS ベースの EAP 認証（EAP）に、各ノードから異なる証明書を関連付けることができます。ただし、これらの各目的に各ノードから関連付けることができる証明書は 1 つのみです。

Web ポータル要求を処理できる展開に複数のポリシー サービス ノード（PSN）がある場合、Cisco ISE には一意の ID が必要です。この ID で、ポータルの通信に使用する必要がある証明書を識別します。ポータルでの使用に指定された証明書を追加またはインポートする場合、証明書グループタグを定義して、それを展開内の各ノードの対応する証明書に関連付ける必要があります。この証明書グループタグを対応するエンドユーザポータル（ゲスト、スポンサー、およびパーソナルデバイス ポータル）に関連付ける必要があります。この証明書グループタグは一意の ID で、Cisco ISE が各ポータルと通信の際に使用する必要がある証明書を識別する場合に役立ちます。ポータルごとに各ノードから 1 つの証明書を指定できます。



(注) EAP-TLS クライアント証明書では、以下の暗号に対し、KeyUsage=Key Agreement および ExtendedKeyUsage=Client Authentication が必要です。

- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-ECDSA-AES256-SHA384

EAP-TLS クライアント証明書では、以下の暗号に対し、KeyUsage=Key Encipherment および ExtendedKeyUsage=Client Authentication が必要です。

- AES256-SHA256
- AES128-SHA256
- AES256-SHA
- AES128-SHA
- DHE-RSA-AES128-SHA
- DHE-RSA-AES256-SHA
- DHE-RSA-AES128-SHA256
- DHE-RSA-AES256-SHA256
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-SHA384
- ECDHE-RSA-AES128-SHA256
- ECDHE-RSA-AES256-SHA
- ECDHE-RSA-AES128-SHA
- EDH-RSA-DES-CBC3-SHA
- DES-CBC3-SHA
- RC4-SHA
- RC4-MD5

Cisco ISE での証明書的一致

展開内で Cisco ISE ノードをセットアップすると、2つのノードが相互に通信します。システムは各 ISE ノードの FQDN を調べ、FQDN が一致することを確認します（たとえば `ise1.cisco.com` と `ise2.cisco.com`、またはワイルドカード証明書を使用している場合は `*.cisco.com`）。また、外

部マシンから ISE サーバに証明書が提示される場合、認証のために提示される外部証明書が、ISE サーバの証明書と照合されます。2 つの証明書が一致すると、認証は成功します。

では、ノード間（2 ノードの場合）、またはと pxGrid の間で照合が実行されます。

Cisco ISE は、サブジェクト名の一致を次のようにして確認します。

1. Cisco ISE により証明書のサブジェクト代替名（SAN）の拡張が確認されます。SAN に 1 つ以上の DNS 名が含まれている場合は、それらの DNS 名の 1 つが Cisco ISE ノードの FQDN に一致している必要があります。ワイルドカード証明書が使用されている場合、ワイルドカードドメイン名は Cisco ISE ノードの FQDN ドメインに一致している必要があります。
2. SAN に DNS 名が存在しない場合、または SAN 全体が欠落している場合は、証明書の [サブジェクト（Subject）] フィールドの一般名（CN）または証明書の [サブジェクト（Subject）] フィールドのワイルドカードドメインが、ノードの FQDN に一致している必要があります。
3. 一致しない場合、証明書は拒否されます。



（注） Cisco ISE にインポートされる X.509 証明書は、Privacy Enhanced Mail（PEM）または Distinguished Encoding Rules（DER）形式である必要があります。証明書チェーン（システム証明書、およびその証明書に署名する一連の信頼された証明書）が含まれたファイルはインポートすることができますが、特定の制限の対象となります。

X.509 証明書の有効性

X.509 証明書が有効なのは、指定された特定の日付までのみです。システム証明書が期限切れになった場合、その証明書に依存する Cisco ISE 機能が影響を受けます。Cisco ISE は、有効期限が 90 日以内になると、システム証明書の有効期間の残りについて通知します。この通知は、いくつかの方法で表示されます。

- 配色された有効期限の状態アイコンが、[システム証明書（System Certificates）] ページに表示されます。
- 期限切れメッセージが Cisco ISE システム診断レポートに表示されます。
- 有効期限のアラームは、有効期限の 90 日前、60 日前に生成され、有効期限前の最後の 30 日間には毎日生成されます。

失効した証明書が自己署名証明書の場合は、この証明書を編集して有効期限を延長できます。CA 署名付き証明書の場合は、CA から新しい証明書を取得するのに十分な期間を確保する必要があります。

Cisco ISE での PKI の有効化

公開キーインフラストラクチャ（PKI）は、セキュアな通信を可能にし、デジタル署名を使用してユーザの ID を確認する暗号化技術です。

ステップ 1 EAP-TLS などの TLS 対応認証プロトコル、管理者ポータル認証、Cisco ISE Web ポータルにアクセスするブラウザおよび REST クライアント、および pxGrid コントローラ向けのシステム証明書を各展開ノードで確立します。

デフォルトで、Cisco ISE ノードには EAP 認証、管理者用ポータル、ポータル、pxGrid コントローラに使用される自己署名証明書があらかじめインストールされています。一般的な企業環境では、この証明書は、信頼された CA によって署名されたサーバ証明書に置き換えられます。

ステップ 2 信頼できる証明書ストアに、ユーザとの信頼を確立するために必要な CA 証明書と、Cisco ISE に提示されるデバイス証明書を配置します。

証明書チェーンがルート CA 証明書と 1 つ以上の中間 CA 証明書で構成される場合は、ユーザまたはデバイスの証明書の信頼性を検証するために、信頼できる証明書ストアにそのチェーン全体をインポートする必要があります。

ノード間の通信では、Cisco ISE 展開内の各ノードに属する管理者システム証明書を検証するために必要な信頼された証明書を、信頼できる証明書ストアに配置する必要があります。ノード間の通信にデフォルトの自己署名証明書を使用する場合は、各 Cisco ISE ノードの [システム証明書 (System Certificates)] ページからこの証明書をエクスポートし、信頼できる証明書ストアにインポートする必要があります。自己署名証明書を CA 署名証明書で置き換える場合に必要なのは、適切なルート CA 証明書および中間 CA 証明書を信頼できる証明書ストアに配置することだけです。この手順を完了するまでは、ノードを Cisco ISE 展開に登録できないことに注意してください。

展開内でクライアントと PSN の間のセキュアな通信に自己署名証明書を使用する場合、BYOD ユーザがある場所から別の場所に移動すると、EAP-TLS ユーザ認証は失敗します。一部の PSN 間で提供される必要があるこのような認証要求の場合、外部で署名された CA 証明書を使用してクライアントと PSN の間の通信を保護するか、または外部の CA によって署名されたワイルドカード証明書を使用する必要があります。

パブリック署名証明書を取得する場合、または Cisco ISE 展開が FIPS モードで動作する場合は、すべてのシステム証明書および信頼できる証明書が FIPS 準拠であることを確認する必要があります。つまり、各証明書のキー サイズが 2048 バイト以上であり、SHA-1 または SHA-256 暗号化を使用する必要があります。

(注) スタンドアロンの Cisco ISE または PAN からバックアップを取得した後に、展開内の 1 つ以上のノードの証明書設定を変更する場合は、データを復元するために別のバックアップを取得する必要があります。そうしないで古いバックアップを使用してデータを復元すると、ノード間の通信が失敗する可能性があります。

関連トピック

[Cisco ISE ノード間通信の信頼できる証明書のインストール](#) (184 ページ)

[ポータルで使用する証明書のセットアップ](#) (184 ページ)

ワイルドカード証明書

ワイルドカード証明書はワイルドカード表記（ドメイン名の前にアスタリスクとピリオドの形式）を使用し、組織の複数のホスト間で証明書を共有できるようにします。たとえば、証明書サブジェクトの CN 値は `aaa.ise.local` などの汎用ホスト名であり、SAN フィールドには、同じ汎用ホスト名と `DNS.1=aaa.ise.local` および `DNS.2=*.ise.local` などのワイルドカード表記が含まれます。

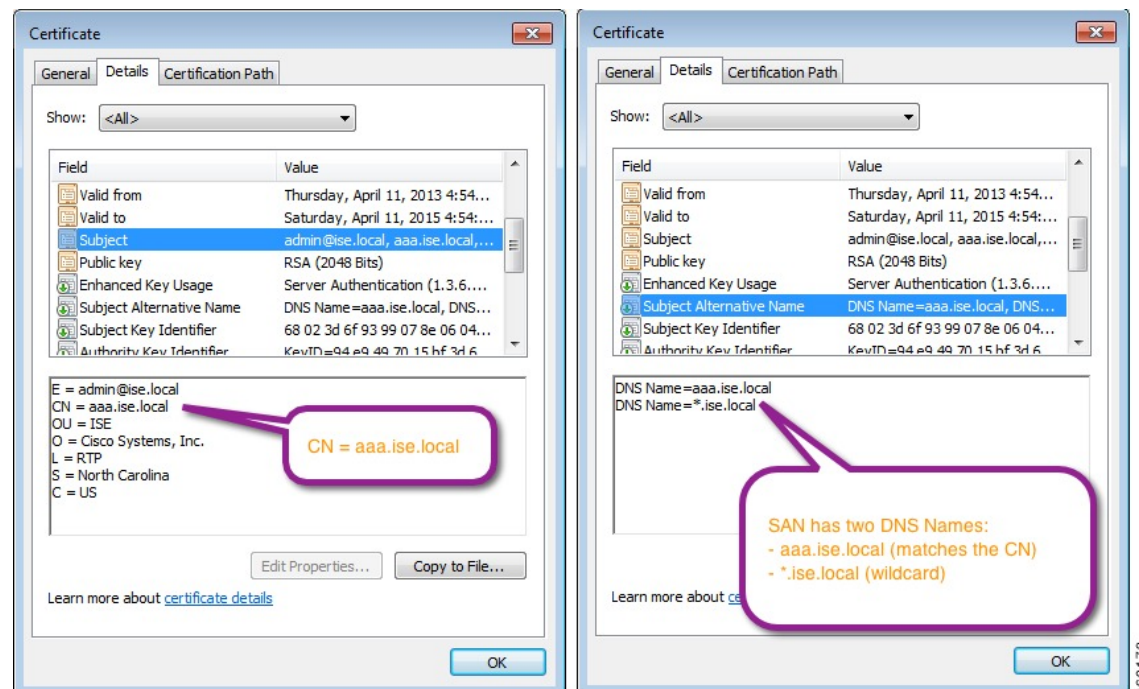
のように `*.ise.local` を使用してワイルドカード証明書を設定すると、その同じ証明書を使用して、次のような、DNS 名が「`ise.local`」で終了する他のすべてのホストを保護することができます。

- `aaa.ise.local`
- `psn.ise.local`
- `mydevices.ise.local`
- `sponsor.ise.local`

ワイルドカード証明書は通常の証明書と同じ方法で通信を保護し、要求は同じ検証方式を使用して処理されます。

次の図に、Web サイトの保護に使用されるワイルドカード証明書の例を示します。

図 5: ワイルドカード証明書の例



Cisco ISE のワイルドカード証明書のサポート

Cisco ISE はワイルドカード証明書をサポートしています。以前のリリースの Cisco ISE では、HTTPS に対して有効になったすべての証明書を検証し、CN フィールドがホストの完全修飾 (FQDN) と正確に一致することを確認していました。フィールドが一致しない場合、その証明書は HTTPS 通信に使用できませんでした。

以前のリリースの Cisco ISE では、CN 値を使用して、url-redirect A-V pair 文字列の変数を置き換えていました。この CN 値は、すべての Centralized Web Authentication (CWA)、オンボーディング、ポスチャリダイレクションなどに使用されました。

Cisco ISE は CN として ISE ノードのホスト名を使用します。

HTTPS および EAP 通信用のワイルドカード証明書

SSL/TLS トンネリングを使用する Admin (Web ベースのサービス) および EAP プロトコルに対して、Cisco ISE でワイルドカードサーバ証明書を使用できます。ワイルドカード証明書を使用することにより、各 Cisco ISE ノードに固有の証明書を生成する必要がなくなります。また、証明書の警告を防ぐために、SAN フィールドに複数の FQDN 値を入力する必要もありません。SAN フィールドでアスタリスク (*) を使用すると、展開内の複数のノードで単一の証明書を共有できるようになり、証明書名の不一致による警告を防止することができます。ただし、ワイルドカード証明書は、各 Cisco ISE ノードに固有のサーバ証明書を割り当てる場合よりも安全性が低いと見なされます。



(注) ワイルドカード証明書を使用する場合は、セキュリティを強化するためにドメイン領域を分割することを推奨します。たとえば、*.example.com の代わりに *.amer.example.com を使用して領域を分割することができます。ドメインを分割しないと、重大なセキュリティ問題が発生する可能性があります。

ワイルドカード証明書では、ドメイン名の前にアスタリスク (*) およびピリオドが使用されます。たとえば、証明書のサブジェクト名の CN 値は aaa.ise.local などの汎用ホスト名になり、SAN フィールドには *.ise.local のようなワイルドカード文字が入力されます。Cisco ISE は、ワイルドカード証明書 (提示される ID の一番左の文字がワイルドカード文字 (*)) をサポートします。たとえば、*.example.com または *.ind.example.com です。提示される ID に追加の文字とワイルドカード文字が含まれた証明書はサポートされません。たとえば、abc*.example.com、a*b.example.com、または *abc.example.com です。

URL リダイレクションの完全修飾ドメイン名

Cisco ISE が許可プロファイルリダイレクトを構築 (中央集中型 Web 認証、デバイス登録 Web 認証、ネイティブ サプリカントのプロビジョニング、モバイル デバイス管理、およびクライアントのプロビジョニングとポスチャサービスに対して) する場合、結果の cisco-av-pair ペアには、次のような文字列が含まれます。

```
url-redirect=https://ip:port/guestportal/gateway?sessionId=SessionIdValue&action=cwa
```

この要求を処理するときに、Cisco ISE は文字列の一部のキーワードを実際の値で置き換えます。たとえば、`SessionIdValue` は、要求の実際のセッション ID に置き換えられます。`eth0` インターフェイスの場合、Cisco ISE は URL 内の IP を Cisco ISE ノードの FQDN で置き換えます。`eth0` 以外のインターフェイスの場合、Cisco ISE は URL 内の IP アドレスを使用します。インターフェイス `eth1` から `eth3` にはホストのエイリアス（名前）を割り当てることができます。このエイリアスは Cisco ISE が URL リダイレクション中に IP アドレスの代わりに置き換えることができます。

これを行うために、次のように、Cisco ISE CLI の `ISE /admin(config)#` プロンプトからコンフィギュレーション モードで `ip host` コマンドを使用できます。

ip host *IP_address host-alias FQDN-string*

ここで、`IP_address` はネットワーク インターフェイス（`eth1` または `eth2` または `eth3`）の IP アドレスで、`host-alias` はネットワーク インターフェイスに割り当てる名前です。`FQDN-string` は、ネットワーク インターフェイスの完全修飾ドメイン名です。このコマンドを使用して、ネットワーク インターフェイスに `host-alias` または `FQDN-string` あるいはその両方を割り当てることができます。

ip host コマンドの使用例：`ip host a.b.c.d sales sales.amerxyz.com`

`eth0` 以外のインターフェイスにホストのエイリアスを割り当てたら、**application start ise** コマンドを使用して Cisco ISE でアプリケーション サービスを再起動する必要があります。

このホスト エイリアスのネットワーク インターフェイスとの関連付けを削除するには、次のようにこのコマンドの `no` 形式を使用します。

no ip host *IP_address host-alias FQDN-string*

ホストのエイリアスの定義を表示するには、**show running-config** コマンドを使用します。

FQDN 文字列を指定している場合は、その FQDN で URL 内の IP アドレスが置き換えられます。ホストのエイリアスのみを指定した場合は、そのホスト エイリアスと設定された IP ドメイン名を結合して完全な FQDN が結合され、URL 内の IP アドレスがその FQDN で置き換えられます。ネットワーク インターフェイスをホストのエイリアスにマッピングしない場合は、URL 内のネットワーク インターフェイスの IP アドレスが使用されます。

クライアントのプロビジョニング、ネイティブ サプリカント、またはゲスト フローに対して `eth0` 以外のインターフェイスを使用する場合は、`eth0` 以外のインターフェイスの IP アドレスまたはホスト エイリアスがポリシー サービス ノードの証明書の SAN フィールドに適切に設定されていることを確認する必要があります。

ワイルドカード証明書を使用する利点

- コスト削減。サードパーティの認証局によって署名された証明書には高額な費用がかかります（特にサーバ数が多い場合）。ワイルドカード証明書は、Cisco ISE 展開内の複数ノードで使用できます。
- 運用の効率化。ワイルドカード証明書は、すべてのポリシー サービス ノード（PSN）EAP および Web サービスが同じ証明書を共有することを可能にします。証明書を 1 回作成し

て、すべての PSN に適用することにより、コストを大幅に削減できるだけでなく、証明書の管理も簡素化されます。

- 認証エラーの低減。ワイルドカード証明書は、クライアントがプロファイル内に信頼された証明書を保存しており、そのクライアントが iOS のキーチェーン（署名ルートが信頼されている）に従っていない Apple iOS デバイスで発生する問題に対処します。iOS クライアントが最初に PSN と通信する際、このクライアントはその PSN の証明書を（信頼された認証局が署名している場合でも）明示的に信頼しません。ワイルドカード証明書を使用すると、この証明書がすべての PSN で同一になるため、ユーザは証明書の受け入れを 1 回行えばよく、その後の異なる PSN に対する認証はエラーやプロンプトが表示されることなく進行します。
- 簡素化されたサブリカントの設定。たとえば、PEAP-MSCHAPv2 およびサーバ証明書の信頼が有効になっている Microsoft Windows サブリカントで、各サーバ証明書を信頼するように指定することが必要とされており、そのように指定されていない場合、そのクライアントが別の PSN を使用して接続を行うと、各 PSN 証明書を信用するように、ユーザにプロンプトが出される可能性があります。ワイルドカード証明書を使用すると、各 PSN の個別の証明書ではなく、単一のサーバ証明書を信頼するだけで済みます。
- ワイルドカード証明書を使用すると、プロンプトの提示が減り、よりシームレスな接続が実現されることにより、ユーザエクスペリエンスが改善されます。

ワイルドカード証明書を使用することの欠点

次に、ワイルドカード証明書に関連するセキュリティ上の考慮事項の一部を説明します。

- 監査性と否認防止性の低下
- 秘密キーの露出の増加
- 一般的ではなく、管理者により理解されていない

ワイルドカード証明書は ISE ノードごとの固有のサーバ証明書よりも安全性が低いと見なされています。ただし、コスト、およびその他の運用関連の要因がセキュリティリスクに勝っています。

ASA などのセキュリティ デバイスも、ワイルドカード証明書をサポートしています。

ワイルドカード証明書を展開する場合には注意が必要です。たとえば、`*.company.local` を使用して証明書を作成したとします。該当の秘密キーを攻撃者が回復できた場合、攻撃者は `company.local` ドメイン内のすべてのサーバをスプーフィングすることができます。したがって、このタイプの危険を回避するために、ドメイン領域を分割することがベストプラクティスと見なされています。

この想定される問題に対処し、利用範囲を制限するために、ワイルドカード証明書を使用して組織の特定のサブドメインを保護することもできます。ワイルドカードを指定する一般名のサブドメイン領域に、アスタリスク (*) を追加します。

たとえば、*.ise.company.local に対してワイルドカード証明書を設定すると、その証明書は次のような、DNS 名が「.ise.company.local」で終わるすべてのホストを保護するために使用できます。

- psn.ise.company.local
- mydevices.ise.company.local
- sponsor.ise.company.local

ワイルドカード証明書の互換性

ワイルドカード証明書は通常、証明書サブジェクトの一般名 (CN) としてリストされているワイルドカードを使用して作成されます。Cisco ISE は、このタイプの作成をサポートします。ただし、すべてのエンドポイントサブリカントが証明書サブジェクトのワイルドカード文字をサポートするわけではありません。

テスト済みのすべての Microsoft ネイティブ サブリカント (Windows Mobile を含む) の一部は、証明書のサブジェクトのワイルドカード文字をサポートしていません。

Cisco AnyConnect Network Access Manager (NAM) など、[サブジェクト (Subject)] フィールドでのワイルドカード文字の使用をサポートできる他のサブリカントを使用することができます。

また、DigiCert の Wildcard Plus など、証明書のサブジェクト代替名に特定のサブドメインを含めることで、互換性のないデバイスを使用するように設計された、特別なワイルドカード証明書を使用することもできます。

Microsoft サブリカントの制限はワイルドカード証明書の使用にとって妨げになるように見えますが、Microsoft のネイティブ サブリカントを含む、セキュアなアクセスについてテスト済みのすべてのデバイスを使用できるようにする代替の方法があります。

このためには、サブジェクトにワイルドカードを使用する代わりに、[Subject Alternative Name (SAN)] フィールドでワイルドカード文字を使用します。SAN フィールドはドメイン名 (DNS 名) を検査するように設計された拡張を保持します。詳細については、RFC 6125 および 2128 を参照してください。

証明書階層

管理者ポータルから、すべてのエンドポイント、システム、および信頼できる証明書の証明書階層または信頼書トラストチェーンを表示できます。証明書階層には、証明書、すべての中間認証局 (CA) の証明書、およびルート証明書が含まれています。たとえば、管理者ポータルからシステム証明書を表示すると、デフォルトでは該当するシステム証明書の詳細が表示されます。証明書階層は、証明書の上部に表示されます。詳細を表示するには、その階層で証明書をクリックします。自己署名証明書には階層または信頼チェーンがありません。

証明書のリスト ページで、[ステータス (Status)] 列に次のアイコンのいずれかが表示されます。

- 緑色のアイコン：有効な証明書 (有効な信頼チェーン) を示します

- 赤色のアイコン：エラーを示します（たとえば、信頼証明書の欠落または期限切れ）
- 黄色のアイコン：証明書が期限切れ間近であることを警告し、更新処理を求めます

システム証明書

Cisco ISE システム証明書は、展開内のその他のノードおよびクライアント アプリケーションに対して Cisco ISE ノードを識別するサーバ証明書です。システム証明書の用途は次のとおりです。

- Cisco ISE 展開でノード間通信に使用されます。この証明書の場合、[使用方法 (Usage)] フィールドで [管理 (Admin)] オプションを選択します。
- Cisco ISE Web ポータルに接続するブラウザおよび REST クライアントで使用されます。この証明書の場合、[使用方法 (Usage)] フィールドで [ポータル (Portal)] オプションを選択します。
- PEAP および EAP-FAST を使用する外部 TLS トンネルを形成するために使用されます。EAP-TLS、PEAP、および EAP-FAST の相互認証の場合、[使用方法 (Usage)] フィールドで [EAP] オプションを選択します。
- RADIUS DTLS サーバ認証に使用されます。
- SAML ID プロバイダー (IdP) との通信に使用されます。この証明書の [使用方法 (Usage)] フィールドで [SAML] オプションを選択します。[SAML] オプションを選択すると、その他のサービスにこの証明書を使用することはできません。
- pxGrid コントローラとの通信に使用されます。この証明書の場合、[使用方法 (Usage)] フィールドで [pxGrid] オプションを選択します。

Cisco ISE 展開で、各ノードで有効なシステム証明書をインストールする必要があります。デフォルトでは、インストール時に Cisco ISE ノードに 2 つの自己署名証明書と、内部 Cisco ISE CA により署名された 1 つの証明書が作成されます。

- [EAP]、[管理 (Admin)]、[ポータル (Portal)]、および [RADIUS DTLS] のための自己署名サーバ証明書（キー サイズは 2048 で 1 年間有効です）。
- SAML IdP との安全な通信に使用できる自己署名 SAML サーバ証明書（キー サイズは 2048 で 1 年間有効です）。
- pxGrid クライアントとの安全な通信に使用できる内部 Cisco ISE CA 署名付きサーバ証明書（キー サイズは 4096 で 1 年間有効です）。

展開をセットアップし、セカンダリ ノードを登録すると、pxGrid コントローラ用の証明書が自動的にプライマリ ノードの CA 署名付き証明書に置き換わります。したがってすべての pxGrid 証明書が同一 PKI トラスト階層の一部となります。



- (注) ワイルドカードシステム証明書をエクスポートして、（ノード間通信用に）他のノードにインポートする場合は、必ず証明書と秘密キーをエクスポートして、暗号化パスワードを指定してください。インポート時は、証明書、秘密キー、および暗号化パスワードが必要です。

シスコでは、セキュリティ向上のために自己署名証明書を CA 署名付き証明書と置き換えることを推奨します。CA 署名付き証明書を取得するには、以下を行う必要があります。

1. 証明書署名要求（CSR）を作成します。
2. 認証局（CA）に送信します。
3. 署名付き証明書を取得します。
4. 関連するルートおよび中間 CA 証明書を信頼できる証明書ストアにインポートします。
5. CSR に署名付き証明書をバインドします。

ISE コミュニティ リソース

[How To: Implement ISE Server-Side Certificates](#)

[Certificate Renewal on Cisco Identity Services Engine Configuration Guide](#)

システム証明書の表示

[システム証明書（System Certificate）] ページに、Cisco ISE に追加されたすべてのシステム証明書が一覧表示されます。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 [管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [システム証明書（System Certificates）] を選択します。

[システム証明書（System Certificate）] ページが表示されます。このページには、システム証明書に関する次の情報が表示されています。

- [フレンドリ名（Friendly Name）]：証明書の名前。
- [使用者（Used By）]：この証明書が使用されるサービス。
- [ポータルグループタグ（Portal group tag）]：ポータルを使用するように指定された証明書に対してのみ適用できます。どの証明書をポータルに使用しなければならないかを指定します。
- [発行先（Issued To）]：証明書のサブジェクトの一般名。
- [発行元（Issued By）]：証明書発行者の一般名
- [有効期限の開始（Valid From）]：証明書の作成日付（Not Before 証明書属性）。

- [期限日 (Expiration Date)] : 証明書の有効期限 (Not After 証明書属性)。証明書の有効期限を示します。ここには、アイコンが関連付けられた 5 つのカテゴリがあります。
 - [91 日以上で期限切れ (Expiring in more than 90 days)] (緑のアイコン)
 - [90 日以内に期限切れ (Expiring in 90 days or less)] (青のアイコン)
 - [60 日以内に期限切れ (Expiring in 60 days or less)] (黄色のアイコン)
 - [30 日以内に期限切れ (Expiring in 30 days or less)] (オレンジのアイコン)
 - [期限切れ (Expired)] (赤のアイコン)

ステップ 2 証明書を選択し、[表示 (View)] を選択して証明書の詳細を表示します。

システム証明書のインポート

管理者ポータルから、任意の Cisco ISE ノードのシステム証明書をインポートできます。

始める前に

- クライアント ブラウザを実行しているシステムに、システム証明書と秘密キー ファイルがあることを確認します。
- インポートするシステム証明書が外部 CA によって署名されている場合は、関連するルート CA および中間 CA 証明書を信頼できる証明書ストアにインポートします ([管理 (Administration)] > [システム (System)] > [証明書 (Certificates)] > [信頼できる証明書 (Trusted Certificates)])。
- Cisco ISE では、SHA-256 より大きいハッシュ アルゴリズムで署名された証明書はサポートされていません。したがって、SHA-256 より大きいハッシュ アルゴリズムで署名されたサーバ証明書はインポートしないでください。
- インポートするシステム証明書に、CA フラグが true に設定された基本制約拡張が含まれている場合は、キー使用拡張が存在すること、および keyEncipherment ビットと keyAgreement ビットのいずれかまたは両方が設定されていることを確認します。
- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 [管理 (Administration)] > [システム (System)] > [証明書 (Certificates)] > [システム証明書 (System Certificates)] を選択します。

ステップ 2 [インポート (Import)] をクリックします。
[サーバ証明書のインポート (Import Server Certificate)] 画面が表示されます。

ステップ 3 インポートする証明書の値を入力します。

ステップ 4 [送信 (Submit)] をクリックします。

自己署名証明書の生成

自己署名証明書を生成することにより、新しいローカル証明書を追加できます。自己署名証明書は、内部テストと評価のニーズに対してのみ使用することを推奨します。実稼働環境に Cisco ISE を展開することを計画している場合は、可能な限り CA 署名付き証明書を使用して、実稼働ネットワーク全体でより均一な受け入れが行われるようにします。



(注) 自己署名証明書を使用しており、Cisco ISE ノードのホスト名を変更する必要がある場合は、Cisco ISE ノードの管理者用ポータルにログインし、古いホスト名が使用された自己署名証明書を削除し、新しい自己署名証明書を生成します。そうしないと、Cisco ISE は古いホスト名が使用された自己署名証明書を引き続き使用します。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 [管理 (Administration)] > [システム (System)] > [証明書 (Certificates)] > [システム証明書 (System Certificates)] を選択します。

セカンダリ ノードから自己署名証明書を生成するには、[管理 (Administration)] > [システム (System)] > [サーバ証明書 (Server Certificate)] を選択します。

ステップ 2 [自己署名証明書の生成 (Generate Self Signed Certificate)] をクリックし、[自己署名証明書の生成 (Generate Self Signed Certificate)] ページに詳細を入力します。

ステップ 3 自己署名したワイルドカード証明書 (サブジェクトの任意の一般名またはサブジェクト代替名の DNS 名、またはその両方にアスタリスク (*) が含まれている証明書) を生成する場合は、[ワイルドカード証明書の許可 (Allow Wildcard Certificates)] チェックボックスをオンにします。たとえば、SAN に割り当てられている DNS 名が *.amer.cisco.com の場合です。

ステップ 4 この証明書を使用するサービスに基づいて [使用方法 (Usage)] 領域のチェックボックスをオンにします。

ステップ 5 証明書を生成するには、[送信 (Submit)] をクリックします。

CLI からセカンダリ ノードを再起動するには、指定された順序で次のコマンドを入力します。

- a) `application stop ise`
- b) `application start ise`

システム証明書の編集

このページを使用して、システム証明書を編集し、自己署名証明書を更新できます。ワイルドカード証明書を編集すると、変更が展開内のすべてのノードに複製されます。ワイルドカード

証明書を削除した場合、そのワイルドカード証明書は展開内のすべてのノードから削除されます。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

- ステップ 1** [管理 (Administration)] > [システム (System)] > [証明書 (Certificates)] > [システム証明書 (System Certificates)] を選択します。
- ステップ 2** 編集する証明書の横にあるチェックボックスをオンにして、[編集 (Edit)] をクリックします。
- ステップ 3** 自己署名証明書を更新するには、[更新期間 (Renewal Period)] チェックボックスをオンにして、有効期限 TTL (存続可能時間) を日、週、月、または年単位で入力します。
- ステップ 4** [Save (保存)] をクリックして変更内容を保存します。

[管理者 (Admin)] チェックボックスがオンになっている場合、Cisco ISE ノードのアプリケーションサーバが再起動されます。また、その Cisco ISE ノードが展開の PAN である場合は、展開内のその他すべてのノードでもアプリケーションサーバが再起動されます。プライマリ管理ノード (PAN) の再起動が完了すると、システムによって一度に 1 つのノードが再起動されます。



- (注) Chrome 65 以上を使用して ISE を起動すると、URL が正しくリダイレクトされたにもかかわらず、BYOD ポータルまたはゲスト ポータルがブラウザで起動に失敗することがあります。これは、すべての [サブジェクトの別名 (Subject Alternative Name)] フィールドに証明書を必要とする、Google で導入された新しいセキュリティ機能が原因です。ISE 2.4 までのすべての ISE リリースで、[サブジェクトの別名 (Subject Alternative Name)] フィールドに記入しないでください。

Chrome 65 以上で起動するには、次の手順に従います。

- 1.[サブジェクトの別名 (Subject Alternative Name)] フィールドに入力することで、ISE GUI から新しい自己署名証明書を生成します。DNS と IP アドレスの両方を入力する必要があります。
- 2.ISE サービスが再起動します。
- 3.Chrome ブラウザでポータルにリダイレクトされます。
- 4.ブラウザで [証明書の表示 (View Certificate)] > [詳細 (Details)] > [コピー (Copy)] の順に選択し、base-64 エンコードを選択して、証明書をコピーします。
- 5.高信頼パスで証明書をインストールします。
- 6.Chrome ブラウザを終了し、ポータルのリダイレクトを試みます。

システム証明書の削除

今後使用しないシステム証明書を削除できます。

システム証明書ストアから複数の証明書を一度に削除できますが、管理および EAP 認証に使用できる証明書を少なくとも 1 つ所有する必要があります。また、管理、EAP 認証、ポータル、または pxGrid コントローラに使用される証明書は削除できません。ただし、サービスがディセーブルの場合は、pxGrid 証明書を削除できます。

ワイルドカード証明書を削除することを選択した場合、証明書は展開内のすべてのノードから削除されます。

ステップ 1 [管理 (Administration)] > [システム (System)] > [証明書 (Certificates)] > [システム証明書 (System Certificates)] を選択します。

ステップ 2 削除する証明書の隣にあるチェックボックスをオンにし、[削除 (Delete)] をクリックします。

警告メッセージが表示されます。

ステップ 3 [はい (Yes)] をクリックして、証明書を削除します。

システム証明書のエクスポート

選択したシステム証明書とその証明書に関連付けられている秘密キーをエクスポートできます。証明書とその秘密キーをバックアップ用にエクスポートする場合は、それらを必要に応じて後で再インポートできます。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 [管理 (Administration)] > [システム (System)] > [証明書 (Certificates)] > [システム証明書 (System Certificates)] を選択します。

ステップ 2 エクスポートする証明書の横にあるチェックボックスをオンにし、[エクスポート (Export)] をクリックします。

ステップ 3 証明書のみをエクスポートするか、証明書と証明書に関連付けられている秘密キーをエクスポートするかを選択します。

ヒント 値が公開される可能性があるため、証明書に関連付けられている秘密キーのエクスポートは推奨しません。秘密キーをエクスポートする必要がある場合（たとえば、ワイルドカードシステム証明書をエクスポートしてノード間通信用に他のノードにインポートする場合は、その秘密キーの暗号化パスワードを指定します。このパスワードは、証明書を別の Cisco ISE ノードにインポートするときに指定して、秘密キーを復号化する必要があります。

ステップ 4 秘密キーをエクスポートする場合は、パスワードを入力します。パスワードは、8 文字以上にする必要があります。

ステップ 5 [エクスポート (Export)] をクリックして、クライアント ブラウザを実行しているファイルシステムに証明書を保存します。

証明書のみをエクスポートする場合、証明書は Privacy Enhanced Mail 形式で保存されます。証明書と秘密キーの両方をエクスポートする場合、証明書は Privacy Enhanced Mail 形式の証明書と暗号化された秘密キーファイルを含む .zip ファイルとしてエクスポートされます。

信頼できる証明書ストア

信頼できる証明書ストアには、信頼に使用される、Simple Certificate Enrollment Protocol (SCEP) 用の X.509 証明書が含まれています。

信頼できる証明書ストア内の証明書は PAN で管理され、Cisco ISE 展開内の他のすべてのノードに複製されます。Cisco ISE はワイルドカード証明書をサポートしています。

Cisco ISE は、次の目的で信頼できる証明書を使用します。

- エンドポイントによる認証と、証明書ベースの管理者認証を使用して ISE-PIC 管理者ポータルにアクセスする Cisco ISE 管理者による認証に使用するクライアント証明書を確認するため。
 - 展開内の Cisco ISE ノード間のセキュアな通信を可能にするため。信頼できる証明書ストアには、展開内の各ノードのシステム証明書との信頼を確立するために必要な CA 証明書のチェーンが含まれている必要があります。
 - 自己署名証明書をシステム証明書に使用する場合は、各ノードの自己署名証明書を PAN の信頼できる証明書ストアに配置する必要があります。
 - CA 署名付き証明書をシステム証明書に使用する場合は、CA ルート証明書だけでなく、信頼チェーン内のすべての中間証明書も PAN の信頼できる証明書ストアに配置する必要があります。
 - セキュア LDAP 認証を有効にするには、SSL を経由してアクセスされる LDAP ID ソースを定義するときに、証明書ストアから証明書を選択する必要があります。
 - パーソナル デバイス ポータルを使用してネットワークへの登録を準備しているパーソナル デバイスに配信するため。Cisco ISE は、パーソナル デバイス登録をサポートするために、ポリシー サービス ノード (PSN) での SCEP を実装しています。登録するデバイスは、SCEP プロトコルを使用して PSN からクライアント証明書を要求します。PSN には中継の役割を果たす登録局 (RA) があります。RA は、登録するデバイスからの要求を受信して検証し、その後クライアント証明書を発行する外部 CA または内部 Cisco ISE CA にその要求を転送します。CA は RA に証明書を返し、RA が証明書をデバイスに返します。
- Cisco ISE によって使用される各 SCEP CA は、SCEP RA プロファイルによって定義されます。SCEP RA のプロファイルが作成されると、次の 2 つの証明書が信頼できる証明書ストアに自動的に追加されます。
- CA 証明書 (自己署名証明書)
 - CA によって署名された RA 証明書 (証明書要求のエージェントの証明書)。

SCEP プロトコルでは、これらの 2 つの証明書が RA によって登録デバイスに提供されている必要があります。信頼できる証明書ストアにこの 2 つの証明書を配置すると、これらのノードの RA が使用するために、証明書がすべての PSN ノードに複製されます。



(注) Cisco ISE にインポートされる X.509 証明書は、Privacy Enhanced Mail (PEM) または Distinguished Encoding Rules (DER) 形式である必要があります。証明書チェーン（システム証明書、およびその証明書に署名する一連の信頼された証明書）が含まれたファイルはインポートすることができますが、特定の制限の対象となります。

ISE コミュニティ リソース

[Install a Third-Party CA Certificate in ISE 2.0](#)

信頼できる証明書ストアの証明書

信頼できる証明書ストアは、次の信頼できる証明書で事前設定されています。製造業者証明書、ルート証明書、その他の信頼できる証明書。ルート証明書（Cisco Root CA）は、製造業者（Cisco CA Manufacturing）証明書に署名します。これらの証明書は、デフォルトでは無効になっています。展開でエンドポイントとして Cisco IP Phone を使用している場合は、これら 2 つの証明書を有効にして、この電話用にシスコが署名した証明書の認証ができるようにします。

信頼できる証明書の命名の制約

CTL の信頼できる証明書には名前の制約の拡張が含まれている場合があります。この拡張は、証明書チェーンの後続のすべての証明書のサブジェクト名とサブジェクト代替名フィールドの値の名前空間を定義します。Cisco ISE は、ルート証明書で指定された制約を検査しません。

次の名前の制約がサポートされています。

- ディレクトリ名

ディレクトリ名の制限は、サブジェクト/SAN のディレクトリ名のプレフィクスです。次の例を参考にしてください。

- 正しいサブジェクト プレフィクス :

CA 証明書の名前の制約 : Permitted: O=Cisco

クライアント証明書のサブジェクト : O=Cisco,CN=Salomon

- 不正なサブジェクト プレフィクス :

CA 証明書の名前の制約 : Permitted: O=Cisco

クライアント証明書のサブジェクト : CN=Salomon,O=Cisco

- DNS

- E-mail
- URI (URI の制約は、http://、https://、ftp://、または ldap:// のような URI プレフィクスで始まる必要があります)。

次の名前の制約はサポートされていません。

- IP アドレス
- Othername

信頼できる証明書にサポートされていない制約が含まれており、検証中の証明書に該当のフィールドが含まれていない場合は、Cisco ISE がサポートされない制約を検証できないため、その証明書は拒否されます。

信頼できる証明書内の名前の制約の定義例を次に示します。

```
X509v3 Name Constraints: critical
    Permitted:
        othername:<unsupported>
        email:.abcde.at
        email:.abcde.be
        email:.abcde.bg
        email:.abcde.by
        DNS:.dir
        DirName: DC = dir, DC = emea
        DirName: C = AT, ST = EMEA, L = AT, O = ABCDE Group, OU = Domestic
        DirName: C = BG, ST = EMEA, L = BG, O = ABCDE Group, OU = Domestic
        DirName: C = BE, ST = EMEA, L = BN, O = ABCDE Group, OU = Domestic
        DirName: C = CH, ST = EMEA, L = CH, O = ABCDE Group, OU = Service Z100

        URI:.dir
        IP:172.23.0.171/255.255.255.255
    Excluded:
        DNS:.dir
        URI:.dir
```

受け入れ可能なクライアント証明書のサブジェクトは、次のように上記の定義に一致します。

```
Subject: DC=dir, DC=emea, OU=+DE, OU=OU-Administration, OU=Users, OU=X1,
CN=cwinwell
```

信頼できるストア証明書の表示

[信頼できる証明書 (Trusted Certificates)] ページに、Cisco ISE に追加されたすべての信頼できる証明書が一覧表示されます。信頼できる証明書を表示するには、スーパー管理者またはシステム管理者である必要があります。

すべての証明書を表示するには、[管理 (Administration)] > [システム (System)] > [証明書 (Certificates)] > [信頼できる証明書 (Trusted Certificates)] を選択します。[信頼できる証明書 (Trusted Certificates)] ページが表示され、すべての信頼できる証明書が一覧表示されます。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

信頼できる証明書ストアの証明書のステータス変更

証明書のステータスが有効になっている必要があります。これにより、Cisco ISE が信頼の確立にこの証明書を使用できるようになります。証明書が信頼できる証明書ストアにインポートされると、この証明書は自動的に有効になります。

ステップ 1 [管理 (Administration)] > [システム (System)] > [証明書 (Certificates)] > [信頼できる証明書 (Trusted Certificates)]。

ステップ 2 有効または無効にする証明書の隣にあるチェックボックスをオンにし、[編集 (Edit)] をクリックします。

ステップ 3 ステータスを変更します。

ステップ 4 [保存 (Save)] をクリックします。

信頼できる証明書ストアへの証明書の追加

[証明書ストア (Certificate Store)] ページを使用して、Cisco ISE に CA 証明書を追加することができます。

始める前に

- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。
- ブラウザを実行しているコンピュータのファイルシステムに、証明書ストアの証明書が存在することを確認します。証明書は PEM または DER 形式である必要があります。
- Admin 認証または EAP 認証に証明書を使用する場合は、基本制約が証明書に定義され、CA フラグが true に設定されていることを確認します。

ステップ 1 [管理 (Administration)] > [システム (System)] > [証明書 (Certificates)] > [信頼できる証明書 (Trusted Certificates)] を選択します。

ステップ 2 [インポート (Import)] をクリックします。

ステップ 3 必要に応じてフィールドの値を設定します。

EAP 認証用に証明書チェーンにサブ CA 証明書を使用する場合は、ルート CA までに証明書チェーンにすべての証明書をインポートする際に [クライアント認証および syslog 用に信頼する (Trust for client authentication and Syslog)] チェックボックスを必ずオンにしてください。

パスワードベースの認証から証明書ベースの認証に認証タイプを変更すると、Cisco ISE は展開内の各ノードでアプリケーション サーバを再起動します。PAN のアプリケーション サーバから開始され、その後に各追加ノードが 1 つずつ続きます。

信頼できる証明書の編集

証明書を信頼できる証明書ストアに追加したら、編集の設定を使用して、その証明書をさらに編集できます。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

-
- ステップ 1** [管理 (Administration)] > [システム (System)] > [証明書 (Certificates)] > [信頼できる証明書 (Trusted Certificates)] を選択します。
- ステップ 2** 編集する証明書の横にあるチェックボックスをオンにして、[編集 (Edit)] をクリックします。
- ステップ 3** 必要に応じて編集可能なフィールドを変更します。
- ステップ 4** [保存 (Save)] をクリックして、証明書ストアに対して行った変更を保存します。
-

信頼できる証明書の削除

今後使用しない信頼できる証明書を削除できます。ただし、ISE 内部 CA (認証局) の証明書は削除しないでください。ISE 内部 CA 証明書を削除できるのは、展開全体の ISE ルート証明書チェーンを置き換える場合のみです。

-
- ステップ 1** [管理 (Administration)] > [システム (System)] > [証明書 (Certificates)] > [信頼できる証明書 (Trusted Certificates)]。
- ステップ 2** 削除する証明書の隣にあるチェックボックスをオンにし、[削除 (Delete)] をクリックします。

警告メッセージが表示されます。ISE 内部 CA 証明書を削除することを選択した場合は、次のとおりにクリックします。

- [削除 (Delete)] : ISE 内部 CA 証明書を削除する場合。ISE 内部 CA によって署名されたすべてのエンドポイント証明書は無効になり、エンドポイントはネットワークにアクセスできません。エンドポイントをネットワークで再度有効にするには、信頼できる証明書ストアに同じ ISE 内部 CA 証明書をインポートします。
- [削除および取消 (Delete & Revoke)] : ISE 内部 CA 証明書を削除して取り消します。ISE 内部 CA によって署名されたすべてのエンドポイント証明書は無効になり、エンドポイントはネットワークにアクセスできません。この操作は取り消すことができません。展開全体の ISE ルート証明書チェーンを置き換える必要があります。

- ステップ 3** [はい (Yes)] をクリックして、証明書を削除します。
-

信頼できる証明書ストアからの証明書のエクスポート

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

-
- ステップ 1** [管理 (Administration)] > [システム (System)] > [証明書 (Certificates)] > [信頼できる証明書 (Trusted Certificates)]。
- ステップ 2** エクスポートする証明書の隣にあるチェックボックスをオンにし、[エクスポート (Export)] をクリックします。一度に 1 つの証明書のみをエクスポートできます。
- ステップ 3** クライアントブラウザを実行しているファイルシステムに Privacy Enhanced Mail ファイルを保存します。
-

信頼できる証明書ストアへのルート証明書のインポート

ルート CA 証明書および中間 CA 証明書をインポートするとき、信頼できる CA 証明書を使用する対象のサービスを指定できます。

始める前に

CSR に署名し、デジタルで署名された CA 証明書を返した認証局のルート証明書および他の中間証明書が必要です。

-
- ステップ 1** [管理 (Administration)] > [システム (System)] > [証明書 (Certificates)] > [信頼できる証明書 (Trusted Certificates)]。
- ステップ 2** [インポート (Import)] をクリックします。
- ステップ 3** [参照 (Browse)] をクリックして、ルート CA 証明書を選択します。
- ステップ 4** わかりやすい名前を入力します。
- わかりやすい名前を入力しない場合、Cisco ISE により、このフィールドには、*common-name#issuer#nnnnnn* の形式でわかりやすい名前が自動的に入力されます。ここで、*nnnnnn* は一意の番号です。再度証明書を編集して、わかりやすい名前を変更できます。
- ステップ 5** CA によって返されたルート証明書を選択します。
- ステップ 6** この信頼できる証明書を使用するサービスの横にあるチェックボックスをオンにします。
- ステップ 7** 説明を入力します。
- ステップ 8** [送信 (Submit)] をクリックします。
-

次のタスク

信頼できる証明書ストアに中間 CA 証明書をインポートします（該当する場合）。

関連トピック

[証明書チェーンのインポート](#) (181 ページ)

証明書チェーンのインポート

証明書ストアから受信した証明書チェーンを含む単一のファイルから、複数の証明書をインポートすることができます。ファイル内のすべての証明書は Privacy-Enhanced Mail (PEM) の形式であり、証明書は次の順序に並べられている必要があります。

- ファイル内の最後の証明書は、CA によって発行されたクライアントまたはサーバ証明書である必要があります。
- 前にあるすべての証明書は、ルート CA 証明書と、発行された証明書の署名のチェーンにあるすべて中間 CA 証明書である必要があります。

証明書チェーンのインポートは、次の 2 ステップのプロセスです。

1. 管理者ポータルで信頼できる証明書ストアに証明書チェーン ファイルをインポートします。この操作により、信頼できる証明書ストアにある最後の 1 つを除き、すべての証明書がファイルからインポートされます。
2. CA 署名付き証明書のバインド操作を使用して証明書チェーン ファイルをインポートします。この操作により、最後の証明書がローカル証明書としてファイルからインポートされます。

証明書署名要求

認証局 (CA) が署名付き証明書を発行するためには、証明書署名要求 (CSR) を作成して CA に送信する必要があります。

自分が作成した証明書署名要求 (CSR) のリストは、[証明書署名要求 (Certificate Signing Requests)] ページで使用できます。認証局 (CA) から署名を取得するには、CSR をエクスポートし、その証明書を CA に送信する必要があります。証明書は CA によって署名され、返されます。

管理者ポータルから証明書を一元的に管理できます。展開内のすべてのノードの CSR を作成およびエクスポートできます。その後、CSR を CA に送信し、CA から CA 署名付き証明書を取得し、CA によって返されたルートおよび中間 CA 証明書を信頼できる証明書ストアにインポートし、CSR に CA 署名付き証明書をバインドする必要があります。

証明書署名要求の作成と認証局への CSR の送信

証明書署名要求 (CSR) を生成して、展開内のノードの CA 署名付き証明書を取得できます。展開の選択ノードまたは展開のすべてのノード用の CSR を生成できます。

ステップ 1 [管理 (Administration)] > [システム (System)] > [証明書 (Certificates)] > [証明書署名要求 (Certificate Signing Requests)] を選択します。

ステップ 2 CSR を生成するための値を入力します。各フィールドの詳細については、[証明書署名要求の設定（1148 ページ）](#) を参照してください。

ステップ 3 [Generate（生成）] をクリックして CSR を生成します。

CSR が生成されます。

ステップ 4 [Export（エクスポート）] をクリックして、メモ帳で CSR を開きます。

ステップ 5 「-----BEGIN CERTIFICATE REQUEST-----」 から 「-----END CERTIFICATE REQUEST-----」 までのすべてのテキストをコピーします。

ステップ 6 選択した CA の証明書要求に、この CSR の内容を貼ってください。

ステップ 7 署名済みの証明書をダウンロードする。

CA によっては、署名付き証明書が電子メールで送信される場合があります。署名付き証明書は、zip ファイルの形式で、Cisco ISE の信頼された証明書ストアに追加する必要がある、新規発行の証明書と CA のパブリック署名証明書が含まれています。デジタル署名された CA 証明書、ルート CA 証明書、および他の中間 CA 証明書（該当する場合）がクライアントブラウザを実行するローカルシステムにダウンロードされます。

関連トピック

[ワイルドカード証明書（164 ページ）](#)

[Cisco ISE のワイルドカード証明書のサポート（165 ページ）](#)

[HTTPS および EAP 通信用のワイルドカード証明書（165 ページ）](#)

[URL リダイレクションの完全修飾ドメイン名（165 ページ）](#)

[ワイルドカード証明書の互換性（168 ページ）](#)

CSR への CA 署名付き証明書のバインド

CA からデジタル署名付き証明書を受け取った後、それを証明書署名要求（CSR）にバインドする必要があります。管理者ポータルから展開内のすべてのノードに対してバインド操作を実行できます。

始める前に

- デジタル署名付き証明書、および関連するルート中間 CA 証明書を CA から受け取る必要があります。
- 関連するルートおよび中間 CA 証明書を信頼できる証明書ストアにインポートします（[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）]）。

ステップ 1 [管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [証明書署名要求（Certificate Signing Requests）] を選択します。

CA 署名付き証明書に CSR をバインドするノードの隣にあるチェックボックスをオンにします。

ステップ 2 [バインド (Bind)] をクリックします。

ステップ 3 [参照 (Browse)] をクリックし、CA 署名付き証明書を選択します。

ステップ 4 証明書の [フレンドリ名 (Friendly Name)] を指定します。

ステップ 5 サブジェクトの CN またはサブジェクト代替名の DNS 名にワイルドカード文字のアスタリスク (*) を含む証明書をバインドするには、[ワイルドカード証明書の許可 (Allow Wildcard Certificates)] チェックボックスをオンにします。

ステップ 6 Cisco ISE に証明書の拡張の検証を許可する場合は、[証明書の拡張の検証を有効にする (Enable Validation of Certificate Extensions)] チェックボックスをオンにします。

[証明書の拡張の検証を有効にする (Enable Validation of Certificate Extensions)] オプションが有効になっており、インポートする証明書に CA フラグが true に設定された基本制約拡張が含まれている場合は、キー使用拡張が存在すること、および keyEncipherment ビットと keyAgreement ビットのいずれかまたは両方が設定されていることを確認します。

ステップ 7 この証明書が使用領域で使用されるサービスを確認します。

この情報は、CSR の生成時に [使用方法 (Usage)] オプションを有効にした場合は自動入力されます。証明書のバインディング時に使用方法を指定しない場合は、[使用方法 (Usage)] オプションをオフにします。後で証明書を編集し、使用方法を指定できます。

ステップ 8 [送信 (Submit)] をクリックし、CA 署名付き証明書をバインドします。

Cisco ISE ノード間通信にこの証明書を使用するように選択した場合、Cisco ISE ノードでアプリケーションサーバが再起動されます。

他のノードで CA 署名付き証明書に CSR をバインドするために、このプロセスを繰り返します。

次のタスク

[信頼できる証明書ストアへのルート証明書のインポート \(180 ページ\)](#)

証明書署名要求のエクスポート

このページを使用して、証明書署名要求をエクスポートすることができます。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 [管理 (Administration)] > [システム (System)] > [証明書 (Certificates)] > [証明書署名要求 (Certificate Signing Requests)] を選択します。

ステップ 2 エクスポートする証明書の隣にあるチェックボックスをオンにし、[エクスポート (Export)] をクリックします。

ステップ 3 [OK] をクリックして、クライアントブラウザを実行しているファイルシステムにファイルを保存します。

Cisco ISE ノード間通信の信頼できる証明書のインストール

展開をセットアップする場合、セカンダリ ノードを登録する前に、セカンダリ ノードの管理者証明書の検証に使用される適切な CA 証明書を PAN の証明書信頼リスト (CTL) に配置する必要があります。PAN の CTL に入力する手順は、シナリオに応じて異なります。

- セカンダリ ノードが管理者ポータルとの通信に CA 署名付き証明書を使用する場合は、セカンダリ ノードの CA 署名付き証明書、関連する中間証明書 (ある場合)、および (セカンダリ ノードの証明書に署名した CA の) ルート CA 証明書を PAN の CTL にインポートする必要があります。
- セカンダリ ノードが管理者ポータルとの通信に自己署名証明書を使用する場合は、PAN の CTL にセカンダリ ノードの自己署名証明書をインポートできます。



(注)

- 登録されたセカンダリ ノードの管理者証明書を変更する場合は、セカンダリ ノードの管理者証明書の検証に使用できる適切な CA 証明書を取得し、PAN の CTL にインポートする必要があります。
- 展開内でクライアントと PSN 間のセキュアな通信に自己署名証明書を使用する場合、BYOD ユーザがある場所から別の場所に移動すると、EAP-TLS ユーザ認証は失敗します。一部の PSN 間で提供される必要があるこのような認証要求の場合、外部で署名された CA 証明書を使用してクライアントと PSN 間の通信を保護するか、または外部の CA によって署名されたワイルドカード証明書を使用する必要があります。

外部 CA から発行された証明書に基本制約が定義されており、CA フラグが **true** に設定されていることを確認します。ノード間通信の CA 署名付き証明書をインストールするには、次の手順を実行します。

ステップ 1 証明書署名要求の作成と認証局への CSR の送信 (181 ページ)

ステップ 2 信頼できる証明書ストアへのルート証明書のインポート (180 ページ)

ステップ 3 CSR への CA 署名付き証明書のバインド (182 ページ)

ポータルで使用する証明書のセットアップ

Web ポータル要求を処理できる展開に複数のポリシー サービス ノード (PSN) がある場合、Cisco ISE には一意の ID が必要です。この ID で、ポータルの通信に使用する必要がある証明書を識別します。ポータルでの使用に指定された証明書を追加またはインポートする場合、証明書グループタグを定義して、それを展開内の各ノードの対応する証明書に関連付ける必要があります。

あります。この証明書グループ タグを対応するエンドユーザポータル（ゲスト、スポンサー、およびパーソナル デバイス ポータル）に関連付ける必要があります。この証明書グループ タグは一意の ID で、Cisco ISE が各ポータルと通信する際に使用する必要がある証明書を識別する場合に役立ちます。ポータルごとに各ノードから 1 つの証明書を指定できます。



(注) Cisco ISE は TCP ポート 8443（またはポータルが使用するよう設定したポート）でポータル証明書を提示します。

ステップ 1 証明書署名要求の作成と認証局への CSR の送信（181 ページ）。

すでに定義済みの証明書グループ タグを選択するか、ポータル用に新しく作成する必要があります。たとえば、mydevicesportal などです。

ステップ 2 信頼できる証明書ストアへのルート証明書のインポート（180 ページ）。

ステップ 3 CSR への CA 署名付き証明書のバインド（182 ページ）。

CA 署名付き証明書へのデフォルトのポータル証明書グループ タグの再割り当て

デフォルトでは、すべての Cisco ISE ポータルは自己署名証明書を使用します。ポータルに CA 署名付き証明書を使用する場合は、デフォルトのポータル証明書グループ タグを CA 署名付き証明書に割り当てることができます。既存の CA 署名付き証明書を使用するか、または CSR を生成して、ポータルに使用する新しい CA 署名付き証明書を取得できます。1 つの証明書から別の証明書をポータル グループ タグを再割り当てすることができます。



(注) 既存の証明書を編集する場合、証明書に関連付けられているポータルタグ（ゲスト）がいずれかのポータルですでに使用されている場合は、デフォルトのポータル証明書グループ タグまたは他のポータル グループ タグをこの証明書に再割り当てすることはできません。「ゲスト」ポータル タグを使用しているポータルのリストが表示されます。

次に、CA 署名付き証明書にデフォルトのポータル証明書グループ タグを再割り当てする手順について説明します。

ステップ 1 [管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [システム証明書（System Certificates）] を選択します。

このタグを使用するポータルのリストを表示するには、デフォルトのポータル証明書グループ タグの横にある **i** アイコンにマウス ポインタを合わせます。このタグが割り当てられているポータル証明書がある展開内の ISE ノードを表示することもできます。

ステップ 2 ポータルに使用する CA 署名付き証明書の横にあるチェックボックスをオンにして、[編集（Edit）] をクリックします。

■ ノードの登録前のポータル証明書タグの関連付け

いずれのポータルでも使用されていない CA 署名付き証明書を選択してください。

ステップ 3 [使用方法 (Usage)] 領域で、[ポータル (Portal)] チェックボックスをオンにして、デフォルトのポータル証明書グループ タグを選択します。

ステップ 4 [保存 (Save)] をクリックします。

警告メッセージが表示されます。

ステップ 5 [はい (Yes)] をクリックして、CA 署名付き証明書にデフォルトのポータル証明書グループ タグを再割り当てします。

ノードの登録前のポータル証明書タグの関連付け

展開内のすべてのポータルに「デフォルトポータル証明書グループ」タグを使用する場合は、新しい ISE ノードを登録する前に、関連する CA 署名付き証明書をインポートし、サービスとして「ポータル」を選択し、この証明書に「デフォルトポータル証明書グループ」タグを関連付けます。

展開に新しいノードを追加すると、デフォルトの自己署名証明書が「デフォルトポータル証明書グループ」タグに関連付けられ、このタグを使用するようにポータルが設定されます。

新しいノードの登録後、証明書グループタグの関連付けは変更できません。したがって、展開にノードを登録する前に、次を実行してください。

ステップ 1 自己署名証明書を作成し、サービスとして「ポータル」を選択し、別の証明書グループタグ（たとえば、tempportaltag）を割り当てます。

ステップ 2 新しく作成した証明書グループタグ（tempportaltag）を使用するようにポータル設定を変更します。

ステップ 3 デフォルト自己署名証明書を編集し、ポータル ロールを削除します。

このオプションは、デフォルトポータル証明書グループタグとデフォルト自己署名証明書との関連付けを削除します。

ステップ 4 次のいずれかを実行します。

オプション	説明
CSR の生成	<p>CSR を生成するときは、次を実行します。</p> <ol style="list-style-type: none"> この証明書を使用する「ポータル」をサービスとして選択し、「デフォルトポータル証明書グループ」タグを関連付けます。 CSR を CA に送信し、署名付きの証明書を取得します。 信頼できる証明書ストアに証明書を署名した CA のルートおよび他の中間証明書をインポートします。 CSR に CA 署名付き証明書をバインドします。

オプション	説明
秘密キーと CA 署名付き証明書のインポート	<p>CA 署名付き証明書をインポートするときは、次を実行します。</p> <ol style="list-style-type: none"> この証明書を使用する「ポータル」をサービスとして選択し、「デフォルト ポータル証明書グループ」タグを関連付けます。 信頼できる証明書ストアに証明書に署名した CA のルートおよび他の中間証明書をインポートします。
既存の CA 署名付き証明書の編集	<p>既存の CA 署名付き証明書を編集するときは、次を実行します。</p> <p>この証明書を使用する「ポータル」をサービスとして選択し、「デフォルト ポータル証明書グループ」タグを関連付けます。</p>

ステップ 5 展開に ISE ノードを登録します。

展開内のポータル構成は「デフォルト ポータル証明書グループ」タグに設定され、ポータルは新しいノードの「デフォルト ポータル証明書グループ」タグに関連付けられた CA 署名付き証明書を使用するように設定されます。

ユーザおよびエンドポイントの証明書の更新

デフォルトでは、Cisco ISE は証明書が期限切れになったデバイスからの要求を拒否します。ただし、このデフォルト動作を変更し、このような要求を処理し、ユーザに証明書の更新を求めるように ISE を設定できます。

ユーザが証明書を更新することを許可する場合は、要求をさらに処理する前に証明書が更新されたかどうかを判断する許可ポリシールールを設定することを推奨します。証明書が期限切れになったデバイスからの要求を処理することで、潜在的なセキュリティ脅威が発生する可能性があります。組織のセキュリティが侵害されていないことを保証するには、適切な許可プロファイルおよびルールを設定する必要があります。

あるデバイスは有効期限の前後に証明書を更新できます。ただし、Windows デバイスでは、期限切れになる前にだけ証明書を更新できます。Apple iOS、Mac OSX、および Android デバイスでは、有効期限の前または後に証明書を更新できます。

ポリシー条件で証明書更新に使用されるディクショナリ属性

Cisco ISE 証明書ディクショナリには、ユーザに証明書更新を許可するポリシー条件で使われる次の属性が含まれます。

- [有効期限までの日数 (Days to Expiry)] : この属性は、証明書が有効な日数を指定します。この属性を使用して、許可ポリシーで使用できる条件を作成できます。この属性には、0 ~ 15 の値を指定できます。0 の値は、証明書の有効期限がすでに切れていることを示します。1 の値は、証明書の有効期限が切れるまで 1 日未満であることを示します。

- [有効期限切れ (Is Expired)] : このブール属性は、証明書が有効期限切れかどうかを示します。証明書の有効期限が近く、有効期限切れではない場合にのみ証明書更新を許可する場合は、許可ポリシー条件でこの属性を使用します。

証明書更新用の許可ポリシー条件

許可ポリシーで CertRenewalRequired の単純条件（デフォルトで使用可能）を使用すると、Cisco ISE が要求を処理する前に証明書（有効期限切れまたはまもなく有効期限が切れる）を更新できます。

証明書を更新するための CWA リダイレクト

ユーザ証明書が期限切れになる前に失効している場合、Cisco ISE は、CA がパブリッシュした CRL をチェックして認証要求を拒否します。失効した証明書の期限が切れている場合は、CA が CRL でこの証明書をパブリッシュしない可能性があります。このシナリオでは、失効した証明書が Cisco ISE によって更新される可能性があります。このことを避けるために、証明書を更新する前に、要求が中央 Web 認証（CWA）にリダイレクトされ、完全認証が実行されるようにします。CWA のユーザをリダイレクトするには、許可プロファイルを作成する必要があります。

ユーザによる証明書の更新を許可する Cisco ISE の設定

ユーザが証明書を更新できるように Cisco ISE を設定するには、この手順で示すタスクを実行する必要があります。

始める前に

WLC で制限されたアクセス ACL を設定して、CWA 要求をリダイレクトします。

ステップ 1 [許可されるプロトコルの設定の更新（188 ページ）](#)

ステップ 2 [CWA リダイレクションの許可ポリシー プロファイルの作成（189 ページ）](#)

ステップ 3 [証明書を更新する許可ポリシー ルールの作成（190 ページ）](#)

ステップ 4 [ゲスト ポータルでの BYOD 設定の有効化（191 ページ）](#)

許可されるプロトコルの設定の更新

ステップ 1 [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] > [認証 (Authentication)] > [許可されるプロトコル (Allowed Protocols)] > [デフォルト ネットワーク アクセス (Default Network Access)] を選択します。

ステップ 2 PEAP および EAP-FAST プロトコルの EAP-TLS プロトコルおよび EAP-TLS 内部方式の下の [許可ポリシーの証明書更新を可能にするために失効した証明書の認証を許可 (Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy)] チェックボックスをオンにします。

EAP-TLS プロトコルを使用する要求が NSP フローを通過します。

PEAP および EAP-FAST プロトコルについては、要求を処理するように Cisco ISE 向け Cisco AnyConnect を手動で設定する必要があります。

ステップ 3 [送信 (Submit)] をクリックします。

次のタスク

[CWA リダイレクションの許可ポリシー プロファイルの作成 \(189 ページ\)](#)

CWA リダイレクションの許可ポリシー プロファイルの作成

始める前に

WLC で制限されたアクセス ACL が設定されていることを確認します。

ステップ 1 [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] > [許可 (Authorization)] > [許可プロファイル (Authorization Profiles)] を選択します。

ステップ 2 [追加 (Add)] をクリックします。

ステップ 3 許可プロファイルの名前を入力します。たとえば、CertRenewal_CWA です。

ステップ 4 [共通タスク (Common Tasks)] 領域の [Web リダイレクション (CWA、DRW、MDM、NSP、CPP) (Web Redirection (CWA, DRW, MDM, NSP, CPP))] チェックボックスをオンにします。

ステップ 5 ドロップダウン リストの [中央集中 Web 認証 (Centralized Web Auth)] および制限されたアクセス ACL を選択します。

ステップ 6 [証明書更新メッセージの表示 (Display Certificates Renewal Message)] チェックボックスをオンにします。
url-redirect 属性値が変更され、この値に証明書が有効である日数が含まれます。

ステップ 7 [送信 (Submit)] をクリックします。



(注) Cisco ISE 1.2 で無線デバイスの次のデバイス登録 WebAuth (DRW) ポリシーを設定している場合：

- 条件 = (Wireless_MAB AND Network Access:UseCase EQUALS HostLookup) およびプロファイル = Wireless-drw-redirect を含む DRW-Redirect ポリシー
- 条件 = (Wireless_MAB AND Network Access:UseCase EQUALS HostLookup) およびプロファイル = Wireless-Permit を含む DRW-Allow ポリシー

ISE 1.3 以上のバージョンにアップグレードした後は、DRW-Allow ポリシー条件を次のように更新する必要があります。

- 条件 = (Wireless_MAB AND Network Access:UseCase EQUALS Guest Flow) およびプロファイル = Wireless-Permit

次のタスク

[証明書を更新する許可ポリシー ルールの作成 \(190 ページ\)](#)

証明書を更新する許可ポリシー ルールの作成

始める前に

中央 Web 認証リダイレクションの許可プロファイルが作成されていることを確認します。

[管理 (Administration)] > [システム (System)] > [設定 (Settings)] > [ポリシーセット (Policy Sets)] でポリシー セットを有効にします。

ステップ 1 [ワーク センター (Work Centers)] > [デバイス管理 (Device Administration)] > [ポリシー セット (Policy Sets)] を選択します。

ステップ 2 [上を作成 (Create Above)] をクリックします。

ステップ 3 新しいルールの名前を入力します。

ステップ 4 次の単純条件と結果を選択します。

CertRenewalRequiredEQUALS True の場合は、権限用に以前に作成した許可プロファイル (CertRenewal_CWA) を選択します。

ステップ 5 [保存 (Save)] をクリックします。

次のタスク

証明書が期限切れになったデバイスを持つ企業ネットワークにアクセスした場合は、[更新 (Renew)] をクリックして、デバイスを再設定します。

ゲストポータルでの BYOD 設定の有効化

ユーザがパーソナルデバイス証明書を更新できるようにするには、選択したゲストポータルで BYOD 設定を有効にする必要があります。

ステップ 1 [ワークセンター (Work Centers)] > [ゲストアクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [ゲストポータル (Guest Portals)] を選択します。

a) 目的の CWA ポータルを選択して、[編集 (Edit)] をクリックします。

ステップ 2 [BYOD 設定 (BYOD Settings)] から [従業員にネットワークでのパーソナルデバイスの使用を許可する (Allow employees to use personal devices on the network)] チェックボックスをオンにします。

ステップ 3 [保存 (Save)] をクリックします。

Apple iOS デバイスの証明書更新の失敗

ISE を使用して Apple iOS デバイスのエンドポイント証明書を更新する場合、「プロファイル済みでインストールできませんでした (Profiled Failed to Install)」エラーメッセージが表示される場合があります。このエラーメッセージは、同じポリシーサービスノード (PSN) または別の PSN で、期限切れ間近または期限切れのネットワークプロファイルが更新のプロセス時に使用されるものとは異なる管理者 HTTPS 証明書によって署名されている場合に表示されます。

回避策としては、展開内のすべての PSN で管理者 HTTPS 用にマルチドメイン SSL 証明書（通称 Unified Communications Certificates (UCC)）またはワイルドカード証明書を使用します。

Cisco ISE CA サービス

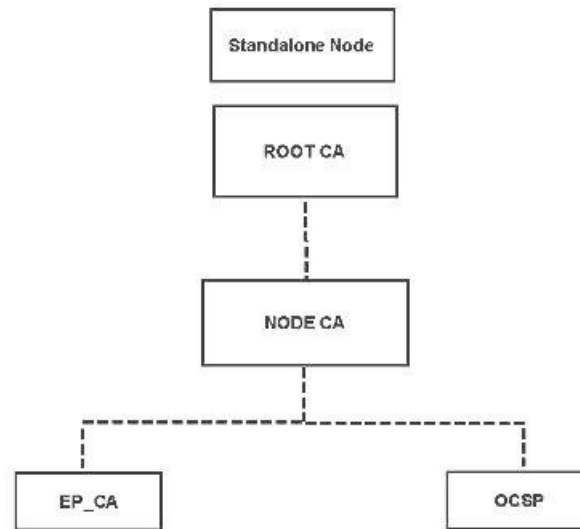
証明書は、自己署名したり、外部の認証局 (CA) がデジタルで署名したりできます。Cisco ISE 内部認証局 (ISE CA) は、従業員が企業ネットワークでパーソナルデバイスを使用できるように、一元的なコンソールからエンドポイントのデジタル証明書を発行し、管理します。CA 署名付きデジタル証明書は、業界標準であり、よりセキュアです。プライマリ PAN は、ルート CA です。ポリシーサービスノード (PSN) は、プライマリ PAN の下位 CA です (SCEP RA)。ISE CA には次の機能があります。

- 証明書の発行：ネットワークに接続するエンドポイントの証明書署名要求 (CSR) を検証し、署名します。
- キー管理：PAN ノードと PSN ノードの両方でキーと証明書を生成し、セキュアに保存します。
- 証明書ストレージ：ユーザやデバイスに発行された証明書を保存します。
- Online Certificate Status Protocol (OCSP) サポート：OCSP 応答側に証明書の有効性を確認する手段を提供します。

管理ノードとポリシー サービス ノードでプロビジョニングされる ISE CA 証明書

インストール後に、Cisco ISE ノードはルート CA 証明書およびノード CA 証明書でプロビジョニングされ、エンドポイントの証明書が管理されます。

図 6: スタンドアロンノードでプロビジョニングされる ISE CA 証明書

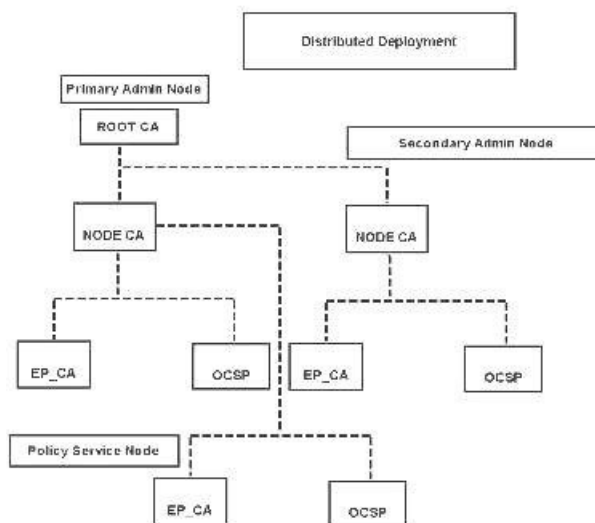


展開をセットアップすると、プライマリ管理ノード（PAN）として指定したノードがルート CA になります。PAN には、ルート CA 証明書と、ルート CA によって署名されたノード CA 証明書があります。

PAN にセカンダリ管理ノードを登録すると、ノード CA 証明書が生成され、プライマリ管理ノードでルート CA によって署名されます。

PAN に登録したポリシー サービス ノード（PSN）には、エンドポイント CA と、PAN のノード CA によって署名された OCSP 証明書がプロビジョニングされます。ポリシー サービス ノード（PSN）は、PAN の下位 CA です。ISE CA を使用すると、PSN のエンドポイント CA によってネットワークにアクセスするエンドポイントに証明書が発行されます。

図 7: 展開内の管理ノードおよびポリシー サービス ノードでプロビジョニングされる ISE CA 証明書



ISE CA チェーンの再生成

Cisco ISE CA チェーンを再生成すると、ルート CA、ノード CA、およびエンドポイント CA 証明書を含むすべての証明書が再生成されます。PAN または PSN のドメイン名またはホスト名を変更すると、ISE CA チェーンを再生成する必要があります。以前のリリースから 2.0 以降にアップグレードするときには、2 つのルート階層から 1 つのルート階層に移行するように ISE CA チェーンを再生成することをお勧めします。

楕円曲線暗号化証明書のサポート

Cisco ISE CA サービスが、楕円曲線暗号化（ECC）アルゴリズムに基づく証明書をサポートするようになりました。ECC は、他のシステムと同レベルのセキュリティをはるかに小さいキーサイズで実現し、他の暗号化アルゴリズムよりも強化されたセキュリティと優れたパフォーマンスを実現します。

暗号化とデジタル署名に必要なキーサイズが、他のシステムよりもはるかに小さくなっています。次の表に、同等のセキュリティ強度を実現するための ECC および RSA のキーサイズを示します。

ECC のキー サイズ（ビット単位）	RSA のキー サイズ（ビット単位）
160	1024
224	2048
256	3072
384	7680
521	15360

キーサイズが小さいため、このシステムでは暗号化のために必要な時間が短く、パフォーマンスが向上します。

Cisco ISE では、次の ECC 曲線タイプがサポートされています。曲線タイプまたはキー サイズが大きくなると、セキュリティが強化されます。

- P-192
- P-256
- P-384
- P-521

Cisco ISE CA サービスは、BYOD フローを介して接続するデバイスの ECC 証明書をサポートします。また、証明書プロビジョニングポータルから ECC 証明書を生成することもできます。



(注) 次の表に、ECC をサポートしているオペレーティング システムおよびバージョンと、サポートされている曲線タイプを示します。デバイスがサポートされているオペレーティング システムを実行していない場合、またはサポートされているバージョンでない場合には、代わりに RSA ベースの証明書を使用することもできます。

オペレーティング システム (Operating System)	サポートされるバージョン	サポートされる曲線タイプ
Windows	8 以降	P-256、P-384、P-521
Android	4.4 以降 (注) Android 6.0 は、ECC 証明書をサポートするために 2016 年 5 月のパッチが必要です。	すべての曲線タイプ (P-192 曲線タイプをサポートしていない Android 6.0 を除く)。

Windows 7 と Apple iOS は、EAP-TLS 認証用の ECC をネイティブでサポートしていません。Cisco ISE のこのリリースでは、Mac OS X デバイスでの ECC 証明書の使用はサポートされていません。

Enrollment over Secure Transport (EST) プロトコルを備えた BYOD フローが適切に機能しない場合は、次のことを確認します。

- 証明書サービスエンドポイントサブ CA 証明書チェーンが完全であること。証明書チェーンが完全かどうかを確認するには：
 1. [管理 (Administration)] > [システム (System)] > [証明書 (Certificates)] > [認証局 (Certificate Authority)] > [認証局証明書 (Certificate Authority Certificates)] の順に選択します。

2. 確認する証明書の横にあるチェックボックスをオンにして、[表示 (View)] をクリックします。
- CA および EST サービスが起動し、実行されていることを確認します。サービスが有効になっていない場合には、[管理 (Administration)] > [システム (System)] > [証明書 (Certificates)] > [認証局 (Certificate Authority)] > [内部 CA の設定 (Internal CA Settings)] に移動して CA サービスを有効にします。
- 2.0 以前の ISE バージョンから Cisco ISE 2.1 にアップグレードしている場合は、アップグレード後に ISE ルート CA 証明書チェーンを置き換えます。手順は次のとおりです。
 1. [管理 (Administration)] > [システム (System)] > [証明書 (Certificates)] > [証明書の管理 (Certificate Management)] > [証明書署名要求 (Certificate Signing Requests)] の順に選択します。
 2. [証明書署名要求 (CSR) の生成 (Generate Certificate Signing Requests (CSR))] をクリックします。
 3. [証明書の使用先 (Certificate(s) will be used for)] ドロップダウン リストから ISE ルート CA を選択します。
 4. [ISE ルート CA 証明書チェーンの置き換え (Replace ISE Root CA Certificate Chain)] をクリックします。



(注) Cisco ISE のこのリリースでは、EST クライアントが Cisco ISE に存在する EST サーバに対して直接認証を行うことはサポートされていません。

Android または Windows エンドポイントでのオンボーディング時に、要求が ECC ベースの証明書用である場合には、EST フローが ISE で内部的にトリガーされます。

Cisco ISE 認証局証明書

[認証局 (CA) 証明書 (Certificate Authority (CA) Certificates)] ページには、内部 Cisco ISE CA に関連するすべての証明書が表示されます。以前のリリースでは、これらの CA 証明書は信頼できる証明書ストアにありましたが、現在は [CA 証明書 (CA Certificates)] ページに移動しています。これらの証明書は、このページにノード方式で表示されます。ノードを展開して、その特定のノードの ISE CA 証明書をすべて表示することができます。プライマリおよびセカンダリ管理ノードには、ルート CA、ノード CA、下位 CA、OCSP レスポンド証明書があります。展開内の他のノードには、エンドポイント下位 CA および OCSP 証明書があります。

Cisco ISE CA サービスを有効にすると、すべてのノードでこれらの証明書が自動的に生成され、インストールされます。また、ISE ルート CA チェーン全体を置き換えると、すべてのノードでこれらの証明書が自動的に再生成され、インストールされます。手動による介入は必要ありません。

Cisco ISE CA 証明書は **Certificate Services** <エンドポイントサブ CA/ノード CA/ルート CA/OCSP レスポンダ>-<ノードのホスト名>#証明書番号という命名規則に従います。

[CA 証明書 (CA Certificates)] ページで Cisco ISE CA 証明書を編集、インポート、エクスポート、削除、表示できます。

Cisco ISE CA 証明書の編集

証明書を Cisco ISE CA 証明書ストアに追加したら、編集の設定を使用して、その証明書をさらに編集できます。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

-
- ステップ 1** [管理 (Administration)] > [システム (System)] > [証明書 (Certificates)] > [認証局 (Certificate Authority)] > [認証局証明書 (Certificate Authority Certificates)] の順に選択します。
 - ステップ 2** 編集する証明書の横にあるチェックボックスをオンにして、[編集 (Edit)] をクリックします。
 - ステップ 3** 必要に応じて編集可能なフィールドを変更します。フィールドの説明については、[証明書設定の編集 \(1158 ページ\)](#) を参照してください。
 - ステップ 4** [保存 (Save)] をクリックして、証明書ストアに対して行った変更を保存します。
-

Cisco ISE CA 証明書のエクスポート

Cisco ISE ルート CA およびノード CA 証明書をエクスポートするには、次の手順を実行します。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

-
- ステップ 1** [管理 (Administration)] > [システム (System)] > [証明書 (Certificates)] > [認証局 (Certificate Authority)] > [認証局証明書 (Certificate Authority Certificates)] を選択します。
 - ステップ 2** エクスポートする証明書の隣にあるチェックボックスをオンにし、[エクスポート (Export)] をクリックします。一度に 1 つの証明書のみをエクスポートできます。
 - ステップ 3** クライアントブラウザを実行しているファイル システムに Privacy Enhanced Mail ファイルを保存します。
-

Cisco ISE CA 証明書のインポート

エンドポイントが別の展開の Cisco ISE CA によって発行された証明書を使用してネットワークへの認証を試みる場合、Cisco ISE ルート CA、ノード CA、エンドポイントサブ CA 証明書をその展開から Cisco ISE の信頼できる証明書ストアにインポートする必要があります。

始める前に

- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。
- ISE ルート CA、ノード CA、エンドポイントサブ CA 証明書を、エンドポイント証明書が署名されている展開からエクスポートし、ブラウザが実行されているコンピュータのファイルシステムに保存します。

ステップ 1 エンドポイントが認証されている展開の管理者用ポータルにログインします。

ステップ 2 [管理 (Administration)] > [システム (System)] > [証明書 (Certificates)] > [信頼できる証明書 (Trusted Certificates)]。

ステップ 3 [インポート (Import)] をクリックします。

ステップ 4 必要に応じてフィールドの値を設定します。詳細については、[信頼できる証明書のインポート設定 \(1161 ページ\)](#) を参照してください。

クライアント証明書ベースの認証が有効である場合は、Cisco ISE により展開内の各ノードのアプリケーションサーバが再起動されます（最初に PAN のアプリケーションサーバが再起動され、続いて追加のノードのアプリケーションサーバが 1 つずつ再起動されます）。

証明書テンプレート

証明書テンプレートには、そのテンプレートに基づいて認証局 (CA) によって発行されたすべての証明書に共通のプロパティが含まれています。証明書テンプレートは、件名、サブジェクト代替名 (SAN)、キータイプ、キーサイズ、使用する必要がある SCEP RA プロファイル、証明書の有効期間、証明書がクライアントまたはサーバの認証またはその両方に使用される必要があるかどうかを指定した拡張キーの使用状況 (EKU) を定義します。内部 Cisco ISE CA (ISE CA) は、証明書テンプレートを使用し、そのテンプレートに基づいて証明書を発行します。

Cisco ISE には、次の ISE CA のデフォルトの証明書テンプレートが付属しています。必要に応じて、追加の証明書テンプレートを作成できます。デフォルトの証明書テンプレートは次のとおりです。

- **CA_SERVICE_Certificate_Template** : Cisco ISE を認証局として使用するその他のネットワーク サービス用。たとえば、ASA VPN ユーザに対し証明書を発行するには、ISE の設定時にこの証明書テンプレートを使用します。この証明書テンプレートでは、有効期間のみを変更できます。
- **EAP_Authentication_Certificate_Template** : EAP 認証用。
- **pxGrid_Certificate_Template** : 証明書プロビジョニングポータルから証明書を生成するときの pxGrid コントローラ用。

証明書テンプレート名の拡張子

Cisco ISE の内部 CA には、エンドポイント証明書を作成するために使用された証明書テンプレートを表す拡張子が含まれています。内部 CA によって発行されたすべてのエンドポイント証明書には、証明書テンプレート名の拡張子が含まれています。この拡張子は、そのエンドポイント証明書を作成するために使用された証明書テンプレートを表します。拡張子の ID は 1.3.6.1.4.1.9.21.2.5 です。CERTIFICATE: テンプレート名属性を許可ポリシーの条件に使用して、評価の結果に基づいて適切なアクセス権限を割り当てることができます。

許可ポリシー条件での証明書テンプレート名の使用

許可ポリシー ルールで証明書テンプレート名の拡張子を使用できます。

ステップ 1 [ポリシー (Policy)] > [許可 (Authorization)] を選択します。

ステップ 2 新しいルールを追加するか、既存のルールを編集します。次に、Compliant_Device_Access ルールを編集する例を示します。

- a) Compliant_Device_Access ルールを編集します。
- b) [属性/値の追加 (Add Attribute/Value)] を選択します。
- c) ディクショナリから、**CERTIFICATE: Template Name** 属性と **Equals** 演算子を選択します。
- d) 証明書テンプレート名の値を入力します。たとえば、EAP_Authentication_Certificate_Template などです。

ステップ 3 [保存 (Save)] をクリックします。

pxGrid コントローラ用の Cisco ISE CA 証明書の展開

Cisco ISE CA は、証明書プロビジョニング ポータルから証明書を生成するための pxGrid コントローラの証明書テンプレートを提供します。

始める前に

pxGrid クライアントの証明書署名要求 (CSR) を生成し、CSR の内容をクリップボードにコピーします。

ステップ 1 ネットワーク アクセス ユーザ アカウントを作成します ([管理 (Administration)] > [ID の管理 (Identity Management)] > [ID (Identities)] > [ユーザ (Users)] > [追加 (Add)])。

ユーザが割り当てられているユーザ グループをメモします。

ステップ 2 証明書プロビジョニング ポータルの設定を編集します ([管理 (Administration)] > [デバイス ポータル管理 (Device Portal Management)] > [証明書プロビジョニング (Certificate Provisioning)])。

- a) 証明書プロビジョニング ポータルを選択して、[編集 (Edit)] をクリックします。

- b) [ポータル設定 (Portal Settings)] ドロップダウン リストをクリックします。[承認済みグループの設定 (Configure authorized groups)] の選択可能なリストから、ネットワーク アクセス ユーザが属すユーザグループを選択して、選択済みリストに移動します。
- c) [証明書プロビジョニング ポータル設定 (Certificate Provisioning Portal Settings)] ドロップダウン リストをクリックします。[pxGrid_Certificate_Template] を選択します。詳細については、[証明書プロビジョニング ポータルのポータル設定 \(1270 ページ\)](#) を参照してください。
- d) ポータル設定を保存します。

ステップ 3 証明書プロビジョニング ポータルを起動します。[ポータルテスト URL (Portal test URL)] リンクをクリックします。

- a) 手順 1 で作成したユーザ アカウントを使用して証明書プロビジョニング ポータルにログインします。
- b) AUP を受け入れ、[続行 (Continue)] をクリックします。
- c) [処理の選択 (I want to)] ドロップダウン リストから、[単一の証明書の生成 (証明書署名要求あり) (Generate a single certificate (with certificate signing request))] を選択します。
- d) [証明書署名要求の詳細 (Certificate Signing Request Details)] フィールドに、クリップボードから CSR の内容を貼り付けます。
- e) [証明書のダウンロード形式 (Certificate Download Format)] ドロップダウン リストから、[PKCS8 形式 (PKCS8 format)] を選択します。

(注) [PKCS12 形式 (PKCS12 format)] を選択する場合は、1 つの証明書ファイルを証明書ファイルとキー ファイルに分けて変換する必要があります。Cisco ISE にインポートする前に、証明書とキー ファイルはバイナリ DER エンコードまたは PEM 形式にする必要があります。

- f) [証明書テンプレートの選択 (Choose Certificate Template)] ドロップダウン リストから、[pxGrid_Certificate_Template] を選択します。
- g) 証明書のパスワードを入力します。
- h) [生成 (Generate)] をクリックします。

証明書が生成されます。

- i) 証明書をエクスポートします。

証明書チェーンとともに証明書がエクスポートされます。

ステップ 4 pxGrid クライアントの信頼できる証明書ストアに Cisco ISE CA チェーンをインポートします。

Simple Certificate Enrollment Protocol プロファイル

ユーザがネットワークで登録できるさまざまなモバイルデバイスの証明書のプロビジョニング機能を有効にするために、1 つ以上の Simple Certificate Enrollment Protocol (SCEP) 認証局 (CA) プロファイル (Cisco ISE 外部 CA 設定と呼ばれます) を設定して、Cisco ISE に複数の CA の場所を指定できます。複数のプロファイルを使用できる利点は、ハイアベイラビリティを実現し、指定した CA の場所の間でロード バランシングを実行できることです。特定の SCEP CA への要求に 3 回連続して応答がなかった場合、Cisco ISE は特定のサーバが使用不能であると

宣言し、次に負荷が小さく応答時間が短い既知の CA に自動的に移動し、サーバがオンラインに復帰するまで、定期的なポーリングを開始します。

Microsoft SCEP サーバを Cisco ISE と相互運用するように設定する方法については、次を参照してください。

http://www.cisco.com/en/US/solutions/collateral/ns340/ns414/ns742/ns744/docs/howto_60_byod_certificates.pdf

発行された証明書

管理者ポータルには、内部 ISE CA によってエンドポイントに対して発行されたすべての証明書のリストが示されます（[管理（Administration）]>[システム（System）]>[証明書（Certificates）]>[エンドポイント証明書（Endpoint Certificates）]）。[発行された証明書（Issued Certificates）] ページでは、証明書ステータスを一目で確認できます。証明書が失効している場合は、[ステータス（Status）] 列の上にマウスカーソルを移動すると、失効の理由を確認できます。[証明書テンプレート（Certificate Template）] 列の上にマウスカーソルを移動すると、キータイプ、キーサイズ、曲線タイプ、サブジェクト、サブジェクト代替名（SAN）、証明書の有効性などの詳細情報を表示できます。エンドポイント証明書をクリックして、証明書を表示できます。

ISE CA によって発行されたすべての証明書（BYOD フローを介して自動的にプロビジョニングされた証明書と証明書プロビジョニングポータルから取得された証明書）は、[エンドポイント証明書（Endpoint Certificates）] ページにリストされます。このページからこれらの証明書を管理できます。

たとえば user7 に発行された証明書を確認する場合は、[フレンドリ名（Friendly Name）] フィールドの下に表示されるテキストボックスに「user7」と入力します。このユーザに Cisco ISE によって発行されたすべての証明書が表示されます。フィルタをキャンセルするには、テキストボックスから検索語を削除します。また、[拡張フィルタ（Advanced Filter）] オプションを使用して、さまざまな検索基準に基づいてレコードを表示することもできます。

この [エンドポイント証明書（Endpoint Certificates）] ページには、必要に応じてエンドポイント証明書を取り消すためのオプションもあります。

[証明書管理概要（Certificate Management Overview）] ページには、展開内の各 PSN ノードによって発行されたエンドポイント証明書の合計数が表示されます。また、失効した証明書の合計数と失敗した証明書の合計数をノードごとに確認することもできます。このページのデータは任意の属性に基づいてフィルタリングできます。



（注） pxGrid 証明書は、[エンドポイント証明書（Endpoint Certificates）] [発行された証明書（Issued Certificates）] ページに表示されません。

Cisco ISE CA 証明書およびキーのバックアップと復元

PPAN に障害が発生し、セカンダリ管理ノードを外部 PKI のルート CA または中間 CA として機能させるために昇格する場合に備え、Cisco ISE CA 証明書およびキーをセキュアにバック

アップして、セカンダリ管理ノードにこれらを復元できるようにする必要があります。Cisco ISE 設定のバックアップには、CA 証明書とキーは含まれていません。CA 証明書およびキーをリポジトリにエクスポートおよびインポートするには、代わりにコマンドラインインターフェイス (CLI) を使用する必要があります。**application configure ise** コマンドには、CA 証明書およびキーのバックアップと復元のための、エクスポートおよびインポートオプションが含まれています。

信頼できる証明書ストアからの次の証明書が、セカンダリ管理ノードで復元されます。

- Cisco ISE ルート CA 証明書
- Cisco ISE サブ CA 証明書
- Cisco ISE エンドポイント RA 証明書
- Cisco ISE OCSP 応答側証明書

次の場合、Cisco ISE CA 証明書およびキーのバックアップおよび復元が必要となります。

- 展開内にセカンダリ管理ノードが存在する
- Cisco ISE CA ルート チェーン全体を置き換える
- 外部 PKI の下位 CA として機能するように Cisco ISE ルート CA を設定する
- リリース 1.2 からそれ以降のリリースにアップグレードする
- 設定のバックアップからデータを復元する。この場合、最初に Cisco ISE CA ルート チェーンを再生成し、次に ISE CA 証明書およびキーのバックアップと復元を行う必要があります。

関連トピック

[Cisco ISE CA 証明書およびキーのエクスポート](#) (201 ページ)

[Cisco ISE CA 証明書およびキーのインポート](#) (202 ページ)

Cisco ISE CA 証明書およびキーのエクスポート

CA 証明書およびキーを PAN からエクスポートし、セカンダリ管理ノードでインポートする必要があります。このオプションでは、PAN がダウンした場合にセカンダリ管理ノードでエンドポイントの証明書を発行および管理し、セカンダリ管理ノードを PAN に昇格させることができます。

始める前に

CA 証明書およびキーを格納するためのリポジトリを作成したことを確認します。

ステップ 1 Cisco ISE CLI から **application configure ise** コマンドを入力します。

ステップ 2 7 を入力して、証明書およびキーをエクスポートします。

ステップ 3 リポジトリの名前を入力します。

ステップ 4 暗号キーを入力します。

エクスポートされた証明書のリスト、件名、発行者、およびシリアル番号とともに成功メッセージが表示されます。

例：

```
The following 4 CA key pairs were exported to repository 'sftp' at 'ise_ca_key_pairs_of_ise-vm1':
Subject:CN=Cisco ISE Self-Signed CA of ise-vm1
Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
Serial#:0x621867df-568341cd-944cc77f-c9820765

Subject:CN=Cisco ISE Endpoint CA of ise-vm1
Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
Serial#:0x7027269d-d80a406d-831d5c26-f5e105fa

Subject:CN=Cisco ISE Endpoint RA of ise-vm1
Issuer:CN=Cisco ISE Endpoint CA of ise-vm1
Serial#:0x1a65ec14-4f284da7-9532f0a0-8ae0e5c2

Subject:CN=Cisco ISE OSCP Responder Certificate of ise-vm1
Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
Serial#:0x6f6d4097-21f74c4d-8832ba95-4c320fb1
ISE CA keys export completed successfully
```

Cisco ISE CA 証明書およびキーのインポート

セカンダリ管理ノードを登録したら、PAN から CA 証明書およびキーをエクスポートし、セカンダリ管理ノードにインポートします。

ステップ 1 Cisco ISE CLI から **application configure ise** コマンドを入力します。

ステップ 2 8 を入力して、CA 証明書およびキーをインポートします。

ステップ 3 リポジトリの名前を入力します。

ステップ 4 インポートするファイルの名前を入力します。

ステップ 5 ファイルを復号化するための暗号キーを入力します。

処理が正常に完了したことを知らせるメッセージが表示されます。

例：

```
The following 4 CA key pairs were imported:
Subject:CN=Cisco ISE Self-Signed CA of ise-vm1
Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
Serial#:0x21ce1000-8008472c-a6bc4fd9-272c8da4

Subject:CN=Cisco ISE Endpoint CA of ise-vm1
Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
Serial#:0x05fa86d0-092542b4-8ff68ed4-f1964a56

Subject:CN=Cisco ISE Endpoint RA of ise-vm1
Issuer:CN=Cisco ISE Endpoint CA of ise-vm1
Serial#:0x77932e02-e8c84b3d-b27e2f1c-e9f246ca

Subject:CN=Cisco ISE OSCP Responder Certificate of ise-vm1
Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
Serial#:0x5082017f-330e412f-8d63305d-e13fd2a5
```



```
Stopping ISE Certificate Authority Service...
Starting ISE Certificate Authority Service...
ISE CA keys import completed successfully
```

プライマリ PAN および PSN でのルート CA および下位 CA の生成

展開をセットアップする場合、Cisco ISE は、プライマリ PAN でルート CA を生成し、ポリシー サービス ノード (PSN) で Cisco ISE CA サービスに対する下位 CA 証明書を生成します。ただし、プライマリ PAN または PSN のドメイン名またはホスト名を変更する場合は、プライマリ PAN でルート CA、PSN で下位 CA をそれぞれ再生成する必要があります。

PSN のホスト名を変更する場合は、プライマリ PAN および PSN でそれぞれルート CA と下位 CA を再生成する代わりに、ホスト名を変更する前に PSN を登録解除し、再登録できます。新しい下位証明書は PSN 上で自動的にプロビジョニングされます。

- ステップ 1 [管理 (Administration)] > [システム (System)] > [証明書 (Certificates)] > [証明書署名要求 (Certificate Signing Requests)] を選択します。
 - ステップ 2 [証明書署名要求 (CSR) の生成 (Generate Certificate Signing Requests (CSR))] をクリックします。
 - ステップ 3 [証明書の使用先 (Certificate(s) will be used for)] ドロップダウンリストから ISE ルート CA を選択します。
 - ステップ 4 [ISE ルート CA 証明書チェーンの置き換え (Replace ISE Root CA Certificate chain)] をクリックします。
- ルート CA と下位 CA 証明書が、展開内のすべてのノードに対して生成されます。

次のタスク

展開にセカンダリ PAN がある場合は、プライマリ PAN から Cisco ISE CA 証明書およびキーのバックアップを取得し、セカンダリ PAN で復元します。これにより、プライマリ PAN の障害が発生した場合に、セカンダリ PAN がルート CA として機能するようになり、セカンダリ PAN をプライマリ PAN に昇格させることができます。

関連トピック

[Cisco ISE CA 証明書およびキーのバックアップと復元](#) (200 ページ)

外部 PKI の下位 CA としての Cisco ISE ルート CA の設定

外部 PKI の下位 CA として機能するプライマリ PAN のルート CA が必要な場合は、ISE 中間 CA 証明書署名要求を生成して、外部 CA に送信し、ルートおよび CA 署名付き証明書を入手して、ルート CA 証明書を信頼できる証明書ストアにインポートし、CA 署名付き証明書を CSR にバインドします。この場合、外部 CA はルート CA、プライマリ PAN は外部 CA の下位 CA、PSN はプライマリ PAN の下位 CA です。

-
- ステップ 1** [管理 (Administration)] > [システム (System)] > [証明書 (Certificates)] > [証明書署名要求 (Certificate Signing Requests)]。
- ステップ 2** [証明書署名要求 (CSR) の生成 (Generate Certificate Signing Requests (CSR))] をクリックします。
- ステップ 3** [証明書の使用目的 (Certificate(s) will be used for)] ドロップダウン リストから [ISE 中間 CA (ISE Intermediate CA)] を選択します。
- ステップ 4** [生成 (Generate)] をクリックします。
- ステップ 5** CSR をエクスポートし、外部 CA に送信して、CA 署名付き証明書を取得します。
- ステップ 6** 信頼できる証明書ストアに外部 CA のルート CA 証明書をインポートします。
- ステップ 7** CSR に CA 署名付き証明書をバインドします。
-

次のタスク

展開にセカンダリ PAN がある場合は、プライマリ PAN から Cisco ISE CA 証明書およびキーのバックアップを取得し、セカンダリ PAN で復元します。これにより、プライマリ PAN の障害が発生した場合に、セカンダリ PAN が外部 PKI の下位 CA として機能するようになり、セカンダリ PAN をプライマリ PAN に昇格させることができます。

関連トピック

[Cisco ISE CA 証明書およびキーのバックアップと復元 \(200 ページ\)](#)

証明書を使用してパーソナル デバイスを許可するための Cisco ISE の設定

ネットワークに接続するエンドポイント (パーソナルデバイス) の証明書を発行し、管理するように Cisco ISE を設定できます。内部 Cisco ISE 認証局 (CA) サービスを使用して、エンドポイントから証明書署名要求 (CSR) に署名したり、外部 CA に CSR を転送したりすることができます。

始める前に

- プライマリ PAN から Cisco ISE CA 証明書およびキーのバックアップを取得し、ディザスタ リカバリのため、安全な場所に保管してください。
- 展開にセカンダリ PAN がある場合は、プライマリ PAN から Cisco ISE CA 証明書およびキーをバックアップし、セカンダリ PAN で復元します。

ステップ 1 [Employee ユーザ グループへのユーザの追加 \(205 ページ\)](#)

内部 ID ストアまたは Active Directory などの外部 ID ストアにユーザを追加できます。

ステップ 2 [TLS ベース認証の証明書認証プロファイルの作成 \(206 ページ\)](#)

ステップ 3 [TLS ベース認証の ID ソース順序の作成 \(206 ページ\)](#)

ステップ 4 クライアント プロビジョニング ポリシーを作成します。

- a) [認証局の設定 \(207 ページ\)](#)
- b) [CA テンプレートの作成 \(208 ページ\)](#)
- c) [クライアント プロビジョニング ポリシーで使用されるネイティブ サプリカント プロファイルの作成 \(210 ページ\)](#)
- d) [Cisco サイトからの Windows および Mac OS X オペレーティング システムのエージェント リソースのダウンロード \(211 ページ\)](#)
- e) [Apple iOS、Android および MACOSX デバイスのクライアント プロビジョニング ポリシー ルールの作成 \(212 ページ\)](#)

ステップ 5 [TLS ベース認証の Dot1X 認証ポリシー ルールの設定 \(213 ページ\)](#)

ステップ 6 TLS ベース認証用の許可ポリシー ルールを設定します。

- a) [中央 Web 認証とサプリカント プロビジョニング フローの許可プロファイルの作成 \(213 ページ\)](#)
- b) [許可ポリシー ルールの作成 \(214 ページ\)](#)

パーソナル デバイスからワイヤレス SSID に接続するときに ECC RSA ベースの証明書を使用すると、2 回目のパスワード入力を行うよう求められます。

関連トピック

[外部 PKI の下位 CA としての Cisco ISE ルート CA の設定 \(203 ページ\)](#)

[Cisco ISE CA 証明書およびキーのバックアップと復元 \(200 ページ\)](#)

Employee ユーザ グループへのユーザの追加

次の手順では、Cisco ISE ID ストアの Employee ユーザ グループにユーザを追加する方法について説明します。外部 ID ストアを使用した場合でも、ユーザを追加できる Employee ユーザ グループがあることを確認します。

ステップ 1 **[管理 (Administration)] > [ID の管理 (Identity Management)] > [ID (Identities)] > [ユーザ (Users)]** を選択します。

ステップ 2 **[追加 (Add)]** をクリックします。

ステップ 3 ユーザの詳細情報を入力します。

ステップ 4 **[パスワード (Passwords)]** セクションで、**[ログインパスワード (Login Password)]** と **[TACACS+イネーブルパスワード (TACACS+ Enable Password)]** を選択し、ネットワーク デバイスにアクセス レベルを設定します。

ステップ 5 **[ユーザ グループ (User Group)]** ドロップダウン リストから **[従業員 (Employee)]** を選択します。
Employee ユーザ グループに属するすべてのユーザが同じ権限セットを共有します。

ステップ 6 **[送信 (Submit)]** をクリックします。

次のタスク

[TLS ベース認証の証明書認証プロファイルの作成 \(206 ページ\)](#)

TLS ベース認証の証明書認証プロファイルの作成

ネットワークに接続するエンドポイントの認証に証明書を使用するには、Cisco ISE で証明書認証プロファイルを定義するか、またはデフォルトの `Preloaded_Certificate_Profile` を編集する必要があります。証明書認証プロファイルには、プリンシパルユーザ名として使用する必要があります証明書フィールドが含まれています。たとえば、ユーザ名が [一般名 (Common Name)] フィールドにある場合は、証明書認証プロファイルを [プリンシパル ユーザ名 (Principal Username)] が [サブジェクト - 一般名 (Subject - Common Name)] であるとして定義できます。これは ID ストアに照らして確認できます。

-
- ステップ 1** [管理 (Administration)] > [ID の管理 (Identity Management)] > [外部 ID ソース (External Identity Sources)] > [証明書認証プロファイル (Certificate Authentication Profile)] を選択します。
- ステップ 2** 証明書認証プロファイルの名前を入力します。たとえば、CAP となります。
- ステップ 3** [サブジェクト - 一般名 (Subject - Common Name)] に [プリンシパル ユーザ名 X509 属性 (Principal Username X509 Attribute)] を選択します。
- ステップ 4** [保存 (Save)] をクリックします。
-

次のタスク

[TLS ベース認証の ID ソース順序の作成 \(206 ページ\)](#)

TLS ベース認証の ID ソース順序の作成

証明書認証プロファイルを作成したら、Cisco ISE が証明書の属性を取得し、定義した ID ソースを ID ソース順序で照合できるように、証明書認証プロファイルを ID ソース順序に追加します。

始める前に

次のタスクが完了していることを確認します。

- Employee ユーザ グループへのユーザの追加。
- 証明書ベースの認証の証明書認証プロファイルの作成。

-
- ステップ 1** [管理 (Administration)] > [ID の管理 (Identity Management)] > [ID ソース順序 (Identity Source Sequences)] を選択します。
- ステップ 2** [追加 (Add)] をクリックします。
- ステップ 3** ID ソース順序の名前を入力します。たとえば、Dot1X となります。

- ステップ 4** [証明書認証プロファイルの選択 (Select Certificate Authentication Profile)] チェックボックスをオンにし、作成した証明書認証プロファイル、つまり CAP を選択します。
- ステップ 5** ユーザ情報を含む ID ソースを [認証検索リスト (Authentication Search List)] 領域の [選択済み (Selected)] リスト ボックスに移動します。
- 追加の ID ソースを追加すると、一致が見つかるまで Cisco ISE は、これらのデータ ストアを順に検索します。
- ステップ 6** [ユーザが見つからなかったとして処理し、順序内の次のストアに進む (Treat as if the user was not found and proceed to the next store in the sequence)] オプション ボタンをクリックします。
- ステップ 7** [送信 (Submit)] をクリックします。

次のタスク

[認証局の設定 \(207 ページ\)](#)

認証局の設定

CSR への署名に外部 CA を使用する場合、外部 CA を設定する必要があります。外部 CA 設定は Cisco ISE の以前のリリースでは、SCEP RA プロファイルと呼ばれていました。Cisco ISE CA を使用する場合、CA 設定を明示的に設定する必要はありません。[管理 (Administration)] > [システム (System)] > [証明書 (Certificates)] > [内部 CA 設定 (Internal CA Settings)] で、内部 CA 設定を確認できます。

ユーザのデバイスが検証済みの証明書を受信すると、証明書はデバイス上の次の表の場所に置かれます。

表 5: デバイス証明書の場所

Device	証明書ストレージの場所	アクセス方式
iPhone/iPad	標準の証明書ストア	[設定 (Settings)] > [一般 (General)] > [プロファイル (Profile)]
Android	暗号化された証明書ストア	エンドユーザに不可視です。 (注) 証明書は、[設定 (Settings)] > [ロケーションおよびセキュリティ (Location & Security)] > [ストレージのクリア (Clear Storage)] を使用して削除できます。

Device	証明書ストレージの場所	アクセス方式
Windows	標準の証明書ストア	/cmd プロンプトから mmc.exe を起動するか、または証明書スナップインで表示します。
Mac	標準の証明書ストア	[アプリケーション (Application)] > [ユーティリティ (Utilities)] > [キーチェーンアクセス (Keychain Access)]

始める前に

証明書署名要求 (CSR) への署名に外部認証局 (CA) を使用する場合は、外部 CA の URL が必要となります。

ステップ 1 [管理 (Administration)] > [システム (System)] > [証明書 (Certificates)] > [外部 CA 設定 (External CA Settings)] を選択します。

ステップ 2 [追加 (Add)] をクリックします。

ステップ 3 外部 CA 設定の名前を入力します。たとえば、EXTERNAL_SCEP などです。

ステップ 4 [URL] テキスト ボックスに、外部 CA サーバの URL を入力します。

外部 CA が到達可能かどうかを確認するには、[テスト接続 (Test Connection)] をクリックします。追加 CA サーバの URL を入力するには、[+] ボタンをクリックします。

ステップ 5 [送信 (Submit)] をクリックします。

次のタスク

[CA テンプレートの作成 \(208 ページ\)](#)

CA テンプレートの作成

証明書テンプレートは、(内部または外部 CA のために) 使用する必要がある SCEP RA プロファイル、キータイプ、キーサイズ、曲線タイプ、サブジェクト、サブジェクト代替名 (SAN)、証明書の有効期間、拡張キーの使用状況を定義します。この例では、内部 Cisco ISE CA を使用すると想定します。外部 CA テンプレートの場合、有効期間は外部 CA によって決定され、指定することはできません。

新しい CA テンプレートを作成するか、デフォルトの証明書テンプレート EAP_Authentication_Certificate_Template を編集できます。

デフォルトでは、次の CA テンプレートが Cisco ISE で使用できます。

- **CA_SERVICE_Certificate_Template** : ISE CA を使用する他のネットワーク サービス用。たとえば、ASA VPN ユーザに対し証明書を発行するには、ISE の設定時にこの証明書テンプレートを使用します。
- **EAP_Authentication_Certificate_Template** : EAP 認証用。
- **pxGrid_Certificate_Template** : 証明書プロビジョニング ポータルから証明書を生成する際の pxGrid コントローラ用。



(注) ECC キー タイプを使用する証明書テンプレートは、内部 Cisco ISE CA とのみ使用することができます。

始める前に

CA が設定されていることを確認します。

ステップ 1 [管理 (Administration)] > [システム (System)] > [CA サービス (CA Service)] > [内部 CA 証明書テンプレート (Internal CA Certificate Template)] を選択します。

ステップ 2 内部 CA テンプレートの名前を入力します。たとえば、Internal_CA_Template とします。

ステップ 3 (オプション) [組織単位 (Organizational Unit)]、[組織 (Organization)]、[市 (City)]、[州/都道府県 (State)]、[国 (Country)] フィールドに値を入力します。

証明書テンプレート フィールド ([組織ユニット (Organizational Unit)]、[組織 (Organization)]、[都市 (City)]、[州 (State)]、および [国 (Country)]) の UTF-8 文字はサポートしていません。UTF-8 文字を証明書テンプレートで使用すると、証明書プロビジョニングが失敗します。

証明書を生成する内部ユーザのユーザ名が、証明書の共通名として使用されます。Cisco ISE 内部 CA は、「+」または「*」の文字を [共通名 (Common Name)] フィールドでサポートしていません。ユーザ名に「+」または「*」の特殊文字が含まれていないことを確認してください。

ステップ 4 サブジェクト代替名 (SAN) および証明書の有効期間を指定します。

ステップ 5 キー タイプを指定します。RSA または ECC を選択します。

次の表に、ECC をサポートしているオペレーティングシステムおよびバージョンと、サポートされている曲線タイプを示します。デバイスがサポートされているオペレーティングシステムを実行していない場合、またはサポートされているバージョンでない場合には、代わりに RSA ベースの証明書を使用することもできます。

オペレーティング システム (Operating System)	サポートされるバージョン	サポートされる曲線タイプ
Windows	8 以降	P-256、P-384、P-521

オペレーティング システム (Operating System)	サポートされるバージョン	サポートされる曲線タイプ
Android	4.4 以降 (注) Android 6.0 は、ECC 証明書をサポートするために 2016 年 5 月のパッチが必要です。	すべての曲線タイプ (P-192 曲線タイプをサポートしていない Android 6.0 を除く)。

Windows 7 と Apple iOS は、EAP-TLS 認証用の ECC をネイティブでサポートしていません。Cisco ISE のこのリリースでは、Mac OS X デバイスでの ECC 証明書の使用はサポートされていません。

ネットワークのデバイスがサポートされていないオペレーティングシステム (Windows 7、MAC OS X、Apple iOS) を実行する場合は、キータイプとして RSA を選択することを推奨します。

- ステップ 6** (RSA キータイプを選択する場合に適用) キーサイズを指定します。1024 以上のキーサイズを選択する必要があります。
- ステップ 7** (ECC キータイプを選択する場合にのみ適用) 曲線タイプを指定します。デフォルトは P-384 です。
- ステップ 8** ISE 内部 CA を SCEP RA プロファイルとして選択します。
- ステップ 9** 有効期間を日数単位で入力します。デフォルトは 730 日です。有効な範囲は 1 ~ 730 です。
- ステップ 10** 拡張キーの使用状況を指定します。証明書をクライアント認証に使用する場合は、[クライアント認証 (Client Authentication)] チェックボックスにマークを付けます。証明書をサーバ認証に使用する場合は、[サーバ認証 (Server Authentication)] チェックボックスにマークを付けます。
- ステップ 11** [送信 (Submit)] をクリックします。

内部 CA 証明書テンプレートが作成され、クライアントプロビジョニングポリシーによって使用されます。

次のタスク

[クライアントプロビジョニングポリシーで使用されるネイティブサブリカントプロファイルの作成 \(210 ページ\)](#)

クライアントプロビジョニングポリシーで使用されるネイティブサブリカントプロファイルの作成

ネイティブサブリカントプロファイルを作成して、ユーザがパーソナルデバイスを企業ネットワークに含めることができます。Cisco ISE では、異なるオペレーティングシステムごとに異なるポリシールールを使用します。各クライアントプロビジョニングポリシールールには、どのオペレーティングシステムにどのプロビジョニングウィザードを使用するかを指定するネイティブサブリカントプロファイルが含まれています。

始める前に

- Cisco ISE で CA 証明書テンプレートを設定します。
- TCP ポート 8905 および UDP ポート 8905 を開き、Cisco NAC Agent、Cisco NAC Web Agent、およびサブリカントプロビジョニングウィザードのインストールを有効にしてください。ポートの使用法の詳細については、『*Cisco Identity Services Engine Hardware Installation Guide*』の付録「Cisco ISE Appliance Ports Reference」を参照してください。

-
- ステップ 1** [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] > [クライアント プロビジョニング (Client Provisioning)] > [リソース (Resources)] を選択します。
- ステップ 2** [追加 (Add)] > [ネイティブ サブリカント プロファイル (Native Supplicant Profile)] を選択します。
- ステップ 3** ネイティブ サブリカント プロファイルの名前を入力します。たとえば、EAP_TLS_INTERNAL となります。
- ステップ 4** [オペレーティング システム (Operating System)] ドロップダウン リストから [すべて (ALL)] を選択します。
- (注) MAC OS バージョン 10.10 のユーザは、デュアル SSID PEAP フローに対してプロビジョニングされた SSID に手動で接続する必要があります。
- ステップ 5** [有線 (Wired)] または [無線 (Wireless)] チェックボックスをオンにします。
- ステップ 6** [許可されるプロトコル (Allowed Protocol)] ドロップダウン リストから [TLS] を選択します。
- ステップ 7** 以前に作成した CA 証明書テンプレートを選択します。
- ステップ 8** [送信 (Submit)] をクリックします。
-

次のタスク

[Cisco サイトからの Windows および Mac OS X オペレーティングシステムのエージェント リソースのダウンロード \(211 ページ\)](#)

Cisco サイトからの Windows および Mac OS X オペレーティングシステムのエージェント リソースのダウンロード

Windows および Mac OS X オペレーティング システムでは、Cisco サイトからリモート リソースをダウンロードする必要があります。

始める前に

ネットワークのプロキシ設定が正しく設定されていることを確認し、適切なリモート ロケーションにアクセスして、クライアントプロビジョニングリソースを Cisco ISE にダウンロードできることを確認します。

-
- ステップ 1** [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [リソース (Resources)] > [クライアント プロビジョニング (Client Provisioning)] > [リソース (Resources)] を選択します。
- ステップ 2** [追加 (Add)] > [Cisco サイトのエージェントリソース (Agent resources from Cisco site)] を選択します。
- ステップ 3** [Windows] および [MAC OS X] パッケージの隣にあるチェックボックスをオンにします。必ず最新バージョンを含めます。
- ステップ 4** [保存 (Save)] をクリックします。
-

次のタスク

[Apple iOS、Android および MACOSX デバイスのクライアント プロビジョニング ポリシー ルールの作成 \(212 ページ\)](#)

Apple iOS、Android および MACOSX デバイスのクライアント プロビジョニング ポリシー ルールの作成

クライアント プロビジョニング リソース ポリシーは、どのユーザがリソース (エージェント、エージェントコンプライアンスモジュール、エージェントカスタマイズパッケージ/プロファイル) のどのバージョン (または複数のバージョン) をログイン時およびユーザセッション開始時に Cisco ISE から受信するかを決定します。

エージェントコンプライアンスモジュールをダウンロードすると、システムで使用している既存のモジュールがあれば常にそれが上書きされます。

従業員が iOS、Android、および MACOSX デバイスを持ち込むことができるようにするには、[クライアントプロビジョニングポリシー (Client Provisioning Policy)] ページでこれらの各デバイスのポリシールールを作成する必要があります。

始める前に

必要なネイティブサブリカントプロファイルを設定し、[クライアントプロビジョニングポリシー (Client Provisioning Policy)] ページから必要なエージェントをダウンロードしておく必要があります。

-
- ステップ 1** [ポリシー (Policy)] > [クライアント プロビジョニング (Client Provisioning)] を選択します。
- ステップ 2** Apple iOS、Android および MACOSX デバイスのクライアント プロビジョニング ポリシー ルールを作成します。
- ステップ 3** [保存 (Save)] をクリックします。
-

次のタスク

[TLS ベース認証の Dot1X 認証ポリシー ルールの設定 \(213 ページ\)](#)

関連トピック

[証明書サービスのクライアントプロビジョニング ポリシー ルール \(215 ページ\)](#)

[証明書サービスのクライアントプロビジョニング ポリシー ルール \(215 ページ\)](#)

TLS ベース認証の Dot1X 認証ポリシー ルールの設定

TLS ベース認証の Dot1X 認証ポリシー ルールを更新する必要があります。

始める前に

TLS ベース認証用に作成された証明書認証プロファイルが存在することを確認します。

ステップ 1 [ポリシー (Policy)] > [認証 (Authentication)] を選択します。

ステップ 2 [ルールベース (Rule-Based)] オプション ボタンをクリックします。

デフォルトのルールベースの認証ポリシーには、Dot1X 認証用のルールが含まれます。

ステップ 3 Dot1X 認証ポリシー ルールを編集します。

ステップ 4 Dot1X ポリシー ルールから [アクション (Actions)] > [新規行を上挿入 (Insert new row above)] を選択します。

ステップ 5 ルールの名前を入力します。たとえば、eap-tls と入力します。

ステップ 6 式ビルダーを使用して、Network Access:EapAuthentication が EAP-TLS に等しい場合は、以前に作成した証明書認証プロファイルを使用するというポリシー条件を作成します。

Network Access:UseCase 属性に基づいて追加のポリシー ルールを作成できます。この属性には、ポリシーを定義するために使用できる EST-CSR-Request 値が含まれるようになりました。

ステップ 7 デフォルト ルールは、そのままにします。

ステップ 8 [保存 (Save)] をクリックします。

次のタスク

[中央 Web 認証とサブリカント プロビジョニング フローの許可プロファイルの作成 \(213 ページ\)](#)

中央 Web 認証とサブリカント プロビジョニング フローの許可プロファイルの作成

許可プロファイルを定義して、証明書ベースの認証の成功後にユーザに付与するアクセスを決定します。

始める前に

ワイヤレス LAN コントローラ (WLC) に必要なアクセス コントロール リスト (ACL) が設定されていることを確認します。WLC での ACL の作成方法については、『*TrustSec How-To Guide: Using Certificates for Differentiated Access*』を参照してください。

この例では、WLC で次の ACL が作成されていると仮定します。

- NSP-ACL : ネイティブ サプリカント プロビジョニング用
- BLACKHOLE : ブラックリストに登録されているデバイスへのアクセスの制限
- NSP-ACL-Google : Android デバイスのプロビジョニング

-
- ステップ 1** [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] > [許可 (Authorization)] > [許可プロファイル (Authorization Profiles)] を選択します。
- ステップ 2** 新しい許可プロファイルを作成するには、[追加 (Add)] をクリックします。
- ステップ 3** 許可プロファイルの名前を入力します。
- ステップ 4** [アクセス タイプ (Access Type)] ドロップダウン リストから、[ACCESS_ACCEPT] を選択します。
- ステップ 5** 中央 Web 認証、Google Play の中央 Web 認証、ネイティブ サプリカント プロビジョニング、および Google のネイティブ サプリカント プロビジョニングの許可プロファイルを追加するには、[追加 (Add)] をクリックします。
- ステップ 6** [保存 (Save)] をクリックします。
-

次のタスク

[許可ポリシー ルールの作成 \(214 ページ\)](#)

関連トピック

[証明書サービスの許可プロファイル \(216 ページ\)](#)

[証明書サービスの許可プロファイル \(216 ページ\)](#)

許可ポリシー ルールの作成

Cisco ISE は、許可ポリシー ルールを評価し、ポリシー ルールで指定された許可プロファイルに基づいてネットワーク リソースへのアクセス権をユーザに付与します。

始める前に

必要な許可プロファイルを作成済みであることを確認します。

-
- ステップ 1** [ポリシー (Policy)] > [承認 (Authorization)] を選択します。
- ステップ 2** デフォルトのルールの上に追加のポリシー ルールを挿入します。
- ステップ 3** [保存 (Save)] をクリックします。
-

関連トピック

[証明書サービスの許可ポリシー ルール \(217 ページ\)](#)

[証明書サービスの許可ポリシー ルール \(217 ページ\)](#)

CA サービス ポリシーのリファレンス

ここでは、Cisco ISE CA サービスを有効にする前に作成する必要がある許可ポリシー ルールおよびクライアント プロビジョニング ポリシー ルールの詳細情報について説明します。

関連トピック

[証明書サービスのクライアント プロビジョニング ポリシー ルール](#) (215 ページ)

[証明書サービスの許可プロファイル](#) (216 ページ)

[証明書サービスの許可ポリシー ルール](#) (217 ページ)

証明書サービスのクライアント プロビジョニング ポリシー ルール

ここでは、Cisco ISE 証明書サービスを使用している場合に作成する必要があるクライアント プロビジョニング ポリシー ルールについて説明します。次の表に詳細を示します。

ルール名 (Rule Name)	ID グループ	オペレーティング システム	その他の条件	結果
iOS	任意 (Any)	Apple iOS すべて	条件	EAP_TLS_INTERNAL (以前に作成したネイティブ サブリカント プロファイル)。外部 CA を使用している場合は、外部 CA 用に作成したネイティブ サブリカント プロファイルを選択します。
Android	任意 (Any)	Android	条件	EAP_TLS_INTERNAL (以前に作成したネイティブ サブリカント プロファイル)。外部 CA を使用している場合は、外部 CA 用に作成したネイティブ サブリカント プロファイルを選択します。

ルール名 (Rule Name)	ID グループ	オペレーティングシステム	その他の条件	結果
MACOSX	任意 (Any)	MACOSX	条件	<p>ネイティブ サプリカントの設定で、次を指定してください。</p> <ol style="list-style-type: none"> 1. 構成ウィザード：シスコのサイトからダウンロードした MACOSX サプリカントのウィザードを選択します。 2. ウィザードのプロファイル：以前作成した EAP-TLS INTERNAL ネイティブ サプリカントのプロファイルを選択します。外部 CA を使用している場合は、外部 CA 用に作成したネイティブ サプリカントプロファイルを選択します。

証明書サービスの許可プロファイル

ここでは、Cisco ISE で証明書ベースの認証を有効にするために作成する必要がある許可プロファイルについて説明します。ワイヤレス LAN コントローラ (WLC) の ACL (NSP-ACL および NSP-ACL-Google) がすでに作成されている必要があります。

- CWA：このプロファイルは、中央 Web 認証フローを使用するデバイス用です。[Web 認証 (Web Authentication)] チェックボックスをオンにして、ドロップダウン リストから [中央集中 (Centralized)] を選択し、ACL テキスト ボックスに NSP-ACL を入力します。

- **CWA_GooglePlay** : このプロファイルは、中央 Web 認証フローを使用する Android デバイス用です。このプロファイルによって、Android デバイスは Google Play ストアにアクセスし、Cisco Network Setup Assistant をダウンロードできます。[Web 認証 (Web Authentication)] チェックボックスをオンにして、ドロップダウンリストから [中央集中 (Centralized)] を選択し、ACL テキスト ボックスに NSP-ACL-Google を入力します。
- **NSP** : このプロファイルは、サブリカントプロビジョニングフローを使用する非 Android デバイス用です。[Web 認証 (Web Authentication)] チェックボックスをオンにして、ドロップダウンリストから [サブリカントプロビジョニング (Supplicant Provisioning)] を選択し、ACL テキスト ボックスに NSP-ACL を入力します。
- **NSP-Google** : このプロファイルは、サブリカントプロビジョニングフローを使用する Android デバイス用です。[Web 認証 (Web Authentication)] チェックボックスをオンにして、ドロップダウンリストから [サブリカントプロビジョニング (Supplicant Provisioning)] を選択し、ACL テキスト ボックスに NSP-ACL-Google を入力します。

デフォルトの Blackhole_Wireless_Access 許可プロファイルを確認します。高度な属性設定を次のように設定する必要があります。

- Cisco:cisco-av-pair = url-redirect=https://ip:port/blacklistportal/gateway?portal=PortalID
- Cisco:cisco-av-pair = url-redirect-acl=BLACKHOLE

証明書サービスの許可ポリシー ルール

ここでは、Cisco ISE CA サービスを有効にするときに作成する必要がある許可ポリシー ルールについて説明します。

- **企業資産** : このルールは、802.1X および MSCHAPV2 プロトコルを使用して企業のワイヤレス SSID に接続する企業のデバイス用です。
- **Android_SingleSSID** : このルールは、Google Play ストアにアクセスして、プロビジョニングのために Cisco Network Setup Assistant をダウンロードする Android デバイス用です。このルールは、シングル SSID 設定に固有です。
- **Android_DualSSID** : このルールは、Google Play ストアにアクセスして、プロビジョニングのために Cisco Network Setup Assistant をダウンロードする Android デバイス用です。このルールは、デュアル SSID 設定に固有です。
- **CWA** : このルールは、中央 Web 認証フローを使用するデバイス用です。
- **NSP** : このルールは、EAP-TLS 認証の証明書を使用するネイティブ サブリカントプロビジョニングフローを使用するデバイス用です。
- **EAP-TLS** : このルールは、サブリカントプロビジョニングフローを完了したデバイスおよび証明書でプロビジョニングされるデバイス用です。デバイスには、ネットワークへのアクセス権限が付与されます。

次の表に、Cisco ISE CA サービスの許可ポリシールールを設定するときに選択する必要がある属性および値を示します。この例では、Cisco ISE で対応する許可プロファイルも設定しているものと想定します。

ルール名 (Rule Name)	条件 (Conditions)	権限 (適用される許可プロファイル)
企業資産	Corp_Assets AND (Wireless 802.1X AND Network Access:AuthenticationMethod EQUALS MSCHAPV2)	PermitAccess
Android_SingleSSID	(Wireless 802.1X AND Network Access:AuthenticationMethod EQUALS MSCHAPV2 AND Session:Device-OS EQUALS Android)	NSP_Google
Android_DualSSID	(Wireless_MAB AND Session:Device-OS EQUALS Android)	CWA_GooglePlay
CWA	Wireless_MAB	CWA
NSP	(Wireless 802.1X AND Network Access:AuthenticationMethod EQUALS MSCHAPV2)	NSP
EAP-TLS	(Wireless 802.1X AND Network Access:AuthenticationMethod EQUALS x509_PKI)	PermitAccess

ISE CA による ASA VPN ユーザへの証明書の発行

ISE CA は、ASA VPN 経由で接続しているクライアントマシンに証明書を発行します。この機能を使用して、ASA VPN 経由で接続しているエンドデバイスに証明書を自動的にプロビジョニングできます。

Cisco ISE は、Simple Certificate Enrollment Protocol (SCEP) を使用して登録を行い、証明書をクライアントマシンにプロビジョニングします。AnyConnect クライアントは、HTTPS 接続で ASA に SCEP 要求を送信します。ASA は、Cisco ISE と ASA の間に確立された HTTP 接続を介して Cisco ISE に要求を中継する前に、要求を評価し、ポリシーを適用します。Cisco ISE CA からの応答はクライアントに中継されます。ASA は、SCEP メッセージの内容を読み取ることとはできず、Cisco ISE CA のプロキシとして機能します。Cisco ISE CA は、クライアントからの SCEP メッセージを復号化し、暗号化された形式で応答を送信します。

ISE CA SCEP URL は `http://<IP Address or FQDN of ISE CA server>:9090/auth/caservice/pkiclient.exe` です。ISE ノードの FQDN を使用する場合は、ASA に接続されている DNS サーバが FQDN を解決できる必要があります。

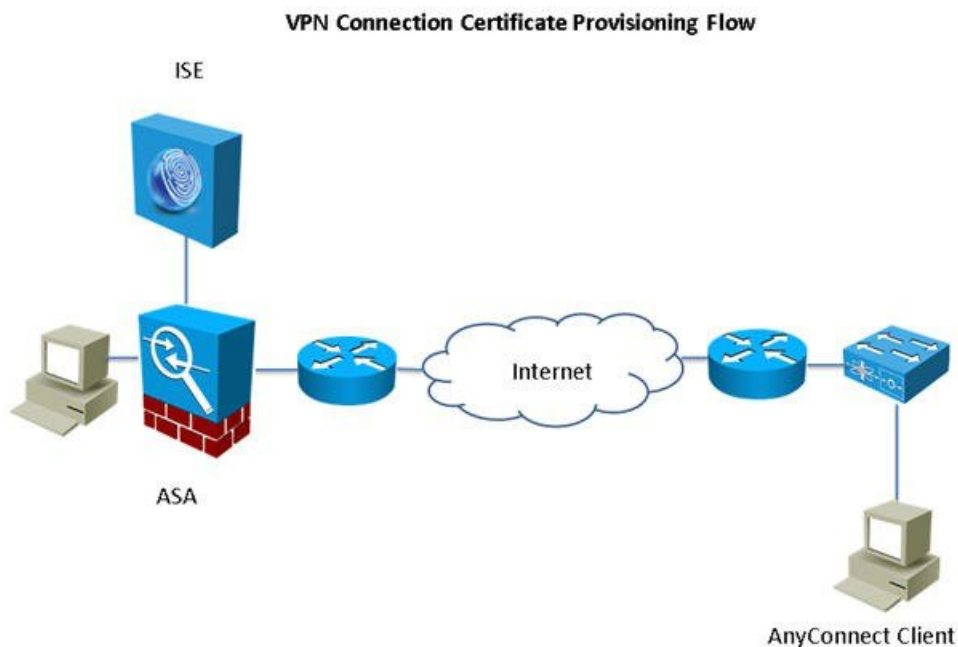
AnyConnect クライアント プロファイルの期限が切れる前に、証明書の更新を設定できます。証明書がすでに期限切れの場合、更新フローは新規登録と同様です。

サポートされているバージョンは次のとおりです。

- ソフトウェア バージョン 8.x を実行する Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス
- Cisco AnyConnect VPN バージョン 2.4 以降

VPN 接続の証明書プロビジョニングフロー

図 8: ASA VPN ユーザの証明書プロビジョニング



1. ユーザが VPN 接続を開始します。
2. AnyConnect クライアントは、クライアント マシンをスキャンし、固有デバイス識別子（たとえば IMEI）などの属性を ASA に送信します。
3. ASA はクライアントからの証明書ベースの認証を要求します。証明書がないため、認証は失敗します。
4. ASA は、ユーザ名/パスワードを使用してプライマリ ユーザ認証（AAA）に進み、情報を認証サーバ（ISE）に渡します。
 1. 認証が失敗すると、接続はただちに終了します。
 2. 認証が成功すると、制限付きアクセスが許可されます。aaa.cisco.sceprequired 属性を使用して証明書を要求するクライアント マシンでダイナミック アクセス ポリシー（DAP）を設定できます。この属性の値を「true」に設定し、ACL および Web ACL を適用できます。

5. VPN 接続は、関連するポリシーと ACL が適用された後に確立されます。クライアントは、AAA 認証が成功し、VPN 接続が確立された後にのみ、SCEP のキー生成を開始します。
6. クライアントは、SCEP 登録を開始し、HTTP を介して ASA に SCEP 要求を送信します。
7. ASA は、要求のセッション情報を検索し、セッションが登録を許可されている場合は、ISE CA に要求をリレーします。
8. ASA は ISE CA からの応答をクライアントにリレー バックします。
9. 登録が成功すると、クライアントにユーザに対する設定可能メッセージが表示され、VPN セッションが接続解除されます。
10. ユーザは証明書を使用して再度認証を行うことができ、正常な VPN 接続が確立されます。

ASA VPN ユーザに証明書を発行する Cisco ISE CA の設定

ASA VPN ユーザに証明書をプロビジョニングするには、Cisco ISE および ASA で次の設定を行う必要があります。

始める前に

- VPN ユーザ アカウントが Cisco ISE の内部または外部の ID ソースに存在することを確認します。
- ASA および Cisco ISE のポリシー サービス ノードが同じ NTP サーバを使用して同期されていることを確認します。

ステップ 1 Cisco ISE で ASA をネットワーク アクセス デバイスとして定義します。ネットワーク デバイスとして ASA を追加する方法については、[Cisco ISE でのネットワーク デバイス定義の作成 \(220 ページ\)](#) を参照してください。

ステップ 2 [ASA でのグループ ポリシーの設定 \(221 ページ\)](#)。

ステップ 3 [SCEP 登録用の AnyConnect 接続プロファイルの設定 \(221 ページ\)](#)。

ステップ 4 [ASDM での VPN クライアント プロファイルの設定 \(222 ページ\)](#)。

ステップ 5 [ASA への Cisco ISE CA 証明書のインポート](#)。

Cisco ISE でのネットワーク デバイス定義の作成

Cisco ISE にネットワーク デバイス定義がない場合に Cisco ISE でネットワーク デバイス定義を作成し、デフォルトのネットワーク デバイス定義を使用できます。

[ワークセンター (Work Centers)] > [デバイス管理 (Device Administration)] > [ネットワークリソース (Network Resources)] > [ネットワークデバイス (Network Devices)] ページで、ネットワーク デバイスの定義を作成することもできます。

-
- ステップ 1** [管理 (Administration)] > [ネットワーク リソース (Network Resources)] > [ネットワーク デバイス (Network Devices)] を選択します。
- ステップ 2** [追加 (Add)] をクリックします。
- ステップ 3** 必須フィールドをすべて指定します。
- ステップ 4** [RADIUS 認証設定 (RADIUS Authentication Settings)] チェックボックスをオンにして、RADIUS プロトコル認証を設定します。
- ステップ 5** [TACACS 認証設定 (TACACS Authentication Settings)] チェックボックスをオンにして、TACACS プロトコル認証を設定します。
- ステップ 6** (任意) [SNMP の設定 (SNMP Settings)] チェックボックスをオンにして、デバイス情報を収集するプロファイリングサービスの簡易ネットワーク管理プロトコルを設定します。
- ステップ 7** (任意) TrustSec 対応デバイスを設定するには [高度な TrustSec 設定 (Advanced Trustsec Settings)] チェックボックスをオンにします。
- ステップ 8** [送信 (Submit)] をクリックします。
-

ASA でのグループポリシーの設定

ASA でグループポリシーを設定し、SCEP 登録要求を転送するための AnyConnect 用の ISE CA URL を定義します。

-
- ステップ 1** Cisco ASA ASDM にログインします。
- ステップ 2** 左側の [リモートアクセスVPN (Remote Access VPN)] ナビゲーション ペインから、[グループポリシー (Group Policies)] をクリックします。
- ステップ 3** [追加 (Add)] をクリックして、グループポリシーを作成します。
- ステップ 4** グループポリシーの名前を入力します。たとえば、ISE_CA_SCEP のようになります。
- ステップ 5** [SCEP 転送 URL (SCEP forwarding URL)] フィールドで、[継承 (Inherit)] チェックボックスをオフにして、ポート番号を含む ISE SCEP URL を入力します。

ISE ノードの FQDN を使用する場合は、ASA に接続されている DNS サーバが ISE ノードの FQDN を解決できる必要があります。

例 :

http://ise01.cisco.com:9090/auth/caservice/pkiclient.exe.

- ステップ 6** [OK] をクリックして、グループポリシーを保存します。
-

関連トピック

[ISE CA SCEP URL](#)

SCEP 登録用の AnyConnect 接続プロファイルの設定

ISE CA サーバ、認証方式、および ISE CA SCEP URL を指定するには、ASA で AnyConnect 接続プロファイルを設定します。

ASDM での VPN クライアント プロファイルの設定

-
- ステップ 1** Cisco ASA ASDM にログインします。
- ステップ 2** 左側の [リモートアクセスVPN (Remote Access VPN)] ナビゲーション ペインから、[AnyConnect接続プロファイル (AnyConnect Connection Profiles)] をクリックします。
- ステップ 3** [追加 (Add)] をクリックして、接続プロファイルを作成します。
- ステップ 4** 接続プロファイルの名前を入力します。たとえば、**Cert-Group** と入力します。
- ステップ 5** (オプション) [エイリアス (Aliases)] フィールドに接続プロファイルの説明を入力します。たとえば、**SCEP-Call-ASA** とします。
- ステップ 6** [認証 (Authentication)] 領域で、次の情報を指定します。
- [方式 (Method)] : [両方 (Both)] オプション ボタンをクリックします
 - [AAAサーバグループ (AAA Server Group)] : [管理 (Manage)] をクリックして ISE サーバを選択します
- ステップ 7** [クライアントアドレスの割り当て (Client Address Assignment)] 領域で、使用する DHCP サーバおよびクライアント アドレス プールを選択します。
- ステップ 8** [デフォルトグループポリシー (Default Group Policy)] 領域で、[管理 (Manage)] をクリックし、ISE SCEP URL とポート番号で作成したグループ ポリシーを選択します。
- 例 :
- たとえば、ISE_CA_SCEP のようになります。
- ステップ 9** [詳細設定 (Advanced)] > [一般 (General)] を選択し、この接続プロファイルに対して [Simple Certificate Enrollment Protocolを有効にする (Enable Simple Certificate Enrollment Protocol)] チェックボックスをオンにします。
- ステップ 10** [OK] をクリックします。
AnyConnect 接続プロファイルが作成されます。
-

次のタスク

ASDM での VPN クライアント プロファイルの設定

SCEP 登録用に AnyConnect で VPN クライアント プロファイルを設定します。

-
- ステップ 1** Cisco ASA ASDM にログインします。
- ステップ 2** 左側の [リモートアクセスVPN (Remote Access VPN)] ナビゲーション ペインから、[AnyConnectクライアントプロファイル (AnyConnect Client Profile)] をクリックします。
- ステップ 3** 使用するクライアント プロファイルを選択して [編集 (Edit)] をクリックします。
- ステップ 4** 左側の [プロファイル (Profile)] ナビゲーション ペインで、[証明書の登録 (Certificate Enrollment)] をクリックします。
- ステップ 5** [証明書の登録 (Certificate Enrollment)] チェックボックスをオンにします。
- ステップ 6** 次のフィールドに値を入力します。

- [証明書失効しきい値 (Certificate Expiration Threshold)] : AnyConnect がユーザに対して証明書の失効が近づいていることを証明書の有効期限の何日前に警告するか (SCEP が有効な場合はサポートされません)。デフォルトは 0 (警告は表示しない) です。値の範囲は 0 ~ 180 日です。
- [自動SCEPホスト (Automatic SCEP Host)] : SCEP 証明書取得が設定されている ASA のホスト名および接続プロファイル (トンネル グループ) を入力します。ASA の完全修飾ドメイン名 (FQDN) または接続プロファイル名を入力してください。たとえば、ホスト名 `asa.cisco.com`、接続プロファイル名 `Cert_Group` などです。
- [CA URL] : SCEP CA サーバを識別します。ISE サーバの FQDN または IP アドレスを入力します。たとえば、`http://ise01.cisco.com:9090/auth/caservice/pkiclient.exe` などです。

ステップ 7 証明書の内容をクライアントが要求する方法を定義する値を [証明書の内容 (Certificate Contents)] に入力します。

ステップ 8 [OK] をクリックします。

AnyConnect クライアントプロファイルが作成されます。詳細については、『[Cisco AnyConnect Secure Mobility Client Administrator Guide](#)』を参照してください。

ASA への Cisco ISE CA 証明書のインポート

Cisco ISE 内部 CA 証明書を ASA にインポートします。

始める前に

Cisco ISE 内部 CA 証明書をエクスポートします。[管理 (Administration)] > [システム (System)] > [証明書 (Certificates)] > [信頼できる証明書 (Trusted certificates)] に移動します。[証明書サービスノードCA (Certificate Services Node CA)] および [証明書サービスルートCA (Certificate Services Root CA)] 証明書の横にあるチェックボックスをオンにして、それらをエクスポートします。

ステップ 1 Cisco ASA ASDM にログインします。

ステップ 2 左側の [リモートアクセスVPN (Remote Access VPN)] ナビゲーションペインから、[証明書管理 (Certificate Management)] > [CA 証明書 (CA Certificates)] を選択します。

ステップ 3 [追加 (Add)] をクリックして Cisco ISE 内部 CA 証明書を選択し、ASA にインポートします。

エンドポイント証明書の失効

従業員のパーソナルデバイスに対して発行された証明書を取り消す必要がある場合は、[エンドポイント証明書 (Endpoint Certificates)] ページから取り消すことができます。たとえば、従業員のデバイスが盗難されたり、紛失したりした場合には、Cisco ISE 管理者ポータルにログインし、そのデバイスに発行された証明書を [エンドポイント証明書 (Endpoint Certificates)] ページから取り消すことができます。フレンドリ名、デバイスの一意の ID、シリアル番号に基づいて、このページのデータをフィルタリングできます。PSN (サブ CA) が侵害された場合は、[エンドポイント証明書 (Endpoint Certificates)] ページの [発行元 (Issued By)] フィー

ルドでフィルタリングすることによって、その PSN によって発行されたすべての証明書を取り消すことができます。

従業員に対して発行された証明書を取り消すときに、アクティブなセッション（その証明書を使用して認証された）がある場合、セッションは即座に終了します。証明書を取り消すと、その直後に、許可されていないユーザはリソースにアクセスできなくなります。

ステップ 1 [管理 (Administration)] > [システム (System)] > [CA サービス (CA Service)] > [エンドポイント証明書 (Endpoint Certificates)] を選択します。

ステップ 2 取り消すエンドポイント証明書の隣にあるチェックボックスをオンにし、[失効 (Revoke)] をクリックします。

フレンドリ名とデバイス タイプに基づいて証明書を検索できます。

ステップ 3 証明書を取り消す理由を入力します。

ステップ 4 [Yes] をクリックします。

OCSP サービス

Online Certificate Status Protocol (OCSP) は、x.509 デジタル証明書のステータスのチェックに使用されるプロトコルです。このプロトコルは証明書失効リスト (CRL) に代わるものであり、CRL の処理が必要となる問題に対処します。

Cisco ISE には HTTP を介して OCSP サーバと通信し、認証で証明書のステータスを検証する機能があります。OCSP のコンフィギュレーションは、Cisco ISE で設定されるいずれかの認証局 (CA) 証明書から参照できる再利用可能な設定オブジェクトで設定されます。

CRL 検証と OCSP 検証の両方または一方を CA ごとに設定できます。両方を選択すると、Cisco ISE では最初に OCSP を介した検証が実行されます。プライマリ OCSP サーバとセカンダリ OCSP サーバの両方で通信の問題が検出された場合、または特定の証明書に対して不明のステータスが返された場合、Cisco ISE は CRL チェックの実行に切り替えます。

Cisco ISE CA サービスの Online Certificate Status Protocol レスポンド

Cisco ISE CA OCSP 応答側は、OCSP クライアントと通信するサーバです。Cisco ISE CA の OCSP クライアントには、Cisco ISE の内部 OCSP クライアントと適応型セキュリティ アプライアンス (ASA) の OCSP クライアントがあります。OCSP クライアントは、RFC 2560、5019 で定義されている OCSP 要求/応答構造を使用して、OCSP 応答側と通信する必要があります。

Cisco ISE CA は、OCSP 応答側に証明書を発行します。OCSP 応答側は、着信要求をポート 2560 でリッスンします。このポートは、OCSP トラフィックのみを許可するように設定されています。

OCSP 応答側は RFC 2560、5019 で規定された構造に従って要求を受け入れます。OCSP 要求ではナンズ拡張がサポートされます。OCSP 応答側は証明書のステータスを取得し、OCSP 応答

を作成して署名します。OCSP 応答は、OCSP 応答側ではキャッシュされませんが、クライアントでは最大24時間OCSP 応答をキャッシュすることができます。OCSP クライアントでは、OCSP 応答の署名を検証する必要があります。

PAN 上の自己署名 CA 証明書（ISE が外部 CA の中間 CA として機能する場合は、中間 CA 証明書）によって、OCSP 応答側証明書が発行されます。PAN 上のこの CA 証明書によって、PAN および PSN の OCSP 証明書が発行されます。この自己署名 CA 証明書は、展開全体に対するルート証明書でもあります。展開全体のすべての OCSP 証明書が、これらの証明書を使用して署名された応答を ISE で検証するために、信頼できる証明書ストアに格納されます。

OCSP 証明書のステータスの値

OCSP サービスでは、所定の証明書要求に対して次の値が返されます。

- [良好 (Good)] : ステータスの問い合わせへの肯定的な応答を示します。証明書が失効していないこと、および状態が次の時間間隔（存続可能時間）値までは良好であることを示します。
- [失効 (Revoked)] : 証明書は失効しています。
- [不明 (Unknown)] : 証明書のステータスは不明です。この OCSP 応答側の CA で証明書が発行されなかった場合、OCSP サービスはこの値を返します。
- [エラー (ERROR)] : OCSP 要求に対する応答を受信しませんでした。

OCSP ハイ アベイラビリティ

Cisco ISE では CA ごとに最大2つの OCSP サーバを設定でき、それらのサーバはプライマリおよびセカンダリ OCSP サーバと呼ばれます。各 OCSP サーバ設定には、次のパラメータが含まれます。

- [URL] : OCSP サーバの URL。
- [ナンス (Nonce)] : 要求で送信される乱数。このオプションにより、リプレイ アタックで古い通信を再利用できないことが保証されます。
- [応答の検証 (Validate Response)] : Cisco ISE は OCSP サーバから受信した応答の署名を検証します。

Cisco ISE がプライマリ OCSP サーバと通信しているときに、タイムアウト（5 秒）が発生した場合、Cisco ISE はセカンダリ OCSP サーバに切り替えます。

Cisco ISE はプライマリ サーバの再使用を試行する前に、設定可能な期間セカンダリ OCSP サーバを使用します。

OCSP の障害

3 つの一般的な OCSP 障害のシナリオは次のとおりです。

- OCSP キャッシュまたは OCSP クライアント側（Cisco ISE）の失敗による障害。

- 失敗した OCSP 応答側のシナリオ。例：

最初のプライマリ OCSP 応答側が応答せず、セカンダリ OCSP 応答側が Cisco ISE OCSP 要求に応答します。

Cisco ISE OCSP 要求からエラーまたは応答が受信されません。

OCSP 応答側が、Cisco ISE OCSP 要求への応答を提供しないか、失敗の OCSP 応答のステータスを返している可能性があります。OCSP 応答のステータス値は次のようになります。

- tryLater
- signRequired
- unauthorized
- internalError
- malformedRequest

OCSP 要求には、多数の日時チェック、署名の有効性チェックなどがあります。詳細については、エラー状態を含むすべての可能性のある状態について説明している『*RFC 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP*』を参照してください。

- 失敗した OCSP レポート

OCSP クライアント プロファイルの追加

[OCSP クライアント プロファイル (OCSP Client Profile)] ページを使用して、Cisco ISE に新しい OCSP クライアント プロファイルを追加できます。

始める前に

認証局 (CA) が非標準ポート (80 または 443 以外) で OCSP サービスを実行している場合は、そのポートで Cisco ISE と CA 間の通信を可能にするためにスイッチで ACL を設定する必要があります。次に例を示します。

```
permit tcp <source ip> <destination ip> eq <OCSP port number>
```

ステップ 1 [管理 (Administration)] > [システム (System)] > [証明書 (Certificates)] > [証明書管理 (Certificate Management)] > [OCSP クライアント プロファイル (OCSP Client Profile)] を選択します。

ステップ 2 OCSP クライアント プロファイルを追加するための値を入力します。

ステップ 3 [送信 (Submit)] をクリックします。

関連トピック

[Cisco ISE CA サービスの Online Certificate Status Protocol レスポンド](#) (224 ページ)

[OCSP 証明書のステータスの値](#) (225 ページ)

[OCSP ハイ アベイラビリティ](#) (225 ページ)

[OCSP の障害](#) (225 ページ)

[OCSP 統計情報カウンタ](#) (227 ページ)

OCSP 統計情報カウンタ

Cisco ISE では、OCSP カウンタを使用して、OCSP サーバのデータと健全性をロギングおよびモニタリングします。ロギングは 5 分ごとに実行されます。Cisco ISE はモニタリング ノードに syslog メッセージを送信し、それはローカル ストアに保持されます。ローカル ストアには過去 5 分のデータが含まれています。Cisco ISE が syslog メッセージを送信した後、カウンタは次の間隔について再計算されます。つまり、5 分後に、新しい 5 分間の間隔が再度開始されます。

次の表に、OCSP syslog メッセージとその説明を示します。

表 6: OCSP Syslog メッセージ

メッセージ	説明
OCSPPrimaryNotResponsiveCount	応答のないプライマリ要求の数
OCSPSecondaryNotResponsiveCount	応答のないセカンダリ要求の数
OCSPPrimaryCertsGoodCount	プライマリ OCSP サーバを使用して返された所定の CA の「良好な」証明書の数
OCSPSecondaryCertsGoodCount	プライマリ OCSP サーバを使用して返された所定の CA の「良好な」ステータスの数
OCSPPrimaryCertsRevokedCount	プライマリ OCSP サーバを使用して返された所定の CA の「失効した」ステータスの数
OCSPSecondaryCertsRevokedCount	セカンダリ OCSP サーバを使用して返された所定の CA の「失効した」ステータスの数
OCSPPrimaryCertsUnknownCount	プライマリ OCSP サーバを使用して返された所定の CA の「不明の」ステータスの数
OCSPSecondaryCertsUnknownCount	セカンダリ OCSP サーバを使用して返された所定の CA の「不明の」ステータスの数
OCSPPrimaryCertsFoundCount	プライマリの送信元からのキャッシュ内に見つかった証明書の数
OCSPSecondaryCertsFoundCount	セカンダリの送信元からのキャッシュ内に見つかった証明書の数

メッセージ	説明
ClearCacheInvokedCount	一定間隔の後にキャッシュのクリアがトリガーされた回数
OCSPCertsCleanedUpCount	t間隔の後にクリーンアップされたキャッシュエントリの数
NumOfCertsFoundInCache	キャッシュから実行された要求の数
OCSPCacheCertsCount	OCSP キャッシュ内に見つかった証明書の数



第 9 章

TACACS+ を使用したデバイス管理の制御

- デバイス管理 (229 ページ)
- デバイス管理ワーク センター (231 ページ)
- Cisco Secure ACS から Cisco ISE へのデータ移行 (232 ページ)
- デバイス管理の展開設定 (232 ページ)
- デバイス管理ポリシー セット (233 ページ)
- TACACS+ 認証設定と共有秘密 (233 ページ)
- デバイス管理：許可ポリシーの結果 (235 ページ)
- デバイス管理ポリシー セットの作成 (243 ページ)
- デバイス管理アクティビティのモニタ (244 ページ)
- TACACS+ のグローバル設定 (245 ページ)

デバイス管理

デバイス管理については 2 つのタイプの管理者がいます。

- デバイス管理者
- ISE 管理者

デバイス管理者は、管理対象デバイスの設定と保守を実行するために、（通常は SSH を介して）スイッチ、ワイヤレス アクセス ポイント、ルータ、ゲートウェイなどのネットワーク デバイスにログインするユーザです。ISE 管理者は、デバイス管理者がログインするデバイスの設定と調整のために ISE にログインします。

ISE にログインしてデバイス管理者の操作を制御する設定を行う ISE 管理者がこのドキュメントの対象読者です。ISE 管理者は、デバイス管理機能 ([ワークセンター (Work centers)] > [デバイス管理 (Device Administration)]) を使用して、ネットワーク デバイスの設定を制御および監査します。デバイスは、Terminal Access Controller Access-Control System (TACACS) のセキュリティ プロトコルを使用して ISE サーバにクエリを行うように設定できます。ISE モニタリング ノードでは、デバイス管理に関する高度なレポートが提供されます。ISE 管理者は、次のタスクを実行できます。

- TACACS+ の詳細（共有秘密）によるネットワーク デバイスの設定。

- 内部ユーザとしてのデバイス管理者の追加、および必要に応じてイネーブルパスワードの設定。
- コマンドセットやシェルプロファイルなどの TACACS 結果をデバイス管理アクセス サービスの許可ポリシー ルールで選択できるようにするポリシー セットの作成。
- デバイス管理者がポリシーセットに基づいてデバイスにアクセスできるようにするための ISE での TACACS サーバの設定。

デバイス管理者は、ISE サーバと通信するためのデバイスの設定タスクを実行します。デバイス管理者がデバイスにログインすると、デバイスは ISE サーバにクエリを行い、次に内部または外部の ID ストアにクエリを行い、デバイス管理者の詳細を検証します。検証が ISE サーバによって行われると、デバイスは、アカウントिंगと監査の目的で、各セッションまたはコマンド許可操作の最終結果を ISE サーバに通知します。

ISE 管理者は、TACACS および Cisco ISE 2.1 を使用してデバイスを管理できます。デバイス管理に関連する設定は、Cisco Secure Access Control System (ACS) サーバのバージョン 5.5、5.6、5.7 および 5.8 から移行することもできます。これ以前のバージョンの場合は、移行の前に 5.5 または 5.6 にアップグレードする必要があります。



- (注) [ワーク センター (Work Centers)] > [デバイス管理 (Device Administration)] > [概要 (Overview)] > [展開 (Deployment)] ページのデバイス管理サービスを有効にする必要があります。



- (注) Cisco ISE では、既存の基本またはモビリティ ライセンスに加えて TACACS+ サービスを使用するには、デバイス管理ライセンスが必要です。デバイス管理ライセンスは永久ライセンスです。以前のリリースから Cisco ISE リリース 2.0 以降にアップグレードして、TACACS+ サービスを有効にするには、個別のアドオンライセンスとしてデバイス管理ライセンスを発注する必要があります。ISE 展開全体に対し、1 つのデバイス管理ライセンスが必要です。

ISE コミュニティ リソース

デバイス管理属性については、「[ISE Device Administration Attributes](#)」を参照してください。ワイヤレス LAN コントローラ、IOS ネットワーク デバイス、Cisco NX-OS ネットワーク デバイス、およびネットワーク デバイスの TACACS+ 設定については、「[ISE Device Administration \(TACACS+\)](#)」を参照してください。

イネーブルパスワードを変更するためのコマンドラインインターフェイスへのアクセス

イネーブルパスワードを変更するには、次の手順を実行します。

始める前に

一部のコマンドは特権モードに割り当てられます。したがって、デバイスの管理者がこのモードに認証されているときしか実行できません。

そのデバイスの管理者が特権モードに入ろうとする際に、デバイスは特別なイネーブル認証タイプを送信します。Cisco ISE は、この特別なイネーブル認証タイプを検証するために別のイネーブル パスワードをサポートします。別のイネーブル パスワードはデバイスの管理者が内部 ID ストアに認証されているときに使用されます。外部 ID ストアとの認証では、同じパスワードが通常のログインに対して使用されます。

ステップ 1 スイッチにログインします。

ステップ 2 Enter を押して次のプロンプトを表示します。

```
Switch>
```

ステップ 3 次のコマンドを実行して、イネーブル パスワードを設定します。

```
Switch> enable
Password: (Press Enter to leave the password blank.)
Enter Old Password: (Enter the old password.)
Enter New Password: (Enter the new password.)
Enter New Password Confirmation: (Confirm the new password.)
```

(注) パスワードの有効期間がログイン パスワードおよびイネーブルパスワードに設定されている場合、パスワードが指定された時間期間内に変更されないと、ユーザ アカウントは無効になります。Cisco ISE が TACACS+ サーバとして構成され、ネットワーク デバイスで [バイパスを有効にする (Enable Bypass)] オプションが設定されている場合、CLI から (telnet 経由で) イネーブルパスワードを変更できません。内部ユーザのイネーブルパスワードを変更するには、[管理 (Administration)] > [ID の管理 (Identity Management)] > [アイデンティティ (Identities)] > [ユーザ (Users)] を選択します。

デバイス管理ワーク センター

[ワークセンター (Work Center)] メニューには、すべてのデバイス管理ページが含まれており、ISE 管理者の単一の始点として機能します。ただし、ユーザ、ユーザ ID グループ、ネットワーク デバイス、デフォルトネットワーク デバイス、ネットワーク デバイス グループ、認証および許可条件などのデバイス管理に固有ではないページは、[管理 (Administration)] などの元のメニュー オプションから、アクセスすることができます。[ワークセンター (Work Centers)] オプションは、正しい TACACS+ ライセンスが取得され、インストールされている場合にのみ使用できます。

[デバイス管理 (Device Administration)] メニューには、次のメニュー オプションが含まれています。[概要 (Overview)]、[ID (Identities)]、[ユーザ ID グループ (User Identity Groups)]、[外部 ID ストア (Ext ID Stores)]、[ネットワーク リソース (Network Resources)]、[ネットワーク デバイス グループ (Network Device Groups)]、[ポリシー要素 (Policy Elements)]、[デ

デバイス管理ポリシーセット (Device Admin Policy Sets)]、[レポート (Reports)] および [設定 (Settings)]。

Cisco Secure ACS から Cisco ISE へのデータ移行

移行ツールを使用して、ACS 5.5、5.6、5.7 および 5.8 からデータをインポートし、すべてのネットワーク デバイスにデフォルトの TACACS+ 秘密を設定できます。[ワーク センター (Work Centers)] > [デバイス管理 (Device Administration)] > [概要 (Overview)] に移動して、[準備 (Prepare)] セクションで、移行ツールのリンクをクリックして移行ツールを開きます[ソフトウェアのダウンロード Web ページ (Download Software Webpage)] をクリックして移行ツールをダウンロードします。ツールを PC に保存し、[migTool] フォルダから migration.bat ファイルを実行し、移行プロセスを開始します。移行に関する詳細については、『[Cisco ISE Migration Guide](#)』を参照してください。

デバイス管理の展開設定

[デバイス管理の展開 (Device Administration Deployment)] ページ ([ワーク センター (Work Centers)] > [デバイス管理 (Device Administration)] > [概要 (Overview)] > [展開 (Deployment)]) では、ISE 管理者は[展開 (deployment)] セクションで各ノードを参照する必要なく、デバイス管理システムを一元的に表示できます。

[デバイス管理の展開 (Device Administration Deployment)] ページには、展開内の PSN が一覧表示されます。これにより、展開内の各 PSN でデバイス管理サービスを個別に有効にする作業が簡単になります。次のオプションを選択することで、多くの PSN に対するデバイス管理サービスを集合的にイネーブルにできます。

オプション	説明
なし (None)	デフォルトでは、デバイス管理サービスはすべてのノードで無効になっています。
すべてのポリシーサービスノード (All Policy Service Nodes)	すべての PSN でデバイス管理サービスを有効にします。このオプションを使用すると、新しい PSN はデバイス管理のために追加されるときに自動的に有効になります。
特定のノード (Specific Nodes)	展開内のすべての PSN をリストしている [ISE ノード (ISE Nodes)] セクションが表示されます。デバイス管理サービスをイネーブルにする必要があるノードを選択できます。



(注) 展開に TACACS+ のライセンスがない場合、上記のオプションはディセーブルになります。

[TACACS+ポート (TACACS Ports)] フィールドでは、最大 4 つの TCP ポートをカンマ区切りで入力できます。ポート値の範囲は 1 ～ 65535 です。Cisco ISE ノードおよびそのインターフェイスは指定されたポートで TACACS+ 要求をリスンします。指定されたポートが他のサービスで使用されないようにする必要があります。デフォルトの TACACS+ ポート値は 49 です。

[保存 (Save)] をクリックすると、変更が [管理 (Administration)] > [システム (System)] > [展開のリスト (Deployment Listing)] ページで指定されたノードと同期されます。

デバイス管理ポリシー セット

[デバイス管理ポリシーセット (Device Admin Policy Sets)] ページ ([ワークセンター (Work Centers)] > [デバイス管理 (Device Administration)] > [デバイス管理ポリシーセット (Device Admin Policy Sets)]) には、ISE 管理者が TACACS+ デバイスマネージャの認証と許可を制御するために管理するポリシーセットのリストが含まれています。各ポリシーでは、[通常 (Regular)] および [プロキシシーケンス (Proxy Sequence)] の 2 つのモードのいずれかを使用できます。

通常のポリシー セットは認証ルール テーブルおよび許可ルール テーブルから成ります。認証ルール テーブルは、許可する必要があるプロトコルを選択するために使用される一連の「外部」ルールで構成されます。各「外部」ルールには、使用する特定の ID ストアを選択するために使用される 1 つ以上の「内部」ルールが含まれています。許可ルール テーブルは、承認ビジネスモデルを実装するために必要な特定の承認結果を選択するための一連のルールが含まれています。各ルールは、連動するようにルールに一致する必要がある 1 つ以上の条件と、許可プロセスを制御するために選択される一連のコマンドセット、および/またはシェルスクリプトで構成されます。各ポリシーセットには、特定の状況のルールを上書きするために使用できる許可例外ルールテーブルがあり、多くの場合、例外テーブルは一時的な状況に使用されます。

プロキシシーケンス ポリシーセットには、単一の選択されたプロキシシーケンスが含まれています。ポリシーセットがこのモードの場合、リモート プロキシサーバが要求の処理に使用されます (しかし、ローカル アカウンティングがプロキシシーケンスで設定されている場合があります)。

TACACS+ 認証設定と共有秘密

次の表では、ネットワーク デバイスの TACACS+ 認証を設定するために使用できる [ネットワークデバイス (Network Devices)] ページのフィールドについて説明します。ナビゲーションパスは次のとおりです。

- (ネットワーク デバイスの場合) [ワークセンター (Work Centers)] > [デバイス管理 (Device Administration)] > [ネットワークリソース (Network Resources)] > [ネットワークデバイス (Network Devices)] > [追加 (Add)] > [TACACS 認証設定 (TACACS Authentication Settings)]。
- (デフォルトのデバイスの場合) [ワークセンター (Work Centers)] > [デバイス管理 (Device Administration)] > [ネットワークリソース (Network Resources)] > [デフォルトのデバイス (Default Devices)] > [TACACS 認証設定 (TACACS Authentication)]

Settings)]。詳細については、「[Cisco ISE でのデフォルトのネットワーク デバイス定義](#)」の項を参照してください。

フィールド	使用上のガイドライン
共有秘密鍵 (Shared Secret)	TACACS+ プロトコルがイネーブルのときにネットワーク デバイスに割り当てられたテキストの文字列。ユーザは、ネットワーク デバイスによってユーザ名およびパスワードが認証される前にテキストを入力する必要があります。ユーザが共有秘密情報を提示するまで、接続は拒否されます。これは必須フィールドではありません。
廃止された共有秘密がアクティブです (Retired Shared Secret is Active)	リタイアメント期間がアクティブな場合に 표시됩니다。
廃止 (Retire)	既存の共有秘密を終了する代わりに廃止します。[廃止 (Retire)] をクリックすると、メッセージ ボックスが表示されます。[はい (Yes)] または [いいえ (No)] をクリックできます。
残りの廃止期間 (Remaining Retired Period)	<p>(上のメッセージ ボックスで [はい (Yes)] を選択した場合にのみ利用可能) 次のナビゲーション パスで指定されたデフォルト値が表示されます。[ワークセンター (Work Centers)] > [デバイス管理 (Device Administration)] > [設定 (Settings)] > [接続設定 (Connection Settings)] > [デフォルトの共有秘密リタイアメント期間 (Default Shared Secret Retirement Period)]。デフォルト値は変更することができます。</p> <p>これにより、新しい共有秘密を入力でき、古い共有秘密は指定された日数にわたってアクティブなままになります。</p>
終了 (End)	(上のメッセージ ボックスで [はい (Yes)] を選択した場合にのみ利用可能) リタイアメント期間が終了し、古い共有秘密が終了します。

フィールド	使用上のガイドライン
シングル接続モードを有効にする (Enable Single Connect Mode)	<p>ネットワークデバイスとのすべての TACACS+ 通信に単一の TCP 接続を使用する場合にオンにします。次のいずれかを実行します。</p> <ul style="list-style-type: none"> • [レガシーシスコデバイス (Legacy Cisco Devices)] • または、[TACACS+ ドラフトコンプライアンスシングル接続のサポート (TACACS+ Draft Compliance Single Connect Support)]。シングル接続モードをディセーブルにすると、ISE はすべての TACACS+ 要求に対して新しい TCP 接続を使用します。

サマリーでは、次の操作を実行できます。

- 廃止期間を日数として指定することで（範囲は 1 ～ 99 です）、古い共有秘密を廃止し、同時に新しい共有秘密を設定することができます。
- 廃止期間中は新旧の共有秘密を使用できます。
- 期限切れになる前に廃止期間を延長できます。
- 廃止期間の終了までは、古い共有秘密のみを使用できます。
- 期限切れになる前に廃止期間を終了できます（[終了 (End)] をクリックしてから [送信 (Submit)] をクリックします）。



(注) [TACACS+ 認証設定 (TACACS+ Authentication Settings)] オプションへは、[管理 (Administration)] > [ネットワークリソース (Network Resources)] > [ネットワークデバイス (Network Devices)] > [追加 (Add)] ページからアクセスすることもできます。

デバイス管理：許可ポリシーの結果

ISE 管理者は、TACACS+ コマンドセットおよび TACACS+ プロファイル（ポリシー結果）を使用して、デバイス管理者に付与される権限およびコマンドを制御することができます。ポリシーはネットワークデバイスと連動して動作するので、行われる可能性がある偶発的または悪意のある設定変更が回避されます。そのような変更が発生した場合は、デバイス管理の監査レポートを使用して、特定のコマンドを実行したデバイス管理者を追跡することができます。

関連トピック

[TACACS+ コマンドセット](#) (236 ページ)

TACACS+ プロファイル (238 ページ)

TACACS+ デバイス管理を許可された FIPS および非 FIPS モードのプロトコル

ポリシーの結果を作成するための Cisco ISE が提供する多数の許可された認証プロトコル サービスがあります。ただし、TACACS+ プロトコルに適用できる PAP/ASCII、CHAP および MS-CHAPv1 などの認証プロトコル サービスは、RADIUS の FIPS 対応 Cisco ISE アプライアンスでディセーブルになっています。その結果、FIPS 対応 ([管理 (Administration)] > [システム設定 (System Settings)] > [FIPS モード (FIPS Mode)]) Cisco ISE アプライアンスを使用している場合は、デバイスの管理のためにこれらのプロトコルを [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] > [許可されているプロトコル (Allowed Protocols)] ページで有効にすることはできません。

したがって、デバイス管理ポリシーの結果で PAP/ASCII、CHAP および MS-CHAPv1 プロトコルを設定するには、FIPS モードと非 FIPS モードのどちらの場合も、[ワークセンター (Work Centers)] > [デバイス管理 (Device Administration)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] > [許可されているプロトコル (Allowed Protocols)] ページに移動する必要があります。FIPS モードを有効にすると、デフォルト デバイス管理で許可されたプロトコル設定のみが使用できます。このオプションは、RADIUS では使用できません。

TACACS+ コマンドセット

コマンドセットは、デバイス管理者が実行できるコマンドの指定されたリストを適用します。デバイス管理者がネットワーク デバイスに対して操作コマンドを発行すると、その管理者がこれらのコマンドの発行を認可されているかどうかを判定する問い合わせが ISE に行われます。これは、コマンド認可とも呼ばれます。

コマンドセットのワイルドカードと正規表現

コマンドラインは、コマンドと 0 個以上の引数から成ります。Cisco ISE は、コマンドライン (要求) を受信すると、次のさまざまな方法でコマンドおよび引数を処理します。

- ワイルドカード照合パラダイムを使用して、要求内のコマンドをコマンドセットのリストに指定されたコマンドと照合します。

例 : Sh?? または S*

- 正規表現 (regex) 照合パラダイムを使用して、要求内の引数をコマンドセットのリストに指定された引数と照合します。

例 : Show interface[1-4] port[1-9]:tty*

コマンドラインおよびコマンドセットのリストの一致

要求されたコマンドラインをワイルドカードおよび正規表現を含むコマンドセットのリストに一致させるには、次の手順を実行します。

1. コマンドセットのリストを反復し、一致するコマンドを検出します。

ワイルドカード照合では以下が許可されています。

- 大文字小文字の区別なし
- コマンドセット内のコマンドの任意の文字を「?」にでき、要求されたコマンドに存在する必要がある個別の文字に一致させることができます。
- コマンドセット内のコマンドの任意の文字を「*」にでき、要求されたコマンド内の 0 個以上の文字に一致させることができます。

次に、例を示します。

要求	コマンドセット	一致	説明
show	show	Y	—
show	SHOW	Y	大文字小文字の区別なし
show	Sh??	Y	任意の文字と一致します
show	Sho??	N	2つ目の「?」は存在しない文字と交差します
show	S*	Y	「*」は任意の文字と一致します
show	S*w	Y	「*」は文字「ho」と一致します
show	S*p	N	文字「p」は対応しません

2. 一致する各コマンドに対し、Cisco ISE は引数を検証します。

コマンドセットのリストには、各コマンドのスペースで区切られた一連の引数が含まれています。

例：Show interface[1-4] port[1-9]:tty.*

このコマンドには、2つの引数があります。

1. 引数 1：interface[1-4]

2. 引数 2：port[1-9]:tty.*

要求内のコマンド引数は、パケットに表示される位置が重要な順序で実行されます。コマンド定義内のすべての引数が要求内の引数に一致すると、このコマンド/引数は一致していると見なされます。要求内の無関係な引数はすべて無視されることに注意してください。



(注) 引数には標準の Unix 正規表現を使用します。

複数のコマンドセットを持つルールの処理

1. コマンドセットにコマンドとその引数との一致が含まれる場合、その一致が **Deny Always** であると、ISEによってそのコマンドセットは **Commandset-DenyAlways** として指定されます。
2. コマンドセット内のコマンドの一致に **Deny Always** がない場合は、最初の一致が見つかるまで、コマンドセット内のすべてのコマンドが順番にチェックされます。
 1. 最初の一致が **Permit** である場合、そのコマンドセットは **Commandset-Permit** として指定されます。
 2. 最初の一致が **Deny** である場合、そのコマンドセットは **Commandset-Deny** として指定されます。
3. ISE は、すべてのコマンドセットを分析したあと、コマンドを次のように認可します。
 1. コマンドセットが **Commandset-DenyAlways** として指定された場合、ISEによってそのコマンドは拒否されます。
 2. **Commandset-DenyAlways** がない場合、コマンドセットが **Commandset-Permit** である場合はそのコマンドが許可されます。そうでない場合、そのコマンドは拒否されます。唯一の例外は、[不一致 (Unmatched)] チェックボックスがオンになっている場合です。

TACACS+ プロファイル

TACACS+ プロファイルは、デバイス管理者の最初のログインセッションを制御します。セッションは、個々の認証、許可、またはアカウントिंगの要求を参照します。ネットワークデバイスへのセッション許可要求により、ISE 応答が発生します。この応答には、ネットワークデバイスにより解釈されるトークンが含まれています。ネットワーク デバイスにより、セッション期間中に実行できるコマンドが制限されます。デバイス管理アクセスサービス用の許可ポリシーでは、単一のシェル プロファイルおよび複数のコマンドセットを含めることができます。TACACS+ プロファイル定義は、次の 2 つのコンポーネントに分けられています。

- 共通タスク
- カスタム属性

[TACACS+プロファイル (TACACS+ Profiles)] ページ ([ワーク センター (Work Centers)] > [デバイス管理 (Device Administration)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] > [TACACS プロファイル (TACACS Profiles)]) には、[タスク属性 (Task Attribute)] ビューと [未処理 (Raw)] ビューの 2 つのビューがあります。共通タスクは [タスク属性 (Task

Attribute)]ビューを使用して入力でき、カスタム属性は[タスク属性 (Task Attribute)]ビューおよび[未処理 (Raw)]ビューで作成できます。

[共通タスク (Common Tasks)]セクションを使用すると、頻繁に使用されるプロファイル属性を選択および設定できます。ここに含まれる属性は、TACACS+プロトコルドラフト仕様で定義された属性です。ただし、これらの値は、他のサービスからの要求の許可に使用される場合があります。[タスク属性 (Task Attribute)]ビューでは、ISE 管理者はデバイス管理者に割り当てられる権限を設定できます。一般的なタスクのタイプは次のとおりです。

- Shell
- WLC
- Nexus
- 汎用 (Generic)

[カスタム属性 (Custom Attributes)]セクションを使用すると、追加の属性を設定できます。[共通タスク (Common Tasks)]セクションで認識されていない属性のリストも提供されます。各定義は、属性名、属性が必須であるか任意であるかの指定、および属性の値で構成されています。[未処理 (Raw)]ビューでは、属性名とその値の間に等号 (=) を使用して必須属性を入力することができ、任意の属性は、属性名とその値の間にアスタリスク (*) を使用して入力できます。[未処理 (Raw)]ビューで入力された属性は、[タスク属性 (Task Attribute)]ビューの [カスタム属性 (Custom Attributes)]セクションに反映され、その逆も同様です。[未処理 (Raw)]ビューは、クリップボードから属性リスト (たとえば、別の製品の属性リスト) を ISE にコピー ペーストするためにも使用されます。カスタム属性は、非シェル サービスに対して定義できます。

共通タスク設定

共通タスクの設定ページを表示するには、[ワーク センター (Work Centers)] > [デバイス管理 (Device Administration)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] > [TACACS プロファイル (TACACS Profiles)] > [追加 (Add)] に移動します。一般的なタスク タイプは、Shell、WLC、Nexus および Generic です。

Shell

次のオプションは、ISE の管理者がデバイスの管理者権限を設定するために使用できます。

オプション	説明
デフォルトの権限 (Default Privilege)	<p>シェル認可のデバイス管理者のデフォルトの (最初の) 権限レベルをイネーブルにします。次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> • 0 ~ 15 の範囲の値を選択します。 • 必要な ID ストア属性を選択します。

オプション	説明
最大権限 (Maximum Privilege)	イネーブル認証の最大権限レベルを有効にします。0 ～ 15 の範囲の値を選択できます。
アクセスコントロールリスト (Access Control List)	ASCII 文字列 (1-251*) または必要な ID ストア属性を選択します。
自動コマンド (Auto Command)	ASCII 文字列 (1-248*) または必要な ID ストア属性を選択します。
エスケープなし (No Escape)	エスケープ文字に、次のいずれかのオプションを選択します。 <ul style="list-style-type: none"> • [True] : エスケープ防止をイネーブルにすることを指定します。 • [False] : エスケープ防止をイネーブルにしないことを指定します。 • 必要な ID ストア属性を選択します。
Timeout	0 ～ 9999 の範囲の値または必要な ID ストア属性を選択します。
アイドル時間 (Idle Time)	0 ～ 9999 の範囲の値または必要な ID ストア属性を選択します。

WLC

次のオプションは、ISE の管理者がデバイス管理者による WLC アプリケーションのタブへのアクセスを制御するために使用できます。WLC アプリケーションには次のタブが含まれます：[WLAN]、[コントローラ (Controller)]、[ワイヤレス (Wireless)]、[セキュリティ (Security)]、[管理 (Management)] および [コマンド (Commands)]。

オプション	説明
すべて (All)	デバイスの管理者はすべての WLC アプリケーションのタブにアクセスできます。
モニタ (Monitor)	デバイス管理者は WLC アプリケーションのタブへの読み取り専用アクセス権を持ちます。
ロビー (Lobby)	デバイス管理者は限定された設定の権限のみを持ちます。

オプション	説明
オン	デバイス管理者は次のチェックボックスから ISE 管理者がチェックしたタブにアクセスできます : [WLAN]、[コントローラ (Controller)]、[ワイヤレス (Wireless)]、[セキュリティ (Security)]、[管理 (Management)] および [コマンド (Commands)]。

Nexus

次のオプションは、ISE の管理者がデバイス管理者による Cisco Nexus スイッチへのアクセスを制御するために使用できます。

オプション	説明
属性の設定	ISE の管理者は、任意または必須として一般的なタスクによって生成された Nexus 属性を指定できます。
[ネットワーク ロール (Network Role)]	<p>Nexus が ISE を使用して認証するように設定されると、デバイス管理者は、デフォルトでは、読み取り専用アクセス権を持ちます。デバイス管理者は、これらのロールのいずれかに割り当てることができます。各ロールは許可された操作を定義します。</p> <ul style="list-style-type: none"> なし (None) : 権限はありません。 オペレータ (Operator) (読み取り専用) : 全 NX-OS デバイスへの完全な読み取りアクセス権を持ちます。 管理者 (Administrator) (読み取り/書き込み) : 全 NX-OS デバイスへの完全な読み取り/書き込みアクセス権を持ちます。
仮想デバイス コンテキスト (VDC)	<p>なし (None) : 権限はありません。</p> <p>オペレータ (Operator) (読み取り専用) : VDC への限定された読み取りアクセス</p> <p>管理者 (Administrator) (読み取り/書き込み) : VDC への限定された読み取り/書き込みアクセス</p>

【汎用（Generic）】

ISE 管理者は、一般的なタスクでは使用できないカスタム属性を指定するオプションを使用します。

TACACS+ コマンドセットの作成

TACACS+コマンドセットのポリシー結果を使用してポリシーセットを作成するには、次の手順を実行します。

ステップ 1 [ワークセンター（Work Centers）]>[デバイス管理（Device Administration）]>[ポリシー結果（Policy Results）]>[TACACSコマンドセット（TACACS Command Sets）]の順に選択します。

ステップ 2 [追加（Add）]をクリックします。

ステップ 3 名前と説明を入力します。

ステップ 4 [追加（Add）]をクリックして、権限の付与、コマンドおよび引数を指定します。

ステップ 5 [付与（Grant）] ドロップダウンで、以下のいずれかを選択できます。

- [許可（Permit）]：指定したコマンドを許可する場合（たとえば、permit show、permit con* Argument terminal など）。
- [拒否（Deny）]：指定したコマンドを拒否する場合（たとえば、deny mtrace）。
- [常に拒否（Deny Always）]：他のコマンドセットで許可されているコマンドをオーバーライドする場合（たとえば、clear auditlogs）。

(注) [付与（Grant）]、[コマンド（Command）]および[引数（Argument）]フィールドの列幅を増やしたり減らしたりするには、アクションアイコンをクリックします。

ステップ 6 [下にリストされていないコマンドを許可（Permit any command that is not listed below）]チェックボックスをオンにして、[付与（Grant）]列で[許可（Permit）]、[拒否（Deny）]または[常に拒否（Deny Always）]として指定されていないコマンドおよび引数を許可します。

TACACS+ プロファイルの作成

TACACS+ プロファイルを作成するには、次の手順を実行します。

ステップ 1 [ワークセンター（Work Centers）]>[デバイス管理（Device Administration）]>[ポリシー要素（Policy Elements）]>[結果（Results）]>[TACACS プロファイル（TACACS Profiles）]の順に選択します。

ステップ 2 [追加（Add）]をクリックします。

ステップ 3 [TACACSプロファイル（TACACS Profile）]セクションで、名前と説明を入力します。

ステップ 4 [タスク属性ビュー（Task Attribute View）]タブで、必要な共通タスクを確認します。[共通タスク設定（239 ページ）](#) ページを参照してください。

ステップ 5 [タスク属性ビュー (Task Attribute View)] タブの [カスタム属性 (Custom Attributes)] セクションで、[追加 (Add)] をクリックして必須属性を入力します。

デバイス管理ポリシー セットの作成

デバイス管理ポリシー セットを作成するには、次の手順を実行します。

始める前に

- TACACS+ 操作に対して、[管理 (Administration)] > [システム (System)] > [展開 (Deployment)] > [ノードの編集 (Edit Node)] > [全般設定 (General Settings)] ページの [デバイス管理サービスの有効化 (Enable Device Admin Service)] チェックボックスがオンになっていることを確認します。



(注) [ワーク センター (Work Centers)] > [デバイス管理 (Device Administration)] > [概要 (Overview)] > [導入 (Deployment)] ページでデバイス管理を有効にすることを推奨します。

- ユーザ ID グループ (たとえば System_Admin、Helpdesk など) が作成されていることを確認します。([ワークセンター (Work Centers)] > [デバイス管理 (Device Administration)] > [ユーザ ID グループ (User Identity Groups)] ページ)
- メンバー ユーザ (たとえば ABC、XYZ など) がユーザ ID グループに含まれていることを確認します。([ワークセンター (Work Centers)] > [デバイス管理 (Device Administration)] > [ID (Identities)] > [ユーザ (Users)] ページ)
- 管理が必要なデバイスで TACACS 設定を行います。(デバイスが ISE にクエリを行いやすいようにするために、[ワークセンター (Work Centers)] > [デバイス管理 (Device Administration)] > [ネットワークリソース (Network Resources)] > [ネットワークデバイス (Network Devices)] > [追加 (Add)] > [TACACS 認証設定 (TACACS Authentication Settings)] チェックボックスがイネーブルで、TACACS およびデバイスの共有秘密が同一になっています)
- デバイス タイプとロケーションに基づいたネットワーク デバイス グループが作成されていることを確認します。([ワークセンター (Work Centers)] > [デバイス管理 (Device Administration)] > [ネットワークデバイスグループ (Network Device Groups)] ページ)

ステップ 1 [ワークセンター (Work Centers)] > [デバイス管理 (Device Administration)] > [デバイス管理ポリシー セット (Device Admin Policy Sets)] の順に選択します。

ステップ 2 左側のペインで、新しいポリシーセットをその上 (下) に追加する現在のポリシーセットを選択します。

ステップ 3 左側のペインで、[上に作成 (Create Above)] をクリックして、新しいポリシー セットを作成します。

- ステップ 4** [編集 (Edit)] をクリックして、名前、説明、および条件を入力し（たとえば、名前：Device_Admin_Policy_1、説明：ISE administrator、条件：DEVICE:Device Type EQUALS Device Type#All Device Types #Cisco_switches）、その条件に基づくルールを設定します。
- ステップ 5** [完了 (Done)] をクリックします。
- ステップ 6** 必要な認証ポリシーを作成します（たとえば、名前：ATN_Internal_Users、ルール：if DEVICE:Location EQUALS Location #All Locations#Europe、条件：Allow Protocols: Device_Admin_protocols and Default: Use Internal Users。この例で、ポリシーはロケーション ヨーロッパにあるデバイスのみを照合し、デバイス管理プロトコルで定義されたプロトコルを許可し、内部ユーザに対して認証を行います）。
- ステップ 7** 必要な許可ポリシーを作成します。

例 1：ルール名：Sys_Admin_rule、条件：if SysAdmin and TACACS User Equals ABC then cmd_Sys_Admin AND Profile_priv_8。この例で、ポリシーはユーザ名 ABC のシステム管理者を照合し、指定されたコマンドの実行を許可し、特権レベル 8 を割り当てます。

例 2：ルール名：HelpDesk AND TACACS User EQUALS XYZ then cmd_HDesk_show AND cmd_HDesk_ping AND Profile_priv_1。この例で、ポリシーはユーザ名 XYZ のシステム管理者を照合し、指定されたコマンドの実行を許可し、特権レベル 1 を割り当てます。

上記の例で、

- コマンドセット cmd_Sys_Admin および cmd_HDesk は、[ワーク センター (Work Centers)] > [デバイス管理 (Device Administration)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] > [TACACS コマンドセット (TACACS Command Sets)] > [追加 (Add)] ページで作成されます。
- TACACS プロファイル Profile_Priv_1 および Profile_priv_8 は、[ワーク センター (Work Centers)] > [デバイス管理 (Device Administration)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] > [TACACS プロファイル (TACACS Profiles)] > [追加 (Add)] ページで作成されます。

(注) 承認結果を作成する際に使用できるように、ポリシー結果はポリシーセットの作成前に作成することを推奨します。

- ステップ 8** [送信 (Submit)] をクリックして、新しいポリシー セットを作成します。

デバイス管理アクティビティのモニタ

Cisco ISE では、TACACS+ で設定されたデバイスのアカウントリング、認証、許可、およびコマンドアカウントリングに関する情報を参照できる、さまざまなレポートおよびログが提供されます。オン デマンドまたはスケジュール ベースでこれらのレポートを実行できます。

- ステップ 1** [ワークセンター (Work Centers)] > [デバイス管理 (Device Administration)] > [レポート (Reports)] > [ISE レポート (ISE Reports)] の順に選択します。

また、[操作 (Operations)] > [レポート (Reports)] > [ISE レポート (ISE Reports)] ページでレポートを表示することもできます。

- ステップ 2** [レポート セレクタ (Report Selector)] で、[デバイス管理 (Device Administration)] を展開し、[認証概要 (AuthenticationSummary)]、[TACACS アカウンティング (TACACS Accounting)]、[TACACS 認証 (TACACS Authentication)]、[TACACS 許可 (TACACS Authorization)] およびレポートを表示します。
- ステップ 3** レポートを選択し、[フィルタ (Filters)] ドロップダウン リストを使用して、検索するデータを選択します。
- ステップ 4** データを表示する [時間範囲 (Time Range)] を選択します。
- ステップ 5** [実行 (Run)] をクリックします。
-

TACACS+ のグローバル設定

TACACS+ のグローバル設定を行うには、次の手順を実行します。

- ステップ 1** [ワーク センター (Work Centers)] > [デバイス管理 (Device Administration)] > [設定 (Settings)] の順に選択します。
- a) [接続設定 (Connection Settings)] タブで、必須フィールドのデフォルト値を変更できます。
- ステップ 2** [パスワード変更制御 (Password Change Control)] タブで、パスワードの更新を TACACS+ を介して許可するかどうかを制御するのに必要なフィールドを定義します。
- [Telnetパスワード変更を有効にする (Enable Telnet Change Password)] セクションのプロンプトは、このオプションが選択されている場合にのみ有効です。選択されていない場合は、[Telnetパスワード変更を無効にする (Disable Telnet Change Password)] のプロンプトが有効になります。パスワードプロンプトはすべてカスタマイズ可能で、必要に応じて変更できます。
- ステップ 3** [セッションキーの割り当て (Session Key Assignment)] タブで、セッションに TACACS+ 要求をリンクするために必要なフィールドを選択します。
- セッション キーは、クライアントからの AAA 要求をリンクするためにモニタリング ノードによって使用されます。デフォルト設定では、[NASアドレス (NAS-Address)]、[ポート (Port)]、[リモートアドレス (Remote-Address)]、および [ユーザ (User)] フィールドが有効になっています。
- ステップ 4** [保存 (Save)] をクリックします。
-



第 10 章

ネットワーク デバイスの管理

- [Cisco ISE のネットワーク デバイス定義 \(247 ページ\)](#)
- [Cisco ISE でのデフォルトのネットワーク デバイス定義 \(248 ページ\)](#)
- [Cisco ISE でのネットワーク デバイス定義の作成 \(249 ページ\)](#)
- [Cisco ISE へのネットワーク デバイスのインポート \(250 ページ\)](#)
- [Cisco ISE からのネットワーク デバイスのエクスポート \(250 ページ\)](#)
- [Cisco ISE でのサードパーティ ネットワーク デバイスのサポート \(251 ページ\)](#)
- [ネットワーク デバイス グループ \(Network Device Groups\) \(259 ページ\)](#)
- [Cisco ISE へのネットワーク デバイス グループのインポート \(260 ページ\)](#)
- [Cisco ISE からのネットワーク デバイス グループのエクスポート \(261 ページ\)](#)
- [Cisco ISE でのテンプレートのインポート \(262 ページ\)](#)
- [Cisco ISE-NAD 通信を保護する IPSec セキュリティ \(267 ページ\)](#)
- [Mobile Device Manager と Cisco ISE との相互運用性 \(278 ページ\)](#)
- [Cisco ISE による MDM サーバの設定 \(284 ページ\)](#)

Cisco ISE のネットワーク デバイス定義

スイッチやルータなどのネットワーク デバイスは、認証、許可、アカウンティング (AAA) クライアントであり、これを使用して、AAA サービス要求が Cisco ISE に送信されます。Cisco ISE がネットワーク デバイスとやり取りするように、ネットワーク デバイスを定義する必要があります。ネットワーク デバイスを RADIUS または TACACS AAA に設定したり、プロファイリング サービスでプロファイリング エンドポイントの Cisco Discovery Protocol 属性および Link Layer Discovery Protocol 属性を収集するための Simple Network Management Protocol (SNMP) を設定したり、TrustSec デバイスの TrustSec 属性を設定することができます。Cisco ISE に定義されていないネットワーク デバイスは、Cisco ISE から AAA サービスを受信できません。

ネットワーク デバイスの定義：

- ネットワーク デバイスに応じたベンダー プロファイルを選択できます。プロファイルには、URL ダイレクトや許可変更の設定などの、デバイスに事前定義された設定が含まれています。

- RADIUS 認証用の RADIUS プロトコルを設定できます。Cisco ISE はネットワーク デバイスから RADIUS 要求を受信すると、対応するデバイス定義を探して設定されている共有秘密を取得します。デバイス定義が見つかった場合、デバイスに設定されている共有秘密を取得し、それを要求内の共有秘密と照合してアクセスを認証します。共有秘密が一致すると、RADIUS サーバは、さらにポリシーと設定に基づいて要求を処理します。一致しない場合は、拒否応答がネットワーク デバイスに送信されます。失敗した認証レポートが生成され、失敗の理由が示されます。
- TACACS+ 認証用の TACACS+ プロトコルを設定できます。Cisco ISE はネットワーク デバイスから TACACS+ 要求を受信すると、対応するデバイス定義を探して設定されている共有秘密を取得します。デバイス定義が見つかった場合、デバイスに設定されている共有秘密を取得し、それを要求内の共有秘密と照合してアクセスを認証します。共有秘密が一致すると、TACACS+ サーバは、さらにポリシーと設定に基づいて要求を処理します。一致しない場合は、拒否応答がネットワーク デバイスに送信されます。失敗した認証レポートが生成され、失敗の理由が示されます。
- プロファイリング サービスがネットワーク デバイスと通信し、ネットワーク デバイ스에 接続されているエンドポイントをプロファイリングするように、ネットワーク デバイ스 定義で簡易ネットワーク管理プロトコル (SNMP) を設定できます。
- Cisco TrustSec ソリューションの一部となる可能性がある TrustSec 対応デバイスからの要求を処理するには、Cisco ISE に TrustSec 対応デバイスを定義する必要があります。TrustSec ソリューションをサポートするスイッチはすべて TrustSec 対応デバイスです。

TrustSec デバイスでは IP アドレスは使用されません。代わりに、TrustSec デバイスが Cisco ISE と通信できるように、その他の設定を定義する必要があります。

TrustSec 対応デバイスは Cisco ISE との通信に TrustSec 属性を使用します。Nexus 7000 シリーズ スイッチ、Catalyst 6000 シリーズ スイッチ、Catalyst 4000 シリーズ スイッチ、Catalyst 3000 シリーズ スイッチなどの TrustSec 対応デバイスは、TrustSec デバイスの追加時に定義した TrustSec 属性を使用して認証されます。

Cisco ISE でのデフォルトのネットワーク デバイス定義

Cisco ISE では、RADIUS および TACACS 認証のデフォルトのデバイス定義がサポートされています。特定の IP アドレスのデバイス定義が見つからない場合、Cisco ISE で使用できるデフォルトのネットワーク デバイスを定義することができます。この機能を使用すると、新しくプロビジョニングされたデバイスのデフォルトの RADIUS または TACACS 共有秘密とアクセス レベルを定義できます。



- (注) 基本的な RADIUS および TACACS 認証のみにデフォルトのデバイス定義を追加することを推奨します。高度なフローについては、ネットワーク デバイスごとに個別のデバイス定義を追加する必要があります。

Cisco ISE は、ネットワーク デバイスから RADIUS または TACACS 要求を受信すると、対応するデバイス定義を検索して、ネットワーク デバイス定義に設定されている共有秘密を取得します。

RADIUS または TACACS 要求が受信されると、Cisco ISE は次の手順を実行します。

1. 要求内の IP アドレスに一致する特定の IP アドレスを探します。
2. 範囲を調べて、要求内の IP アドレスが指定された範囲内にあるかどうかを確認します。
3. ステップ 1 と 2 の両方が失敗すると、要求の処理にデフォルトのデバイス定義（定義されている場合）が使用されます。

Cisco ISE は、そのデバイスのデバイス定義に設定されている共有秘密を取得し、それを RADIUS または TACACS 要求内の共有秘密と照合してアクセスを認証します。デバイス定義が見つからない場合、Cisco ISE はデフォルトのネットワーク デバイス定義から共有秘密を取得し、RADIUS または TACACS 要求を処理します。

Cisco ISE でのネットワーク デバイス定義の作成

Cisco ISE にネットワーク デバイス定義がない場合に Cisco ISE でネットワーク デバイス定義を作成し、デフォルトのネットワーク デバイス定義を使用できます。

[ワークセンター (Work Centers)] > [デバイス管理 (Device Administration)] > [ネットワーク リソース (Network Resources)] > [ネットワークデバイス (Network Devices)] ページで、ネットワーク デバイスの定義を作成することもできます。

-
- ステップ 1 [管理 (Administration)] > [ネットワーク リソース (Network Resources)] > [ネットワーク デバイス (Network Devices)] を選択します。
 - ステップ 2 [追加 (Add)] をクリックします。
 - ステップ 3 必須フィールドをすべて指定します。
 - ステップ 4 [RADIUS 認証設定 (RADIUS Authentication Settings)] チェックボックスをオンにして、RADIUS プロトコル認証を設定します。
 - ステップ 5 [TACACS 認証設定 (TACACS Authentication Settings)] チェックボックスをオンにして、TACACS プロトコル認証を設定します。
 - ステップ 6 (任意) [SNMP の設定 (SNMP Settings)] チェックボックスをオンにして、デバイス情報を収集するプロファイリングサービスの簡易ネットワーク管理プロトコルを設定します。
 - ステップ 7 (任意) TrustSec 対応デバイスを設定するには [高度な TrustSec 設定 (Advanced Trustsec Settings)] チェックボックスをオンにします。
 - ステップ 8 [送信 (Submit)] をクリックします。
-

Cisco ISE へのネットワーク デバイスのインポート

カンマ区切り形式（CSV）ファイルを使用して、Cisco ISE ノードにデバイス定義のリストをインポートできます。Cisco ISE にネットワーク デバイスをインポートする前に、インポートしたテンプレートを更新する必要があります。同じリソースタイプのインポートを同時に実行できません。たとえば、2つの異なるインポートファイルから同時にネットワーク デバイスをインポートできません。

管理者ポータルから CSV テンプレートをダウンロードし、テンプレートにデバイス定義の詳細を入力し、Cisco ISE にインポート可能な CSV ファイルとしてテンプレートを保存できます。

デバイスのインポート中に、新しいレコードを作成するか、または既存のレコードを更新できます。インポートされたデバイスの数の概要が表示され、インポートプロセス中に見つかったエラーが報告されます。デバイスをインポートする場合、Cisco ISE で最初のエラーが発生した場合、既存のデバイス定義を新しい定義で上書きするか、またはインポートプロセスを停止するかを定義できます。

リリース間でインポートテンプレートが異なるため、Cisco ISE の以前のリリースでエクスポートされたネットワーク デバイスをインポートすることはできません。

ステップ 1 [管理（Administration）] > [ネットワーク リソース（Network Resources）] > [ネットワーク デバイス（Network Devices）] を選択します。

ステップ 2 [インポート（Import）] をクリックします。

ステップ 3 [参照（Browse）] をクリックして、クライアント ブラウザを実行しているシステムから CSV ファイルを選択します。

ステップ 4 [新しいデータで既存のデータを上書き（Overwrite Existing Data with New Data）] チェックボックスをオンにします。

ステップ 5 [最初のエラーでインポートを停止（Stop Import on First Error）] チェックボックスをオンにします。

ステップ 6 [インポート（Import）] をクリックします。

Cisco ISE からのネットワーク デバイスのエクスポート

Cisco ISE で設定されたネットワーク デバイスを CSV ファイル形式でエクスポートし、これを使用して別の Cisco ISE ノードにそれらのネットワーク デバイスをインポートできます。

ステップ 1 [管理（Administration）] > [ネットワーク リソース（Network Resources）] > [ネットワーク デバイス（Network Devices）] を選択します。

ステップ 2 [エクスポート（Export）] をクリックします。

ステップ 3 ネットワーク デバイスをエクスポートするには、次のいずれかを行うことができます。

- エクスポートするデバイスの隣にあるチェックボックスをオンにし、[エクスポート (Export)] > [選択済みをエクスポート (Export Selected)] を選択します。
- 定義されているすべてのネットワーク デバイスをエクスポートするには、[エクスポート (Export)] > [すべてエクスポート (Export All)] を選択します。

ステップ 4 ローカル ハード ディスクに export.csv ファイルを保存します。

Cisco ISE でのサードパーティ ネットワーク デバイスのサポート

Cisco ISE は、ネットワーク デバイス プロファイルを使用して、サードパーティ製ネットワーク アクセス デバイス (NAD) をサポートします。NAD プロファイルは、ベンダー側の導入に関係なく、シンプルなポリシー設定でサードパーティ デバイスの機能を定義します。ネットワーク デバイス プロファイルには、次のものが含まれています。

- RADIUS、TACACS+、TrustSec などの、ネットワーク デバイスがサポートするプロトコル。デバイスに存在するベンダー固有の RADIUS ディクショナリを Cisco ISE にインポートできます。
- デバイスが有線 MAB、802.1x などのさまざまなフローに使用する属性および値。これを使用して、Cisco ISE は使用される属性に従ってデバイスに適切なフロー タイプを検出できます。
- デバイスが持つ認可変更 (CoA) 機能。RFC 5176 では CoA 要求のタイプが定義されますが、要求に必要な属性はデバイスによって異なります。RFC 5176 サポート付きのほとんどのシスコ以外のデバイスは、「プッシュ」および「切断」機能もサポートします。RADIUS CoA タイプをサポートしていないデバイスについては、ISE も SNMP CoA をサポートします。CoA タイプの詳細については、以降に説明します。
- デバイスが MAB に使用する属性およびプロトコル。さまざまなベンダーからのネットワーク デバイスは、MAB 認証を異なる方法で実行します。
- デバイスで使用される VLAN および ACL の権限。プロファイルを保存すると、Cisco ISE は設定された各権限に対し許可プロファイルを自動的に生成します。
- URL リダイレクションは、BYOD、ゲスト、ポスチャなどの高度なフローに必要です。デバイス内で見つかる URL リダイレクションには、スタティックとダイナミックの 2 つのタイプがあります。スタティック URL リダイレクションの場合は、ISE ポータル URL をコピーして設定に貼り付けることができます。ダイナミック URL リダイレクションの場合、ISE は RADIUS 属性を使用して、リダイレクト先をネットワーク デバイスに伝えます。また、デバイスがダイナミック URL もスタティック URL もサポートしていない場合には、ISE が URL リダイレクトをシミュレートする認証 VLAN を提供します。認証 VLAN は、ISE ボックスで実行されている DHCP/DNS サービスに基づいています。認証 VLAN を作成するには、DHCP/DNS サービス設定を定義します。詳細については、[DHCP および](#)

[DNS サービス \(1201 ページ\)](#) を参照してください。URL リダイレクトフローの詳細については、以降に説明します。

ISE でデバイスを定義したら、これらのデバイス プロファイルを設定するか、ISE によって提供された事前設定済みデバイスプロファイルを使用して、Cisco ISE が基本フローや、プロファイル、ゲスト、BYOD、MAB、ポスチャなどの高度なフローを有効にするために使用する機能を定義します。

URL リダイレクト メカニズムと認証 VLAN

ネットワークでサードパーティデバイスが使用されていて、デバイスがダイナミックまたはスタティック URL リダイレクトをサポートしていない場合、ISE が URL リダイレクトフローをシミュレートします。このようなデバイスの URL リダイレクトシミュレーションフローは、ISE ボックスで DHCP/DNS サービスを実行することで動作します（詳細については、[#unique_347](#)を参照してください）。認証 VLAN フローは次のとおりです。

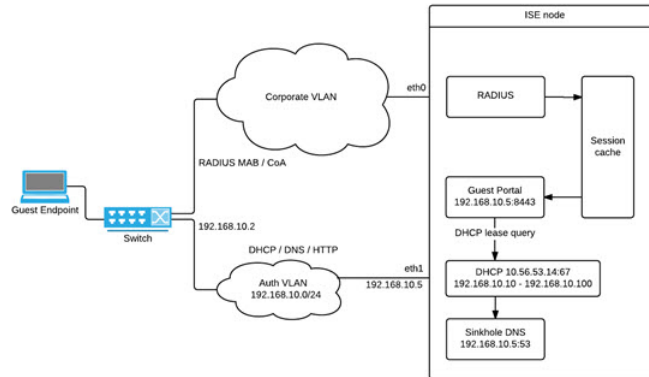
1. ゲスト エンドポイントが NAD に接続します。
2. デバイスが ISE に RADIUS/MAB 要求を送信します。
3. ISE が認証/承認ポリシーを実行し、ユーザ アカウンティング情報を保存します。
4. ISE が認証 VLAN ID を含む RADIUS アクセス/承認メッセージを送信します。
5. ゲスト エンドポイントがネットワーク アクセスを受け取ります。
6. エンドポイントが DHCP 要求を送信し、ISE DHCP サービスからクライアント IP アドレスと ISE シンクホール DNS IP アドレスを取得します。
7. ゲストエンドポイントがブラウザを開きます。ブラウザが DNS クエリを送信し、ISE IP アドレスを受け取ります。
8. エンドポイント HTTP または HTTPS 要求が ISE ボックスに送られます。
9. ISE は HTTP 301/Moved で応答し、ゲスト ポータル URL を提供します。エンドポイントブラウザがゲスト ポータル ページにリダイレクトされます。
10. ゲスト エンドポイント ユーザが認証のためにログインします。
11. コンプライアンスの検証が完了すると、ISE は NAD に応答し、CoA の送信、エンドポイントの認証、シンクホールのバイパスを行います。
12. CoA に基づいて適切なアクセスがユーザに提供され、エンドポイントが企業 DHCP から IP アドレスを受信し、ユーザがネットワークを使用できるようになります。

エンドポイントが認証を通過する前にゲスト エンドポイントによって不正なネットワーク アクセスが行われないように、認証 VLAN は社内ネットワークから分離する必要があります。認証 VLAN IP ヘルパーを設定して ISE マシンを示すか、いずれかの ISE ネットワーク インターフェイスを認証 VLAN に接続します。VLAN (DHCP/DNS サーバ) 設定の詳細については、[#unique_347](#)を参照してください。NAD 設定から VLAN IP ヘルパーを設定することで、複数の VLAN を1つのネットワーク インターフェイスカードに接続することができます。IP ヘルパー

の設定の詳細については、デバイス用のアドミニストレーションガイドの指示を参照してください。さらに、ゲストフローについて、通常のゲストフローと同様にゲストポータルを定義して、MAB 認証にバインドされる認証プロファイルでそのポータルを選択します。ゲストポータルの詳細については、[Cisco ISE ゲスト サービス \(521 ページ\)](#) を参照してください。

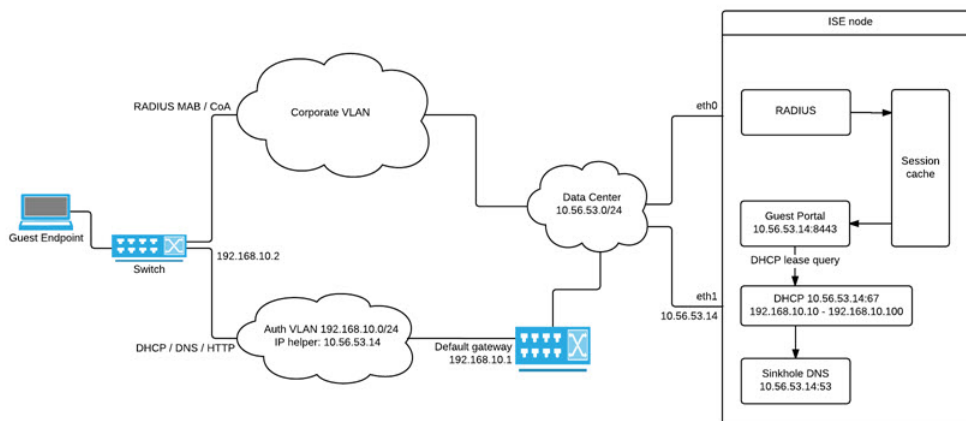
次の図に、認証 VLAN が定義されているときの基本的なネットワーク設定を示します（認証 VLAN が Cisco ISE ノードに直接接続されています）。

図 9: Cisco ISE ノードに接続する認証 VLAN



次の図に、認証 VLAN と IP ヘルパーを備えたネットワークを示します。

図 10: IP ヘルパーを備えた認証 VLAN



CoA タイプ

ISE は、RADIUS と SNMP の両方の CoA タイプをサポートします。RADIUS または SNMP CoA タイプのサポートは、基本的なフローでは必須ではありませんが、NAD が複雑なフローで機能するために必要です。ISE から NAD を設定するときにデバイスによってサポートされる RADIUS および SNMP の設定を定義し、NAD プロファイルを設定するときに特定のフローのために使用される CoA タイプを示します。NAD のプロトコルの定義の詳細については、[ネッ](#)

[トワーク デバイス \(1227 ページ\)](#) を参照してください。ISE でデバイスと NAD のプロファイルを作成する前に、NAD でどのタイプがサポートされているかをサードパーティ サプライヤーに確認してください。

ネットワーク デバイス プロファイル

Cisco ISE は、ネットワーク デバイス プロファイルを使用して、一部のサードパーティ製ネットワーク アクセス デバイス (NAD) をサポートします。これらのプロファイルによって、基本フローと、ゲスト、BYOD、MAB、ポスチャなどの高度なフローを有効にするために Cisco ISE が使用する機能が定義されます。

Cisco ISE には、いくつかのベンダーからのネットワーク デバイスの定義済みプロファイルが含まれています。Cisco ISE 2.1 は、次の表に記載されているベンダー デバイスでテストされています。

表 7: Cisco ISE 2.1 でテスト済みのベンダー デバイス

デバイス タイプ (Device Type)	ベンダー	CoA タイ プ	URL リ ダイレク ト タイ プ	サポートされる/検証済みの使用例				
				802.1X/ MAB	CoA のな いプロ ファイル	CoA があ るプロ ファイル	ポスチャ (Posture)	ゲス ト/BYOD
ワイヤレ ス	Aruba 7000、 InstantAP	RADIUS	スタ ティック URL	√	√	√	√	√
	Motorola RFS 4000	RADIUS	ダイナ ミック URL	√	√	√	√	√
	HP 830	RADIUS	スタ ティック URL	√	√	√	√	√
	Ruckus ZD 1200	RADIUS	—	√	√	√	√	√

有線	HP A5500	RADIUS	ISE が提供する認証 VLAN	√	√	√	√	√
	HP 3800 および 2920 (PoE+)	RADIUS	ISE が提供する認証 VLAN	√	√	√	√	√
	Alcatel 6850	SNMP	ダイナミック URL	√	√	√	√	√
	Brocade ICX 6610	RADIUS	ISE が提供する認証 VLAN	√	√	√	√	√
	Juniper EX3300-24p	RADIUS	ISE が提供する認証 VLAN	√	√	√	√	√
その他のサードパーティ製 NAD の場合は、デバイスのプロパティおよび機能を識別し、Cisco ISE でカスタム NAD プロファイルを作成する必要があります。				√	√	CoA サポートが必要	CoA サポートが必要です。URL リダイレクトについて、有線デバイスに URL リダイレクトがない場合は、ISE 認証 VLAN を利用します。ワイヤレスデバイスは認証 VLAN でテストされていません。	

定義済みプロファイルがないその他のサードパーティ製ネットワーク デバイス用のカスタム NAD プロファイルを作成できます。ゲスト、BYOD、ポスチャなどの高度なフローの場合、デバイスは RFC 5176、許可変更 (CoA) をサポートしている必要があります。これらのフローに対するサポートは、NAD の機能によって異なります。ネットワーク デバイス プロファイルに必要な多くの属性については、デバイスの管理ガイドを参照する必要があります。カスタム NAD プロファイルの作成方法については、[Cisco ISE でのサードパーティ製ネットワーク デバイスの設定 \(256 ページ\)](#) を参照してください。

リリース 2.0 以前のシスコ以外の NAD を展開し、それらを使用するようにポリシー ルール/RADIUS デictionary を作成した場合、これらはアップグレード後に通常どおりに機能し続けます。

ISE Community Resource

サードパーティ製 NAD プロファイルについては、「[ISE Third-Party NAD Profiles and Configs](#)」を参照してください。

Cisco ISE でのサードパーティ製ネットワーク デバイスの設定

Cisco ISE は、ネットワーク デバイス プロファイルを使用して、サードパーティ製ネットワーク アクセス デバイス (NAD) をサポートします。これらのプロファイルによって、ゲスト、BYOD、MAB、ポスチャなどのフローを有効にするために Cisco ISE が使用する機能が定義されます。

始める前に

『Cisco Identity Services Engine 管理者ガイド』の[ネットワーク デバイス プロファイル \(254 ページ\)](#) の定義を確認してください。

-
- ステップ 1** デバイスが ISE で設定されていることを確認します。ゲスト、BYOD またはポスチャのワークフローを設定している場合、認可変更 (CoA) が定義され、NAD の URL リダイレクト機能が、関連する ISE ポータルをポイントするように設定されていることを確認します。URL リダイレクトの場合は、ポータルのランディング ページから ISE ポータルの URL をコピーできます。ISE の NAD の CoA タイプおよび URL リダイレクトの設定に関する詳細については、[ネットワーク デバイス \(1227 ページ\)](#) を参照してください。さらに、手順については、サードパーティ デバイスの管理ガイドを参照してください。
- ステップ 2** デバイスに適切な NAD プロファイルが ISE で利用できることを確認します。既存のプロファイルを表示するには、**[管理 (Administration)] > [ネットワーク リソース (Network Resources)] > [ネットワーク デバイス プロファイル (Network Device Profiles)]** を選択します。適切なプロファイルが ISE に存在しない場合は、カスタムプロファイルを作成します。カスタムプロファイルの作成方法の詳細については、[ネットワーク デバイス プロファイルの作成 \(257 ページ\)](#) を参照してください。
- ステップ 3** 設定する NAD に NAD プロファイルを割り当てます。**[管理 (Administration)] > [ネットワーク リソース (Network Resources)] > [ネットワーク デバイス (Network Devices)]** を選択します。プロファイルを割り当てるデバイスを開き、**[デバイス プロファイル (Device Profile)]** ドロップダウンリストから適切なプロファイルを選択します。
- ステップ 4** ポリシー ルールを設定する場合は、許可プロファイルをステップ 1 で NAD プロファイルに明示的に設定する必要があります。または、VLAN または ACL を使用するだけの場合、あるいはネットワークに異なるベンダーからのさまざまなデバイスがある場合は、**[いずれか (Any)]** に設定します。許可プロファイルの NAD プロファイルを設定するには、**[ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] > [認証 (Authorization)] > [許可プロファイル (Authorization Profiles)]** を選択します。関連する認可プロファイルを開き、**[ネットワーク デバイス プロファイル (Network Device Profiles)]** ドロップダウンリストから関連する NAD プロファイルを選択します。ゲストフロー用に認証 VLAN を使用する場合、通常のゲストフローと同様に、ゲストポータルを定義し、MAB 認証にバインドされた認証プロファイルでそのポータルを選択する必要があります。ゲストポータルの詳細については、[Cisco ISE ゲストサービス \(521 ページ\)](#) を参照してください。
-

ネットワーク デバイス プロファイルの作成

始める前に

- カスタム プロファイルの作成方法の詳細については、『[Network Access Device Profiles with Cisco Identity Services Engine](#)』ドキュメントを確認してください。
- ほとんどの NAD には、標準の IETF RADIUS 属性に加えて多数のベンダー固有の属性を提供する、ベンダー固有の RADIUS ディクショナリがあります。ネットワーク デバイスにベンダー固有の RADIUS ディクショナリがある場合は、それを Cisco ISE にインポートします。RADIUS ディクショナリが必要な手順については、サードパーティ製デバイスの管理ガイドを参照してください。ISE から、**[ポリシー要素 (Policy Elements)] > [ディクショナリ (Dictionaries)] > [RADIUS] > [RADIUS ベンダー (Radius Vendors)] >** を選択します。RADIUS ディクショナリのインポートの詳細については、[RADIUS ベンダー ディクショナリの作成 \(310 ページ\)](#) を参照してください。
- ゲストやポスチャなどの複雑なフローの場合、デバイスは RFC 5176、許可変更 (CoA) をサポートしている必要があります。
- ネットワーク デバイスのプロファイルを作成するためのフィールドと値の詳細については、[ネットワーク デバイス プロファイル設定 \(1248 ページ\)](#) を参照してください。

-
- ステップ 1** **[管理 (Administration)] > [ネットワークリソース (Network Resources)] > [ネットワークデバイスプロファイル (Network Device Profiles)]** を選択します。
- ステップ 2** **[追加 (Add)]** をクリックします。
- ステップ 3** ネットワーク デバイスの名前と説明を入力します。
- ステップ 4** ネットワーク デバイスのベンダーを選択します。
- ステップ 5** デバイスがサポートするプロトコルのチェックボックスをオンにします。デバイスが RADIUS、TACACS+、TrustSec をサポートする場合には、各ボックスにマークを付けます。実際に使用するプロトコルにのみマークを付ける必要があります。デバイスが RADIUS をサポートしている場合は、**[RADIUS ディクショナリ (RADIUS Dictionaries)]** フィールドのダイナミック ドロップダウン リストからネットワーク デバイスで使用する RADIUS ディクショナリを選択します。
- ステップ 6** **[テンプレート (Templates)]** セクションから次のように関連情報を入力します。
- a) **[認証/許可 (Authentication/Authorization)]** から、フローのタイプ、属性エイリアシングおよびホスト ルックアップに対するデバイスのデフォルト設定を設定します。**[フロータイプの条件 (Flow Type Conditions)]** には、デバイスが有線 MAB または 802.1x などのさまざまなフローに使用する、属性と値を入力してください。これにより、Cisco ISE は使用される属性に従ってデバイスに適切なフロー タイプを検出できます。MAB 用の IETF 標準がないため、ベンダーごとに異なる値が **Service-Type** に使用されています。正しい設定を判断するには、デバイスのユーザ ガイドを参照するか、または MAB 認証のスニファトレースを使用してください。**[属性エイリアシング (Attribute Aliasing)]** から、デバイス固有の属性名を共通名にマップして、ポリシールールを簡素化することができます。現在は、SSID のみが定義されています。デバイスにワイヤレス SSID の概念がある場合には、使用される属性に対してこれを設定します。ISE は、これを正規化された RADIUS ディクショナリの SSID という属性にマッピングします。これは、1 つのルールの SSID を参照でき、基盤となる属性が異なっても複数のデ

バイスで動作するので、ポリシールールを設定を簡素化します。[ホストルックアップ (HostLookup)] から、[ホストルックアップの処理 (Process Host Lookup)] オプションを有効にして、サードパーティの指示に基づいて、デバイスに関連する MAB プロトコルと属性を選択します。

- b) [権限 (Permissions)] から、VLAN および ACL に関するネットワーク デバイスのデフォルト設定を行います。これらは自動的に、ISE で作成した認可プロファイルに基づいてマッピングされます。
- c) [許可変更 (CoA) (Change of Authorization (CoA))] から、デバイスの CoA 機能を設定します。
- d) [リダイレクト (Redirect)] セクションを展開し、デバイスの URL リダイレクト機能を設定します。URL リダイレクションは、ゲスト、BYOD およびポスチャに必要です。

ステップ 7 [送信 (Submit)] をクリックします。

Cisco ISE からのネットワーク デバイス プロファイルのエクスポート

XML ファイルを編集してから、そのファイルを新しいネットワーク プロファイルとしてインポートするために、Cisco ISE で設定された単一または複数のネットワーク デバイス プロファイルを XML 形式でエクスポートします。

始める前に

『[Network Access Device Profiles with Cisco Identity Services Engine](#)』のドキュメントを参照してください。

ステップ 1 [管理 (Administration)] > [ネットワーク リソース (Network Resources)] > [ネットワーク デバイス プロファイル (Network Device Profiles)] を選択します。

ステップ 2 [エクスポート (Export)] をクリックします。

ステップ 3 エクスポートするデバイスの隣にあるチェックボックスをオンにし、[エクスポート (Export)] > [選択済みをエクスポート (Export Selected)] を選択します。

ステップ 4 DeviceProfiles.xml ファイルがローカル ハード ディスクにダウンロードされます。

Cisco ISE へのネットワーク デバイス プロファイルのインポート

Cisco ISE XML 構造を備えた単一の XML ファイルを使用して、ISE に単一または複数のネットワーク デバイス プロファイルをインポートできます。複数のインポート ファイルから同時にネットワーク デバイス プロファイルをインポートすることはできません。

通常は、まずテンプレートとして使用するために管理者ポータルから既存のプロファイルをエクスポートします。必要に応じてデバイスプロファイルの詳細をファイルに入力し、XML ファイルとして保存してから、編集したファイルを Cisco ISE に再度インポートします。複数のプロファイルを扱うには、単一の XML ファイルとして一緒に構造化された複数のプロファイルをエクスポートし、ファイルを編集してから一緒にインポートして、ISE で複数のファイルを作成します。

デバイスプロファイルのインポート中は、新しいレコードの作成のみができます。既存のプロファイルは上書きできません。既存のプロファイルを編集してから上書きするには、既存のプロファイルをエクスポートし、ISE からそのプロファイルを削除してから、適切に編集した後、そのプロファイルをインポートします。

始める前に

『[Network Access Device Profiles with Cisco Identity Services Engine](#)』のドキュメントを参照してください。

-
- ステップ 1** [管理 (Administration)] > [ネットワーク リソース (Network Resources)] > [ネットワーク デバイス プロファイル (Network Device Profiles)] を選択します。
- ステップ 2** [インポート (Import)] をクリックします。
- ステップ 3** [参照 (Browse)] をクリックして、クライアントブラウザを実行しているシステムから XML ファイルを選択します。
- ステップ 4** [インポート (Import)] をクリックします。
-

ネットワークデバイスグループ (NetworkDeviceGroups)

Cisco ISE では、階層型ネットワーク デバイス グループ (NDG) を作成できます。NDG は、地理的な場所、デバイス タイプ、ネットワーク内での相対的な位置 (アクセス レイヤ、データ センターなど) のようなさまざまな基準に基づいて、ネットワーク デバイスを論理的にグループ化するために使用できます。たとえば、地理的な場所に基づいてネットワーク デバイスを編成するには、大陸、地域、または国でグループ化できます。

- アフリカ -> 南部 -> ナミビア
- アフリカ -> 南部 -> 南アフリカ
- アフリカ -> 南部 -> ボツワナ

デバイス タイプに基づいてネットワーク デバイスをグループ化することもできます。

- アフリカ -> 南部 -> ボツワナ -> ファイアウォール
- アフリカ -> 南部 -> ボツワナ -> ルータ
- アフリカ -> 南部 -> ボツワナ -> スイッチ

ネットワーク デバイスは、1 つ以上の階層型 NDG に割り当てることができます。したがって、Cisco ISE が、設定された NDG の順序リスト全体を参照して特定のデバイスに割り当てる適切なグループを決定するとき、同じデバイス プロファイルが複数のデバイス グループに適用されている場合、Cisco ISE は最初に一致したデバイス グループを適用します。

作成できる NDG の最大数に制限はありません。階層レベルの最大数にも制限はありません。

ツリー ビューやフラット テーブル ビューでデバイス グループ階層を表示できます。ツリー ビューで、ルート ノードはツリーの最上位に表示され、子グループが階層順序で次に続きます。各ルートグループに属するすべてのデバイスを表示するには、[すべて展開 (Expand All)] をクリックします。ルートグループだけを表示するには、[すべて折りたたむ (Collapse All)] をクリックします。

フラットテーブルビューでは、各デバイスグループの階層が[グループ階層 (Group Hierarchy)] 列に表示されます。

また、各子グループに割り当てられたネットワークデバイスの数を確認できます。そのデバイス グループに割り当てられているすべてのネットワーク デバイスを一覧表示する、[ネットワーク デバイス (Network Devices)] ウィンドウを起動するには、この番号付きリンクをクリックしてください。デバイス グループに追加デバイスを追加したり、別のデバイス グループに既存のデバイスを移動できます。

デバイス グループを追加するときに、新しいグループをルート グループとして追加するか、親グループとして既存のグループを選択する必要があるかどうかを指定できます。



(注) デバイスが割り当てられているデバイス グループは削除できません。デバイス グループを削除する前に、すべての既存のデバイスを別のデバイス グループに移動する必要があります。

ルート ネットワーク デバイス グループ

Cisco ISE には、すべてのデバイス タイプとすべてのロケーションという 2 つの定義済みルート NDG が含まれます。これらの事前定義された NDG を編集、複製、または削除することはできませんが、それらの下に新しいデバイス グループを追加できます。

ルート ネットワーク デバイス グループ (NDG) を作成し、[ネットワーク デバイス グループ (Network Device Groups)] ページでそのルート グループの下に子 NDG を作成できます。

ポリシー評価で Cisco ISE が使用するネットワーク デバイスの属性

新しいネットワーク デバイス グループを作成すると、新しいネットワーク デバイス属性がシステムに定義されているデバイスディクショナリに追加され、ポリシー定義に使用できるようになります。Cisco ISE では、デバイス タイプ、ロケーション、モデル名、およびネットワーク デバイス上で実行しているソフトウェア バージョンなどのデバイス ディクショナリ属性に基づいて認証ポリシーと許可ポリシーを設定できます。

Cisco ISE へのネットワーク デバイス グループのインポート

カンマ区切り形式 (CSV) ファイルを使用して Cisco ISE ノードにネットワーク デバイス グループをインポートできます。同じリソースタイプのインポートを同時に実行できません。た

たとえば、2つの異なるインポート ファイルから同時にネットワーク デバイス グループをインポートできません。

管理者ポータルから CSV テンプレートをダウンロードし、テンプレートにデバイス グループの詳細を入力し、Cisco ISE にインポート可能な CSV ファイルとしてテンプレートを保存できます。

デバイス グループのインポート中に、新しいレコードを作成するか、または既存のレコードを更新できます。デバイス グループをインポートする場合、Cisco ISE で最初のエラーが発生した場合、既存のデバイス グループを新しいグループで上書きするか、またはインポート プロセスを停止するかを定義できます。

-
- ステップ 1** [管理 (Administration)] > [ネットワーク リソース (Network Resources)] > [ネットワーク デバイス グループ (Network Device Groups)] > [グループ (Groups)] を選択します。
- ステップ 2** [インポート (Import)] をクリックします。
- ステップ 3** [参照 (Browse)] をクリックして、クライアント ブラウザを実行しているシステムから CSV ファイルを選択します。
- ステップ 4** [新しいデータで既存のデータを上書き (Overwrite Existing Data with New Data)] チェックボックスをオンにします。
- ステップ 5** [最初のエラーでインポートを停止 (Stop Import on First Error)] チェックボックスをオンにします。
- ステップ 6** [ネットワーク デバイス グループ (Network Device Groups)] リスト ページに戻るには、[インポート (Import)] または [ネットワーク デバイス グループ リスト (Network Device Groups List)] リンクをクリックします。
-

Cisco ISE からのネットワーク デバイス グループのエクスポート

Cisco ISE に設定されたネットワーク デバイス グループを CSV ファイル形式でエクスポートし、これを使用して別の Cisco ISE ノードにそれらのネットワーク デバイス グループをインポートできます。

-
- ステップ 1** [管理 (Administration)] > [ネットワーク リソース (Network Resources)] > [ネットワーク デバイス グループ (Network Device Groups)] > [グループ (Groups)] を選択します。
- ステップ 2** ネットワーク デバイス グループをエクスポートするには、次のいずれかを行うことができます。
- エクスポートするデバイス グループの横にあるチェックボックスをオンにし、[エクスポート (Export)] > [選択済みをエクスポート (Export Selected)] を選択します。
 - [エクスポート (Export)] > [すべてエクスポート (Export All)] を選択して、定義されたネットワーク デバイス グループをすべてエクスポートします。

ステップ 3 ローカル ハード ディスクに export.csv ファイルを保存します。

Cisco ISE でのテンプレートのインポート

Cisco ISE では、カンマ区切り形式（CSV）ファイルを使用して大量のネットワーク デバイスやネットワーク デバイス グループをインポートできます。テンプレートには、フィールドのフォーマットを定義するヘッダー行が含まれます。ヘッダー行は編集しないでそのまま使用してください。

デフォルトで、[テンプレートの生成（Generate a Template）] リンクを使用して、Microsoft Office Excel アプリケーションに CSV ファイルをダウンロードし、このファイル形式をシステム上にローカルに保存できます。[テンプレートの生成（Generate a Template）] リンクをクリックすると、Cisco ISE サーバは、[template.csv を開く（Opening template.csv）] ダイアログを表示します。このダイアログを使用すると、template.csv ファイルを開いて、その template.csv ファイルにネットワーク デバイスおよびネットワーク デバイス グループに適切な名前を付けて、システム上にローカルに保存できます。このダイアログで template.csv ファイルを開くことを選択した場合、このファイルはデフォルトで Microsoft Office Excel アプリケーションで開かれます。

ネットワーク デバイスのインポート テンプレート形式

次の表では、テンプレート ヘッダーのフィールドとネットワーク デバイスの CSV ファイルにおけるこれらのフィールドの説明を示します。

表 8: ネットワーク デバイスの CSV テンプレートのフィールドと説明

フィールド	説明
Name : 文字列 (32)	(必須) このフィールドはネットワーク デバイスの名前です。これは、最大 32 文字の英数字文字列です。
Description:String(256)	このフィールドは、ネットワーク デバイスの任意の説明です。最大 256 文字の文字列。
IP Address:Subnets (a.b.c.d/m ...)	(必須) このフィールドは、ネットワーク デバイスの IP アドレスおよびサブネットマスクです。(パイプ記号「 」で区切って複数の値を指定できます)。
Model Name : 文字列 (32)	(必須) このフィールドはネットワーク デバイスのモデル名です。これは、最大 32 文字の文字列です。

フィールド	説明
Software Version : 文字列 (32)	(必須) このフィールドはネットワーク デバイスのソフトウェアバージョンです。これは、最大 32 文字の文字列です。
Network Device Groups : 文字列 (100)	(必須) このフィールドは、既存のネットワーク デバイス グループにする必要があります。サブグループを指定できますが、親グループとサブグループの両方をスペースで区切って含める必要があります。最大 100 文字の文字列 (たとえば、Location#All Location#US) です。
Authentication:Protocol:String(6)	これはオプションのフィールドです。認証に使用するプロトコルです。唯一の有効な値は RADIUS です (大文字と小文字は区別されません)。
Authentication:Shared Secret:String(128)	(認証プロトコルのフィールドの値を入力した場合は必須) このフィールドは、最大 128 文字の文字列です。
EnableKeyWrap : ブール (true false)	これはオプションのフィールドです。これはネットワーク デバイスでサポートされている場合に限り有効です。有効な値は true または false です。
EncryptionKey : 文字列 (ascii:16 hexa:32)	(KeyWrap を有効にした場合は必須) セッションの暗号化に使用される暗号キーを示します。 ASCII : 16 文字 (バイト) の長さ 16 進数 : 32 文字 (バイト) の長さ。
AuthenticationKey : 文字列 (ascii:20 hexa:40)	(KeyWrap を有効にした場合は必須) 。RADIUS メッセージに対するキー付き Hashed Message Authentication Code (HMAC) の計算を示します。 ASCII : 20 文字 (バイト) の長さ 16 進数 : 40 文字 (バイト) の長さ。
InputFormat : 文字列 (32)	暗号化と認証キーの入力形式を示します。有効な値は、ASCII または Hexadecimal です。

フィールド	説明
SNMP:Version : 列挙 (1 2c 3)	これはオプションのフィールドで、プロファイラ サービスによって使用されます。SNMP プロトコルのバージョンです。有効な値は1、2c、または3です。
SNMP:RO Community:String(32)	(SNMP バージョンのフィールドの値を入力した場合は必須) SNMP 読み取り専用のコミュニティ。これは、最大32文字の文字列です。
SNMP:RW Community:String(32)	(SNMP バージョンのフィールドの値を入力した場合は必須) SNMP 読み取り書き込みコミュニティ。これは、最大32文字の文字列です。
SNMP:Username:String(32)	これはオプションのフィールドです。これは、最大32文字の文字列です。
SNMP:Security Level:Enumeration(Auth No Auth Priv)	(SNMP バージョン3を選択した場合は必須) 有効な値は、Auth、No Auth、または Priv です。
SNMP:Authentication Protocol:Enumeration(MD5 SHA)	(SNMP セキュリティ レベルで Auth または Priv を入力した場合は必須) 有効な値は、MD5 または SHA です。
SNMP:Authentication Password:String(32)	(SNMP セキュリティ レベルで Auth を入力した場合は必須) これは、最大32文字の文字列です。
SNMP:Privacy Protocol:Enumeration(DES AES128 AES192 AES256 3DES)	(SNMP セキュリティ レベルで Priv を入力した場合は必須) 有効な値は、DES、AES128、AES192、AES256、または 3DES です。
SNMP:Privacy Password:String(32)	(SNMP セキュリティ レベルで Priv を入力した場合は必須) これは、最大32文字の文字列です。
SNMP:Polling Interval:Integer:600-86400 seconds	これはオプションのフィールドで、SNMP ポーリング間隔を設定します。有効な値は600～86400の整数です。
SNMP:Is Link Trap Query:Boolean(true false)	これはオプションのフィールドで、SNMP リンク トラップを有効または無効にします。有効な値は true または false です。

フィールド	説明
SNMP:Is MAC Trap Query : ブール (true false)	これはオプションのフィールドで、SNMP MAC トラップを有効または無効にします。有効な値は true または false です。
SNMP:Originating Policy Services Node : 文字列 (32)	これはオプションのフィールドです。SNMP データのポーリングに使用される ISE サーバを示します。デフォルトでは自動ですが、別の値を割り当てて設定を上書きできます。
Trustsec:Device Id : 文字列 (32)	これはオプションのフィールドです。これは、TrustSec デバイス ID で、最大 32 文字の文字列です。
Trustsec:Device Password : 文字列 (256)	(TrustSec デバイス ID を入力した場合は必須) これは TrustSec デバイスのパスワードで、最大 256 文字の文字列です。
Trustsec:Environment Data Download Interval : 整数 : 1-2147040000 秒	これはオプションのフィールドです。これは TrustSec 環境データのダウンロード間隔です。有効な値は 1 ~ 24850 の整数です。
Trustsec:Peer Authorization Policy Download Interval : 整数 : 1-2147040000 秒	これはオプションのフィールドです。これは TrustSec のピア許可ポリシーのダウンロード間隔です。有効な値は 1 ~ 24850 の整数です。
Trustsec:Reauthentication Interval : 整数 : 1-2147040000 秒	これはオプションのフィールドです。これは TrustSec の再認証間隔です。有効な値は 1 ~ 24850 の整数です。
Trustsec:SGACL List Download Interval : 整数 : 1-2147040000 秒	これはオプションのフィールドです。また、TrustSec SGACL リストのダウンロード間隔です。有効な値は 1 ~ 24850 の整数です。
Trustsec:Is Other Trustsec Devices Trusted : ブール (true false)	これはオプションのフィールドです。TrustSec が信頼できるかどうかを示します。有効な値は true または false です。
Trustsec:Notify this device about Trustsec configuration changes : 文字列 (ENABLE_ALL DISABLE_ALL)	これはオプションのフィールドです。TrustSec デバイスに対する TrustSec 設定変更を通知します。有効な値は ENABLE_ALL または DISABLE_ALL です
Trustsec:Include this device when deploying Security Group Tag Mapping Updates : ブール (true false)	これはオプションのフィールドです。これは、SGT に含まれる TrustSec デバイスです。有効な値は true または false です。

フィールド	説明
Deployment:Execution Mode Username:String(32)	これはオプションのフィールドです。デバイス設定を編集する権限を持っているユーザ名です。これは、最大 32 文字の文字列です。
Deployment:Execution Mode Password:String(32)	これはオプションのフィールドです。デバイスパスワードで、最大 32 文字の文字列です。
Deployment:Enable Mode Password:String(32)	これはオプションのフィールドです。設定を編集するためのデバイスのイネーブルパスワードで、最大 32 文字の文字列です。
Trustsec:PAC issue date : 日付	これは、TrustSec デバイス用に Cisco ISE によって生成された最後の TrustSec PAC の発行日を表示するフィールドです。
Trustsec:PAC expiration date : 日付	これは、TrustSec デバイス用に Cisco ISE によって生成された最後の TrustSec PAC の有効期限を表示するフィールドです。
Trustsec:PAC issued by : 文字列	これは、TrustSec デバイス用に Cisco ISE によって生成された最後の TrustSec PAC の発行者 (TrustSec 管理者) の名前を表示するフィールドです。文字列です。

ネットワーク デバイス グループのインポート テンプレート形式

次の表に、テンプレートヘッダーのフィールドとネットワーク デバイス グループの CSV ファイルにおけるこれらのフィールドの説明を示します。

表 9: ネットワーク デバイス グループの CSV テンプレートのフィールドと説明

フィールド	説明
Name : 文字列 (100)	(必須) このフィールドはネットワーク デバイス グループの名前です。最大 100 文字の文字列です。NDG の完全な名前の長さは、最大 100 文字です。たとえば、親グループ Global>Asia の下にサブグループ India を作成している場合、作成する NDG の完全な名前は Global#Asia#India になり、この完全な名前の長さは 100 文字を超えることはできません。NDG の完全な名前の長さが 100 文字を超えた場合、NDG の作成は失敗します。

フィールド	説明
Description:String(1024)	これは、オプションのネットワーク デバイス グループの説明です。これは、最大 1024 文字の文字列です。
Type : 文字列 (64)	(必須) このフィールドはネットワーク デバイス グループのタイプです。これは、最大 64 文字の文字列です。
Is Root : ブール (true false)	(必須) これは、特定のネットワーク デバイス グループがルート グループかどうかを示すフィールドです。有効な値は true または false です。

Cisco ISE-NAD 通信を保護する IPSec セキュリティ

Internet Protocol セキュリティ (IPSec) は、Internet Protocol にセキュリティを提供するプロトコルのセットです。AAA プロトコル、RADIUS および TACACS+ は MD5 ハッシュ アルゴリズムを使用します。セキュリティを強化するため、Cisco ISE には IPSec 機能があります。IPSec は、送信元を認証し、送信中のデータ変更を検出し、送信されたデータを暗号化することで通信を保護します。

Cisco ISE は、トンネル モードとトランスポート モードで IPSec をサポートしています。Cisco ISE インターフェイスで IPSec を有効にし、ピアを設定すると、通信を保護するため Cisco ISE と NAD の間に IPSec トンネルが作成されます。

事前共有キーを定義するか、または IPSec 認証に X.509 証明書を使用できます。IPSec は、ギガビット イーサネット 1~5 のインターフェイスで有効にできます。IPSec は PSN あたり 1 つの Cisco ISE インターフェイスでのみ設定できます。



(注) ギガビット イーサネット 0 と ボンド 0 (ギガビット イーサネット 0 および ギガビット イーサネット 1 インターフェイスが ボンディング されている場合) は、Cisco ISE CLI の管理 インターフェイスです。ギガビット イーサネット 0 および ボンド 0 では IPSec はサポートされていません。

必要なコンポーネントには次のものがあります。

- Cisco ISE、リリース 2.2
- Cisco IOS ソフトウェア、C5921 ソフトウェア (C5921_I86-UNIVERSALK9-M)、バージョン 15.5(2)T2 (Cisco 5921 埋め込み型サービス ルータ (ESR)) : ESR 5921 設定では、デフォルトでトンネル モードとトランスポート モードで IPSec がサポートされています。Diffie-Hellman Group 14 および Group 16 がサポートされています。



- (注) C5921 ESR ソフトウェアは Cisco ISE リリース 2.2 に付属しています。このソフトウェアを使用可能にするには ESR ライセンスが必要です。ESR ライセンスの情報については、『[Cisco 5921 Embedded Services Router Integration Guide](#)』を参照してください。

Cisco ISE での RADIUS IPsec の設定

Cisco ISE で RADIUS IPsec を設定するには、次の操作を行う必要があります。

ステップ 1 Cisco ISE CLI からインターフェイスで IP アドレスを設定します。

ギガビット イーサネット 1 からギガビット イーサネット 5 インターフェイス（ボンド 1 およびボンド 2）では、IPsec がサポートされています。ただし、IPsec は Cisco ISE ノードの 1 つのインターフェイスでのみ設定できます。

ステップ 2 直接接続ネットワーク デバイスを IPsec ネットワーク デバイス グループに追加します。

(注) RADIUS IPsec では、スタティック ルート ゲートウェイがデバイスのインターフェイスに直接接続している必要があります。

- [管理 (Administration)] > [ネットワーク リソース (Network Resources)] > [ネットワーク デバイス (Network Devices)] の順に選択します。
- [ネットワーク デバイス (Network Devices)] ページで [追加 (Add)] をクリックします。
- 追加するネットワーク デバイスの名前、IP アドレス、サブネットを入力します。
- [IPSEC] ドロップダウンリストから、[はい (Yes)] を選択します。
- [RADIUS 認証設定 (RADIUS Authentication Settings)] チェックボックスをオンにします。
- [共有秘密 (Shared Secret)] フィールドに、ネットワーク デバイスに設定した共有秘密キーを入力します。
- [送信 (Submit)] をクリックします。

ステップ 3 (オプション。スマートライセンスでのみ必要)。Cisco Smart Software Manager (CSSM) とのやりとりのために個別の管理インターフェイスを追加します。また、ESR には [スマート ソフトウェア マネージャ サテライト](#) も使用できます。このためには、Cisco ISE CLI から次のコマンドを実行し、対応する管理インターフェイス（ギガビット イーサネット 1 ～ 5（またはボンド 1 または 2））を選択します。

```
ise/admin# license esr smart {interface}
```

このインターフェイスは、Cisco.com に到達してシスコのオンライン ライセンス サーバにアクセスできる必要があります。

ステップ 4 Cisco ISE CLI から直接接続ゲートウェイにネットワーク デバイスを追加します。

```
ip route [destination network] [network mask] gateway [next-hop address]
```

ステップ 5 IPsec に対し Cisco ISE ノードを有効にします。

- a) [管理 (Administration)] > [システム (System)] > [設定 (Settings)] > [プロトコル (Protocols)] > [IPSec] を選択します。
展開内のすべての Cisco ISE ノードがこのページにリストされます。
- b) IPSec を有効にする Cisco ISE ノードの横のチェックボックスをオンにして、[有効化 (Enable)] オプション ボタンをクリックします。
- c) IPSec 通信に使用するインターフェイスを選択します。
- d) 次のオプションから、選択されている ISE ノードの認証タイプを選択します。
 - [事前共有キー (Pre-shared Key)] : このオプションを選択した場合は、事前共有キーを入力し、ネットワーク デバイスで同じキーを設定する必要があります。事前共有キーには英数字を使用してください。特殊文字はサポートされていません。ネットワーク デバイスで事前共有キーを設定する方法については、ネットワーク デバイスのマニュアルを参照してください。事前共有キー設定の出力例については、[例 : Cisco Catalyst 3850 での事前共有キー設定の出力 \(277 ページ\)](#) を参照してください。
 - [X.509 証明書 (X.509 Certificates)] : このオプションを選択した場合は、Cisco ISE CLI から ESR シェルに進み、ESR 5921 の X.509 証明書を設定してインストールします。次に、ネットワーク デバイスで IPSec を設定します。この説明については、[ESR-5921 での X.509 証明書の設定とインストール \(271 ページ\)](#) を参照してください。
- e) [保存 (Save)] をクリックします。
 - (注) IPSec 設定を直接変更することはできません。IPSec が有効な場合にトンネルまたは認証を変更するには、現在の IPsec トンネルを無効にし、IPSec 設定を変更し、異なる設定で IPSec トンネルを再度有効にします。
 - (注) IPSec が有効になると、Cisco ISE インターフェイスから IP アドレスが削除され、インターフェイスがシャットダウンします。ユーザが Cisco ISE CLI からログインすると、インターフェイスが表示されますが IP アドレスは表示されず、シャットダウン状態になります。この IP アドレスは ESR-5921 インターフェイスで設定されます。

ステップ 6 esr と入力して ESR シェルを開始します。

```
ise/admin# esr
% Entering ESR 5921 shell
% Cisco IOS Software, C5921 Software (C5921_I86-UNIVERSALK9-M), Version 15.5(2)T2, RELEASE SOFTWARE (fc3)
% Technical Support: http://www.cisco.com/techsupport
% Copyright (c) 1986-2015 Cisco Systems, Inc.

Press RETURN to get started, CTRL-C to exit

ise-esr5921>
ise-esr5921>
```

- (注) FIPS に準拠するため、8 文字以上のシークレットパスワードを設定する必要があります。 **Enable secret level 1** コマンドを入力して、パスワードを指定します。

```
ise-esr5921(config)#enable secret level 1 ?
0 Specifies an UNENCRYPTED password will follow
5 Specifies a MD5 HASHED secret will follow
8 Specifies a PBKDF2 HASHED secret will follow
9 Specifies a SCRYPT HASHED secret will follow
LINE The UNENCRYPTED (cleartext) 'enable' secret
```

- (注) カスタム RADIUS ポートを GUI から設定する場合（1645、1646、1812、および 1813 以外）、ESR シェルで次の CLI コマンドを入力し、設定した RADIUS ポートを受け入れます。

```
ip nat inside source static udp 10.1.1.2 [port_number] interface Ethernet0/0 [port_number]
```

ステップ 7 (オプション: ステップ 3 でスマートライセンスを有効にしていない場合にのみ必要)。Classic ライセンスまたは Evaluation ライセンス (有効期間 90 日) を Cisco ISE アプライアンスに追加します。

- Cisco ISE CLI から次のコマンドを実行してライセンス ファイルをダウンロードします。

```
ise/admin# license esr classic import esr.lic repository esrepo
```

Classic ライセンスの詳細については、『[Cisco 5921 Embedded Services Router Integration Guide](#)』の「Licensing the Software with Classic Licensing」を参照してください。

ステップ 8 IPSec トンネルと、IPSec トンネル経由での RADIUS 認証を検証します。

- Cisco ISE にユーザを追加し、ユーザ グループに割り当てます ([管理 (Administration)] > [ID 管理 (Identity Management)] > [ID (Identities)] > [ユーザ (Users)])。
- Cisco ISE と NAD の間で IPSec トンネルが確立されていることを確認します。手順は次のとおりです。

1. ping コマンドを使用して、Cisco ISE と NAD の間の接続が確立されているかどうかをテストします。
2. ESR シェルまたは NAD CLI から次のコマンドを実行して、接続がアクティブ状態であるかどうかを確認します。 **show crypto isakmp sa**

```
ise-esr5921#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst          src          state          conn-id status
192.168.30.1 192.168.30.3  QM_IDLE       1001  ACTIVE
```

3. ESR シェルまたは NAD CLI から次のコマンドを実行して、トンネルが確立されているかどうかを確認します。 **show crypto ipsec sa**

```
ise-esr5921#show crypto ipsec sa

interface: Ethernet0/0
  Crypto map tag: radius, local addr 192.168.30.1

protected vrf: (none)
local  ident (addr/mask/prot/port): (192.168.30.1/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (192.168.30.2/255.255.255.255/0/0)
current_peer 192.168.30.2 port 500
  PERMIT, flags={}
  #pkts encaps: 52, #pkts encrypt: 52, #pkts digest: 52
  #pkts decaps: 57, #pkts decrypt: 57, #pkts verify: 57
  #pkts compressed: 0, #pkts decompressed: 0
```

```
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 192.168.30.1, remote crypto endpt.: 192.168.30.2
plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
current outbound spi: 0x393783B6(959939510)
PFS (Y/N): N, DH group: none

inbound esp sas:
spi: 0x8EA0F6EE(2392913646)
  transform: esp-aes esp-sha256-hmac ,
  in use settings ={Tunnel, }
  conn id: 99, flow_id: SW:99, sibling_flags 80000040, crypto map: radius
  sa timing: remaining key lifetime (k/sec): (4237963/2229)
  IV size: 16 bytes
  replay detection support: Y
  Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcsp sas:

outbound esp sas:
spi: 0x393783B6(959939510)
  transform: esp-aes esp-sha256-hmac ,
  in use settings ={Tunnel, }
  conn id: 100, flow_id: SW:100, sibling_flags 80000040, crypto map: radius
  sa timing: remaining key lifetime (k/sec): (4237970/2229)
  IV size: 16 bytes
  replay detection support: Y
  Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcsp sas:
```

c) 次のいずれかの方法で RADIUS 認証を検証します。

- ステップ 8 (a) で作成したユーザのクレデンシャルを使用してネットワーク デバイスにログインします。RADIUS 認証要求が Cisco ISE ノードに送信されます。[ライブ認証 (Live Authentications)] ページで詳細を確認します。
- エンドホストをネットワーク デバイスに接続し、802.1X 認証を設定します。ステップ 8 (a) で作成したユーザのクレデンシャルを使用してエンドホストにログインします。RADIUS 認証要求が Cisco ISE ノードに送信されます。[ライブ認証 (Live Authentications)] ページで詳細を確認します。

ESR-5921 での X.509 証明書の設定とインストール

ESR-5921 で X.509 証明書を設定およびインストールするには、次の手順を実行します。

ステップ 1 **esr** と入力して ESR シェルを開始します。

```

ise/admin# esr
% Entering ESR 5921 shell
% Cisco IOS Software, C5921 Software (C5921_I86-UNIVERSALK9-M), Version 15.5(2)T2, RELEASE SOFTWARE (fc3)
% Technical Support: http://www.cisco.com/techsupport
% Copyright (c) 1986-2015 Cisco Systems, Inc.

Press RETURN to get started, CTRL-C to exit

ise-esr5921>
ise-esr5921>

```

(注) FIPS に準拠するため、8 文字以上のシークレットパスワードを設定する必要があります。**Enable secret level 1** コマンドを入力して、パスワードを指定します。

```

ise-esr5921(config)#enable secret level 1 ?
0 Specifies an UNENCRYPTED password will follow
5 Specifies a MD5 HASHED secret will follow
8 Specifies a PBKDF2 HASHED secret will follow
9 Specifies a SCRYPT HASHED secret will follow
LINE The UNENCRYPTED (cleartext) 'enable' secret

```

(注) カスタム RADIUS ポートを GUI から設定する場合 (1645、1646、1812、および 1813 以外)、ESR シェルで次の CLI コマンドを入力し、設定した RADIUS ポートを受け入れます。

```
ip nat inside source static udp 10.1.1.2 [port_number] interface Ethernet0/0 [port_number]
```

ステップ 2 次のコマンドを使用して RSA キー ペアを生成します。

例 :

```
crypto key generate rsa label rsa2048 exportable modulus 2048
```

ステップ 3 次のコマンドを使用してトラスト ポイントを作成します。

例 :

```

crypto pki trustpoint trustpoint-name

enrollment terminal
serial-number none
fqdn none
ip-address none
subject-name cn=networkdevicename.cisco.com
revocation-check none
rsa keypair rsa2048

```

ステップ 4 次のコマンドを使用して CSR を生成します。

例 :

```

crypto pki enroll rsaca-mytrustpoint

Display Certificate Request to terminal? [yes/no]: yes

```

ステップ 5 CSR の出力をテキスト ファイルにコピーし、署名のために外部 CA に送信し、署名された証明書と CA 証明書を取得します。

ステップ 6 次のコマンドを使用して CA をインポートします。

例 :

```
crypto pki authenticate rsaca-mytrustpoint
```

CA 証明書の内容（「—BEGIN—」行と「—End—」行を含む）をコピーして貼り付けます。

ステップ 7 次のコマンドを使用して、署名付き証明書をインポートします。

例：

```
crypto pki import rsaca-mytrustpoint
```

署名付き証明書の内容（「—BEGIN—」行と「—End—」行を含む）をコピーして貼り付けます。

以下に、Cisco 5921 ESR で X.509 証明書を設定してインストールするときの出力の例を示します。

```
ise-esr5921#show running-config
!
hostname ise-esr5921
!
boot-start-marker
boot host unix:default-config
boot-end-marker
!
no aaa new-model
bsd-client server url https://cloudsso.cisco.com/as/token.oauth2
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
call-home
! If contact email address in call-home is configured as sch-smart-licensing@cisco.com
! the email address configured in Cisco Smart License Portal will be used as contact email address
to send SCH notifications.
contact-email-addr sch-smart-licensing@cisco.com
profile "CiscoTAC-1"
  active
  destination transport-method http
  no destination transport-method email
!
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
crypto pki trustpoint SLA-TrustPoint
enrollment pkcs12
revocation-check crl
!
crypto pki trustpoint rsaca-mytrustpoint
enrollment terminal
serial-number none
fqdn none
ip-address none
subject-name cn=ise-5921.cisco.com
revocation-check none
rsakeypair rsa2048
!
crypto pki certificate chain SLA-TrustPoint
certificate ca 01
  30820321 30820209 A0030201 02020101 300D0609 2A864886 F70D0101 0B050030
  32310E30 0C060355 040A1305 43697363 6F312030 1E060355 04031317 43697363
  6F204C69 63656E73 696E6720 526F6F74 20434130 1E170D31 33303533 30313934
  3834375A 170D3338 30353330 31393438 34375A30 32310E30 0C060355 040A1305
  43697363 6F312030 1E060355 04031317 43697363 6F204C69 63656E73 696E6720
  526F6F74 20434130 82012230 0D06092A 864886F7 0D010101 05000382 010F0030
  82010A02 82010100 A6BCBD96 131E05F7 145EA72C 2CD686E6 17222EA1 F1EFF64D
```

```

CBB4C798 212AA147 C655D8D7 9471380D 8711441E 1AAF071A 9CAE6388 8A38E520
1C394D78 462EF239 C659F715 B98C0A59 5BBB5CBD 0CFEBEA3 700A8BF7 D8F256EE
4AA4E80D DB6FD1C9 60B1FD18 FFC69C96 6FA68957 A2617DE7 104FDC5F EA2956AC
7390A3EB 2B5436AD C847A2C5 DAB553EB 69A9A535 58E9F3E3 C0BD23CF 58BD7188
68E69491 20F320E7 948E71D7 AE3BCC84 F10684C7 4BC8E00F 539BA42B 42C68BB7
C7479096 B4CB2D62 EA2F505D C7B062A4 6811D95B E8250FC4 5D5D5FB8 8F27D191
C55F0D76 61F9A4CD 3D992327 A8BB03BD 4E6D7069 7CBADF8B DF5F4368 95135E44
DFC7C6CF 04DD7FD1 02030100 01A34230 40300E06 03551D0F 0101FF04 04030201
06300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604 1449DC85
4B3D31E5 1B3E6A17 606AF333 3D3B4C73 E8300D06 092A8648 86F70D01 010B0500
03820101 00507F24 D3932A66 86025D9F E838AE5C 6D4DF6B0 49631C78 240DA905
604EDCDE FF4FED2B 77FC460E CD636FDB DD44681E 3A5673AB 9093D3B1 6C9E3D8B
D98987BF E40CBD9E 1AECA0C2 2189BB5C 8FA85686 CD98B646 5575B146 8DFC66A8
467A3DF4 4D565700 6ADF0F0D CF835015 3C04FF7C 21E878AC 11BA9CD2 55A9232C
7CA7B7E6 C1AF74F6 152E99B7 B1FCF9BB E973DE7F 5BDDEB86 C71E3B49 1765308B
5FB0DA06 B92AFE7F 494E8A9E 07B85737 F3A58BE1 1A48A229 C37C1E69 39F08678
80DDCD16 D6BACECA EEB7C7CF 8428787B 35202CDC 60E4616A B623CDBD 230E3AFB
418616A9 4093E049 4D10AB75 27E86F73 932E35B5 8862FDAE 0275156F 719BB2F0
D697DF7F 28
quit
crypto pki certificate chain rsaca-mytrustpoint
certificate 39
30820386 3082026E A0030201 02020139 300D0609 2A864886 F70D0101 0B050030
61310B30 09060355 04061302 5553310B 30090603 5504080C 024E4331 0C300A06
03550407 0C035254 50310E30 0C060355 040A0C05 43495343 4F310C30 0A060355
040B0C03 53544F31 19301706 03550403 0C107273 6163612E 65726368 616F2E63
6F6D301E 170D3136 30393031 32313037 34335A17 0D313730 39303132 31303734
335A301D 311B3019 06035504 03131269 73652D35 3932312E 63697363 6F2E636F
6D308201 22300D06 092A8648 86F70D01 01010500 0382010F 00308201 0A028201
0100EE87 CABFBA18 7E0405A8 ACAAAB23 E7CB6109 2CF98BAE 8EE93536 BF1EBBD3
73E60BE7 F430B5AF EBF8B0C5 969B2828 A6783BB4 64E333E4 29C8744E 6E783617
194AF1B0 7F04B4EA B89FD6EB F9C4F2DD 196DC6E0 CAA49B8B 665B6E0D 2FBC1D2F
8E8181B9 60FAE126 D1B2E4E4 1F321A97 10C1B76A C2BB3174 361B13FA 2CB7BDFE
22C0C33F 2792D714 C41E2237 00B1AE49 6593DCC3 A799D526 D81F9706 A71DA14E
5ED76038 7A2C84B4 C668E35C 337BA1DC 9CA56AC2 C8E0059F 660CE39C 925310A0
F9A21FFB 3C3C507A 20B924F7 E0125D60 6552321C 35736079 42449401 15E68DA6
B4776DAA FB5AFDF8 59E31373 263175E3 1F14416A 24C21D69 A46173B6 96CC84FB
5B9D0203 010001A3 818C3081 89300906 03551D13 04023000 302C0609 60864801
86F84201 0D041F16 1D4F7065 6E53534C 2047656E 65726174 65642043 65727469
66696361 7465301D 0603551D 0E041604 146DD31C 03690B98 330B67FA 6EDC7B20
F99FB924 60301F06 03551D23 04183016 8014966A 0C21AF96 3E827690 423599CC
EE8087A1 2909300E 0603551D 0F0101FF 04040302 05A0300D 06092A86 4886F70D
01010B05 00038201 0100C0B9 D2845D97 6FFC16DB 01559659 BC1DECA6 E1A01965
1F6CD459 E03D7ABE 91179FEB 08BF5B9B 84B62C36 236F528E E30C921C 81DA29E1
EA3DFDC1 B0B0EEBA 14EADAEC 078576E4 D643A0EF 7D8E0880 C5FC3965 811B08C0
5696DBF5 FADA4092 ACF549B8 2257F508 636D52AA 6CDC9596 AB43313F 6C33C9C1
2CFDDBE3 EA9D407C 8D1B0F49 BBACD0CD 2832AC12 CD3FEFC8 501E1639 A4EFDC27
69CA0147 971A1B2D DB2758E6 A84AFC86 4F9A4942 3D7EDBCC 7BDCC1BB 61F69B31
BF13E39B 10AAC31C 55E73C8B C30BE516 7C506FF4 AC367D94 814A6880 EF201A6D
CD2E1A95 7BBEC982 01CE867D 931F56E1 1EF1C457 9DC9A0BE 9DB2DC9B 19873585
89AE82F6 A37E51D6 EECB
quit
certificate ca 008DD3A81106B14664
308203A2 3082028A A0030201 02020900 8DD3A811 06B14664 300D0609 2A864886
F70D0101 05050030 61310B30 09060355 04061302 5553310B 30090603 5504080C
024E4331 0C300A06 03550407 0C035254 50310E30 0C060355 040A0C05 43495343
4F310C30 0A060355 040B0C03 53544F31 19301706 03550403 0C107273 6163612E
65726368 616F2E63 6F6D301E 170D3135 31303231 32313135 34335A17 0D323531
30313832 31313534 335A3061 310B3009 06035504 06130255 53310B30 09060355
04080C02 4E43310C 300A0603 5504070C 03525450 310E300C 06035504 0A0C0543
4953434F 310C300A 06035504 0B0C0353 544F3119 30170603 5504030C 10727361
63612E65 72636861 6F2E636F 6D308201 22300D06 092A8648 86F70D01 01010500
0382010F 00308201 0A028201 0100CB82 2AECCE38 1BCB27B9 FA5F2FBD 8609B190
16A6F741 5BEC18B8 8B260CAF 190EA1CE 063BC558 556DC085 6FAC5425 14AFE225

```



```
0E9E3A12 05F3DA7E D17E03F2 7FFE92FB 38D67027 DBC5C175 EB53E96B 66C20D11
B4C32D38 AE04385C 8FD4CB74 31A97824 CA1CAFD5 091806C3 6F9CBF8D DC42DD5B
D985703D F3BB9ED1 7DE99614 422D765C 86AB25CD E80008C5 22049BE8 66D1CA27
E1EB6D4F 4FD3CC18 E091BBF0 6FE0EB52 B33F231A 6D6B7190 4196C929 D22E2C42
B9CD2BBD 24550E82 8CD8838F C41B4DAD 2FA1636A 5787BBB2 F21E4718 335B005B
DFBE6EA7 56EBE30B D52DE85F FFAF0189 E372CBFC 44BFF235 4DA7C9EF DAAC6D0A
A196DA5A 1B525175 C26B3581 EA4B0203 010001A3 5D305B30 1D060355 1D0E0416
0414966A 0C21AF96 3E827690 423599CC EE8087A1 2909301F 0603551D 23041830
16801496 6A0C21AF 963E8276 90423599 CCEE8087 A1290930 0C060355 1D130405
30030101 FF300B06 03551D0F 04040302 02A4300D 06092A86 4886F70D 01010505
00038201 01002334 A3F0E5D3 4D229985 67A07754 73EC52E3 05B7D05F 926CC863
220F849B 861C36B2 EF7C3485 474D4EF0 73895879 CAE08BBB 183B7CFA A20C4354
86C6D9DF D445DACE C252C608 236F6673 F3F3C329 474B22E8 660BF91E 41054B8D
43B80E44 AE69C164 2C9F41A2 8284F577 21FFAB8E A6771A5E DD34EBE4 A0DC2EAD
95702010 02964566 478DA90F 5E134643 81A5F5EA 362D0394 1F9F23D1 DEE50B07
12938299 1AF11A36 82DAFC6A 164B2F66 8B0AB7CC 9A723EBC B50E740B 0A9270E3
60E2ED42 7F10D1A6 F6735144 AE93BF86 3D5A0502 6811D2BD 6E694693 28DE84C5
3747CF0A D2B8D6C9 6CBEB0A0 D1137CF8 E31CBF6B 437D82DD D74A4A9F 3557B3D9
D0BD055F 65A8
quit
license udi pid CISCO5921-K9 sn 9XG4481W768
username lab password 0 lab
!
redundancy
!
crypto keyring MVPN-spokes
rsa-publickey address 0.0.0.0
address 0.0.0.0
key-string
quit
!
crypto isakmp policy 10
encr aes
hash sha256
group 16
!
crypto isakmp policy 20
encr aes
hash sha256
group 14
crypto isakmp profile MVPN-profile
description LAN-to-LAN for spoke router(s) connection
keyring MVPN-spokes
match identity address 0.0.0.0
!
crypto ipsec transform-set radius esp-aes esp-sha256-hmac
mode tunnel
crypto ipsec transform-set radius-2 esp-aes esp-sha256-hmac
mode transport
!
crypto dynamic-map MVPN-dynmap 10
set transform-set radius radius-2
!
crypto map radius 10 ipsec-isakmp dynamic MVPN-dynmap
!
interface Ethernet0/0
description e0/0->connection to external NAD
ip address 192.168.20.1 255.255.255.0
ip nat outside
ip virtual-reassembly in
no ip route-cache
crypto map radius
!
interface Ethernet0/1
```

```

description e0/1->tap0 internal connection to ISE
ip address 10.1.1.1 255.255.255.252
ip nat inside
ip virtual-reassembly in
no ip route-cache
!
interface Ethernet0/2
no ip address
shutdown
!
interface Ethernet0/3
no ip address
shutdown
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
ip nat inside source list 1 interface Ethernet0/0 overload
ip nat inside source static udp 10.1.1.2 1645 interface Ethernet0/0 1645
ip nat inside source static udp 10.1.1.2 1646 interface Ethernet0/0 1646
ip nat inside source static udp 10.1.1.2 1812 interface Ethernet0/0 1812
ip nat inside source static udp 10.1.1.2 1813 interface Ethernet0/0 1813
!
access-list 1 permit 10.1.1.0 0.0.0.3
!
control-plane
!
line con 0
logging synchronous
line aux 0
line vty 0 4
login
transport input none
!
end

```

以下に、Cisco Catalyst 3850 で X.509 証明書を設定してインストールするときの出力の例を示します。

```

cat3850#show running-config

enable password lab
!
username lab password 0 lab
aaa new-model

!

aaa group server radius ise
server name ise-vm
deadtime 60
!
aaa authentication login default group radius local

aaa authentication enable default group radius enable

!

crypto isakmp policy 10

encr aes

hash sha256
authentication rsa-sig
group 16

```

```
!  
crypto ipsec security-association lifetime seconds 86400  
!  
crypto ipsec transform-set radius esp-aes esp-sha256-hmac  
mode tunnel  
  
!  
  
crypto ipsec profile radius-profile  
  
!  
  
crypto map radius 10 ipsec-isakmp  
set peer 192.168.20.1  
set transform-set radius  
  
match address 100  
  
!  
  
interface GigabitEthernet1/0/1  
no switchport  
ip address 192.168.20.2 255.255.255.0  
  
crypto map radius  
  
!  
access-list 100 permit ip host 192.168.20.2 host 192.168.20.1  
!  
snmp-server community public RO  
snmp-server community private RW  
!  
radius server rad-ise  
address ipv4 192.168.20.1 auth-port 1645 acct-port 1646  
  
key secret
```

例 : Cisco Catalyst 3850 での事前共有キー設定の出力

Cisco Catalyst 3850 で事前共有キーを設定する場合の出力の例を次に示します。

```
cat3850#show running-config  
  
enable password lab  
!  
username lab password 0 lab  
aaa new-model  
!  
aaa group server radius ise  
server name ise-vm  
deadtime 60  
!  
aaa authentication login default group radius local  
  
aaa authentication enable default group radius enable  
  
!  
  
crypto isakmp policy 10
```

```

encr aes

hash sha256
authentication pre-share
group 16
crypto isakmp key 123456789 address 0.0.0.0
!
crypto ipsec security-association lifetime seconds 86400
!
crypto ipsec transform-set radius esp-aes esp-sha256-hmac
mode tunnel
!
crypto ipsec profile radius-profile
!
crypto map radius 10 ipsec-isakmp
set peer 192.168.20.1
set transform-set radius
match address 100
!
interface GigabitEthernet1/0/1
no switchport
ip address 192.168.20.2 255.255.255.0

crypto map radius
!
access-list 100 permit ip host 192.168.20.2 host 192.168.20.1
!
snmp-server community public RO
snmp-server community private RW
!
radius server rad-ise
address ipv4 192.168.20.1 auth-port 1645 acct-port 1646

key secret

```

Mobile Device Manager と Cisco ISE との相互運用性

モバイルデバイス管理（MDM）サーバはモバイル事業者、サービスプロバイダー、企業にわたって展開されたモバイルデバイスの保護、モニタ、管理、およびサポートを行います。MDMサーバはポリシーサーバとして機能し、ポリシーサーバは展開環境のモバイルデバイスにある一部のアプリケーション（電子メールアプリケーションなど）の使用を制御します。ただし、ネットワークは、ACLに基づいてエンドポイントへのきめ細かいアクセス権を提供できる唯一のエンティティです。Cisco ISEは必要なデバイス属性についてMDMサーバにクエリを行い、それらのデバイスに対してネットワークアクセスコントロールを提供するACLを作成します。

さまざまなベンダーからのサーバなど、複数のアクティブなMDMサーバをネットワークで実行できます。これにより、ロケーションやデバイスタイプなどのデバイスの要因に基づいて、異なるMDMサーバに異なるエンドポイントをルーティングすることができます。

また、Cisco ISEは、シスコのMDM APIバージョン2を使用してMDMサーバと統合し、デバイスがAnyConnect 4.1 およびCisco ASA 9.3.2以降を介してVPN経由でネットワークにアクセスできるようにします。

この図では、Cisco ISEが適用ポイントで、MDMポリシーサーバがポリシー情報ポイントです。Cisco ISEは、MDMサーバからデータを取得して、完全なソリューションを提供します。

図 11: MDM の Cisco ISE との相互運用性

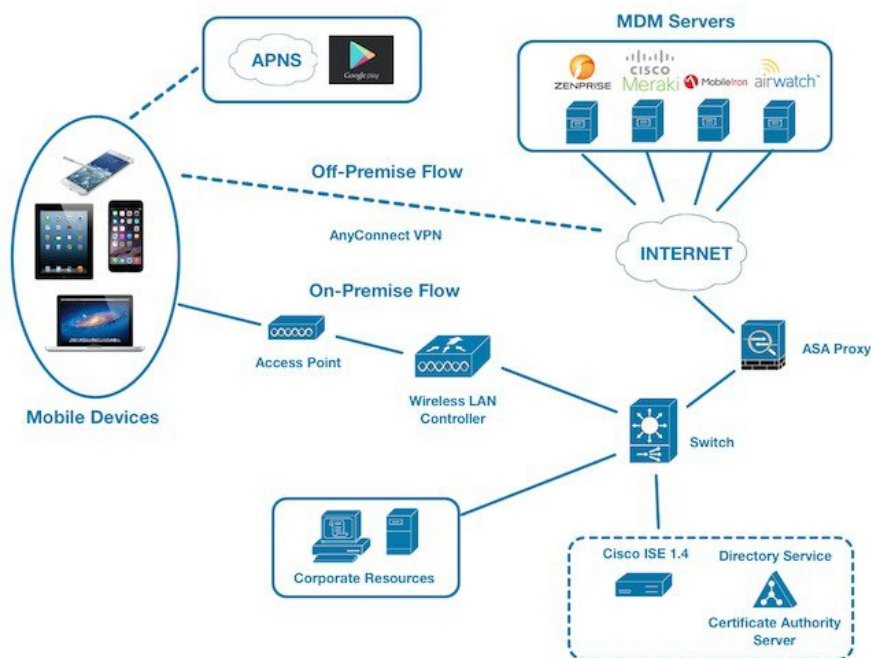


表 10: MDM 設定で使用するコンポーネント

コンポーネント	仕様
Cisco Identity Services Engine, Release 2.0	次のいずれか：ISE 3495、または VMware
MDM サーバ	—
(任意) 認証権限サーバ	Microsoft の仕様どおり (Windows 2008 R2 Enterprise SP2、Windows 2012 R2)
ワイヤレス LAN コントローラ (WLC) (Wireless LAN Controller (WLC))	<ul style="list-style-type: none"> ハードウェア：5500 シリーズ、2500 シリーズ、WLSM-2 ソフトウェア：Unified Wireless Network ソフトウェア、リリース 7.2、WLC 8.1
モバイル デバイス	<p>MDM ベンダーでサポートされているデバイス。</p> <p>たとえば、Apple iOS 5.0 以降、Google Android 3.x 以降。</p>

1 つ以上の外部 Mobile Device Manager (MDM) サーバと相互運用するように Cisco ISE を設定できます。サードパーティのこのタイプの接続を設定することによって、MDM データベースにある詳細情報を活用できます。Cisco ISE は REST API コールを使用して、外部 MDM サーバから情報を取得します。Cisco ISE はスイッチ、アクセスルータ、ワイヤレス アクセス ポイン

ト、その他のネットワーク アクセス ポイントに適切なアクセス コントロール ポリシーを適用して、Cisco ISE ネットワークへのリモート デバイス アクセスをより適切に制御します。

サポートされる MDM ベンダーは次のとおりです。 [サポートされる MDM サーバ \(281 ページ\)](#)

サポートされる MDM の使用例

Cisco ISE が外部 MDM サーバと連携して実行する機能は、次のとおりです。

- デバイス登録の促進：ネットワークにアクセスする未登録のエンドポイントは、MDM サーバ上でホストされている登録ページにリダイレクトされ、ユーザ ロール、デバイス タイプなどに基づいて登録されます。
- デバイスの修復の処理：エンドポイントには制限付きアクセス権だけが付与されます。
- エンドポイント データの増加：Cisco ISE プロファイラを使用して収集できない、MDM サーバの情報でエンドポイント データベースを更新します。エンドポイントが MDM のモニタ対象デバイスの場合、Cisco ISE は **[ワーク センター (Work Centers)] > [ネットワーク アクセス (Network Access)] > [ID (Identities)] > [エンドポイント (Endpoints)]** ページを使用して表示できる 6 つのデバイス属性を使用します。次に例を示します。
 - MDMMei: 99 000100 160803 3
 - MDMManufacturer: Apple
 - MDMMModel: iPhone
 - MDMMOSVersion: iOS 6.0.0
 - MDMPhoneNumber: 9783148806
 - MDMSerialNumber: DNPGQZGUDTF9
- Cisco ISE は、4 時間ごとに MDM サーバをポーリングし、デバイス コンプライアンス データを確認します。これは管理者が設定できます。
- MDM サーバを介したデバイス手順の発行：MDM サーバを介してユーザのデバイスに対するリモートアクションを発行します。管理者は、ISE コンソールからリモート操作を開始します。

Cisco ISE では、次の属性に基づいて MDM ポリシーを設定できます。

- DeviceRegisterStatus
- DeviceCompliantStatus
- DiskEncryptionStatus
- PinLockStatus
- JailBrokenStatus
- Manufacturer
- IMEI

- SerialNumber
- OsVersion
- PhoneNumber
- MDMServerName
- MDMServerReachable
- MEID
- モデル
- UDID

サポートされる MDM サーバ

サポートされる MDM サーバは、次のベンダーの製品です。

- 絶対値 (Absolute)
- AirWatch
- Citrix XenMobile
- Globo
- Good Technology
- IBM MaaS360
- JAMF ソフトウェア
- Meraki SM/EMM
- MobileIron



(注) 一部のバージョンの MobileIron は ISE では動作しません。MobileIron はこの問題を認識しており、修正があります。詳細については、MobileIron までご連絡ください。

- SAP Afaria
- SOTI
- Symantec
- Tangoe
- Microsoft Intune - モバイル デバイス用
- Microsoft SCCM - デスクトップ デバイス用

[ISE コミュニティ リソース](#)[How To: Meraki EMM / MDM Integration with ISE](#)

MDM サーバにより使用されるポート

次の表に、相互に通信ができるように Cisco ISE と MDM サーバ間で開く必要のあるポートを示します。MDM エージェントおよびサーバで開く必要があるポートのリストについては、MDM サーバのドキュメントを参照してください。

表 11: MDM サーバにより使用されるポート

MDM サーバ	ポート
MobileIron	443
Zenprise	443
Good	19005
Airwatch	443
Afaria	443
Fiberlink MaaS	443
Meraki	443
Microsoft Intune	80 および 443
Microsoft SCCM	80 および 443

MDM デクショナリ属性

Cisco ISE に MDM サーバ定義を追加すると、MDM デクショナリ属性は Cisco ISE で使用可能になり、許可ポリシーで使用できます。許可ポリシーに使用可能なデクショナリ属性を表示できます。

MDM 統合プロセス フロー

ここでは、MDM 統合プロセスについて説明します。

1. ユーザはデバイスを SSID に関連付けます。
2. Cisco ISE は、MDM サーバに対して API コールを実行します。
3. この API コールは、このユーザのデバイスとデバイスのポスチャ ステータスのリストを返します。



(注) 入力パラメータは、エンドポイントデバイスの MAC アドレスです。構外の Apple iOS デバイスの場合は UDID です。

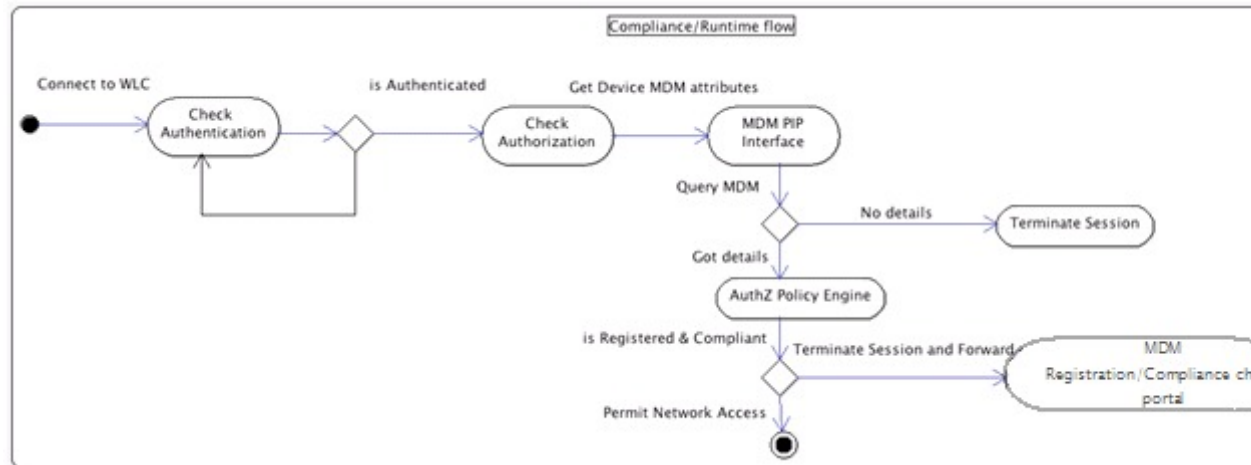
4. ユーザのデバイスがこのリストにない場合、デバイスが登録されていないことを意味します。Cisco ISE は、Cisco ISE にリダイレクトされる許可要求を NAD に送信します。ユーザが MDM サーバ ページに表示されます。



(注) MDM ポータルを介して Cisco ISE ネットワークの外の MDM サーバに登録済みのデバイスを登録する必要があります。これは Cisco ISE、リリース 1.4 以降に適用されます。ISE の以前のバージョンでは、Cisco ISE ネットワークの外に登録済みのデバイスはポスチャ ポリシーに準拠している場合に自動的に登録されます。

5. Cisco ISE は、MDM を使用してデバイスをプロビジョニングし、デバイスを登録するための適切なページをユーザに表示します。
6. ユーザは MDM サーバにデバイスを登録し、MDM サーバは Cisco ISE に要求をリダイレクトします（自動リダイレクションまたは手動のブラウザ リフレッシュによって）。
7. Cisco ISE は MDM サーバに対して再度ポスチャ ステータスのクエリーを実行します。
8. ユーザのデバイスが MDM サーバで設定されているポスチャ（コンプライアンス）ポリシーに準拠していない場合、デバイスがポリシーに準拠しておらず、準拠する必要があることがユーザに通知されます。
9. ユーザのデバイスがポリシーに準拠するようになった後、MDM のサーバは内部テーブルのデバイスのステータスを更新します。
10. ここでユーザがブラウザをリフレッシュすると、制御が Cisco ISE に返されます。
11. Cisco ISE はコンプライアンス情報を取得するために MDM サーバを 4 時間ごとにポーリングし、必要に応じて許可変更（CoA）を発行します。これは管理者が設定できます。また、Cisco ISE は 5 分ごとに MDM サーバをチェックして使用できるかどうかを確認します。

次の図は、MDM プロセス フローを示しています。



(注) 一度に 1 つの MDM サーバに登録できるデバイスは 1 台のみです。別のベンダーから MDM サービスに同じデバイスを登録する場合、デバイスから前のベンダーのプロファイルを削除する必要があります。MDM サービスは通常、「企業ワイプ」を提供し、これはデバイスからベンダーの設定のみを削除します（デバイス全体ではありません）。ユーザはこのファイルを削除することもできます。たとえば、IOS デバイスで、[設定 (Settings)] > [全般 (General)] > [デバイス管理 (Device management)] の順に移動し、削除の管理をクリックすることができます。または、ISE の MyDevices ポータルに移動し、企業ワイプをクリックすることができます。

Cisco ISE による MDM サーバの設定

Cisco ISE で MDM サーバを設定するには、次の高レベル タスクを実行します。

- ステップ 1 Azure に PAN の証明書をインポートする Intune を除き、Cisco ISE に MDM のサーバ証明書をインポートします。
- ステップ 2 Mobile Device Manager の定義を作成します。
- ステップ 3 ワイヤレス LAN コントローラの ACL を設定します。
- ステップ 4 未登録のデバイスをリダイレクトするための許可プロファイルを設定します。
- ステップ 5 ネットワークに複数の MDM サーバがある場合は、各ベンダーに個別の許可プロファイルを設定します。
- ステップ 6 MDM 使用例の許可ポリシー ルールを設定します。

Cisco ISE への MDM サーバ証明書のインポート

Cisco ISE を MDM サーバに接続するには、Cisco ISE 証明書ストアに MDM サーバ証明書をインポートする必要があります。MDM サーバに CA 署名付き証明書がある場合は、Cisco ISE 証明書ストアにルート CA をインポートする必要があります。



(注) Microsoft Azure の場合は、ISE 証明書を Azure にインポートします。詳細については、[MDM サーバとしての Microsoft Intune の設定 \(289 ページ\)](#) を参照してください。

- ステップ 1 MDM サーバ証明書を MDM サーバからエクスポートして、ローカルマシンに保存します。
- ステップ 2 [管理 (Administration)] > [システム (System)] > [証明書 (Certificates)] > [信頼できる証明書 (Trusted Certificate)] > [インポート (Import)] を選択します。
- ステップ 3 [参照 (Browse)] をクリックして、MDM サーバから取得した MDM サーバ証明書を選択します。
- ステップ 4 わかりやすい名前を追加します。
- ステップ 5 [ISE内の認証用に信頼する (Trust for authentication within ISE)] チェックボックスをオンにします。
- ステップ 6 [送信 (Submit)] をクリックします。
- ステップ 7 [証明書ストア (Certificate Store)] リスト ページに MDM サーバ証明書が一覧表示されることを確認します。

次のタスク

[ISE でのモバイル デバイス管理サーバの定義 \(285 ページ\)](#)

ISE でのモバイル デバイス管理サーバの定義

外部 MDM サーバ用のモバイル デバイス管理 (MDM) 定義とデスクトップ デバイス マネージャ (SCCM) 定義を 1 つ以上作成できます。

1. [管理 (Administration)] > [ネットワーク リソース (Network Resources)] > [外部 MDM (External MDM)] の順に選択します。
2. [追加 (Add)] をクリックします。
3. 追加する MDM サーバの名前と説明を入力します。
4. [サーバタイプ (Server Type)] で、[モバイル デバイス マネージャ (Mobile Device Manager)] または [デスクトップ デバイス マネージャ (Desktop Device Manager)] を選択します。どちらを選択するかで、どのフィールドが次に表示されるかが決定します。[デスクトップ デバイス マネージャ (Desktop Device Manager)] を選択した場合は、「[デスク](#)

[トップデバイス管理 \(287ページ\)](#)]に進みます。[モバイルデバイスマネージャ (Mobile Device Manager)]を選択した場合は、次の手順を続行します。

5. [認証タイプ (Authentication Type)]で、[ベーシック (Basic)]または[OAuth - クライアント クレデンシャル (OAuth - Client Credentials)]を選択します。Microsoft Intune サーバを設定する [OAuth - クライアント クレデンシャル (OAuth - Client Credentials)]を選択した場合は、「[モバイル デバイス管理 - OAuth - クライアント クレデンシャル \(Mobile Device Management - OAuth - Client Credentials\) \(286 ページ\)](#)」に進みます。[ベーシック (Basic)]を選択した場合は、次の手順を続行します。
6. すべての画面で、MDM サーバ定義の名前と説明が求められます。ここでは、サーバと認証タイプに基づいて、その他のフィールドと手順について説明しています。

モバイル デバイス管理 : ベーシック

- [ホスト名 / IP アドレス (Host Name / IP Address)] : MDM サーバのホスト名または IP アドレスを入力します。
 - **ポート (Port)** : MDM サーバとの接続に使用するポートを入力します。通常は 443。
 - **インスタンス名 (Instance Name)** : この MDM サーバに複数のインスタンスがある場合に、接続するインスタンスを入力します。
 - [ポーリング間隔 (Polling Interval)] : Cisco ISE が MDM サーバをポーリングしてコンプライアンス チェック情報を確認するためのポーリング間隔 (分単位) を入力します。MDM サーバ上のポーリング間隔に一致するようにこの値を設定します。有効な範囲は 15 ~ 240 分です。デフォルト値は 240 分です。ネットワーク上の少数のアクティブクライアントをテストする場合のみポーリング間隔を 60 分未満に設定することを推奨します。多くのアクティブクライアントを持つ実稼働環境でこの値を 60 分未満に設定すると、システムの負荷が大幅に増加し、パフォーマンスに悪影響を与える場合があります。
- ポーリング間隔を 0 に設定すると、ISE は MDM サーバとの通信をディセーブルにします。

モバイル デバイス管理 - OAuth - クライアント クレデンシャル (Mobile Device Management - OAuth - Client Credentials)

OAuth を使用するには、OAuth サーバの設定が必要です。これについては、次で説明します。
[MDM サーバとしての Microsoft Intune の設定 \(289 ページ\)](#)

- [自動検出 URL (Auto Discovery URL)] : 前のステップの [Microsoft Azure AD Graph API エンドポイント (Microsoft Azure AD Graph API Endpoint)] の値を入力します。この URL は、アプリケーションが Graph API を使用して Microsoft Azure AD ディレクトリのデータに直接アクセスできるエンドポイントです。URL の形式は `https://<hostname>/<tenant id>`、たとえば、`https://graph.ppe.windows.net/47f09275-5bc0-4807-8aae-f35cb0341329` です。この URL の拡大バージョンもプロパティ ファイルに含まれます。形式は、`https://<Graph_API_Endpoint>/<TenantId_Or_Domain>/servicePrincipalsByAppId/<Microsoft Intune AppId>/serviceEndpoints?api-version=1.6&client-request-id=<Guid.NewGuid()>` です。

- **クライアント ID (Client ID)** : アプリケーションの固有識別子。アプリケーションが、Microsoft Azure AD Graph API、Microsoft Intune API などの他のアプリケーションのデータにアクセスする場合に、この属性を使用します。
- **トークン発行 URL (Token Issuing URL)** : 前のステップの [OAuth2.0 認証エンドポイント (Oauth2.0 Authorization Endpoint)] の値を入力します。これは、アプリケーションが OAuth2.0 を使用してアクセス トークンを取得できるエンドポイントです。アプリケーションが認証されると、Microsoft Azure AD はアプリケーション (ISE) にアクセス トークンを発行します。このトークンを使用するとアプリケーションから Graph API/Intune API を呼び出すことができます。
- **トークン対象者 (Token Audience)** : トークンが対象とする受信者リソース。パブリックの既知の Microsoft Intune API の APP ID URL。
- **[ポーリング間隔 (Polling Interval)]** : Cisco ISE が MDM サーバをポーリングしてコンプライアンス チェック情報を確認するためのポーリング間隔 (分単位) を入力します。MDM サーバ上のポーリング間隔に一致するようにこの値を設定します。有効な範囲は 15 ~ 240 分です。デフォルト値は 240 分です。ネットワーク上の少数のアクティブクライアントをテストする場合のみポーリング間隔を 60 分未満に設定することを推奨します。多くのアクティブクライアントを持つ実稼働環境でこの値を 60 分未満に設定すると、システムの負荷が大幅に増加し、パフォーマンスに悪影響を与える場合があります。
ポーリング間隔を 0 に設定すると、ISE は MDM サーバとの通信をディセーブルにします。

デスクトップ デバイス管理

次の設定では、ISE と通信できるように SCCM サーバの WMI を設定する必要があります。詳細については、[ISE 用の Microsoft SCCM サーバの設定 \(293 ページ\)](#) を参照してください。

- **[ホスト名 / IP アドレス (Host Name / IP Address)]** : MDM サーバのホスト名または IP アドレスを入力します。
- **サイトまたはインスタンス名 (Site or Instance Name)** : サイト名または、MDM サーバに複数のインスタンスがある場合はインスタンス名を入力します。

Microsoft Intune および SCCM のための ISE MDM サポート

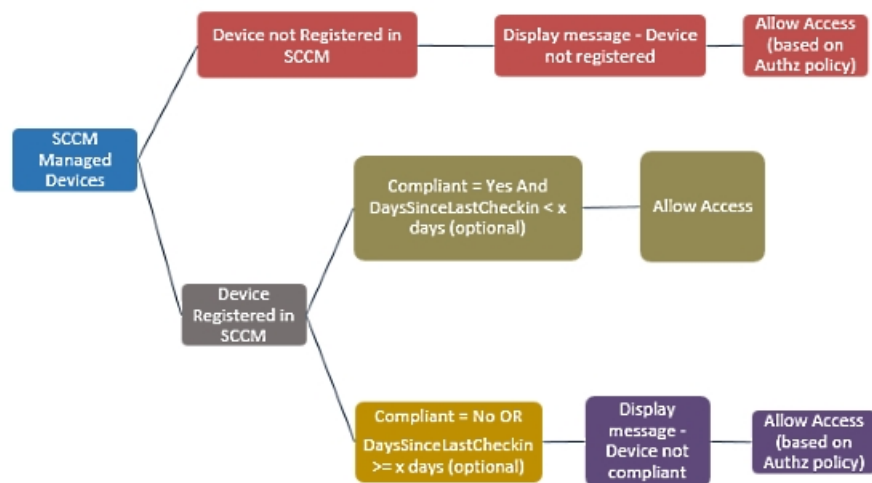
- **Microsoft Intune** : MDM-ISE はパートナー MDM サーバ管理モバイル デバイスとして、Microsoft の Intune デバイス管理をサポートします。
Intune サーバ管理モバイル デバイスの OAuth 2.0 クライアント アプリケーションとして ISE を設定します。ISE は、Azure からトークンを取得し、ISE Intune アプリケーションとのセッションを確立します。
Intune がクライアント アプリケーションとどのように通信するかについての詳細は、<https://msdn.microsoft.com/en-us/library/azure/dn645543.aspx> を参照してください。
- **デスクトップ デバイス マネージャ (Microsoft SCCM)** : ISE は Microsoft System Center Configuration Manager (SCCM) を Windows コンピュータの管理用パートナー MDM サー

バとしてサポートします。ISE は、WMI を使用してコンプライアンス情報を SCCM サーバから取得し、その情報を使用してユーザの Windows デバイスへのネットワーク アクセスを許可または拒否します。

SCCM のワークフロー

ISE はデバイスが登録されているかについて、また登録済みの場合は準拠しているかどうかについて SCCM サーバから情報を取得できます。次の図に、SCCM により管理されるデバイス用のワークフローを示します。

図 12: SCCM のワークフロー



デバイスを接続し、SCCM ポリシーが一致すると、ISE はコンプライアンスと最終ログイン（チェックイン）時間を取得するために、許可ポリシーで指定されている SCCM サーバを照会します。この情報を使用して、ISE はエンドポイントのリストのデバイスのコンプライアンスステータスと lastCheckinTimeStamp を更新します。

デバイスが準拠していないか SCCM に登録されていない、およびリダイレクトプロファイルが許可ポリシーで使用されている場合、デバイスが準拠していないか SCCM に登録されていないというメッセージがユーザに表示されます。ユーザがメッセージを受け取った後、ISE は SCCM 登録サイトへ CoA を発行できます。承認ポリシーおよびプロファイルに基づいてユーザにアクセスを許可できます。

Microsoft SCCM サーバ接続の監視

ポーリングは SCCM 用に設定できません。

ISE は、SCCM サーバへの接続を検証し、ISE が SCCM サーバへの接続を失うとアラームを発生させる、MDM ハートビートジョブを実行します。ハートビートジョブの間隔は設定できません。

MDM サーバとしての Microsoft Intune の設定

ISE の MDM サーバとして Microsoft Intune を設定することは、他の MDM サーバの設定とは少し異なります。Azure への ISE の接続および ISE への Azure の接続を設定するには、次の手順を使用します。

- パブリック証明書を Intune/Azure Active Directory テナントから取得し、ISE にインポートして SSL ハンドシェイクをサポートします。
 1. サイトがテナントを持つ Intune 管理コンソールまたは Azure 管理コンソールにログインします。
 2. ブラウザを使用して証明書の詳細を取得します。たとえば、Internet Explorer の場合は次のように操作します。
 1. ブラウザのツールバーのロックシンボルをクリックしてから、[証明書の表示 (View Certificates)] をクリックします。
 2. [証明書 (Certificate)] ウィンドウで、[認証パス (Certification Path)] タブを選択します。
 3. Baltimore Cyber Trust ルートを見つけて、そのルート証明書をエクスポートします。
 3. ISE で、[管理 (Administration)] > [システム (System)] > [証明書 (Certificates)] > [信頼できる証明書 (Trusted Certificates)] の順に選択し、保存したルート証明書をインポートします。証明書に Azure MDM などのわかりやすい名前を付けます。
- ISE 自己署名証明書をエクスポートし、Intune/Azure 用に準備をします。
 - PAN で、[管理 (Administration)] > [システム (System)] > [証明書 (Certificates)] > [システム証明書 (System Certificates)] の順に移動し、デフォルトの自己署名サーバ証明書を選択して、[エクスポート (Export)] をクリックします。
 - [証明書のみエクスポート (Export Certificate Only)] (デフォルト) を選択し、保存する場所を選択します。

エクスポートされた証明書ファイルに次の PowerShell スクリプトを実行します。

```
$cer = New-Object System.Security.Cryptography.X509Certificates.X509Certificate2
$cer.Import("mycer.cer")
$bin = $cer.GetRawCertData()
$base64Value = [System.Convert]::ToBase64String($bin)

$bin = $cer.GetCertHash()
$base64Thumbprint = [System.Convert]::ToBase64String($bin)

$keyid = [System.Guid]::NewGuid().ToString()
```

次の手順で使用するため、\$base64Thumbprint、\$base64Value、\$keyid の値をメモしておきます。

- Intune で ISE アプリケーションを作成します。

1. Microsoft Azure 管理ポータルで顧客ドメインにサインインし、[ディレクトリ (Directory)] > [アプリケーション (Applications)] > [アプリケーションの追加 (Add an Application)] に移動して、[自分の組織が開発中のアプリケーションの追加 (Add an application my organization is developing)] を選択します。
2. 次のパラメータを使用して、Azure で ISE アプリケーションを設定します。
 - アプリケーション名 (Application Name) : **ISE** と入力します。
 - [Web アプリケーションまたは Web アプリ (WEB APPLICATION AND/OR WEB APP)] を選択します。
 - サインオン URL およびアプリ ID URL (SIGN-ON URL and APP ID URL) : 任意の有効な URL を追加します。この値は ISE では使用されません。

4. Azure からマニフェスト ファイルを取得し、ISE 証明書情報を追加して、更新されたマニフェストを Azure にアップロードします。

1. Microsoft Azure 管理ポータル (<https://manage.windowsazure.com>) で、AAD スナップインを開き、ISE アプリケーションに移動します。

[マニフェストの管理 (Manage Manifest)] メニューからアプリケーション マニフェスト ファイルをダウンロードします。

5. *Base64 Encoded String of ISE PAN cert* を、PowerShell スクリプトの \$base64Value である、エクスポートされ編集された ISE からの証明書ファイルと置き換えて、次の例のようにマニフェスト json ファイルの [keyCredentials] フィールドを更新します。

```
"keyCredentials": [
    {
      "customKeyIdentifier": "$base64Thumbprint_from_above",
      "keyId": "$keyid_from_above",
      "type": "AsymmetricX509Cert",
      "usage": "Verify",
      "value": "Base64 Encoded String of ISE PAN cert"
    }
  ]
```



(注) マニフェスト ファイルの名前は変更しないようにします。

KeyCredentials の複雑なタイプは、<http://msdn.microsoft.com/en-us/library/azure/dn151681.aspx> でドキュメント化されています。

6. Azure に更新されたマニフェスト ファイルをアップロードします。
7. Microsoft Azure 管理ポータルで、アプリ エンドポイントのリストに移動します。次のエンドポイント属性の値を使用して ISE を設定します。
 - MICROSOFT AZURE AD GRAPH API ENDPOINT
 - OAUTH 2.0 TOKEN ENDPOINT

8. ISE で、ISE の Intune サーバを設定します。設定と外部 MDM サーバの詳細については、[ISE でのモバイル デバイス管理サーバの定義（285 ページ）](#)を参照してください。Intune にとって重要なフィールドは次のとおりです。

- **[自動検出 URL (Auto Discovery URL)]** : 前のステップの [Microsoft Azure AD Graph API エンドポイント (Microsoft Azure AD Graph API Endpoint)] の値を入力します。この URL は、アプリケーションが Graph API を使用して Microsoft Azure AD ディレクトリのデータに直接アクセスできるエンドポイントです。URL の形式は `https://<hostname>/<tenant id>`、たとえば、
`https://graph.ppe.windows.net/47f09275-5bc0-4807-8aae-f35cb0341329` です。この URL の拡大バージョンもプロパティ ファイルに含まれます。形式は、
`https://<Graph_API_Endpoint>/<TenantId_Or_Domain>/servicePrincipalsByAppId/<Microsoft Intune AppId>/serviceEndpoints?api-version=1.6&client-request-id=<Guid.NewGuid()>` です。
- **クライアント ID (Client ID)** : アプリケーションの固有識別子。アプリケーションが、Microsoft Azure AD Graph API、Microsoft Intune API などの他のアプリケーションのデータにアクセスする場合に、この属性を使用します。
- **トークン発行 URL (Token Issuing URL)** : 前のステップの [OAuth2.0 認証エンドポイント (OAuth2.0 Authorization Endpoint)] の値を入力します。これは、アプリケーションが OAuth2.0 を使用してアクセス トークンを取得できるエンドポイントです。アプリケーションが認証されると、Microsoft Azure AD はアプリケーション (ISE) にアクセス トークンを発行します。このトークンを使用するとアプリケーションから Graph API/Intune API を呼び出すことができます。
- **トークン対象者 (Token Audience)** : トークンが対象とする受信者リソース。パブリックの既知の Microsoft Intune API の APP ID URL。

Intune アプリケーションの詳細については、次のリンクを参照してください。

- <https://msdn.microsoft.com/en-us/library/azure/dn645543.aspx>
- <https://msdn.microsoft.com/en-us/library/azure/dn645543.aspx>
- <https://azure.microsoft.com/en-us/documentation/articles/active-directory-authentication-scenarios>
- <https://azure.microsoft.com/en-us/documentation/articles/active-directory-integrating-applications>
- <https://azure.microsoft.com/en-us/documentation/articles/active-directory-application-manifest>

Microsoft SCCM のポリシー設定の例

ポリシーでは次の新しいディクショナリ エントリが使用され、SCCM をサポートすることができます。

- **MDM.DaysSinceLastCheckin** : ユーザが最後に確認してからの日数、または SCCM のデバイスと同期してからの日数で、1 ~ 365 日です。

- MDM.UserNotified : 値は Y または N です。ユーザが登録されていないことをユーザに通知したかどうかを示します。さらに、登録ポータルへの制限付きアクセスやリダイレクトを許可し、またはアクセスを拒否できます。
- MDM.ServerType : 値はモバイルデバイス マネージャの場合 MDM またはデスクトップデバイス マネージャの場合 DM です。

次のサンプル ポリシー セットで SCCM をサポートする一連のポリシーを示します。

条件 (IF) リ ン ク 名	実行される ア ク シ ョ ン
Wireless_802.1X AND MDM:MDMServerName EQUALS ScmServer1 AND MDM:DeviceRegisterStatus EQUALS Registered	
Wireless_802.1X AND MDM:MDMServerName EQUALS ScmServer1 AND MDM:DeviceCompliantStatus EQUALS NonCompliant AND MDM:UserNotified EQUALS 28	
Wireless_802.1X AND MDM:MDMServerName EQUALS ScmServer1 AND MDM:MDMDeviceCompliantStatus EQUALS Registered AND MDM:DaysSinceLastCheckin EQUALS 28	
Wireless_802.1X AND MDM:MDMServerName EQUALS ScmServer1 AND MDM:DeviceCompliantStatus EQUALS NonCompliant AND MDM:DeviceRegisterStatus EQUALS Registered	
Wireless_802.1X AND MDM:DeviceRegisterStatus EQUALS Registered AND MDM:UserNotified EQUALS Yes	

ISE 用の Microsoft SCCM サーバの設定

ISE は、WMI を使用して SCCM サーバと通信します。WMI は、SCCM を実行している Windows サーバで設定する必要があります。



(注) ISE 統合に使用するユーザ アカウントは、次のいずれかの条件を満たしている必要があります。

- SMS 管理ユーザ グループのメンバーである。
- WMI 名前空間で SMS オブジェクトと同じアクセス許可がある。

```
root\sms\site_<sitecode>
```

サイトコードは SCCM サイトです。

AD ユーザがドメイン管理グループに属しているときの権限の設定

Windows 2008 R2、Windows 2012 および Windows 2012 R2 の場合、ドメイン管理グループは、デフォルトで Windows オペレーティング システムの特定のレジストリ キーを完全に制御することができません。Active Directory の管理者は、Active Directory ユーザに次のレジストリ キーに対する完全制御権限を提供する必要があります。

- HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}
- HKLM\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}

次の Active Directory のバージョンでは、レジストリ変更は必要ありません。

- Windows 2003
- Windows 2003R2
- Windows 2008

完全な制御を許可するには、次に示すように、まず Active Directory 管理者がキーの所有権を取得する必要があります。

ステップ 1 キーを右クリックして [オーナー (Owner)] タブに移動します。

ステップ 2 [アクセス許可 (Permissions)] をクリックします。

ステップ 3 [詳細設定 (Advanced)] をクリックします。

AD ユーザがドメイン管理グループの一部ではない場合に必要な権限

Windows 2012 R2 の場合は、Active Directory ユーザに次のレジストリ キーに対する完全制御権限を提供します。

- HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}
- HKLM\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}

Active Directory ユーザがドメイン管理グループの一部ではなく、ドメイン ユーザ グループの一部である場合は、次の権限も必要です。

- ISEがドメインコントローラに接続できるようにするレジストリ キーを追加します（下記を参照）
- [ドメイン コントローラで DCOM を使用するための権限（295 ページ）](#)
- [WMI ルート/CIMv2 名前空間にアクセスするための権限の設定（296 ページ）](#)

これらの権限は、次の Active Directory のバージョンでのみ必要となります。

- Windows 2003
- Windows 2003R2
- Windows 2008
- Windows 2008 R2
- Windows 2012
- Windows 2012 R2
- Windows 2016

ISE がドメイン コントローラに接続できるようにするレジストリ キーを追加する

ISEがドメインユーザとして接続し、ログイン認証イベントを取得できるようにするには、ドメイン コントローラに一部のレジストリ キーを手動で追加する必要があります。エージェントはドメイン コントローラまたはドメイン内のマシンでは必要ありません。

次のレジストリのスクリプトは追加するキーを示しています。これをコピーしてテキストファイルに貼り付け、.reg の拡張子でファイルを保存し、ファイルをダブルクリックすることでレジストリの変更を行うことができます。レジストリ キーを追加するには、ルート キーのオーナーである必要があります。

Windows Registry Editor Version 5.00

```
[HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"AppID"="{76A64158-CB41-11D1-8B02-00600806D9B6}"
```

```
[HKEY_CLASSES_ROOT\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"DllSurrogate"=" " "
```

```
[HKEY_CLASSES_ROOT\Wow6432Node\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"DllSurrogate"=" " "
```

キー **DllSurrogate** の値には、2 つのスペースが含まれていることを確認します。

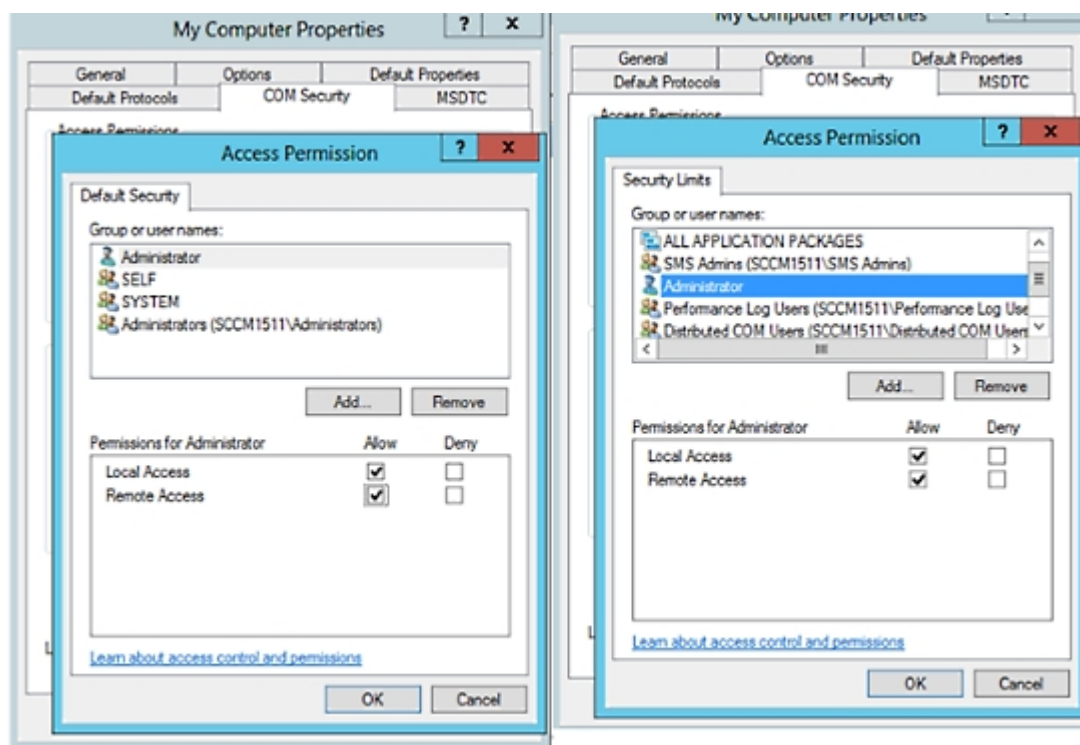
上記のスクリプトに示すように、ファイルの末尾の空の行を含む、空の行を保持してください。

ドメインコントローラで DCOM を使用するための権限

ISE パッシブ ID サービスに使用される Active Directory ユーザは、ドメインコントローラで DCOM（リモート COM）を使用する権限がなければなりません。 **dcomcnfg** コマンドラインツールを使用して権限を設定できます。

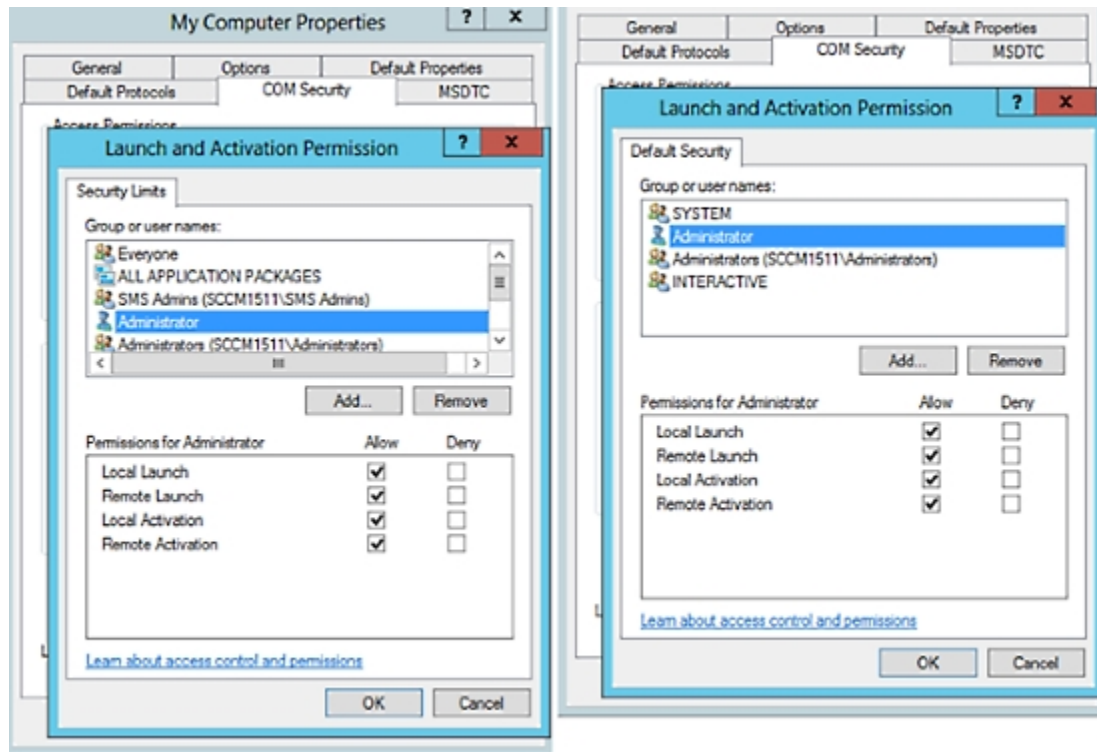
- ステップ 1 コマンドラインから **dcomcnfg** ツールを実行します。
- ステップ 2 [コンポーネントサービス（Component Services）] を展開します。
- ステップ 3 [コンピュータ（Computers）] > [マイコンピュータ（My Computer）] を展開します。
- ステップ 4 メニューバーで [アクション（Action）] を選択して、[プロパティ（properties）] をクリックし、[COMセキュリティ（COM Security）] をクリックします。
- ステップ 5 アクセスおよび起動の両方に対して ISE が使用するアカウントに許可権限があることを確認します。 Active Directory ユーザは、4 つのオプション（[アクセス権限（Access Permissions）] および [起動およびアクティベーションの権限（Launch and Activation Permissions）] の両方に対する [制限の編集（Edit Limits）] と [デフォルトの編集（Edit Default）]）のすべてに追加される必要があります。
- ステップ 6 [アクセス権限（Access Permissions）] および [起動およびアクティベーションの権限（Launch and Activation Permissions）] の両方に対してローカルおよびリモートアクセスをすべて許可します。

図 13: [アクセス権限（Access Permissions）] のローカルおよびリモートアクセス



WMI ルート/CIMv2 名前空間にアクセスするための権限の設定

図 14: [起動およびアクティベーションの権限 (Launch and Activation Permissions)] のローカルおよびリモート アクセス

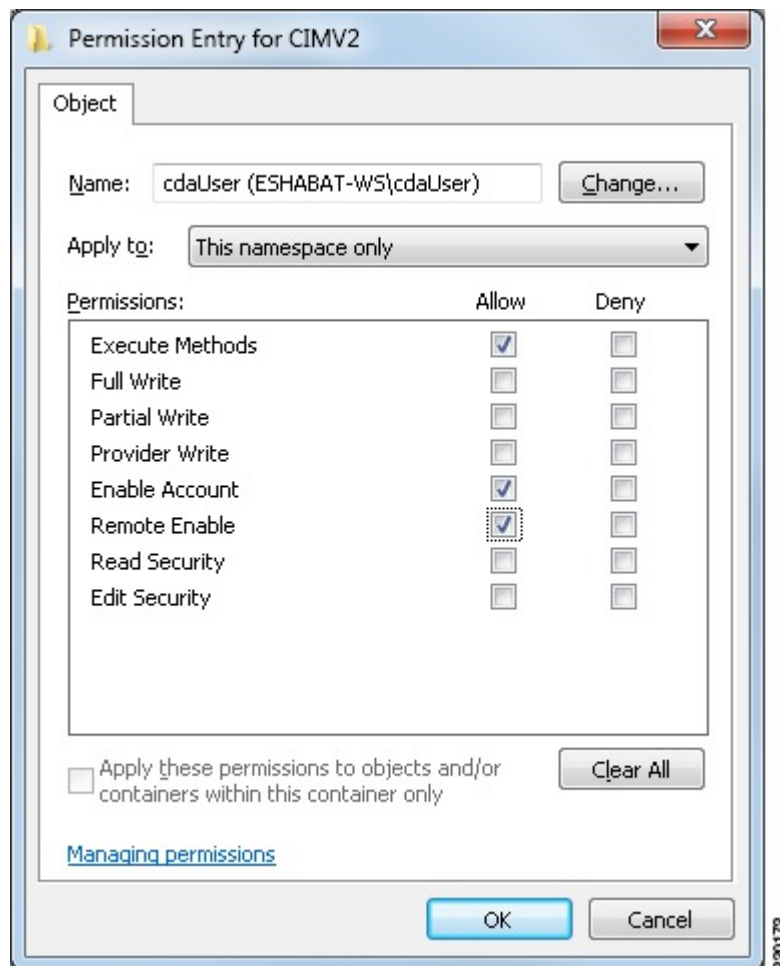


WMI ルート/CIMv2 名前空間にアクセスするための権限の設定

デフォルトでは、Active Directory ユーザには実行メソッドおよびリモートイネーブルのための権限がありません。wmimgmt.msc MMC コンソールを使用してアクセス権を付与できます。

- ステップ 1 [スタート]>[Run] をクリックし、wmimgmt.msc と入力します。
- ステップ 2 [WMI Control] を右クリックし、[プロパティ] をクリックします。
- ステップ 3 [セキュリティ] タブで [ルート] を展開し、[CIMV2] を選択します。
- ステップ 4 [セキュリティ (Security)] をクリックします。
- ステップ 5 下に示すように、Active Directory ユーザを追加し、必要な権限を設定します。

図 15: WMI Root\CIMv2 名前空間に必要な権限



320173

AD ユーザがドメイン管理グループに属しているときの権限の設定

Windows 2008 R2、Windows 2012 および Windows 2012 R2 の場合、ドメイン管理グループは、デフォルトで Windows オペレーティング システムの特定のレジストリ キーを完全に制御することができません。Active Directory の管理者は、Active Directory ユーザに次のレジストリ キーに対する完全制御権限を提供する必要があります。

- HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}
- HKLM\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}

次の Active Directory のバージョンでは、レジストリ変更は必要ありません。

- Windows 2003
- Windows 2003R2

- Windows 2008

完全な制御を許可するには、次に示すように、まず Active Directory 管理者がキーの所有権を取得する必要があります。

ステップ 1 キーを右クリックして [オーナー (Owner)] タブに移動します。

ステップ 2 [アクセス許可 (Permissions)] をクリックします。

ステップ 3 [詳細設定 (Advanced)] をクリックします。

AD ユーザがドメイン管理グループの一部ではない場合に必要な権限

Windows 2012 R2 の場合は、Active Directory ユーザに次のレジストリ キーに対する完全制御権限を提供します。

- HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}
- HKLM\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}

Active Directory ユーザがドメイン管理グループの一部ではなく、ドメイン ユーザ グループの一部である場合は、次の権限も必要です。

- ISE がドメインコントローラに接続できるようにするレジストリ キーを追加します (下記を参照)
- [ドメイン コントローラで DCOM を使用するための権限 \(295 ページ\)](#)
- [WMI ルート/CIMv2 名前空間にアクセスするための権限の設定 \(296 ページ\)](#)

これらの権限は、次の Active Directory のバージョンでのみ必要となります。

- Windows 2003
- Windows 2003R2
- Windows 2008
- Windows 2008 R2
- Windows 2012
- Windows 2012 R2
- Windows 2016

ISE がドメイン コントローラに接続できるようにするレジストリ キーを追加する

ISE がドメイン ユーザとして接続し、ログイン認証イベントを取得できるようにするには、ドメイン コントローラに一部のレジストリ キーを手動で追加する必要があります。エージェントはドメイン コントローラまたはドメイン内のマシンでは必要ありません。

次のレジストリのスクリプトは追加するキーを示しています。これをコピーしてテキストファイルに貼り付け、.reg の拡張子でファイルを保存し、ファイルをダブルクリックすることでレジストリの変更を行うことができます。レジストリ キーを追加するには、ルート キーのオーナーである必要があります。

Windows Registry Editor Version 5.00

```
[HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"AppID"="{76A64158-CB41-11D1-8B02-00600806D9B6}"
```

```
[HKEY_CLASSES_ROOT\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"DllSurrogate"=" " "
```

```
[HKEY_CLASSES_ROOT\Wow6432Node\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"DllSurrogate"=" " "
```

キー **DllSurrogate** の値には、2 つのスペースが含まれていることを確認します。

上記のスクリプトに示すように、ファイルの末尾の空の行を含む、空の行を保持してください。

ドメインコントローラで DCOM を使用するための権限

ISE パッシブ ID サービスに使用される Active Directory ユーザは、ドメインコントローラで DCOM（リモート COM）を使用する権限がなければなりません。 **dcomcnfg** コマンドライン ツールを使用して権限を設定できます。

-
- ステップ 1 コマンドラインから **dcomcnfg** ツールを実行します。
 - ステップ 2 [コンポーネントサービス (Component Services)] を展開します。
 - ステップ 3 [コンピュータ (Computers)] > [マイコンピュータ (My Computer)] を展開します。
 - ステップ 4 メニューバーで [アクション (Action)] を選択して、[プロパティ (properties)] をクリックし、[COM セキュリティ (COM Security)] をクリックします。
 - ステップ 5 アクセスおよび起動の両方に対して ISE が使用するアカウントに許可権限があることを確認します。Active Directory ユーザは、4 つのオプション ([アクセス権限 (Access Permissions)] および [起動およびアクティベーションの権限 (Launch and Activation Permissions)] の両方に対する [制限の編集 (Edit Limits)] と [デフォルトの編集 (Edit Default)]) のすべてに追加される必要があります。
 - ステップ 6 [アクセス権限 (Access Permissions)] および [起動およびアクティベーションの権限 (Launch and Activation Permissions)] の両方に対してローカルおよびリモート アクセスをすべて許可します。

ドメインコントローラで **DCOM** を使用するための権限

図 16: [アクセス権限 (Access Permissions)] のローカルおよびリモート アクセス

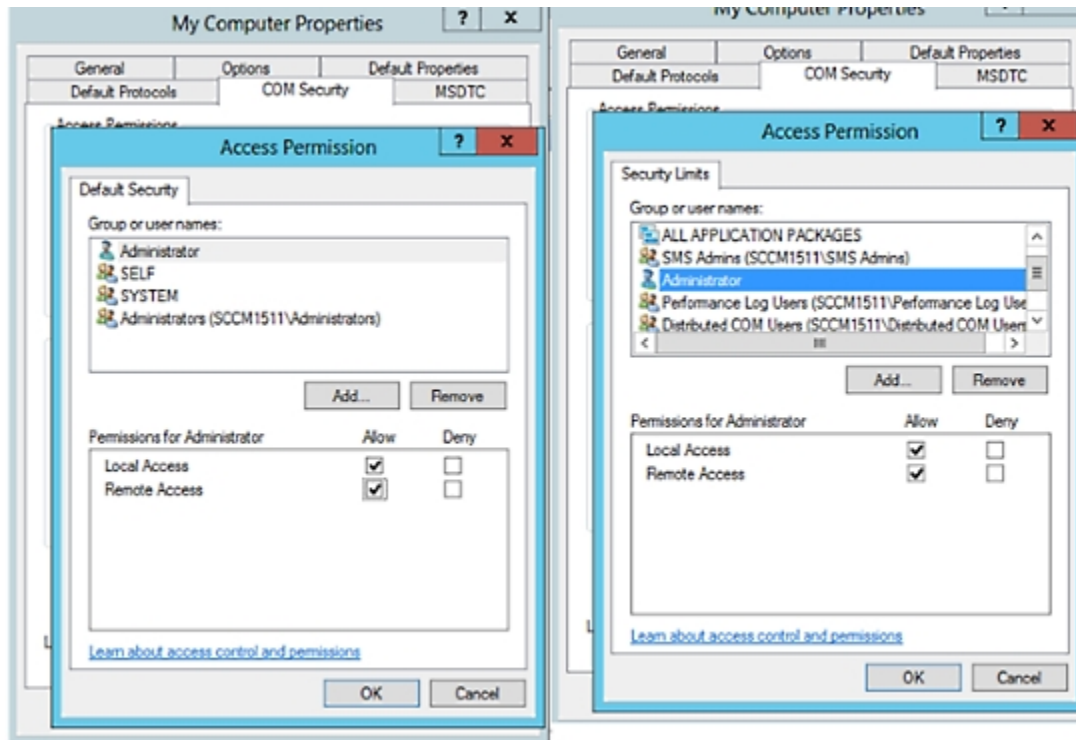
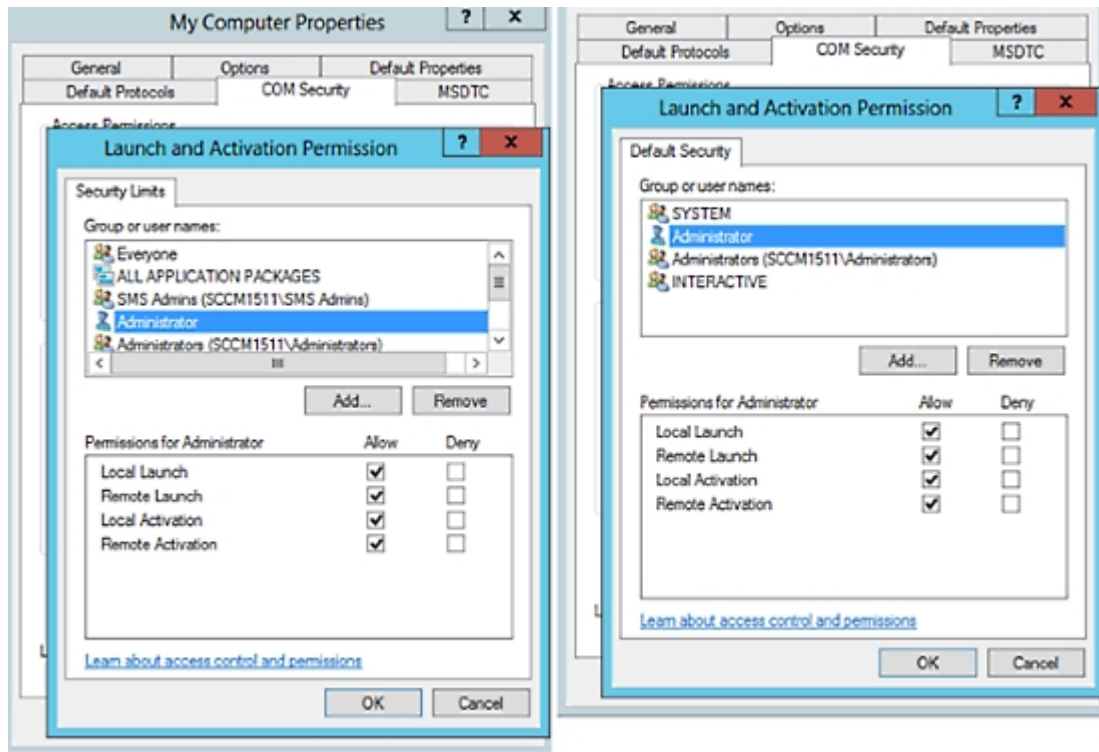


図 17: [起動およびアクティベーションの権限 (Launch and Activation Permissions)] のローカルおよびリモート アクセス

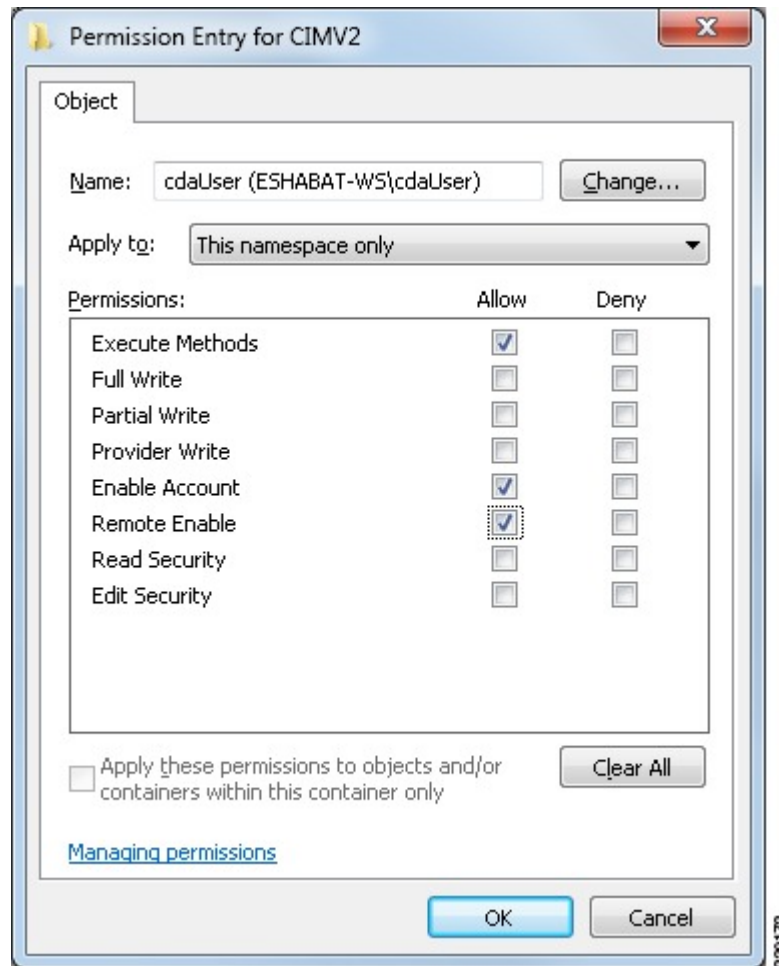


WMI ルート/CIMv2 名前空間にアクセスするための権限の設定

デフォルトでは、Active Directory ユーザには実行メソッドおよびリモートイネーブルのための権限がありません。wmimgmt.msc MMC コンソールを使用してアクセス権を付与できます。

- ステップ 1 [スタート]>[Run] をクリックし、wmimgmt.msc と入力します。
- ステップ 2 [WMI Control] を右クリックし、[プロパティ] をクリックします。
- ステップ 3 [セキュリティ] タブで [ルート] を展開し、[CIMV2] を選択します。
- ステップ 4 [セキュリティ (Security)] をクリックします。
- ステップ 5 下に示すように、Active Directory ユーザを追加し、必要な権限を設定します。

図 18 : WMI Root\CIMv2 名前空間に必要な権限



WMI アクセス用にファイアウォール ポートを開く

Active Directory ドメイン コントローラのファイアウォール ソフトウェアは、WMI へのアクセスをブロックすることがあります。ファイアウォールをオフにするか、または次のポートへの特定の IP (ISE IP アドレス) のアクセスを許可することができます。

- TCP 135 : 一般的な RPC ポート。非同期 RPC 発信をすると、このポートでリスニングしているサービスが、クライアントに、この要求を処理できるコンポーネントが使用しているポートを通知します。
- UDP 138 : NetBIOS データグラム サービス
- TCP 139 : NetBIOS セッション サービス
- TCP 445 : SMB

数値の大きいポートは動的に割り当てられ、手動で設定できます。ターゲットとして %SystemRoot%\System32\dlhhost.exe を追加することを推奨します。このプログラムは、ポートを動的に管理します。

すべてのファイアウォールルールを、特定の IP アドレス（ISE IP）に割り当てることができます。

未登録のデバイスのリダイレクトのための許可プロファイルの設定

各外部 MDM サーバの未登録のデバイスをリダイレクトするには、Cisco ISE で許可プロファイルを設定する必要があります。

始める前に

- Cisco ISE で MDM サーバ定義を作成したことを確認します。正常に MDM サーバと ISE を統合した後に限り、MDM ディクショナリにデータが入力され、MDM ディクショナリ属性を使用して許可ポリシーを作成できます。
- 未登録のデバイスをリダイレクトするために、ワイヤレス LAN コントローラの ACL を設定します。
- インターネット接続にプロキシを使用していて、MDM サーバが内部ネットワークの一部である場合は、プロキシバイパスリストに MDM サーバ名または IP アドレスを追加する必要があります。[管理 (Administration)] > [設定 (Settings)] > [プロキシ設定 (Proxy Settings)] の順に選択して、このアクションを実行します。

-
- ステップ 1** [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] > [許可 (Authorization)] > [許可プロファイル (Authorization Profiles)] > [追加 (Add)] を選択します。
- ステップ 2** 準拠していないまたは登録されていない未登録デバイスをリダイレクトするための許可プロファイルを作成します。
- ステップ 3** MDM サーバ名と一致する許可プロファイルの名前を入力します。
- ステップ 4** アクセスタイプとして ACCESS_ACCEPT を選択します。
- ステップ 5** [Web リダイレクション (Web Redirection)] チェックボックスをオンにし、ドロップダウンリストから [MDM リダイレクト (MDM Redirect)] を選択します。
- ステップ 6** ワイヤレス LAN コントローラ上で設定した ACL の名前を [ACL] フィールドに入力します。
- ステップ 7** [値 (Value)] ドロップダウンリストから MDM ポータルを選択します。
- ステップ 8** ドロップダウンリストから、使用する MDM サーバを選択します。
- ステップ 9** [送信 (Submit)] をクリックします。
-

次のタスク

MDM 使用例の許可ポリシー ルールの設定。

MDM 使用例の許可ポリシー ルールの設定

MDM 設定を完了するには、Cisco ISE で許可ポリシー ルールを設定する必要があります。

始める前に

- Cisco ISE 証明書ストアに MDM サーバ証明書を追加します。
- Cisco ISE で MDM サーバ定義を作成したことを確認します。正常に MDM サーバと ISE を統合した後に限り、MDM ディクショナリにデータが入力され、MDM ディクショナリ属性を使用して許可ポリシーを作成できます。
- 未登録のデバイスまたは非準拠のデバイスをリダイレクトするために、ワイヤレス LAN コントローラの ACL を設定します。

ステップ 1 [ポリシー (Policy)] > [許可 (Authorization)] > [新規ルールを下に挿入 (Insert New Rule Below)] を選択します。

ステップ 2 [ポリシー (Policy)] > [ポリシー セット (Policy Sets)] を選択し、許可ポリシー ルールを表示するポリシー セットを展開します。

ステップ 3 次のルールを追加します。

- [MDM_Un_Registered_Non_Compliant] : MDM サーバに登録されていないか、MDM ポリシーに準拠していないデバイスの場合。要求がこのルールに一致すると、ISE MDM ページが表示され、MDM でのデバイスの登録に関する情報が示されます。
- [PERMIT] : デバイスが Cisco ISE および MDM に登録されており、Cisco ISE および MDM ポリシーに準拠している場合、Cisco ISE で設定されたアクセス コントロール ポリシーに基づいてネットワークへのアクセス権が付与されます。

次の図は、この設定の例を示します。

図 19: MDM の使用例の許可ポリシー ルール



ステップ 4 [保存 (Save)] をクリックします。

デバイスのワイプまたはロック

Cisco ISE では、失われたデバイスをワイプしたり、PIN ロックをオンにしたりできます。これは [エンドポイント (Endpoints)] ページから行うことができます。

ステップ 1 [ワーク センター (Work Centers)] > [ネットワーク アクセス (Network Access)] > [ID (Identities)] > [エンドポイント (Endpoints)] を選択します。

ステップ 2 ワイプまたはロックするデバイスの横にあるチェックボックスをオンにします。

ステップ 3 [MDM アクセス (MDM Access)] ドロップダウン リストから、次のオプションのいずれかを選択します。

- [完全ワイプ (Full Wipe)] : このオプションを使用すると、MDM ベンダーに応じて、企業アプリケーションが削除されるか、またはデバイスが工場出荷時の設定にリセットされます。
- [企業ワイプ (Corporate Wipe)] : MDM サーバ ポリシーで設定したアプリケーションを削除します
- [PIN ロック (PIN Lock)] : デバイスをロックします

ステップ 4 [はい (Yes)] をクリックして、デバイスをワイプまたはロックします。

Mobile Device Manager のレポートの表示

Cisco ISE では、MDM サーバ定義のすべての追加、更新、および削除を記録します。これらのイベントは、選択された期間での任意のシステム管理者によるすべての設定変更を報告する「変更設定監査」レポートで表示できます。

[操作 (Operations)] > [レポート (Reports)] > [変更設定監査 (Change Configuration Audit)] > [MDM] を選択し、結果のレポートで表示する期間を指定します。

Mobile Device Manager のログの表示

[メッセージ カタログ (Message Catalog)] ページを使用して、Mobile Device Manager のログ メッセージを表示できます。[管理 (Administration)] > [システム (System)] > [ロギング (Logging)] > [メッセージ カタログ (Message Catalog)] を選択します。MDM ログ エントリのデフォルトのレポート レベルは「INFO」です。レポート レベルを「DEBUB」または「TRACE」に変更できます。



第 11 章

リソースの管理

- [ディクショナリおよびディクショナリ属性 \(307 ページ\)](#)
- [RADIUS ベンダー ディクショナリ \(310 ページ\)](#)

ディクショナリおよびディクショナリ属性

ディクショナリは、ドメインのアクセスポリシーの定義に使用できる属性と許容値のドメイン固有カタログです。個々のディクショナリは、属性タイプの同種の集合です。ディクショナリで定義された属性は同じ属性タイプを持ち、タイプは特定の属性のソースまたはコンテキストを示します。

属性タイプは次のいずれかになります。

- MSG_ATTR
- ENTITY_ATTR
- PIP_ATTR

属性と許容値に加えて、ディクショナリには名前と説明、データ型、デフォルト値などの属性に関する情報が含まれます。属性は、次のいずれかのデータ型となります。BOOLEAN、FLOAT、INTEGER、IPv4、IPv6、OCTET_STRING、STRING、UNIT32、および UNIT64。

Cisco ISE ではインストール中にシステム ディクショナリが作成され、ユーザ ディクショナリを作成できます。

システム定義のディクショナリとディクショナリ属性

Cisco ISE は、インストール中にシステム ディクショナリを作成します。これは、[システム ディクショナリ (System Dictionaries)] ページで確認できます。システム定義のディクショナリ属性は、読み取り専用の属性です。その特性のため、既存のシステム定義のディクショナリは表示することのみができます。システム定義の値またはシステムディクショナリ内の属性を作成、編集、削除することはできません。

システム定義のディクショナリ属性は、属性の記述名、ドメインによって認識される内部名、および許容値とともに表示されます。

また、Cisco ISE は Internet Engineering Task Force (IETF) で定義され、システム定義のディクショナリにも含まれる IETF RADIUS 属性セット用にディクショナリ デフォルトを作成します。ID を除くすべてのフリー IETF RADIUS 属性フィールドを編集できます。

関連トピック

[システム ディクショナリおよびディクショナリ属性の表示](#) (308 ページ)

[ユーザ定義のディクショナリとディクショナリ属性](#) (308 ページ)

システム ディクショナリおよびディクショナリ属性の表示

システムディクショナリ内のシステム定義の属性を作成、変更、削除することはできません。システム定義された属性は表示することのみができます。ディクショナリの名前と説明に基づくクイック検索またはユーザ定義の検索ルールに基づく高度な検索を実行できます。

-
- ステップ 1** [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [ディクショナリ (Dictionaries)] > [システム (System)] を選択します。
- ステップ 2** [システム ディクショナリ (System Dictionaries)] ページからシステム ディクショナリを選択して [表示 (View)] をクリックします。
- ステップ 3** [ディクショナリ属性 (Dictionary Attributes)] をクリックします。
- ステップ 4** リストからシステム ディクショナリを選択して [表示 (View)] をクリックします。
- ステップ 5** [システム ディクショナリ (System Dictionaries)] ページに戻るには、[ディクショナリ (Dictionaries)] リンクをクリックします。
-

ユーザ定義のディクショナリとディクショナリ属性

Cisco ISE では、[ユーザ ディクショナリ (User Dictionary)] ページで作成したユーザ定義ディクショナリが表示されます。システムで作成され、保存された既存のユーザディクショナリの [ディクショナリ名 (Dictionary Name)] または [ディクショナリ タイプ (Dictionary Type)] の値は変更できません。

[ユーザ ディクショナリ (User Dictionaries)] ページでは、次の操作を実行できます。

- ユーザディクショナリを編集および削除します。
- 名前および説明に基づいてユーザディクショナリを検索します。
- ユーザディクショナリのユーザ定義のディクショナリ属性を追加、編集、および削除します。
- NMAP スキャン機能を使って、NMAP 拡張ディクショナリの属性を削除します。カスタムポートが [NMAP スキャンアクション (NMAP Scan Actions)] ページで追加または削除されると、対応するカスタムポート属性がディクショナリで追加、削除または更新されます。
- ディクショナリ属性の許容値を追加または削除します。

関連トピック

[ユーザ定義のディクショナリの作成](#) (309 ページ)

[ユーザ定義のディクショナリ属性の作成](#) (309 ページ)

ユーザ定義のディクショナリの作成

ユーザ定義のディクショナリを作成、編集、または削除できます。

-
- ステップ 1** [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [ディクショナリ (Dictionaries)] > [ユーザ (User)] を選択します。
- ステップ 2** [追加 (Add)] をクリックします。
- ステップ 3** ユーザ ディクショナリの名前、オプションの説明、およびバージョンを入力します。
- ステップ 4** [ディクショナリ属性タイプ (Dictionary Attribute Type)] ドロップダウン リストから属性タイプを選択します。
- ステップ 5** [送信 (Submit)] をクリックします。
-

関連トピック

[ユーザ定義のディクショナリ属性の作成](#) (309 ページ)

ユーザ定義のディクショナリ属性の作成

ユーザディクショナリの、ユーザ定義のディクショナリ属性を追加、編集および削除したり、ディクショナリ属性に使用できる値を追加または削除したりすることができます。

-
- ステップ 1** [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [ディクショナリ (Dictionaries)] > [ユーザ (User)] を選択します。
- ステップ 2** [ユーザ ディクショナリ (User Dictionaries)] ページからユーザ ディクショナリを選択して [編集 (Edit)] をクリックします。
- ステップ 3** [ディクショナリ属性 (Dictionary Attributes)] をクリックします。
- ステップ 4** [追加 (Add)] をクリックします。
- ステップ 5** ディクショナリ属性の属性名、オプションの説明、および内部名を入力します。
- ステップ 6** [データ型 (Data Type)] ドロップダウン リストからデータ型を選択します。
- ステップ 7** [追加 (Add)] をクリックして、[使用できる値 (Allowed Values)] テーブルで名前、使用できる値、およびデフォルト ステータスを設定します。
- ステップ 8** [送信 (Submit)] をクリックします。
-

RADIUS ベンダー ディクショナリ

Cisco ISE では、一連の RADIUS ベンダー ディクショナリを定義したり、それぞれの一連の属性を定義したりできます。リスト内の各ベンダー定義には、ベンダー名、ベンダー ID、および簡単な説明が含まれています。

Cisco ISE では、次の RADIUS ベンダー ディクショナリがデフォルトで提供されます。

- Airespace
- Cisco
- Cisco-BBSM
- Cisco-VPN3000
- Microsoft

RADIUS プロトコルは、これらのベンダーディクショナリと、許可プロファイルとポリシー条件で使用するベンダー固有属性をサポートします。

関連トピック

[RADIUS ベンダー ディクショナリの作成](#) (310 ページ)

[RADIUS ベンダー ディクショナリ属性の作成](#) (311 ページ)

RADIUS ベンダー ディクショナリの作成

RADIUS ベンダーディクショナリを作成、編集、削除、エクスポート、およびインポートすることもできます。

ステップ 1 [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [ディクショナリ (Dictionaries)] > [システム (System)] > [RADIUS (Radius)] > [RADIUS ベンダー (Radius Vendors)] を選択します。

ステップ 2 [追加 (Add)] をクリックします。

ステップ 3 RADIUS ベンダーの Internet Assigned Numbers Authority (IANA) で承認されている RADIUS ベンダー ディクショナリの名前、オプションの説明、およびベンダー ID を入力します。

ステップ 4 属性値から取得したバイト数を選択して、[ベンダー属性タイプフィールド長 (Vendor Attribute Type Field Length)] ドロップダウンリストから属性タイプを指定します。有効な値は、1、2、および4です。デフォルト値は1です。

ステップ 5 属性値から取得したバイト数を選択して、[ベンダー属性サイズフィールド長 (Vendor Attribute Size Field Length)] ドロップダウン リストから属性長を指定します。有効な値は0と1です。デフォルト値は1です。

ステップ 6 [送信 (Submit)] をクリックします。

関連トピック

[RADIUS ベンダー ディクショナリ属性の作成](#) (311 ページ)

RADIUS ベンダー ディクショナリ属性の作成

Cisco ISE がサポートする RADIUS ベンダー属性を作成、編集、および削除できます。各 RADIUS ベンダー属性には、名前、データ型、説明、および方向（要求のみに関連する、応答のみに関連する、または両方に関連するかどうかを指定）が含まれています。

-
- ステップ 1 [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [ディクショナリ (Dictionaries)] > [システム (System)] > [RADIUS (Radius)] > [RADIUS ベンダー (Radius Vendors)] を選択します。
 - ステップ 2 RADIUS ベンダーディクショナリ リストから RADIUS ベンダーディクショナリを選択して [編集 (Edit)] をクリックします。
 - ステップ 3 [ディクショナリ属性 (Dictionary Attributes)] をクリックし、[追加 (Add)] をクリックします。
 - ステップ 4 RADIUS ベンダー属性の属性名とオプションの説明を入力します。
 - ステップ 5 [データ型 (Data Type)] ドロップダウン リストからデータ型を選択します。
 - ステップ 6 [MAC オプションの有効化 (Enable MAC option)] チェックボックスを選択します。
 - ステップ 7 RADIUS 要求のみ、RADIUS 応答のみ、またはその両方に適用される方向を [方向 (Direction)] ドロップダウン リストから選択します。
 - ステップ 8 [ID] フィールドにベンダー属性 ID を入力します。
 - ステップ 9 [タグ付けの許可 (Allow Tagging)] チェックボックスをオンにします。
 - ステップ 10 [プロファイルのこの属性の複数インスタンスを許可する (Allow multiple instances of this attribute in a profile)] チェックボックスをオンにします。
 - ステップ 11 [追加 (Add)] をクリックして、[使用できる値 (Allowed Values)] テーブルにベンダー属性の使用できる値を追加します。
 - ステップ 12 [送信 (Submit)] をクリックします。
-

HP RADIUS IETF サービス タイプ属性

Cisco ISE では、RADIUS IETF サービス タイプ属性に 2 つの新しい値が導入されました。RADIUS IETF サービス タイプ属性は、[ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [ディクショナリ (Dictionaries)] > [システム (System)] > [RADIUS] > [IETF] で使用できます。ポリシーの条件で次の 2 つの値を使用できます。これら 2 つの値は、特に HP のデバイスがユーザの権限を理解できるように設計されています。

列挙名	列挙値
HP-Oper	252
HP-User	255



第 12 章

ロギング メカニズム

- [Cisco ISE ロギング メカニズム \(313 ページ\)](#)
- [Cisco ISE システム ログ \(314 ページ\)](#)
- [リモート syslog 収集場所の設定 \(319 ページ\)](#)
- [Cisco ISE メッセージコード \(320 ページ\)](#)
- [Cisco ISE メッセージカタログ \(321 ページ\)](#)
- [デバッグ ログ \(321 ページ\)](#)
- [エンドポイントのデバッグ ログ コレクタ \(322 ページ\)](#)
- [収集フィルタ \(323 ページ\)](#)

Cisco ISE ロギング メカニズム

Cisco ISE には、監査、障害管理、およびトラブルシューティングに使用されるロギング メカニズムが備わっています。このロギング メカニズムは、展開されたサービスの障害状態を識別したり、問題のトラブルシューティングを効率的に行う場合に役立ちます。また、プライマリ ノードのモニタリングおよびトラブルシューティングのロギング出力が一貫した形式で生成されます。

仮想ループバック アドレスを使用してローカル システムにログを収集するように Cisco ISE ノードを設定できます。ログを外部に収集するには、ターゲットと呼ばれる外部 syslog サーバを設定します。ログは事前定義された各種のカテゴリに分類されます。ターゲット、重大度レベルなどに応じてカテゴリを編集することにより、ロギング出力をカスタマイズできます。



(注) モニタリング ノードがネットワーク デバイスの syslog サーバとして設定されている場合、ロギング ソースが次の形式で正しいネットワーク アクセス サーバ (NAS) の IP アドレスを送信することを確認してください。

`<message_number>sequence_number: NAS_IP_address: timestamp: syslog_type: <message_text>`

そうしないと、これは NAS の IP アドレスに依存する機能に影響を及ぼすことがあります。

ローカル ログの消去の設定

このプロセスを使用して、ローカル ログ格納期間を設定し、特定の期間後にローカル ログを削除します。

-
- ステップ 1** [管理 (Administration)] > [システム (System)] > [ロギング (Logging)] > [ローカル ログ設定 (Local Log Settings)] を選択します。
- ステップ 2** [ローカル ログ格納期間 (Local Log Storage Period)] フィールドに、設定ソースでログ エントリを保持する最大日数を入力します。
- ステップ 3** 格納期間が経過する前に既存のログ ファイルを削除するには、[今すぐログを削除 (Delete Logs Now)] をクリックします。
- ステップ 4** [保存 (Save)] をクリックします。
-

Cisco ISE システム ログ

Cisco ISE では、システム ログはロギング ターゲットと呼ばれる場所で収集されます。ターゲットは、ログを収集して格納するサーバの IP アドレスを参照します。ログをローカルで生成して格納することも、FTP ファシリティを使用して外部サーバに転送することもできます。Cisco ISE には、次のデフォルト ターゲットがあり、これらはローカル システムのループバック アドレスに動的に設定されます。

- LogCollector : ログ コレクタのデフォルトの syslog ターゲット。
- ProfilerRadiusProbe : プロファイラ Radius プローブのデフォルトの syslog ターゲット。

デフォルトでは、AAA 診断サブカテゴリとシステム診断サブカテゴリのロギング ターゲットは、ディスク領域を減らすために、新規 Cisco ISE インストールまたはアップグレード時に無効になります。これらのサブカテゴリのロギングターゲットを手動で設定できますが、これらのサブカテゴリのローカル ロギングは常に有効です。

Cisco ISE インストールの最後にローカルに設定されるデフォルトのロギング ターゲットを使用するか、またはログを保存する外部ターゲットを作成することができます。



- (注) syslog サーバが分散展開で設定されている場合、syslog メッセージは MnT ノードではなく認証 PSN から syslog サーバへ直接送信されます。

関連トピック

[Cisco ISE メッセージ コード \(320 ページ\)](#)

ローカルストア syslog メッセージの形式

ログメッセージは、次の syslog メッセージフォーマットでローカルストアに送信されます。

timestamp sequence_num msg_ode msg_sev msg_class msg_text attr =value

フィールド	説明
<i>timestamp</i>	<p>次の形式での、生成元の Cisco ISE ノードのローカルクロックに従ったメッセージ生成の日付。</p> <p><i>YYYY-MM-DD hh:mm:ss:xxx +/-zh:zm</i></p> <p>値は次のとおりです。</p> <ul style="list-style-type: none"> • YYYY = 年を表す数字。 • MM = 月を表す数字。1桁の月（1～9）の場合は、数字の前に 0 が付きます。 • DD = 日を表す数字。1桁の日（1～9）の場合、数字の前に 0 が付きます。 • hh = 時間：00～23。 • mm = 分：00～59。 • ss = 秒：00～59。 • xxx = ミリ秒：000～999。 • +/-zh:zm = Cisco ISE サーバのタイムゾーンからのタイムゾーンオフセット。zh はオフセットの時間数、zm はオフセットの分数です。すべて先頭に、オフセットの方向を示すマイナスまたはプラス記号が付きます。たとえば、+02:00 は、タイムスタンプによって示された時刻に、Cisco ISE サーバのタイムゾーンよりも 2 時間先行する Cisco ISE ノードでメッセージが発生したことを示します。
<i>sequence_num</i>	<p>各メッセージのグローバルカウンタ。1つのメッセージがローカルストアに送信され、次に syslog サーバターゲットに送信された場合は、カウンタが 2 つ増加します。有効な値は 0000000001～999999999 です。</p>
<i>msg_ode</i>	<p>ロギングカテゴリで定義されているメッセージコード。</p>

フィールド	説明
<i>msg_sev</i>	ログ メッセージのメッセージ重大度レベル。 [管理 (Administration)] > [システム (System)] > [ロギング (Logging)] > [ロギング カテゴリ (Logging Categories)] を参照してください。
<i>msg_class</i>	同じコンテキストを持つメッセージのグループを識別するメッセージ クラス。
<i>msg_text</i>	英語の説明テキスト メッセージ。
<i>attr=value</i>	<p>ロギングされたイベントの詳細を示す属性と値のペアのセット。カンマ (,) で各ペアを区切ります。</p> <p>属性名は Cisco ISE デictionary で定義されています。</p> <p>応答方向属性セットの値は、Response という 1 つの属性にバンドルされ、中カッコ {} で囲まれます。また、Response 内の属性と値のペアはセミコロンで区切られます。</p> <p>例：Response={RadiusPacketType=AccessAccept; AuthenticationResult=UnknownUser; cisco-av-pair=sga:security-group-tag=0000-00;}</p>

リモート syslog メッセージの形式

Web インターフェイスを使用して、ロギング カテゴリ メッセージがリモート syslog サーバターゲットに送信されるように設定できます。ログ メッセージは、syslog プロトコル標準 (RFC-3164 を参照) に従ってリモート syslog サーバターゲットに送信されます。syslog プロトコルはセキュアでない UDP です。

メッセージは、イベントが発生したときに生成されます。イベントは、プログラムの終了時に表示されるメッセージやアラームなどのステータスを表示するものである場合があります。カーネル、メール、ユーザレベルなど、異なるファシリティから生成されたさまざまなタイプのイベント メッセージがあります。イベント メッセージは重大度レベルに関連付けられており、管理者はメッセージをフィルタリングし、優先度付けできます。数値コードはファシリティおよび重大度レベルに割り当てられます。Syslog サーバはイベント メッセージ コレクタで、これらのファシリティからイベントメッセージを収集します。管理者は、重大度レベルに基づいて、メッセージを転送するイベントメッセージ コレクタを選択できます。Cisco ISE の重大度レベルについては、「[ロギング カテゴリの設定](#)」の項を参照してください。

ログ メッセージは、ローカルストア syslog メッセージフォーマットに先行する次の syslog メッセージヘッダー フォーマットでリモート syslog サーバに送信されます。

pri_num YYYY Mmm DD hh:mm:ss xx:xx:xx:xx/host_name cat_name msg_id total_seg seg_num

フィールド	説明
<i>pri_num</i>	<p>メッセージのプライオリティ値。メッセージのファシリティ値と重大度値の組み合わせです。プライオリティ値 = (ファシリティ値 * 8) + 重大度値。セキュリティレベルについては、「メッセージコードの重大度レベルの設定」を参照してください。</p> <p>ファシリティコードの有効なオプションは次のとおりです。</p> <ul style="list-style-type: none">• LOCAL0 (コード = 16)• LOCAL1 (コード = 17)• LOCAL2 (コード = 18)• LOCAL3 (コード = 19)• LOCAL4 (コード = 20)• LOCAL5 (コード = 21)• LOCAL6 (コード = 22、デフォルト)• LOCAL7 (コード = 23)

フィールド	説明
時刻	<p>生成元の Cisco ISE サーバのローカルクロックに従った、YYYY Mmm DD hh:mm:ss フォーマットでのメッセージ生成の日付。</p> <p>値は次のとおりです。</p> <ul style="list-style-type: none"> • YYYY = 年を表す数字。 • Mmm = 月の表現 (Jan、Feb、Mar、Apr、May、Jun、Jul、Aug、Sep、Oct、Nov、Dec)。 • DD = 日を表す数字。1桁の日付 (1～9) の場合は、数字の前に空白が付きます。 • hh = 時間 : 00 ～ 23。 • mm = 分 : 00 ～ 59。 • ss = 秒 : 00 ～ 59。 <p>一部のデバイスは、タイムゾーンを -/+hhmm のフォーマットで指定するメッセージを送信します。 - と + は、Cisco ISE サーバのタイムゾーンからのオフセット方向を示します。 hh はオフセットの時間数、mm はオフセット時間の分数です。たとえば、+02:00 は、タイムスタンプによって示された時刻に、Cisco ISE サーバのタイムゾーンよりも 2 時間先行する Cisco ISE ノードでメッセージが発生したことを示します。</p>
xx:xx:xx:xx/host_name	発信元の Cisco ISE ノードの IP アドレスまたはホスト名。
cat_name	先頭に CSCOxxx 文字列が付いたロギングカテゴリ名。
msg_id	固有のメッセージ ID。1～4294967295 です。メッセージ ID は、新しいメッセージごとに 1 つ増加します。メッセージ ID は、アプリケーションが再起動するたびに 1 から再開します。

フィールド	説明
<i>total_seg</i>	ログ メッセージ内のセグメントの総数。長いメッセージは複数のセグメントに分割されます。 (注) <i>total_seg</i> は、[リモート ロギング ターゲット (Remote Logging Targets)] ページの [最大長 (Maximum Length)] 設定によって異なります。「リモート ロギング ターゲットの設定」を参照してください。
<i>seg_num</i>	メッセージ内のセグメントの順序番号。この数値を使用して、メッセージのどのセグメントを表示しているかを判断します。

syslog メッセージデータまたはペイロードは、[ローカル ストア syslog メッセージの形式](#)と同じです。リモート syslog サーバターゲットは、ファシリティ コード名 LOCAL0～LOCAL7 によって識別されます (LOCAL6 がデフォルトのロギング ロケーションです)。リモート syslog サーバに割り当てるログ メッセージは、Linux syslog のデフォルトの場所 (/var/log/messages) に送信されますが、サーバで別の場所を設定できます。

リモート syslog 収集場所の設定

syslog を保存する外部の場所を作成できます。

UDP syslog (ログ コレクタ) はデフォルトのリモート ロギング ターゲットです。このロギング ターゲットは、無効にすると、ログ コレクタとして動作しなくなり、[ロギング カテゴリ (Logging Categories)] ページから削除されます。このロギング ターゲットを有効にした場合は、[ロギング カテゴリ (Logging Categories)] ページのログ コレクタになります。

- ステップ 1** [管理 (Administration)] > [システム (System)] > [ロギング (Logging)] > [リモート ロギング ターゲット (Remote Logging Targets)] を選択します。
- ステップ 2** [追加 (Add)] をクリックします。
- ステップ 3** 次の必須詳細情報を入力します。
- ステップ 4** [保存 (Save)] をクリックします。
- ステップ 5** [リモート ロギング ターゲット (Remote Logging Targets)] ページに移動し、新しいターゲットが作成されたことを確認します。

その後、ロギングターゲットを、以下のそれぞれのロギング カテゴリにマッピングできます。PSN ノードは、それらのノードで有効になっているサービスに応じて、該当するログをリモート ロギング ターゲットに送信します。

- AAA 監査

- AAA の診断
- アカウンティング (Accounting)
- 外部 MDM
- パッシブ ID
- ポスチャおよびクライアントプロビジョニングの監査 (Posture and Client Provisioning Audit)
- ポスチャおよびクライアントプロビジョニングの診断 (Posture and Client Provisioning Diagnostics)
- プロファイラ

展開内のすべてのノードによって、次のカテゴリのログがロギング ターゲットに送信されます。

- 管理および操作の監査 (Administrative and Operational Audit)
- システム診断
- システム統計

Cisco ISE メッセージコード

ロギング カテゴリは、ACS の機能、フロー、または使用例を説明するメッセージ コードのバンドルです。Cisco ISE では、各ログにはログ メッセージの内容に従ってロギング カテゴリにバンドルされているメッセージ コードが関連付けられています。ロギング カテゴリは、含まれているメッセージの内容を説明する場合に役立ちます。

ロギング カテゴリはロギング設定で役立ちます。各カテゴリには、アプリケーションの要件に応じて設定可能な名前、ターゲット、および重大度レベルがあります。

Cisco ISE では、サービスに対して事前定義されたロギング カテゴリ ([ポスチャ (Posture)]、[プロファイラ (Profiler)]、[ゲスト (Guest)]、[AAA (認証、許可、アカウンティング)

(AAA (authentication, authorization, and accounting))] など) が提供されており、これらにログ ターゲットを割り当てることができます。

関連トピック

[メッセージ コードの重大度レベルの設定](#) (320 ページ)

メッセージ コードの重大度レベルの設定

ログの重大度レベルを設定し、選択したカテゴリのログが格納されるロギングターゲットを選択できます。

ステップ 1 [管理 (Administration)] > [システム (System)] > [ロギング (Logging)] > [ロギング カテゴリ (Logging Categories)] を選択します。

- ステップ2 編集するカテゴリの隣のオプション ボタンをクリックにして、[編集 (Edit)] をクリックします。
- ステップ3 必須フィールドの値を変更します。
- ステップ4 [保存 (Save)] をクリックします。
- ステップ5 [ロギング カテゴリ (Logging Categories)] ページに移動し、特定のカテゴリに対して行われた設定の変更内容を確認します。

Cisco ISE メッセージ カタログ

可能性があるすべてのログメッセージと説明を表示するために、[メッセージカタログ (Message Catalog)] ページを使用できます。[管理 (Administration)] > [システム (System)] > [ロギング (Logging)] > [メッセージ カタログ (Message Catalog)] を選択します。

[ログメッセージカタログ (Log Message Catalog)] ページが表示されます。このページでは、ログ ファイルに記録される可能性があるすべてのログ メッセージを表示できます。このページで利用可能なデータは、表示専用です。

デバッグ ログ

デバッグログにより、ブートストラップ、アプリケーション設定、ランタイム、展開、モニタリングとレポート、および公開キー インフラストラクチャ (PKI) に関する情報が取得されます。過去 30 日間の重大アラームと警告アラーム、および過去 7 日間の情報アラームがデバッグ ログに含まれます。

個々のコンポーネントのデバッグ ログ重大度レベルを設定できます。

ノードまたはコンポーネントで [デフォルトにリセット (Reset to Default)] オプションを使用して、ログ レベルを出荷時のデフォルト値に戻すことができます。

ローカル サーバにデバッグ ログを保存できます。



- (注) デバッグ ログの設定は、システムをバックアップから復元した場合やアップグレードした場合には保存されません。

関連トピック

[デバッグ ログの重大度レベルの設定](#) (322 ページ)

ノードのロギング コンポーネントの表示

- ステップ1 [管理 (Administration)] > [システム (System)] > [ロギング (Logging)] > [デバッグ ログ設定 (Debug Log Configuration)] を選択します。

ステップ 2 ログイング コンポーネントを表示するノードを選択し、[編集 (Edit)] をクリックします。

[デバッグ レベルの設定 (Debug Level Configuration)] ページが表示されます。次の詳細情報を表示できます。

- 選択したノードで実行中のサービスに基づくログイング コンポーネントのリスト
- 各コンポーネントの説明
- 個々のコンポーネントに設定されている現在のログ レベル

デバッグ ログの重大度レベルの設定

デバッグ ログの重大度レベルを設定できます。

ステップ 1 [管理 (Administration)] > [システム (System)] > [ログイング (Logging)] > [デバッグ ログの設定 (Debug Log Configuration)] を選択します。

ステップ 2 ノードを選択して、[編集 (Edit)] をクリックします。

[デバッグ ログの設定 (Debug Log Configuration)] ページには、選択したノードで実行されているサービス、および個別のコンポーネントに対して設定されている現在のログ レベルに基づいたコンポーネントのリストが表示されます。

ノードまたはコンポーネントで [デフォルトにリセット (Reset to Default)] オプションを使用して、ログ レベルを出荷時のデフォルト値に戻すことができます。

ステップ 3 ログ重大度レベルを設定するコンポーネントを選択し、[編集 (Edit)] をクリックします。[ログレベル (Log Level)] ドロップダウン リストから目的のログ重大度レベルを選択し、[保存 (Save)] をクリックします。

(注) runtime-AAA コンポーネントのログ重大度レベルを変更すると、サブコンポーネント prrt-JNI のログレベルも変更されます。サブコンポーネントのログレベルを変更しても、その親コンポーネントには影響はありません。

関連トピック

[Cisco ISE デバッグ ログ](#) (1088 ページ)

エンドポイントのデバッグ ログ コレクタ

特定のエンドポイントの問題をトラブルシューティングするために、IP アドレスまたは MAC アドレスに基づいて、特定のエンドポイントのデバッグ ログをダウンロードできます。その特定のエンドポイント固有のログが、展開内のさまざまなノードから1つのファイルに収集されるため、迅速かつ効率的に問題をトラブルシューティングできます。このトラブルシューティ

ングツールは、一度に1つのエンドポイントに対してのみ実行できます。ログファイルがGUIに表示されます。1つのノードまたは展開内のすべてのノードからエンドポイントのログをダウンロードできます。

特定のエンドポイントのデバッグ ログのダウンロード

ネットワーク内の特定のエンドポイントの問題をトラブルシューティングするには、管理者ポータルからデバッグ エンドポイント ツールを使用できます。または、このツールを [認証 (Authentications)] ページから実行できます。[認証 (Authentications)] ページの [エンドポイント ID (Endpoint ID)] を右クリックして、[エンドポイント デバッグ (Endpoint Debug)] をクリックします。このツールでは、単一ファイルの特定のエンドポイントに関連するすべてのサービスに関するすべてのデバッグ情報が提供されます。

始める前に

デバッグ ログを収集するエンドポイントの IP アドレスまたは MAC アドレスが必要です。

-
- ステップ 1** [操作 (Operations)] > [トラブルシューティング (Troubleshoot)] > [診断ツール (Diagnostic Tools)] > [一般ツール (General Tools)] > [エンドポイント デバッグ (Endpoint Debug)] を選択します。
- ステップ 2** [MAC アドレス (MAC Address)] または [IP] オプション ボタンをクリックし、エンドポイントの MAC または IP アドレスを入力します。
- ステップ 3** 一定の時間が経過した後ログ収集を停止する場合は、[*n* 分後に自動的に無効化 (Automatic disable after *n* Minutes)] チェックボックスをオンにします。このチェックボックスをオンにする場合は、1 ~ 60 分の時間を入力する必要があります。
- 次のメッセージが表示されます。「エンドポイントデバッグによって、展開のパフォーマンスが低下します。続行しますか? (Endpoint Debug degrades the deployment performance.Would you like to continue?)」
- ステップ 4** ログを収集するには、[続行 (Continue)] をクリックします。
- ステップ 5** 手動でログの収集を中止する場合は、[停止 (Stop)] をクリックします。
-

関連トピック

[エンドポイントのデバッグ ログ コレクタ](#) (322 ページ)

収集フィルタ

収集フィルタを設定して、モニタリングサーバおよび外部サーバに送信される syslog メッセージを抑制できます。抑制は、異なる属性タイプに基づいてポリシー サービス ノード レベルで実行できます。特定の属性タイプおよび対応する値を使用して複数のフィルタを定義できます。

モニタリング ノードまたは外部サーバに syslog メッセージを送信する前に、Cisco ISE は送信する syslog メッセージのフィールドとそれらの値を比較します。一致が見つかった場合、対応するメッセージは送信されません。

収集フィルタの設定

さまざまな属性のタイプに基づいて複数の収集フィルタを設定できます。フィルタ数を 20 に制限することを推奨します。収集フィルタを追加、編集、または削除できます。

ステップ 1 [管理 (Administration)] > [システム (System)] > [ロギング (Logging)] > [収集フィルタ (Collection Filters)] を選択します。

ステップ 2 [追加 (Add)] をクリックします。

ステップ 3 次のリストから **フィルタ タイプ** を選択します。

- ユーザ名 (User Name)
- MAC アドレス (MAC Address)
- ポリシー セット名
- NAS IP アドレス
- Device IP Address (デバイス IP アドレス)

ステップ 4 選択したフィルタ タイプの対応する **値** を入力します。

ステップ 5 ドロップダウン リストから **結果** を選択します。結果は、[すべて (All)]、[成功 (Passed)]、または [失敗 (Failed)] になります。

ステップ 6 [送信 (Submit)] をクリックします。

関連トピック

[収集フィルタ](#) (323 ページ)

[イベント抑制バイパス フィルタ](#) (324 ページ)

イベント抑制バイパス フィルタ

Cisco ISE では、フィルタを設定し、収集フィルタを使用して、一部の syslog メッセージがモニタリングノードおよび他の外部サーバに送信されることを抑制できます。場合によっては、これらの抑制されたログ メッセージにアクセスすることが必要になります。Cisco ISE は、設定可能な時間について、ユーザ名などの属性に基づいてイベント抑制をバイパスするオプションを提供します。デフォルトは 50 分ですが、5 分から 480 分 (8 時間) の期間を設定できます。イベント抑制バイパスは、設定した後すぐに有効になります。設定した期間が経過すると、バイパス抑制フィルタは失効します。

抑制バイパス フィルタは、Cisco ISE ユーザ インターフェイスの [収集フィルタ (Collection Filters)] ページから設定できます。この機能を使用して、特定の ID (ユーザ) のすべてのログを表示し、その ID の問題をリアルタイムでトラブルシューティングできます。

フィルタは有効または無効にできます。バイパス イベント フィルタで設定した期間が経過すると、フィルタは再度有効にするまで自動的に無効になります。

Cisco ISE は設定変更監査レポートでこれらの設定変更を取得します。このレポートは、イベント抑制またはバイパス抑制を設定したユーザ、およびイベントが抑制された期間または抑制がバイパスされた期間に関する情報を提供します。



第 13 章

バックアップ/復元操作

- [バックアップデータのタイプ \(327 ページ\)](#)
- [バックアップ/復元リポジトリ \(328 ページ\)](#)
- [オンデマンドおよびスケジュール バックアップ \(331 ページ\)](#)
- [Cisco ISE 復元操作 \(337 ページ\)](#)
- [認証および許可ポリシー設定のエクスポート \(344 ページ\)](#)
- [分散環境でのプライマリ ノードとセカンダリ ノードの同期 \(345 ページ\)](#)
- [スタンドアロンおよび分散展開での失われたノードの復元 \(345 ページ\)](#)

バックアップデータのタイプ

Cisco ISE では、プライマリ PAN とモニタリング ノードからデータをバックアップすることができます。バックアップは CLI またはユーザ インターフェイスから実行できます。

Cisco ISE では次のタイプのデータのバックアップが可能です。

- **設定データ**：アプリケーション固有および Cisco ADE オペレーティング システム両方の設定データが含まれます。バックアップは、GUI または CLI を使用してプライマリ PAN を介して実行できます。
- **運用データ**：モニタリングおよびトラブルシューティング データが含まれます。バックアップは、プライマリ PAN GUI を介して、またはモニタリング ノードの場合は CLI を使用して実行できます。

Cisco ISE が VMware で実行されている場合、ISE データをバックアップするのに、VMware スナップショットはサポートされていません。



(注) Cisco ISE は、ISE データのバックアップ用の VMware スナップショットをサポートしていません。これは、VMware スナップショットが特定の時点で VM のステータスを保存するためです。マルチノード Cisco ISE 環境では、すべてのノードのデータは、現在のデータベース情報と継続的に同期されます。スナップショットを復元すると、データベースのレプリケーションと同期の問題を引き起こす可能性があります。シスコは、データのバックアップおよび復元用に、Cisco ISE に含まれるバックアップ機能を使用することを推奨します。

VMware スナップショットまたはサードパーティのバックアップを使用して ISE データをバックアップすると、Cisco ISE サービスが停止します。バックアップが VMware または Comvault SAN レベルのバックアップのようなサードパーティによって開始された場合、ファイル システムを休止してクラッシュ整合を維持するため、ISE のフリーズを引き起こします。ISE のサービスを再開するには再起動が必要です。

例：VM スナップショット、Comvault SAN レベルのバックアップなど。

復元操作は、以前のバージョンの Cisco ISE のバックアップ ファイルを使用して実行でき、以降のバージョンで復元できます。たとえば、Cisco ISE リリース 1.3 または 1.4 からの ISE ノードのバックアップがある場合、そのバックアップを Cisco ISE リリース 2.1 で復元できます。

Cisco ISE リリース 2.2 は、リリース 1.4 以降から取得したバックアップからの復元をサポートしています。

バックアップ/復元リポジトリ

Cisco ISE では管理者ポータルを使用してリポジトリを作成および削除することができます。次のタイプのリポジトリを作成できます。

- ディスク (DISK)
- FTP
- SFTP
- NFS
- CD-ROM
- HTTP
- HTTPS



(注) リポジトリは、各デバイスに対してローカルです。



- (注) 小規模な展開（100 個以下のエンドポイント）では、10 GB のリポジトリを、中規模の展開では 100 GB のリポジトリを、大規模な展開では 200 GB のリポジトリを用意することを推奨します。

関連トピック

[リポジトリの作成](#)（329 ページ）

[オンデマンドおよびスケジュールバックアップ](#)（331 ページ）

リポジトリの作成

リポジトリを作成するには、CLI と GUI を使用できます。次の理由により、GUI を使用することを推奨します。

- CLI で作成されたリポジトリはローカルに保存され、他の展開ノードに複製されません。これらのリポジトリは、GUI のリポジトリ ページに表示されません。
- プライマリ PAN で作成されたリポジトリは、他の展開ノードに複製されます。

キーはプライマリ PAN でのみ GUI で生成されます。このためアップグレード時に、新しいプライマリ管理ノードの GUI でキーを再生成して、SFTP サーバにエクスポートする必要があります。展開からノードを除去する場合、非管理ノードの GUI でキーを生成し、SFTP サーバにエクスポートする必要があります。

RSA 公開キー認証を使用する Cisco ISE の SFTP リポジトリを設定できます。データベースとログを暗号化するために管理者が作成したパスワードを使用する代わりに、セキュアキーを使用する RSA 公開キー認証を選択できます。RSA 公開キーを使用して作成された SFTP リポジトリの場合、GUI から作成されたリポジトリは CLI では複製されず、CLI から作成されたリポジトリは GUI では複製されません。CLI と GUI で同じリポジトリを設定するには、CLI と GUI の両方で RSA 公開キーを生成し、この両方のキーを SFTP サーバにエクスポートします。

始める前に

- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。
- RSA 公開キー認証を使用する SFTP リポジトリを作成する場合は、次を実行してください。
 - SFTP リポジトリの RSA 公開キー認証を有効にします。詳細については、[SFTP リポジトリでの RSA 公開キー認証の有効化](#)（330 ページ）を参照してください。
 - `crypto host_key add` コマンドを使用して Cisco ISE CLI から SFTP サーバのホスト キーを入力します。ホスト キー文字列は、リポジトリの設定ページで、[パス (Path)] フィールドに入力したホスト名と一致する必要があります。
 - GUI でキーペアを生成し、ローカルシステムに公開キーをエクスポートします。Cisco ISE CLI から `crypto key generate rsa passphrase test123` コマンドを使用してキー ペアを

生成し（この場合パスフレーズは5文字以上でなければなりません）、キーを任意のリポジトリ（ローカルディスクまたは設定されているその他のリポジトリ）にエクスポートします。

- エクスポートした RSA 公開キーを PKI 対応の SFTP サーバにコピーし、「authorized_keys」ファイルに追加します。

-
- ステップ 1** [管理 (Administration)] > [システム (System)] > [メンテナンス (Maintenance)] > [リポジトリ (Repository)] を選択します。
- ステップ 2** [追加 (Add)] をクリックして、新しいリポジトリを追加します。
- ステップ 3** 新しいリポジトリのセットアップの必要に応じて値を入力します。フィールドの説明については、[リポジトリの設定 \(1171 ページ\)](#) を参照してください。
- ステップ 4** [送信 (Submit)] をクリックしてリポジトリを作成します。
- ステップ 5** 左側の [操作 (Operations)] ナビゲーションペインで [リポジトリ (Repository)] をクリックするか、このページ上部の [リポジトリ リスト (Repository List)] リンクをクリックして、リポジトリのリスト ページに移動して、リポジトリが正常に作成されていることを確認します。
-

次のタスク

- 作成したリポジトリが有効であることを確認します。これは、リポジトリのリストページから行います。リポジトリを選択し、[確認 (Validate)] をクリックします。また、Cisco ISE コマンドライン インターフェイスから次のコマンドを実行することもできます。

show repository repository_name

ここで、*repository_name* は作成したリポジトリの名前です。



- (注) リポジトリの作成時に指定したパスが存在しない場合、「%無効なディレクトリです (%Invalid Directory)」というエラーが表示されます。

- オンデマンド バックアップを実行するかバックアップのスケジュールを設定します。

関連トピック

[オンデマンド バックアップの実行 \(332 ページ\)](#)

[バックアップのスケジュール \(334 ページ\)](#)

SFTP リポジトリでの RSA 公開キー認証の有効化

SFTP リポジトリの RSA 公開キー認証を有効にするには、以下のステップに従います。

ステップ 1 `/etc/ssh/sshd_config` ファイルを編集する権限を持つアカウントで SFTP サーバにログインします。

(注) `sshd_config` ファイルのロケーションは、インストールされているオペレーティング システムによって異なる可能性があります。

ステップ 2 `vi /etc/ssh/sshd_config` コマンドを入力します。

`Sshd_config` ファイルの内容がリストされます。

ステップ 3 RSA 公開キー認証を有効にするには、以下の行の「#」記号を削除します。

- `RSAAuthentication yes`
- `PubkeyAuthentication yes`

(注) `Public Auth Key` が `no` の場合は `yes` に変更してください。

- `AuthorizedKeysFile ~/.ssh/authorized_keys`

オンデマンドおよびスケジュール バックアップ

Cisco ISE では、プライマリ PAN およびプライマリ モニタリング ノードのオンデマンド バックアップができます。バックアップ データがすぐに必要な場合にオンデマンド バックアップを実行します。

Cisco ISE では、1 回、毎日、毎週、または毎月実行するようにシステム レベルのバックアップをスケジュールできます。バックアップ操作は長時間かかる場合がありますが、スケジュールできるため中断が発生することはありません。Cisco ISE 管理者ポータルからバックアップをスケジュールできます。



(注) Cisco ISE リリース 1.2 にアップグレードする場合は、バックアップ ジョブのスケジュール設定を再作成する必要があります。

関連トピック

- [バックアップのスケジュール](#) (334 ページ)
- [オンデマンド バックアップの実行](#) (332 ページ)
- [CLI を使用したバックアップ](#) (336 ページ)
- [バックアップ履歴](#) (336 ページ)
- [バックアップの失敗](#) (336 ページ)
- [Cisco ISE 復元操作](#) (337 ページ)
- [メンテナンスの設定](#) (1171 ページ)

オンデマンドバックアップの実行

オンデマンドバックアップを実行して、即座に設定データまたはモニタリング（運用）データをバックアップすることができます。復元操作では、バックアップ取得時の設定状態に Cisco ISE が復元されます。



重要

バックアップと復元を行う場合、復元では、ターゲットシステムの信頼できる証明書のリストがソースシステムの証明書のリストで上書きされます。バックアップおよび復元機能に内部認証局（CA）の証明書に関連付けられた秘密キーが含まれないことに注意することが非常に重要です。

1 つのシステムから別のシステムにバックアップと復元を行う場合は、エラーを回避するために、次のオプションのいずれかを選択する必要があります。

• オプション 1 :

CA 証明書をソース ISE ノードから CLI を使用してエクスポートし、ターゲットシステムに CLI を使用してインポートします。

長所： ソースシステムからエンドポイントに発行されたすべての証明書が引き続き信頼されます。ターゲットシステムによって発行された新しい証明書は、同じキーによって署名されます。

短所： 復元機能を使用する前にターゲットシステムによって発行された証明書は信頼されないため、再発行する必要があります。

• オプション 2 :

復元処理の後、内部 CA のすべての新しい証明書を生成します。

長所： このオプションは推奨される適切な方法です。元のソースの証明書も元のターゲットの証明書も使用されません。元のソースシステムによって発行された証明書は引き続き信頼されます。

短所： 復元機能の前にターゲットシステムによって発行された証明書は信頼されず、再発行される必要があります。

始める前に

- この作業を実行する前に、Cisco ISE のバックアップデータのタイプの基本を理解する必要があります。
- バックアップ ファイルを格納するリポジトリを作成したことを確認します。
- ローカル リポジトリを使用してバックアップしないでください。リモート モニタリング ノードのローカル リポジトリで、モニタリング データをバックアップすることはできません。
- バックアップを取得する前に、すべての証明書関連の変更を実行します。

- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。



(注) バックアップ/復元操作では、次のリポジトリタイプはサポートされていません。CD-ROM、HTTP、HTTPS、またはTFTP。これは、これらのリポジトリタイプが読み取り専用であるか、またはプロトコルでファイルのリストがサポートされないためです。バックアップを復元するには、リポジトリを選択し、[復元 (Restore)] をクリックします。

- ステップ 1** [管理 (Administration)] > [システム (System)] > [バックアップ/復元 (Backup and Restore)] を選択します。
- ステップ 2** [すぐにバックアップ (Backup Now)] をクリックします。
- ステップ 3** バックアップを実行するために必要な値を入力します。
- ステップ 4** [OK][バックアップ (Backup)] をクリックします。
- ステップ 5** バックアップが正常に完了したことを確認します。

Cisco ISE はタイムスタンプを持つバックアップファイル名を付け、指定されたリポジトリにファイルを保存します。タイムスタンプに加えて、Cisco ISE は設定バックアップには CFG タグ、操作バックアップには OPS タグを追加します。バックアップファイルが指定リポジトリにあることを確認します。

分散展開では、バックアップの実行中にノードのロールを変更したり、ノードの設定を行ったりすることはできません。バックアップの実行中にノードのロールを変更すると、すべてのプロセスがシャットダウンし、データに不一致が生じる場合があります。ノードのロールを変更する際は、バックアップが完了するまで待機してください。

バックアップの実行中はノードを昇格しないでください。これによりすべてのプロセスがシャットダウンし、バックアップを同時に実行中の場合はデータに不一致が生じる場合があります。ノードを変更する際は、バックアップが完了するまで待ってください。

- (注) バックアップが実行されているときに、高い CPU 使用率が観察されたり、[負荷平均が高い (High Load Average)] アラームが表示されたりする可能性があります。バックアップが完了すると、CPU 使用率は通常に戻ります。

関連トピック

- [バックアップデータのタイプ](#) (327 ページ)
- [リポジトリの作成](#) (329 ページ)
- [バックアップ/復元リポジトリ](#) (328 ページ)
- [バックアップのスケジュール](#) (334 ページ)
- [CLI を使用したバックアップ](#) (336 ページ)
- [バックアップ履歴](#) (336 ページ)

[バックアップの失敗](#) (336 ページ)

[Cisco ISE 復元操作](#) (337 ページ)

[認証および許可ポリシー設定のエクスポート](#) (344 ページ)

バックアップのスケジュール

オンデマンドバックアップを実行して、即座に設定データまたはモニタリング（運用）データをバックアップすることができます。復元操作では、バックアップ取得時の設定状態に Cisco ISE が復元されます。



重要

バックアップと復元を行う場合、復元では、ターゲットシステムの信頼できる証明書のリストがソースシステムの証明書のリストで上書きされます。バックアップおよび復元機能に内部認証局（CA）の証明書に関連付けられた秘密キーが含まれないことに注意することが非常に重要です。

1 つのシステムから別のシステムにバックアップと復元を行う場合は、エラーを回避するために、次のオプションのいずれかを選択する必要があります。

• オプション 1 :

CA 証明書をソース ISE ノードから CLI を使用してエクスポートし、ターゲットシステムに CLI を使用してインポートします。

長所： ソースシステムからエンドポイントに発行されたすべての証明書が引き続き信頼されます。ターゲットシステムによって発行された新しい証明書は、同じキーによって署名されます。

短所： 復元機能を使用する前にターゲットシステムによって発行された証明書は信頼されないため、再発行する必要があります。

• オプション 2 :

復元処理の後、内部 CA のすべての新しい証明書を生成します。

長所： このオプションは推奨される適切な方法です。元のソースの証明書も元のターゲットの証明書も使用されません。元のソースシステムによって発行された証明書は引き続き信頼されます。

短所： 復元機能の前にターゲットシステムによって発行された証明書は信頼されず、再発行される必要があります。

始める前に

- この作業を実行する前に、Cisco ISE のバックアップデータのタイプの基本を理解している必要があります。
- リポジトリを設定していることを確認します。

- ローカル リポジトリを使用してバックアップしないでください。リモート モニタリング ノードのローカル リポジトリで、モニタリング データをバックアップすることはできません。
- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。
- Cisco ISE 1.1 以前のリリースから Cisco ISE 1.2 にアップグレードする場合、バックアップのスケジュールを再設定する必要があります。『*Cisco Identity Services Engine Upgrade Guide, Release 1.2*』の「Known Upgrade Issues」の項を参照してください。



(注) バックアップ/復元操作では、次のリポジトリ タイプはサポートされていません。CD-ROM、HTTP、HTTPS、またはTFTP。これは、これらのリポジトリ タイプが読み取り専用であるか、またはプロトコルでファイルのリストがサポートされないためです。

- ステップ 1** [管理 (Administration)] > [システム (System)] > [バックアップ/復元 (Backup and Restore)] を選択します。
- ステップ 2** [作成 (Create)] [スケジュール (Schedule)] をクリックして、設定または操作バックアップをスケジュールします。
- ステップ 3** 必要に応じてバックアップをスケジュールするための値を入力します。
- ステップ 4** [保存 (Save)] をクリックして、バックアップをスケジュールします。
- ステップ 5** このページの上部にある[更新 (Refresh)] リンクをクリックして、スケジュールバックアップのリストを表示します。

作成できる設定または操作バックアップのスケジュールは 1 回に 1 つだけです。スケジュールバックアップは有効化または無効化できますが、削除はできません。

関連トピック

- [バックアップ データのタイプ](#) (327 ページ)
- [オンデマンドおよびスケジュール バックアップ](#) (331 ページ)
- [オンデマンド バックアップの実行](#) (332 ページ)
- [CLI を使用したバックアップ](#) (336 ページ)
- [バックアップ履歴](#) (336 ページ)
- [バックアップの失敗](#) (336 ページ)
- [バックアップ/復元リポジトリ](#) (328 ページ)

CLI を使用したバックアップ

CLI と GUI の両方からバックアップをスケジュールできますが、GUI から実行することを推奨します。ただし、セカンダリ モニタリング ノードの操作バックアップは、CLI からのみ実行できます。

バックアップ履歴

バックアップ履歴は、スケジュールまたはオンデマンドバックアップに関する基本情報です。バックアップ履歴には、バックアップ名、バックアップファイルのサイズ、バックアップが保存されているリポジトリ、バックアップが取られたタイムスタンプを表示します。この情報は、操作監査レポートまたは、履歴テーブルの [バックアップ/復元 (Backup and Restore)] ページから入手できます。

バックアップが失敗すると、Cisco ISE がアラームをトリガーします。バックアップ履歴ページに失敗の原因が表示されます。障害の原因は操作監査レポートにも記載されます。障害の原因が欠落しているか明確でない場合は、Cisco ISE CLI から **backup-logs** コマンドを実行し、ADE.log でより詳細な情報を確認できます。

バックアップ操作の実行中は、**show backup status** CLI コマンドを使用して、バックアップ操作の進行状況を確認することができます。

バックアップ履歴は、Cisco ADE オペレーティングシステムの設定データとともに保存されています。つまり、アプリケーションのアップグレード後もそこに残っており、PAN のイメージを再作成した場合にのみ削除されます。

バックアップの失敗

バックアップが失敗した場合は、次を確認してください。

- 他のバックアップが同時に実行されていないことを確認します。
- 設定したリポジトリの使用可能なディスク領域を確認します。
 - (操作) バックアップのモニタリングは、モニタリングデータがモニタリングデータベースに割り当てられたサイズの 75% を超えると失敗します。たとえばモニタリング ノードに 600 GB 割り当てられており、モニタリングデータがストレージの 450 GB を超える領域を消費すると、モニタリングのバックアップは失敗します。
 - データベースのディスク使用量が 90% を超える場合、消去が発生してデータベースを割り当てられたサイズの 75% 以下のサイズにします。
- 消去が進行中かどうかを確認します。消去の進行中はバックアップ/復元操作は動作しません。
- リポジトリが正しく設定されていることを確認します。

Cisco ISE 復元操作

プライマリまたはスタンドアロン 管理ノードで設定データを復元できます。プライマリ PAN にデータを復元したら、手動でセカンダリ ノードをプライマリ PAN と同期する必要があります。

運用データを復元するプロセスは、展開のタイプによって異なります。



- (注) Cisco ISE の新しいバックアップ/復元ユーザインターフェイスでは、バックアップファイル名にメタデータが使用されます。したがって、バックアップが完了後に、バックアップファイル名を手動で変更しないでください。バックアップ ファイルの名前を手動で変更すると、Cisco ISE バックアップ/復元ユーザ インターフェイスがそのバックアップ ファイルを認識できなくなります。バックアップファイル名を変更しなければならない場合は、バックアップの復元に Cisco ISE CLI を使用する必要があります。

関連トピック

[CLI からの設定またはモニタリング \(操作\) バックアップの復元 \(338 ページ\)](#)

[GUI からの設定バックアップの復元 \(341 ページ\)](#)

[モニタリング データベースの復元 \(341 ページ\)](#)

[分散環境でのプライマリ ノードとセカンダリ ノードの同期 \(345 ページ\)](#)

データの復元に関するガイドライン

次は、Cisco ISE バックアップ データを復元する場合に従うべきガイドラインです。

- Cisco ISE では、ある ISE ノード (A) からバックアップを取得して、別の ISE ノード (B) に復元することができます。両方のノードは同じホスト名 (IP アドレスは異なる) です。ただし、ノード B 上のバックアップを復元した後は、証明書とポータル グループ タグの問題が生じる可能性があるため、ノード B のホスト名を変更することはできません。
- あるタイムゾーン内のプライマリ PAN からバックアップを取得して、別のタイムゾーン内の別の Cisco ISE ノードに復元する場合、復元プロセスが失敗することがあります。この問題は、バックアップ ファイルのタイムスタンプが、バックアップが復元される Cisco ISE ノードのシステム時刻より新しい場合に発生します。同じバックアップを、取得後 1 日経過してから復元すると、バックアップ ファイルのタイムスタンプが過去のものになり、復元プロセスは成功します。
- バックアップを取得したホスト名と別のホスト名を持つプライマリ PAN にバックアップを復元すると、プライマリ PAN はスタンドアロン ノードになります。展開が切断し、セカンダリ ノードは機能しなくなります。スタンドアロン ノードをプライマリ ノードにし、セカンダリ ノードの設定をリセットしてプライマリ ノードに再登録する必要があります。Cisco ISE ノードの設定をリセットするには、Cisco ISE CLI から次のコマンドを入力してください。

• application reset-config ise

- システムのタイムゾーンは、最初の Cisco ISE インストールおよびセットアップ後に変更しないことを推奨します。
- 展開の 1 つ以上のノードの証明書設定を変更した場合は、データを復元するための別のバックアップをスタンドアロン Cisco ISE ノードまたはプライマリ PAN から取得する必要があります。そうしないで古いバックアップを使用してデータを復元すると、ノード間の通信が失敗する可能性があります。
- プライマリ PAN 上で設定バックアップを復元した後に、以前にエクスポートした Cisco ISE CA 証明書およびキーをインポートできます。



(注) Cisco ISE CA 証明書およびキーをエクスポートしなかった場合は、プライマリ PAN 上で設定バックアップを復元した後に、プライマリ PAN およびポリシー サービス ノード (PSN) でルート CA および下位 CA を生成します。

- Cisco ISE がバックアップ ファイルを格納するデータ リポジトリが必要です。オンデマンドまたはスケジュール設定されたバックアップを実行する前に、リポジトリを作成する必要があります。
- スタンドアロン管理ノードに障害が発生した場合、設定バックアップを実行して復元する必要があります。プライマリ PAN で障害が発生した場合、分散セットアップを使用してセカンダリ管理ノードをプライマリに昇格できます。その後、新しいプライマリ PAN にデータを復元できます。



(注) Cisco ISE では、**backup-logs** CLI コマンドも使用できます。このコマンドを使用して、ログやコンフィギュレーションファイルの収集を行い、これらをトラブルシューティングに利用できます。

CLI からの設定またはモニタリング（操作）バックアップの復元

Cisco ISE CLI から設定データを復元するには、EXEC モードで **restore** コマンドを使用します。設定または操作バックアップからデータを復元するには、次のコマンドを使用します。

restore filename repository repository-name encryption-key hash|plain encryption-key nameinclude-adeos

構文の説明

restore	設定または操作バックアップからデータを復元するには、このコマンドを入力します。
----------------	---

<i>filename</i>	リポジトリに存在するバックアップ ファイルのファイル名。最大 120 文字の英数字をサポートします。 (注) ファイル名の後に、 tar.gpg という拡張子を付ける必要があります (myfile.tar.gpg など)。
repository	バックアップを含むリポジトリを指定します。
<i>repository-name</i>	バックアップを復元するリポジトリの名前。
encryption-key	(オプション) バックアップを復元するユーザ定義の暗号キーを指定します。
hash	バックアップを復元するためのハッシュされた暗号キー。使用する暗号化された (ハッシュ化された) 暗号化キーを指定します。40 文字までで指定します。
plain	バックアップを復元するためのプレーン テキストの暗号キー。使用する暗号化されたプレーンテキストの暗号化キーを指定します。15 文字までで指定します。
<i>encryption-key name</i>	暗号キーを入力します。
include-adeos	(オプション、設定バックアップのみに該当) 設定バックアップから ADE-OS 設定を復元する場合に、このコマンドオペレータパラメータを入力します。設定バックアップを復元する場合にこのパラメータを含めないと、Cisco ISE は Cisco ISE アプリケーション設定データのみを復元します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

EXEC

使用上のガイドライン

Cisco ISE で **restore** コマンドを使用すると、Cisco ISE サーバが自動的に再起動します。

データの復元処理で、暗号キーはオプションです。暗号キーを指定しなかった以前のバックアップの復元をサポートするために、暗号キーなしで **restore** コマンドを使用できます。

例

```

ise/admin# restore mybackup-100818-1502.tar.gpg repository myrepository encryption-key
plain Lab12345
Restore may require a restart of application services. Continue? (yes/no) [yes] ? yes
Initiating restore. Please wait...
ISE application restore is in progress.
This process could take several minutes. Please wait...
Stopping ISE Application Server...
Stopping ISE Monitoring & Troubleshooting Log Processor...
Stopping ISE Monitoring & Troubleshooting Log Collector...
Stopping ISE Monitoring & Troubleshooting Alert Process...
Stopping ISE Monitoring & Troubleshooting Session Database...
Stopping ISE Database processes...
Starting ISE Database processes...
Starting ISE Monitoring & Troubleshooting Session Database...
Starting ISE Application Server...
Starting ISE Monitoring & Troubleshooting Alert Process...
Starting ISE Monitoring & Troubleshooting Log Collector...
Starting ISE Monitoring & Troubleshooting Log Processor...
Note: ISE Processes are initializing. Use 'show application status ise'
      CLI to verify all processes are in running state.
ise/admin#

```

関連コマンド

	説明
backup	バックアップ（Cisco ISE と Cisco ADE OS）を実行して、そのバックアップをリポジトリに保存します。
backup-logs	システム ログをバックアップします。
repository	バックアップ設定のリポジトリ サブモードを入力します。
show repository	特定のリポジトリにある使用可能なバックアップ ファイルを表示します。
show backup history	システムのバックアップ履歴を表示します。
show backup status	バックアップ操作のステータスを表示します。
show restore status	復元操作のステータスを表示します。

いずれかのセカンダリ ノードでアプリケーション復元後の同期ステータスおよび複製ステータスが [非同期（Out of Sync）] になっている場合、該当セカンダリ ノードの証明書をプライマリ PAN に再インポートして、手動同期を実行する必要があります。

関連トピック

[GUI からの設定バックアップの復元](#)（341 ページ）

[復元履歴](#)（344 ページ）

[分散環境でのプライマリ ノードとセカンダリ ノードの同期](#)（345 ページ）

GUI からの設定バックアップの復元

管理者ポータルで設定バックアップを復元できます。GUIには現在のリリースから取得されたバックアップのみが表示されます。このリリースより前のバックアップを復元するには、CLI から `restore` コマンドを使用します。

始める前に

プライマリ PAN の自動フェールオーバー設定が展開でイネーブルになっている場合はオフにします。設定バックアップを復元すると、アプリケーションサーバプロセスが再起動されます。これらのサービスが再起動されるまで遅延が発生する場合があります。このサービスの再起動の遅延により、セカンダリ PAN の自動フェールオーバーが開始される場合があります。

-
- ステップ 1** [管理 (Administration)] > [システム (System)] > [バックアップ/復元 (Backup and Restore)] を選択します。
- ステップ 2** バックアップの名前を設定バックアップのリストから選択し、[復元 (Restore)] をクリックします。
- ステップ 3** バックアップ時に使用した暗号キーを入力します。
- ステップ 4** [復元 (Restore)] をクリックします。
-

次のタスク

Cisco ISE CA サービスを使用する場合は、次のことを実行する必要があります。

1. Cisco ISE CA ルート チェーン全体を再生成します。
2. Cisco ISE CA 証明書およびキーのバックアップをプライマリ PAN から取得し、セカンダリ PAN で復元します。これにより、プライマリ PAN の障害が発生した場合に、セカンダリ PAN が外部 PKI のルート CA または下位 CA として機能するようになり、セカンダリ PAN をプライマリ PAN に昇格させることができます。

関連トピック

[CLI からの設定またはモニタリング \(操作\) バックアップの復元 \(338 ページ\)](#)

モニタリング データベースの復元

モニタリングデータベースを復元するプロセスは、展開のタイプによって異なります。次の項では、スタンドアロンおよび分散展開でモニタリングデータベースを復元する方法について説明します。

Cisco ISE の以前のリリースからのオンデマンド モニタリング データベースのバックアップを復元するには、CLI を使用する必要があります。Cisco ISE リリース間でのスケジュール バックアップの復元はサポートされていません。



- (注) データが取得されたノードとは別のノードにデータを復元しようとする場合、新しいノードを指すロギングターゲット設定を設定する必要があります。これにより、モニタリング syslog が正しいノードに送信されるようになります。

関連トピック

[スタンドアロン環境でのモニタリング（運用）バックアップの復元](#) (342 ページ)

[管理およびモニタリングペルソナによるモニタリングバックアップの復元](#) (342 ページ)

[モニタリングペルソナによるモニタリングバックアップの復元](#) (343 ページ)

スタンドアロン環境でのモニタリング（運用）バックアップの復元

GUIには現在のリリースから取得されたバックアップのみが表示されます。前のリリースから取得されたバックアップを復元するには、CLI から `restore` コマンドを使用します。

始める前に

- 古いモニタリング データを消去します。
- バックアップをスケジュールするか、オンデマンドバックアップを実行します。

ステップ 1 [管理 (Administration)] > [システム (System)] > [バックアップ/復元 (Backup and Restore)] を選択します。

ステップ 2 バックアップの名前を操作バックアップのリストから選択し、[復元 (Restore)] をクリックします。

ステップ 3 バックアップ時に使用した暗号キーを入力します。

ステップ 4 [復元 (Restore)] をクリックします。

関連トピック

[バックアップのスケジュール](#) (334 ページ)

[オンデマンドバックアップの実行](#) (332 ページ)

[CLI からの設定またはモニタリング（操作）バックアップの復元](#) (338 ページ)

[管理およびモニタリングペルソナによるモニタリングバックアップの復元](#) (342 ページ)

[モニタリングペルソナによるモニタリングバックアップの復元](#) (343 ページ)

管理およびモニタリングペルソナによるモニタリングバックアップの復元

管理およびモニタリングペルソナを使用して、分散環境でのモニタリングバックアップを復元することができます。

始める前に

- 古いモニタリング データを消去します。

- バックアップをスケジュールするか、オンデマンド バックアップを実行します。

ステップ 1 別の Cisco ISE ノードを PAN として昇格する準備を行います。そのためには、このノードを、バックアップする既存のプライマリ ノードと同期します。

これにより、プロモートする Cisco ISE ノードの設定は最新になります。

ステップ 2 新しく同期した管理ノードをプライマリ ステータスに昇格します。

ステップ 3 バックアップされるノードを登録解除する準備を行います。そのためには、モニタリング ペルソナを展開内の別のノードに割り当てます。

展開内に、機能中のモニタリング ノードが少なくとも 1 つ必要です。

ステップ 4 バックアップされるノードを登録解除します。

ステップ 5 新しく登録解除されたノードにモニタリング バックアップを復元します。

ステップ 6 現在の管理ノードにより新たに復元されたノードを登録します。

ステップ 7 新たに復元されて登録されたノードを PAN に昇格します。

関連トピック

[バックアップのスケジュール](#) (334 ページ)

[オンデマンド バックアップの実行](#) (332 ページ)

[分散環境でのプライマリ ノードとセカンダリ ノードの同期](#) (345 ページ)

[スタンドアロン環境でのモニタリング \(運用\) バックアップの復元](#) (342 ページ)

[モニタリング ペルソナによるモニタリング バックアップの復元](#) (343 ページ)

モニタリング ペルソナによるモニタリング バックアップの復元

分散環境のモニタリング バックアップは、モニタリング ペルソナによってのみ復元できます。

始める前に

- 古いモニタリング データを消去します。
- バックアップをスケジュールするか、オンデマンド バックアップを実行します。

ステップ 1 復元されるノードを登録解除する準備を行います。そのためには、モニタリング ペルソナを展開内の別のノードに割り当てます。

展開内に、機能中のモニタリング ノードが少なくとも 1 つ必要です。

ステップ 2 復元されるノードを登録解除します。

(注) 登録解除が完了するのを待機してから、復元に進みます。復元を続行する前に、ノードがスタンバイ状態になっている必要があります。

ステップ 3 新しく登録解除されたノードにモニタリングバックアップを復元します。

ステップ 4 現在の管理ノードにより新たに復元されたノードを登録します。

ステップ 5 新たに復元されて登録されたノードを PAN に昇格します。

関連トピック

[スタンドアロン環境でのモニタリング（運用）バックアップの復元（342 ページ）](#)

[管理およびモニタリングペルソナによるモニタリングバックアップの復元（342 ページ）](#)

復元履歴

操作監査レポートからは、すべての復元操作、ログイベント、ステータスに関する情報を取得することができます。



(注) ただし操作監査レポートには、前回の復元操作に対応する開始時間に関する情報はありません。

トラブルシューティング情報を入手するには、Cisco ISE CLI から **backup-logs** コマンドを実行して、ADE.log ファイルを調べる必要があります。

復元操作の進行中は、すべての Cisco ISE サービスは停止します。**show restore status** CLI コマンドを使用して、復元操作の進行状況を確認できます。

認証および許可ポリシー設定のエクスポート

認証および許可ポリシー設定を XML ファイルの形式でエクスポートし、これをオフラインで読み取って設定エラーを特定し、トラブルシューティングのために使用できます。この XML ファイルには認証および許可ポリシールール、単純および複合ポリシー条件、dACL、および許可プロファイルが含まれます。XML ファイルを電子メールで送信するか、ローカルシステムに保存することを選択できます。

ステップ 1 [管理（Administration）] > [システム（System）] > [バックアップ/復元（Backup & Restore）] を選択します。

ステップ 2 [ポリシーのエクスポート（Policy Export）] をクリックします。

ステップ 3 必要に応じて値を入力します。

ステップ 4 [エクスポート（Export）] をクリックします。

XML ファイルの内容を表示するには、ワードパッドなどのテキストエディタを使用します。

分散環境でのプライマリノードとセカンダリノードの同期

分散環境では、PAN のバックアップ ファイルの復元後に、プライマリおよびセカンダリ ノードの Cisco ISE データベースが自動的に同期されないことがあります。この場合には、PAN からセカンダリ ISE ノードへの完全複製を手動で強制実行できます。強制同期は、PAN からセカンダリ ノードにのみ可能です。同期操作中は、設定を変更することはできません。Cisco ISE では、同期が完全に完了した後のみ、他の Cisco ISE 管理者ポータル ページに移動して設定変更を行うことができます。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

-
- ステップ 1 [管理 (Administration)] > [システム (System)] > [展開 (Deployment)] を選択します。
 - ステップ 2 非同期レプリケーション ステータスのセカンダリ ISE ノードの横にあるチェックボックスをオンにします。
 - ステップ 3 [同期を更新 (Syncup)] をクリックし、ノードが PAN と同期されるまで待ちます。Cisco ISE 管理者ポータルへのアクセスは、このプロセスが完了するのを待たなければなりません。
-

スタンドアロンおよび分散展開での失われたノードの復元

この項では、スタンドアロンおよび分散展開での失われたノードの復元に使用できるトラブルシューティング情報を提供します。次の使用例の一部では、失われたデータの復旧にバックアップと復元機能を使用し、その他の使用例では、複製機能を使用しています。

分散展開での既存 IP アドレスとホスト名を使用しての失われたノードの復元

シナリオ

分散展開では、自然災害が全ノードの損失につながります。復元後に、既存 IP アドレスとホストネームを使用します。

たとえば、2 つのノード、N1 (プライマリ ポリシー管理ノードすなわちプライマリ PAN) と N2 (セカンダリ ポリシー管理ノードすなわちセカンダリ PAN) があります。時刻 T1 に取得

された N1 ノードのバックアップが利用可能です。自然災害のために、N1 と N2 両方のノードに障害が発生しました。

前提

展開内のすべての Cisco ISE ノードが破壊されました同じホスト名と IP アドレスを使用して、新しいハードウェアのイメージが作成されました。

解決手順 (Resolution Steps)

1. N1 および N2 ノードの両方を置き換える必要があります。N1 および N2 ノードはスタンダアロン構成になりました。
2. N1 と N2 のノードの UDI を使用してライセンスを取得し、N1 ノードにインストールします。
3. 置き換えた N1 ノードでバックアップを復元する必要があります。復元スクリプトは N2 にデータを同期しようとしませんが、N2 はスタンダアロン ノードであるため同期は失敗します。N1 のデータは時刻 T1 にリセットされます。
4. N1 の管理者ポータルにログインして、N2 ノードを削除して再登録する必要があります。これで、N1 および N2 ノードのデータが時刻 T1 にリセットされます。

関連トピック

[CLI からの設定またはモニタリング \(操作\) バックアップの復元](#) (338 ページ)

分散展開の新 IP アドレスとホスト名を使用しての失われたノードの復元

シナリオ

分散展開では、自然災害が全ノードの損失につながります。新しいハードウェアのイメージが新しい場所で再作成され、新しい IP アドレスとホスト名が必要です。

たとえば、2 つの ISE ノード N1 (プライマリ ポリシー管理ノード (プライマリ PAN)) と N2 (セカンダリ ポリシー サービス ノード) があります。時刻 T1 に取得された N1 ノードのバックアップが利用可能です。自然災害のために、N1 と N2 両方のノードに障害が発生しました。Cisco ISE ノードが新しいロケーションで置き換えられ、新しいホスト名は N1A (プライマリ PAN) および N2A (セカンダリ ポリシー サービス ノード) です。N1A および N2A はこの時点ではスタンダアロン ノードです。

前提条件

展開内のすべての Cisco ISE ノードが破壊されました新しいハードウェアのイメージが、異なるホスト名と IP アドレスを使用して異なる場所で作成されました。

解決手順 (Resolution Steps)

1. N1 のバックアップを入手し、これを N1A 上で復元します。復元スクリプトは、ホスト名とドメイン名の変更を認識し、現在のホスト名に基づいて展開設定内のホスト名とドメイン名を更新します。
2. 新しい自己署名証明書を生成する必要があります。
3. N1A で Cisco ISE 管理者ポータルにログインし、**[管理 (Administration)] > [システム (System)] > [展開 (Deployment)]** を選択して、次の操作を行う必要があります。

古い N2 ノードを削除します。

新しい N2A ノードをセカンダリ ノードとして登録します。N1A ノードのデータが N2A ノードに複製されます。

関連トピック

[CLI からの設定またはモニタリング \(操作\) バックアップの復元 \(338 ページ\)](#)

スタンドアロン展開の既存 IP アドレスとホスト名によるノードの復元

シナリオ

スタンドアロン管理ノードがダウンします。

たとえば、スタンドアロン管理ノード N1 があったとします。N1 データベースのバックアップは、時刻 T1 に取得されました。物理的な障害により N1 ノードがダウンし、イメージの再作成または新しいハードウェアが必要です。N1 ノードを、同じ IP アドレスとホスト名を使用して回復させる必要があります。

前提条件

この展開はスタンドアロン展開であり、新規またはイメージを再作成したハードウェアは、同じ IP アドレスとホスト名を持ちます。

解決手順 (Resolution Steps)

イメージの再作成後、または同一 IP アドレスとホスト名で新しい Cisco ISE ノードを導入した後に N1 ノードが起動したら、古い N1 ノードから取得したバックアップを復元する必要があります。ロールを変更する必要はありません。

関連トピック

[CLI からの設定またはモニタリング \(操作\) バックアップの復元 \(338 ページ\)](#)

スタンドアロン展開の新 IP アドレスとホスト名によるノードの復元

シナリオ

スタンドアロン管理ノードがダウンします。

たとえば、スタンドアロン管理ノード N1 があったとします。時刻 T1 に取得された N1 データベースのバックアップが利用可能です。物理的な障害により N1 ノードがダウンし、異なる IP アドレスとホスト名を使用した新しいハードウェアに別のロケーションで置き換えられます。

前提条件

これはスタンドアロン展開であり、置き換えられたハードウェアは、異なる IP アドレスとホスト名を持ちます。

解決手順 (Resolution Steps)

1. 新しいハードウェアで N1 ノードを置き換えます。このノードはスタンドアロン状態となり、ホスト名は N1B です。
2. バックアップを N1B ノード上で復元できます。ロールを変更する必要はありません。

関連トピック

[CLI からの設定またはモニタリング \(操作\) バックアップの復元](#) (338 ページ)

設定のロールバック

問題

意図せずに設定を変更してしまい、後でそれが正しくないことがわかる場合があります。たとえば、いくつかの NAD を削除したり、一部の RADIUS 属性を誤って修正したりして、数時間後にこの問題に気付く場合があります。この場合、変更を行う前に取得したバックアップを復元することにより、元の設定に戻すことができます。

考えられる原因

N1 (プライマリ ポリシー管理ノードすなわちプライマリ PAN) と N2 (セカンダリ ポリシー管理ノードすなわちセカンダリ PAN) の 2 つのノードがあり、N1 ノードのバックアップを使用できます。N1 上で誤った変更をいくつか行い、変更を元に戻す必要があります。

ソリューション

誤った設定変更を行う前に取得した N1 ノードのバックアップを入手します。N1 ノード上でこのバックアップを復元します。復元スクリプトにより、N1 のデータで N2 が同期されます。

関連トピック

[CLI からの設定またはモニタリング \(操作\) バックアップの復元](#) (338 ページ)

分散展開での障害発生時のプライマリ ノードの復元

シナリオ

マルチノード展開内で、PAN に障害が発生しました。

たとえば、2 つの Cisco ISE ノード、N1 (PAN) と N2 (セカンダリ管理ノード) があります。ハードウェアの問題で N1 に障害が発生します。

前提条件

分散展開内のプライマリ ノードのみに障害が発生します。

解決手順 (Resolution Steps)

1. N2 管理者ポータルにログインします。[管理 (Administration)] > [システム (System)] > [展開 (Deployment)] を選択して、N2 をプライマリ ノードとして設定します。

N1 ノードが新しいハードウェアで置き換えられ、イメージが再作成され、スタンドアロン状態となります。

2. N2 管理者ポータルで、セカンダリ ノードとして新しい N1 ノードを登録します。

これで、N2 ノードがプライマリ ノードになり、N1 ノードがセカンダリ ノードになります。

N1 ノードを再びプライマリ ノードにするには、N1 の管理者ポータルにログインして、このノードをプライマリ ノードに設定します。N2 は、自動的にセカンダリ サーバとなります。データが失われることはありません。

分散展開での障害発生時のセカンダリ ノードの復元

シナリオ

マルチノード展開で、1 台のセカンダリ ノードに障害が発生しました。復元の必要はありません。

たとえば、N1 (プライマリ PAN)、N2 (セカンダリ PAN)、N3 (セカンダリ ポリシー サービス ノード)、N4 (セカンダリ ポリシー サービス ノード) の複数のノードが存在します。セカンダリ ノードの 1 つである N3 に障害が発生しました。

解決手順 (Resolution Steps)

1. 新しい N3A ノードのイメージを再作成して、デフォルトのスタンドアロン状態にします。
2. N1 の管理者ポータルにログインし、N3 ノードを削除します。
3. N3A ノードを登録します。

N1 から N3A へ、データが複製されます。復元の必要はありません。



第 14 章

適応型ネットワーク制御のセットアップ

- [Cisco ISE での適応型ネットワーク制御の有効化 \(351 ページ\)](#)
- [ネットワーク アクセスの設定 \(351 ページ\)](#)
- [適応型ネットワーク制御 \(353 ページ\)](#)
- [ANC 隔離と隔離解除フロー \(356 ページ\)](#)
- [ANC NAS ポートのシャットダウンフロー \(357 ページ\)](#)
- [エンドポイントの消去の設定 \(357 ページ\)](#)

Cisco ISE での適応型ネットワーク制御の有効化

適応型ネットワーク制御（ANC）はデフォルトでは無効になっています。pxGridが有効にされた場合にのみ有効になり、管理者ポータルでサービスを手動で無効にするまで有効のままになります。

関連トピック

[ネットワーク アクセスの設定 \(351 ページ\)](#)

ネットワーク アクセスの設定

適応型ネットワーク制御（ANC）によって、ネットワーク アクセス ステータスをリセットして、ポートを隔離、隔離解除、またはシャットダウンすることができます。これにより、ネットワーク アクセス ステータスに応じたネットワークへの許可が定義されます。

エンドポイントの隔離や隔離解除、またはエンドポイントが接続されているネットワーク アクセス サーバ（NAS）ポートのシャットダウンを行うには、エンドポイントの IP アドレスまたは MAC アドレスを使用します。同時に実行しない限り、同じエンドポイントに複数回、隔離操作および隔離解除操作を実行できます。ネットワーク上に悪意のあるエンドポイントを見つけた場合は、ANC を使用してそのエンドポイントのアクセスをシャットダウンし、NAS ポートを閉じることができます。

ANC ポリシーをエンドポイントに割り当てるには、次の手順を実行します。

始める前に

- ANC を有効にする必要があります。
- ANC の許可プロファイルおよび例外タイプの許可ポリシーを作成する必要があります。

ステップ 1 [操作 (Operations)] > [適応型ネットワーク制御 (Adaptive Network Control)] > [ポリシーリスト (Policy List)] の順に選択します。

ステップ 2 [追加 (Add)] をクリックします。

ステップ 3 ANC ポリシーの名前を入力し、ANC アクションを指定します。次のオプションを使用できます。

- 検疫 (Quarantine)
- シャットダウン (Shut_Down)
- ポートバウンス (Port_Bounce)

1 つまたは複数のアクションを選択できますが、[シャットダウン (Shut_Down)] および [ポートバウンス (Port_Bounce)] を他の ANC アクションと組み合わせることはできません。

ステップ 4 [ポリシー (Policy)] > [承認 (Authorization)] の順に選択し、ANCPolicy 属性を使用して ANC ポリシーを対応する許可ポリシーに関連付けます。

ステップ 5 [操作 (Operations)] > [適応型ネットワーク制御 (Adaptive Network Control)] > [エンドポイント割り当て (Endpoint Assignment)] の順に選択します。

ステップ 6 [追加 (Add)] をクリックします。

ステップ 7 エンドポイントの IP アドレスまたは MAC アドレスを入力し、[ポリシー割り当て (Policy Assignment)] ドロップダウン リストからポリシーを選択します。

ステップ 8 [送信 (Submit)] をクリックします。

関連トピック

[隔離済みエンドポイントがポリシー変更の後に認証を更新しない](#) (352 ページ)

隔離済みエンドポイントがポリシー変更の後に認証を更新しない

問題

ポリシー変更または ID の追加後に認証が失敗し、再認証が行われません。認証が失敗するか、問題のエンドポイントがネットワークに接続できなくなります。この問題は、ユーザロールに割り当てられるポスチャ ポリシーごとのポスチャ評価に失敗するクライアント マシンで頻繁に発生します。

考えられる原因

クライアントマシンで認証タイマーが正しく設定されていないか、またはスイッチ上で認証間隔が正しく設定されていません。

ソリューション

この問題には、解決策がいくつか考えられます。

1. Cisco ISE で、指定された NAD またはスイッチの **Session Status Summary** レポートを検査し、インターフェイスに適切な認証間隔が設定されていることを確認します。
2. NAD/スイッチ上で "show running configuration" と入力し、適切な「authentication timer restart」設定でインターフェイスが設定されていることを確認します（たとえば、「authentication timer restart 15」および「authentication timer reauthenticate 15」）。
3. NAD/スイッチ上で "interface shutdown" および "no shutdown" と入力してポートをバウンスし、Cisco ISE で変更があったと考えられる場合には再認証を適用します。



(注) CoA は MAC アドレスまたはセッション ID を必要とするので、Network Device SNMP レポートに表示されるポートをバウンスしないように推奨しています。

適応型ネットワーク制御

適応型ネットワーク制御（ANC）は、管理ノードで実行されるサービスで、エンドポイントのネットワークアクセスのモニタリングと制御に使用できます。ANC は、ISE 管理者が管理 GUI で呼び出すことも、サードパーティ システムから pxGrid を介して呼び出すこともできます。ANC は有線展開とワイヤレス展開をサポートし、Plus ライセンスが必要です。

ANC を使用すると、システムの許可ポリシー全体を変更することなく許可状態を変更できます。ANC を使用すると、EPSSStatus を確認してネットワークアクセスを制限または拒否するように許可ポリシーが定義されている場合、確立された許可ポリシーの結果としてエンドポイントを隔離するときの許可状態を設定することができます。エンドポイントを隔離解除して、フル ネットワーク アクセスを可能にできます。ネットワークからエンドポイントを接続解除する Network Attached System（NAS）上のポートをシャットダウンすることもできます。

一度に隔離できるユーザの数に制限はなく、また隔離期間の長さにも制限はありません。

ANCによってネットワークアクセスをモニタおよび制御するには、次の操作を実行できます。

- **隔離**：例外ポリシー（許可ポリシー）を使用して、ネットワークへのエンドポイントアクセスを制限または拒否することができます。EPSSStatus に応じて異なる許可プロファイル（権限）を割り当てるために、例外ポリシーを作成する必要があります。隔離状態に設定すると、基本的に、デフォルトの VLAN から指定した隔離 VLAN にエンドポイントが移動します。エンドポイントと同じ NAS でサポートされる隔離 VLAN を事前に定義する必要があります。
- **隔離解除**：エンドポイントのネットワークへのフルアクセスを許可し、エンドポイントを元の VLAN に戻す隔離ステータスを反転することができます。
- **シャットダウン**：NAS上のポートを非アクティブ化し、ネットワークからエンドポイントを接続解除することができます。エンドポイントが接続されている NAS 上のポートが

シャットダウンされた後、エンドポイントがネットワークに接続できるようにするには、NAS上のポートを手動で再度リセットする必要があります。このことは無線展開では実行できません。

アクティブ エンドポイントに対する隔離および隔離解除操作は、セッション ディレクトリ レポートからトリガーできます。



(注) 隔離されていたセッションが隔離解除された場合、新たに隔離解除されたセッションの開始方法は、スイッチ設定で指定されている認証方法によって決まります。

関連トピック

[ANC によるネットワーク アクセスの許可プロファイルの作成](#) (354 ページ)

[ANC 操作は IP アドレスまたは MAC アドレスが見つからない場合に失敗する](#) (355 ページ)

[外部認証された管理者が ANC 操作を実行できない](#) (355 ページ)

[ANC によるネットワーク アクセスの例外ポリシーの作成](#) (354 ページ)

ANC によるネットワーク アクセスの許可プロファイルの作成

ANC に使用する許可プロファイルを作成する必要があります。許可プロファイルは、標準許可プロファイルのリストに表示されます。エンドポイントはネットワークで認証および許可されますが、ネットワークへのアクセスが制限されています。

- ステップ 1 [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [許可 (Authorization)] > [許可プロファイル (Authorization Profiles)] を選択します。
- ステップ 2 [追加 (Add)] をクリックします。
- ステップ 3 許可プロファイルの一意の名前と説明を入力し、[アクセス タイプ (Access Type)] は [ACCESS_ACCEPT] のままにします。
- ステップ 4 [DACL 名 (DACL Name)] チェックボックスをオンにし、ドロップダウンリストから [DENY_ALL_TRAFFIC] を選択します。
- ステップ 5 [送信 (Submit)] をクリックします。

ANC によるネットワーク アクセスの例外ポリシーの作成

ANC 許可用に、すべての標準許可ポリシーの前に処理される隔離例外ポリシーを作成する必要があります。例外許可ポリシーは、特別な条件や権限、または緊急の要件を満たすために制限付きアクセスを許可することを目的としています。標準許可ポリシーは変更しないようにし、権限の共通セットを共有するユーザ、デバイス、グループの大規模なグループに適用します。

始める前に

ANC とともに使用できるように標準許可プロファイルを正常に作成しておく必要があります。

-
- ステップ 1 [ポリシー (Policy)] > [許可 (Authorization)] を選択し、[例外 (Exceptions)] を展開します。
 - ステップ 2 [有効 (Enabled)] または [無効 (Disabled)] または [モニタのみ (Monitor Only)] オプションを選択します。
 - ステップ 3 [新しいルールの作成 (Create a New Rule)] をクリックします。
 - ステップ 4 例外ルール名を入力します。
 - ステップ 5 プラス (+) 記号をクリックして、ID グループを選択します。
 - ステップ 6 プラス (+) 記号をクリックして、[新しい条件の作成 (高度なオプション) (Create New Condition (Advanced Option))] を選択します。
 - ステップ 7 最初のフィールドの下向き矢印アイコンをクリックして、ディクショナリリストを表示し、[セッション (Session)] > [EPSSStatus] を選択します。
 - ステップ 8 2 番目のフィールドのドロップダウン リストから [等しい (Equals)] を選択します。
 - ステップ 9 3 番目のフィールドのドロップダウン リストから [隔離 (Quarantine)] を選択します。
 - ステップ 10 [保存 (Save)] をクリックします。
-

ANC 操作は IP アドレスまたは MAC アドレスが見つからない場合に失敗する

エンドポイントで実行する ANC 操作は、そのエンドポイントのアクティブなセッションに IP アドレスに関する情報が含まれていない場合に失敗します。このことは、そのエンドポイントの MAC アドレスおよびセッション ID にも適用されます。



- (注) ANC を介してエンドポイントの許可状態を変更する場合は、エンドポイントの IP アドレスまたは MAC アドレスを指定する必要があります。IP アドレスまたは MAC アドレスがエンドポイントのアクティブなセッションで見つからない場合、「この MAC アドレス、IP アドレスまたはセッション ID のアクティブなセッションが見つかりません。(No active session found for this MAC address, IP Address or Session ID.)」というエラー メッセージが表示されます。
-

外部認証された管理者が ANC 操作を実行できない

外部認証された管理者がライブセッションから CoA 隔離を発行しようとする、Cisco ISE は次のエラー メッセージを返します。

「xx: xx: xx: xx: xx: xx に対する隔離の CoA アクションを開始できません。(CoA Action of Quarantine for xx:xx:xx:xx:xx:xx can not be initiated.) 原因: 内部でユーザが見つかりません。」

(Cause:User not found internally.) サポートされていない外部認証されたユーザを使用している可能性があります (Possible use of unsupported externally authenticated user) 」

外部認証された管理者が、エンドポイントの IP アドレスまたは MAC アドレスを使用して、Cisco ISE 管理者ポータル内の [操作 (Operations)] > [適応型ネットワーク制御 (Adaptive Network Control)] から ANC 操作を実行すると、Cisco ISE は次のエラー メッセージを返します。

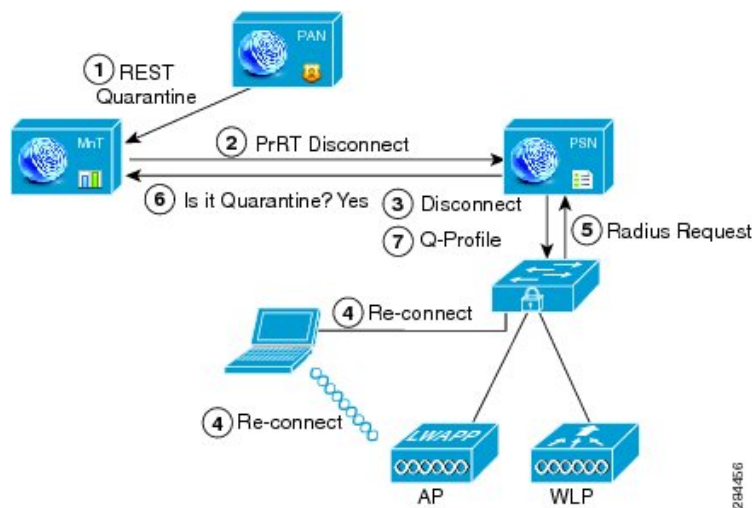
「サーバ障害：内部でユーザが見つかりません。(Server failure: User not found internally.) サポートされていない外部認証されたユーザを使用している可能性があります (Possible use of unsupported externally authenticated user) 」

ANC 隔離と隔離解除フロー

選択したエンドポイントのネットワークへのアクセスを制限するために、ANC を使用してこれらを隔離できます。エンドポイントを隔離し、ステータスに応じて異なる許可プロファイルを割り当てる例外許可ポリシーを確立できます。許可プロファイルは許可ポリシーで定義される権限のコンテナとして機能し、許可ポリシーによって特定のネットワーク サービスへのアクセスが許可されます。許可が完了すると、ネットワークアクセス要求に権限が付与されます。エンドポイントの妥当性が認められた場合には、エンドポイントの隔離を解除してネットワークへのフルアクセスを許可できます。

この図は、隔離フローを示しています。許可ルールが設定され、ANC セッションが確立されていることを前提としています。

図 20: ANC 隔離フロー



1. クライアントデバイスがワイヤレス デバイス (WLC) を通じてネットワークにログインし、隔離の REST API コールが管理 ノード (PAP) からモニタリング ノード (MnT) に発行されます。
2. 続いて、モニタリング ノードは、ポリシー サービス ISE ノード (PDP) を通じて PrRT をコールし、CoA を呼び出します。

3. クライアント デバイスが切断されます。
4. 続いて、クライアント デバイスが再認証および再接続されます。
5. クライアント デバイスに対する RADIUS 要求が、モニタリング ノードに返送されます。
6. チェックが行われている間、クライアント デバイスは隔離されます。
7. Q プロファイル許可ポリシーが適用され、クライアント デバイスの妥当性が確認されます。
8. クライアント デバイスの隔離が解除され、ネットワークにフル アクセスできるようになります。

ANC NAS ポートのシャットダウン フロー

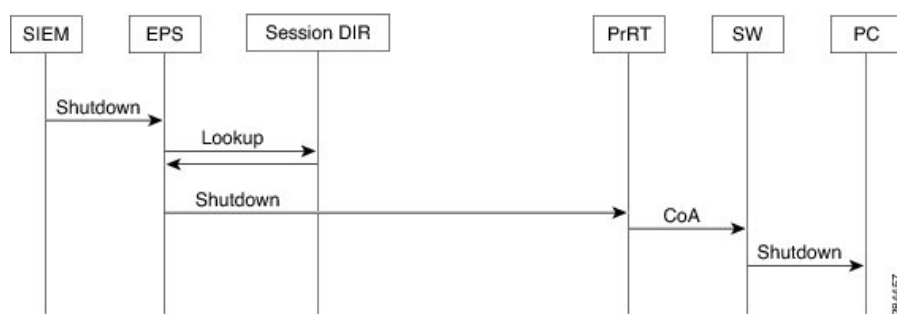
エンドポイントの IP アドレスまたは MAC アドレスを使用して、エンドポイントの接続先 NAS ポートをシャットダウンできます。

シャットダウンでは、MAC アドレスに対して指定された IP アドレスに基づいて NAS ポートを閉じることが可能です。また、手動でポートを復元して、エンドポイントをネットワークに戻す必要があります。これは、有線メディアで接続されたエンドポイントのみに有効です。

シャットダウンはすべてのデバイスでサポートされているわけではありません。ただし、大部分のスイッチでシャットダウン コマンドがサポートされています。getResult() コマンドを使用すると、シャットダウンが正常に実行されたかどうかを確認できます。

この図は、ANC のシャットダウンのフローを示しています。図のクライアント デバイスでは、このクライアント デバイスがネットワークにアクセスするために使用する NAS でシャットダウン操作が実行されます。

図 21: ANC のシャットダウン フロー



エンドポイントの消去の設定

[管理 (Administration)] > [ID の管理 (Identity Management)] > [設定 (Settings)] > [エンドポイント消去 (Endpoint Purge)] を使用して、ID グループおよび他の条件に基づいて、設定ルールによってエンドポイント パージ ポリシーを定義できます。指定したエンドポイントを

消去しないことや、選択したプロファイリング条件に基づいてエンドポイントを消去することを選択できます。

エンドポイント消去ジョブをスケジュールできます。このエンドポイント消去スケジュールはデフォルトで有効です。Cisco ISE はデフォルトで、30 日よりも古い登録デバイスとエンドポイントを削除します。消去ジョブは、プライマリ PAN で設定された時間帯に基づいて毎日午前 1 時に実行されます。

次に、エンドポイントの消去に使用できる条件と例の一部を示します。

- **InactivityDays** : エンドポイントでの最後のプロファイリングアクティビティまたは更新からの日数。
 - この条件によって、時間の経過に伴って蓄積した古いデバイス（一般的には一時的なゲストやパーソナルデバイス）、または廃止されたデバイスが消去されます。これらのエンドポイントは、ネットワーク上でアクティブでないか、近い将来に使用される可能性が低いと見なされるため、ほとんどの展開でノイズを表す傾向があります。それらが再度接続した場合は、必要に応じて再検出、プロファイリング、登録などが行われます。
 - エンドポイントから更新が発生すると、**InactivityDays** はプロファイリングが有効である場合にのみ 0 にリセットされます。
- **ElapsedDays** : オブジェクトが作成されてからの日数。
 - この条件は、ゲストまたは請負業者のエンドポイント、ネットワーク アクセスに **WebAuth** を利用する従業員などの、未認証アクセスまたは条件付きアクセスが一定期間認められたエンドポイントに使用できます。許可された接続猶予期間が経過した後、それらは完全に再認証および登録される必要があります。
- **PurgeDate** : エンドポイントを消去する日付。
 - このオプションは、作成または開始時間に関係なく一定期間のアクセスを許可する、特別なイベントやグループに使用できます。このオプションでは、すべてのエンドポイントを同時に消去できます。たとえば、展示会、会議、または毎週メンバーが入れ替わる週ごとのトレーニングクラスでは、絶対的な日/週/月ではなく、特定の週や月にアクセスを許可する場合に使用します。



第 **IV** 部

ユーザおよびエンドユーザ ポータルの管理

- [ユーザおよび外部 ID ソースの管理 \(361 ページ\)](#)
- [ゲスト アクセスの設定 \(521 ページ\)](#)
- [デバイス アクセスのサポート \(583 ページ\)](#)
- [エンドユーザ Web ポータルのカスタマイズ \(613 ページ\)](#)



第 15 章

ユーザおよび外部 ID ソースの管理

- [Cisco ISE ユーザ](#) (361 ページ)
- [内部 ID ソースと外部 ID ソース](#) (374 ページ)
- [証明書認証プロファイル](#) (378 ページ)
- [外部 ID ソースとしての Active Directory](#) (379 ページ)
- [Active Directory で Easy Connect および パッシブ ID サービス をサポートするための要件](#) (406 ページ)
- [Easy Connect](#) (417 ページ)
- [PassiveID ワーク センター](#) (423 ページ)
- [LDAP](#) (482 ページ)
- [ODBC ID ソース](#) (491 ページ)
- [RADIUS トークン ID ソース](#) (499 ページ)
- [RSA ID ソース](#) (504 ページ)
- [外部 ID ソースとしての SAMLv2 ID プロバイダ](#) (511 ページ)
- [ID ソース順序](#) (517 ページ)
- [レポートでの ID ソースの詳細](#) (518 ページ)

Cisco ISE ユーザ

この章では、ユーザという用語はネットワークに定期的にアクセスする従業員と請負業者に加え、スポンサーおよびゲストユーザを意味します。スポンサーは、スポンサー ポータルからゲストユーザ アカウントを作成および管理する組織の従業員または請負業者となります。ゲストユーザは、一定期間組織のネットワーク リソースへのアクセスを必要とする外部ビジターです。

Cisco ISE ネットワーク上のリソースとサービスにアクセスするすべてのユーザのアカウントを作成する必要があります。従業員、請負業者、およびスポンサーユーザは、管理者ポータルから作成されます。

ユーザ ID

ユーザ ID は、ユーザに関する情報を保持するコンテナに似ており、ユーザのネットワーク アクセス クレデンシャルを形成します。各ユーザの ID はデータにより定義され、ユーザ名、電子メール アドレス、パスワード、アカウントの説明、関連付けられている管理者グループ、ユーザ グループ、ロールなどが含まれます。

ユーザ グループ

ユーザ グループは、特定の一連の Cisco ISE サービスおよび機能へのアクセスを許可する共通の権限セットを共有する個々のユーザの集合です。

ユーザ ID グループ

ユーザのグループ ID は、同じグループに属している特定のユーザ グループを識別および説明する要素で構成されています。グループ名は、このグループのメンバーが持っている機能ロールの説明です。グループは、そのグループに属しているユーザのリストです。

デフォルト ユーザ ID グループ

Cisco ISE には、次の事前定義されたユーザ ID グループが用意されています。

- 従業員：組織の従業員はこのグループに所属します。
- SponsorAllAccount：Cisco ISE ネットワークのすべてのゲスト アカウントを一時停止または復元できるスポンサー ユーザ。
- SponsorGroupAccounts：同じスポンサー ユーザ グループのスポンサー ユーザが作成したゲスト アカウントを一時停止できるスポンサー ユーザ。
- SponsorOwnAccounts：自身が作成したゲスト アカウントのみを一時停止できるスポンサー ユーザ。
- ゲスト：ネットワークのリソースへの一時的なアクセスを必要とする訪問者。
- ActivatedGuest：アカウントが有効で、アクティブになっているゲスト ユーザ。

ユーザ ロール

ユーザ ロールは、ユーザが Cisco ISE ネットワークで実行できるタスクやアクセスできるサービスを決定する権限セットです。ユーザ ロールは、ユーザ グループに関連付けられています（ネットワーク アクセス ユーザなど）。

ユーザ アカウントのカスタム属性およびパスワード ポリシー

Cisco ISE では、ユーザ属性に基づいてユーザのネットワーク アクセスを制限することができます。Cisco ISE では、一連の事前定義されたユーザ属性が用意されており、カスタム属性を作成することもできます。両方のタイプの属性が認証ポリシーを定義する条件で使用できます。パスワードが指定された基準を満たすように、ユーザ アカウントのパスワード ポリシーも定義できます。

カスタム ユーザ属性

[ユーザのカスタム属性 (User Custom Attributes)] ページ ([管理 (Administration)] > [ID の管理 (Identity Management)] > [設定 (Settings)] > [ユーザのカスタム属性 (User Custom Attributes)]) で、追加のユーザ アカウント属性を設定できます。このページに事前定義済みユーザ属性のリストを表示することもできます。事前定義済みユーザ属性を編集することはできません。

新しいカスタム属性を追加するには、[ユーザのカスタム属性 (User Custom Attributes)] ページに必要な詳細を入力します。[ユーザのカスタム属性 (User Custom Attributes)] ページに追加するカスタム属性とデフォルト値が、ネットワークアクセスユーザ ([管理 (Administration)] > [ID の管理 (Identity Management)] > [ID (Identities)] > [ユーザ (Users)] > [追加 (Add)]/[編集 (Edit)]) または管理者ユーザ ([管理 (Administration)] > [システム (System)] > [管理者アクセス (Admin Access)] > [管理者 (Administrators)] > [管理者ユーザ (Admin Users)] > [追加 (Add)]/[編集 (Edit)]) の追加または編集時に表示されます。これらのデフォルト値は、ネットワーク アクセスまたは管理者ユーザの追加または編集時に変更できます。

ユーザが [ユーザのカスタム属性 (User Custom Attributes)] ページで、カスタム属性に対し次のデータ型を選択できます。

- [文字列 (String)] : 文字列の最大長 (文字列属性値の最大許容長) を指定できます。
- [整数 (Integer)] : 最小値と最大値を設定できます (最小、最大の許容可能な整数値を指定します) 。
- [列挙 (Enum)] : 各パラメータに次の値を指定できます。
 - 内部値
 - 表示値

デフォルト パラメータを指定することもできます。ネットワーク アクセスまたは管理者ユーザの追加または編集時に、[表示 (Display)] フィールドに追加する値が表示されます。

- 浮動小数点数 (Float)
- パスワード (Password) : 最大文字列の長さを指定できます。
- [Long 型 (Long)] : 最小値と最大値を設定できます。
- [IP] : デフォルトの IPv4 または IPv6 アドレスを指定できます。

- [ブール型 (Boolean)] : True または False をデフォルト値として設定できます。
- [日付 (Date)] : カレンダーから日付を選択し、デフォルト値として設定できます。日付は yyyy-mm-dd 形式で表示されます。

ネットワーク アクセスまたは管理者ユーザの追加または編集時、これを必須属性とする場合は、[必須 (Mandatory)] チェック ボックスをオンにします。カスタム属性のデフォルト値を設定することもできます。

カスタム属性は、認証ポリシーで使用できます。カスタム属性に設定するデータ型と許容範囲は、ポリシー条件のカスタム属性の値に適用されます。

ユーザ認証の設定

[ユーザ認証設定 (User Authentication Settings Password Policy)] ページで、ユーザ アカウントパスワードが満たす必要がある基準を定義できます。[管理 (Administration)] > [ID の管理 (Identity Management)] > [設定 (Settings)] > [ユーザ認証設定 (User Authentication Settings)] > [パスワード ポリシー (Password Policy)] を選択します。

次の表に、[パスワード ポリシー (User Password Policy)] ページのフィールドを示します。

表 12: ユーザパスワードポリシーの設定

フィールド	説明
最小長 (Minimum Length)	パスワードの最小長 (文字数) を設定します。

フィールド	説明
パスワードに使用できない文字 (Password may not contain)	[ユーザ名 (User name)] : ユーザ名またはその文字の逆の順序での使用を制限します。
	[cisco] : 「cisco」 またはその文字の逆の順序での使用を制限します。
	[この単語 (This word)] : 定義した単語またはその文字の逆順での使用を制限します。
	[4 回以上連続して繰り返す文字列 (Repeated characters four or more times consecutively)] : 4 回以上連続する繰り返し文字の使用を制限します。
	<p>[辞書の単語 (Dictionary words)] : 辞書の単語、辞書の単語の逆順での使用、単語内の文字を別の文字で置き換えた単語の使用を制限する場合に選択します。</p> <p>「s」を「\$」、「a」を「@」、「o」を「0」、「l」を「1」、「i」を「!」、「e」を「3」に置き換えることはできません。たとえば Pa\$\$w0rd などです。</p> <ul style="list-style-type: none"> • [デフォルトの辞書 (Default Dictionary)] : Cisco ISE でデフォルトの Linux 辞書を使用するには、このオプションを選択します。デフォルトの辞書には約 480,000 件の英単語が含まれています。 デフォルトでは、このオプションが選択されています。 • [カスタム辞書 (Custom Dictionary)] : カスタマイズした辞書を使用するには、このオプションを選択します。[ファイルの選択 (Choose File)] をクリックし、カスタム辞書ファイルを選択します。このテキストファイルでは、単語が改行文字で区切られており、拡張子は .dic、サイズは 20 MB 以下である必要があります。

フィールド	説明
必須の文字 (Required characters)	<p>ユーザ パスワードに、次のタイプの文字がそれぞれ少なくとも 1 つは含まれている必要があります。</p> <ul style="list-style-type: none"> • 小文字の英文字 (Lowercase alphabetic characters) • 大文字の英文字 (Uppercase alphabetic characters) • 数字 (Numeric characters) • 英数字以外の文字 (Non-alphanumeric characters) <p>ユーザパスワードポリシーが大文字と小文字を必要としており、ユーザの言語でこれらの文字がサポートされていない場合、ユーザはパスワードを設定できません。UTF-8 文字をサポートするユーザパスワードフィールドの場合は、次のチェックボックス オプションをオフにする必要があります。</p> <ul style="list-style-type: none"> • 小文字の英文字 (Lowercase alphabetic characters) • 大文字の英文字 (Uppercase alphabetic characters)
パスワード履歴 (Password History)	<p>同じパスワードが繰り返し使用されることを防ぐために、パスワードが異なっている必要がある以前のバージョンの数を指定します。</p>
パスワードライフタイム (Password Lifetime)	<p>次のオプションを指定して、指定した期間後にパスワードを変更するようユーザに強制します。</p> <ul style="list-style-type: none"> • パスワードが変更されなかった場合にユーザ アカウントを無効にするまでの時間 (日数) (Time (in days) before the user account is disabled if the password is not changed) • ユーザ アカウントが無効になるまでのリマインダ (日数) (Reminder (in days) before the user account is disabled)

ユーザおよび管理者用の自動パスワードの生成

Cisco ISE では、ユーザおよび管理者の作成ページで Cisco ISE パスワード ポリシーに従うインスタントパスワードを生成するための [パスワードの生成 (Generate Password)] オプションが導入されています。これにより、ユーザまたは管理者は設定する安全なパスワードを考えるために時間を費やすことなく、Cisco ISE によって生成されたパスワードを使用することができます。

[パスワードの生成 (Generate Password)] オプションは、Cisco ISE Web インターフェイスの次の 3 つの場所で使用できます。

- ユーザ : [管理 (Administration)] > [ID の管理 (Identity Management)] > [ID (Identities)] > [ユーザ (Users)]。
- 管理者 : [管理 (Administration)] > [システム (System)] > [管理者アクセス (Admin Access)] > [管理者 (Administrators)] > [管理者ユーザ (Admin Users)]。
- ログイン管理者 (現在の管理者) : [設定 (Settings)] > [アカウント設定 (Account Settings)] > [パスワードの変更 (Change Password)]。

ユーザの追加

Cisco ISE では、Cisco ISE ユーザの属性を表示、作成、編集、複製、削除、ステータス変更、インポート、エクスポート、または検索できます。

Cisco ISE 内部データベースを使用する場合、Cisco ISE ネットワークのリソースまたはサービスへのアクセスを必要とするすべての新規ユーザのアカウントを作成する必要があります。

ステップ 1 [管理 (Administration)] > [ID の管理 (Identity Management)] > [ID (Identities)] > [ユーザ (Users)] を選択します。

[ワークセンター (Work Centers)] > [デバイス管理 (Device Administration)] > [ID (Identities)] > [ユーザ (Users)] ページにアクセスすることによって、ユーザを作成することもできます。

ステップ 2 新しいユーザを作成するには、[追加 (Add)] (+) をクリックします。

ステップ 3 フィールドの値を入力します。

ユーザ名にはスペース、+、* の文字を含めないようにします。BYOD 用に Cisco ISE 内部認証局 (CA) を使用する場合、ここに入力したユーザ名がエンドポイント証明書の共通名として使用されます。Cisco ISE 内部 CA は、「+」または「*」の文字を [共通名 (Common Name)] フィールドでサポートしていません。

ステップ 4 [送信 (Submit)] をクリックして、Cisco ISE 内部データベースに新しいユーザを作成します。

Cisco ISE ユーザ データのエクスポート

Cisco ISE 内部データベースからユーザ データをエクスポートしなければならない場合があります。Cisco ISE では、パスワード保護された csv ファイル形式でユーザ データをエクスポートすることができます。

-
- ステップ 1** [管理 (Administration)] > [ID の管理 (Identity Management)] > [ID (Identities)] > [ユーザ (Users)] を選択します。
- ステップ 2** データをエクスポートするユーザに対応するチェックボックスをオンにします。
- ステップ 3** [選択済みをエクスポート (Export Selected)] をクリックします。
- ステップ 4** [キー (Key)] フィールドに、パスワードを暗号化するためのキーを入力します。
- ステップ 5** [エクスポート開始 (Start Export)] をクリックして、users.csv ファイルを作成します。
- ステップ 6** [OK] をクリックして、users.csv ファイルをエクスポートします。
-

Cisco ISE 内部ユーザのインポート

新しい内部アカウントを作成するために、CSV ファイルを使用して新しいユーザデータを ISE にインポートできます。ユーザアカウントをインポートできるページから、テンプレート CSV ファイルをダウンロードできます。[管理 (Administration)] > [ID の管理 (Identity Management)] > [ID (Identities)] > [ユーザ (Users)] でユーザをインポートできます。スポンサーはスポンサー ポータルでユーザをインポートできます。ゲストアカウントのインポート方法については、『Sponsor Portal Guide』で説明しています。スポンサーゲストアカウントで使用される情報タイプの設定については、[スポンサー アカウント作成のためのアカウントコンテンツの設定 \(564 ページ\)](#) を参照してください。



-
- (注) CSV ファイルにカスタム属性が含まれている場合、カスタム属性に設定するデータ タイプと許容範囲は、インポート時にカスタム属性の値に適用されます。
-

-
- ステップ 1** [管理 (Administration)] > [ID の管理 (Identity Management)] > [ID (Identities)] > [ユーザ (Users)] を選択します。
- ステップ 2** [インポート (Import)] をクリックして、カンマ区切りテキストファイルからユーザをインポートします。
カンマ区切りテキスト ファイルがない場合は、[テンプレートの生成 (Generate a Template)] をクリックし、ヘッダー行に値が取り込まれている CSV ファイルを作成します。
- ステップ 3** [ファイル (File)] テキスト ボックスに、インポートするユーザが含まれたファイル名を入力するか、[参照 (Browse)] をクリックして、ファイルが配置されている場所に移動します。

ステップ 4 新しいユーザの作成、および既存のユーザの更新の両方を実行する必要がある場合は、[新しいユーザの作成、および新しいデータで既存のユーザを更新（Create new user(s) and update existing user(s) with new data）] チェックボックスをオンにします。

ステップ 5 Cisco ISE 内部データベースに変更を保存するには、[保存（Save）] をクリックします。



(注) すべてのネットワーク アクセス ユーザを一度に削除しないことを推奨します。一度に削除すると、特に非常に大規模なデータベースを使用している場合は、CPU スパイクとサービスのクラッシュにつながる場合があります。

ユーザ ID グループの作成

ユーザ ID グループを追加する前に、ユーザ ID グループを作成する必要があります。

ステップ 1 [管理（Administration）] > [ID の管理（Identity Management）] > [グループ（Groups）] > [アイデンティティグループ（Identity Groups）] > [ユーザ ID グループ（User Identity Groups）] > [追加（Add）] を選択します。

[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [ユーザ ID グループ（User Identity Groups）] > [アイデンティティグループ（Identity Groups）] > [ユーザ ID グループ（User Identity Groups）] > [追加（Add）] ページにアクセスして、ユーザ ID グループを作成することもできます。

ステップ 2 [名前（Name）] フィールドおよび [説明（Description）] フィールドに値を入力します。[名前（Name）] フィールドでサポートされる文字は次のとおりです：スペース、# \$ & ' () * + - . / @ _。

ステップ 3 [送信（Submit）] をクリックします。

関連トピック

[ユーザ グループ](#)（362 ページ）

[ユーザ ID グループ](#)（362 ページ）

[デフォルト ユーザ ID グループ](#)

[ユーザ ID グループのインポート](#)（370 ページ）

ユーザ ID グループのエクスポート

Cisco ISE では、ローカルに設定されたユーザ ID グループを csv ファイル形式でエクスポートすることができます。

ステップ 1 [管理（Administration）] > [ID の管理（Identity Management）] > [グループ（Groups）] > [ID グループ（Identity Groups）] > [ユーザ ID グループ（User Identity Groups）] を選択します。

ステップ 2 エクスポートするユーザ ID グループに対応するチェックボックスをオンにし、[エクスポート (Export)] をクリックします。

ステップ 3 [OK] をクリックします。

ユーザ ID グループのインポート

Cisco ISE では、ユーザ ID グループを csv ファイル形式でインポートすることができます。

ステップ 1 [管理 (Administration)] > [ID の管理 (Identity Management)] > [グループ (Groups)] > [ID グループ (Identity Groups)] > [ユーザ ID グループ (User Identity Groups)] を選択します。

ステップ 2 インポートファイルに使用するテンプレートを取得するには、[テンプレートの生成 (Generate a Template)] をクリックします。

ステップ 3 [インポート (Import)] をクリックして、カンマ区切りテキストファイルからネットワーク アクセス ユーザをインポートします。

ステップ 4 新しいユーザ ID グループの追加、および既存のユーザ ID グループの更新の両方を実行する必要がある場合は、[新しいデータで既存のデータを上書き (Overwrite existing data with new data)] チェックボックスをオンにします。

ステップ 5 [インポート (Import)] をクリックします。

ステップ 6 Cisco ISE データベースに変更を保存するには、[保存 (Save)] をクリックします。

外部 ID ソースを使用した許可ポリシーの作成

次に、外部 ID ソースを使用して許可ポリシーを作成する手順を示します。

ステップ 1 [ポリシー (Policy)] > [認証 (Authorization)] を選択して、[標準 (Standard)] ポリシーで新しい許可ポリシー ルールを作成します。

ポリシー セットをイネーブルにした場合は、[ポリシー (Policy)] > [ポリシー セット (Policy Set)] を選択し、このポータルに使用するポリシー セットを選択して、[承認ポリシー (Authorization Policy)] を展開し、新しいルールを追加します。

ステップ 2 [条件 (Conditions)] には、ポータルの検証に使用するエンドポイント ID グループを選択します。

外部 ID ソース（たとえば、RSA SecurID）を内部ユーザ グループとともに使用する場合は、次の構文を使用して条件を作成する必要があります。

```
InternalUser:IdentityGroup EQUALS User Identity Groups:Group_Name
```

グループ名の前に「User Identity Groups:」を引用符なしで追加します。

ステップ 3 [権限 (Permissions)] には、作成したポータル許可プロファイルを選択します。

最大同時セッション数の設定

最適なパフォーマンスを得るために、同時ユーザセッション数を制限できます。ユーザ レベルまたはグループレベルで制限を設定できます。最大ユーザセッションの設定に応じて、セッション カウントはユーザに適用されます。

ISE ノードごとに各ユーザの同時セッションの最大数を設定できます。この制限を超えるセッションは拒否されます。

ステップ 1 [管理 (Administration)] > [システム (System)] > [設定 (Settings)] > [最大セッション数 (Max Sessions)] > [ユーザ (User)] の順に選択します。

ステップ 2 次のいずれかを実行します。

- 各ユーザに許可される同時セッションの最大数を、[ユーザごとの最大セッション数 (Maximum Sessions per User)] フィールドに入力します。

または

- ユーザのセッション数を無制限にするには、[セッション数無制限 (Unlimited Sessions)] チェック ボックスをオンにします。このオプションは、デフォルトで選択されます。

ステップ 3 [保存 (Save)] をクリックします。

セッションの最大数がユーザ レベルとグループ レベルの両方で設定されている場合、小さい方の値が優先されます。たとえば、ユーザの最大セッション値が 10 に設定されていて、ユーザが属するグループの最大セッション値が 5 に設定されている場合、ユーザは最大で 5 つのセッションのみを持つことができます。

最大セッション数を 1 に設定しており、ユーザが接続する WLC でサポートされているバージョンの WLC が稼働していない場合、ユーザに対し、切断してから再接続するよう指示するエラーが表示されます。「Cisco Identity Services Engine Network Component Compatibility」を参照してください。 http://www.cisco.com/c/en/us/td/docs/security/ise/2-2/compatibility/ise_sdt.html

グループの最大同時セッション数

ID グループの最大同時セッション数を設定できます。

グループ内の少人数のユーザによってすべてのセッションが使用される場合があります。他のユーザからの新しいセッションの作成要求は、セッション数がすでに最大設定値に達しているため、拒否されます。Cisco ISE では、グループ内の各ユーザに最大セッション制限を設定できます。特定の ID グループに所属する各ユーザは、同じグループの他のユーザが開いているセッション数に関係なく、制限以上はセッションを開くことができません。特定のユーザのセッション制限を計算する場合は、ユーザ 1 人あたりのグローバルセッション制限、ユーザが所属する ID グループあたりのセッション制限、グループ内のユーザ 1 人あたりのセッション制限のいずれかの最小設定値が優先されます。

ID グループの同時セッションの最大数を設定するには、次の手順に従います。

カウンタの時間制限の設定

ステップ 1 [管理 (Administration)] > [システム (System)] > [設定 (Settings)] > [最大セッション数 (Max Sessions)] > [グループ (Group)] の順に選択します。

設定した ID グループがすべて一覧表示されます。

ステップ 2 編集するグループの横にある [編集 (Edit)] アイコンをクリックして、次の値を入力します。

- そのグループに許可される同時セッションの最大数。グループのセッションの最大数を 100 に設定した場合、グループのすべてのメンバーによって確立されたすべてのセッションの総数は 100 を超えることはできません。

(注) グループ階層に基づいてグループ レベルのセッションが適用されます。

- そのグループの各ユーザに許可される同時セッションの最大数。このオプションは、グループの最大セッション数を上書きします。

グループの同時セッションの最大数、またはグループ内のユーザの同時セッションの最大数を [無制限 (Unlimited)] に設定するには、[グループの最大セッション数/グループ内のユーザの最大セッション数 (Max Sessions for User in Group/Max Sessions for User in Group)] フィールドを空白にし、ティック アイコンをクリックし、[保存 (Save)] をクリックします。デフォルトでは、両方の値が [無制限 (Unlimited)] に設定されています。

ステップ 3 [保存 (Save)] をクリックします。

カウンタの時間制限の設定

同時ユーザセッションのタイムアウトを設定できます。

ステップ 1 [管理 (Administration)] > [システム (System)] > [設定 (Settings)] > [最大セッション数 (Max Sessions)] > [カウンタの時間制限 (Counter Time Limit)] の順に選択します。

ステップ 2 次のオプションのいずれかを選択します。

- 無制限 (Unlimited) : セッションのタイムアウトまたは時間制限を設定しない場合は、このチェックボックスにマークを付けます。
- [経過後にセッションを削除 (Delete sessions after)] : 日、時間、分の単位で同時セッションのタイムアウト値を入力できます。セッションが時間制限を超えると、Cisco ISE はカウンタからセッションを削除してセッション数を更新するため、新しいセッションが許可されます。ユーザは、セッションの時間制限を超えた場合、ログアウトされません。

ステップ 3 [保存 (Save)] をクリックします。

[RADIUS ライブ ログ (RADIUS Live Logs)] ページでセッション カウントをリセットできます。[ID (Identity)]、[ID グループ (Identity Group)]、[サーバ (Server)] 列に表示される [アクション (Actions)] アイコンをクリックして、セッションカウントをリセットします。セッ

セッションをリセットすると、セッションはカウンタから削除されます（これにより、新しいセッションが許可されます）。ユーザのセッションがカウンタから削除されても、ユーザの接続は切断されません。

アカウント無効化ポリシー

Cisco ISE は、Cisco Secure ACS と同等の機能を実現するために、ユーザおよび管理者のアカウント無効化ポリシーを導入しています。ユーザまたは管理者の認証または問い合わせ時に、Cisco ISE は [管理 (Administration)] > [ID の管理 (Identity Management)] > [設定 (Settings)] > [ユーザ認証設定 (User Authentication Settings)] ページでグローバル アカウント無効化ポリシー設定を確認し、その設定に基づいて認証または結果を返します。

Cisco ISE は、次の 3 つのポリシーを確認します。

- 指定した日付 (yyyy-mm-dd) を超えたらユーザ アカウントを無効にする (Disable user accounts that exceed a specified date (yyyy-mm-dd)) : 設定された日付にユーザ アカウントを無効にします。ただし、[管理 (Administration)] > [ID の管理 (Identity Management)] > [ID (Identities)] > [ユーザ (Users)] > [アカウント無効化ポリシー (Account Disable Policy)] で設定された個々のネットワーク アクセス ユーザのアカウント無効化ポリシー設定はグローバル設定よりも優先されます。
- アカウント作成時または最後の有効化から *n* 日後にユーザ アカウントを無効にする (Disable user account after *n* days of account creation or last enable) : アカウントの作成またはアカウントが有効になった最後の日から指定した日数後にユーザ アカウントを無効にします。[管理 (Administration)] > [ID の管理 (Identity Management)] > [ID (Identities)] > [ユーザ (Users)] > [ステータス (Status)] でユーザのステータスを確認できます。
- 非アクティブになってから *n* 日後にアカウントを無効にする (Disable accounts after *n* days of inactivity) : 設定した連続日数、認証されなかった管理者およびユーザ アカウントを無効化します。

Cisco Secure ACS から Cisco ISE に移行する際、Cisco Secure ACS ではネットワーク アクセス ユーザ用に指定したアカウント無効化ポリシーの設定は Cisco ISE に移行されます。

個別のユーザ アカウントの無効化

Cisco ISE では、アカウントの無効日が管理者ユーザによって指定された日付を超えた場合は、各個人ユーザのユーザ アカウントを無効にすることができます。

-
- ステップ 1** [管理 (Administration)] > [ID の管理 (Identity Management)] > [ID (Identities)] > [ユーザ (Users)] の順に選択します。
- ステップ 2** [追加 (Add)] をクリックして新しいユーザを作成するか、既存のユーザの横のチェックボックスをオンにして [編集 (Edit)] をクリックして既存のユーザの詳細を編集します。
- ステップ 3** [日付を超えたらアカウントを無効化する (Disable account if the date exceeds)] チェックボックスをオンにして、日付を選択します。

このオプションによって、ユーザレベルで設定した日付を超えたときに、ユーザアカウントをディセーブルにすることができます。必要に応じて、異なるユーザに異なる失効日を設定できます。このオプションは、個々のユーザのグローバルコンフィギュレーションを無効にします。日付には、現在のシステム日付または将来の日付を設定できます。

(注) 現在のシステム日付よりも古い日付は入力できません。

ステップ 4 [送信 (Submit)] をクリックして、個々のユーザのアカウント無効化ポリシーを設定します。

グローバルにユーザ アカウントを無効にする

Cisco ISE では、特定の日付、アカウントの作成または最終アクセス日からの日数、およびアカウントの非アクティブの日数の後に、ユーザ アカウントを無効にすることができます。

ステップ 1 [管理 (Administration)] > [ID の管理 (Identity Management)] > [設定 (Settings)] > [ユーザ認証設定 (User Authentication Settings)] > [アカウント無効化ポリシー (Account Disable Policy)] を選択します。

ステップ 2 次のいずれかの操作を実行します。

- [日付を超えるとアカウントを無効にする (Disable account if date exceeds)] チェック ボックスをオンにして、yyyy-mm-dd 形式の適切な日付を選択します。このオプションによって、設定した日付が超過したときに、ユーザ アカウントを無効にすることができます。ただし、ユーザ レベルでの [日付を超えるとアカウントを無効にする (Disable account if date exceeds)] オプションはグローバル設定よりも優先されます。
- [アカウントの作成または最後に有効になってから n 日後にアカウントを無効にする (Disable account after n days of account creation or last enable)] チェック ボックスをオンにして、日数を入力します。このオプションは、アカウントの作成日または最終アクセス日が指定した日数を超えたときにユーザ アカウントを無効にすることができます。管理者は、無効化されたユーザ アカウントを手動で有効にでき、日数の数は、ユーザ アカウントを有効にすると、自動的にリセットされます。
- [非アクティブになってから n 日後にアカウントを無効にする (Disable account after n days of inactivity)] チェック ボックスをオンにして、日数を入力します。このオプションは、アカウントが指定した日数非アクティブのときにユーザ アカウントを無効にすることができます。

ステップ 3 [送信 (Submit)] をクリックし、グローバル アカウント無効化ポリシーを設定します。

内部 ID ソースと外部 ID ソース

ID ソースには、Cisco ISE がユーザ認証時にクレデンシャルを検証するために使用するユーザ情報が含まれます。このユーザ情報は、ユーザに関連付けられたグループ情報およびその他の属性を取得して許可ポリシーで使用するためにも使用されます。これらは、レコード形式で

ユーザ情報を保存するデータベースです。ID ソースに対してユーザ情報の追加、編集、および削除を行うことができます。

Cisco ISE では内部 ID ソースと外部 ID ソースがサポートされます。どちらのソースも、スポンサーユーザ認証およびゲストユーザ認証の認証ソースとして使用できます。

内部 ID ソース

Cisco ISE には、ユーザ情報を保存するために使用できる内部ユーザデータベースがあります。内部ユーザ データベースのユーザは、内部ユーザと呼ばれます。Cisco ISE には、Cisco ISE に接続するすべてのデバイスおよびエンドポイントに関する情報を格納する内部エンドポイントデータベースもあります。

外部 ID ソース

Cisco ISE では、ユーザ情報を含む外部 ID ソースを設定することができます。Cisco ISE は外部 ID ソースに接続して、認証用のユーザ情報を取得します。外部 ID ソースには、Cisco ISE サーバおよび証明書認証プロファイルの証明書情報も含まれます。Cisco ISE は外部 ID ソースとの通信に認証プロトコルを使用します。次の表に、認証プロトコルおよびサポートされる外部 ID ソースを示します。

表 13: 認証プロトコルとサポートされている外部 ID ソース

プロトコル (認証タイプ)	内部データベース	Active Directory	LDAP	RADIUS トークンサーバまたは RSA
EAP-GTC、PAP (プレーンテキストパスワード)	○	○	○	○
MS-CHAP パスワードハッシュ: MSCHAPv1/v2 EAP-MSCHAPv2 (PEAP、EAP-FAST、EAP-TTLS の内部メソッドとして) LEAP	○	○	[いいえ (No)]	[いいえ (No)]
EAP-MD5 CHAP	[はい (Yes)]	[いいえ (No)]	[いいえ (No)]	[いいえ (No)]

プロトコル（認証タイプ）	内部データベース	Active Directory	LDAP	RADIUS トークンサーバまたは RSA
EAP-TLS PEAP-TLS (証明書取得) (注) TLS 認証 (EAP-TLS と PEAP-TLS) に ID ソースは必須ではありませんが、許可ポリシー条件のために任意で追加できます。	なし	○	○	[いいえ (No)]

外部 ID ソースの作成

Cisco ISE では、Active Directory、LDAP、RADIUS トークン、RSA SecurID サーバなどの外部 ID ソースに接続して、認証/許可のユーザ情報を取得できます。外部 ID ソースには、証明書ベースの認証に必要な証明書認証プロファイルも含まれています。



(注) 認証済みユーザ ID を受信して共有できるようにするパッシブ ID サービスを使用するには、[その他のパッシブ ID サービスプロバイダー \(433 ページ\)](#) を参照してください。

ステップ 1 [管理 (Administration)] > [ID の管理 (Identity Management)] > [外部 ID ソース (External Identity Sources)] を選択します。

ステップ 2 次のオプションのいずれかを選択します。

- [証明書認証プロファイル (Certificate Authentication Profile)] : 証明書ベースの認証の場合。
- [Active Directory] : 外部 ID ソースとして Active Directory に接続する場合（詳細は [外部 ID ソースとしての Active Directory \(379 ページ\)](#) を参照）。
- [LDAP] : LDAP ID ソースを追加する場合（詳細は [LDAP \(482 ページ\)](#) を参照）。
- [RADIUS トークン (RADIUS Token)] : RADIUS トークン サーバを追加する場合（詳細は [RADIUS トークン ID ソース \(499 ページ\)](#) を参照）。
- [RSA SecurID] : RSA SecurID サーバを追加する場合（詳細は [RSA ID ソース \(504 ページ\)](#) を参照）。

- [SAML ID プロバイダー (SAML Id Providers)] : Oracle Access Manager などの ID プロバイダー (IdP) を追加する場合 (詳細は [外部 ID ソースとしての ID プロバイダ \(14 ページ\)](#) を参照)。

関連トピック

- [内部 ID ソースと外部 ID ソース \(374 ページ\)](#)
- [内部 ID ソース](#)
- [外部 ID ソース](#)
- [証明書認証プロファイルの追加 \(378 ページ\)](#)
- [外部 ID ソースとしての Active Directory の設定 \(385 ページ\)](#)
- [Active Directory の複数参加設定のサポート \(393 ページ\)](#)
- [LDAP ID ソースの追加 \(487 ページ\)](#)
- [RADIUS トークン サーバの追加 \(502 ページ\)](#)
- [RSA ID ソースの追加 \(507 ページ\)](#)
- [ID ソース順序 \(517 ページ\)](#)
- [ID ソース順序の作成 \(517 ページ\)](#)
- [レポートでの ID ソースの詳細 \(518 ページ\)](#)
- [\[認証 \(Authentications\)\] ダッシュレット \(519 ページ\)](#)
- [ID ソース レポート \(519 ページ\)](#)

外部 ID ストア パスワードに対する内部ユーザの認証

Cisco ISE では、外部 ID ストア パスワードに対して内部ユーザを認証できます。Cisco ISE では、[管理 (Administration)] > [ID の管理 (Identity Management)] > [ID (Identities)] > [ユーザ (Users)] ページから、内部ユーザのパスワード ID ストアを選択するオプションが提供されます。管理者は、Cisco ISE の外部 ID ソースのリストから ID ストアを選択することができ、[ユーザ (Users)] ページでユーザを追加するか、または編集します。内部ユーザのデフォルトのパスワード ID ストアは内部 ID ストアです。Cisco Secure ACS ユーザは、Cisco Secure ACS から Cisco ISE への移行中および移行後、同じパスワード ID ストアを維持します。Cisco ISE の旧バージョンから Cisco ISE 2.1 にアップグレードすると、Cisco ISE 2.1 では、すべての内部ユーザのデフォルトの ID ストアとして内部 ID ストアが設定されます。

Cisco ISE はパスワード タイプに対し次の外部 ID ストアをサポートします。

- Active Directory
- LDAP
- ODBC
- RADIUS トークン サーバ
- RSA SecurID サーバ

証明書認証プロファイル

プロファイルごとに、プリンシパルユーザ名として使用する証明書フィールドと、証明書のバイナリ比較を行うかどうかを指定する必要があります。

証明書認証プロファイルの追加

Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) 証明書ベースの認証方式を使用する場合は、証明書認証プロファイルを作成する必要があります。従来のユーザ名とパスワードの方法で認証する代わりに、Cisco ISE はクライアントから受信した証明書をサーバ内の証明書と比較してユーザの信頼性を確認します。

始める前に

スーパー管理者またはシステム管理者である必要があります。

ステップ 1 [管理 (Administration)] > [ID の管理 (Identity Management)] > [外部 ID ソース (External Identity Sources)] > [証明書認証プロファイル (Certificate Authentication Profile)] > [追加 (Add)] を選択します。

ステップ 2 証明書認証プロファイルの名前と説明 (任意) を入力します。

ステップ 3 ドロップダウン リストから ID ストアを選択します。

基本証明書のチェックは ID ソースを必要としません。証明書にバイナリ比較チェックが必要な場合は、ID ソースを選択する必要があります。ID ソースとして **Active Directory** を選択した場合は、サブジェクト名、一般名、およびサブジェクト代替名 (すべての値) を使用してユーザを検索できます。

ステップ 4 [証明書属性 (Certificate Attribute)] または [証明書の任意のサブジェクトまたは代替名属性 (Any Subject or Alternative Name Attributes in the Certificate)] から ID の使用を選択します。これは、ログで検索のために使用されます。

[証明書の任意のサブジェクトまたは代替名属性 (Any Subject or Alternative Name Attributes in the Certificate)] を選択すると、**Active Directory UPN** がログ用のユーザ名として使用され、証明書のすべてのサブジェクト名および代替名がユーザの検索に試行されます。このオプションは、ID ソースとして **Active Directory** を選択した場合にのみ使用できます。

ステップ 5 クライアント証明書を ID ストアの証明書と照合する場合に選択します。この場合、ID ソース (LDAP または **Active Directory**) を選択する必要があります。[**Active Directory**] を選択した場合は、ID のあいまいさを解決するためにのみ証明書を照合することを選択できます。

- [なし (Never)] : このオプションは、バイナリ比較を実行しません。
- [ID のあいまいさを解決する目的のみ (Only to resolve identity ambiguity)] : このオプションは、あいまいさが見つかった場合にだけ、クライアント証明書と **Active Directory** のアカウントの証明書とのバイナリ比較を実行します。たとえば、複数の **Active Directory** アカウントが証明書の識別名に一致することがあります。

- [常にバイナリ比較を実行する (Always perform binary comparison)] : このオプションは、クライアント証明書と ID ストア (Active Directory または LDAP) 内のアカウントの証明書とのバイナリ比較を常に実行します。

ステップ 6 [送信 (Submit)] をクリックして、証明書認証プロファイルを追加するか、変更を保存します。

外部 ID ソースとしての Active Directory

Cisco ISE は、ユーザ、マシン、グループ、属性などのリソースにアクセスするために、Microsoft Active Directory を外部 ID ソースとして使用します。Active Directory でのユーザとマシンの認証では、Active Directory にリストされているユーザとデバイスに対してのみネットワークアクセスを許可します。

[ISE コミュニティ リソース](#)

[ISE Administrative Portal Access with AD Credentials Configuration Example](#)

Active Directory でサポートされる認証プロトコルおよび機能

Active Directory は、一部のプロトコルを使用したユーザとマシンの認証、Active Directory ユーザパスワードの変更などの機能をサポートしています。次の表に、Active Directory でサポートされる認証プロトコルおよびそれぞれの機能を示します。

表 14: Active Directory でサポートされる認証プロトコル

認証プロトコル	機能
EAP-FAST およびパスワードベースの Protected Extensible Authentication Protocol (PEAP)	MS-CHAPv2 および EAP-GTC の内部方式で EAP-FAST と PEAP を使用するパスワード変更機能を備えたユーザとマシンの認証
Password Authentication Protocol (PAP)	ユーザおよびマシン認証
Microsoft Challenge Handshake Authentication Protocol Version 1 (MS-CHAPv1)	ユーザおよびマシン認証
Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAPv2)	ユーザおよびマシン認証
Extensible Authentication Protocol-Generic Token Card (EAP-GTC)	ユーザおよびマシン認証
Extensible Authentication Protocol-Transport Layer Security (EAP-TLS)	<ul style="list-style-type: none"> • ユーザおよびマシン認証 • グループおよび属性取得 • 証明書のバイナリ比較

認証プロトコル	機能
Extensible Authentication Protocol- Flexible Authentication via Secure Tunneling-Transport Layer Security (EAP-FAST-TLS)	<ul style="list-style-type: none"> ユーザおよびマシン認証 グループおよび属性取得 証明書のバイナリ比較
Protected Extensible Authentication Protocol-Transport Layer Security (PEAP-TLS)	<ul style="list-style-type: none"> ユーザおよびマシン認証 グループおよび属性取得 証明書のバイナリ比較
Lightweight Extensible Authentication Protocol (LEAP)	ユーザ認証

許可ポリシーで使用する Active Directory 属性およびグループの取得

Cisco ISE は、許可ポリシー ルールで使用するために Active Directory からユーザまたはマシンの属性およびグループを取得します。これらの属性は Cisco ISE ポリシーで使用され、ユーザまたはマシンの承認レベルを決定します。Cisco ISE は、認証が成功した後にユーザおよびマシンの Active Directory 属性を取得します。認証とは別に、許可のために属性を取得することもできます。

Cisco ISE は、外部 ID ストア内のグループを使用してユーザまたはコンピュータに権限を割り当てることがあります（たとえば、ユーザをスポンサー グループにマップします）。Active Directory のグループ メンバーシップの次の制限事項に注意してください。

- ポリシーールの条件は、次のいずれかを参照します。ユーザまたはコンピュータのプライマリ グループ、ユーザまたはコンピュータが直接メンバーであるグループ、または間接的（ネストされた）グループ。
- ユーザまたはコンピュータのアカウント ドメイン外のドメイン ローカルグループはサポートされません。



(注) Active Directory 属性の値 msRadiusFramedIPAddress を IP アドレスとして使用できます。この IP アドレスは、許可プロファイルのネットワーク アクセス サーバ (NAS) に送信できます。msRADIUSFramedIPAddress 属性は IPv4 アドレスだけをサポートします。ユーザ認証では、ユーザに対し取得された msRadiusFramedIPAddress 属性値が IP アドレス形式に変換されます。

属性およびグループは、参加ポイントごとに取得され、管理されます。これらは許可ポリシーで使用されます（まず参加ポイントを選択し、次に属性を選択します）。許可範囲ごとに属性またはグループを定義することはできませんが、認証ポリシーに範囲を使用できます。認証ポリシーで範囲を使用する場合、ユーザは1つの参加ポイントで認証されますが、ユーザのアカウント ドメインへの信頼できるパスがある別の参加ポイント経由で属性またはグループを取得

することができます。認証ドメインを使用して、1つの範囲内にある2つの参加ポイントで認証ドメインが重複しないようにすることができます。



- (注) 使用可能な Active Directory グループの最大数については、Microsoft の制限を参照してください。[http://technet.microsoft.com/en-us/library/active-directory-maximum-limits-scalability\(v=WS.10\).aspx](http://technet.microsoft.com/en-us/library/active-directory-maximum-limits-scalability(v=WS.10).aspx)

ルールに、/、!、@、\、#、\$、%、^、&、*、(、)、_、+、または~のような特殊文字を使用した Active Directory グループ名が含まれる場合、許可ポリシーは失敗します。

ブール属性のサポート

Cisco ISE は、Active Directory および LDAP ID ストアからのブール属性の取得をサポートしています。

Active Directory または LDAP のディレクトリ属性を設定する際に、ブール属性を設定できます。これらの属性は、Active Directory または LDAP による認証時に取得されます。

ブール属性は、ポリシー ルール条件の設定に使用できます。

ブール属性値は、文字列型として Active Directory または LDAP サーバから取得されます。Cisco ISE は、次のブール属性値をサポートしています。

ブール属性	サポートされる値
[はい (True)]	t、T、true、TRUE、True、1
いいえ (False)	f、F、false、FALSE、False、0



- (注) 属性置換はブール属性ではサポートされません。

文字列型としてブール属性（たとえば、msTSAllowLogon）を設定すると、Active Directory または LDAP サーバの属性のブール値は Cisco ISE の文字列属性に設定されます。属性タイプをブール型に変更したり、ブール型として属性を手動で追加できます。

証明書ベース認証の Active Directory 証明書の取得

Cisco ISE では、EAP-TLS プロトコルを使用するユーザまたはマシン認証のための証明書取得がサポートされています。Active Directory 上のユーザまたはマシン レコードには、バイナリデータ型の証明書属性が含まれています。この証明書属性に1つ以上の証明書を含めることができます。Cisco ISE ではこの属性は userCertificate として識別され、この属性に対して他の名前を設定することはできません。Cisco ISE はこの証明書を取得し、バイナリ比較の実行に使用します。

証明書認証プロファイルは、証明書の取得に使用する Active Directory のユーザを検索するためにユーザ名を取得するフィールド（たとえば、サブジェクト代替名 (SAN) または一般名）を

決定します。Cisco ISE は、証明書を取得した後、この証明書とクライアント証明書とのバイナリ比較を実行します。複数の証明書が受信された場合、Cisco ISE は、いずれかが一致するかどうかをチェックするために証明書を比較します。一致が見つかった場合、ユーザまたはマシン認証に合格します。

Active Directory ユーザ認証プロセス フロー

ユーザの認証または問い合わせ時に、Cisco ISE は次のことをチェックします。

- MS-CHAP および PAP 認証では、ユーザが無効かどうか、ロックアウトされているかどうか、期限切れかどうか、またはログイン時間外かどうかを確認します。これらの条件のいくつかが true の場合、認証が失敗します。
- EAP-TLS 認証では、ユーザが無効かどうか、ロックアウトされているかどうかを確認します。これらの条件のいくつかが一致する場合、認証が失敗します。

Active Directory マルチドメイン フォレストのサポート

Cisco ISE では、マルチドメイン フォレストの Active Directory がサポートされます。各フォレスト内で、Cisco ISE は単一のドメインに接続しますが、Cisco ISE が接続されているドメインと他のドメイン間に信頼関係が確立されている場合は、Active Directory フォレストの他のドメインからリソースにアクセスできます。

Active Directory サービスをサポートする Windows サーバオペレーティングシステムのリストについては、『Release Notes for Cisco Identity Services Engine』を参照してください。



- (注) Cisco ISE は、ネットワーク アドレス トランスレータの背後にあり、ネットワーク アドレス変換 (NAT) アドレスを持つ Microsoft Active Directory サーバをサポートしません。

Active Directory と Cisco ISE の統合の前提条件

ここでは、Cisco ISE と統合する Active Directory を設定するために必要な手動での作業手順を説明します。ただしほとんどの場合、Cisco ISE が Active Directory を自動的に設定することができます。次に、Cisco ISE と Active Directory を統合するための前提条件を示します。

- ISE でのスーパー管理者またはシステム管理者の権限があることを確認します。
- Cisco ISE サーバと Active Directory 間の時間を同期するために Network Time Protocol (NTP) サーバ設定を使用します。Cisco ISE CLI で NTP を設定できます。
- Cisco ISE は、双方向信頼がなく、相互の信頼がゼロである複数の Active Directory ドメインと接続できます。特定の参加ポイントから他のドメインを照会する場合は、参加ポイントと、アクセスする必要があるユーザ情報およびマシン情報があるその他のドメインの間に信頼関係が確立されていることを確認します。信頼関係が確立されていない場合は、信

頼できないドメインへの別の参加ポイントを作成する必要があります。信頼関係の確立の詳細については、Microsoft Active Directory のドキュメントを参照してください。

- Cisco ISE の参加先ドメインでは、少なくとも 1 つのグローバルカタログサーバが動作し、Cisco ISE からアクセス可能である必要があります。

さまざまな操作の実行に必要な Active Directory アカウント権限

参加操作	脱退処理	Cisco ISE マシン アカウント
<p>参加操作の実行に使用されるアカウントには、次のアクセス許可が必要です。</p> <ul style="list-style-type: none"> • Active Directory を検索する権限 (Cisco ISE マシンアカウントがすでにあるかどうかの確認) • ドメインに Cisco ISE マシンアカウントを作成する権限 (マシンアカウントが存在しない場合) • 新しいマシンアカウントに属性を設定する権限 (Cisco ISE マシンアカウント パスワード、SPN、dnsHostname など) <p>参加操作を実行するために、ドメイン管理者である必要はありません。</p>	<p>脱退操作の実行に使用するアカウントには、次の権限が必要です。</p> <ul style="list-style-type: none"> • Active Directory を検索する権限 (Cisco ISE マシンアカウントがすでにあるかどうかの確認) • ドメインから Cisco ISE マシンアカウントを削除する権限 <p>強制脱退 (パスワードなしの脱退) を実行する場合、ドメインからマシンアカウントは削除されません。</p>	<p>Active Directory 接続との通信のために新規に作成された Cisco ISE マシンアカウントには、次の権限が必要です。</p> <ul style="list-style-type: none"> • 自分のパスワードの変更 • 認証対象のユーザ/マシンに対応するユーザ/マシンオブジェクトを読み取る権限 • 必要な情報を取得するために Active Directory の一部をクエリする権限 (信頼ドメイン、代替の UPN サフィックスなど) • tokenGroups 属性を読み取る権限 <p>Active Directory でマシンアカウントを事前に作成できます。SAM の名前が Cisco ISE アプライアンスのホスト名と一致する場合は、参加操作中に検索して再利用する必要があります。</p> <p>複数の参加操作を実行すると、参加ごとに複数のマシンアカウントが Cisco ISE 内で保持されます。</p>



- (注) 参加操作または脱退操作に使用するクレデンシヤルは Cisco ISE に保存されません。新規に作成された Cisco ISE マシン アカウントのクレデンシヤルのみが保存されます。これによって、エンドポイント プローブも実行できるようになります。

通信用に開放するネットワーク ポート

プロトコル	ポート (リモート ローカル)	ターゲット (Target)	認証	注記 (Notes)
DNS (TCP/UDP)	49152 以上の乱数	DNS サーバ/AD ドメイン コント ローラ	なし	—
MSRPC	445	ドメイン コント ローラ	○	—
Kerberos (TCP/UDP)	88	ドメイン コント ローラ	あり (Kerberos)	MS AD/KDC
LDAP (TCP/UDP)	389	ドメイン コント ローラ	○	—
LDAP (GC)	3268	グローバル カタ ログ サーバ	○	—
NTP	123	NTP サーバ/ドメ イン コントロー ラ	なし	—
IPC	80	展開内の他の ISE ノード	あり (RBAC クレ デンシヤルを使 用)	—

DNS サーバ

DNS サーバを設定する場合は、次の処理を実行します。

- Cisco ISE に設定されている DNS サーバで、使用するドメインのすべての正引きおよび逆引き DNS クエリを解決できるようにする必要があります。
- DNS 再帰によって遅延が発生してパフォーマンスが重大な悪影響を受ける可能性があるので、権威 DNS サーバで Active Directory レコードを解決することをお勧めします。
- すべての DNS サーバで、追加サイト情報の有無に関係なく、DC、GC、および KDC の SRV クエリに回答できるようにする必要があります。

- パフォーマンスを向上するために、SRV 応答にサーバ IP アドレスを追加することを推奨します。
- パブリック インターネットでクエリを実行する DNS サーバを使用しないでください。不明な名前を解決する必要がある場合に、ネットワークの情報が漏洩する可能性があります。

外部 ID ソースとしての Active Directory の設定

Easy Connect や PassiveID ワーク センター などの機能を設定する際に、Active Directory を外部 ID ソースとして設定します。これらの機能の詳細については、[Easy Connect \(417 ページ\)](#) と [PassiveID ワーク センター \(423 ページ\)](#) を参照してください。

外部 ID ソースとして Active Directory を設定する前に、次のことを確認します。

- Microsoft Active Directory サーバがネットワーク アドレス トランスレータの背後にないこと、およびネットワーク アドレス変換 (NAT) アドレスを持たないこと。
- 参加操作の Microsoft Active Directory アカウントが有効であり、[次回ログイン時にパスワードを変更 (Change Password on Next Login)] を使用して設定されていないこと。
- ISE のスーパー管理者またはシステム管理者の権限があること。



(注) Cisco ISE が Active Directory に接続されているときに操作に関する問題がある場合は、**[操作 (Operations)]** > **[レポート (Reports)]** で AD コネクタ操作レポートを参照してください。

外部 ID ソースとして Active Directory を設定するには、次のタスクを実行する必要があります。

1. [Active Directory 参加ポイントの追加および参加ポイントへの Cisco ISE ノードの参加 \(386 ページ\)](#)
2. [認証ドメインの設定 \(390 ページ\)](#)
3. [Active Directory ユーザ グループの設定 \(390 ページ\)](#)
4. [Active Directory ユーザとマシンの属性の設定 \(391 ページ\)](#)
5. (オプション) [パスワード変更、マシン認証、およびマシン アクセス制限の設定の変更 \(392 ページ\)](#)

関連トピック

[外部 ID ソースとしての Active Directory \(379 ページ\)](#)

[Active Directory でサポートされる認証プロトコルおよび機能 \(379 ページ\)](#)

[許可ポリシーで使用する Active Directory 属性およびグループの取得 \(380 ページ\)](#)

[証明書ベース認証の Active Directory 証明書の取得 \(381 ページ\)](#)

[Active Directory ユーザ認証プロセス フロー \(382 ページ\)](#)

- [Active Directory マルチドメイン フォレストのサポート \(382 ページ\)](#)
- [Active Directory の複数参加設定のサポート \(393 ページ\)](#)
- [Cisco ISE 2.x の Active Directory の主な機能](#)
- [外部 ID ソースとして Active Directory を設定するためのガイドライン](#)
- [Active Directory の問題の診断 \(400 ページ\)](#)
- [Active Directory デバッグ ログの有効化 \(401 ページ\)](#)
- [トラブルシューティング用の Active Directory ログ ファイルの入手 \(401 ページ\)](#)
- [Active Directory の高度な調整 \(402 ページ\)](#)

Active Directory 参加ポイントの追加および参加ポイントへの Cisco ISE ノードの参加

始める前に

Cisco ISE ノードが、NTP サーバ、DNS サーバ、ドメインコントローラ、グローバル カタログ サーバが配置されているネットワークと通信できることを確認します。ドメイン診断ツールを実行して、これらのパラメータをチェックできます。

Active Directory と、パッシブ ID ワーク センターのエージェント、syslog、SPAN、およびエンドポイントの各プローブを使用するには、参加ポイントを作成する必要があります。

ステップ 1 [管理 (Administration)] > [ID の管理 (Identity Management)] > [外部 ID ソース (External Identity Sources)] > [Active Directory] を選択します。

ステップ 2 [追加 (Add)] をクリックして、Active Directory 参加ポイント名設定のドメイン名と ID ストア名を入力します。

ステップ 3 [送信 (Submit)] をクリックします。

新しく作成された参加ポイントがドメインに参加させるかどうかを確認するポップアップウィンドウが表示されます。すぐに参加させる場合は [はい (Yes)] をクリックします。

[いいえ (No)] をクリックした場合、設定を保存すると、Active Directory ドメインの設定が (プライマリおよびセカンダリのポリシー サービス ノードに) グローバルに保存されますが、いずれの Cisco ISE ノードもまだドメインに参加しません。

ステップ 4 作成した新しい Active Directory 参加ポイントの横にあるチェックボックスをオンにして [編集 (Edit)] をクリックするか、または左側のナビゲーションペインから新しい Active Directory 参加ポイントをクリックします。展開の参加/脱退テーブルに、すべての Cisco ISE ノード、ノードのロール、およびそのステータスが表示されます。

ステップ 5 関連する Cisco ISE ノードの横にあるチェックボックスをオンにし、[参加 (Join)] をクリックして Active Directory ドメインに Cisco ISE ノードを参加させます。

設定を保存した場合も、これを明示的に実行する必要があります。1 回の操作で複数の Cisco ISE ノードをドメインに参加させるには、使用するアカウントのユーザ名とパスワードがすべての参加操作で同じである必要があります。各 Cisco ISE ノードを追加するために異なるユーザ名とパスワードが必要な場合は、Cisco ISE ノードごとに参加操作を個別に実行する必要があります。

ステップ 6 表示される [ドメインへの参加 (Join Domain)] ダイアログボックスで Active Directory のユーザ名とパスワードを入力します。

[クレデンシャルの保存 (Store Credentials)] を選択することを強く推奨します。これにより、管理者のユーザ名とパスワードが保存され、モニタ対象として設定されているすべてのドメインコントローラ (DC) に使用されます。

参加操作に使用するユーザは、ドメイン自体に存在する必要があります。ユーザが異なるドメインまたはサブドメインに存在する場合、ユーザ名は `jdoe@acme.com` のように、UPN 表記で表記する必要があります。

ステップ 7 (任意) [組織ユニットの指定 (Specify Organizational Unit)] チェックボックスをオンにします。

このチェックボックスは、Cisco ISE ノードのマシン アカウントを

CN=Computers,DC=someDomain,DC=someTLD 以外の特定の組織ユニットに配置する場合に、オンにする必要があります。Cisco ISE は、指定された組織ユニットの下にマシンアカウントを作成するか、またはマシンアカウントがすでにある場合は、この場所に移動します。組織ユニットが指定されない場合、Cisco ISE はデフォルトの場所を使用します。値は完全識別名 (DN) 形式で指定する必要があります。構文は、Microsoft のガイドラインに準拠する必要があります。特別な予約文字 (/+,=, < など)、改行、スペース、およびキャリッジリターンは、バックスラッシュ (\) によってエスケープする必要があります。たとえば、OU=Cisco ISE\US,OU=IT Servers,OU=Servers\ や Workstations,DC=someDomain,DC=someTLD のようにします。マシンアカウントがすでに作成されている場合、このチェックボックスをオンにする必要はありません。Active Directory ドメインに参加したマシンアカウントのロケーションを後で変更することもできます。

ステップ 8 [OK] をクリックします。

Active Directory ドメインに参加する複数のノードを選択できます。

参加操作に失敗した場合、失敗メッセージが表示されます。各ノードの失敗メッセージをクリックして、そのノードの詳細なログを表示します。

(注) 参加が完了すると、Cisco ISE によりその AD グループと対応する SIDS が更新されます。Cisco ISE は自動的に SID の更新プロセスを開始します。このプロセスを完了できるようにする必要があります。

(注) DNS SRV レコードが欠落している (参加しようとしているドメインに対し、ドメインコントローラが SRV レコードをアドバタイズしない) 場合は、Active Directory ドメインに Cisco ISE を参加させることができない可能性があります。トラブルシューティング情報については、次の Microsoft Active Directory のマニュアルを参照してください。

- <http://support.microsoft.com/kb/816587>
- <http://technet.microsoft.com/en-us/library/bb727055.aspx>

次のタスク

[Active Directory ユーザ グループの設定 \(390 ページ\)](#)

認証ドメインを設定します。

ドメインコントローラの追加

- ステップ 1** [ワーク センター (Work Centers)] > [PassiveID] > [プロバイダー (Providers)] を選択し、左側のパネルから [Active Directory] を選択します。
- ステップ 2** 作成した Active Directory 参加ポイントの隣にあるチェックボックスをオンにし、[編集 (Edit)] をクリックします。展開の参加/脱退テーブルが、すべての Cisco ISE ノード、ノードのロール、およびそのステータスとともに表示されます。詳細については、[表 17:\[Active Directory 参加/脱退 \(Active Directory Join/Leave\)\] テーブル \(430 ページ\)](#) を参照してください。
- ステップ 3** (注) パッシブ ID サービスの新しいドメイン コントローラ (DC) を追加するには、その DC のログイン クレデンシャルが必要です。

[PassiveID] タブに移動し、[DC の追加 (Add DCs)] をクリックします。

- ステップ 4** モニタ対象として参加ポイントに追加するドメイン コントローラの隣にあるチェックボックスをオンにし、[OK] をクリックします。
ドメイン コントローラが [PassiveID] タブの [ドメイン コントローラ (Domain Controllers)] リストに表示されます。
- ステップ 5** ドメイン コントローラを設定します。
- ドメイン コントローラをオンにし、[編集 (Edit)] をクリックします。[アイテムの編集 (Edit Item)] 画面が表示されます。
 - 必要に応じて、各種ドメインコントローラフィールドを編集します。詳細については、[Active Directory の設定 \(429 ページ\)](#) を参照してください。
 - WMI プロトコルを選択した場合は、[設定 (Configure)] をクリックして WMI を自動的に設定するか、または [テスト (Test)] をクリックして接続をテストします。WMI の自動設定の詳細については、[WMI の設定 \(388 ページ\)](#) を参照してください。

WMI の設定

- ステップ 1** [管理 (Administration)] > [ID の管理 (Identity Management)] > [外部 ID ソース (External Identity Sources)] > [Active Directory] を選択します。
- ステップ 2** 作成した Active Directory 参加ポイントの隣にあるチェックボックスをオンにし、[編集 (Edit)] をクリックします。展開の参加/脱退テーブルが、すべての Cisco ISE ノード、ノードのロール、およびそのステータスとともに表示されます。詳細については、[表 17:\[Active Directory 参加/脱退 \(Active Directory Join/Leave\)\] テーブル \(430 ページ\)](#) を参照してください。
- ステップ 3** [パッシブ ID (Passive ID)] タブに移動し、該当するドメイン コントローラの隣にあるチェックボックスをオンにし、[WMI の設定 (Config WMI)] をクリックして、選択したドメイン コントローラが ISE により自動的に設定されるようにします。

Active Directory とドメイン コントローラを手動で設定する場合、または設定の問題のトラブルシューティングを行う場合は、[Active Directory と Cisco ISE の統合の前提条件](#)（382 ページ）を参照してください。

Active Directory ドメインの脱退

この Active Directory ドメインまたはこの参加ポイントからユーザとマシンを認証する必要がない場合は、Active Directory ドメインを脱退できます。

コマンドライン インターフェイスから Cisco ISE アプリケーション設定をリセットする場合、またはバックアップやアップグレードの後に設定を復元する場合、脱退操作が実行され、Cisco ISE ノードがすでに参加している場合は、Active Directory ドメインから切断されます。ただし、Cisco ISE ノードのアカウントは、Active Directory ドメインから削除されません。脱退操作では Active Directory ドメインからノード アカウントも削除されるため、脱退操作は管理者ポータルから Active Directory クレデンシャルを使用して実行することを推奨します。これは、Cisco ISE ホスト名を変更する場合にも推奨されます。

始める前に

Active Directory ドメインを脱退したが、認証の ID ソースとして（直接または ID ソース順序の一部として）Active Directory を使用している場合、認証が失敗する可能性があります。

ステップ 1 [管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [Active Directory] を選択します。

ステップ 2 作成した Active Directory 参加ポイントの隣にあるチェックボックスをオンにし、[編集（Edit）] をクリックします。展開の参加/脱退テーブルが、すべての Cisco ISE ノード、ノードのロール、およびそのステータスとともに表示されます。

ステップ 3 Cisco ISE ノードの隣にあるチェックボックスをオンにして [脱退（Leave）] をクリックします。

ステップ 4 Active Directory のユーザ名とパスワードを入力し、[OK] をクリックしてドメインを脱退し、Cisco ISE データベースからマシン アカウントを削除します。

Active Directory クレデンシャルを入力すると、Cisco ISE ノードは Active Directory ドメインを脱退し、Active Directory データベースから Cisco ISE マシン アカウントが削除されます。

（注） Active Directory データベースから Cisco ISE マシン アカウントを削除するには、ここに入力する Active Directory クレデンシャルに、ドメインからマシン アカウントを削除する権限がなければなりません。

ステップ 5 Active Directory クレデンシャルがない場合は、[使用可能なクレデンシャルなし（No Credentials Available）] チェックボックスをオンにして、[OK] をクリックします。

[クレデンシャルなしでドメインを脱退（Leave domain without credentials）] チェックボックスをオンにすると、プライマリ Cisco ISE ノードが Active Directory ドメインから脱退します。参加時に Active Directory で作成されたマシン アカウントは、Active Directory 管理者が手動で削除する必要があります。

認証ドメインの設定

Cisco ISE が参加しているドメインは、信頼関係を持つ他のドメインに対して可視性があります。デフォルトでは、Cisco ISE はこれらすべての信頼ドメインに対する認証を許可するように設定されます。認証ドメインのサブセットに対して、Active Directory 展開との相互作用を制限できます。ドメイン認証を設定することにより、接続ポイントごとに特定のドメインを選択して、選択されたドメインに対してのみ認証が実行されるようになります。認証ドメインでは、接続ポイントから信頼されたすべてのドメインではなく、選択されたドメインのユーザのみを認証するように Cisco ISE に指示するため、セキュリティが向上します。また、認証ドメインでは検索範囲（着信したユーザ名または ID に一致するアカウントの検索）が制限されるため、認証要求処理のパフォーマンスと遅延が改善されます。このことは、着信したユーザ名または ID にドメイン マークアップ（プレフィックスまたはサフィックス）が含まれていない場合に特に重要です。これらの理由から、認証ドメインを設定することをベストプラクティスとして強く推奨します。

ステップ 1 [管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [Active Directory] を選択します。

ステップ 2 [認証ドメイン（Authentication Domains）] タブをクリックします。

表に、信頼ドメインのリストが表示されます。デフォルトでは、Cisco ISE はすべての信頼ドメインに対する認証を許可します。

ステップ 3 指定したドメインのみを許可するには、[認証にすべての Active Directory ドメインを使用する（Use all Active Directory domains for authentication）] チェックボックスをオフにします。

ステップ 4 認証を許可するドメインの隣にあるチェックボックスをオンにし、[選択対象の有効化（Enable Selected）] をクリックします。[認証（Authenticate）] カラムで、このドメインのステータスが [はい（Yes）] に変わります。

また、選択したドメインを無効にすることもできます。

ステップ 5 [使用できないドメインを表示（Show Unusable Domains）] をクリックして、使用できないドメインのリストを表示します。使用できないドメインは、単方向の信頼や選択的な認証などの理由により、Cisco ISE が認証に使用できないドメインです。

次のタスク

Active Directory ユーザ グループを設定します。

Active Directory ユーザ グループの設定

Active Directory ユーザ グループを許可ポリシーで使えるようにするため、Active Directory ユーザ グループを作成する必要があります。内部的には、Cisco ISE はグループ名のあいまいさの問題を解決し、グループマッピングを向上させるためにセキュリティ ID（SID）を使用します。SID により、グループ割り当てが正確に一致します。

-
- ステップ 1** [管理 (Administration)] > [ID の管理 (Identity Management)] > [外部 ID ソース (External Identity Sources)] > [Active Directory] を選択します。
- ステップ 2** [グループ (Groups)] タブをクリックします。
- ステップ 3** 次のいずれかを実行します。
- a) [追加 (Add)] > [ディレクトリからグループを選択 (Select Groups From Directory)] を選択して、既存のグループを選択します。
 - b) [追加 (Add)] > [グループの追加 (Add Group)] を選択して、グループを手動で追加します。グループ名と SID の両方を指定するか、またはグループ名のみを指定し、[SID を取得 (Fetch SID)] を押します。
- ユーザ インターフェイス ログインのグループ名に二重引用符 (") を使用しないでください。
- ステップ 4** グループを手動で選択する場合は、フィルタを使用してグループを検索できます。たとえば、**admin*** をフィルタ基準として入力し、[グループの取得 (Retrieve Groups)] をクリックすると、**admin** で始まるユーザグループが表示されます。アスタリスク (*) ワイルドカード文字を入力して、結果をフィルタリングすることもできます。一度に取得できるのは 500 グループのみです。
- ステップ 5** 許可ポリシーで使用可能にするグループの隣にあるチェックボックスをオンにし、[OK] をクリックします。
- ステップ 6** グループを手動で追加する場合は、新しいグループの名前と SID を入力します。
- ステップ 7** [OK] をクリックします。
- ステップ 8** [保存 (Save)] をクリックします。
- (注) グループを削除し、そのグループと同じ名前で作成する場合は、[SID 値の更新 (Update SID Values)] をクリックして、新しく作成したグループに新しい SID を割り当てる必要があります。アップグレードすると、最初の参加の後に SID が自動的に更新されます。
-

次のタスク

Active Directory のユーザ属性を設定します。

Active Directory ユーザとマシンの属性の設定

許可ポリシーの条件でできるように Active Directory ユーザとマシンの属性を設定する必要があります。

-
- ステップ 1** [管理 (Administration)] > [ID の管理 (Identity Management)] > [外部 ID ソース (External Identity Sources)] > [Active Directory] を選択します。
- ステップ 2** [属性 (Attributes)] タブをクリックします。
- ステップ 3** [追加 (Add)] > [属性の追加 (Add Attribute)] を選択して属性を手動で追加するか、[追加 (Add)] > [ディレクトリから属性を選択 (Select Attributes From Directory)] を選択してディレクトリから属性のリストを選択します。

ステップ 4 ディレクトリからの属性の追加を選択した場合、ユーザの名前を[サンプルユーザ (Sample User)] フィールドまたは[マシンアカウント (Machine Account)] フィールドに入力し、[属性の取得 (Retrieve Attributes)] をクリックしてユーザの属性のリストを取得します。たとえば、管理者属性のリストを取得するには **administrator** を入力します。アスタリスク (*) ワイルドカード文字を入力して、結果をフィルタリングすることもできます。

(注) サンプルユーザ名を入力するときは、Cisco ISE が接続されている Active Directory ドメインからユーザを選択することを確認してください。マシン属性を取得するためにサンプルマシンを選択するときは、マシン名に「host/」というプレフィックスを付加するか、または **SAM\$** 形式を使用します。たとえば、host/myhost を使用します。属性の取得時に表示される値の例は説明のみを目的としており、保存されません。

ステップ 5 選択する Active Directory の属性の隣にあるチェックボックスをオンにし、[OK] をクリックします。

ステップ 6 属性を手動で追加する場合は、新しい属性の名前を入力します。

ステップ 7 [保存 (Save)] をクリックします。

パスワード変更、マシン認証、およびマシンアクセス制限の設定の変更

始める前に

Active Directory ドメインに Cisco ISE を参加させる必要があります。詳細については、[Active Directory 参加ポイントの追加および参加ポイントへの Cisco ISE ノードの参加 \(386 ページ\)](#) を参照してください。

ステップ 1 [管理 (Administration)] > [ID の管理 (Identity Management)] > [外部 ID ソース (External Identity Sources)] > [Active Directory] を選択します。

ステップ 2 該当する Cisco ISE ノードの隣にあるチェックボックスをオンにして [編集 (Edit)] をクリックします。

ステップ 3 [高度な設定 (Advanced Settings)] タブをクリックします。

ステップ 4 必要に応じて、パスワード変更、マシン認証、およびマシンアクセス制限 (MAR) の設定を変更します。これらのオプションはデフォルトで有効になっています。

ステップ 5 [ダイヤルインチェックを有効にする (Enable dial-in check)] チェックボックスをオンにして、認証中またはクエリ中にユーザのダイヤルインアクセス権をチェックします。ダイヤルインアクセス権が拒否されている場合は、チェックの結果により認証拒否の原因になります。

ステップ 6 認証中またはクエリ中にサーバからユーザにコールバックするようにするには、[ダイヤルインクライアントのコールバックチェックを有効にする (Enable callback check for dial-in clients)] チェックボックスをオンにします。サーバによって使用される IP アドレスまたは電話番号は、発信者またはネットワーク管理者によって設定されます。チェックの結果は、RADIUS 応答でデバイスに返されます。

ステップ 7 プレーンテキスト認証に Kerberos を使用する場合は、[プレーンテキスト認証に Kerberos を使用 (Use Kerberos for Plain Text Authentications)] チェックボックスをオンにします。デフォルトの推奨オプションは MS-RPC です。Kerberos は ISE 1.2 で使用されます。

マシン アクセス制限 (MAR) キャッシュの維持

Cisco ISE アプリケーション サービスを手動で停止すると、Cisco ISE は MAR キャッシュ コンテンツ、calling-station-ID リスト、および対応するタイムスタンプを、ローカルディスクのファイルに保存します。アプリケーション サービスを誤って再起動した場合、Cisco ISE はインスタンスの MAR キャッシュ エントリを保存しません。

Cisco ISE アプリケーション サービスが再起動した場合、Cisco ISE はキャッシュ エントリの存続時間に基づいて、ローカルディスクのファイルから MAR キャッシュ エントリを読み取ります。再起動後に Cisco ISE インスタンスのアプリケーション サービスが起動すると、Cisco ISE はそのインスタンスの現在の時刻と MAR キャッシュ エントリの時刻を比較します。現在の時刻と MAR エントリの時刻の差が MAR キャッシュ エントリの存続時間よりも大きい場合は、Cisco ISE はディスクからそのエントリを取得しません。それ以外の場合、Cisco ISE は MAR キャッシュ エントリを取得し、その MAR キャッシュ エントリの存続時間を更新します。

カスタム スキーマの設定

始める前に

Active Directory ドメインに Cisco ISE を参加させる必要があります。

ステップ 1 [管理 (Administration)] > [ID の管理 (Identity Management)] > [外部 ID ソース (External Identity Sources)] > [Active Directory] を選択します。

ステップ 2 参加ポイントを選択します。

ステップ 3 [高度な設定 (Advanced Settings)] タブをクリックします。

ステップ 4 [スキーマ (Schema)] セクションの [スキーマ (Schema)] ドロップダウンリストから [カスタム (Custom)] オプションを選択します。必要に応じて、ユーザ情報の属性を更新できます。これらの属性は、ユーザ情報 (名、姓、電子メール、電話番号、地域など) の収集に使用されます。

事前設定された属性は、Active Directory スキーマ (組み込みのスキーマ) に使用されます。事前定義されたスキーマの属性を編集すると、Cisco ISE が自動的にカスタム スキーマを作成します。

Active Directory の複数参加設定のサポート

Cisco ISE では、Active Directory ドメインへの複数参加がサポートされます。Cisco ISE では、50 までの Active Directory 参加がサポートされます。Cisco ISE は、双方向信頼がなく、相互の信頼がゼロである複数の Active Directory ドメインと接続できます。Active Directory の複数ドメイン参加は、各参加の独自のグループ、属性、および許可ポリシーを持つ個別の Active Directory ドメインのセットで構成されます。

同じフォレストに複数回参加できます。つまり、必要に応じて、同じフォレスト内の複数のドメインに参加できます。

Cisco ISE は、単方向の信頼があるドメインに参加できます。このオプションで、単方向の信頼によって生じる権限の問題を回避できます。いずれかの信頼ドメインに参加できるため、両方のドメインを確認できます。

- **参加ポイント**：Cisco ISE では、Active Directory ドメインへの個別参加は、参加ポイントと呼ばれます。Active Directory の参加ポイントは、Cisco ISE の ID ストアであり、認証ポリシーで使用できます。属性およびグループの関連ディクショナリがあり、許可条件で使用できます。
- **スコープ**：グループ化された Active Directory の参加ポイントのサブセットは、スコープと呼ばれます。単一参加ポイントの代わりに、認証結果として認証ポリシーでスコープを使用できます。スコープは、複数の参加ポイントに対してユーザを認証するために使用されます。各参加ポイントに複数のルールを使用する代わりにスコープを使用すると、単一のルールで同じポリシーを作成することができ、Cisco ISE で要求の処理やパフォーマンスの向上にかかる時間を短縮できます。参加ポイントには、複数のスコープが含まれる場合があります。スコープは、ID ソース順序に含まれる場合があります。スコープには関連するディクショナリがないため、許可ポリシー条件にスコープを使用することはできません。

新しい Cisco ISE のインストールを実行する場合、デフォルトでスコープは存在しません。これは、ノー スコープ モードと呼ばれます。スコープを追加すると、Cisco ISE はマルチスコープモードになります。必要に応じて、ノー スコープ モードに戻すことができます。すべての参加ポイントは [Active Directory] フォルダに移動されます。

- **Initial_Scope** は、ノー スコープ モードで追加された Active Directory 参加ポイントの格納に使用される暗黙のスコープです。マルチスコープモードを有効にすると、すべての Active Directory 参加ポイントが自動作成された Initial_Scope に移動します。Initial_Scope の名前を変更できます。
- **All_AD_Instances** は組み込み型の疑似スコープで、Active Directory 設定には表示されません。これは、認証結果としてポリシーおよび ID 順序にのみ示されます。Cisco ISE で設定されたすべての Active Directory 参加ポイントを選択する場合は、このスコープを選択できます。

Active Directory 参加ポイントを追加する新しい範囲の作成

ステップ 1 [管理 (Administration)] > [ID の管理 (Identity Management)] > [外部 ID ソース (External Identity Sources)] > [Active Directory] を選択します。

ステップ 2 [範囲モード (Scope Mode)] をクリックします。
Initial_Scope と呼ばれるデフォルトの範囲が作成され、現在のすべての参加ポイントがこの範囲に配置されます。

ステップ 3 より多くの範囲を作成するには、[追加 (Add)] をクリックします。

ステップ 4 新しい範囲の名前と説明を入力します。

ステップ 5 [送信 (Submit)] をクリックします。

ID 書き換え

ID 書き換えは、外部 Active Directory システムに渡される前に ID を操作するよう Cisco ISE に指示する拡張機能です。ID を必要な形式（任意のドメインプレフィックスやサフィックスまたはその他の追加マークアップを含むまたは除く）に変更するためのルールを作成できます。

ID 書き換えルールは、サブジェクト検索、認証クエリー、許可クエリーなどの操作のために、クライアントから受信したユーザ名またはホスト名に対して Active Directory に渡される前に適用されます。Cisco ISE は条件のトークンを照合し、最初の 1 つが一致するとポリシーの処理を停止して、結果に応じて ID 文字列を書き換えます。

書き換え時、角カッコ [] で囲まれている ([IDENTITY] など) 内容はすべて、評価側では評価されず、代わりに文字列内のその場所に一致する文字列が付加される変数です。角カッコなしはすべて、ルールの評価側と書き換え側の両方で、固定文字列として評価されます。

次に、ユーザによって入力された ID が ACME\jdoe であるとした場合の ID 書き換えの例を示します。

- ID が ACME\[IDENTITY] と一致する場合、[IDENTITY] に書き換えます。

結果は jdoe です。このルールは、ACME プレフィックスを持つすべてのユーザ名を削除するよう Cisco ISE に指示します。

- ID が ACME\[IDENTITY] と一致する場合、[IDENTITY]@ACME.com に書き換えます。

結果は jdoe@ACME.com です。このルールは、形式をプレフィックス表記からサフィックス表記に、または NetBIOS 形式から UPN 形式に変更するよう Cisco ISE に指示します。

- ID が ACME\[IDENTITY] と一致する場合、ACME2\[IDENTITY] に書き換えます。

結果は ACME2\jdoe です。このルールは、特定のプレフィックスを持つすべてのユーザ名を代替プレフィックスに変更するよう Cisco ISE に指示します。

- ID が [ACME]\jdoe.USA と一致する場合、[IDENTITY]@[ACME].com に書き換えます。

結果は jdoe\ACME.com です。このルールは、ドットの後の領域を削除するよう Cisco ISE に指示します。この場合は国名で、正しいドメインに置き換えられます。

- ID が E=[IDENTITY] と一致する場合、[IDENTITY] に書き換えます。

結果は jdoe です。これは、ID が証明書から取得され、フィールドが電子メール アドレスで、Active Directory がサブジェクトで検索するように設定されている場合に作成可能なルールの例です。このルールは、「E=」を削除するように Cisco ISE に指示します。

- ID が E=[EMAIL],[DN] と一致する場合、[DN] に書き換えます。

このルールは、証明書サブジェクトを、E=jdoe@acme.com、CN=jdoe、DC=acme、DC=com から単なる DN、CN=jdoe、DC=acme、DC=com に変換します。これは、ID が証明書サブジェクトから取得され、Active Directory が DN でユーザ検索するように設定されている場合に作成可能なルールの例です。このルールは、電子メールプレフィックスを削除し、DN を生成するよう Cisco ISE に指示します。

次に、ID 書き換えルールを記述する際によくある間違いを示します。

- ID が [DOMAIN]\[IDENTITY] と一致する場合、[IDENTITY]@DOMAIN.com に書き換えます。

結果は jdoe@DOMAIN.com です。このルールは、ルールの書き換え側の角カッコ [] に [DOMAIN] がありません。

- ID が DOMAIN\[IDENTITY] と一致する場合、[IDENTITY]@[DOMAIN].com に書き換えます。

この場合も、結果は jdoe@DOMAIN.com です。このルールは、ルールの評価側の角カッコ [] に [DOMAIN] がありません。

ID 書き換えルールは、常に、Active Directory 参加ポイントのコンテキスト内で適用されます。認証ポリシーの結果としてスコープが選択されている場合でも、書き換えルールは、各 Active Directory 参加ポイントに適用されます。EAP-TLS が使用されている場合、これらの書き換えルールは、証明書から取得される ID にも適用されます。

ID 書き換えの有効化



(注) この設定タスクは任意です。あいまいな識別エラーなどのさまざまな理由で発生する認証失敗を減らすために実行できます。

始める前に

Active Directory ドメインに Cisco ISE を参加させる必要があります。

ステップ 1 [管理 (Administration)] > [ID の管理 (Identity Management)] > [外部 ID ソース (External Identity Sources)] > [Active Directory] を選択します。

ステップ 2 [高度な設定 (Advanced Settings)] タブをクリックします。

ステップ 3 [ID 書き換え (Identity Rewrite)] セクションで、ユーザ名を変更する書き換えルールを適用するかどうかを選択します。

ステップ 4 一致条件および書き換え結果を入力します。表示されるデフォルトルールを削除し、要件に応じてルールを入力できます。Cisco ISE は順番にポリシーを処理し、要求ユーザ名に一致する最初の条件が適用されます。一致トークン (角カッコ内に含まれるテキスト) を使用して、元のユーザ名の要素を結果に転送できます。いずれのルールにも一致しない場合、識別名は変更されません。[テスト開始 (Launch Test)] ボタンをクリックして、書き換え処理をプレビューできます。

ID 解決の設定

一部のタイプの ID には、プレフィックスまたはサフィックスのようなドメイン マークアップが含まれます。たとえば、ACME\jdoe などの NetBIOS ID では、「ACME」がドメイン マークアップのプレフィックスで、同様に jdoe@acme.com などの UPN ID では、「acme.com」がドメイ

ン マークアップのサフィックスです。ドメイン プレフィックスは、組織内の Active Directory ドメインの NetBIOS (NTLM) 名に一致し、ドメインサフィックスは、組織内の Active Directory ドメインの DNS 名または代替 UPN サフィックスに一致する必要があります。たとえば、gmail.com は Active Directory ドメインの DNS 名ではないため、jdoe@gmail.com はドメインマークアップなしとして処理されます。

ID 解決設定では、Active Directory 展開に一致するように、セキュリティおよびパフォーマンスのバランスを調整する重要な設定を指定できます。これらの設定を使用して、ドメインマークアップのないユーザ名およびホスト名の認証を調整できます。Cisco ISE でユーザのドメインを認識できない場合、すべての認証ドメインでユーザを検索するように設定できます。ユーザが 1 つのドメインで見つかった場合でも、Cisco ISE は ID のあいまいさがなく確実にするために、すべての応答を待ちます。この処理は、ドメインの数、ネットワークの遅延、負荷などに応じて、時間がかかる場合があります。

ID 解決問題の回避

認証時に、ユーザおよびホストに完全修飾名（つまり、ドメインマークアップが含まれている名前）を使用することを強く推奨します。たとえば、ユーザの UPN と NetBIOS 名、およびホストの FQDN SPN です。これは、複数の Active Directory アカウントが受信ユーザ名と一致する（たとえば、jdoe が jdoe@emea.acme.com および jdoe@amer.acme.com と一致する）など、あいまいエラーが頻繁に生じる場合に特に重要です。場合によっては、完全修飾名を使用することが、問題を解決する唯一の方法になります。また、ユーザに一意のパスワードが設定されていることを保証するだけで十分な場合もあります。したがって、一意の ID を最初から使用すると、効率が向上し、パスワード ロックアウトの問題が減少します。

ID 解決の設定



(注) この設定タスクは任意です。あいまいな識別エラーなどのさまざまな理由で発生する認証失敗を減らすために実行できます。

始める前に

Active Directory ドメインに Cisco ISE を参加させる必要があります。

ステップ 1 [管理 (Administration)] > [ID の管理 (Identity Management)] > [外部 ID ソース (External Identity Sources)] > [Active Directory] を選択します。

ステップ 2 [高度な設定 (Advanced Settings)] タブをクリックします。

ステップ 3 [ID 解決 (Identity Resolution)] セクションで、ユーザ名またはマシン名の ID 解決についての次の設定を定義します。この設定によって、ユーザの検索と認証を詳細に制御できます。

最初に、マークアップなしの ID に対する設定を行います。このような場合、次のオプションのいずれかを選択できます。

- [要求を拒否する (Reject the request)] : このオプションを使用すると、SAM 名などのドメインマークアップがないユーザの認証は失敗します。このことは、複数参加ドメインで、Cisco ISE がすべての参加グローバル カタログの ID を検索する必要があることによって、安全性が低下する可能性がある場合に役立ちます。このオプションによって、ドメインマークアップを含むユーザ名を使用することがユーザに対して強制されます。
- [結合されたフォレストの「認証ドメイン」のみで検索する (Only search in the “Authentication Domains” from the joined forest)] : このオプションを使用すると、認証ドメインの セクションで指定した、結合ポイントのフォレスト内のドメインのみで ID が検索されます。これはデフォルト オプションであり、SAM アカウント名に対する Cisco ISE 1.2 の動作と同じです。
- [すべての「認証ドメイン」セクションで検索する (Search in all the “Authentication Domains” sections)] : このオプションを使用すると、すべての信頼されたフォレストのすべての認証ドメインで ID が検索されます。これにより、遅延が増加し、パフォーマンスに影響する可能性があります。

Cisco ISE で認証ドメインがどのように設定されているかに基づいて選択します。特定の認証ドメインのみを選択した場合は、それらのドメインのみが検索されます（「結合されたフォレスト」と「すべてのフォレスト」のいずれを選択した場合も）。

2 番目の設定は、Cisco ISE が、[認証ドメイン (Authentication Domains)] セクションで指定された設定に準拠するために必要となるすべてのグローバル カタログ (GC) と通信できない場合に使用します。このような場合、次のオプションのいずれかを選択できます。

- [使用可能なドメインで続行する (Proceed with available domains)] : このオプションを使用すると、使用できないいずれかのドメインで一致が見つかった場合に認証が続行されます。
- [要求をドロップする (Drop the request)] : このオプションを使用すると、ID 解決で到達不能または使用できないドメインが検出された場合に認証要求がドロップされます。

Active Directory 認証のためのユーザのテスト

Active Directory からユーザ認証を検証するには、[ユーザのテスト (Test User)] ツールを使用できます。グループおよび属性を取得して調査することもできます。単一の参加ポイントまたは範囲のテストを実行できます。

ステップ 1 [管理 (Administration)] > [ID の管理 (Identity Management)] > [外部 ID ソース (External Identity Sources)] > [Active Directory] を選択します。

ステップ 2 次のいずれかのオプションを選択します。

- すべての参加ポイントのテストを実行するには、[拡張ツール (Advanced Tools)] > [すべての参加ポイントのユーザをテスト (Test User for All Join Points)] を選択します。
- 特定の参加ポイントのテストを実行するには、参加ポイントを選択し、[編集 (Edit)] をクリックします。Cisco ISE ノードを選択し、[ユーザのテスト (Test User)] をクリックします。

ステップ 3 Active Directory のユーザ（またはホスト）のユーザ名とパスワードを入力します。

ステップ 4 認証タイプを選択します。ステップ 3 のパスワード入力は、ルックアップ オプションを選択する場合には必要ありません。

- ステップ 5** すべての参加ポイントに対してこのテストを実行する場合は、このテストを実行する Cisco ISE ノードを選択します。
- ステップ 6** Active Directory からグループおよび属性を取得するには、[グループを取得 (Retrieve Groups)] および [属性の取得 (Retrieve Attributes)] チェック ボックスにチェックを付けます。
- ステップ 7** [テスト (Test)] をクリックします。
テスト操作の結果と手順が表示されます。手順で失敗の原因を特定し、トラブルシューティングできます。
また、Active Directory がそれぞれの処理手順（認証、参照、グループおよび属性の取得）を実行するのに要する時間（ミリ秒単位）を表示することもできます。操作にかかる時間がしきい値を超えると、Cisco ISE に警告メッセージが表示されます。

Active Directory の設定の削除

Active Directory を外部 ID ソースとして使用しない場合は、Active Directory の設定を削除する必要があります。別の Active Directory ドメインに参加する場合は、設定を削除しないでください。現在参加しているドメインから脱退し、新しいドメインに参加できます。

始める前に

Active Directory ドメインが残っていることを確認します。

-
- ステップ 1** [管理 (Administration)] > [ID の管理 (Identity Management)] > [外部 ID ソース (External Identity Sources)] > [Active Directory] を選択します。
- ステップ 2** 設定された Active Directory の横のチェックボックスをオンにします。
- ステップ 3** [ローカル ノード ステータス (Local Node Status)] が [参加していない (Not Joined)] としてリストされていることを確認します。
- ステップ 4** [削除 (Delete)] をクリックします。
Active Directory データベースから設定を削除しました。後で Active Directory を使用する場合は、有効な Active Directory の設定を再送信できます。

ノードの Active Directory の参加の表示

特定の Cisco ISE ノードのすべての Active Directory 参加ポイントのステータスまたはすべての Cisco ISE ノードのすべての参加ポイントのリストを表示するには、[Active Directory] ページの [ノード ビュー (Node View)] ボタンを使用できます。

-
- ステップ 1** [管理 (Administration)] > [ID の管理 (Identity Management)] > [外部 ID ソース (External Identity Sources)] > [Active Directory] を選択します。
- ステップ 2** [ノード ビュー (Node View)] をクリックします。

- ステップ 3** [ISE Node (ISE ノード)] ドロップダウン リストからノードを選択します。
テーブルに、Active Directory のステータスがノード別に一覧されます。展開に複数の参加ポイントと複数の Cisco ISE ノードがある場合、このテーブルが更新されるまでに数分かかる場合があります。
- ステップ 4** その Active Directory 参加ポイントのページに移動し、その他の特定のアクションを実行するには、参加ポイントの [名前 (Name)] リンクをクリックします。
- ステップ 5** [診断ツール (Diagnostic Tools)] ページに移動して特定の問題のトラブルシューティングを行うには、[診断概要 (Diagnostic Summary)] 列のリンクをクリックします。診断ツールでは、ノードごとに各参加ポイントの最新の診断結果が表示されます。
-

Active Directory の問題の診断

診断ツールは、各 Cisco ISE ノードで実行されるサービスです。診断ツールを使用して、Active Directory 展開を自動的にテストおよび診断したり、Cisco ISE によって Active Directory が使用される場合に機能やパフォーマンスの障害の原因となる可能性がある問題を検出するための一連のテストを実行したりすることができます。

Cisco ISE が Active Directory に参加できない、または Active Directory に対して認証できない理由は、複数あります。このツールは、Cisco ISE を Active Directory に接続するための前提条件が正しく設定されていることを確認するのに役立ちます。また、ネットワーク、ファイアウォール設定、クロック同期、ユーザ認証などの問題の検出に役立ちます。このツールは、手順をステップごとに説明したガイドとして機能し、必要に応じて、中間の各レイヤの問題の修正を支援します。

- ステップ 1** [管理 (Administration)] > [ID の管理 (Identity Management)] > [外部 ID ソース (External Identity Sources)] > [Active Directory] を選択します。
- ステップ 2** [拡張ツール (Advanced Tools)] ドロップダウン リストをクリックし、[診断ツール (Diagnostic Tools)] を選択します。
- ステップ 3** 診断を実行する Cisco ISE ノードを選択します。
Cisco ISE ノードを選択しない場合は、すべてのノードでテストが実行されます。
- ステップ 4** 特定の Active Directory 参加ポイントを選択します。
Active Directory 参加ポイントを選択しない場合は、すべての参加ポイントでテストが実行されます。
- ステップ 5** [ノードに対するすべてのテストを実行 (Run All Tests on Node)] をクリックして、テストを開始します。
- ステップ 6** 警告ステータスまたは失敗ステータスのテストの詳細を確認するには、[テストの詳細の表示 (View Test Details)] をクリックします。
このテーブルを使用して、特定のテストの再実行、実行中のテストの停止、特定のテストのレポートの表示を行うことができます。
-

Active Directory デバッグ ログの有効化

Active Directory デバッグ ログはデフォルトでは記録されません。展開でポリシー サービス ペルソナを担当する Cisco ISE ノードでこのオプションを有効にする必要があります。Active Directory のデバッグ ログを有効にすると、ISE のパフォーマンスに影響する場合があります。

-
- ステップ 1** [管理 (Administration)] > [システム (System)] > [ロギング (Logging)] > [デバッグ ログの設定 (Debug Log Configuration)] を選択します。
- ステップ 2** Active Directory のデバッグ情報を取得する Cisco ISE ポリシー サービス ノードの隣のオプション ボタンをクリックし、[編集 (Edit)] をクリックします。
- ステップ 3** [Active Directory] オプション ボタンをクリックし、[編集 (Edit)] をクリックします。
- ステップ 4** [Active Directory] の隣にあるドロップダウン リストから [DEBUG] を選択します。これにはエラー、警告、および verbose ログが含まれます。完全なログを取得するには、[TRACE] を選択します。
- ステップ 5** [保存 (Save)] をクリックします。
-

トラブルシューティング用の Active Directory ログ ファイルの入手

可能性がある問題をトラブルシューティングするには、Active Directory のデバッグ ログをダウンロードし、表示します。

始める前に

Active Directory のデバッグ ロギングを有効にする必要があります。

-
- ステップ 1** [操作 (Operations)] > [トラブルシューティング (Troubleshoot)] > [ログのダウンロード (Download Logs)] を選択します。
- ステップ 2** Active Directory のデバッグ ログ ファイルを取得するノードをクリックします。
- ステップ 3** [デバッグ ログ (Debug Logs)] タブをクリックします。
- ステップ 4** このページを下にスクロールして ad_agent.log ファイルを見つけます。このファイルをクリックしてダウンロードします。
-

Active Directory のアラームおよびレポート

Cisco ISE は、Active Directory に関連するアクティビティをモニタリングし、トラブルシューティングを実行するためのさまざまなアラームおよびレポートを提供します。

アラーム

Active Directory のエラーおよび問題に対して、次のアラームがトリガーされます。

- 構成済みネーム サーバが使用不可 (Configured nameserver not available)
- 参加しているドメインが使用不可 (Joined domain is unavailable)
- 認証ドメインが使用不可 (Authentication domain is unavailable)
- Active Directory フォレストが使用不可 (Active Directory forest is unavailable)
- AD コネクタを再起動する必要があります (AD Connector had to be restarted)
- AD : ISE アカウント パスワードの更新に失敗 (AD: ISE account password update failed)
- AD : マシン TGT のリフレッシュに失敗 (AD: Machine TGT refresh failed)

レポート

次の 2 つのレポートで Active Directory に関連するアクティビティをモニタリングできます。

- **RADIUS 認証レポート** : このレポートは、Active Directory の認証および許可の詳細な手順を示します。このレポートは、**[操作 (Operations)] > [レポート (Reports)] > [認証サービス ステータス (Auth Services Status)] > [RADIUS 認証 (RADIUS Authentications)]** にあります。
- **AD コネクタ操作レポート** : AD コネクタ操作レポートは、AD コネクタが実行するバックグラウンド操作 (Cisco ISE サーバパスワードのリフレッシュ、Kerberos チケットの管理、DNS クエリー、DC 検出、LDAP、および RPC 接続管理など) のログを提供します。Active Directory の障害が発生した場合は、考えられる原因を特定するために、このレポートで詳細を確認できます。このレポートは、**[操作 (Operations)] > [レポート (Reports)] > [認証サービス ステータス (Auth Services Status)] > [AD コネクタ操作 (AD Connector Operations)]** にあります。

Active Directory の高度な調整

高度な調整機能により、シスコのサポート担当者の管理下で、サポート操作に使用されるノード固有の設定が可能となり、システムのさらに深いレベルでパラメータを調整できるようになります。これらの設定は、通常の管理フローを対象としていません。ガイダンスに従って使用する必要があります。

Active Directory アイデンティティ検索属性

Cisco ISE は、SAM と CN のいずれか、または両方の属性を使用してユーザを識別します。Cisco ISE リリース 2.2 パッチ 5 以降、および 2.3 パッチ 2 以降は、sAMAccountName 属性をデフォルトの属性として使用します。これ以前のリリースでは、SAM と CN の両方の属性がデフォルトで検索されていました。この動作はリリース 2.2 パッチ 5 以降と 2.3 パッチ 2 以降で、[CSCv21978](#) バグ修正の一部として変更されました。これらのリリースでは、sAMAccountName 属性のみがデフォルトの属性として使用されます。

実際の環境で必要に応じて、SAM と CN のいずれか、または両方を使用するように Cisco ISE を設定できます。SAM および CN が使用される場合、SAMAccountName 属性の値が一意でない、Cisco ISE は CN 属性値も比較します。

Active Directory アイデンティティ検索の属性の設定

1. [管理 (Administration)] > [IDの管理 (Identity Management)] > [外部IDソース (External Identity Sources)] > [Active Directory] を選択します。[Active Directory] ウィンドウで、[拡張ツール (Advanced Tools)] をクリックし、[高度な調整 (Advanced Tuning)] を選択します。次の詳細を入力します。

- [ISE ノード (ISE Node)] : Active Directory に接続される ISE ノードを選択します。
- [名前 (Name)] : 変更するレジストリ キーを入力します。Active Directory 検索属性を変更するには、
`REGISTRY.Services\lsass\Parameters\Providers\ActiveDirectory\IdentityLookupField` と入力します。
- 値 : ユーザを識別するために ISE で使用する属性を入力します。
 - SAM : クエリで SAM のみを使用します (このオプションがデフォルトです)。
 - CN : クエリで CN のみを使用します。
 - SAMCN : クエリで CN と SAM を使用します。
- コメント : 変更内容を記述します (たとえば「デフォルト動作を SAM および CN に変更」)。

2. [値の更新 (Update Value)] をクリックしてレジストリを更新します。

ポップアップウィンドウが表示されます。メッセージを読み取り、変更を受け入れます。ISE の AD コネクタ サービスが再起動します。

検索文字列の例

次の例では、ユーザ名が userd2only であると想定します。

- SAM 検索文字列 :

```
filter=[(&(| (objectCategory=person) (objectCategory=computer)) (| (cn=userd2only) (sAMAccountName=userd2only)))]
```

- SAM および CN 検索文字列 :

```
filter=[(&(| (objectCategory=person) (objectCategory=computer)) (sAMAccountName=userd2only)))]
```

Active Directory が構成された Cisco ISE をセットアップするための補足情報

Active Directory が構成された Cisco ISE を設定するには、グループ ポリシーを設定し、マシン認証のサブリカントを設定する必要があります。

Active Directory のグループ ポリシーの設定

グループポリシー管理エディタにアクセスする方法の詳細については、Microsoft Active Directory のマニュアルを参照してください。

ステップ 1 次の図に示すように、グループポリシー管理エディタを開きます。

[グループポリシー オブジェクト (Group Policy Objects)] の選択



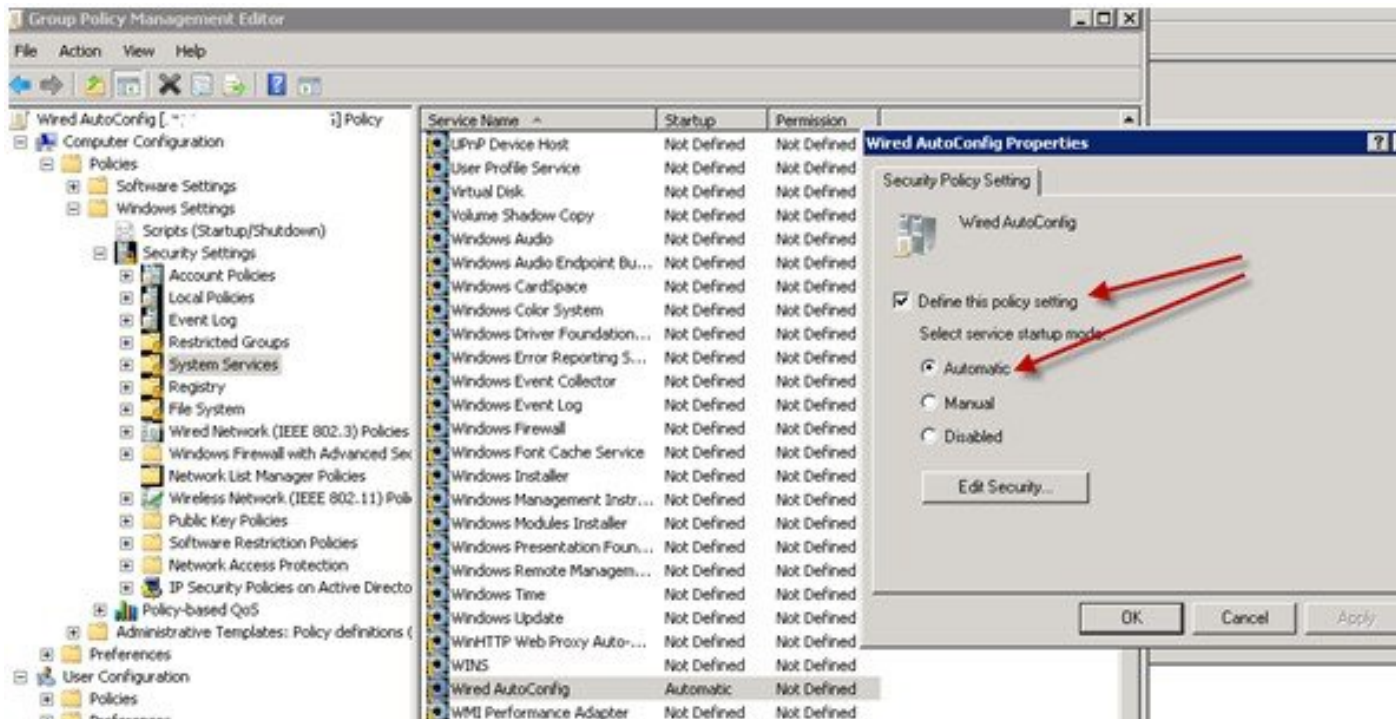
ステップ 2 新しいポリシーを作成し、その説明的な名前を入力するか、既存のドメイン ポリシーに追加します。

例：

次の例では、ポリシー名に Wired Autoconfiguration を使用しています。

ステップ 3 次の図に示すように、[このポリシー設定を定義する (Define this policy setting)] チェックボックスをオンにして、サービス起動モードの [自動 (Automatic)] オプション ボタンをクリックします。

ポリシー プロパティ



ステップ 4 目的の組織ユニットまたはドメイン Active Directory レベルでポリシーを適用します。

コンピュータは再起動したときにポリシーを受信し、このサービスが有効になります。

Active Directory に対する EAP-TLS マシン認証のための Odyssey 5.X サプリカントの設定

Active Directory に対する EAP-TLS マシン認証に Odyssey 5.x サプリカントを使用している場合は、サプリカントで次の設定を行う必要があります。

ステップ 1 Odyssey アクセス クライアントを起動します。

ステップ 2 [ツール (Tools)] メニューから [Odyssey アクセス クライアント管理者 (Odyssey Access Client Administrator)] を選択します。

ステップ 3 [マシン アカウント (Machine Account)] アイコンをダブルクリックします。

ステップ 4 [マシン アカウント (Machine Account)] ページから、EAP-TLS 認証のプロファイルを設定する必要があります。

- a) [設定 (Configuration)] > [プロファイル (Profiles)] を選択します。
- b) EAP-TLS プロファイルの名前を入力します。
- c) [認証 (Authentication)] タブで、認証方式として [EAP-TLS] を選択します。
- d) [証明書 (Certificate)] タブで、[証明書を使用したログインを許可 (Permit login using my certificate)] チェックボックスをオンにして、サプリカント マシンの証明書を選択します。
- e) [ユーザ情報 (User Info)] タブで、[マシン クレデンシヤルを使用 (Use machine credentials)] チェックボックスをオンにします。

このオプションが有効になっている場合、Odyssey サプリカントは `host\<machine_name>` の形式でマシン名を送信します。Active Directory は要求をマシンから送信されていると識別し、認証を実行するコンピュータ オブジェクトを検索します。このオプションが無効になっている場合、Odyssey サプリカントは `host\` プレフィクスなしでマシン名を送信します。Active Directory はユーザ オブジェクトを検索し、認証は失敗します。

マシン認証のための AnyConnect エージェント

マシン認証のために AnyConnect エージェントを設定する場合、次のいずれかを実行できます。

- デフォルトのマシン ホスト名 (プレフィクス「host/」を含む) を使用する。
- 新しいプロファイルを設定する。その場合、マシン名の前にプレフィクス「host/」を付加する必要があります。

Active Directory で Easy Connect および パッシブ ID サービス をサポートするための要件

Easy Connect および パッシブ ID サービス では、Active Directory ドメイン コントローラによって生成される Active Directory ログイン監査イベントを利用して、ユーザ ログイン情報を収集します。ISE ユーザが接続を行い、ユーザ ログイン情報を取得できるように、Active Directory サーバを適切に設定する必要があります。ここでは、Easy Connect および パッシブ ID サービス をサポートするように Active Directory ドメイン コントローラを設定する方法（Active Directory 側からの設定）について説明します。

Easy Connect および パッシブ ID サービス の使用をサポートするように Active Directory ドメイン コントローラを設定するには（Active Directory 側からの設定）、次の手順に従います。

1. ISE から Active Directory の参加ポイントとドメイン コントローラを設定します。[Active Directory 参加ポイントの追加および参加ポイントへの Cisco ISE ノードの参加（386 ページ）](#) および [ドメイン コントローラの追加（388 ページ）](#) を参照してください。
2. ドメイン コントローラごとに WMI を設定します。[WMI の設定（388 ページ）](#) を参照してください。
3. Active Directory で次の操作を実行します。
 - [パッシブ ID サービス の Active Directory の設定（406 ページ）](#)
 - [Windows 監査ポリシーの設定（410 ページ）](#)
4. （オプション）Active Directory で ISE により実行された自動設定のトラブルシューティングを行うには、次の操作を実行します。
 - [AD ユーザがドメイン管理グループに属しているときの権限の設定（293 ページ）](#)
 - [AD ユーザがドメイン管理グループの一部ではない場合に必要な権限（293 ページ）](#)
 - [ドメイン コントローラで DCOM を使用するための権限（295 ページ）](#)
 - [WMI ルート/CIMv2 名前空間にアクセスするための権限の設定（296 ページ）](#)
 - [AD ドメイン コントローラのセキュリティ イベント ログへのアクセス権の付与（415 ページ）](#)

パッシブ ID サービス の Active Directory の設定

ISE Easy Connect および パッシブ ID サービス では、ユーザ ログイン情報を収集するため、Active Directory ドメイン コントローラにより生成される Active Directory ログイン監査イベントが使用されます。ISE は Active Directory に接続し、ユーザ ログイン情報を取得します。

次の手順は、Active Directory ドメイン コントローラから実行する必要があります。

ステップ 1 該当する Microsoft のパッチが Active Directory ドメイン コントローラにインストールされていることを確認します。

a) Windows Server 2008 には次のパッチが必要です。

- <http://support.microsoft.com/kb/958124>

このパッチは、ISE がドメイン コントローラと正常な接続を確立するのを妨げる Microsoft WMI のメモリ リークを解消します (ISE 管理者は、ISE Active Directory ドメイン コントローラの GUI ページでこの問題を体験する場合があります。この GUI ページでは、接続が正常に確立されたときにステータスが「up」になる必要があります)。

- <http://support.microsoft.com/kb/973995>

このパッチは、Microsoft WMI の別のメモリ リークを解消します。このメモリ リークは、Active Directory ドメイン コントローラが必要なユーザ ログイン イベントをドメイン コントローラのセキュリティ ログに書き込むのを散発的に妨げます。結果として、ISE はこのドメイン コントローラからすべてのユーザ ログイン イベントを取得できない場合があります。

b) Windows Server 2008 R2 では、(SP1 がインストールされていない場合) 次のパッチが必要です。

- <http://support.microsoft.com/kb/981314>

このパッチは、Microsoft WMI のメモリ リークを解消します。このメモリ リークは、Active Directory ドメイン コントローラが必要なユーザ ログイン イベントをドメイン コントローラのセキュリティ ログに書き込むのを散発的に妨げます。結果として、ISE はこのドメイン コントローラからすべてのユーザ ログイン イベントを取得できない場合があります。

- <http://support.microsoft.com/kb/2617858>

このパッチは、Windows Server 2008 R2 での予期しない起動やログインプロセスの遅れを解消します。

c) Windows プラットフォームの WMI 関連問題には、次のリンクにリストされているパッチが必要です。

- <http://support.microsoft.com/kb/2591403>

これらのホットフィックスは、WMI サービスおよび関連コンポーネントの動作と機能に関連付けられます。

ステップ 2 Active Directory がユーザ ログイン イベントを Windows セキュリティ ログに記録するのを確認します。

「監査ポリシー」(「グループポリシーの管理」設定の一部) が、正常なログインによって、Windows セキュリティ ログに必要なイベントが生成されるように設定されていることを確認します (これはデフォルトの Windows 設定ですが、この設定が適切であることを明示的に確認する必要があります)。「Windows 監査ポリシーの設定」を参照してください。

ステップ 3 ISE が Active Directory に接続するための十分な権限を持つ Active Directory ユーザを設定する必要があります。次の手順では、管理ドメイングループのユーザ、または管理ドメイングループではないユーザに対して権限を定義する方法を示します。

- Active Directory ユーザがドメイン管理グループのメンバーである場合に必要な権限 (2 ~ 4 ページ)

- Active Directory ユーザがドメイン管理グループのメンバーでない場合に必要な権限 (2 ~ 4 ページ)

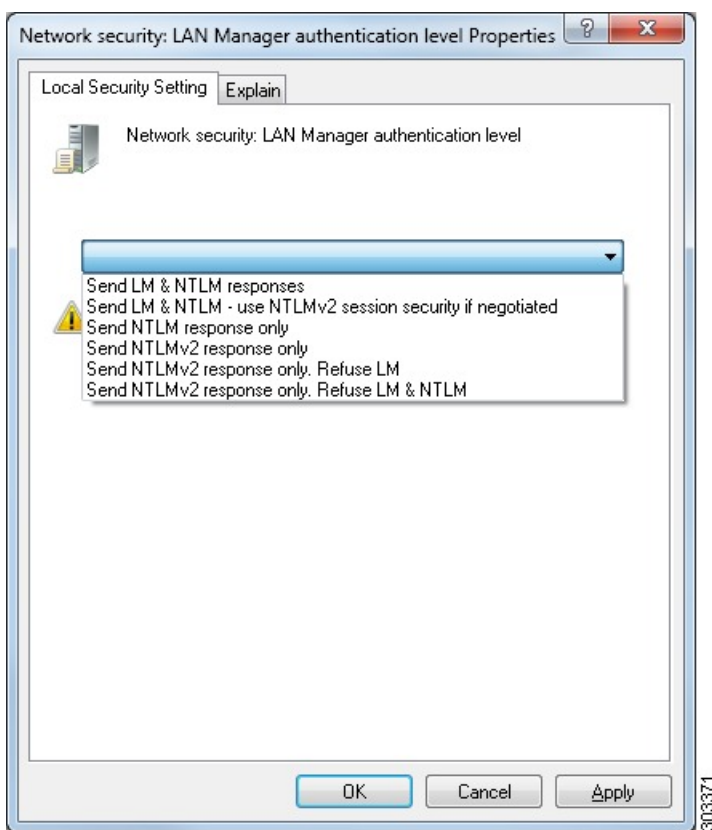
ステップ 4 ISE によって使用される Active Directory ユーザは、NT Lan Manager (NTLM) v1 または v2 のいずれかによって認証を受けることができます。ISE と Active Directory ドメイン コントローラ間の正常な認証済み接続を確実にを行うために、Active Directory NTLM の設定が ISE NTLM の設定と合っていることを確認する必要があります。次の表に、すべての Microsoft NTLM オプションと、サポート対象の ISE NTLM アクションを示します。ISE が NTLMv2 に設定される場合、記載されている 6 つのオプションがすべてサポートされます。NTLMv1 をサポートするように ISE が設定されている場合、最初の 5 つのオプションだけがサポートされます。

表 15: ISE と AD NTLM のバージョン設定に基づいてサポートされる認証タイプ

ISE NTLM の設定オプションおよび Active Directory (AD) NTLM の設定オプション NTLMv1 NTLMv2	NTLMv1	NTLMv2
LM & NTLM 応答を送信接続を許可接続を許可 (Send LM & NTLM responses connection is allowed connection is allowed)	接続が受け入れられます	接続が受け入れられます
LM & NTLM を送信: ネゴシエートされた接続が許可された場合に NTLMv2 セッションセキュリティを使用接続を許可 (Send LM & NTLM - use NTLMv2 session security if negotiated connection is allowed connection is allowed)	接続が受け入れられます	接続が受け入れられます
接続が許可された場合にのみ NTLM 応答を送信接続を許可 (Send NTLM response only connection is allowed connection is allowed)	接続が受け入れられます	接続が受け入れられます
接続が許可された場合にのみ NTLMv2 応答を送信接続を許可 (Send NTLMv2 response only connection is allowed connection is allowed)	接続が受け入れられます	接続が受け入れられます
NTLMv2 応答のみを送信 (Send NTLMv2 response only)。LM を拒否接続を許可接続を許可 (Refuse LM connection is allowed connection is allowed)	接続が受け入れられます	接続が受け入れられます

ISE NTLM の設定オプションおよび Active Directory (AD) NTLM の設定 オプション NTLMv1 NTLMv2	NTLMv1	NTLMv2
NTLMv2 応答のみを送信 (Send NTLMv2 response only)。LM & NTLM を拒否 接続を拒否 接続を許可 (Refuse LM & NTLM connection is refused connection is allowed)	接続は拒否されます	接続が受け入れられます

図 22: MS NTLM 認証タイプのオプション



ステップ 5 Active Directory ドメイン コントローラで `dllhost.exe` へのトラフィックを許可するファイアウォールルールを作成していることを確認します。

ファイアウォールをオフにするか、または次のポートへの特定の IP (ISE IP アドレス) のアクセスを許可することができます。

- TCP 135 : 一般的な RPC ポート。非同期 RPC 発信をすると、このポートでリスニングしているサービスが、クライアントに、この要求を処理できるコンポーネントが使用しているポートを通知します。
- UDP 137 : NetBIOS 名前解決
- UDP 138 : NetBIOS データグラム サービス

- TCP 139 : NetBIOS セッション サービス
- TCP 445 : SMB

数値の大きいポートは動的に割り当てられ、手動で設定できます。ターゲットとして %SystemRoot%\System32\dlhhost.exe を追加することを推奨します。このプログラムは、ポートを動的に管理します。

すべてのファイアウォールルールを、特定の IP アドレス (ISE IP) に割り当てることができます。

Windows 監査ポリシーの設定

監査ポリシー (グループポリシー管理設定の一部) が正常なログインを許可していることを確認します。これには、AD ドメイン コントローラ マシンの Windows セキュリティ ログに必要なイベントを生成する必要があります。これはデフォルトの Windows 設定ですが、この設定が正しいことを確認する必要があります。

ステップ 1 [スタート] > [Programs] > [Administrative Tools] > [Group Policy Management] を選択します。

ステップ 2 [Domains] で関連するドメインに移動し、ナビゲーション ツリーを展開します。

ステップ 3 [Default Domain Controller Policy] を選択し、右クリックして、[編集] を選択します。

グループ ポリシー管理エディターが表示されます。

ステップ 4 [デフォルトのドメイン コントローラ ポリシー (Default Domain Controllers Policy)] > [コンピュータ設定 (Computer Configuration)] > [ポリシー (Policies)] > [Windows 設定 (Windows Settings)] > [セキュリティ設定 (Security Settings)] の順に選択します。

- Windows Server 2003 または Windows Server 2008 (R2 以外) の場合は [ローカルポリシー (Local Policies)] > [監査ポリシー (Audit Policy)] の順に選択します。2 つのポリシー項目 ([Audit Account Logon Events] と [Audit Logon Events]) で、対応する [Policy Setting] に [Success] 状態が直接的または間接的に含まれていることを確認します。[Success] 状況を間接的に含めるには、[Policy Setting] に [Not Defined] を設定します。この場合、上位ドメインから有効値が継承されるため、[Success] 状態を明示的に含めるようにその上位ドメインの [Policy Setting] を設定する必要があります。
- Windows Server 2008 R2 および Windows 2012 の場合、[Advanced Audit Policy Configuration] > [Audit Policies] > [Account Logon] を選択します。2 つのポリシー項目 ([Audit Kerberos Authentication Service] と [Audit Kerberos Service Ticket Operations]) に対応する [Policy Setting] に、前述のように [Success] 状態が直接または間接的に含まれていることを確認します。

ステップ 5 [監査ポリシー] の項目設定が変更されている場合は、gpupdate /force を実行して新しい設定を強制的に有効にする必要があります。

AD ユーザがドメイン管理グループに属しているときの権限の設定

Windows 2008 R2、Windows 2012 および Windows 2012 R2 の場合、ドメイン管理グループは、デフォルトで Windows オペレーティング システムの特定のレジストリ キーを完全に制御することができません。Active Directory の管理者は、Active Directory ユーザに次のレジストリ キーに対する完全制御権限を提供する必要があります。

- HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}
- HKLM\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}

次の Active Directory のバージョンでは、レジストリ変更は必要ありません。

- Windows 2003
- Windows 2003R2
- Windows 2008

完全な制御を許可するには、次に示すように、まず Active Directory 管理者がキーの所有権を取得する必要があります。

ステップ 1 キーを右クリックして [オーナー (Owner)] タブに移動します。

ステップ 2 [アクセス許可 (Permissions)] をクリックします。

ステップ 3 [詳細設定 (Advanced)] をクリックします。

AD ユーザがドメイン管理グループの一部ではない場合に必要な権限

Windows 2012 R2 の場合は、Active Directory ユーザに次のレジストリ キーに対する完全制御権限を提供します。

- HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}
- HKLM\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}

Active Directory ユーザがドメイン管理グループの一部ではなく、ドメイン ユーザ グループの一部である場合は、次の権限も必要です。

- ISE がドメイン コントローラに接続できるようにするレジストリ キーを追加します (下記を参照)
- [ドメイン コントローラで DCOM を使用するための権限 \(295 ページ\)](#)
- [WMI ルート/CIMv2 名前空間にアクセスするための権限の設定 \(296 ページ\)](#)

これらの権限は、次の Active Directory のバージョンでのみ必要となります。

- Windows 2003
- Windows 2003R2

- Windows 2008
- Windows 2008 R2
- Windows 2012
- Windows 2012 R2
- Windows 2016

ISE がドメイン コントローラに接続できるようにするレジストリ キーを追加する

ISE がドメイン ユーザとして接続し、ログイン認証イベントを取得できるようにするには、ドメイン コントローラに一部のレジストリ キーを手動で追加する必要があります。エージェントはドメイン コントローラまたはドメイン内のマシンでは必要ありません。

次のレジストリのスクリプトは追加するキーを示しています。これをコピーしてテキストファイルに貼り付け、.reg の拡張子でファイルを保存し、ファイルをダブルクリックすることでレジストリの変更を行うことができます。レジストリ キーを追加するには、ルート キーのオーナーである必要があります。

Windows Registry Editor Version 5.00

```
[HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"AppID"="{76A64158-CB41-11D1-8B02-00600806D9B6}"
```

```
[HKEY_CLASSES_ROOT\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"DllSurrogate"=" "
```

```
[HKEY_CLASSES_ROOT\Wow6432Node\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"DllSurrogate"=" "
```

キー **DllSurrogate** の値には、2 つのスペースが含まれていることを確認します。

上記のスクリプトに示すように、ファイルの末尾の空の行を含む、空の行を保持してください。

ドメイン コントローラで DCOM を使用するための権限

ISE パッシブ ID サービスに使用される Active Directory ユーザは、ドメイン コントローラで DCOM (リモート COM) を使用する権限がなければなりません。dcomcnfg コマンドライン ツールを使用して権限を設定できます。

ステップ 1 コマンドラインから **dcomcnfg** ツールを実行します。

ステップ 2 [コンポーネントサービス (Component Services)] を展開します。

ステップ 3 [コンピュータ (Computers)] > [マイコンピュータ (My Computer)] を展開します。

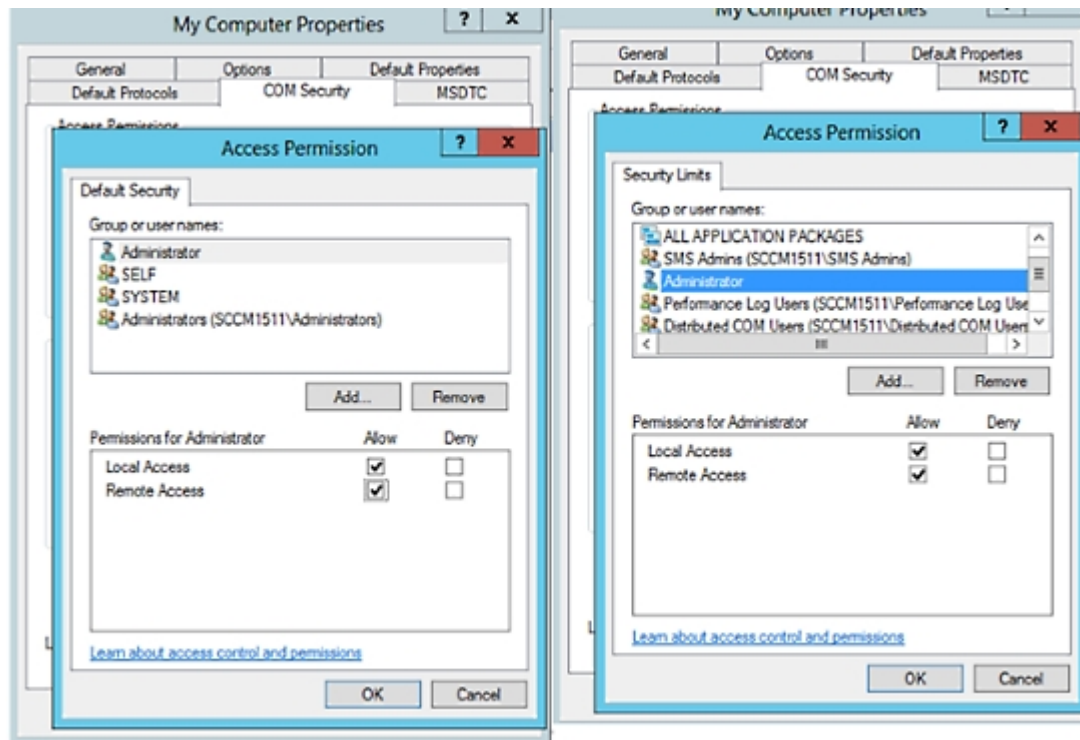
ステップ 4 メニュー バーで [アクション (Action)] を選択して、[プロパティ (properties)] をクリックし、[COM セキュリティ (COM Security)] をクリックします。

ステップ 5 アクセスおよび起動の両方に対して ISE が使用するアカウントに許可権限があることを確認します。Active Directory ユーザは、4 つのオプション ([アクセス権限 (Access Permissions)] および [起動およびアクティ

バージョンの権限 (Launch and Activation Permissions)] の両方に対する [制限の編集 (Edit Limits)] と [デフォルトの編集 (Edit Default)] のすべてに追加される必要があります。

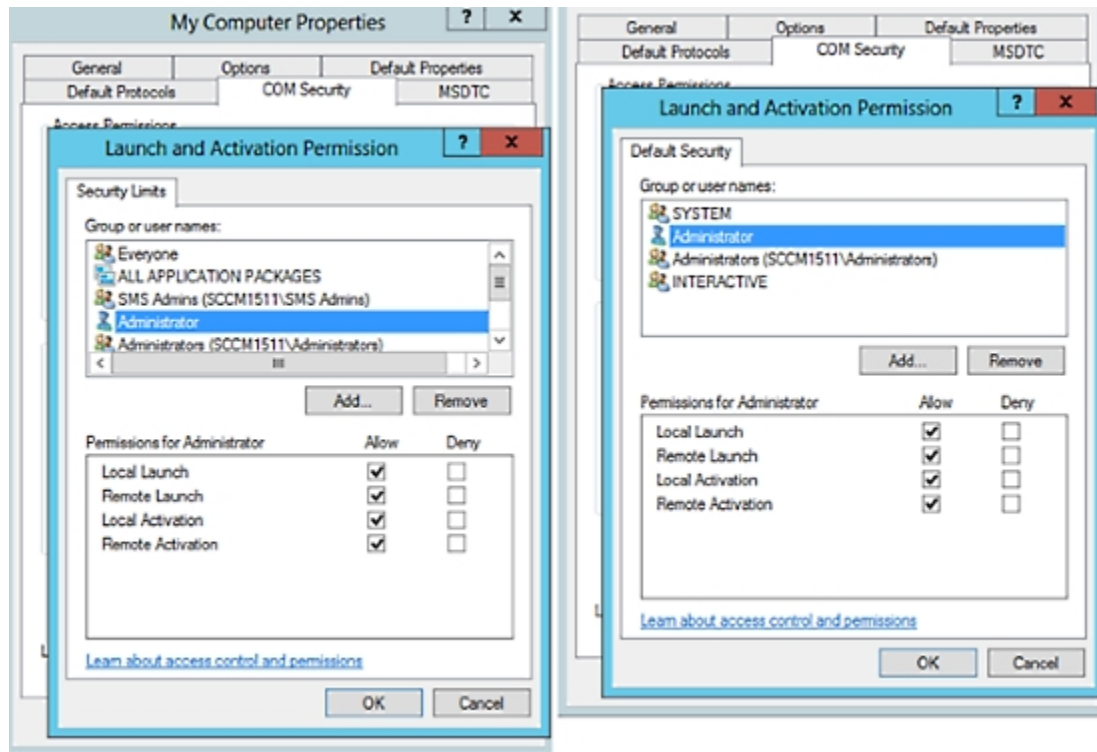
ステップ 6 [アクセス権限 (Access Permissions)] および [起動およびアクティベーションの権限 (Launch and Activation Permissions)] の両方に対してローカルおよびリモート アクセスをすべて許可します。

図 23: [アクセス権限 (Access Permissions)] のローカルおよびリモート アクセス



WMI ルート/CIMv2 名前空間にアクセスするための権限の設定

図 24: [起動およびアクティベーションの権限 (Launch and Activation Permissions)] のローカルおよびリモート アクセス

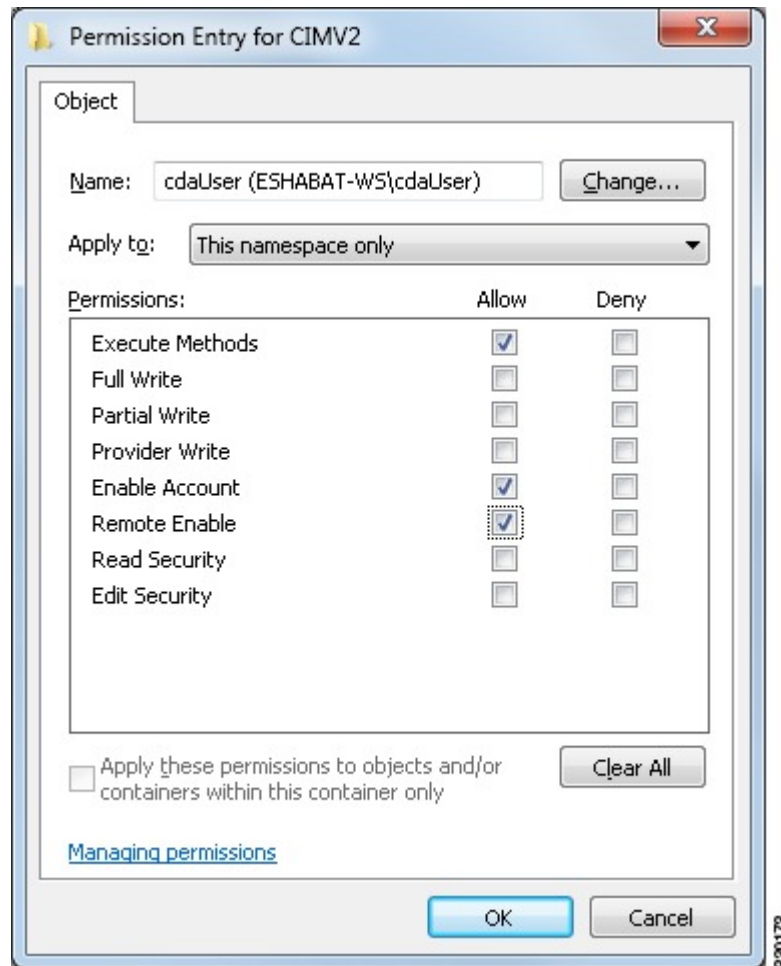


WMI ルート/CIMv2 名前空間にアクセスするための権限の設定

デフォルトでは、Active Directory ユーザには実行メソッドおよびリモート イネーブルのための権限がありません。wmimgmt.msc MMC コンソールを使用してアクセス権を付与できます。

- ステップ 1 [スタート]>[Run] をクリックし、wmimgmt.msc と入力します。
- ステップ 2 [WMI Control] を右クリックし、[プロパティ] をクリックします。
- ステップ 3 [セキュリティ] タブで [ルート] を展開し、[CIMV2] を選択します。
- ステップ 4 [セキュリティ (Security)] をクリックします。
- ステップ 5 下に示すように、Active Directory ユーザを追加し、必要な権限を設定します。

図 25: WMI Root\CIMv2 名前空間に必要な権限



AD ドメインコントローラのセキュリティ イベント ログへのアクセス権の付与

Windows 2008 以降では、ISE ID マッピング ユーザを Event Log Reader と呼ばれるグループに追加することで、AD ドメイン コントローラのログへのアクセス権を付与できます。

Windows のすべての旧バージョンでは、次に示すようにレジストリ キーを編集する必要があります。

ステップ 1 セキュリティ イベント ログへのアクセス権を委任するには、アカウントの SID を検索します。

ステップ 2 すべての SID アカウントを表示するには、次の図に示すように、コマンドラインから次のコマンドを使用します。

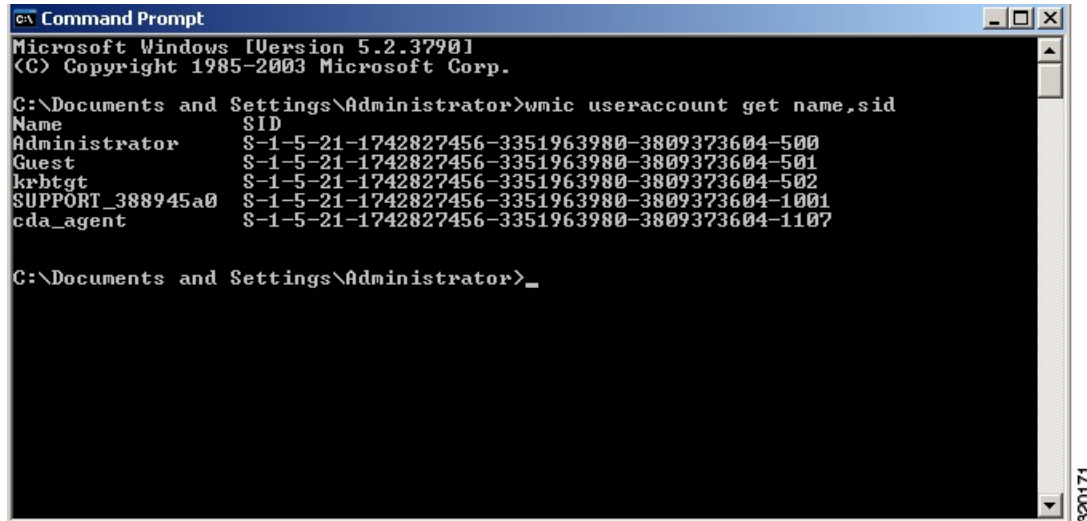
AD ドメインコントローラのセキュリティ イベント ログへのアクセス権の付与

```
wmic useraccount get name,sid
```

特定のユーザ名とドメインに対して、次のコマンドを使用することもできます。

```
wmic useraccount where name="iseUser" get domain,name,sid
```

図 26: すべての SID アカウントの表示



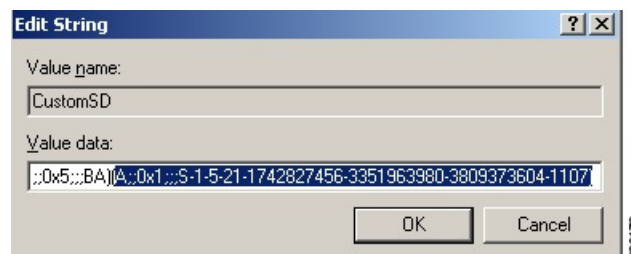
ステップ 3 SID を見つけ、レジストリ エディタを開き、次の場所を参照します。

HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/Eventlog

ステップ 4 [セキュリティ (Security)] をクリックし、[CustomDS] をダブルクリックします。図 2 ~ 7 を参照してください。

たとえば、ise_agent アカウント (SID: S-1-5-21-1742827456-3351963980-3809373604-1107) への読み取りアクセスを許可するには、「(A;;0x1;;;S-1-5-21-1742827456-3351963980-3809373604-1107)」と入力します。

図 27: CustomSD 文字列の編集



ステップ 5 ドメインコントローラ上で WMI サービスを再起動します。次の 2 とおりの方法で WMI サービスを再起動できます。

a) CLI から次のコマンドを実行します。

```
net stop winmgmt
```

```
net start winmgmt
```

- b) `services.msc` を実行します。これにより、Windows サービス管理ツールが開きます。Windows サービス管理ウィンドウで、「**Windows Management Instrumentation**」サービスを検索し、右クリックして [再起動] を選択します。

Easy Connect

Easy Connect により、セキュアな方法で有線接続されたエンドポイントからネットワークにユーザを簡単に接続し、Cisco ISE ではなく Active Directory ドメイン コントローラからユーザを認証することで、それらのユーザをモニタすることができます。Easy Connect により、ISE は Active Directory ドメイン コントローラからユーザ認証情報を収集します。Easy Connect は MS WMI インターフェイスを使用して Windows システム (Active Directory) に接続し、Windows イベント メッセージからのログにクエリを行うため、現在は Windows がインストールされているエンドポイントのみをサポートしています。Easy Connect は MAB を使用した有線接続をサポートし、これは 802.1X よりもずっと設定が容易です。802.1X とは異なり、Easy Connect と MAB では、

- サプリカントを設定する必要がありません
- PKI を設定する必要がありません
- ISE は外部サーバ (AD) がユーザを認証した後に CoA を発行します

Easy Connect は次の動作モードをサポートしています。

- 適用モード : ISE がユーザクレデンシャルに基づいて、適用のために認証ポリシーをネットワーク デバイスにアクティブにダウンロードします。
- 可視性モード : ISE がセッション マージをパブリッシュし、情報を pxGrid に送信するために NAD デバイス センサーから受信した情報をアカウントिंगします。

どちらの場合も、Active Directory (AD) で認証されたユーザは、Cisco ISE のライブ セッションビューに表示され、サードパーティ製アプリケーションによる Cisco pxGrid インターフェイスを使用してセッションディレクトリからクエリすることができます。既知の情報としては、ユーザ名、IP アドレス、AD DC ホスト名と AD DC NetBIOS 名があります。pxGrid の詳細については、[pxGrid ノード \(76 ページ\)](#) を参照してください。

Easy Connect のセットアップが完了したら、ユーザの名前または IP アドレスに基づいて特定ユーザをフィルタリングできます。たとえば IT サービスの管理者が、そのエンドポイントの標準ユーザを支援するためにエンドポイントにログインする場合、管理者アクティビティをフィルタリングにより除外して [ライブ セッション (Live Sessions)] に表示されないようにし、そのエンドポイントの標準ユーザだけが表示されるようにできます。パッシブ ID サービスをフィルタリングするには、[パッシブ ID サービスのフィルタリング \(474 ページ\)](#) を参照してください。

Easy Connect の制限

- MAC 認証バイパス (MAB) は Easy Connect をサポートします。MAB と 802.1X の両方を同じポートで設定できますが、各サービス用に異なる ISE ポリシーが必要です。
- 現在は MAB 接続のみがサポートされています。許可ポリシーで定義されている Easy Connect 条件によって接続が許可され、権限が付与されるため、接続についての独自の認証ポリシーは不要です。
- Easy Connect はハイ アベイラビリティ モードでサポートされます。パッシブ ID を使用して、複数のノードを定義して有効にすることができます。ISE はその後自動的に 1 つの PSN を有効にしますが、その他のノードはスタンバイ状態のままです。
- シスコのネットワーク アクセス デバイス (NAD) のみがサポートされています。
- IPv6 はサポートされていません。
- ワイヤレス接続は現在サポートされていません。
- Kerberos 認証イベントのみが追跡されるため、Easy Connect はユーザ認証のみを有効にし、マシン認証をサポートしません。

Easy Connect は ISE で設定する必要があるため、Active Directory ドメイン サーバには Microsoft によって発行された指示とガイドラインに基づいた適切なパッチと設定が必要です。ISE の Active Directory ドメイン コントローラの設定については、次の項を参照してください。 [Active Directory で Easy Connect および パッシブ ID サービス をサポートするための要件 \(406 ページ\)](#)

Easy Connect 適用モード

Easy Connect により、ユーザは MAC アドレス バイパス (MAB) プロトコルを使用し、認証のための Active Directory (AD) にアクセスすることで、Windows オペレーティング システムを備えた有線接続されたエンドポイント (通常は PC) からセキュアなネットワークにログオンすることができます。ISE の Easy Connect は、認証されるユーザに関する情報のために Active Directory サーバからの Windows Management Instrumentation (WMI) イベントをリスンします。AD がユーザを認証すると、ドメイン コントローラがユーザに割り当てられたユーザ名と IP アドレスを含むイベント ログを生成します。ISE が AD からログインの通知を受信し、RADIUS の認可変更 (CoA) を発行します。



- (注) RADIUS サービス タイプが call-check に設定されている場合、MAC アドレス ルックアップは MAB 要求のために行われません。そのため、この要求への応答は access-accept です。これは ISE のデフォルト設定です。

Easy Connect 適用モードのプロセス フロー

Easy Connect 適用モードのプロセスは次のとおりです。

1. ユーザが有線接続されたエンドポイント (PC など) から NAD に接続します。

2. (MAB 用に設定された) NAD が ISE にアクセス要求を送信します。ISE がアクセスに応答し、ユーザ設定に基づいて、ユーザに AD へのアクセスを許可します。設定では、少なくとも DNS、DHCP、AD へのアクセスを許可する必要があります。
3. ユーザがドメインにログインし、セキュリティ監査イベントが ISE に送信されます。
4. ISE は RADIUS から MAC アドレスを収集し、セキュリティ監査イベントから IP アドレス、ドメイン名、ユーザに関するアカウント情報 (ログイン情報) を収集します。
5. ISE セッションディレクトリですべてのデータが収集されてマージされると、(ポリシーサービスノード (PSN) で管理されている適切なポリシーに基づいて) ISE が NAD に CoA を発行し、そのポリシーに基づいて NAD によりユーザにネットワークへのアクセスが提供されます。

図 28: Easy Connect 適用モードの基本フロー

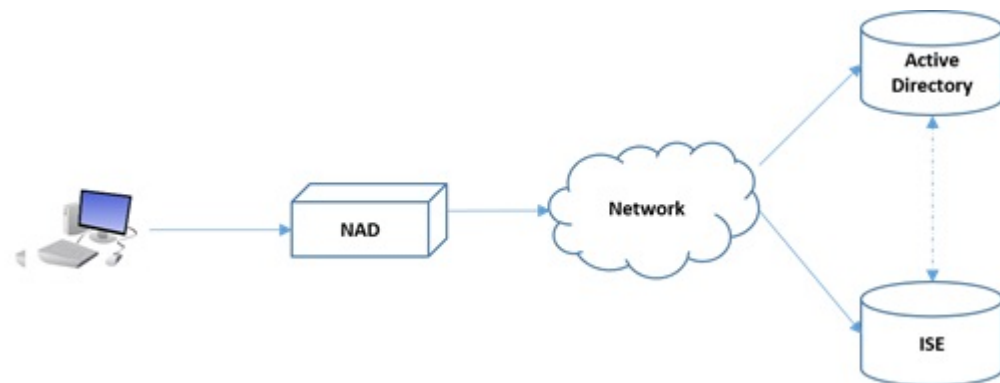
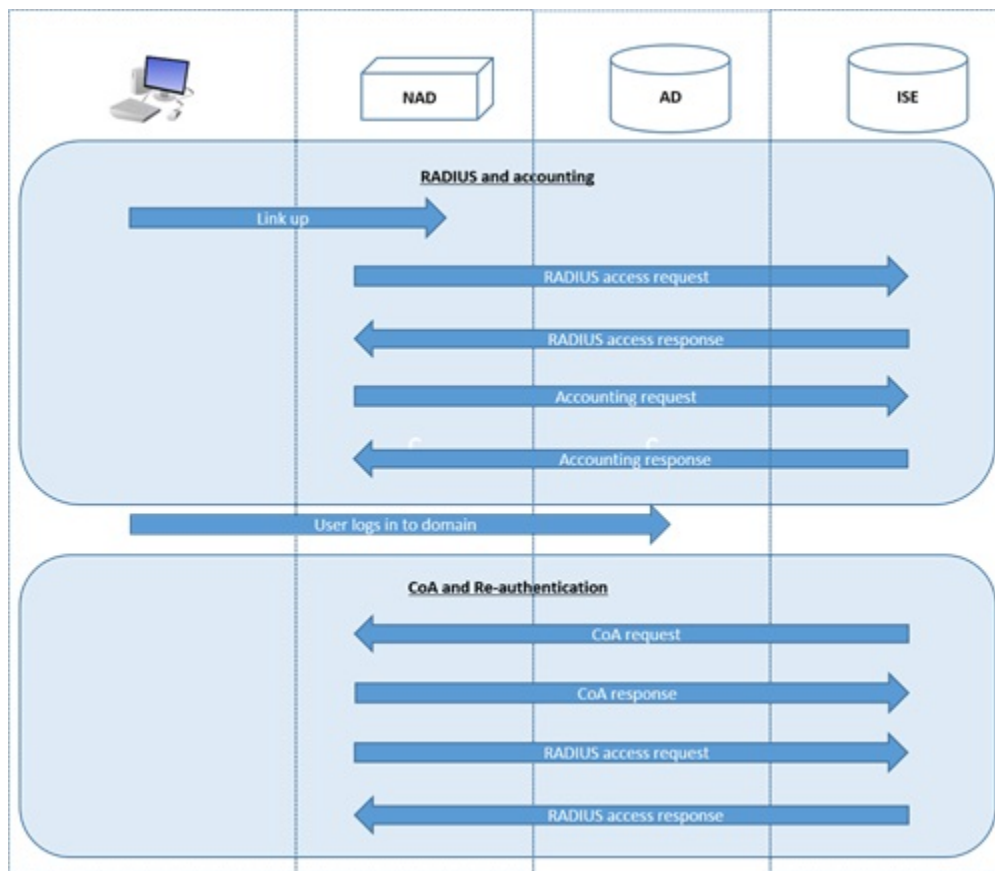


図 29: Easy Connect 適用モードの詳細フロー

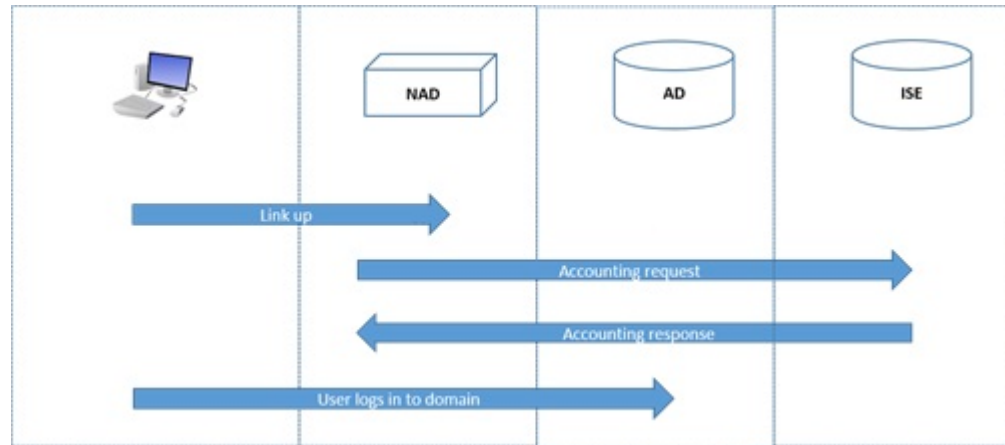


適用モードの設定の詳細については、[Easy Connect 適用モードの設定](#)（421 ページ）を参照してください。

Easy Connect 可視性モード

可視性モードでは、ISE は RADIUS からのアカウントリング情報のみをモニタし（NAD のデバイスセンサー機能の一部）、認証は行いません。Easy Connect は RADIUS アカウントリングと WMI イベントをリッスンし、ログとレポート（およびオプションで pxGrid）にその情報をパブリッシュします。pxGrid が設定されている場合、Active Directory を使用したユーザ ログイン中に RADIUS のアカウントリング開始とセッション終了の両方が pxGrid にパブリッシュされます。

図 30: Easy Connect 可視性モードのフロー



Easy Connect 可視性モードの設定の詳細については、[Easy Connect 表示モードの設定](#)（422 ページ）を参照してください。

Easy Connect 適用モードの設定

始める前に

- 最適なパフォーマンスを得るには、WMI イベントを受け取るための専用の PSN を導入します。
- AD ログイン イベントを受け取る、WMI ノードの Active Directory ドメイン コントローラ のリストを作成します。
- Active Directory からユーザ グループを取得するために ISE が参加する必要がある Microsoft ドメインを決定します。
- 認証ポリシーでリファレンスとして使用される Active Directory グループを決定します。
- pxGrid を使用してネットワーク デバイスからのセッションデータを他の pxGrid 対応システムと共有する場合は、導入内で pxGrid ペルソナを定義します。pxGrid の詳細については、次を参照してください。[pxGrid ノード](#)（76 ページ）
- MAB が成功した後、NAD は、（概要で説明されているように）そのポートのユーザが Active Directory サーバにアクセスできるようにする、制限付きアクセスプロファイルを提供する必要があります。

ステップ 1 （注） パッシブ ID サービスは複数のノードで有効にできますが、Easy Connect は一度に 1 つのノードでのみ操作できます。複数のノードのサービスを有効にすると、ISE はアクティブな Easy Connect セッションのために使用するノードを自動的に決定します。

Easy Connect に使用する専用ポリシー サーバ (PSN) でパッシブ ID サービスを有効にして、ISE がグループ情報とイベント情報を Active Directory から取得できるようにします。[管理 (Administration)] > [システム (System)] > [導入 (Deployment)] の順に選択してノードを開き、[全般設定 (General Settings)] の下で [パッシブ ID サービスの有効化 (Enable Passive Identity Service)] を有効にします。

ステップ 2 Easy Connect が使用する Active Directory 参加ポイントとドメイン コントローラを設定します。この操作の実行方法と詳細については、[Active Directory で Easy Connect および パッシブ ID サービス をサポートするための要件 \(406 ページ\)](#) を参照してください。

ステップ 3 必要に応じて、さまざまなユーザのグループ用のさまざまなポリシーを作成するために (マーケティング部門従業員と管理部門従業員のための異なるポリシーなど)、AD ドメイン コントローラ グループをマッピングします。[管理 (Administration)] > [ID の管理 (Identity Management)] > [外部 ID ソース (External Identity Sources)] > [Active Directory] の順に選択し、使用する Active Directory を選択して [グループ (Groups)] タブを選択し、認証ポリシーで使用する Active Directory グループを追加します。ドメイン コントローラ用にマッピングした Active Directory グループは PassiveID ディクショナリで動的に更新され、ポリシー条件ルールを設定するときに使用することができます。

ステップ 4 (注) Easy Connect プロセスが適切に実行され、ISE が有効にされて CoA が発行できるように、Easy Connect 認証に使用されるすべてのプロファイルで [パッシブ ID 追跡 (Passive Identity Tracking)] を有効にする必要があります。

パッシブ ID 追跡を有効にします。[ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] > [認証 (Authorization)] > [認証プロファイル (Authorization Profiles)] の順に選択します。Easy Connect によって使用されるプロファイルについて、プロファイルを開いて [パッシブ ID 追跡 (Passive Identity Tracking)] を有効にします。

ステップ 5 ポリシー ルールを作成します。[ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [条件 (Conditions)] > [認証 (Authorization)] > [単純条件 (Simple Conditions)] の順に選択し、Easy Connect 用のルールを作成します。[追加 (Add)] をクリックします。次に、条件を定義します。

- 役立つ名前と説明を入力します。
- [属性 (Attribute)] から PassiveID ディクショナリに移動し、PassiveID_Groups を選択してドメイン コントローラ グループ用の条件を作成するか、PassiveID_user を選択して個々のユーザ用の条件を作成します。
- 正しい操作を入力します。
- ポリシーに含めるユーザ名またはグループ名を入力します。

ステップ 6 [送信 (Submit)] をクリックします。

Easy Connect 表示モードの設定

始める前に

- 最適なパフォーマンスを得るには、WMI イベントを受け取るための専用の PSN を導入します。
- AD ログイン イベントを受け取る、WMI ノードの Active Directory ドメイン コントローラのリストを作成します。

- Active Directory からユーザ グループを取得するために ISE が参加する必要がある Microsoft ドメインを決定します。
- pxGrid を使用してネットワーク デバイスからのセッションデータを他の pxGrid 対応システムと共有する場合は、導入内で pxGrid ペルソナを定義します。pxGrid の詳細については、次を参照してください。 [pxGrid ノード \(76 ページ\)](#)

-
- ステップ 1** Easy Connect に使用する専用ポリシー サーバ (PSN) でパッシブ ID サービスを有効にして、ISE がグループ情報とイベント情報を Active Directory から取得できるようにします。[管理 (Administration)] > [システム (System)] > [導入 (Deployment)] の順に選択してノードを開き、[全般設定 (General Settings)] の下で [パッシブ ID サービスの有効化 (Enable Passive Identity Service)] を有効にします。
- ステップ 2** Easy Connect が使用する Active Directory 参加ポイントとドメイン コントローラを設定します。この操作の実行方法と詳細については、[#unique_559](#)を参照してください。
-

PassiveID ワーク センター

パッシブ ID コネクタ (PassiveID ワーク センター) は一元的なワンストップ インストールおよび実装を提供します。これにより、ユーザ ID 情報を受信してさまざまなセキュリティ製品 (Cisco Firepower Management Center (FMC) や Stealthwatch など) のサブスクリバと共有するように、ネットワークを容易に設定できます。パッシブ ID の完全なブローカとして、PassiveID ワーク センター はさまざまなプロバイダー ソース (Active Directory ドメイン コントローラ (AD DC) など) からユーザ ID を収集し、ユーザ ログイン情報を使用中の該当する IP アドレスにマッピングし、そのマッピング情報を、設定されているサブスクリバセキュリティ製品と共有します。

パッシブ ID について

認証、許可、およびアカウンティング (AAA) サーバを提供し、802.1X や Web 認証などのテクノロジーを使用する Cisco Identity Services Engine (ISE) で提供される標準フローは、ユーザまたはエンドポイントと直接通信し、ネットワークへのアクセスを要求し、ログインクレデンシャルを使用して ID を検証およびアクティブに認証します。

パッシブ ID サービスはユーザを直接認証しませんが、ユーザ ID と IP アドレスをプロバイダーと呼ばれる外部認証サーバ (Active Directory など) から収集し、その情報をサブスクリバと共有します。PassiveID ワーク センター は最初に、通常はユーザ ログインとパスワードに基づいてプロバイダーからユーザ ID 情報を受信します。次に、そのユーザ ID を該当する IP アドレスと関連付けるために必要なチェックとサービスを実行し、認証済み IP アドレスをサブスクリバに送信します。

パッシブ ID コネクタ (PassiveID ワーク センター) のフロー

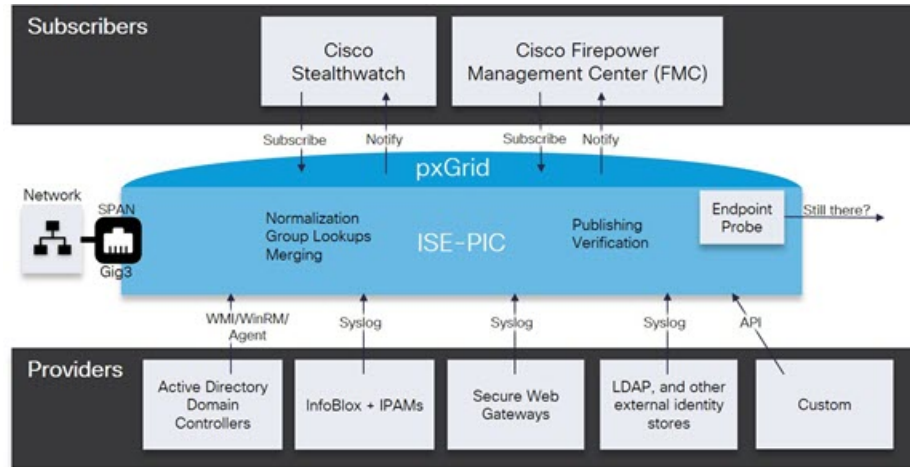
PassiveID ワーク センター のフローは次のとおり。

1. プロバイダーがユーザまたはエンドポイントの認証を実行します。

2. プロバイダーが認証済みユーザ情報を に送信します。
3. ISE によりユーザ情報の正規化、ルックアップ、マージ、解析、および IP アドレスへのマッピングが行われ、マッピングされた詳細情報が pxGrid に対して公開されます。
4. pxGrid サブスクライバはマッピングされたユーザの詳細情報を受信します。

次の図は、ISE の全体的なフローを示します。

図 31: 全体的なフロー



初期セットアップと設定

Cisco PassiveID ワーク センター をすぐに使用できるようにするには、次のフローに従います。

1. DNS サーバを適切に設定していることを確認します。これには、ISE からのクライアント マシンの逆引きの設定も含まれます。詳細については、[DNS サーバ \(384 ページ\)](#) を参照してください。
2. パッシブ ID サービスに使用する専用ポリシー サーバ (PSN) で、パッシブ ID サービスと pxGrid サービスを有効にします。**[管理 (Administration)] > [システム (System)] > [展開 (Deployment)]** を選択し、該当するノードを開き、**[全般設定 (General Settings)]** の下の **[パッシブ ID サービスの有効化 (Enable Passive Identity Service)]** と **[pxGrid]** をオンにします。
3. NTP サーバのクロック設定を同期します。詳細については、[システム時刻と NTP サーバ設定の指定 \(95 ページ\)](#) を参照してください。
4. ISE パッシブ ID セットアップで、最初のプロバイダーを設定します。詳細については、次を参照してください。[PassiveID セットアップの使用を開始する \(427 ページ\)](#)
5. 1つまたは複数のサブスクライバを設定します。詳細については、次を参照してください。[サブスクライバ \(477 ページ\)](#)

最初のプロバイダーとサブスクライバのセットアップが完了したら、追加のプロバイダーを容易に作成でき（[その他のパッシブ ID サービスプロバイダー（433 ページ）](#)）を参照）、また PassiveID ワーク センター でさまざまなプロバイダーからのパッシブ ID を管理できます。

- [RADIUS ライブ セッション（1454 ページ）](#)
- [Cisco ISE アラーム（1042 ページ）](#)
- [レポート（1095 ページ）](#)
- [着信トラフィックを検証する TCP ダンプ ユーティリティ（1080 ページ）](#)

PassiveID ワーク センター ダッシュボード

Cisco PassiveID ワーク センター ダッシュボードには、効果的なモニタリングおよびトラブルシューティングに必要な、統合され、関連付けられた概要と統計データが表示されます。ダッシュボードはリアルタイムに更新されます。特に指定がない限り、ダッシュレットには過去24時間のアクティビティが表示されます。ダッシュボードにアクセスするには、**[ワーク センター（Work Centers）] > [PassiveID]** を選択し、左側のパネルで **[ダッシュボード（Dashboard）]** を選択します。Cisco PassiveID ワーク センター ダッシュボードはプライマリ管理ノード（PAN）でのみ表示できます。

[ホーム（Home）] ページには、PassiveID ワーク センター データのビューを表示する2つのデフォルト ダッシュボードがあります。

- **[メイン（Main）]** : このビューには、線形の **[メトリクス（Metrics）]** ダッシュボード、**チャート ダッシュレット**、および **リスト ダッシュレット** が表示されます。PassiveID ワーク センター では、ダッシュレットは設定できません。使用可能なダッシュレットには次のものがあります。
 - **[パッシブ ID メトリック（Passive Identity Metrics）]** : **[パッシブ ID メトリック（Passive Identity Metrics）]** では、現在追跡中の固有のライブセッションの総数、システムに設定されている ID プロバイダーの総数、ID データをアクティブに配信しているエージェントの総数、および現在設定されているサブスクライバの総数の概要が示されます。
 - **[プロバイダー（Providers）]** : プロバイダーはユーザ ID 情報を PassiveID ワーク センター に渡します。ISE プロローブ(特定のソースからデータを収集するメカニズム)を設定します。プロローブを介してプロバイダーソースからの情報を受信します。たとえば、Active Directory（AD）プロローブとエージェント プロローブはいずれも ISE-PIC による AD からのデータ収集を支援しますが、syslog プロローブは、syslog メッセージを読み取るパーサーからデータを収集します。
 - **[サブスクライバ（Subscribers）]** : サブスクライバは ISE に接続し、ユーザ ID 情報を取得します。
 - **[OS タイプ（OS Types）]** : 表示できる唯一の OS タイプは Windows です。Windows のタイプが Windows バージョン別に表示されます。プロバイダーは OS タイプを報告しませんが、ISE はこの情報を取得するため Active Directory を照会できます。ダッ

シュレットに表示できるエントリの最大数は 1000 です。この数を超えるエンドポイントがある場合、または Windows 以外の OS タイプを表示する場合には、ISE にアップグレードできます。

- [アラーム (Alarms)] : ユーザ ID 関連アラーム。

プローブおよびプロバイダーとしての Active Directory

Active Directory (AD) は、ユーザ ID 情報 (ユーザ名、IP アドレス、ドメイン名など) の取得元である安全性が高く正確なソースです。

AD プローブ () は、WMI テクノロジーを使用して AD からユーザ ID 情報を収集しますが、その他のプローブはその他のテクノロジーや手法で AD をユーザ ID プロバイダーとして使用します。パッシブ ID サービスISE のその他のプローブとプロバイダー タイプの詳細については、[その他のパッシブ ID サービスプロバイダー \(433 ページ\)](#) を参照してください。

Active Directory プローブを設定すると、次の (ソースとして Active Directory を使用する) その他のプローブも迅速に設定して有効にできます。

- エージェント : [Active Directory エージェント \(436 ページ\)](#)



(注) Active Directory エージェントは、Windows Server 2008 以降でのみサポートされます。

- SPAN : [SPAN \(447 ページ\)](#)
- エンドポイント プローブ : [エンドポイント プローブ \(474 ページ\)](#)

また、ユーザ情報の収集時に AD ユーザ グループを使用するために Active Directory プローブを設定します。AD、エージェント、SPAN、および syslog プローブで AD ユーザ グループを使用できます。AD グループの詳細については、[Active Directory ユーザ グループの設定 \(390 ページ\)](#) を参照してください。

Active Directory (WMI) プローブのセットアップ

パッシブ ID サービス向けに Active Directory と WMI を設定するには、[パッシブ ID ワーク センター ウィザード (Passive ID Work Center Wizard)] ([PassiveID セットアップの使用を開始する \(427 ページ\)](#) を参照) を使用するか、または次の手順に従います (追加情報については [Active Directory で Easy Connect およびパッシブ ID サービス をサポートするための要件 \(406 ページ\)](#) を参照)。

1. Active Directory プローブを設定します。 [Active Directory 参加ポイントの追加および参加ポイントへの Cisco ISE ノードの参加 \(386 ページ\)](#) を参照してください。
2. AD ログイン イベントを受信する 1 つ以上の WMI 設定ノードの Active Directory ドメイン コントローラのリストを作成します。 [ドメイン コントローラの追加 \(388 ページ\)](#) を参照してください。

3. Active Directory を ISE と統合するため Active Directory を設定します。[WMI の設定 \(388 ページ\)](#) を参照してください。
4. (任意) [Active Directory プロバイダーの管理 \(429 ページ\)](#)。

PassiveID セットアップの使用を開始する

ISE-PIC には、Active Directory からユーザ ID を受信するために、Active Directory を最初のユーザ ID プロバイダーとして容易に設定できるウィザードがあります。ISE-PIC に Active Directory を設定することで、後でその他のプロバイダータイプを設定するプロセスも簡素化されます。Active Directory を設定したら、ユーザデータを受信するクライアントを定義するため、サブスクライバ (Cisco Firepower Management Center (FMC) や Stealthwatch など) を設定する必要があります。サブスクライバの詳細については、[サブスクライバ \(477 ページ\)](#) を参照してください。

始める前に

- Microsoft Active Directory サーバがネットワーク アドレス トランスレータの背後にないこと、およびネットワーク アドレス変換 (NAT) アドレスを持たないことを確認します。
- 参加操作の Microsoft Active Directory アカウントが有効であり、[次回ログイン時にパスワードを変更 (Change Password on Next Login)] を使用して設定されていないことを確認します。
- ISE でのスーパー管理者またはシステム管理者の権限があることを確認します。
- パッシブ ID サービスに使用する専用ポリシー サーバ (PSN) で、パッシブ ID サービスと pxGrid サービスを有効にします。[管理 (Administration)] > [システム (System)] > [展開 (Deployment)] を選択し、該当するノードを開き、[全般設定 (General Settings)] の下の [パッシブ ID サービスの有効化 (Enable Passive Identity Service)] と [pxGrid] をオンにします。
- ISE のエントリがドメイン ネーム サーバ (DNS) にあることを確認します。ISE からのクライアント マシンの逆引き参照を適切に設定していることを確認します。詳細については、[次を参照してください。DNS サーバ \(384 ページ\)](#)

ステップ 1 [ワーク センター (Work Centers)] > [PassiveID] を選択します。[パッシブ ID コネクタの概要 (Passive Identity Connector Overview)] 画面で [パッシブ ID ウィザード (Passive Identity Wizard)] をクリックします。

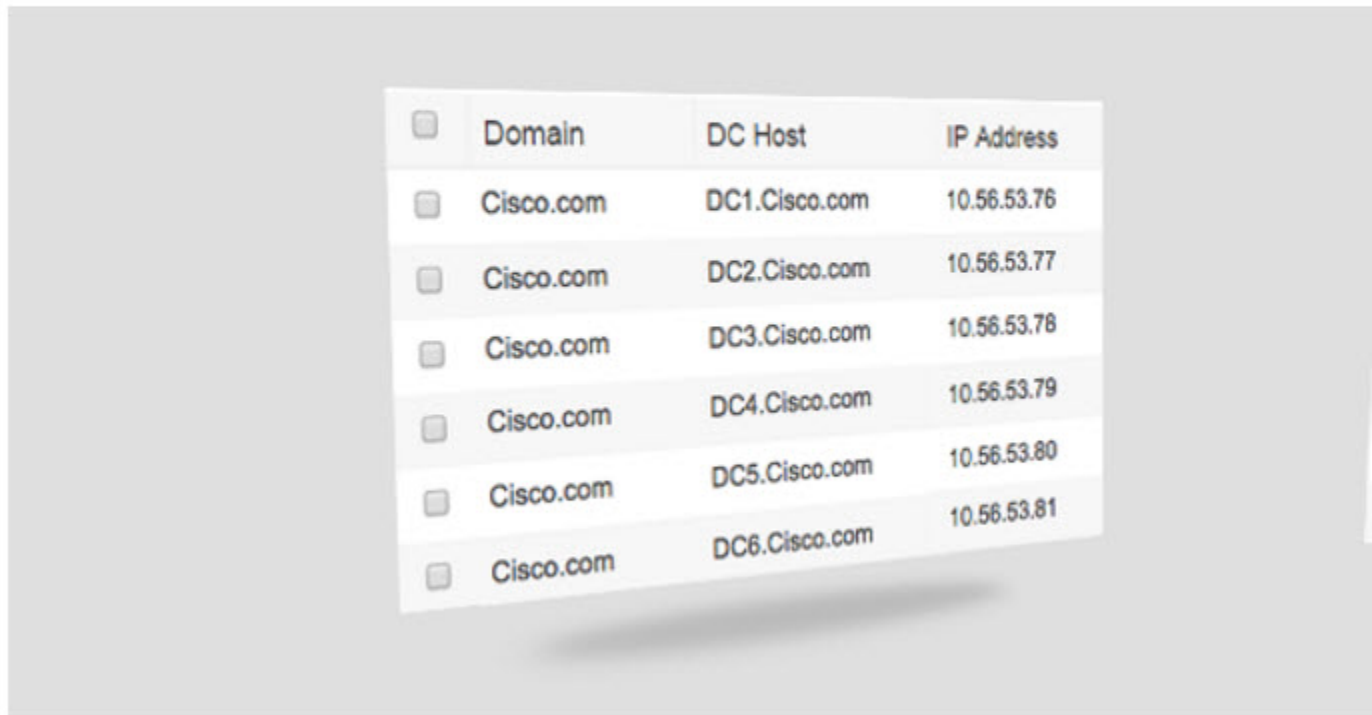
[PassiveID セットアップ (PassiveID Setup)] が表示されます。

図 32: [PassiveID セットアップ (PassiveID Setup)]

PassiveID Setup

[Welcome](#)
1 Active Directory
2 Groups
3 Domain Controllers
4 Custom selection
5 Summary

This wizard will setup passive identity using Active Directory.
 If you prefer to use Syslogs, SPAN or API providers, then exit wizard and
 Identity Providers of all types may be added at a later date.



ステップ 2 [次へ (Next)] をクリックしてウィザードを開始します。

ステップ 3 [Active Directory] ステップで、設定されているこの Active Directory 参加ポイントを容易に区別できる一意の名前を [参加ポイント名 (Join Point Name)] に入力し、Active Directory ドメインから、このノードが接続している Active Directory ドメインのドメイン名を入力し、Active Directory 管理者ユーザの名前とパスワードを入力します。Active Directory のこの設定とその他の設定の詳細については、[Active Directory の設定 \(429 ページ\)](#) を参照してください。

[クレデンシャルの保存 (Store Credentials)] を選択することを強く推奨します。これにより、管理者のユーザ名とパスワードが保存され、モニタ対象として設定されているすべてのドメインコントローラ (DC) に使用されます。

- ステップ 4** [次へ (Next)] をクリックし、Active Directory グループを定義し、追加してモニタするユーザ グループをすべてオンにします。
前のステップで設定した Active Directory 参加ポイントに基づいて Active Directory ユーザ グループが自動的に表示されます。
- ステップ 5** [次へ (Next)] を再度クリックして、[ドメインコントローラ (Domain Controllers)] ステップに進みます。
[ドメイン コントローラ (Domain Controllers)] ステップから、モニタ対象 DC を選択します。[カスタム (Custom)] を選択した場合は、次の画面でモニタする特定の DC を選択します。完了したら、[次へ (Next)] をクリックします。
特定の DC を選択したら、最初の Active Directory プロバイダーの作成は完了です。サマリー画面に、選択した DC とその詳細が表示されます。
- ステップ 6** [終了 (Exit)] をクリックして、ウィザードを終了します。

次のタスク

最初のプロバイダーとして Active Directory の設定を完了したら、追加のプロバイダー タイプも容易に設定できます。詳細については、[その他のパッシブ ID サービスプロバイダー \(433 ページ\)](#) を参照してください。さらに、定義したいいずれかのプロバイダーが収集したユーザ ID 情報を受信するためのサブスクライバも設定できるようになりました。詳細については、[サブスクライバ \(477 ページ\)](#) を参照してください。

Active Directory プロバイダーの管理

Active Directory 参加ポイントの作成と設定が完了したら、次の作業を行い Active Directory プロバイダーを管理します。

- [Active Directory 認証のためのユーザのテスト \(398 ページ\)](#)
- [ノードの Active Directory の参加の表示 \(399 ページ\)](#)
- [Active Directory の問題の診断 \(400 ページ\)](#)
- [Active Directory ドメインの脱退 \(389 ページ\)](#)
- [Active Directory の設定の削除 \(399 ページ\)](#)
- [Active Directory デバッグ ログの有効化 \(401 ページ\)](#)

Active Directory の設定

Active Directory (AD) は、安全性が高く正確なソースであり、ここからユーザ情報 (ユーザ名、IP アドレスなど) が取得されます。

参加ポイントを作成、編集することで Active Directory プロバイダーを作成、管理するには、[ワーク センター (Work Centers)] > [PassiveID] > [プロバイダー (Providers)] を選択し、左側のパネルから [Active Directory] を選択します。

詳細については、[Active Directory 参加ポイントの追加および参加ポイントへの Cisco ISE ノードの参加 \(386 ページ\)](#) を参照してください。

表 16: Active Directory 参加ポイント名の設定と [ドメインへの参加 (Join Domain)] 画面

フィールド	説明
[参加ポイント名 (Join Point Name)]	設定したこの参加ポイントを容易に区別できる一意の名前。
Active Directory ドメイン (Active Directory Domain)	このノードが接続している Active Directory ドメインのドメイン名。
[ドメイン管理者 (Domain Administrator)]	管理者権限を持つ Active Directory ユーザのユーザ プリンシパル名またはユーザ アカウント名。
[パスワード (Password)]	Active Directory で設定されているドメイン管理者のパスワード。
[組織単位の指定 (Specify Organizational Unit)]	管理者の組織単位の情報を入力します。
[クレデンシャルの保存 (Store Credentials)]	<p>[クレデンシャルの保存 (Store Credentials)] を選択することを強く推奨します。これにより、管理者のユーザ名とパスワードが保存され、モニタ対象として設定されているすべてのドメインコントローラ (DC) に使用されます。</p> <p>エンドポイントプローブの場合は、[クレデンシャルの保存 (Store Credentials)] を選択する必要があります。</p>

表 17: [Active Directory 参加/脱退 (Active Directory Join/Leave)] テーブル

フィールド	説明
ISE ノード (ISE Node)	インストール環境での特定のノードの URL。
[ISE ノードのロール (ISE Node Role)]	インストール環境でそのノードがプライマリ ノードまたはセカンダリ ノードのいずれであるかを指定します。
ステータス (Status)	ノードが Active Directory ドメインにアクティブに参加しているかどうかを示します。
ドメイン コントローラ	Active Directory に参加しているノードの場合、この列には Active Directory ドメインでノードが接続している特定のドメイン コントローラが表示されます。

フィールド	説明
サイト	Active Directory フォレストが ISE に参加する場合、このフィールドには、[Active Directory サイトおよびサービス (Active Directory Sites & Services)] 領域に示されるフォレスト内の特定の Active Directory サイトが示されます。

[プロバイダー (Providers)] > [Active Directory] > [PassiveID] を選択します。

表 18: [パッシブ ID ドメインコントローラ (DC) (Passive ID Domain Controllers (DC))] リスト

フィールド	説明
ドメイン (Domain)	ドメイン コントローラが存在しているサーバの完全修飾ドメイン名。
[DC ホスト (DC Host)]	ドメインコントローラが存在しているホスト。
サイト	Active Directory フォレストが ISE に参加する場合、このフィールドには、[Active Directory サイトおよびサービス (Active Directory Sites & Services)] 領域に示されるフォレスト内の特定の Active Directory サイトが示されます。
[IP アドレス (IP Address)]	ドメイン コントローラの IP アドレス。
[モニタ方法 (Monitor Using)]	次のいずれかの方法で、ユーザ ID 情報を取得するため Active Directory ドメイン コントローラをモニタします。 <ul style="list-style-type: none"> • [WMI] : WMI インフラストラクチャを使用して Active Directory を直接モニタします。 • [エージェント名 (Agent name)] : ユーザ情報を取得するために Active Directory をモニタするエージェントを定義している場合は、Agent プロトコルを選択し、ドロップダウン リストから使用するエージェントを選択します。エージェントの詳細については、#unique_573 を参照してください。

[プロバイダー (Providers)] > [Active Directory] > [PassiveID] を選択します。編集する AD 参加ポイントのリンクをクリックし、[PassiveID] タブに移動して [編集 (Edit)] をクリックし、リストから既存のドメイン コントローラを編集します。

表 19: [パッシブ ID ドメイン コントローラ (DC) (Passive ID Domain Controllers (DC))] 編集画面

フィールド	説明
[ホスト FQDN (Host FQDN)]	ドメイン コントローラが存在しているサーバの完全修飾ドメイン名を入力します。
説明	このドメイン コントローラを容易に特定できるように、一意の説明を入力します。
ユーザ名 (User Name)	Active Directory にアクセスするための管理者のユーザ名。
[パスワード (Password)]	Active Directory にアクセスするための管理者のパスワード。
プロトコル	次のいずれかの方法で、ユーザ ID 情報を取得するため Active Directory ドメイン コントローラをモニタします。 <ul style="list-style-type: none"> • [WMI] : WMI インフラストラクチャを使用して Active Directory を直接モニタします。 • [エージェント名 (Agent name)] : ユーザ情報を取得するために Active Directory をモニタするエージェントを定義している場合は、Agent プロトコルを選択し、ドロップダウン リストから使用するエージェントを選択します。エージェントの詳細については、#unique_573 を参照してください。

表 20: Active Directory グループ

説明
Active Directory グループは Active Directory から定義および管理されます。このノードに参加している Active Directory のグループは、このタブで確認できます。Active Directory の詳細については、 https://msdn.microsoft.com/en-us/library/bb742437.aspx を参照してください。

表 21 : *Active Directory* の詳細設定

フィールド	説明
[履歴期間 (History interval)]	すでに発生したユーザ ログインの情報をパッシブ ID サービスが読み取る期間。これは、パッシブ ID サービスの起動時または再起動時に、このサービスが使用不可であった間に生成されたイベントを確認するために必要となります。エンドポイントプローブがアクティブな場合、この期間の頻度が維持されます。
[ユーザセッションのエージングタイム (User session aging time)]	ユーザがログインできる時間です。パッシブ ID サービスでは、DC からの新しいユーザ ログインイベントが識別されますが、DC はユーザがログオフする時点を報告しません。エージングタイムを使用すると、Cisco ISE で、ユーザがログインする時間間隔を決定できます。
[NTLM プロトコル設定 (NTLM Protocol settings)]	Cisco ISE と DC の間の通信プロトコルとして [NTLMv1] または [NTLMv2] を選択できます。推奨されるデフォルトは [NTLMv2] です。

その他のパッシブ ID サービスプロバイダー

ISE が ID 情報 (パッシブ ID サービス) を、service をサブスクライブするコンシューマ (サブスクライバ) に提供できるようにするため、最初に ISE プローブを設定する必要があります。このプローブは ID プロバイダーに接続します。

ISE にマッピングされ、情報をアクティブに送信するプロバイダーは、[ライブセッション (Live Sessions)] メニューから、セッションディレクトリで確認できます。[ライブセッション (Live Sessions)] の詳細については、[RADIUS ライブセッション \(1454 ページ\)](#) を参照してください。

次の表に、ISE から使用可能なプロバイダーとプローブのすべてのタイプについて詳しく説明します。この章の残りの部分では、Active Directory 以外で使用するすべてのタイプについて説明していますが、Active Directory で使用できるタイプについては、専用の章で詳しく説明します。詳細については、[プローブおよびプロバイダーとしての Active Directory \(426 ページ\)](#) を参照してください。

定義できるプロバイダー タイプを次に示します。

表 22: プロバイダー タイプ

プロバイ ダータイプ (プロー ブ)	説明	送信元シス テム (プロ バイダー)	テクノロジー	収集されるユー ザ ID 情報	ドキュメント リ ンク
Active Directory (AD)	<p>ユーザ情報の取得元である安全性が高く正確で最も一般的なソース。</p> <p>プローブとして機能する場合、AD は WMI テクノロジーを使用して認証済みユーザ ID を送信します。</p> <p>また AD 自体が、プローブではなく、その他のプローブがユーザデータを取得するソース システム (プロバイダー) として機能します。</p>	Active Directory ド メイン コ ントローラ	WMI	<ul style="list-style-type: none"> ユーザ名 (User name) IP アドレス ドメイン 	プローブおよびプロバイダーとしての Active Directory (426 ページ)
エージェン ト (Agents)	<p>Active Directory ドメイン コントローラまたはメンバー サーバにインストールされているネイティブ 32 ビットアプリケーション。エージェン トプローブは、ユーザ ID 情報に Active Directory を使用する場合は簡単で効率的なソリューションです。</p>		ドメインコン トローラまたはメンバー サーバにイン ストールされ ているエー ジェント。	<ul style="list-style-type: none"> ユーザ名 (User name) IP アドレス ドメイン 	<p>Active Directory エージェント (436 ページ)</p> <p>(注) Active Directory エージェントは、Windows Server 2008 以降でのみサポートされます。</p>

プロバイダータイプ (プローブ)	説明	送信元システム (プロバイダー)	テクノロジー	収集されるユーザ ID 情報	ドキュメント リンク
エンドポイント (Endpoint)	設定されているその他のプローブに加えて、ユーザが接続しているかどうかを確認するため、常にバックグラウンドで実行されます。		WMI	ユーザが接続しているかどうか	エンドポイント プローブ (474 ページ)
SPAN	ネットワーク トラフィックをリッスンし、Active Directory データに基づいてユーザ ID 情報を抽出するため、ネットワーク スイッチに導入されています。		SPAN (スイッチにインストール) と Kerberos メッセージ	<ul style="list-style-type: none"> ユーザ名 (User name) IP アドレス ドメイン 	SPAN (447 ページ)
API プロバイダー	ISE が提供する RESTful API サービスを使用して、RESTful API クライアントと通信するようにプログラミングされている任意のシステムから、ユーザ ID 情報を収集します。	REST API クライアントと通信するようにプログラミングされている任意のシステム。	RESTful API。JSON 形式でサブスクライバに送信されるユーザ ID。	<ul style="list-style-type: none"> ユーザ名 (User name) IP アドレス ポート範囲 (Port range) ドメイン (Domain) 	API プロバイダー (441 ページ)

プロバイダタイプ (プローブ)	説明	送信元システム (プロバイダー)	テクノロジー	収集されるユーザ ID 情報	ドキュメントリンク
Syslog	syslog メッセージを解析し、ユーザ ID (MAC アドレスを含む) を取得します。	<ul style="list-style-type: none"> 標準 syslog メッセージ プロバイダー DHCP サーバ 	syslog メッセージ	<ul style="list-style-type: none"> ユーザ名 (User name) IP アドレス MAC アドレス ドメイン 	syslog プロバイダー (449 ページ)

Active Directory エージェント

パッシブ ID サービス ワーク センターから、ネイティブ 32 ビット アプリケーション、ドメイン コントローラ (DC) エージェントを、(設定に応じて) Active Directory (AD) ドメイン コントローラ (DC) またはメンバー サーバ上の任意の場所にインストールし、設定したサブスクライバにこれらの ID を送信します。エージェント プローブは、ユーザ ID 情報に Active Directory を使用する場合は簡単で効率的なソリューションです。エージェントは個別のドメインまたは AD ドメインにインストールできます。インストールされたエージェントは、1 分ごとに ISE にステータス更新情報を提供します。

エージェントは ISE が自動的にインストールおよび設定するか、またはユーザが手動でインストールすることができます。インストールが完了すると、次のようになります。

- エージェントとその関連ファイルはパス **Program Files/Cisco/Cisco ISE PassiveID Agent** にインストールされています。
- エージェントのロギング レベルを指定する **PICAgent.exe.config** という設定ファイルがインストールされます。この設定ファイル内でロギング レベルを手動で変更できます。
- CiscoISEPICAgent.log ファイルにはすべてのロギング メッセージが保存されます。
- nodes.txt ファイルには、展開内でエージェントが通信できるすべてのノードのリストが含まれています。エージェントはリストの最初のノードと通信します。このノードと通信できない場合、エージェントはリストのノード順序に従ってノードとの通信を試行します。手動でのインストールの場合、このファイルを開き、ノード IP アドレスを入力する必要があります。(手動または自動での) インストールの完了後にこのファイルを変更するには、このファイルを手動で更新する必要があります。ファイルを開き、ノード IP アドレスを必要に応じて追加、変更、または削除します。
- Cisco ISE PassiveID Agent サービスはマシン上で稼働します。このサービスは [Windows サービス (Windows Services)] ダイアログボックスから管理できます。

- ISE は最大 100 個のドメイン コントローラをサポートでき、それぞれのエージェントは最大 10 個のドメイン コントローラをモニタできます。



(注) 100 個のドメイン コントローラをモニタするには、10 個のエージェントを設定する必要があります。



(注) Active Directory エージェントは、Windows Server 2008 以降でのみサポートされます。

エージェントをインストールできない場合、パッシブ ID サービスには Active Directory プローブを使用します。詳細については、[プローブおよびプロバイダーとしての Active Directory \(426 ページ\)](#) を参照してください。

Active Directory (AD) エージェントの自動インストールおよび展開

ユーザ ID についてドメイン コントローラをモニタするようにエージェント プロバイダーを設定するときには、エージェントがメンバー サーバまたはドメイン コントローラのいずれかにインストールされている必要があります。エージェントは ISE が自動的にインストールするか、またはユーザが手動でインストールすることができます。手動または自動でのインストール後に、インストールされたエージェントが、デフォルト WMI ではなく指定のドメイン コントローラをモニタするように設定する必要があります。このプロセスでは、自動インストールを有効にし、ドメイン コントローラをモニタするようにエージェントを設定する方法について説明します。

始める前に

始める前に：

- サーバ側からの関連 DNS サーバの逆引き参照を設定します。ISE の DNS サーバ設定要件の詳細については、次を参照してください。 [DNS サーバ \(384 ページ\)](#)
- エージェント用に指定されたマシンで Microsoft .NET Framework がバージョン 4.0 以上に更新されていることを確認します。.NET フレームワークの詳細については、<https://www.microsoft.com/net/framework> を参照してください。
- アクティブなパッシブ ID および pxGrid サービス。詳細については、[初期セットアップと設定 \(424 ページ\)](#) を参照してください。
- AD 参加ポイントを作成し、1 つ以上のドメイン コントローラを追加します。参加ポイントの作成の詳細については、[プローブおよびプロバイダーとしての Active Directory \(426 ページ\)](#) を参照してください。

AD、エージェント、SPAN、および syslog プローブで AD ユーザ グループを使用します。AD グループの詳細については、[Active Directory ユーザ グループの設定 \(390 ページ\)](#) を参照してください。

-
- ステップ 1** 現在設定されているすべてのドメインコントローラ (DC) エージェントを表示し、既存のエージェントを編集、削除し、新しいエージェントを設定するには、[ワークセンター (WorkCenters)] > [PassiveID] > [プロバイダー (Providers)] を選択し、左側のパネルから [エージェント (Agents)] を選択します。
- ステップ 2** 新しいエージェントを追加するには、テーブルの上部で [追加 (Add)] をクリックします。既存のクライアントを編集または変更するには、テーブルでエージェントをオンにし、テーブル上部で [編集 (Edit)] をクリックします。
- ステップ 3** 新しいエージェントを作成し、この設定で指定するホストに自動的にインストールするには、[新規エージェントの展開 (Deploy New Agent)] を選択します。
- ステップ 4** クライアントを正しく設定するため、すべての必須フィールドに入力します。詳細については、[Active Directory \(AD\) エージェントの設定 \(440 ページ\)](#) を参照してください。
- ステップ 5** [展開 (Deploy)] をクリックします。
設定で指定したドメインに基づいてエージェントが自動的にホストにインストールされ、設定が保存されます。エージェントは [エージェント (Agents)] テーブルに表示されます。これで、指定したドメインコントローラにこのエージェントを適用できます。これについては以降のステップで説明します。
- ステップ 6** [ワークセンター (WorkCenters)] > [PassiveID] > [プロバイダー (Providers)] を選択し、左側のパネルから [Active Directory] を選択して、現在設定されているすべての参加ポイントを表示します。
- ステップ 7** 作成したエージェントを有効にする参加ポイントのリンクをクリックします。
- ステップ 8** 前提条件の一部として追加したドメインコントローラを使用するため、[パッシブ ID (Passive ID)] タブを選択します。
- ステップ 9** 作成したエージェントを使用してモニタするドメインコントローラをオンにし、[編集 (Edit)] をクリックします。
- ステップ 10** 表示されるダイアログボックスで、必須フィールドに値が入力されていることを確認し、[プロトコル (Protocol)] ドロップダウンから [エージェント (Agent)] を選択します。表示される [エージェント (Agent)] フィールドのドロップダウンリストから、作成したエージェントを選択します。エージェントのユーザ名およびパスワードのクレデンシャルを作成している場合は、このクレデンシャルを入力して [保存 (Save)] をクリックします。
ドメインコントローラに対してエージェントが有効になり、ダイアログボックスが閉じます。
-

Active Directory (AD) エージェントの手動インストールおよび展開

ユーザ ID についてドメインコントローラをモニタするようにエージェントプロバイダーを設定するときには、エージェントがメンバーサーバまたはドメインコントローラのいずれかにインストールされている必要があります。エージェントは ISE が自動的にインストールするか、またはユーザが手動でインストールすることができます。手動または自動でのインストール後に、インストールされたエージェントが、デフォルト WMI ではなく指定のドメインコントローラをモニタするように設定する必要があります。このプロセスでは、エージェントを手動でインストールし、ドメインコントローラをモニタするように設定する方法について説明します。

始める前に

始める前に：

- サーバ側からの関連 DNS サーバの逆引き参照を設定します。ISE の DNS サーバ設定要件の詳細については、次を参照してください。 [DNS サーバ \(384 ページ\)](#)
- エージェント用に指定されたマシンで Microsoft .NET Framework がバージョン 4.0 以上に更新されていることを確認します。.NET フレームワークの詳細については、<https://www.microsoft.com/net/framework>を参照してください。
- アクティブなパッシブ ID および pxGrid サービス。詳細については、[初期セットアップと設定 \(424 ページ\)](#) を参照してください。
- AD 参加ポイントを作成し、1 つ以上のドメイン コントローラを追加します。参加ポイントの作成の詳細については、[プローブおよびプロバイダーとしての Active Directory \(426 ページ\)](#) を参照してください。

AD、エージェント、SPAN、および syslog プローブで AD ユーザ グループを使用します。AD グループの詳細については、[Active Directory ユーザ グループの設定 \(390 ページ\)](#) を参照してください。

-
- ステップ 1** 現在設定されているすべてのドメインコントローラ (DC) エージェントを表示し、既存のエージェントを編集、削除し、新しいエージェントを設定するには、**[ワーク センター (Work Centers)] > [PassiveID] > [プロバイダー (Providers)]** を選択し、左側のパネルから **[エージェント (Agents)]** を選択します。
- ステップ 2** **[エージェントのダウンロード (Download Agent)]** をクリックし、手動でインストールするための **picagent-installer.zip** ファイルをダウンロードします。
このファイルは Windows の標準ダウンロード フォルダにダウンロードされます。
- ステップ 3** ZIP ファイルを指定のホスト マシンに保存してインストールを実行します。
- ステップ 4** ISE GUI から **[ワーク センター (Work Centers)] > [PassiveID] > [プロバイダー (Providers)]** をもう一度選択し、左側のパネルから **[エージェント (Agents)]** を選択します。
- ステップ 5** 新しいエージェントを設定するには、テーブルの上部で **[追加 (Add)]** をクリックします。既存のクライアントを編集または変更するには、テーブルでエージェントをオンにし、テーブル上部で **[編集 (Edit)]** をクリックします。
- ステップ 6** すでにホストマシンにインストールしているエージェントを設定するには、**[既存のエージェントの登録 (Register Existing Agent)]** を選択します。
- ステップ 7** クライアントを正しく設定するため、すべての必須フィールドに入力します。詳細については、[Active Directory \(AD\) エージェントの設定 \(440 ページ\)](#) を参照してください。
- ステップ 8** **[保存 (Save)]** をクリックします。
エージェント設定が保存されます。エージェントは **[エージェント (Agents)]** テーブルに表示されます。これで、指定したドメイン コントローラにこのエージェントを適用できます。これについては以降のステップで説明します。
- ステップ 9** **[ワーク センター (Work Centers)] > [PassiveID] > [プロバイダー (Providers)]** を選択し、左側のパネルから **[Active Directory]** を選択して、現在設定されているすべての参加ポイントを表示します。
- ステップ 10** 作成したエージェントを有効にする参加ポイントのリンクをクリックします。

- ステップ 11** 前提条件の一部として追加したドメイン コントローラを使用するため、[パッシブ ID (Passive ID)] タブを選択します。
- ステップ 12** 作成したエージェントを使用してモニタするドメインコントローラをオンにし、[編集 (Edit)] をクリックします。
- ステップ 13** 表示されるダイアログボックスで、必須フィールドに値が入力されていることを確認し、[プロトコル (Protocol)] ドロップダウンから [エージェント (Agent)] を選択します。表示される [エージェント (Agent)] フィールドのドロップダウンリストから、作成したエージェントを選択します。エージェントのユーザ名およびパスワードのクレデンシアルを作成している場合は、このクレデンシアルを入力して [保存 (Save)] をクリックします。
ドメイン コントローラに対してエージェントが有効になり、ダイアログボックスが閉じます。

エージェントのアンインストール

自動または手動でインストールされたエージェントは、Windows から直接（手動で）簡単にアンインストールできます。

- ステップ 1** [Windows] ダイアログで [プログラムと機能 (Programs and Features)] に移動します。
- ステップ 2** インストールされているプログラムのリストで [Cisco ISE PassiveID エージェント (Cisco ISE PassiveID Agent)] を見つけて選択します。
- ステップ 3** [アンインストール (Uninstall)] をクリックします。

Active Directory (AD) エージェントの設定

ISE が、さまざまなドメイン コントローラ (DC) からユーザ ID 情報を取得し、その情報をパッシブ ID サービス サブスクリバに配信するために、ネットワーク内の指定されたホストにエージェントを自動的にインストールすることを許可します。

エージェントを作成および管理するには、[プロバイダー (Providers)] > [エージェント (Agents)] を選択します。 [Active Directory \(AD\) エージェントの自動インストールおよび展開 \(437 ページ\)](#) を参照してください。

[エージェント (Agents)] テーブルで現在のエージェントのステータスを確認します。[プロバイダー (Providers)] > [エージェント (Agents)] を選択します。

表 23: [エージェント (Agents)] テーブル

フィールド	説明
[名前 (Name)]	設定したエージェント名。
ホスト	エージェントがインストールされているホストの完全修飾ドメイン名。
モニタリング (Monitoring)	指定されたエージェントがモニタするドメイン コントローラのカンマ区切りリストです。

表 24: [新規エージェント (Agents New)]

フィールド	説明
[新規エージェントの展開 (Deploy New Agent)] または [既存のエージェントの登録 (Register Existing Agent)]	<ul style="list-style-type: none"> • [新規エージェントの展開 (Deploy New Agent)] : 指定されたホストに新規エージェントをインストールします。 • [既存のエージェントの登録 (Register Existing Agent)] : ホストにエージェントを手動でインストールし、パッシブ ID サービス がサービスを有効にできるようにするため、この画面でそのエージェントを設定します。
[名前 (Name)]	エージェントを容易に把握できる名前を入力します。
説明	エージェントを容易に把握できる説明を入力します。
[ホスト FQDN (Host FQDN)]	エージェントがインストールされているホスト(既存のエージェントの登録の場合) またはインストールされるホスト (自動展開の場合) の完全修飾ドメイン名です。
ユーザ名 (User Name)	エージェントをインストールするホストにアクセスするためのユーザ名を入力します。パッシブ ID サービス はこれらのクレデンシャルを使用してエージェントを自動的にインストールします。
[パスワード (Password)]	エージェントをインストールするホストにアクセスするためのパスワードを入力します。パッシブ ID サービス はこれらのクレデンシャルを使用してエージェントを自動的にインストールします。

API プロバイダー

Cisco ISE の API プロバイダー機能では、カスタマイズしたプログラムまたはターミナルサーバ (TS) エージェントから組み込み ISE パッシブ ID サービス REST API サービスにユーザ ID 情報をプッシュできます。これにより、ネットワークからプログラミング可能なクライアントをカスタマイズして、任意のネットワークアクセス制御 (NAC) システムから収集されたユーザ ID をこのサービスに送信するようになります。さらに Cisco ISE API プロバイダーにより、すべてのユーザの IP アドレスが同一であるが、各ユーザに固有のポートが割り当てられるネットワーク アプリケーション (Citrix サーバの TS-Agent など) と対話できます。

たとえば、Active Directory (AD) サーバに対して認証されたユーザの ID マッピングを提供する Citrix サーバで稼働するエージェントは、新しいユーザがログインまたはログオフするたびに、ユーザセッションを追加または削除する REST 要求を ISE に送信できます。ISE は、クライアントから送信されたユーザ ID 情報 (IP アドレス、割り当てられたポートなど) を取得し、事前に設定されているサブスクライバ (Cisco Firepower Management Center (FMC) など) に送信します。

ISE REST API フレームワークは、HTTPS プロトコルを介した REST サービスを実装し (クライアント証明書の検証は不要)、ユーザ ID 情報が JSON (JavaScript Object Notation) 形式で送信されます。JSON の詳細については、<http://www.json.org/> を参照してください。

ISE REST API サービスは、1 つのシステムに同時にログインしている複数のユーザを区別するため、ユーザ ID を解析し、その情報をポート範囲にマッピングします。ポートがユーザに割り当てられるたびに、API がメッセージを ISE に送信します。

REST API プロバイダーのフロー

カスタマイズしたクライアントを ISE のプロバイダーとして宣言し、そのカスタマイズしたプログラム (クライアント) が RESTful 要求を送信できるようにして、ISE からカスタマイズしたクライアントへのブリッジを設定している場合、ISE REST サービスは次のように機能します。

1. ISE はクライアント認証のために認証トークンを必要とします。通信開始時と、ISE から以前のトークンの期限が切れたことが通知されるたびに、クライアントマシンのカスタマイズしたプログラムから認証トークンを求める要求が送信されます。この要求への応答としてトークンが返されます。これによりクライアントと ISE サービス間の継続的な通信が可能になります。
2. ユーザがネットワークにログインすると、クライアントはユーザ ID 情報を取得し、API Add コマンドを使用してこの情報を ISE REST サービスに送信します。
3. ISE はユーザ ID 情報を受信してマッピングします。
4. ISE はマッピングされたユーザ ID 情報をサブスクライバに送信します。
5. 必要な場合は常に、カスタマイズされたマシンはユーザ情報削除要求を送信できます。このためには、Remove API コールを送信し、Add コールの送信時に応答として受信したユーザ ID を含めます。

ISE での REST API プロバイダーの操作

ISE で REST サービスをアクティブにするには、次の手順に従います。

1. クライアント側を設定します。詳細については、クライアント ユーザ マニュアルを参照してください。
2. パッシブ ID サービスと pxGrid サービスをアクティブにします。詳細については、[初期セットアップと設定 \(424 ページ\)](#) を参照してください。

3. DNS サーバを適切に設定していることを確認します。これには、ISE からのクライアントマシンの逆引きの設定も含まれます。の DNS サーバ設定の要件の詳細については、次を参照してください。 [DNS サーバ \(384 ページ\)](#)
4. [パッシブ ID サービス の ISE REST サービスへのブリッジの設定 \(443 ページ\)](#) を参照してください。



(注) TS-Agent と連携するように API プロバイダーを設定するには、ISE からそのエージェントへのブリッジの作成時に TS-Agent 情報を追加します。その後、TS-Agent のマニュアルで API コールの送信について確認してください。

5. 認証トークンを生成し、追加要求と削除要求を API サービスに送信します。 [#unique_581](#)。

パッシブ ID サービス の ISE REST サービスへのブリッジの設定

ISE REST API サービスが特定のクライアントから情報を受信できるようにするには、まず ISE でその特定のクライアントを定義する必要があります。異なる IP アドレスを使用して複数の REST API クライアントを定義できます。

始める前に

始める前に：

- パッシブ ID サービスと pxGrid サービスをアクティブにしていることを確認します。詳細については、[初期セットアップと設定 \(424 ページ\)](#) を参照してください。
- DNS サーバを適切に設定していることを確認します。これには、ISE からのクライアントマシンの逆引きの設定も含まれます。ISE の DNS サーバ設定要件の詳細については、次を参照してください。 [DNS サーバ \(384 ページ\)](#)

-
- ステップ 1** 現在設定されているすべてのクライアントを表示し、既存のクライアントを編集、削除し、新しいクライアントを設定するには、[ワーク センター (Work Centers)] > [PassiveID] > [プロバイダー (Providers)] を選択し、左側のパネルから [API プロバイダー (API Providers)] を選択します。
[API プロバイダー (API Providers)] テーブルが表示されます。このテーブルには既存の各クライアントのステータス情報が含まれています。
 - ステップ 2** 新しいクライアントを追加するには、テーブルの上部で [追加 (Add)] をクリックします。既存のクライアントを編集または変更するには、テーブルでクライアントをオンにし、テーブル上部で [編集 (Edit)] をクリックします。
 - ステップ 3** クライアントを正しく設定するため、すべての必須フィールドに入力します。詳細については、[API プロバイダーの設定 \(444 ページ\)](#) を参照してください。
 - ステップ 4** [送信 (Submit)] をクリックします。

クライアント設定が保存され、更新された [API プロバイダー (API Providers)] テーブルが画面に表示されます。これで、クライアントは ISE REST サービスにポストを送信できるようになりました。

次のタスク

認証トークンとユーザ ID を ISE REST サービスに送信するように、カスタマイズしたクライアントをセットアップします。[パッシブ ID REST サービスへの API コールの送信 \(444 ページ\)](#) を参照してください。

パッシブ ID REST サービスへの API コールの送信

始める前に

[パッシブ ID サービス の ISE REST サービスへのブリッジの設定 \(443 ページ\)](#)

- ステップ 1 Cisco ISE URL をブラウザのアドレス バーに入力します (たとえば `https://<ise hostname or ip address>/admin/`)。
- ステップ 2 ISE GUI の [API プロバイダー (API Providers)] 画面で指定および設定したユーザ名とパスワードを入力します。詳細については、[パッシブ ID サービス の ISE REST サービスへのブリッジの設定 \(443 ページ\)](#) を参照してください。
- ステップ 3 Enter キーを押します。
- ステップ 4 ターゲット ノードの [URL アドレス (URL Address)] フィールドに API コールを入力します。
- ステップ 5 [送信 (Send)] をクリックして API コールを発行します。

次のタスク

さまざまな API コールとそのスキーマおよび結果の詳細については、[API コール \(445 ページ\)](#) を参照してください。

API プロバイダーの設定

[プロバイダー (Providers)] > [API プロバイダー (Providers)] を選択して、の新しい REST API クライアントを設定します。



(注) 次のようにリクエスト コールを使用して完全な API 定義とオブジェクト スキーマを取得できます。

- 完全な API の指定 (wadl) : https://YOUR_ISE:9094/application.wadl
- API モデルとオブジェクト スキーマ : https://YOUR_ISE:9094/application.wadl/xsd0.xsd

表 25: API プロバイダーの設定

フィールド	説明
[名前 (Name)]	このクライアントを他のクライアントから容易に区別できる一意の名前を入力します。
説明	このクライアントのわかりやすい説明を入力します。
ステータス (Status)	設定完了後すぐにクライアントが REST サービスとやりとりできるようにするには、[有効 (Enabled)] を選択します。
[ホスト/IP (Host/ IP)]	クライアント ホスト マシンの IP アドレスを入力します。DNS サーバを適切に設定していることを確認します。これには、ISEからのクライアント マシンの逆引きの設定も含まれます。
ユーザ名 (User name)	REST サービスへの送信時に使用する一意のユーザ名を作成します。
[パスワード (Password)]	REST サービスへの送信時に使用する一意のパスワードを作成します。

API コール

Cisco ISE でパッシブ ID サービスのユーザ ID イベントを管理するには、次の API コールを使用します。

目的：認証トークンの生成

• 要求

POST

`https://<PIC IP アドレス>:9094/api/fmi_platform/v1/identityauth/generatetoken`

この要求には BasicAuth 許可ヘッダーが含まれている必要があります。ISE-PIC GUI で以前に作成した API プロバイダーのクレデンシャルを提供します。詳細については、[API プロバイダーの設定 \(444 ページ\)](#) を参照してください。

• 応答ヘッダー

このヘッダーには X-auth-access-token が含まれています。これは、追加の REST 要求を送信するときに使用するトークンです。

• 応答本文

HTTP 204 No Content

目的：ユーザの追加

- 要求

POST

https://<PIC IP アドレス>:9094/api/identity/v1/identity/useridentity

POST 要求のヘッダーに X-auth-access-token を追加します。（例：ヘッダー：X-auth-access-token、値：f3f25d81-3ac5-43ee-bbfb-20955643f6a7）

- 応答ヘッダー

201 Created

- 応答本文

```
{
  "user": "<ユーザ名>",
  "srcPatRange": {
    "userPatStart": "<ユーザ PAT 開始値>",
    "userPatEnd": "<ユーザ PAT 終了値>",
    "patRangeStart": "<PAT 範囲開始値>"
  },
  "srcIpAddress": "<src IP アドレス>",
  "agentInfo": "<エージェント名>",
  "timestamp": "<ISO_8601 形式、例：'YYYY-MM-DDTHH:MM:SSZ' >",
  "domain": "<ドメイン>"
}
```

- 注記 (Notes)

- 上記の JSON で 1 つの IP ユーザ バインディングを作成するには srcPatRange を削除します。
- 応答本文には「ID」（作成されたユーザ セッション バインディングの固有識別子）が含まれています。削除するユーザを指定する DELETE 要求を送信するときに、この ID を使用してください。
- この応答には、新たに作成されたユーザ セッション バインディングの URL であるセルフ リンクも含まれています。

目的：ユーザの削除

- 要求

DELETE

`https://<PIC IP アドレス>:9094/api/identity/v1/identity/useridentity/<id>`

<id> に、Add 応答で受信した ID を入力します。

DELETE 要求のヘッダーに X-auth-access-token を追加します。（例：ヘッダー：X-auth-access-token、値：f3f25d81-3ac5-43ee-bbfb-20955643f6a7）

- 応答ヘッダー

200 OK

- 応答本文

応答本文には、削除されたユーザ セッション バインディングの詳細が含まれています。

SPAN

SPAN は、ISE がネットワークをリッスンし、ユーザ情報を取得できるようにユーザが容易に設定できるようにする、パッシブ ID サービスです。このとき、Active Directory が ISE と直接連携するように設定する必要はありません。SPAN はネットワーク トラフィックをスニフリングし、特に Kerberos メッセージを調べ、Active Directory により保存されているユーザ ID 情報を抽出し、その情報を ISE に送信します。ISE は次にその情報を解析し、最終的にはユーザ名、IP アドレス、およびドメイン名を、ISE から既に設定しているサブスクライバに送信します。

SPAN がネットワークをリッスンし、Active Directory ユーザ情報を抽出できるようにするには、ISE と Active Directory の両方がネットワーク上の同一スイッチに接続している必要があります。これにより、SPAN は Active Directory からすべてのユーザ ID データをコピーおよびミラーリングできます。

SPAN により、ユーザ情報は次のように取得されます。

1. ネットワーク上のユーザ エンドポイントがログインします。
2. ログイン データとユーザ データは Kerberos メッセージに保存されます。
3. ユーザがログインし、ユーザ データがスイッチを通過すると、SPAN がネットワーク データをミラーリングします。
4. ISE は、ユーザ情報を取得するためネットワークをリッスンし、ミラーリングされたデータをスイッチから取得します。
5. ISE はユーザ情報を解析し、パッシブ ID マッピングを更新します。
6. ISE は解析後のユーザ情報をサブスクライバに送信します。

SPAN の使用

始める前に

ISE がネットワーク スイッチから SPAN トラフィックを受信できるようにするには、最初にそのスイッチをリッスンするノードとノード インターフェイスを定義する必要があります。イン

ストールされている複数の ISE ノードをリッスンするには、SPAN を設定します。ネットワークをリッスンするように設定できるインターフェイスは、ノードごとに1つのみです。また、リッスンするために使用するインターフェイスは SPAN 専用である必要があります。

開始する前に、パッシブ ID サービスと pxGrid サービスをアクティブにしていることを確認します。SPAN の設定に使用可能なインターフェイスのリストには、パッシブ ID が有効なノードだけが表示されます。詳細については、[初期セットアップと設定（424ページ）](#)を参照してください。

また、次の操作を行う必要があります。

- ネットワークで Active Directory が設定されていることを確認します。
- スイッチが ISE と通信できることを確認するために、Active Directory に接続しているネットワーク上のスイッチで CLI を実行します。
- AD からネットワークをミラーリングするようにスイッチを設定します。
- SPAN 専用の ISE ネットワーク インターフェイス カード（NIC）を設定します。この NIC は SPAN トラフィック専用で使用されます。
- SPAN 専用の NIC が、コマンドライン インターフェイスからアクティブにされていることを確認します。
- Kerberos トラフィックのみを SPAN ポートに送信する VACL を作成します。

ステップ 1 [ワーク センター（Work Centers）] > [PassiveID] > [プロバイダー（Providers）] を選択し、次に左側のパネルから [SPAN] を選択して SPAN を設定します。

ステップ 2 （注） GigabitEthernet0 ネットワーク インターフェイス カード（NIC）は使用可能なままにし、SPAN の設定には使用可能な別の NIC を選択することが推奨されます。GigabitEthernet0 は、システム管理の目的で使用されます。

わかりやすい説明を入力し（オプション）、[有効（Enabled）]ステータスを選択し、ネットワークスイッチのリッスンに使用する関連 NIC とノードを選択します。詳細については、[SPAN 設定（448 ページ）](#)を参照してください。

ステップ 3 [保存（Save）] をクリックします。

SPAN 設定が保存され、ISE-PICISE がネットワーク トラフィックをアクティブにリッスンします。

SPAN 設定

SPAN をクライアント ネットワークにインストールすることで、展開した各ノードから、ISE がユーザ ID を受信することを簡単に設定できます。

表 26: SPAN 設定

フィールド	説明
説明	現在有効なノードとインターフェイスがわかる固有の説明を入力します。
ステータス	設定完了後すぐにクライアントを有効にするには、[有効化 (Enabled)] を選択します。
[インターフェイス NIC (Interface NIC)]	<p>ISE にインストールされている 1 つ以上のノードを選択してから、選択したノードごとに、ネットワークをリッスンして情報を得るノードインターフェイスを選択します。</p> <p>(注) GigabitEthernet0 NIC を引き続き使用可能にし、SPAN の設定には他に使用可能な NIC を選択することが推奨されます。GigabitEthernet0 は、システム管理の目的で使用されます。</p>

syslog プロバイダー

syslog 機能により、パッシブ ID サービスは syslog メッセージを配信する任意のクライアント (ID データ プロバイダー) からの syslog メッセージを解析し、MAC アドレスなどのユーザ ID 情報を送信します。syslog メッセージには、通常の syslog メッセージ (InfoBlox、Blue Coat、BlueCat、Lucent などのプロバイダーからのメッセージ) と DHCP syslog メッセージがあります。このマッピングされたユーザ ID データがサブスクライバに配信されます。

管理者がパッシブ ID および pxGrid サービスをアクティブにし、GUI から syslog クライアントを設定すると、パッシブ ID サービスはさまざまなプロバイダーから受信した syslog メッセージを使用します。管理者はプロバイダーの設定時に、接続方法 (TCP または UDP) と解析に使用する syslog テンプレートを指定します。



(注) 設定されている接続タイプが TCP であり、メッセージヘッダーに問題があるためにホスト名を解析できない場合、ISE はパケットで受信した IP アドレスを、ISE で設定されている syslog メッセージのプロバイダー リストのすべてのプロバイダーの IP アドレスと照合しようとします。このリストを表示するには、[ワーク センター (Work Centers)] > [PassiveID] > [プロバイダー (Providers)] > [syslog プロバイダー (Syslog Providers)] を選択します。メッセージヘッダーを調べ、解析が正常に実行されるように、必要に応じてカスタマイズすることが推奨されます。ヘッダーのカスタマイズの詳細については、[#unique_587](#) を参照してください。

設定が完了したら、syslog プローブは受信した syslog メッセージを ISE パーサーに送信します。パーサーはユーザ ID 情報をマッピングし、その情報を ISE に公開します。次に ISE が、

解析およびマッピングされたユーザ ID 情報を パッシブ ID サービス サブスクライバに配信します。



- (注) DHCP syslog メッセージにはユーザ名は含まれていません。したがって、これらのメッセージはパーサーから遅れて配信されます。これにより ISE は、ユーザ ID 情報を正しく解析して配信するために、最初にローカルセッション ディレクトリに登録されているユーザ ([ライブ セッション (Live Sessions)] で表示) を調べ、その後各ユーザの IP アドレスと受信した DHCP syslog メッセージに指定されている IP アドレスを照合してユーザ照合を試行します。DHCP syslog メッセージから受信したデータが、現在ログインしているユーザに一致しない場合、メッセージは解析されず、ユーザ ID は配信されません。

ISE からの syslog メッセージを解析してユーザ ID を取得するには、次の操作を行います。

- ユーザ ID データの送信元 syslog クライアントを設定します: [syslog クライアントの設定 \(450 ページ\)](#)
- 1 つのメッセージ ヘッダーをカスタマイズします: [syslog ヘッダーのカスタマイズ \(458 ページ\)](#)
- テンプレートを作成してメッセージ本文をカスタマイズします: [syslog メッセージ本文のカスタマイズ \(456 ページ\)](#)
- 解析に使用するメッセージテンプレートとして syslog クライアントを設定する場合には、ISE で事前に定義されているメッセージテンプレートを使用します。あるいは、これらの事前定義テンプレートに基づいてヘッダーまたは本文のテンプレートをカスタマイズします。 [syslog 事前定義メッセージテンプレートの使用 \(462 ページ\)](#)

syslog クライアントの設定

ISE が特定のクライアントからの syslog メッセージをリッスンできるようにするには、最初に ISE でその特定のクライアントを定義する必要があります。異なる IP アドレスを使用して複数のプロバイダーを定義できます。

始める前に

開始する前に、パッシブ ID サービスと pxGrid サービスをアクティブにしていることを確認します。詳細については、[初期セットアップと設定 \(424 ページ\)](#) を参照してください。

- ステップ 1** 現在設定されているすべてのクライアントを表示し、既存のクライアントを編集、削除し、新しいクライアントを設定するには、[ワーク センター (Work Centers)] > [PassiveID] > [syslog プロバイダー (Syslog Providers)] を選択し、左側のパネルから [エージェント (Agents)] を選択します。[syslog プロバイダー (syslog Providers)] テーブルが表示されます。このテーブルには既存の各クライアントのステータス情報が含まれています。

- ステップ 2** 新しい syslog クライアントを設定するには、テーブルの上部で [追加 (Add)] をクリックします。以前に設定したクライアントを編集または変更するには、テーブルでクライアントをオンにし、テーブル上部で [編集 (Edit)] をクリックします。
- ステップ 3** クライアントを正しく設定するため、すべての必須フィールドを入力し（詳細については[Syslog の設定 \(Syslog Settings\)](#) (451 ページ) を参照）、必要に応じてメッセージテンプレートを作成します（詳細については[syslog メッセージ本文のカスタマイズ](#) (456 ページ) を参照）。
- ステップ 4** [送信 (Submit)] をクリックします。
クライアント設定が保存され、更新された [syslog プロバイダー (Syslog Providers)] テーブルが画面に表示されます。

Syslog の設定 (Syslog Settings)

特定のクライアントから syslog メッセージによってユーザ ID (MAC アドレスを含む) を受信するように ISE を設定します。異なる IP アドレスを使用して複数のプロバイダーを定義できます。

[ワーク センター (Work Centers)] > [PassiveID] > [プロバイダー (Providers)] を選択し、左側のパネルから [syslog プロバイダー (Syslog Providers)] を選択し、テーブルで [追加 (Add)] をクリックして、新しい syslog クライアントを作成します。

表 27: syslog プロバイダー

フィールド	説明
[名前 (Name)]	設定したこのクライアントを容易に区別できる一意の名前を入力します。
説明	この syslog プロバイダーのわかりやすい説明。
ステータス (Status)	設定完了後すぐにクライアントを有効にするには、[有効化 (Enabled)] を選択します。
ホスト	ホスト マシンの FQDN を入力します。

フィールド	説明
接続タイプ (Connection Type)	<p>ISE が syslog メッセージをリスンするチャネルを指定するため、UDP または TCP を入力します。</p> <p>(注) 設定されている接続タイプが TCP であり、メッセージヘッダーに問題があるためにホスト名を解析できない場合、ISE-PICISE はパケットで受信した IP アドレスを、ISE-PICISE で設定されている syslog メッセージのプロバイダーリストのすべてのプロバイダーの IP アドレスと照合しようとします。</p> <p>このリストを表示するには、[ワークセンター (Work Centers)] > [PassiveID] > [プロバイダー (Providers)] > [syslog プロバイダー (Syslog Providers)] を選択します。メッセージヘッダーを調べ、解析が正常に実行されるように、必要に応じてカスタマイズすることが推奨されます。ヘッダーのカスタマイズの詳細については、#unique_587 を参照してください。</p>

フィールド	説明
テンプレート (Template)	

フィールド	説明
	<p>テンプレートにより正確な本文メッセージ構造が指定されます。これにより、パーサーは syslog メッセージ内で解析、マッピング、配信する必要がある各情報部分を識別できます。</p> <p>たとえば、テンプレートでは正確なユーザ名部分を指定できます。これにより、パーサーは受信するすべてのメッセージでユーザ名を検出できます。</p> <p>このフィールドでは、syslog メッセージを認識して正しく解析するために使用される (syslog メッセージの本文の) テンプレートを指定します。</p> <p>事前定義のドロップダウンリストから選択するか、または [新規 (New)] をクリックして独自のカスタム テンプレートを作成します。新しいテンプレートの作成の詳細については、#unique_593を参照してください。ほとんどの事前定義テンプレートでは正規表現が使用されています。カスタム テンプレートでも正規表現を使用する必要があります。</p> <p>(注) 編集または削除できるのはカスタム テンプレートだけであり、ドロップダウンの事前定義システム テンプレートは変更できません。</p> <p>現在 ISE に含まれている事前定義 DHCP プロバイダー テンプレートを次に示します。</p> <ul style="list-style-type: none"> • InfoBlox • BlueCat • Lucent_QIP • DHCPD • MSAD DHCP <p>(注) DHCP syslog メッセージにはユーザ名は含まれていません。したがって、これらのメッセージはパーサーから遅れて配信されます。これにより ISE-PICISE は、ユーザ ID 情報を正しく解析して配信するために、最初にローカル セッション ディレク</p>

フィールド	説明
	<p>トリに登録されているユーザ ([ライブセッション (Live Sessions)] で表示) を調べ、その後各ユーザの IP アドレスと受信した DHCP syslog メッセージに指定されている IP アドレスを照合してユーザ照合を試行します。</p> <p>DHCP syslog メッセージから受信したデータが、現在ログインしているユーザに一致しない場合、メッセージは解析されず、ユーザ ID は配信されません。</p> <p>ISE には次の事前定義の標準 syslog プロバイダー テンプレートがあります。</p> <ul style="list-style-type: none"> • ISE • ACS • F5_VPN • ASA_VPN • Blue Coat • Aerohive • Safe connect_NAC • Nortel_VPN <p>テンプレートについては、#unique_594を参照してください。</p>
デフォルト ドメイン (Default Domain)	<p>syslog メッセージで特定のユーザに対してドメインが指定されていない場合、このデフォルト ドメインが自動的にそのユーザに割り当てられます。これにより、すべてのユーザにドメインが割り当てられます。</p> <p>デフォルト ドメインまたはメッセージから解析されたドメインにユーザ名が付加され、username@domain となります。したがって、ユーザとユーザグループに関する詳細情報を取得するためには、ドメインを含めます。</p>

syslog メッセージ構造のカスタマイズ (テンプレート)

テンプレートは正確なメッセージ構造を指定します。これにより、パーサーはsyslogメッセージ内で解析、マッピング、配信する必要がある各情報部分を識別できます。たとえば、テンプレートでは正確なユーザ名部分を指定できます。これにより、パーサーは受信するすべてのメッセージでユーザ名を検出できます。テンプレートにより、新規マッピングメッセージとマッピング削除メッセージの両方に対応する構造が決定します。

Cisco ISE では、パッシブ ID パーサーが使用する 1 つのメッセージヘッダーと複数の本文構造をカスタマイズできます。

パッシブ ID パーサーが、メッセージがユーザ ID マッピングを追加するためのメッセージであるかまたは削除するためのメッセージであるかを正しく識別し、ユーザの詳細情報を正しく解析できるようにするため、テンプレートには、ユーザ名、IP アドレス、MAC アドレス、およびドメインの構造を定義する正規表現が含まれている必要があります。

メッセージテンプレートをカスタマイズするときに、事前定義オプションで使用されている正規表現とメッセージ構造を調べ、ISE-PICISE の事前定義メッセージテンプレートに基づいてカスタマイズを行うかどうかを決定できます。事前定義テンプレートの正規表現、メッセージ構造、例などの詳細については、[#unique_594](#) を参照してください。

次の内容をカスタマイズできます。

- 1 つのメッセージヘッダー : [syslog ヘッダーのカスタマイズ \(458 ページ\)](#)
- 複数のメッセージ本文 : [syslog メッセージ本文のカスタマイズ \(456 ページ\)](#)。



(注) DHCP syslog メッセージにはユーザ名は含まれていません。したがって、これらのメッセージはパーサーから遅れて配信されます。これにより ISE-PICISE は、ユーザ ID 情報を正しく解析して配信するために、最初にローカルセッションディレクトリに登録されているユーザ ([ライブセッション (Live Sessions)] で表示) を調べ、その後各ユーザの IP アドレスと受信した DHCP syslog メッセージに指定されている IP アドレスを照合してユーザ照合を試行します。DHCP syslog メッセージから受信したデータが、現在ログインしているユーザに一致しない場合、メッセージは解析されず、ユーザ ID は配信されません。

DHCP メッセージの詳細情報を適切に照合、解析、マッピングするために必要な遅延は、カスタマイズされたテンプレートには適用できません。したがって、DHCP メッセージテンプレートをカスタマイズすることは推奨されません。代わりに、事前定義の DHCP テンプレートを使用してください。

syslog メッセージ本文のカスタマイズ

Cisco ISE では、パッシブ ID パーサーにより解析される syslog メッセージテンプレートをカスタマイズできます (メッセージ本文のカスタマイズ)。テンプレートには、ユーザ名、IP アドレス、MAC アドレス、およびドメインの構造を定義する正規表現が含まれている必要があります。



(注) DHCP syslog メッセージにはユーザ名は含まれていません。したがって、これらのメッセージはパーサーから遅れて配信されます。これにより ISE-PICISE は、ユーザ ID 情報を正しく解析して配信するために、最初にローカルセッションディレクトリに登録されているユーザ ([ライブセッション (Live Sessions)] で表示) を調べ、その後各ユーザの IP アドレスと受信した DHCP syslog メッセージに指定されている IP アドレスを照合してユーザ照合を試行します。DHCP syslog メッセージから受信したデータが、現在ログインしているユーザに一致しない場合、メッセージは解析されず、ユーザ ID は配信されません。

DHCP メッセージの詳細情報を適切に照合、解析、マッピングするために必要な遅延は、カスタマイズされたテンプレートには適用できません。したがって、DHCP メッセージテンプレートをカスタマイズすることは推奨されません。代わりに、事前定義の DHCP テンプレートを使用してください。

syslog クライアント設定画面から、syslog メッセージ本文テンプレートを作成および編集します。



(注) 各自でカスタマイズしたテンプレートだけを編集できます。システムに用意されている事前定義テンプレートは変更できません。

- ステップ 1** 現在設定されているすべてのクライアントを表示し、既存のクライアントを編集、削除し、新しいクライアントを設定するには、[ワーク センター (Work Centers)] > [PassiveID] > [syslog プロバイダー (Syslog Providers)] を選択し、左側のパネルから [エージェント (Agents)] を選択します。
[syslog プロバイダー (syslog Providers)] テーブルが表示されます。このテーブルには既存の各クライアントのステータス情報が含まれています。
- ステップ 2** 新しい syslog クライアントを追加するには [追加 (Add)] をクリックし、すでに設定されているクライアントを更新するには [編集 (Edit)] をクリックします。テンプレートを追加または編集する場合、どのオプションを選択するかは関係ありません。syslog クライアントの設定と更新については、[#unique_596](#)を参照してください。
- ステップ 3** [syslog プロバイダー (Syslog Providers)] 画面の [テンプレート (Template)] フィールドの隣にある [新規 (New)] をクリックし、新しいメッセージテンプレートを作成します。既存のテンプレートを編集するには、ドロップダウンリストからテンプレートを選択して [編集 (Edit)] をクリックします。
[syslog テンプレート (Syslog Template)] 画面が表示されます。
- ステップ 4** 必須フィールドをすべて指定します。
値を正しく入力する方法の詳細については、[syslog カスタマイズ テンプレートの設定と例 \(459 ページ\)](#)を参照してください。
- ステップ 5** [テスト (Test)] をクリックして、入力した文字列に基づいてメッセージが正しく解析されていることを確認します。
- ステップ 6** [保存 (Save)] をクリックします。

カスタマイズしたテンプレートが保存され、新しい syslog クライアントの設定時と既存の syslog クライアントの更新時に [テンプレート (Template)] フィールドのドロップダウンリストにこのテンプレートが表示されます。

syslog ヘッダーのカスタマイズ

syslog ヘッダーには、メッセージの送信元のホスト名が他の詳細情報と共に含まれています。syslog メッセージが ISE メッセージパーサーで認識されない場合は、ホスト名の後に続く区切り文字を設定し、ISE がホスト名を認識してメッセージを正しく解析できるようにすることで、メッセージヘッダーをカスタマイズする必要がある場合があります。この画面のフィールドの詳細については、[syslog カスタマイズテンプレートの設定と例 \(459 ページ\)](#) を参照してください。カスタマイズされたヘッダーの設定は保存され、メッセージを受信するたびにパーサーが使用するヘッダー タイプにこの設定が追加されます。



(注) 1 つのヘッダーだけをカスタマイズできます。ヘッダーのカスタマイズ後に、[カスタムヘッダー (Custom Header)] をクリックして保存するテンプレートを作成し、[送信 (Submit)] をクリックすると、最新の設定が保存され、以前のカスタマイズ内容が上書きされます。

- ステップ 1** 現在設定されているすべてのクライアントを表示し、既存のクライアントを編集、削除し、新しいクライアントを設定するには、[ワークセンター (Work Centers)] > [PassiveID] > [syslog プロバイダー (Syslog Providers)] を選択し、左側のパネルから [エージェント (Agents)] を選択します。
[syslog プロバイダー (syslog Providers)] テーブルが表示されます。このテーブルには既存の各クライアントのステータス情報が含まれています。
- ステップ 2** [カスタムヘッダー (Custom Header)] をクリックして [syslog カスタムヘッダー (Syslog Custom Header)] 画面を開きます。
- ステップ 3** [サンプル syslog を貼り付ける (Paste sample syslog)] に、syslog メッセージのヘッダー形式の例を入力します。たとえば、メッセージの 1 つからヘッダー `<181>Oct 10 15:14:08 Cisco.com` をコピーして貼り付けます。
- ステップ 4** [区切り文字 (Separator)] フィールドで、単語をスペースとタブのいずれで区切るかを指定します。
- ステップ 5** [ヘッダーのホスト名の位置 (Position of hostname in header)] フィールドで、ヘッダーのどの位置がホスト名であるかを指定します。たとえば、前述のヘッダーではホスト名は 4 番目の単語です。これを指定するには 4 と入力します。

[ホスト名 (Hostname)] フィールドに、最初の 3 つのフィールドに示される詳細情報に基づいてホスト名が表示されます。たとえば、[syslog の例を貼り付ける (Paste sample syslog)] でのヘッダーの例の場合は次のようになります。

```
<181>Oct 10 15:14:08 Cisco.com
```

区切り文字として [スペース (Space)] を指定し、[ヘッダーのホスト名の位置 (Position of hostname in header)] には 4 を入力します。

[ホスト名 (Hostname)] には自動的に Cisco.com と表示されます。これは、[syslog の例を貼り付ける (Paste sample syslog)] フィールドに貼り付けたヘッダー フレーズの 4 番目の単語です。

ホスト名が正しく表示されない場合は、[区切り文字 (Separator)] フィールドと [ヘッダーのホスト名の位置 (Position of hostname in header)] フィールドに入力したデータを確認してください。

この例を次のスクリーン キャプチャに示します。

図 33: syslog ヘッダーのカスタマイズ

Syslog Custom Header

If some or all of the syslogs are not being accepted, it may be because they have an uncommon header format. Define a custom header here.

Paste sample syslog * <181>Oct 10 15:14:08 Hostname Message

Separator * Space

Position of hostname in header * 4

Hostname Hostname

Cancel Submit

ステップ 6 (注) 1 つのヘッダーだけをカスタマイズできます。ヘッダーのカスタマイズ後に、[カスタムヘッダー (Custom Header)] をクリックして保存するテンプレートを作成し、[送信 (Submit)] をクリックすると、最新の設定が保存され、以前のカスタマイズ内容が上書きされます。

[送信 (Submit)] をクリックします。

カスタマイズされたヘッダーの設定は保存され、メッセージを受信するたびにパーサーが使用するヘッダータイプにこの設定が追加されます。

syslog カスタマイズ テンプレートの設定と例

Cisco ISE では、パッシブ ID パーサーにより解析される syslog メッセージテンプレートをカスタマイズできます。カスタマイズされたテンプレートは、新規マッピングメッセージとマッピング削除メッセージの両方に対応する構造を決定します。パッシブ ID パーサーが、メッセージがユーザ ID マッピングを追加するためのメッセージであるかまたは削除するためのメッセージであるかを正しく識別し、ユーザの詳細情報を正しく解析できるようにするため、テンプレートには、ユーザ名、IP アドレス、MAC アドレス、およびドメインの構造を定義する正規表現が含まれている必要があります。



- (注) ほとんどの事前定義テンプレートでは正規表現が使用されます。カスタマイズテンプレートでも正規表現を使用してください。

syslog ヘッダーの各部分

ホスト名の後に続く区切り文字を設定することで、syslog プロンプトが認識する単一ヘッダーをカスタマイズできます。

[ワーク センター (Work Centers)] > [PassiveID] > [プロバイダー (Providers)] を選択し、左側のパネルから [syslog プロバイダー (Syslog Providers)] を選択し、テーブルで [カスタム ヘッダー (Custom Header)] をクリックして、カスタム syslog メッセージヘッダーを作成します。

次の表に、カスタム syslog ヘッダーに組み込むことができるさまざまな部分とフィールドについて説明します。正規表現の詳細については、[表 30: カスタマイズ テンプレートの正規表現 \(462 ページ\)](#) を参照してください。

表 28: syslog カスタム ヘッダー

フィールド	説明
[syslog の例を貼り付ける (Paste sample syslog)]	syslog メッセージにヘッダー形式の例を入力します。たとえば、次のヘッダーをコピーして貼り付けます。 <181>Oct 10 15:14:08 Hostname Message
区切り文字	単語をスペースまたはタブのいずれかで区切るかを指定します。
[ヘッダーのホスト名の位置 (Position of hostname in header)]	ヘッダーでのホスト名の位置を指定します。たとえば、前述のヘッダーではホスト名は 4 番目の単語です。これを指定するには 4 と入力します。

フィールド	説明
ホストネーム	<p>最初の 3 つのフィールドに示される詳細情報に基づいて、ホスト名を表示します。たとえば、[syslog の例を貼り付ける (Paste sample syslog)] でのヘッダーの例の場合は次のようになります。</p> <p><181>Oct 10 15:14:08 Hostname Message</p> <p>区切り文字として [スペース (Space)] を指定し、[ヘッダーのホスト名の位置 (Position of hostname in header)] には 4 を入力します。</p> <p>[ホスト名 (Hostname)] には Hostname が自動的に表示されます。</p> <p>ホスト名が正しく表示されない場合は、[区切り文字 (Separator)] フィールドと [ヘッダーのホスト名の位置 (Position of hostname in header)] フィールドに入力したデータを確認してください。</p>

メッセージ本文の syslog テンプレートの各部分と説明

次の表に、カスタマイズ syslog メッセージテンプレートに組み込むことができるさまざまな部分とフィールドについて説明します。正規表現の詳細については、[表 30: カスタマイズ テンプレートの正規表現 \(462 ページ\)](#) を参照してください。

表 29: syslog テンプレート

パート	フィールド	説明
	[名前 (Name)]	このテンプレートの目的がわかる一意の名前。
[マッピング操作 (Mapping Operations)]	[新規マッピング (New mapping)]	新しいユーザを追加するためにこのテンプレートで使用されるマッピングの正規表現。たとえば、F5 VPN にログインした新しいユーザを示すには、フィールドに「logged on from」と入力します。
	[削除されたマッピング (Removed Mapping)]	ユーザを削除するためにこのテンプレートで使用されるマッピングのタイプの正規表現。たとえば、削除する必要がある ASA VPN のユーザを示すには、フィールドに「session disconnect」と入力します。

パート	フィールド	説明
ユーザデータ (User Data)	[IPアドレス (IP Address)]	キャプチャする IP アドレスを示す正規表現。 たとえば Bluecat メッセージの場合、この IP アドレス範囲内のユーザの ID をキャプチャするには、次のように入力します。 (on\s to\s)((?:25[0-5] 2[0-4][0-9] [01]?[0-9][0-9]?)\.){3}(?:25[0-5] 2[0-4][0-9] [01]?[0-9][0-9]?)
	ユーザ名	キャプチャするユーザ名形式を示す正規表現。
	ドメイン	キャプチャするドメインを示す正規表現。
	MAC アドレス (Mac Address)	キャプチャする MAC アドレスの形式を示す正規表現。

正規表現の例

メッセージを解析するため、正規表現を使用します。ここでは、IP アドレス、ユーザ名、およびマッピング追加メッセージを解析する正規表現の例を示します。

たとえば、正規表現を使用して次のメッセージを解析します。

```
<174>192.168.0.1 %ASA-4-722051: Group <DfltGrpPolicy> User <user1> IP <192.168.0.10> IPv4 Address <192.168.0.6> IPv6 address <::> assigned to session
```

```
<174>192.168.0.1 %ASA-6-713228: Group = xyz, Username = user1, IP = 192.168.0.12, Assigned private IP address 192.168.0.8 to remote user
```

次の表に、正規表現の定義を示します。

表 30: カスタマイズ テンプレートの正規表現

パート	正規表現
IP アドレス (IP address)	Address <([^\s]+)> address ([^\s]+)
ユーザ名 (User name)	User <([^\s]+)> Username = ([^\s]+)
マッピング追加メッセージ (Add mapping message)	(%ASA-4-722051 %ASA-6-713228)

syslog 事前定義メッセージ テンプレートの使用

syslog メッセージには、ヘッダーとメッセージ本文を含む標準構造があります。

ここでは、メッセージの送信元に基づいてサポートされているヘッダーの内容の詳細や、サポートされている本文の構造など、Cisco ISE が提供する事前定義テンプレートについて説明します。

また、システムで事前に定義されていないソース用に、カスタマイズした本文コンテンツを使用した独自のテンプレートを作成することもできます。ここでは、カスタムテンプレートでサポートされる構造について説明します。メッセージの解析時には、システムで事前定義されているヘッダーに加え、1つのカスタマイズヘッダーを設定できます。また、メッセージ本文には、服すのカスタマイズテンプレートを設定できます。ヘッダーのカスタマイズの詳細については、[#unique_587](#)を参照してください。本文のカスタマイズの詳細については、[syslog メッセージ本文のカスタマイズ \(456 ページ\)](#)を参照してください。



(注) ほとんどの事前定義テンプレートでは正規表現が使用されています。カスタムテンプレートでも正規表現を使用する必要があります。

メッセージヘッダー

パーサーで認識されるヘッダータイプには、すべてのクライアントマシンのすべてのメッセージタイプ（新規および削除）について認識される2つのタイプがあります。これらのヘッダーは次のとおりです。

- <171>Host message
- <171>Oct 10 15:14:08 Host message

受信されたヘッダーはホスト名を検出するため解析されます。ホスト名は、IPアドレス、ホスト名、または完全 FQDN のいずれかです。

ヘッダーもカスタマイズできます。ヘッダーをカスタマイズするには、[#unique_587](#)を参照してください。

syslog ASA VPN 事前定義テンプレート

ASA VPN でサポートされる syslog メッセージの形式とタイプについて説明します。

ヘッダー

パーサーでサポートされるヘッダーはすべてのクライアントで同一です（[syslog 事前定義メッセージテンプレートの使用 \(462 ページ\)](#)を参照）。

新規マッピング本文メッセージ

次の表では、パーサーが認識するさまざまな ASA VPN 本文メッセージについて説明します。

本文メッセージ	解析例
%ASA-6-109005 Authentication succeeded for user UserA from 10.0.0.11/100 to 10.10.11.11/20 on interface eth1/1	[UserA,10.0.0.11]
%ASA-6-602303 IPSEC: An direction tunnel_type SA (SPI=spi) between local_IP and 10.0.0.11 (UserA) has been created.	
%ASA-6-721016 (device) WebVPN session for client user UserA, IP 10.0.0.11 has been created.	
%ASA-6-603104 PPTP Tunnel created, tunnel_id is number, remote_peer_ip is remote_address, ppp_virtual_interface_id is number, \ client_dynamic_ip is 10.0.0.11, ffg123 #% UserA is UserA, MPPE_key_strength is string	
%ASA-6-603106 L2TP Tunnel created, tunnel_id is number, remote_peer_ip is remote_address, ppp_virtual_interface_id is number, \ client_dynamic_ip is 10.0.0.11, UserA is user	
%ASA-6-113039 Group group User UserA IP 10.0.0.11 AnyConnect parent session started.	
%ASA-6-802001 User UserA IP 10.100.1.1 OS os_name UDID number MDM action session started.	[UserA,172.16.0.11] (注) このメッセージタイプから解析される IP アドレスは、メッセージに示されているようにプライベート IP アドレスです。
%ASA-6-713228: Group = xyz, UserA = xxxx227, IP = 192.168.0.11, Assigned private IP address 172.16.0.11 to remote user	
%ASA-4-722051: Group <DfltGrpPolicy> User <UserA> IP <172.16.0.12> IPv4 Address <172.16.0.21> IPv6 address <::> assigned to session	[UserA,172.16.0.12] (注) このメッセージタイプから解析された IP アドレスは IPv4 アドレスです。

マッピング削除本文メッセージ

ここではパーサーで ASA VPN のためにサポートされている マッピング削除メッセージについて説明します。

受信された本文が解析され、次のようにユーザの詳細が判明します。

[UserA,10.1.1.1]

本文メッセージ
%ASA-4-113019 Group = group, UserA = UserA, IP = 10.1.1.1, Session disconnected.Session Type: type, Duration:\ duration, Bytes xmt: count,Bytes rcv: count, Reason: reason
%ASA-4-717052 Group group name User UserA IP 10.1.1.1 Session disconnected due to periodic certificate authentication failure.Subject Name id subject name Issuer Name id issuer name\ Serial Number id serial number
%ASA-6-602304 IPSEC: An direction tunnel_type SA (SPI=spi) between local_IP and 10.1.1.1 (UserA) has been deleted.
%ASA-6-721018 WebVPN session for client user UserA, IP 10.1.1.1 has been deleted.
%ASA-4-722049 Group group User UserA IP 10.1.1.1 Session terminated: SVC not enabled or invalid image on the ASA
%ASA-4-722050 Group group User UserA IP 10.1.1.1 Session terminated: SVC not enabled for the user.
%ASA-6-802002 User UserA IP 10.1.1.1 OS os_name UDID number MDM action session terminated.
%ASA-3-716057 Group group User UserA IP 10.1.1.1 Session terminated, no type license available.
%ASA-3-722046 Group group User UserA IP 10.1.1.1 Session terminated: unable to establish tunnel.
%ASA-4-113035 Group group User UserA IP 10.1.1.1 Session terminated: AnyConnect not enabled or invalid AnyConnect image on the ASA.
%ASA-4-716052 Group group-name User UserA IP 10.1.1.1 Pending session terminated.
%ASA-6-721018 WebVPN session for client user UserA, IP 10.1.1.1 has been deleted.

syslog Bluecat 事前定義テンプレート

Bluecat でサポートされる syslog メッセージの形式とタイプについて説明します。

ヘッダー

パーサーでサポートされるヘッダーはすべてのクライアントで同一です（[syslog 事前定義メッセージテンプレートの使用](#)（462 ページ）を参照）。

新規マッピング本文メッセージ

ここでは、Bluecat syslog で新規マッピングとしてサポートされるメッセージについて説明します。

受信された本文が解析され、次のようにユーザの詳細が判明します。

[macAddress=nn:xx:nn:ca:xx:nn,ip=172.16.0.12]

本文
Nov 7 23:37:32 xx-campus1 dhcpd: DHCPACK on 172.16.0.13 to nn:xx:nn:ca:xx:nn via 172.16.0.17

マッピング削除メッセージ

Bluecat のマッピング削除メッセージはありません。

syslog F5 VPN 事前定義テンプレート

F5 VPN でサポートされる syslog メッセージの形式とタイプについて説明します。

ヘッダー

パーサーでサポートされるヘッダーはすべてのクライアントで同一です（[syslog 事前定義メッセージ テンプレートの使用 \(462 ページ\)](#) を参照）。

新規マッピング本文メッセージ

次の表では、パーサーが認識するさまざまな F5 VPN 本文メッセージについて説明します。

受信された本文が解析され、次のようにユーザの詳細が判明します。

[user=UserA,ip=172.16.0.12]

本文
Apr 10 09:33:58 Oct 2 08:28:32 abc.xyz.org security[nnnnn]: [UserA@vendor-abcr] User UserA logged on from 172.16.0.21 to \ 172.16.0.12 Sid = xyz\

マッピング削除メッセージ

現在、F5 VPN でサポートされている削除メッセージはありません。

syslog Infoblox 事前定義テンプレート

Infoblox でサポートされる syslog メッセージの形式とタイプについて説明します。

ヘッダー

パーサーでサポートされるヘッダーはすべてのクライアントで同一です（[syslog 事前定義メッセージ テンプレートの使用 \(462 ページ\)](#) を参照）。

新規マッピング本文メッセージ

次の表では、パーサーが認識するさまざまな ASA VPN 本文メッセージについて説明します。

受信された本文が解析され、次のようにユーザの詳細が判明します。

[macAddress= nn:xx:xx:xx:nn:nn,ip=10.0.10.100]

本文メッセージ
Nov 15 11:37:26 user1-lnx dhcpd[3179]: DHCPACK on 10.0.0.14 to nn:xx:xx:xx:nn:nn (android-df67ddcbb1271593) via eth2 relay 10.0.0.24 lease-duration 3600
Nov 15 11:38:11 user1-lnx dhcpd[3179]: DHCPACK on 172.16.0.18 to nn:xx:xx:xx:nn:nn (DESKTOP-HUDGAAQ) via eth2 relay 172.16.0.13 lease-duration 691200 (RENEW)

本文メッセージ

Nov 15 11:38:11 192.168.0.12 dhcpd[25595]: DHCPACK to 10.0.0.11 (nn:xx:xx:xn:nn:nx) via eth1

マッピング削除メッセージ

マッピング削除では次のメッセージがサポートされています。

パーサーはさまざまな本文メッセージをマッピング削除メッセージとして認識します。これについて次の表で説明します。

受信された本文が解析され、次のようにユーザの詳細が判明します。

- MAC アドレスが含まれている場合 :
[00:0c:29:a2:18:34,10.0.10.100]
- MAC アドレスが含まれていない場合 :
[10.0.10.100]

本文メッセージ

07-11-2016 23:37:32 Daemon.Info 10.0.10.2 Jul 12 10:42:26 10.0.10.2 dhcpd[26083]: DHCP_EXPIRE 10.0.10.100 has expired

07-11-2016 23:37:32 Daemon.Info 10.0.10.2 Jul 12 10:42:26 10.0.10.2 dhcpd[26083]: DHCP_RELEASE of 10.0.10.100 from 00:0c:29:a2:18:34 \ (win10) via eth1 uid 01:00:0c:29:a2:18:34

07-11-2016 23:37:32 Daemon.Info 10.0.10.2 Jul 12 10:42:26 10.0.10.2 dhcpd[25595]: RELEASE on 10.20.31.172 to c0:ce:cd:44:4f:bd

syslog Linux DHCPd3 事前定義テンプレート

Linux DHCPd3 でサポートされる syslog メッセージの形式とタイプについて説明します。

ヘッダー

パーサーでサポートされるヘッダーはすべてのクライアントで同一です ([syslog 事前定義メッセージ テンプレートの使用 \(462 ページ\)](#) を参照)。

新規マッピング メッセージ

次の表では、パーサーが認識するさまざまな Linux DHCPd3 本文メッセージについて説明します。

受信された本文が解析され、次のようにユーザの詳細が判明します。

[macAddress=24:ab:81:ca:f2:72,ip=172.16.0.21]

本文メッセージ

Nov 11 23:37:32 dhcprsv dhcpd: DHCPACK on 10.0.10.100 to 00:0c:29:a2:18:34 (win10) via eth1

Nov 11 23:37:32 dhcprsv dhcpd: DHCPACK on 10.0.10.100 (00:0c:29:a2:18:34) via eth1

マッピング削除本文メッセージ

ここではパーサーで Linux DHCPd3 のためにサポートされているマッピング削除メッセージについて説明します。

受信された本文が解析され、次のようにユーザの詳細が判明します。

[00:0c:29:a2:18:34,10.0.10.100]

本文メッセージ
Nov 11 23:37:32 dhcprsv dhcpd: DHCP_EXPIRE 10.0.10.100 has expired
Nov 11 23:37:32 dhcprsv dhcpd: DHCP_RELEASE of 10.0.10.100 from 00:0c:29:a2:18:34 (win10) via eth1

syslog MS DHCP 事前定義テンプレート

MS DHCP でサポートされる syslog メッセージの形式とタイプについて説明します。

ヘッダー

パーサーでサポートされるヘッダーはすべてのクライアントで同一です ([syslog 事前定義メッセージテンプレートの使用 \(462 ページ\)](#) を参照)。

新規マッピング本文メッセージ

次の表では、パーサーが認識するさまざまな MS DHCP 本文メッセージについて説明します。

受信すると、パーサーはカンマ (,) を検索してデータを分割し、これらの形式のメッセージが次の例に示すように解析されます。

[macAddress=000C29912E5D,ip=10.0.10.123]

本文メッセージ
Nov 11 23:37:32 10/07/21/16,16:55:22,Assign,10.0.10.123,win10.IDCSPAN.Local,000C29912E5D,,724476048,0,,,0x4D53465420352E30,MSFT,5.0

マッピング削除本文メッセージ

ここではパーサーで MS DHCP のためにサポートされているマッピング削除メッセージについて説明します。

受信すると、パーサーはカンマ (,) を検索してデータを分割し、これらの形式のメッセージが次の例に示すように解析されます。

[macAddress=000C29912E5D,ip=10.0.10.123]

本文メッセージ
Nov 11 23:37:32 12,07/21/16,16:55:18,Release,10.0.10.123,win10.IDCSPAN.Local,000C29912E5D,,3128563632,\0,,,,,,,,,0

syslog SafeConnect NAC 事前定義テンプレート

SafeConnect NAC でサポートされる syslog メッセージの形式とタイプについて説明します。

ヘッダー

パーサーでサポートされるヘッダーはすべてのクライアントで同一です ([syslog 事前定義メッセージ テンプレートの使用 \(462 ページ\)](#) を参照)。

新規マッピング本文メッセージ

次の表では、パーサーが認識するさまざまな SafeConnect NAC 本文メッセージについて説明します。

受信された本文が解析され、次のようにユーザの詳細が判明します。

[user=galindk1i,p=xxxx.xx.xxx.xxd,domain=Resnet-Macs]

本文メッセージ
Apr 10 09:33:58 nac Safe*Connect: authenticationResult xxx.xx.xxx.xxx xxx.xx.xxx.xxx UserA true Resnet-Macs TCNJ-Chain 001b63b79018 MAC

マッピング削除メッセージ

現在、Safe Connect でサポートされている削除メッセージはありません。

syslog Aerohive 事前定義テンプレート

Aerohive でサポートされる syslog メッセージの形式とタイプについて説明します。

ヘッダー

パーサーでサポートされるヘッダーはすべてのクライアントで同一です ([syslog 事前定義メッセージ テンプレートの使用 \(462 ページ\)](#) を参照)。

新規マッピング本文メッセージ

次の表では、パーサーが認識するさまざまな Aerohive 本文メッセージについて説明します。

本文で解析される詳細には、ユーザ名と IP アドレスがあります。解析に使用される正規表現の例を次に示します。

- New mapping-auth\:
- IP-ip ([A-F0-9a-f:.]+)
- User name-UserA ([a-zA-Z0-9_]+)

受信された本文が解析され、次のようにユーザの詳細が判明します。

[UserA,10.5.50.52]

本文メッセージ

```
2013-04-01 14:06:05 info ah auth: Station 1cab:a7e6:cf7f ip 10.5.50.52 UserA UserA
```

マッピング削除メッセージ

現在、Aerohive からのマッピング削除メッセージはサポートされていません。

syslog Blue Coat 事前定義テンプレート : Main Proxy、Proxy SG、Squid Web Proxy

Blue Coat の次のメッセージ タイプがサポートされています。

- BlueCoat Main Proxy
- BlueCoat Proxy SG
- BlueCoat Squid Web Proxy

BlueCoat メッセージでサポートされる syslog メッセージの形式とタイプについて説明します。

ヘッダー

パーサーでサポートされるヘッダーはすべてのクライアントで同一です ([syslog 事前定義メッセージテンプレートの使用 \(462 ページ\)](#) を参照)。

新規マッピング本文メッセージ

次の表では、パーサーが認識するさまざまな Blue Coat 本文メッセージについて説明します。

受信された本文が解析され、次のようにユーザの詳細が判明します。

[UserA,192.168.10.24]

本文メッセージ (この例は、**BlueCoat プロキシ SG** メッセージからの引用です)

```
2016-09-21 23:05:33 58 10.0.0.1 UserA -- PROXIED "none" http://www.example.com/ 200 TCP_MISS
GET application/json;charset=UTF-8 http site.api.example.com 80 /apis/v2/scoreboard/header
?rand=1474499133503 - "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/46.0.2486.0 Safari/537.36 Edge/13.10586" 192.168.10.24 7186 708 - "unavailable"
```

次の表では、新規マッピングメッセージに使用されるクライアント別の正規表現構造について説明します。

クライアント	正規表現
BlueCoat Main Proxy	<p>新規マッピング</p> <p>(TCP_HIT TCP_MEM){1}</p> <p>IP</p> <p>\((?:09(13) 309(13))(?:azA-Z09(14)(12)(17)azA-Z09(14))s</p> <p>ユーザ名 (User name)</p> <p>\s\-\s([a-zA-Z0-9_]+\)\s\-\s</p>

クライアント	正規表現
BlueCoat Proxy SG	新規マッピング <code>(\sPROXIED){1}</code> IP <code>([0-9]{1,3}\.){3}[0-9]{1,3}</code> ユーザ名 (User name) <code>([a-zA-Z0-9_]{1,32})</code>
BlueCoat Squid Web Proxy	新規マッピング <code>(TCP_HIT TCP_MEM){1}</code> IP <code>([0-9]{1,3}\.){3}[0-9]{1,3}</code> ユーザ名 (User name) <code>([a-zA-Z0-9_]{1,32})</code>

マッピング削除メッセージ

Blue Coat クライアントではマッピング削除メッセージがサポートされていますが、現在利用できる例はありません。

次の表では、マッピング削除メッセージに使用されるクライアント別の既知の正規表現構造について説明します。

クライアント	正規表現
BlueCoat Main Proxy	<code>(TCP_MISS TCP_NC_MISS){1}</code>
BlueCoat Proxy SG	現在利用できる例はありません。
BlueCoat Squid Web Proxy	<code>(TCP_MISS TCP_NC_MISS){1}</code>

syslog ISE および ACS 事前定義テンプレート

パーサーは ISE または ACS クライアントをリッスンするときに、次のメッセージタイプを受信します。

- 認証成功：ユーザが ISE または ACS により認証されると、認証が成功したことを通知し、ユーザの詳細情報を記述した認証成功メッセージが発行されます。このメッセージが解析され、このメッセージのユーザの詳細とセッション ID が保存されます。
- アカウント開始およびアカウント更新メッセージ（新規マッピング）：ISE または ACS から受信したアカウント開始メッセージまたはアカウント更新メッセージは、認証成功メッセージから保存されたユーザの詳細とセッション ID を使用して解析され、ユーザがマッピングされます。

- アカウンティング終了（マッピング削除）：ISE または ACS から受信されると、システムからユーザ マッピングが削除されます。

ISE および ACS でサポートされる syslog メッセージの形式とタイプについて説明します。

認証成功メッセージ

認証成功メッセージとして次のメッセージがサポートされています。

• ヘッダー

```
<181>Sep 13 10:51:41 Server logTag messageId totalFragments currentFragments message
```

例：<181>Sep 13 10:51:41 Positron CISE_PassiveID 0000005255 1 0 message

• 本文

```
Passed-Authentication 000011 1 0 2016-05-09 12:48:11.011 +03:00 0000012435 5200 NOTICE
Passed-Authentication: Authentication succeeded, ConfigVersionId=104, Device IP Address=10.0.0.12,
DestinationIPAddress=10.0.0.18, DestinationPort=1812, UserA=UserA, Protocol=Radius,
RequestLatency=45, NetworkDeviceName=DefaultNetworkDevice, User-Name=UserA,
NAS-IP-Address=1.1.1.1, Session-Timeout=90, Calling-Station-ID=, cisco-av-pair=audit-session-id=5
```

• 解析例

ユーザ名とセッション ID だけが解析されます。

[UserA,5]

アカウンティング開始/更新（新規マッピング）メッセージ

新規マッピング メッセージとして次のメッセージがサポートされています。

• ヘッダー

```
<181>Sep 13 10:51:41 Server logTag messageId totalFragments currentFragments message
```

例：<181>Sep 13 10:51:41 Positron CISE_PassiveID 0000005255 1 0 message

• 本文

```
CISE_RADIUS_Accounting 000011 1 0 2016-05-09 12:53:52.823 +03:00 0000012451 3000 NOTICE
Radius-Accounting: RADIUS Accounting start request, ConfigVersionId=104, Device IP
Address=10.0.0.12, RequestLatency=12, NetworkDeviceName=DefaultNetworkDevice,
User-Name=UserA, NAS-IP-Address=10.0.0.1, Framed-IP-Address=10.0.0.16, Session-Timeout=90,
Calling-Station-ID=, Acct-Status-Type=Start, Acct-Session-Id=6, cisco-av-pair=audit-session-id=5
```

• 解析例

解析される詳細には、ユーザ名、フレーム IP アドレス、および MAC アドレス（メッセージに含まれている場合）などがあります。

[UserA,10.0.0.16]

マッピング削除メッセージ

マッピング削除では次のメッセージがサポートされています。

• ヘッダー

```
<181>Sep 13 10:51:41 Server logTag messageId totalFragments currentFragments message
```

例 : <181>Sep 13 10:51:41 Positron CISE_PassiveID 0000005255 1 0 message

• 本文

```
2016-05-09 12:56:27.274 +03:00 0000012482 3001 NOTICE Radius-Accounting: RADIUS
Accounting stop request, ConfigVersionId=104, Device IP Address=10.0.0.17, RequestLatency=13,
NetworkDeviceName=DefaultNetworkDevice, User-Name=UserA, NAS-IP-Address=10.0.0.1,
Framed-IP-Address=10.0.0.16, Session-Timeout=90, Calling-Station-ID=, Acct-Status-Type=Stop,
Acct-Session-Id=104, cisco-av-pair=audit-session-id=5
```

• 解析例

解析される詳細には、ユーザ名、フレーム IP アドレス、および MAC アドレス（メッセージに含まれている場合）などがあります。

[UserA,10.0.0.16]

syslog Lucent QIP 事前定義テンプレート

Lucent QIP でサポートされる syslog メッセージの形式とタイプについて説明します。

ヘッダー

パーサーでサポートされるヘッダーはすべてのクライアントで同一です（[syslog 事前定義メッセージテンプレートの使用](#)（462 ページ）を参照）。

新規マッピング本文メッセージ

次の表では、パーサーが認識するさまざまな Lucent QIP 本文メッセージについて説明します。これらのメッセージの正規表現構造を次に示します。

DHCP_GrantLease|DHCP_RenewLease

受信された本文が解析され、次のようにユーザの詳細が判明します。

[00:0C:29:91:2E:5D,10.0.0.11]

本文メッセージ
DHCP:subtype=0:Single:\$IGNORE_N\$ DHCP_GrantLease: Host=\$HOSTNAME\$ P=10.0.0.11 MAC=00:0C:29:91:2E:5D
DHCP:subtype=0:Single:\$IGNORE_N\$ DHCP_RenewLease: Host=\$HOSTNAME\$ P=10.0.0.11 MAC=00:0C:29:91:2E:5D

マッピング削除本文メッセージ

次の表では、パーサーが認識するさまざまな Lucent QIP 本文メッセージについて説明します。これらのメッセージの正規表現構造を次に示します。

Delete Lease:|DHCP Auto Release:

受信された本文が解析され、次のようにユーザの詳細が判明します。

[10.0.0.11]

本文メッセージ
DHCP:subtype=0:Single:\$IGNORE_N\$ Delete Lease: IP=10.0.0.11 \$IGNORE_N\$
DHCP:subtype=0:Single:\$IGNORE_N\$ DHCP Auto Release: IP=10.0.0.11 \$IGNORE_N\$

パッシブ ID サービスのフィルタリング

特定のユーザを名前や IP アドレスに基づいてフィルタリングできます。たとえば IT サービスの管理者が、そのエンドポイントの標準ユーザを支援するためにエンドポイントにログインする場合、管理者アクティビティをフィルタリングにより除外して [ライブセッション (Live Sessions)] に表示されないようにし、そのエンドポイントの標準ユーザだけが表示されるようにできます。[ライブセッション (Live Session)] には、マッピングフィルタでフィルタリングされていないパッシブ ID サービス コンポーネントが表示されます。フィルタは必要なだけ追加できます。「OR」論理演算子をフィルタの間に適用します。両方のフィールドを 1 つのフィルタで指定する場合は、「AND」論理演算子をこれらのフィールドの間に適用します。

-
- ステップ 1** [ワーク センター (Work Centers)] > [PassiveID] > [プロバイダー (Providers)] を選択し、左側のパネルから [マッピング フィルタ (Mapping Filters)] を選択します。
- ステップ 2** [プロバイダー (Providers)] > [マッピング フィルタ (Mapping Filters)] を選択します。
- ステップ 3** [追加 (Add)] をクリックし、フィルタするユーザのユーザ名や IP アドレスを入力して、[送信 (Submit)] をクリックします。
- ステップ 4** 現在モニタリングセッションディレクトリにログインしてしているフィルタリングされていないユーザを表示するには、[操作 (Operations)] > [RADIUS ライブログ (RADIUS Livelog)] を選択します。
-

エンドポイント プローブ

設定可能なカスタム プロバイダーの他に、パッシブ ID サービス がアクティブになると ISE でエンドポイント プローブが有効になります。エンドポイント プローブは、特定の各ユーザがまだシステムにログインしているかどうかを定期的にチェックします。



- (注) エンドポイントがバックグラウンドで実行されることを確認するには、まず最初の **Active Directory** 参加ポイントを設定し、[クレデンシャルの保存 (Store Credentials)] を選択していることを確認します。エンドポイントプローブの設定の詳細については、[#unique_609](#)を参照してください。

エンドポイントのステータスを手動で確認するには、[アクション (Actions)] 列から [ライブセッション (Live Sessions)] に移動し、[アクションを表示 (Show Actions)] をクリックし、次の図に示すように [現在のユーザを確認 (Check current user)] を選択します。

図 34: 現在のユーザの確認

Session Status	Action	Endpoint ID	Identity
▼			Identity
terminated	Show Actions		Administrator
terminated	Show Actions		istern
terminated	Show Actions	10.56.53.179	Administrator
terminated	Show Actions	10.56.63.172	Administrator
terminated	Show Actions	10.56.53.204	Administrator
terminated	Show Actions	10.56.53.197	Administrator
terminated	Show Actions	10.56.14.19	

Click for Authentication Summary Report

T+0200 (Jerusalem Standard Time)

エンドポイントユーザのステータスと手動でのチェックの実行の詳細については、[RADIUS ライブセッション \(1454 ページ\)](#) を参照してください。

エンドポイントプローブはユーザが接続していることを認識します。特定のエンドポイントのセッションが最後に更新された時点から4時間経過している場合には、ユーザがまだログインしているかどうかを確認し、次のデータを収集します。

- MAC アドレス
- オペレーティング システムのバージョン

このチェックに基づいてプローブは次の操作を実行します。

- ユーザがまだログインしている場合、プローブはISEを[アクティブユーザ (Active User)] ステータスで更新します。
- ユーザがログアウトしている場合、セッション状態は[終了 (Terminated)] に更新され、15 分経過後にユーザはセッションディレクトリから削除されます。

- ユーザと通信できない場合、たとえばファイアウォールによって通信が防止されているか、エンドポイントがシャットダウンしている場合などには、ステータスが [到達不可能 (Unreachable)] として更新され、サブスクリバポリシーによってユーザセッションの処理方法が決定します。エンドポイントは引き続きセッションディレクトリに残ります。

エンドポイント プローブの使用

始める前に

サブネット範囲に基づいてエンドポイント プローブを作成および有効にできます。PSN ごとに1つのエンドポイントプローブを作成できます。エンドポイントプローブを使用するには、次のように設定していることを確認してください。

- エンドポイントはポート 445 とのネットワーク接続が必要です。
- ISE から 1 番目の Active Directory 参加ポイントを設定し、プロンプトが表示されたら [クレデンシャルの選択 (Select Credentials)] を選択してください。参加ポイントの詳細については、[プローブおよびプロバイダーとしての Active Directory \(426 ページ\)](#) を参照してください。



(注) エンドポイントがバックグラウンドで実行するようにするため、最初に 1 番目の Active Directory 参加ポイントを設定する必要があります。これにより、Active Directory プローブが完全に設定されていない場合でもエンドポイントプローブを実行できるようになります。

ステップ 1 [ワーク センター (Work Centers)] > [パッシブ ID (Passive ID)] > [プロバイダー (Providers)] を選択し、[エンドポイント プローブ (Endpoint Probes)] を選択します。

ステップ 2 新しいエンドポイント プローブを作成するには、[追加 (Add)] をクリックします。

ステップ 3 必須フィールドに入力し、[ステータス (Status)] フィールドで [有効化 (Enable)] を選択していることを確認してから、[送信 (Submit)] をクリックします。詳細については、[エンドポイントプローブ設定 \(476 ページ\)](#) を参照してください。

エンドポイント プローブ設定

サブネット範囲に基づいて PSN ごとに 1 つのエンドポイント プローブを作成します。展開で複数の PSN を使用している場合、個別のサブネットセットに各 PSN を割り当てるができます。この場合、各プローブを異なるユーザ グループに使用します。

[ワーク センター (Work Centers)] > [パッシブ ID (Passive ID)] > [プロバイダー (Providers)] を選択し、次に [エンドポイント プローブ (Endpoint Probes)] を選択して、PSN に新しいエンドポイント プローブを設定します。

表 31: エンドポイント プローブ設定

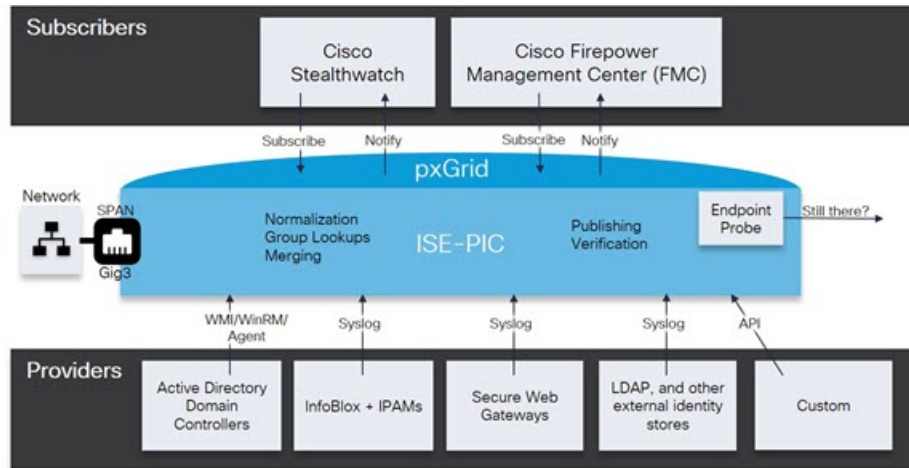
フィールド	説明
[名前 (Name)]	このプローブの用途を示す一意の名前を入力します。
説明	このプローブの用途を示す一意の説明を入力します。
[ステータス (Status)]	このプローブをアクティブにするには[有効化 (Enable)]を選択します。
ホスト名 (Host Name)	展開で使用可能な PSN のリストから、このプローブの PSN を選択します。
サブネット (Subnets)	<p>このプローブがチェックする必要があるエンドポイントのグループのサブネット範囲を入力します。標準のサブネット マスク範囲と、カンマで区切ったサブネット アドレスを使用します。</p> <p>例 :</p> <p>10.56.14.111/32,1.1.1.1/24,2.55.2.0/16,2.2.3.0/16,1.2.3.4/32</p> <p>各範囲は一意である必要があり、相互に重複してはなりません。たとえば、範囲 2.2.2.0/16,2.2.3.0/16 は相互に重複しているため、同一プローブに対して入力できません。</p>

サブスクライバ

パッシブ ID サービス は、さまざまなプロバイダーから収集し、Cisco ISE セッション ディレクトリにより保存された認証済みユーザ ID を、Cisco Stealthwatch や Cisco Firepower Management Center (FMC) などのその他のネットワーク システムに送信するため、Cisco pxGrid サービスを使用します。

次の図に示すように、pixGrid は ISE ノードにインストールされており、ユーザ ID を収集します。これらのユーザ ID は外部プロバイダーから取得され、解析され、マッピングされます。次に pxGrid はフォーマットされたユーザ ID をパッシブ ID サービス サブスクライバに送信します。

図 35: パッシブ ID サービス フロー



Cisco ISE に接続するサブスクリバは、pxGrid サービスの使用を登録する必要があります。サブスクリバは、クライアントになるために pxGrid SDK を介してシスコから使用可能な pxGrid クライアント ライブラリを採用する必要があります。サブスクリバは、一意の名前と証明書ベースの相互認証を使用して pxGrid にログインできます。Cisco pxGrid サブスクリバは、有効な証明書を送信すると、ISE により自動的に承認されます。

サブスクリバは設定されている pxGrid サーバのホスト名または IP アドレスのいずれかに接続できます。不必要なエラーが発生することを防ぎ、DNS クエリが適切に機能するようにするため、ホスト名を使用することが推奨されます。公開および登録するためにサブスクリバの pxGrid で作成される、情報トピックまたはチャネル機能があります。Cisco ISE では SessionDirectory と IdentityGroup だけがサポートされています。機能情報は、公開、ダイレクト クエリ、または一括ダウンロード クエリによりパブリッシャから取得でき、[機能 (Capabilities)] タブの [サブスクリバ (Subscribers)] で確認できます。

サブスクリバが ISE から情報を受信できるようにするには、次の操作を行います。

1. 必要に応じて、サブスクリバ側から証明書を生成します。
2. [サブスクリバの pxGrid 証明書の生成 \(479 ページ\)](#) PassiveID ワーク センターから。
3. [サブスクリバの有効化 \(480 ページ\)](#)。サブスクリバが ISE からユーザ ID を受信できるようにするため、このステップを実行するか、または承認を自動的に有効にする必要があります。[サブスクリバの設定 \(481 ページ\)](#) を参照してください。

サブスクリバの詳細については、次を参照してください。

サブスクライバの pxGrid 証明書の生成

始める前に

pxGrid とサブスクライバの間の相互信頼を保証するため、pxGrid サブスクライバの証明書を生成できます。これにより、ISE からサブスクライバにユーザ ID を渡すことが可能になります。次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 [ワーク センター (Work Centers)] > [PassiveID] > [サブスクライバ (Subscribers)] を選択し、[証明書 (Certificates)] タブに移動します。

ステップ 2 [処理の選択 (I want to)] ドロップダウン リストから、以下のいずれかのオプションを選択します。

- 単一の証明書の生成（証明書署名要求なし）（Generate a single certificate without a certificate signing request）：このオプションを選択すると、コモン ネーム (CN) を入力する必要があります。[コモン ネーム (Common Name)] フィールドに、pxGrid をプレフィックスとして含む pxGrid FQDN を入力します。たとえば `www.pxgrid-ise.ise.net` です。あるいはワイルドカードを使用します。たとえば `*.ise.net` です。
- 単一の証明書の生成（証明書署名要求あり）（Generate a single certificate with a certificate signing request）：このオプションを選択すると、証明書署名要求の詳細を入力する必要があります。
- 一括証明書の生成（Generate bulk certificates）：必要な詳細を含む CSV ファイルをアップロードすることができます。
- [ルート証明書チェーンのダウンロード (Download root certificate chain)]：pxGrid クライアントの信頼できる証明書ストアに追加するために、ISE パブリックルート証明書をダウンロードします。ISE pxGrid ノードは、新規に署名された pxGrid クライアント証明書だけを信頼します（あるいはこの逆）。これにより、外部の認証局を使用する必要がなくなります。

ステップ 3 （オプション）この証明書の説明を入力できます。

ステップ 4 この証明書のベースとなる pxGrid 証明書テンプレートを表示または編集します。証明書テンプレートには、そのテンプレートに基づいて認証局 (CA) によって発行されたすべての証明書に共通のプロパティが含まれています。証明書テンプレートは、件名、サブジェクト代替名 (SAN)、キー タイプ、キー サイズ、使用する必要がある SCEPRA プロファイル、証明書の有効期間、証明書がクライアントまたはサーバの認証またはその両方に使用される必要があるかどうかを指定した拡張キーの使用状況 (EKU) を定義します。内部 Cisco ISE CA (ISE CA) は、証明書テンプレートを使用し、そのテンプレートに基づいて証明書を発行します。このテンプレートを編集するには、[管理 (Administration)] > [証明書 (Certificates)] > [認証局 (Certificate Authority)] > [証明書テンプレート (Certificate Templates)] を選択します。

ステップ 5 サブジェクト代替名 (SAN) を指定します。複数の SAN を追加できます。次のオプションを使用できます。

- FQDN：ISE ノードの完全修飾ドメイン名を入力します。たとえば `www.isepic.ise.net` です。あるいは FQDN にワイルドカードを使用します。たとえば `*.ise.net` です。

pxGrid FQDN も入力できる追加の行を FQDN に追加できます。これは [コモンネーム (Common Name)] フィールドで使用する FQDN と同一である必要があります。

- [IP アドレス (IP address)] : この証明書に関連付ける ISE ノードの IP アドレスを入力します。サブスクライバが FQDN ではなく IP アドレスを使用する場合には、この情報を入力する必要があります。

(注) このフィールドは、[一括証明書の生成 (Generate bulk certificates)] オプションを選択している場合には表示されません。

ステップ 6 [証明書のダウンロード形式 (Certificate Download Format)] ドロップダウン リストから、以下のいずれかのオプションを選択します。

- Private Enhanced Electronic Mail (PEM) 形式の証明書、PKCS8 PEM 形式のキー (証明書チェーンを含む) : ルート証明書、中間 CA 証明書、およびエンドエンティティ証明書は PEM 形式で表されます。PEM 形式の証明書は BASE64 エンコード ASCII ファイルです。各証明書は「-----BEGIN CERTIFICATE-----」タグで始まり、「-----END CERTIFICATE-----」タグで終わります。エンドエンティティの秘密キーは PKCS* PEM を使用して格納されています。「-----BEGIN ENCRYPTED PRIVATE KEY-----」タグで始まり、「-----END ENCRYPTED PRIVATE KEY-----」タグで終わります。
- PKCS12 形式 (証明書チェーンを含む。つまり証明書チェーンとキーの両方で 1 ファイル) : 1 つの暗号化ファイルにルート CA 証明書、中間 CA 証明書、およびエンドエンティティの証明書と秘密キーを格納するバイナリ形式。

ステップ 7 証明書のパスワードを入力します。

ステップ 8 [作成 (Create)] をクリックします。

サブスクライバの有効化

サブスクライバが からユーザ ID を受信できるようにするため、このタスクを実行するか、または承認を自動的に有効にする必要があります。[サブスクライバの設定 \(481 ページ\)](#) を参照してください。

始める前に

- Cisco pxGrid クライアントからの要求を表示するには、少なくとも 1 つのノードで pxGrid ペルソナを有効にします。
- パッシブ ID サービスを有効にします。詳細については、[Easy Connect \(417 ページ\)](#) を参照してください。

ステップ 1 [ワーク センター (Work Centers)] > [PassiveID] > [サブスクライバ (Subscribers)] を選択し、[クライアント (Clients)] タブが表示されることを確認します。

ステップ 2 サブスクライバの隣にあるチェックボックスをオンにして [承認 (Approve)] をクリックします。

ステップ 3 [リフレッシュ (Refresh)] をクリックすると、最新のステータスが表示されます。

ライブ ログからのサブスクライバイベントの表示

[ライブ ログ (Live Logs)] ページにはすべてのサブスクライバイベントが表示されます。イベント情報には、イベントタイプ、タイムスタンプ、サブスクライバ名、機能名が含まれています。

[サブスクライバ (Subscribers)] に移動し、[ライブ ログ (Live Log)] タブを選択し、イベントリストを表示します。ログを消去して、リストを再同期またはリフレッシュすることもできます。

サブスクライバの設定

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 [管理 (Administration)] > [pxGrid サービス (pxGrid Services)] > [設定 (Settings)] を選択します。

ステップ 2 必要に応じて、次のオプションを選択します。

- **新しいアカウントの自動承認 (Automatically Approve New Accounts)** : このチェック ボックスにマークを付けると、新しい pxGrid クライアントからの接続要求が自動的に承認されます。
- **パスワード ベースのアカウント作成の許可 (Allow Password Based Account Creation)** : このチェック ボックスにマークを付けると、pxGrid クライアントのユーザ名/パスワードベースの認証が有効になります。このオプションを有効にした場合、pxGrid クライアントを自動的に承認することはできません。

pxGrid クライアントは、REST API を介してユーザ名を送信することで、pxGrid コントローラに自身を登録できます。pxGrid コントローラは、クライアント登録時に pxGrid クライアントのパスワードを生成します。管理者は接続要求を承認または拒否できます。

ステップ 3 [保存 (Save)] をクリックします。

PassiveID ワーク センター でのサービスのモニタリングとトラブルシューティング

モニタリング、トラブルシューティング、およびレポーティングの各ツールを使用して PassiveID ワーク センター を管理する方法について説明します。

- [RADIUS ライブ セッション \(1454 ページ\)](#)
- [Cisco ISE アラーム \(1042 ページ\)](#)
- [レポート \(1095 ページ\)](#)
- [着信トラフィックを検証する TCP ダンプ ユーティリティ \(1080 ページ\)](#)

LDAP

Lightweight Directory Access Protocol (LDAP) は、RFC 2251 で定義されている、TCP/IP 上で動作するディレクトリ サービスの問い合わせおよび変更のためのネットワーキング プロトコルです。LDAP は、X.500 ベースのディレクトリ サーバにアクセスするためのライトウェイトメカニズムです。

Cisco ISE は、LDAP プロトコルを使用して LDAP 外部データベース (ID ソースとも呼ばれる) と統合します。

LDAP ディレクトリ サービス

LDAP ディレクトリ サービスは、クライアント/サーバモデルに基づきます。クライアントは、LDAP サーバに接続し、操作要求をサーバに送信することで、LDAP セッションを開始します。サーバは、応答を送信します。1 台以上の LDAP サーバに、LDAP ディレクトリ ツリーまたは LDAP バックエンド データベースからのデータが含まれています。

ディレクトリ サービスは、情報を保持するデータベースであるディレクトリを管理します。ディレクトリ サービスは、情報を保存するために分散モデルを使用します。その情報は、通常はディレクトリ サーバ間で複製されます。

LDAP ディレクトリは、単純なツリー階層で編成されており、数多くのサーバ間で分散できます。各サーバには、定期的に同期化されるディレクトリ全体の複製バージョンを配置できます。

ツリーのエントリには属性のセットが含まれており、各属性には名前 (属性タイプまたは属性の説明) と 1 つ以上の値があります。属性はスキーマに定義されます。

各エントリには、固有識別情報、つまり識別名 (DN) があります。この名前には、エントリ内の属性で構成されている相対識別名 (RDN) と、それに続く親エントリの DN が含まれています。DN は完全なファイル名、RDN はフォルダ内の相対ファイル名と考えることができます。

複数の LDAP インスタンス

IP アドレスまたはポートの設定が異なる複数の LDAP インスタンスを作成することにより、異なる LDAP サーバを使用するか、または同じ LDAP サーバ上の異なるデータベースを使用して認証を行うように、Cisco ISE を設定できます。プライマリ サーバの各 IP アドレスおよびポートの設定は、セカンダリ サーバの IP アドレスおよびポートの設定とともに、Cisco ISE LDAP ID ソース インスタンスに対応する LDAP インスタンスを形成します。

Cisco ISE では、個々の LDAP インスタンスが一意的 LDAP データベースに対応している必要はありません。複数の LDAP インスタンスを、同一のデータベースにアクセスするように設定できます。この方法は、LDAP データベースにユーザまたはグループのサブツリーが複数含まれている場合に役立ちます。各 LDAP インスタンスでは、ユーザとグループに対してそれぞれ単一のサブツリーディレクトリだけをサポートするため、Cisco ISE が認証要求を送信するユー

ザ ディレクトリとグループ ディレクトリのサブツリーの組み合わせごとに、別々の LDAP インスタンスを設定する必要があるからです。

LDAP フェールオーバー

Cisco ISE は、プライマリ LDAP サーバとセカンダリ LDAP サーバ間でのフェールオーバーをサポートします。フェールオーバーは、LDAP サーバがダウンしているかまたは到達不可能なために Cisco ISE で LDAP サーバに接続できないことが原因で認証要求が失敗した場合に発生します。

フェールオーバー設定が指定され、Cisco ISE で接続しようとした最初の LDAP サーバが到達不可能な場合、Cisco ISE は常に 2 番目の LDAP サーバへの接続を試行します。再度、Cisco ISE で最初の LDAP サーバを使用する場合は、[フェールバック再試行の遅延 (Failback Retry Delay)] テキスト ボックスに値を入力する必要があります。



(注) Cisco ISE では、常にプライマリ LDAP サーバを使用して、認証ポリシーで使用するグループと属性を管理者ポータルから取得します。このため、プライマリ LDAP サーバはこれらの項目を設定するときにアクセス可能である必要があります。Cisco ISE では、フェールオーバーの設定に従って、実行時に認証と許可にのみセカンダリ LDAP サーバを使用します。

LDAP 接続管理

Cisco ISE では、複数の同時 LDAP 接続がサポートされます。接続は、最初の LDAP 認証時にオンデマンドで開かれます。最大接続数は、LDAP サーバごとに設定されます。事前に接続を開いておくと、認証時間が短縮されます。同時バインディング接続に使用する最大接続数を設定できます。開かれる接続の数は、LDAP サーバ（プライマリまたはセカンダリ）ごとに異なる場合があります、サーバごとに設定される最大管理接続数に基づいて決まります。

Cisco ISE は、Cisco ISE で設定されている LDAP サーバごとに、開いている LDAP 接続（バインディング情報を含む）のリストを保持します。認証プロセス中に、Connection Manager は開いている接続をプールから検索しようとします。開いている接続が存在しない場合、新しい接続が開かれます。

LDAP サーバが接続を閉じた場合、Connection Manager はディレクトリを検索する最初のコールでエラーをレポートし、接続を更新しようとします。認証プロセスが完了した後、Connection Manager は接続を解放します。

LDAP ユーザ認証

LDAP は、Cisco ISE ユーザ認証のための外部データベースとして使用できます。Cisco ISE ではプレーン パスワード認証がサポートされます。ユーザ認証には次の処理が含まれます。

- LDAP サーバでの、要求のユーザ名に一致するエントリの検索
- ユーザ パスワードを LDAP サーバで見つかったパスワードと照合する

- ポリシーで使用するグループ メンバーシップ情報の取得
- ポリシーおよび許可プロファイルで使用するよう指定された属性の値の取得

ユーザを認証するために、Cisco ISE は LDAP サーバにバインド要求を送信します。バインド要求には、ユーザの DN およびユーザ パスワードがクリア テキストで含まれています。ユーザの DN およびパスワードが LDAP ディレクトリ内のユーザ名およびパスワードと一致した場合に、ユーザは認証されます。

Secure Sockets Layer (SSL) を使用して LDAP サーバへの接続を保護することを推奨します。



- (注) パスワード変更のオプションは、パスワードの有効期限が切れた後にアカウントの残りの猶予ログインがあるときにのみ、LDAP でサポートされます。LDAP サーバの bindResponse は LDAP_SUCCESS であり、bindResponse メッセージに残りの猶予ログインの制御フィールドが含まれる必要があります。bindResponse メッセージにさらなる制御フィールド (残りの猶予ログイン以外) が含まれる場合は、ISE に復号化エラーが発生する可能性があります。

許可ポリシーで使用する LDAP グループおよび属性の取得

Cisco ISE は、ディレクトリ サーバでバインド操作を実行し、サブジェクトを検索および認証することによって、LDAP ID ソースに対してサブジェクト (ユーザまたはホスト) を認証できます。認証が成功した後、Cisco ISE は要求された場合は常にサブジェクトに所属するグループおよび属性を取得できます。Cisco ISE 管理者ポータルで取得されるように属性を設定するには、[管理 (Administration)] > [ID の管理 (Identity Management)] > [外部 ID ソース (External Identity Sources)] > [LDAP] を選択します。Cisco ISE は、これらのグループおよび属性を使用してサブジェクトを許可できます。

ユーザの認証または LDAP ID ソースの問い合わせを行うために、Cisco ISE は LDAP サーバに接続し、接続プールを保持します。

Active Directory が LDAP ストアとして設定されている場合は、グループ メンバーシップに関する次の制限事項に注意する必要があります。

- ユーザまたはコンピュータは、ポリシー条件でポリシールールに一致するように定義されたグループの直接的なメンバーである必要があります。
- 定義されたグループは、ユーザまたはコンピュータのプライマリ グループではない可能性があります。この制限は、Active Directory が LDAP ストアとして設定されている場合にのみ適用されます。

LDAP グループ メンバーシップ情報の取得

ユーザ認証、ユーザ ルックアップ、および MAC アドレス ルックアップのために、Cisco ISE は LDAP データベースからグループ メンバーシップ情報を取得する必要があります。LDAP サーバは、サブジェクト (ユーザまたはホスト) とグループ間の関連付けを次の方法のいずれかで表します。

- グループがサブジェクトを参照：グループオブジェクトには、サブジェクトを指定する属性が含まれています。サブジェクトの識別子は、次のものとしてグループに供給できます。

- 識別名
- プレーン ユーザ名

- サブジェクトがグループを参照：サブジェクトオブジェクトには、所属するグループを指定する属性が含まれています。

LDAP ID ソースには、グループ メンバーシップ情報の取得のために次のパラメータが含まれています。

- [参照方向 (Reference direction)]：このパラメータは、グループ メンバーシップを決定するときに使用する方法を指定します（グループからサブジェクトへまたはサブジェクトからグループへ）。
- [グループマップ属性 (Group Map Attribute)]：このパラメータは、グループ メンバーシップ情報を含む属性を示します。
- [グループ オブジェクト クラス (Group Object Class)]：このパラメータは、特定のオブジェクトがグループとして認識されることを決定します。
- [グループ検索サブツリー (Group Search Subtree)]：このパラメータは、グループ検索の検索ベースを示します。
- [メンバー タイプ オプション (Member Type Option)]：このパラメータは、グループ メンバー属性にメンバーが保存される方法を指定します（DN として、またはプレーン ユーザ名として）。

LDAP 属性の取得

ユーザ認証、ユーザ ルックアップ、および MAC アドレス ルックアップのために、Cisco ISE は LDAP データベースからサブジェクト属性を取得する必要があります。LDAP ID ソースのインスタンスごとに、ID ソースディクショナリが作成されます。これらのディレクトリでは、次のデータ型の属性がサポートされています。

- 文字列
- 符号なし 32 ビット整数
- IPv4 アドレス

符号なし整数および IPv4 属性の場合、Cisco ISE は取得した文字列を対応するデータ型に変換します。変換が失敗した場合、または属性の値が取得されなかった場合、Cisco ISE ではデバッグ メッセージをロギングしますが、認証またはルックアップ プロセスは失敗しません。

変換が失敗した場合、または Cisco ISE で属性の値が取得されない場合に、Cisco ISE で使用できるデフォルトの属性値を任意で設定できます。

LDAP 証明書の取得

ユーザ ルックアップの一部として証明書取得を設定した場合、Cisco ISE は証明書属性の値を LDAP から取得する必要があります。証明書属性の値を LDAP から取得するには、LDAP ID ソースの設定時に、アクセスする属性のリストで証明書属性をあらかじめ設定しておく必要があります。

LDAP サーバによって返されるエラー

次のエラーが認証プロセス中に発生する可能性があります。

- 認証エラー：Cisco ISE は、認証エラーを Cisco ISE ログ ファイルに記録します。

LDAP サーバがバインディング（認証）エラーを返す理由で考えられるのは、次のとおりです。

- パラメータ エラー：無効なパラメータが入力された
- ユーザアカウントが制限されている（無効、ロックアウト、期限切れ、パスワード期限切れなど）
- 初期化エラー：LDAP サーバのタイムアウト設定を使用して、LDAP サーバでの接続または認証が失敗したと判断する前に Cisco ISE が LDAP サーバからの応答を待つ秒数を設定します。

LDAP サーバが初期化エラーを返す理由で考えられるのは、次のとおりです。

- LDAP がサポートされていない。
- サーバがダウンしている。
- サーバがメモリ不足である。
- ユーザに特権がない。
- 間違った管理者クレデンシャルが設定されている。

外部リソースエラーとして次のエラーがロギングされ、LDAP サーバで考えられる問題が示されます。

- 接続エラーが発生した
- タイムアウトが期限切れになった
- サーバがダウンしている
- サーバがメモリ不足である

未知ユーザ エラーとして次のエラーがロギングされます。

- データベースにユーザが存在しない

ユーザは存在するが送信されたパスワードが無効である場合、無効パスワードエラーとして次のエラーがロギングされます。

- 無効なパスワードが入力された

LDAP ユーザ ルックアップ

Cisco ISE は LDAP サーバを使用したユーザ ルックアップ機能をサポートしています。この機能を使用すると、認証なしで LDAP データベース内のユーザを検索し、情報を取得できます。ユーザ ルックアップ プロセスには次のアクションが含まれます。

- LDAP サーバでの、要求のユーザ名に一致するエントリの検索
- ポリシーで使用するユーザ グループ メンバーシップ情報の取得
- ポリシーおよび許可プロファイルで使用するよう指定された属性の値の取得

LDAP MAC アドレス ルックアップ

Cisco ISE は MAC アドレス ルックアップ機能をサポートしています。この機能を使用すると、認証なしで LDAP データベース内の MAC アドレスを検索し、情報を取得できます。MAC アドレス ルックアップ プロセスには次のアクションが含まれます。

- デバイスの MAC アドレスと一致するエントリの LDAP サーバを検索する
- ポリシーで使用するデバイスの MAC アドレス グループ情報の取得
- ポリシーで使用する指定された属性の値の取得

LDAP ID ソースの追加

始める前に

- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。
- Cisco ISE は、許可ポリシーで使用するグループおよび属性を取得するためにプライマリ LDAP サーバを常に使用します。このため、プライマリ LDAP サーバはこれらの項目を設定するときに到達可能である必要があります。

ステップ 1 [管理 (Administration)] > [ID の管理 (Identity Management)] > [外部 ID ソース (External Identity Sources)] > [LDAP] > [追加 (Add)] を選択します。

ステップ 2 値を入力します。

ステップ 3 [送信 (Submit)] をクリックして、LDAP インスタンスを作成します。

関連トピック

- [LDAP](#) (482 ページ)
- [LDAP ディレクトリ サービス](#) (482 ページ)
- [複数の LDAP インスタンス](#) (482 ページ)
- [LDAP フェールオーバー](#) (483 ページ)
- [LDAP 接続管理](#) (483 ページ)
- [LDAP ユーザ認証](#) (483 ページ)
- [許可ポリシーで使用する LDAP グループおよび属性の取得](#) (484 ページ)
- [LDAP グループ メンバーシップ情報の取得](#) (484 ページ)
- [LDAP 属性の取得](#) (485 ページ)
- [LDAP 証明書の取得](#) (486 ページ)
- [LDAP サーバによって返されるエラー](#) (486 ページ)
- [LDAP ユーザ ルックアップ](#) (487 ページ)
- [LDAP MAC アドレス ルックアップ](#) (487 ページ)
- [プライマリおよびセカンダリ LDAP サーバの設定](#) (488 ページ)
- [LDAP サーバからの属性を取得するための Cisco ISE の有効化](#) (489 ページ)
- [LDAP サーバからのグループ メンバーシップ詳細の取得](#) (489 ページ)
- [LDAP サーバからのユーザ属性の取得](#) (490 ページ)
- [LDAP ID ソースによるセキュア認証の有効化](#) (490 ページ)

LDAP スキーマの設定

ステップ 1 [管理 (Administration)] > [ID の管理 (Identity Management)] > [外部 ID ソース (External Identity Sources)] > [LDAP] を選択します。

ステップ 2 LDAP インスタンスを選択します。

ステップ 3 [全般 (General)] タブをクリックします。

ステップ 4 [スキーマ (Schema)] オプションの近くにあるドロップダウン矢印をクリックします。

ステップ 5 [スキーマ (Schema)] ドロップダウンリストから必要なスキーマを選択します。[カスタム (Custom)] オプションを選択して、要件に基づいて属性を更新できます。

事前定義属性は、組み込みスキーマ (Active Directory、Sun directory Server、Novell eDirectory など) に使用されます。事前定義されたスキーマの属性を編集すると、Cisco ISE が自動的にカスタムスキーマを作成します。

プライマリおよびセカンダリ LDAP サーバの設定

LDAP インスタンスを作成したら、プライマリ LDAP サーバに対する接続を設定する必要があります。セカンダリ LDAP サーバの設定は、オプションです。

-
- ステップ 1** [管理 (Administration)] > [ID の管理 (Identity Management)] > [外部 ID ソース (External Identity Sources)] > [LDAP] を選択します。
- ステップ 2** 編集する LDAP インスタンスの隣にあるチェックボックスをオンにし、[編集 (Edit)] をクリックします。
- ステップ 3** [接続 (Connection)] タブをクリックして、プライマリおよびセカンダリ サーバを設定します。
- ステップ 4** 「LDAP ID ソースの設定」の説明に従って、値を入力します。
- ステップ 5** [送信 (Submit)] をクリックして接続パラメータを保存します。
-

LDAP サーバからの属性を取得するための Cisco ISE の有効化

Cisco ISE で LDAP サーバからユーザとグループのデータを取得するには、Cisco ISE で LDAP ディレクトリの詳細を設定する必要があります。LDAP ID ソースでは、次の 3 つの検索が適用されます。

- 管理のためのグループ サブツリーのすべてのグループの検索
- ユーザを特定するためのサブジェクト サブツリーのユーザの検索
- ユーザが所属するグループの検索

-
- ステップ 1** [管理 (Administration)] > [ID の管理 (Identity Management)] > [外部 ID ソース (External Identity Sources)] > [LDAP] を選択します。
- ステップ 2** 編集する LDAP インスタンスの隣にあるチェックボックスをオンにし、[編集 (Edit)] をクリックします。
- ステップ 3** [ディレクトリ構成 (Directory Organization)] タブをクリックします。
- ステップ 4** 「LDAP ID ソースの設定」の説明に従って、値を入力します。
- ステップ 5** [送信 (Submit)] をクリックして設定を保存します。
-

LDAP サーバからのグループ メンバーシップ詳細の取得

新しいグループを追加するか、LDAP ディレクトリからグループを選択できます。

-
- ステップ 1** [管理 (Administration)] > [ID の管理 (Identity Management)] > [外部 ID ソース (External Identity Sources)] > [LDAP] を選択します。
- ステップ 2** 編集する LDAP インスタンスの隣にあるチェックボックスをオンにし、[編集 (Edit)] をクリックします。
- ステップ 3** [グループ (Groups)] タブをクリックします。
- ステップ 4** [追加 (Add)] > [グループの追加 (Add Group)] を選択して新しいグループを追加するか、[追加 (Add)] > [ディレクトリからグループを選択 (Select Groups From Directory)] を選択して LDAP ディレクトリからグループを選択します。
- a) グループの追加を選択した場合は、新しいグループの名前を入力します。

- b) ディレクトリから選択する場合は、フィルタ基準を入力し、[グループの取得 (Retrieve Groups)] をクリックします。検索条件には、アスタリスク (*) ワイルドカード文字を含めることができます。

ステップ 5 選択するグループの隣にあるチェックボックスをオンにし、[OK] をクリックします。

選択したグループが [グループ (Groups)] ページに表示されます。

ステップ 6 グループ選択を保存するには、[送信 (Submit)] をクリックします。



(注) Active Directory の組み込みグループは、Active Directory が Cisco ISE の LDAP ID ストアとして設定されているときにはサポートされません。

LDAP サーバからのユーザ属性の取得

許可ポリシーで使用する LDAP サーバからユーザ属性を取得できます。

ステップ 1 [管理 (Administration)] > [ID の管理 (Identity Management)] > [外部 ID ソース (External Identity Sources)] > [LDAP] を選択します。

ステップ 2 編集する LDAP インスタンスの隣にあるチェックボックスをオンにし、[編集 (Edit)] をクリックします。

ステップ 3 [属性 (Attributes)] タブをクリックします。

ステップ 4 [追加 (Add)] > [属性の追加 (Add Attribute)] を選択して新しい属性を追加するか、[追加 (Add)] > [ディレクトリから属性を選択 (Select Attributes From Directory)] を選択して LDAP サーバから属性を選択します。

- a) 属性を追加する場合は、新しい属性の名前を入力します。
- b) ディレクトリから選択する場合は、例のユーザを入力し、[属性の取得 (Retrieve Attributes)] をクリックしてユーザの属性を取得します。アスタリスク (*) ワイルドカード文字を使用できます。

ステップ 5 選択する属性の隣にあるチェックボックスをオンにし、[OK] をクリックします。

ステップ 6 属性選択を保存するには、[送信 (Submit)] をクリックします。

LDAP ID ソースによるセキュア認証の有効化

LDAP 設定ページで [セキュア認証 (Secure Authentication)] オプションを選択すると、Cisco ISE は LDAP ID ソースとのセキュアな通信に SSL を使用します。LDAP ID ソースへのセキュアな接続は以下を使用して確立されます。

- SSL トンネル : SSL v3 または TLS v1 (LDAP サーバでサポートされる最も強力なバージョン) を使用
- サーバ認証 (LDAP サーバの認証) : 証明書ベース

- クライアント認証（Cisco ISE の認証）：なし（管理者のバインドは SSL トンネル内で使用されます）
- 暗号スイート：Cisco ISE でサポートされるすべての暗号スイート

最も強力な暗号化と Cisco ISE がサポートする暗号方式を備えている TLS v1 を使用することを推奨します。

Cisco ISE が LDAP ID ソースと安全に通信できるようにするには、次の手順を実行します。

始める前に

- Cisco ISE は、LDAP サーバに接続する必要があります
- TCP ポート 636 を開く必要があります

ステップ 1 LDAP サーバにサーバ証明書を発行した CA の認証局（CA）チェーン全体を Cisco ISE にインポートします（[管理（Administration）]>[システム（System）]>[証明書（Certificates）]>[信頼できる証明書（Trusted Certificates）]）。

完全な CA チェーンは、ルート CA 証明書および中間 CA 証明書を参照し、LDAP サーバ証明書は参照しません。

ステップ 2 LDAP ID ソースとの通信時にセキュア認証を使用するように Cisco ISE を設定します（[管理（Administration）]>[ID の管理（Identity Management）]>[外部 ID ソース（External Identity Sources）]>[LDAP]。[接続設定（Connection Settings）] タブで [セキュア認証（Secure Authentication）] チェックボックスを必ずオンにしてください）。

ステップ 3 LDAP ID ストアでルート CA 証明書を選択します。

ODBC ID ソース

オープン データベース コネクティビティ（ODBC）準拠データベースは、ユーザとエンドポイントを認証する外部 ID ソースとして使用できます。ODBC ID ストアは、ID ストアの順序で、ゲストおよびスポンサーの認証に使用できます。また、BYOD フローにも使用できます。

サポートされているデータベース エンジンはおおむね次のとおりです。

- MySQL
- Oracle
- PostgreSQL
- Microsoft SQL Server
- Sybase

ODBC 準拠データベースに対して認証するように Cisco ISE を設定しても、データベースの設定には影響を与えません。データベースを管理するには、データベースのマニュアルを参照してください。

ODBC データベースのクレデンシャル チェック

Cisco ISE は、ODBC データベースに対する 3 つの異なるタイプのクレデンシャル チェックをサポートしています。それぞれのクレデンシャルチェックタイプに適切な SQL ストアドプロシージャを設定する必要があります。ストアドプロシージャは、ODBC データベースで適切なテーブルをクエリし、ODBC データベースから出力パラメータやレコードセットを受信するために使用されます。データベースは、ODBC クエリに応答してレコードセットまたは名前付きパラメータのセットを返すことができます。

パスワードは、クリアテキストまたは暗号化形式で ODBC データベースに保存できます。Cisco ISE によって呼び出された場合は、ストアドプロシージャでパスワードをクリアテキストに復号化できます。

クレデンシャル チェックタイプ	ODBC 入力パラ メータ	ODBC 出力パラ メータ	クレデンシャル チェック	認証プロトコル
ODBC データ ベースのプレー ンテキストパ スワード認証	[ユーザ名 (Username)] [パスワード (Password)]	結果 グループ アカウント情報 エラー文字列	ユーザ名とパスワー ドが一致すると、関 連するユーザ情報が 返されます。	PAP EAP-GTC (PEAP または EAP-FAST の内 部メソッドとし て) TACACS
ODBC データ ベースから取得 したプレーンテ キストパスワー ド	[ユーザ名 (Username)]	結果 グループ アカウント情報 エラー文字列 [パスワード (Password)]	ユーザ名が見つかった 場合、そのパス ワードと関連する ユーザ情報がストア ドプロシージャに よって返されます。 Cisco ISE は、認証方 式に基づいてパス ワードハッシュを計 算し、クライアント から受信したものと 比較します。	CHAP MSCHAPv1/v2 EAP-MD5 LEAP EAP-MSCHAPv2 (PEAP または EAP-FAST の内 部メソッドとし て) TACACS

クレデンシャル チェック タイプ	ODBC 入力パラ メータ	ODBC 出力パラ メータ	クレデンシャル チェック	認証プロトコル
ルックアップ	[ユーザ名 (Username)]	結果 グループ アカウント情報 エラー文字列 (注) 出力パ ラメー タで返 される グルー プは、 Cisco ISE では 使用さ れませ ん。グ ループ の取得 ストア ドプロ シー ジャに よって 取得さ れたグ ループ のみが Cisco ISE で使 用され ます。 アカウ ント情 報は、 認証の 監査ロ グにの み含ま れてい ます。	ユーザ名が見つかった場合、該当するユーザ情報が返されます。	MAB PEAP、 EAP-FAST、 EAP-TTLS の高速再接続

次の表に、ODBC データベース ストアド プロシージャと Cisco ISE 認証結果コードによって返される、結果コード間のマッピングを示します。

(ストアド プロシージャによって返される) 結果コード	説明	Cisco ISE 認証結果コード
[0]	CODE_SUCCESS	該当なし (認証成功)
1	CODE_UNKNOWN_USER	UnknownUser
2	CODE_INVALID_PASSWORD	失敗しました (Failed)
3	CODE_UNKNOWN_USER_OR_INVALID_PASSWORD	UnknownUser
4	CODE_INTERNAL_ERROR	エラー (Error)
10001	CODE_ACCOUNT_DISABLED	DisabledUser
10002	CODE_PASSWORD_EXPIRED	NotPerformedPasswordExpired



(注) Cisco ISE は、このマッピングされた認証結果コードに基づいて実際の認証/ルックアップ操作を実行します。

ODBC データベースからグループと属性を取得するためにストアド プロシージャを使用できます。

プレーンテキストパスワード認証用のレコードセットを返すサンプルのプロシージャ (Microsoft SQL Server 用)

```
CREATE PROCEDURE [dbo].[ISEAuthUserPlainReturnsRecordset]
    @username varchar(64), @password varchar(255)
AS
BEGIN
    IF EXISTS( SELECT username
    FROM NetworkUsers
    WHERE username = @username
    AND password = @password )
    SELECT 0,11,'give full access','No Error'
    FROM NetworkUsers
    WHERE username = @username
    ELSE
    SELECT 3,0,'odbc','ODBC Authen Error'
END
```

プレーンテキストパスワード取得用のレコードセットを返すサンプルのプロシージャ (Microsoft SQL Server 用)

```
CREATE PROCEDURE [dbo].[ISEFetchPasswordReturnsRecordset]
    @username varchar(64)
```

```

AS
BEGIN
    IF EXISTS( SELECT  username
FROM  NetworkUsers
WHERE  username = @username)
    SELECT 0,11,'give full access','No Error',password
FROM  NetworkUsers
WHERE  username = @username
ELSE
    SELECT 3,0,'odbc','ODBC Authen Error'
END

```

ルックアップ用のレコードセットを返すサンプルのプロシージャ (Microsoft SQL Server 用)

```

CREATE PROCEDURE [dbo].[ISEUserLookupReturnsRecordset]
    @username varchar(64)
AS
BEGIN
    IF EXISTS( SELECT  username
FROM  NetworkUsers
WHERE  username = @username)
    SELECT 0,11,'give full access','No Error'
FROM  NetworkUsers
WHERE  username = @username
ELSE
    SELECT 3,0,'odbc','ODBC Authen Error'
END

```

プレーン テキスト パスワード 認証用のパラメータを返すサンプルのプロシージャ (Microsoft SQL Server 用)

```

CREATE PROCEDURE [dbo].[ISEAuthUserPlainReturnsParameters]
    @username varchar(64), @password varchar(255), @result INT OUTPUT, @group
varchar(255) OUTPUT, @acctInfo varchar(255) OUTPUT, @errorString varchar(255) OUTPUT
AS
BEGIN
    IF EXISTS( SELECT  username
FROM  NetworkUsers
WHERE  username = @username
AND  password = @password )
    SELECT @result=0, @group=11, @acctInfo='give full access', @errorString='No
Error'
FROM  NetworkUsers
WHERE  username = @username
ELSE
    SELECT @result=3, @group=0, @acctInfo='odbc', @errorString='ODBC Authen Error'
END

```

プレーン テキスト パスワード 取得用のパラメータを返すサンプルのプロシージャ (Microsoft SQL Server 用)

```

CREATE PROCEDURE [dbo].[ISEFetchPasswordReturnsParameters]
    @username varchar(64), @result INT OUTPUT, @group varchar(255) OUTPUT, @acctInfo
varchar(255) OUTPUT, @errorString varchar(255) OUTPUT, @password varchar(255) OUTPUT
AS
BEGIN
    IF EXISTS( SELECT  username
FROM  NetworkUsers
WHERE  username = @username)
    SELECT @result=0, @group=11, @acctInfo='give full access', @errorString='No
Error', @password=password
FROM  NetworkUsers

```

ODBC データベースのクレデンシャル チェック

```

WHERE username = @username
ELSE
SELECT @result=3, @group=0, @acctInfo='odbc', @errorString='ODBC Authen Error'
END

```

ルックアップ用のパラメータを返すサンプルのプロシージャ (Microsoft SQL Server 用)

```

CREATE PROCEDURE [dbo].[ISEUserLookupReturnsParameters]
    @username varchar(64), @result INT OUTPUT, @group varchar(255) OUTPUT, @acctInfo
    varchar(255) OUTPUT, @errorString varchar(255) OUTPUT
AS
BEGIN
    IF EXISTS( SELECT username
FROM NetworkUsers
WHERE username = @username)
SELECT @result=0, @group=11, @acctInfo='give full access', @errorString='No
Error'
FROM NetworkUsers
WHERE username = @username
ELSE
SELECT @result=3, @group=0, @acctInfo='odbc', @errorString='ODBC Authen Error'
END

```

Microsoft SQL Server からグループを取得するサンプルのプロシージャ

```

CREATE PROCEDURE [dbo].[ISEGroupsH]
    @username varchar(64), @result int output
AS
BEGIN
    if exists (select * from NetworkUsers where username = @username)
begin
        set @result = 0
        select 'accountants', 'engineers', 'sales','test_group2'
    end
    else
        set @result = 1
END

```

ユーザ名が「*」の場合にすべてのユーザのすべてのグループを取得するサンプルのプロシージャ (Microsoft SQL Server 用)

```

ALTER PROCEDURE [dbo].[ISEGroupsH]
    @username varchar(64), @result int output
AS
BEGIN
    if @username = '*'
begin
        -- if username is equal to '*' then return all existing
        groups
        set @result = 0
        select 'accountants', 'engineers',
'sales','test_group1','test_group2','test_group3','test_group4'
    end
    else
        if exists (select * from NetworkUsers where username = @username)
begin
        set @result = 0
        select 'accountants'
    end
    else
        set @result = 1
END

```

Microsoft SQL Server から属性を取得するサンプルのプロシージャ

```
CREATE PROCEDURE [dbo].[ISEAttrSH]
    @username varchar(64), @result int output
AS
BEGIN
    if exists (select * from NetworkUsers where username = @username)
    begin
        set @result = 0
        select phone as phone, username as username, department
        as department, floor as floor, memberOf as memberOf, isManager as isManager from
        NetworkUsers where username = @username
    end
    else
        set @result = 1
END
```

ODBC ID ソースの追加

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

-
- ステップ 1** [管理 (Administration)] > [ID の管理 (Identity Management)] > [外部 ID ソース (External Identity Sources)] を選択します。
- ステップ 2** [ODBC] をクリックします。
- ステップ 3** [追加 (Add)] をクリックします。
- ステップ 4** [一般 (General)] タブで、ODBC ID ソースの名前と説明を入力します。
- ステップ 5** [接続 (Connection)] タブで、次の詳細情報を入力します。

- ODBC データベースのホスト名または IP アドレス（データベースに非標準 TCP ポートが使用されている場合は、次の形式でポート番号を指定できます。ホスト名または IP アドレス:ポート）
- ODBC データベースの名前
- 管理者のユーザ名およびパスワード（Cisco ISE がこれらのクレデンシャルを使用してデータベースに接続します）
- 秒単位のサーバのタイムアウト（デフォルトは 5 秒）
- 接続の試行（デフォルトは 1）
- データベース タイプを選択します。次のいずれかを実行します。
 - MySQL
 - Oracle
 - PostgreSQL
 - Microsoft SQL Server
 - Sybase

ステップ 6 [テスト接続 (Test Connection)] をクリックして ODBC データベースとの接続を確認し、設定された使用例用のストアードプロシージャの存在を確認します。

ステップ 7 [ストアードプロシージャ (Stored Procedures)] タブで、次の詳細情報を入力します。

- ストアドプロシージャのタイプ (Stored Procedure Type) : データベースが提供する出力のタイプを選択します。
 - レコードセットを返す (Returns Recordset) : データベースは、ODBC クエリに応じてレコードセットを返します。
 - [パラメータを返す (Returns Parameters)] : データベースは、ODBC クエリに応じて名前付きパラメータのセットを返します。
- プレーン テキスト パスワード 認証 (Plain Text Password Authentication) : プレーン テキスト パスワード 認証のために ODBC サーバ上で実行するストアードプロシージャの名前を入力します。PAP、EAP-GTC 内部メソッド、TACACS 用に使用されます。
- プレーン テキスト パスワード の取得 (Plain Text Password Fetching) : プレーン テキスト パスワード の取得のために ODBC サーバ上で実行するストアードプロシージャの名前を入力します。CHAP、MS-CHAPv1/v2、LEAP、EAP-MD5、EAP-MSCHAPv2 内部メソッド、TACACS 用に使用されます。
- ユーザ名またはマシンの存在を確認する (Check username or machine exists) : ユーザ/MAC アドレス ルックアップのために ODBC サーバ上で実行するストアードプロシージャの名前を入力します。MAB、および PEAP、EAP-FAST、EAP-TTLS の高速再接続用に使用されます。
- グループの取得 (Fetch Groups) : ODBC データベースからグループを取得するストアードプロシージャの名前を入力します。
- 属性の取得 (Fetch Attributes) : ODBC データベースから属性とその値を取得するストアードプロシージャの名前を入力します。
- この形式の MAC アドレスを検索 (Search for MAC address in format) : 着信 MAC アドレスは、選択した MAC 形式に基づいて正規化されます。

ステップ 8 [属性 (Attributes)] タブに必要な属性を追加します。属性の追加時に、属性名が認証ポリシー ルールでどのように表示されるかを指定できます。

ODBC データベースから属性を取得することもできます。ユーザ名と MAC アドレスの両方を使用して ODBC データベースから属性を取得することができます。文字列、ブール値、整数の属性がサポートされています。これらの属性は、認証ポリシーで使用できます。

ステップ 9 [グループ (Groups)] タブにユーザ グループを追加します。また、ユーザ名または MAC アドレスを指定して ODBC データベースからグループを取得することもできます。これらのグループは、認証ポリシーで使用できます。

グループおよび属性の名前を変更できます。デフォルトでは、[ISE の名前 (Name in ISE)] フィールドに表示される名前は ODBC データベースのものと同等ですが、この名前は変更できます。この名前が認証ポリシーで使用されます。

ステップ 10 [送信 (Submit)] をクリックします。

RADIUS トークン ID ソース

RADIUS プロトコルをサポートし、ユーザおよびデバイスに認証、許可、アカウントिंग (AAA) サービスを提供するサーバは、RADIUS サーバと呼ばれます。RADIUS ID ソースは、サブジェクトとそのクレデンシャルの集合を含み、通信に RADIUS プロトコルを使用する外部 ID ソースです。たとえば、Safeword トークンサーバは、複数のユーザおよびそのクレデンシャルをワンタイム パスワードとして含めることができる ID ソースであり、Safeword トークンサーバによって提供されるインターフェイスでは、RADIUS プロトコルを使用して問い合わせることができます。

Cisco ISE では、RADIUS RFC 2865 準拠のいずれかのサーバが外部 ID ソースとしてサポートされています。Cisco ISE では、複数の RADIUS トークンサーバ ID がサポートされています。たとえば、RSA SecurID サーバや SafeWord サーバなどです。RADIUS ID ソースは、ユーザを認証するために使用される任意の RADIUS トークン サーバと連携できます。

RADIUS トークン サーバでサポートされる認証プロトコル

Cisco ISE では、RADIUS ID ソースに対して次の認証プロトコルがサポートされています。

- RADIUS PAP
- 内部拡張認証プロトコル汎用トークン カード (EAP-GTC) を含む保護拡張認証プロトコル (PEAP)
- 内部 EAP-GTC を含む EAP-FAST

通信に RADIUS トークン サーバで使用されるポート

RADIUS ID トークン サーバでは、認証セッションに UDP ポートが使用されます。このポートはすべての RADIUS 通信に使用されます。Cisco ISE で RADIUS ワンタイム パスワード (OTP) メッセージを RADIUS 対応トークン サーバに送信するには、Cisco ISE と RADIUS 対応トークン サーバの間のゲートウェイ デバイスが、UDP ポートを介した通信を許可するように設定されている必要があります。UDP ポートは、管理者ポータルを介して設定できます。

RADIUS 共有秘密

Cisco ISE で RADIUS ID ソースを設定するときに、共有秘密を指定する必要があります。この共有秘密情報は、RADIUS トークンサーバ上で設定されている共有秘密情報と同一である必要があります。

RADIUS トークン サーバでのフェールオーバー

Cisco ISE では、複数の RADIUS ID ソースを設定できます。各 RADIUS ID ソースには、プライマリとセカンダリの RADIUS サーバを指定できます。Cisco ISE からプライマリ サーバに接続できない場合は、セカンダリ サーバが使用されます。

RADIUS トークン サーバの設定可能なパスワード プロンプト

RADIUS ID ソースでは、パスワード プロンプトを設定できます。パスワード プロンプトは、管理者ポータルを介して設定できます。

RADIUS トークン サーバのユーザ認証

Cisco ISE は、ユーザ クレデンシャル（ユーザ名とパスコード）を取得し、RADIUS トークン サーバに渡します。また、Cisco ISE は RADIUS トークン サーバ認証処理の結果をユーザに中継します。

RADIUS トークン サーバのユーザ属性キャッシュ

RADIUS トークン サーバでは、デフォルトではユーザ ルックアップはサポートされていません。ただし、ユーザ ルックアップは次の Cisco ISE 機能に不可欠です。

- PEAP セッション再開：この機能によって、認証の成功後、EAP セッションの確立中に PEAP セッションを再開できます。
- EAP/FAST 高速再接続：この機能によって、認証の成功後、EAP セッションの確立中に高速再接続が可能になります。

Cisco ISE では、これらの機能のユーザ ルックアップ要求を処理するために、成功した認証の結果がキャッシュされます。成功した認証すべてについて、認証されたユーザの名前と取得された属性がキャッシュされます。失敗した認証はキャッシュに書き込まれません。

キャッシュは、実行時にメモリで使用可能であり、分散展開の Cisco ISE ノード間で複製されません。管理者ポータルを介してキャッシュの存続可能時間（TTL）制限を設定できます。ID キャッシングオプションを有効にし、エージングタイムを分単位で設定する必要があります。指定した時間、キャッシュはメモリで使用可能です。

ID 順序での RADIUS ID ソース

ID ソース順序で認証順序用の RADIUS ID ソースを追加できます。ただし、属性取得順序用の RADIUS ID ソースを追加することはできません。これは、認証しないで RADIUS ID ソースを問い合わせることはできないためです。RADIUS サーバによる認証中、Cisco ISE では異なるエラーを区別できません。すべてのエラーに対して RADIUS サーバから Access-Reject メッセージが返されます。たとえば、RADIUS サーバでユーザが見つからない場合、RADIUS サーバからは User Unknown ステータスの代わりに Access-Reject メッセージが返されます。

RADIUS サーバがすべてのエラーに対して同じメッセージを返す

RADIUS サーバでユーザが見つからない場合、RADIUS サーバからは Access-Reject メッセージが返されます。Cisco ISE では、管理者ポータルを使用してこのメッセージを [認証失敗 (Authentication Failed)] メッセージまたは [ユーザが見つからない (User Not Found)] メッセージとして設定するためのオプションを使用できます。ただし、このオプションを使用すると、ユーザが未知の状況だけでなく、すべての失敗状況に対して「ユーザが見つからない (User Not Found)」メッセージが返されます。

次の表は、RADIUS ID サーバで発生するさまざまな失敗状況を示しています。

表 32: エラー処理

失敗状況	失敗の理由
認証に失敗	<ul style="list-style-type: none"> ユーザが未知である。 ユーザが不正なパスコードでログインしようとしている。 ユーザ ログイン時間が期限切れになった。
プロセスの失敗	<ul style="list-style-type: none"> RADIUS サーバが Cisco ISE で正しく設定されていない。 RADIUS サーバが使用できない。 RADIUS パケットが偽装として検出されている。 RADIUS サーバとのパケットの送受信の問題。 タイムアウト。
不明なユーザ	認証が失敗し、[拒否で失敗 (Fail on Reject)] オプションが false に設定されている。

Safeword サーバでサポートされる特別なユーザ名の形式

Safeword トークンサーバでは、次のユーザ名フォーマットでの認証がサポートされています。

ユーザ名 : Username, OTP

Cisco ISE では、認証要求を受信するとすぐにユーザ名が解析され、次のユーザ名に変換されます。

ユーザ名 : Username

SafeWord トークン サーバでは、これらの両方のフォーマットがサポートされています。Cisco ISE はさまざまなトークン サーバと連携します。SafeWord サーバを設定する場合、Cisco ISE でユーザ名を解析して指定のフォーマットに変換するには、管理者ポータルで [SafeWord サーバ (SafeWord Server)] チェックボックスをオンにする必要があります。この変換は、要求が RADIUS トークン サーバに送信される前に、RADIUS トークン サーバ ID ソースで実行されます。

RADIUS トークン サーバでの認証要求と応答

Cisco ISE が RADIUS 対応トークン サーバに認証要求を転送する場合、RADIUS 認証要求には次の属性が含まれます。

- User-Name (RADIUS 属性 1)
- User-Password (RADIUS 属性 2)
- NAS-IP-Address (RADIUS 属性 4)

Cisco ISE は次の応答のいずれかを受信すると想定されます。

- Access-Accept : 属性は必要ありませんが、応答には RADIUS トークン サーバの設定に基づいてさまざまな属性が含まれる場合があります。
- Access-Reject : 属性は必要ありません。
- Access-Challenge : RADIUS RFC ごとに必要な属性は次のとおりです。
 - State (RADIUS 属性 24)
 - Reply-Message (RADIUS 属性 18)
 - 次の 1 つ以上の属性 : Vendor-Specific、Idle-Timeout (RADIUS 属性 28)、Session-Timeout (RADIUS 属性 27)、Proxy-State (RADIUS 属性 33)
 Access-Challenge ではそれ以外の属性は使用できません。

RADIUS トークン サーバの追加

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 [管理 (Administration)] > [ID の管理 (Identity Management)] > [外部 ID ソース (External Identity Sources)] > [RADIUS トークン (RADIUS Token)] > [追加 (Add)] を選択します。

ステップ 2 [一般 (General)] タブおよび [接続 (Connection)] タブに値を入力します。

ステップ 3 [認証 (Authentication)] タブをクリックします。

このタブでは、RADIUS トークンサーバからの Access-Reject メッセージへの応答を制御できます。この応答は、クレデンシャルが無効であること、またはユーザが不明であることのいずれかを意味する場合があります。Cisco ISE は、認証失敗か、またはユーザが見つからないかのいずれかの応答を受け入れます。このタブでは、ID キャッシングを有効にし、キャッシュのエイジングタイムを設定することもできます。パスワードを要求するプロンプトを設定することもできます。

- a) RADIUS トークンサーバからの Access-Reject 応答を認証失敗として処理する場合は、[拒否を「認証失敗」]として処理 (Treat Rejects as 'authentication failed')] オプション ボタンをクリックします。
- b) RADIUS トークンサーバからの Access-Reject 応答を未知ユーザ エラーとして処理する場合は、[拒否を「ユーザが見つからない」]として処理 (Treat Rejects as 'user not found')] オプション ボタンをクリックします。

ステップ 4 RADIUS トークンサーバとの最初の認証の成功の後、Cisco ISE でキャッシュにパスワードを保存し、設定された期間内に発生した後続の認証に対しキャッシュされたユーザのクレデンシャルを使用する場合、[パスワード キャッシングの有効化 (Enable Passcode Caching)] チェック ボックスをオンにします。

パスワードをキャッシュ内に保存する必要がある秒数を [エイジング タイム (Aging Time)] フィールドに入力します。この期間内にユーザは同じパスワードで複数回の認証を行うことができます。デフォルト値は 30 秒です。有効な範囲は 1 ~ 300 秒です。

(注) Cisco ISE は、認証が初めて失敗した後でキャッシュをクリアします。ユーザは新しい有効なパスワードを入力する必要があります。

(注) EAP-FAST-GTC などの、パスワードの暗号化をサポートするプロトコルを使用する場合にのみこのオプションを有効にすることを強く推奨します。RADIUS トークンサーバでサポートされている認証プロトコルについては、次を参照してください。 [RADIUS トークンサーバでサポートされる認証プロトコル \(499 ページ\)](#)

ステップ 5 [許可 (Authorization)] タブをクリックします。

このタブでは、Cisco ISE への Access-Accept 応答を送信中に RADIUS トークンサーバによって返されるこの属性に対して表示される名前を設定できます。この属性は、許可ポリシー条件で使用できます。デフォルト値は CiscoSecure-Group-Id です。

ステップ 6 [送信 (Submit)] をクリックします。

関連トピック

- [RADIUS トークン ID ソース \(499 ページ\)](#)
- [RADIUS トークンサーバでサポートされる認証プロトコル \(499 ページ\)](#)
- [通信に RADIUS トークンサーバで使用するポート \(499 ページ\)](#)
- [RADIUS 共有秘密 \(499 ページ\)](#)
- [RADIUS トークンサーバでのフェールオーバー \(500 ページ\)](#)
- [RADIUS トークンサーバの設定可能なパスワードプロンプト \(500 ページ\)](#)
- [RADIUS トークンサーバのユーザ認証 \(500 ページ\)](#)
- [RADIUS トークンサーバのユーザ属性キャッシュ \(500 ページ\)](#)
- [ID 順序での RADIUS ID ソース \(500 ページ\)](#)

[RADIUS サーバがすべてのエラーに対して同じメッセージを返す](#) (501 ページ)

[Safeword サーバでサポートされる特別なユーザ名の形式](#) (501 ページ)

[RADIUS トークン サーバでの認証要求と応答](#) (502 ページ)

RADIUS トークン サーバの削除

始める前に

- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。
- ID ソース順序に含まれる RADIUS トークン サーバを選択していないことを確認します。ID ソース順序に含まれる RADIUS トークン サーバを削除用を選択した場合、削除操作は失敗します。

ステップ 1 [管理 (Administration)] > [ID の管理 (Identity Management)] > [外部 ID ソース (External Identity Sources)] > [RADIUS トークン (RADIUS Token)] を選択します。

ステップ 2 削除する RADIUS トークン サーバの隣にあるチェックボックスをオンにし、[削除 (Delete)] をクリックします。

ステップ 3 [OK] をクリックして、選択した RADIUS トークン サーバを削除します。

削除する RADIUS トークン サーバを複数選択し、その 1 つが ID ソース順序で使用されている場合、削除操作は失敗し、いずれの RADIUS トークン サーバも削除されません。

RSA ID ソース

Cisco ISE では、外部データベースとして RSA SecurID サーバがサポートされています。RSA SecurID の 2 要素認証は、ユーザの PIN と、タイムコードアルゴリズムに基づいて使い捨てのトークンコードを生成する個別に登録された RSA SecurID トークンで構成されます。異なるトークンコードが固定間隔（通常は 30 または 60 秒ごと）で生成されます。RSA SecurID サーバでは、この動的な認証コードが検証されます。各 RSA SecurID トークンは固有であり、過去のトークンに基づいて将来のトークンの値を予測することはできません。そのため、正しいトークンコードが PIN とともに提示された場合、その人が有効なユーザである確実性が高くなります。したがって、RSA SecurID サーバでは、従来の再利用可能なパスワードよりも信頼性の高い認証メカニズムが提供されます。

Cisco ISE では、次の RSA ID ソースがサポートされています。

- RSA ACE/Server 6.x シリーズ
- RSA Authentication Manager 7.x および 8.0 シリーズ

次のいずれかの方法で、RSA SecurID 認証テクノロジーと統合できます。

- RSA SecurID エージェントの使用：ユーザは、RSA のネイティブプロトコルによってユーザ名およびパスワードで認証されます。
- RADIUS プロトコルの使用：ユーザは、RADIUS プロトコルによってユーザ名およびパスワードで認証されます。

Cisco ISE の RSA SecurID トークン サーバは、RSA SecurID 認証テクノロジーと RSA SecurID エージェントを使用して接続します。

Cisco ISE では、1 つの RSA 領域だけがサポートされています。

Cisco ISE と RSA SecurID サーバの統合

Cisco ISE と RSA SecurID サーバを接続するには、次の 2 つの管理ロールが必要です。

- RSA サーバ管理者：RSA システムおよび統合を設定および維持します
- Cisco ISE 管理者：Cisco ISE を RSA SecurID サーバに接続するように設定し、設定を維持します

ここでは、Cisco ISE に RSA SecurID サーバを外部 ID ソースとして接続するために必要なプロセスについて説明します。RSA サーバについての詳細は、RSA に関するドキュメントを参照してください。

Cisco ISE の RSA 設定

RSA 管理システムでは `sdconf.rec` ファイルが生成されます。このファイルは RSA システム管理者によって提供されます。このファイルを使用すると、Cisco ISE サーバを領域内の RSA SecurID エージェントとして追加できます。このファイルを参照して Cisco ISE に追加する必要があります。プライマリ Cisco ISE サーバは、複製のプロセスによってこのファイルをすべてのセカンダリ サーバに配布します。

RSA SecurID サーバに対する RSA エージェント認証

`sdconf.rec` ファイルがすべての Cisco ISE サーバにインストールされると、RSA エージェントモジュールが初期化され、RSA 生成のクレデンシャルによる認証が各 Cisco ISE サーバで実行されます。展開内の各 Cisco ISE サーバ上のエージェントが正常に認証されると、RSA サーバとエージェントモジュールは `securid` ファイルをダウンロードします。このファイルは Cisco ISE ファイルシステムに存在し、RSA エージェントによって定義された既知の場所にあります。

分散 Cisco ISE 環境の RSA ID ソース

分散 Cisco ISE 環境で RSA ID ソースを管理するには、次の操作が必要です。

- `sdconf.rec` および `sdopts.rec` ファイルのプライマリ サーバからセカンダリ サーバへの配布。
- `securid` および `sdstatus.12` ファイルの削除。

Cisco ISE 展開の RSA サーバの更新

Cisco ISE で `sdconf.rec` ファイルを追加した後、RSA サーバを廃止する場合、または新しい RSA セカンダリ サーバを追加する場合、RSA SecurID 管理者は `sdconf.rec` ファイルを更新することがあります。更新されたファイルは RSA SecurID 管理者によって提供されます。更新されたファイルによって Cisco ISE を再設定できます。Cisco ISE では、更新されたファイルが複製プロセスによって展開内のセカンダリ Cisco ISE サーバに配布されます。Cisco ISE では、まずファイル システムのファイルを更新し、RSA エージェント モジュールに合わせて調整して再起動プロセスを適切に段階的に行います。`sdconf.rec` ファイルが更新されると、`sdstatus.12` および `securid` ファイルがリセット（削除）されます。

自動 RSA ルーティングの上書き

領域内に複数の RSA サーバを持つことができます。`sdopts.rec` ファイルはロード バランサの役割を果たします。Cisco ISE サーバと RSA SecurID サーバはエージェント モジュールを介して動作します。Cisco ISE に存在するエージェント モジュールは、領域内の RSA サーバを最大限に利用するためにコストベースのルーティング テーブルを保持します。ただし、領域の各 Cisco ISE サーバの手動設定を使用してこのルーティングを上書きするには、管理者ポータルで `sdopts.rec` と呼ばれるテキスト ファイルを使用します。このファイルの作成方法については、RSA に関するドキュメントを参照してください。

RSA ノード秘密リセット

`securid` ファイルは秘密 ノード キー ファイルです。RSA が最初に設定されると、RSA では秘密を使用してエージェントが検証されます。Cisco ISE に存在する RSA エージェントが RSA サーバに対して初めて正常に認証されると、`securid` と呼ばれるファイルがクライアント マシン上に作成され、このファイルを使用して、マシン間で交換されるデータが有効であることが確認されます。展開内の特定の Cisco ISE サーバまたはサーバのグループから `securid` ファイルを削除する必要がある場合があります（たとえば、RSA サーバでのキーのリセット後など）。領域に対する Cisco ISE サーバからこのファイルを削除するには、Cisco ISE 管理者ポータルを使用できます。Cisco ISE の RSA エージェントが次回正常に認証されたとき、新しい `securid` ファイルが作成されます。



(注) Cisco ISE の最新リリースへのアップグレード後に認証が失敗した場合は、RSA 秘密をリセットします。

RSA の自動可用性のリセット

`sdstatus.12` ファイルは、領域内の RSA サーバのアベイラビリティに関する情報を提供します。たとえば、いずれのサーバがアクティブで、いずれのサーバがダウンしているかに関する情報を提供します。エージェント モジュールは領域内の RSA サーバと連携して、このアベイラビリティ ステータスを維持します。この情報は、`sdstatus.12` ファイルに連続的に表示されます。このファイルは、Cisco ISE ファイル システムの既知の場所に供給されます。このファイルは古くなり、現在のステータスが反映されていないことがあります。その場合、現在のステータ

スが反映されるように、このファイルを削除する必要があります。特定の領域に対する固有の Cisco ISE サーバからファイルを削除するには、管理者ポータルを使用できます。Cisco ISE は RSA エージェントに合わせて調整して、再起動が正しく段階的に行われるようにします。

アベイラビリティ ファイル `sdstatus.12` は、`securid` ファイルがリセットされるか、`sdconf.rec` または `sdopts.rec` ファイルが更新されるたびに削除されます。

RSA ID ソースの追加

RSA ID ソースを作成するには、RSA コンフィギュレーション ファイル (`sdconf.rec`) をインポートする必要があります。RSA 管理者から `sdconf.rec` ファイルを取得する必要があります。このタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

RSA ID ソースを追加するには、次のタスクを実行します。

関連トピック

- [RSA ID ソース \(504 ページ\)](#)
- [Cisco ISE と RSA SecurID サーバの統合 \(505 ページ\)](#)
- [Cisco ISE の RSA 設定 \(505 ページ\)](#)
- [RSA SecurID サーバに対する RSA エージェント認証 \(505 ページ\)](#)
- [分散 Cisco ISE 環境の RSA ID ソース \(505 ページ\)](#)
- [Cisco ISE 展開の RSA サーバの更新 \(506 ページ\)](#)
- [自動 RSA ルーティングの上書き \(506 ページ\)](#)
- [RSA ノード秘密リセット \(506 ページ\)](#)
- [RSA の自動可用性のリセット \(506 ページ\)](#)
- [RSA コンフィギュレーション ファイルのインポート \(507 ページ\)](#)
- [Cisco ISE サーバのオプション ファイルの設定および SecurID ファイルと `sdstatus.12` ファイルのリセット \(508 ページ\)](#)
- [RSA ID ソースの認証制御オプションの設定 \(509 ページ\)](#)
- [RSA プロンプトの設定 \(510 ページ\)](#)
- [RSA メッセージの設定 \(510 ページ\)](#)

RSA コンフィギュレーション ファイルのインポート

Cisco ISE に RSA ID ソースを追加するには、RSA コンフィギュレーション ファイルをインポートする必要があります。

ステップ 1 [管理 (Administration)] > [ID の管理 (Identity Management)] > [外部 ID ソース (External Identity Sources)] > [RSA SecurID] > [追加 (Add)] を選択します。

ステップ 2 [参照 (Browse)] をクリックして、クライアントブラウザを実行しているシステムから新しい `sdconf.rec` ファイルまたは更新された `sdconf.rec` ファイルを選択します。

初めて RSA ID ソースを作成する場合、[新しい `sdconf.rec` ファイルのインポート (Import new `sdconf.rec` file)] フィールドは必須フィールドです。これ以降は、既存の `sdconf.rec` ファイルを更新されたファイルで置き換えることができますが、既存のファイルの置き換えは任意です。

- ステップ 3** サーバのタイムアウト値を秒単位で入力します。Cisco ISE はタイムアウトになる前に、指定された秒数 RSA サーバからの応答を待ちます。この値には、1 ～ 199 の任意の整数を指定できます。デフォルト値は 30 秒です。
- ステップ 4** PIN が変更された場合に強制的に再認証するには、[変更 PIN で再認証 (Reauthenticate on Change PIN)] チェックボックスをオンにします。
- ステップ 5** [保存 (Save)] をクリックします。
- Cisco ISE は、次のシナリオもサポートします。
- Cisco ISE サーバのオプション ファイルの設定および SecurID ファイルと sdstatus.12 ファイルのリセット。
 - RSA ID ソースの認証制御オプションの設定。

Cisco ISE サーバのオプション ファイルの設定および SecurID ファイルと sdstatus.12 ファイルのリセット

- ステップ 1** Cisco ISE サーバにログインします。
- ステップ 2** [管理 (Administration)] > [ID の管理 (Identity Management)] > [外部 ID ソース (External Identity Sources)] > [RSA SecurID] > [追加 (Add)] を選択します。
- ステップ 3** [RSA インスタンス ファイル (RSA Instance Files)] タブをクリックします。
- このページには、展開内のすべての Cisco ISE サーバの sdopts.rec servers ファイルが一覧表示されます。
- ユーザが RSA SecurID トークン サーバに対して認証されると、ノードのシークレット ステータスは [作成済み (Created)] と表示されます。ノードのシークレット ステータスは、[作成済み (Created)] または [未作成 (Not Created)] のどちらかになります。クリアされると、ノードのシークレット ステータスは [未作成 (Not Created)] と表示されます。
- ステップ 4** 特定の Cisco ISE サーバの sdopts.rec ファイルの横にあるオプション ボタンをクリックし、[オプション ファイルの更新 (Update Options File)] をクリックします。
- [現在のファイル (Current File)] 領域に既存のファイルが表示されます。
- ステップ 5** 次のいずれかを実行します。
- [RSA エージェントが保持する自動ロード バランシング ステータスを使用 (Use the Automatic Load Balancing status maintained by the RSA agent)] : RSA エージェントでロード バランシングを自動的に管理する場合は、このオプションを選択します。
 - [次で選択された sdopts.rec ファイルで自動ロード バランシング ステータスを上書き (Override the Automatic Load Balancing status with the sdopts.rec file selected below)] : 特定のニーズに基づいて手動でロード バランシングを設定する場合は、このオプションを選択します。このオプションを選択する場合は、[参照 (Browse)] をクリックして、クライアント ブラウザを実行しているシステムから新しい sdopts.rec ファイルを選択する必要があります。

ステップ 6 [OK] をクリックします。

ステップ 7 Cisco ISE サーバに対応する行をクリックして、そのサーバの securid および sdstatus.12 ファイルをリセットします。

- a) ドロップダウン矢印をクリックし、[securid ファイルのリセット (Reset securid File)] 列と [sdstatus.12 ファイルのリセット (Reset sdstatus.12 File)] 列の [送信で削除 (Remove on Submit)] を選択します。

(注) [sdstatus.12 ファイルのリセット (Reset sdstatus.12 File)] フィールドはユーザのビューから非表示になっています。このフィールドを表示するには、最も内側のフレームで垂直および水平スクロールバーを使用して、下にスクロールし、次に右にスクロールします。

- b) この行で [保存 (Save)] をクリックして変更を保存します。

ステップ 8 [保存 (Save)] をクリックします。

RSA ID ソースの認証制御オプションの設定

Cisco ISE がどのように認証失敗を定義し、ID キャッシングを有効にするかを指定できます。RSA ID ソースでは、「認証失敗」エラーと「ユーザが見つからない」エラーは区別されず、Access-Reject 応答が送信されます。

Cisco ISE で、要求の処理および失敗のレポート中に、これらの失敗をどのように処理するかを定義できます。ID キャッシングによって、Cisco ISE では、Cisco ISE サーバに対して認証に失敗した要求を 2 回目に処理できます。前の認証から取得された結果および属性を、キャッシュで利用できます。

ステップ 1 [管理 (Administration)] > [ID の管理 (Identity Management)] > [外部 ID ソース (External Identity Sources)] > [RSA SecurID] > [追加 (Add)] を選択します。

ステップ 2 [認証制御 (Authentication Control)] タブをクリックします。

ステップ 3 次のいずれかを実行します。

- [拒否を「認証失敗」として処理 (Treat Rejects as "authentication failed")] : 拒否された要求を認証失敗として処理する場合は、このオプションを選択します。
- [拒否を「ユーザが見つからない」として処理 (Treat Rejects as "user not found")] : 拒否された要求をユーザが見つからないエラーとして処理する場合は、このオプションを選択します。

ステップ 4 最初に認証が成功した後に Cisco ISE がキャッシュにパスコードを保存し、設定された期間内に認証が行われた場合にキャッシュされたユーザクレデンシャルを後続の認証のために使用するようにする場合は、[パスコード キャッシュの有効化 (Enable Passcode Caching)] チェック ボックスにマークを付けます。

パスコードをキャッシュ内に保存する必要がある秒数を [エージング タイム (Aging Time)] フィールドに入力します。この期間内にユーザは同じパスコードで複数回の認証を行うことができます。デフォルト値は 30 秒です。有効な範囲は 1 ~ 300 秒です。

(注) Cisco ISE は、認証が初めて失敗した後でキャッシュをクリアします。ユーザは新しい有効なパスコードを入力する必要があります。

(注) EAP-FAST-GTC などの、パスコードの暗号化をサポートするプロトコルを使用する場合にのみこのオプションを有効にすることを強く推奨します。

ステップ 5 [保存 (Save)] をクリックして、設定を保存します。

RSA プロンプトの設定

Cisco ISE では、RSA SecurID サーバに送信される要求の処理中にユーザに表示される RSA プロンプトを設定できます。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 [管理 (Administration)] > [ID の管理 (Identity Management)] > [外部 ID ソース (External Identity Sources)] > [RSA SecurID] を選択します。

ステップ 2 [プロンプト (Prompts)] をクリックします。

ステップ 3 「RSA SecurID ID ソースの設定」の説明に従って、値を入力します。

ステップ 4 [送信 (Submit)] をクリックします。

RSA メッセージの設定

Cisco ISE では、RSA SecurID サーバに送信される要求の処理中にユーザに表示されるメッセージを設定できます。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 [管理 (Administration)] > [ID の管理 (Identity Management)] > [外部 ID ソース (External Identity Sources)] > [RSA SecurID] を選択します。

ステップ 2 [プロンプト (Prompts)] をクリックします。

ステップ 3 [メッセージ (Messages)] タブをクリックします。

ステップ 4 「RSA SecurID ID ソースの設定」の説明に従って、値を入力します。

ステップ 5 [送信 (Submit)] をクリックします。

外部 ID ソースとしての SAMLv2 ID プロバイダ

Security Assertion Markup Language (SAML) は XML ベースのオープン規格のデータ形式であり、いずれかのアプリケーションにサインインした後に、管理者は定義された一連のアプリケーションにシームレスにアクセスできます。SAML では、信頼できるビジネス パートナー間で、セキュリティに関連した情報交換を記述します。SAML により、ID プロバイダ (IdP) とサービスプロバイダー (この場合は ISE) の間で、セキュリティ認証情報を交換できます。

SAML シングルサインオン (SSO) は、IdP とサービスプロバイダーの間のプロビジョニングプロセスの一部として、メタデータと証明書を交換することで信頼の輪 (CoT) を確立します。サービスプロバイダは IdP のユーザ情報を信頼して、さまざまなサービスやアプリケーションにアクセスできるようにします。

SAML SSO を有効にすると、次のようないくつかの利点が得られます。

- 異なるユーザ名とパスワードの組み合わせを入力する必要がなくなるため、パスワードの劣化が軽減します。
- 同じ ID に資格情報を再入力する時間が省けるため、生産性が向上します。
- アプリケーションをホストしているお使いのシステムからサードパーティのシステムに、認証を転送します。
- 認証情報を保護し、安全に保ちます。暗号化機能により、IdP、サービスプロバイダ、ユーザの間で認証情報を保護します。SAML SSO では、IdP とサービスプロバイダー間で転送される認証メッセージを外部ユーザから保護することもできます。
- パスワードをリセットするためのヘルプデスクへの問い合わせが減るため、コスト削減につながります。

IdP は、ユーザ、システム、またはサービスの ID 情報を作成、維持、管理する認証モジュールです。IdP は、ユーザクレデンシャルを保管、検証し、ユーザがサービスプロバイダーの保護リソースにアクセスできる SAML 応答を生成します。



- (注) IdP サービスをよく理解している必要があります。現在インストールされていて、操作可能であることを確認してください。

SAML SSO は次のポータルでサポートされます。

- ゲスト ポータル (スポンサー付きおよびアカウント登録)
- スポンサー ポータル
- デバイス ポータル
- 証明書プロビジョニング ポータル

BYOD ポータルでは外部 ID ソースとして IdP を選択できませんが、ゲスト ポータルでは IdP を選択し、BYOD フローをイネーブルにできます。

Cisco ISE は SAMLv2 に準拠しており、Base64 でエンコードされた証明書を使用するすべての SAMLv2 準拠 IdP をサポートしています。次に示す IdP が Cisco ISE でテストされました。

- Oracle Access Manager (OAM)
- Oracle Identity Federation (OIF)
- SecureAuth
- PingOne
- PingFederate
- Azure Active Directory

IdP は、ID ソース順序に追加できません ([ID ソース順序 \(517 ページ\)](#) を参照)。

指定された時間 (デフォルトでは5分) にアクティビティがない場合は、SSOセッションが終了し、セッションタイムアウトのエラーメッセージが表示されます。

ポータルの [エラー (Error)] ページに [再度サインオン (Sign On Again)] ボタンを追加する場合は、[ポータルエラー (Portal Error)] ページの [オプションコンテンツ (Optional Content)] フィールドに次の JavaScript を追加します。

```
<button class="cisco-ise" data-inline="true" data-mini="true" data-theme="b"
id="ui_aup_accept_button" onclick="location.href='PortalSetup.action?portal=<Portal ID>'
type="button">SignOn Again</button>
```

SAML ID プロバイダーの追加

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

-
- ステップ 1** 証明書が IdP で自己署名されていない場合は、信頼できる証明書ストアに認証局 (CA) 証明書をインポートします。[管理 (Administration)] > [システム (System)] > [証明書 (Certificates)] > [信頼できる証明書 (Trusted Certificates)] > [インポート (Import)] の順に選択し、CA 証明書をインポートします。
 - ステップ 2** [管理 (Administration)] > [ID の管理 (Identity Management)] > [外部 ID ソース (External Identity Sources)] [[ワーク センター (Work Centers)] > [ネットワーク アクセス (Network Access)] > [外部 ID ソース (External Identity Sources)] を選択します。
 - ステップ 3** [SAML ID プロバイダー (SAML Id Providers)] をクリックします。
 - ステップ 4** [追加 (Add)] をクリックします。
 - ステップ 5** [SAML ID プロバイダー (SAML Identity Provider)] ページで、次の詳細情報を入力します。
 - ステップ 6** [送信 (Submit)] をクリックします。

ステップ 7 [ポータル設定 (Portal Settings)] ページ (ゲスト ポータル、証明書プロビジョニングまたはデバイス ポータル) に移動して、[認証方式 (Authentication Method)] フィールドでそのポータルにリンクする IdP を選択します。

[ポータル設定 (Portal Settings)] ページにアクセスするには、次の手順を実行します。

- ゲスト ポータル : [ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals and Components)] > [ゲスト ポータル (Guest Portals)] > [作成、編集または複製 (Create, Edit, or Duplicate)] > [ポータルの動作およびフローの設定 (Portal Behavior and Flow Settings)] > [ポータル設定 (Portal Settings)] の順に選択します ([クレデンシャルを持つゲスト ポータルのポータル設定 \(1296 ページ\)](#) を参照)。
- スポンサー ポータル : [ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals and Components)] > [スポンサー ポータル (Sponsor Portals)] > [作成、編集または複製 (Create, Edit, or Duplicate)] > [ポータルの動作およびフローの設定 (Portal Behavior and Flow Settings)] > [ポータル設定 (Portal Settings)] の順に選択します ([スポンサー ポータルのポータル設定 \(1314 ページ\)](#) を参照)。
- デバイス ポータル : [ワーク センター (Work Centers)] > [BYOD] > [設定 (Configure)] > [デバイス ポータル (My Devices Portals)] > [作成、編集または複製 (Create, Edit, or Duplicate)] > [ポータルの動作およびフローの設定 (Portal Behavior and Flow Settings)] > [ポータル設定 (Portal Settings)] [管理 (Administration)] > [デバイス ポータル管理 (Device Portal Management)] > [デバイス (My Devices)] > [作成、編集または複製 (Create, Edit, or Duplicate)] > [ポータルの動作およびフローの設定 (Portal Behavior and Flow Settings)] > [ポータル設定 (Portal Settings)] を選択します ([デバイス ポータルのポータル設定 \(1278 ページ\)](#) を参照)。
- 証明書プロビジョニングポータル : [管理 (Administration)] > [デバイス ポータル管理 (Device Portal Management)] > [証明書プロビジョニング (Certificate Provisioning)] > [作成、編集または複製 (Create, Edit, or Duplicate)] > [ポータルの動作およびフローの設定 (Portal Behavior and Flow Settings)] > [ポータル設定 (Portal Settings)] の順に選択します ([証明書プロビジョニング ポータルのポータル設定 \(1270 ページ\)](#) を参照)。

ステップ 8 [保存 (Save)] をクリックします。

ステップ 9 [管理 (Administration)] > [ID の管理 (Identity Management)] > [外部 ID ソース (External Identity Sources)] > [SAML ID プロバイダー (SAML Id Providers)] [ワーク センター (Work Centers)] > [ネットワーク アクセス (Network Access)] > [外部 ID ソース (External Identity Sources)] > [SAML ID プロバイダー (SAML Id Providers)] を選択します。そのポータルにリンクする IdP を選択し、[編集 (Edit)] をクリックします。

ステップ 10 (オプション) [サービス プロバイダー情報 (Service Provider Info)] タブで、ロード バランサの詳細を追加します。ISE ノードの前にロード バランサを追加することで、ID プロバイダーの設定を簡素化し、ISE ノードの負荷を最適化できます。

ロード バランサはソフトウェアベースまたはハードウェアベースのアプライアンスである可能性があります。導入の ISE ノードに要求を転送できる必要があります ([ポータル設定 (Portal Settings)] ページで指定されたポートを使用して)。

ロード バランサを使用する場合は、ロード バランサの URL のみがサービス プロバイダーのメタデータ ファイルで提供されます。ロード バランサが追加されていない場合は、複数の AssertionConsumerService URL がサービス プロバイダーのメタデータ ファイルに含まれます。

(注) ポータル FQND 設定でロード バランサに同じ IP アドレスを使用しないようにすることが推奨されます。

ステップ 11 [サービスプロバイダー情報 (Service Provider Info)] タブで、[エクスポート (Export)] をクリックして、サービス プロバイダーのメタデータ ファイルをエクスポートします。

エクスポートされたメタデータには、Cisco ISE の署名証明書が含まれています。署名証明書は、選択したポータルの証明書と同一です。

エクスポートされたメタデータの ZIP ファイルには、各 IdP の設定に関する基本的な説明を含む Readme ファイルが含まれています (Azure Active Directory、PingOne、PingFederate、SecureAuth、OAM など)。

(注) ロード バランサが設定されていない、または次のようなポータル設定に変更がある場合は、サービス プロバイダーのメタデータを再度エクスポートする必要があります。

- 新しい ISE ノードが登録された場合
- ノードのホスト名または IP アドレスが変更された場合
- デバイス、スポンサー、または証明書プロビジョニング ポータルの完全修飾ドメイン名 (FQDN) が変わりました
- ポートまたはインターフェイス設定が変更された

更新されたメタデータが再エクスポートされない場合、ユーザ認証が IdP 側で失敗する可能性があります。

ステップ 12 ダイアログボックスで [参照 (Browse)] をクリックして、圧縮ファイルをローカルに保存します。メタデータ ファイルのフォルダを解凍します。フォルダを解凍すると、ポータルの名前が付いたメタデータ ファイルを取得します。メタデータ ファイルには、プロバイダー ID とバインディング URI が含まれています。

ステップ 13 管理ユーザとして IdP にログインし、サービス プロバイダーのメタデータ ファイルをインポートします。サービス プロバイダーのメタデータ ファイルをインポートする方法の詳細については、ID プロバイダーのメタデータ ファイルをインポートする方法の詳細については、ID プロバイダーのユーザユーザ マニュアルを参照してください。

ステップ 14 [グループ (Groups)] タブで、必要なユーザ グループを追加します。

[グループ メンバーシップ属性 (Group Membership Attribute)] フィールドにユーザのグループ メンバーシップを指定するアサーション属性を入力します。

ステップ 15 [属性 (Attributes)] タブにユーザ属性を追加します。属性を追加するときに、属性が IdP から返されたアサーションでどのように表示されるかを指定できます。[ISE の名前 (Name in ISE)] フィールドに指定した名前はポリシー ルールに表示されます。属性でサポートされているのは、次のデータ型です。

- 文字列
- 整数 (Integer)

- IPv4
- ブール値

(注) グループと属性の追加は必須ではありません。これらのグループと属性は、ポリシーとルールの設定に使用できます。スポンサー ポータルを使用している場合は、グループを追加してこれらのグループを選択し、スポンサー グループの設定を構成することができます。

ステップ 16 [詳細設定 (Advanced Settings)] タブで、次のオプションを設定します。

- [ID属性 (Identity Attribute)] : 認証中のユーザの ID を指定する属性を選択します。[属性 (Attribute)] ドロップダウン リストからサブジェクト名属性または属性を選択できます。

(注) サブジェクト名が永続的ではない (一時サブジェクト名) 場合、認証は失敗します。

- [メール属性 (Email attribute)] : スポンサーの電子メール アドレスを含む属性を選択します。これには、セルフサービスのゲストの要求とスポンサーが一致する必要があります。
- 複数値属性の場合は、次のいずれかのオプションを選択します。
 - [個別のXML要素で各値 (Each value in a separate XML element)] : 個別の XML 要素で同じ属性の複数の値を IdP が返すには、このオプションをクリックします。
 - [単一のXML要素で複数の値 (Multiple values in a single XML element)] : 単一の XML 要素で複数を IdP が返すには、このオプションをクリックします。テキスト ボックスにデリミタを指定できます。

- ログアウト設定 (Logout Settings)

- [ログアウト要求の署名 (Sign Logout Requests)] : ログアウト要求に署名されるようにする場合は、このチェックボックスをオンにします。このオプションは、OAMおよびOIFでは表示されません。

(注) SecureAuth は SAML ログアウトをサポートしていません。

- [ログアウト URL (Logout URL)] : ロード バランサが設定されていなければ、このオプションは OAM および OIF だけに表示されます。ユーザがスポンサー ポータルまたはデバイス ポータルからログアウトすると、ユーザは SSO セッションを終了するために IdP でログアウト URL にリダイレクトされ、その後、ログイン ページにリダイレクトされます。
- [リダイレクトパラメータ名 (Redirect Parameter Name)] : ロード バランサが設定されていなければ、このオプションは OAM および OIF だけに表示されます。リダイレクトパラメータは、ユーザがログアウト後にリダイレクトされる必要があるログインページの URL を渡すために使用されます。リダイレクトパラメータ名は、IdP に基づいて異なる場合があります (たとえば `end_url` や `returnURL`)。このフィールドは大文字と小文字が区別されます。

ログアウトが正常に動作しない場合は、ログアウト URL およびリダイレクトパラメータ名について、ID プロバイダーのマニュアルを確認してください。マニュアルを確認してください。

ステップ 17 [送信 (Submit)] をクリックします。

例

Ping Federate の設定の例については、『[Configure ISE 2.1 Guest Portal with PingFederate SAML SSO](#)』を参照してください。

ID プロバイダの削除

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

削除する IdP がいずれのポータルにもリンクされていないことを確認します。IdP がポータルにリンクされている場合、削除操作は失敗します。

ステップ 1 [管理 (Administration)] > [ID の管理 (Identity Management)] > [外部 ID ソース (External Identity Sources)] > [SAML ID プロバイダー (SAML Id Providers)] [ワーク センター (Work Centers)] > [ネットワーク アクセス (Network Access)] > [外部 ID ソース (External Identity Sources)] > [SAML ID プロバイダー (SAML Id Providers)] を選択します。

ステップ 2 削除する IdP の隣のチェックボックスをオンにして、[削除 (Delete)] をクリックします。

ステップ 3 [OK] をクリックして、選択した IdP を削除します。

認証失敗ログ

SAML ID ストアに対する認証が失敗し、IdP がユーザを ISE ポータルに (SAML 応答を通じて) リダイレクトすると、ISE は認証ログに障害の理由を報告します。ゲスト ポータルで (BYOD フローの有効無効に関係なく)、認証の失敗の原因を知るために、RADIUS Livelog ([操作 (Operations)] > [RADIUS] > [ライブ ログ (Live Logs)]) を確認できます。ポータルおよびスポンサー ポータル認証失敗の原因を把握するためには、デバイス ポータルおよびスポンサー ポータルで、デバイス ログイン/監査レポートとスポンサー ログイン/監査レポート ([操作 (Operations)] > [レポート (Reports)] > [ゲスト (Guest)]) を確認できます。

ログアウトで障害が発生した場合、My Devices、スポンサーおよびゲストポータルの障害の原因を知るためにレポートおよびログを確認することができます。

認証が失敗する原因には次のものが考えられます。

- SAML 応答の解析エラー
- SAML 応答の検証エラー (不正な発行者など)
- SAML アサーションの検証エラー (誤った対象者など)

- SAML 応答署名の検証エラー（不正な署名など）
- IdP 署名証明書のエラー（失効した証明書など）

認証に失敗した場合は、認証ログの「DetailedInfo」属性を確認することを推奨します。この属性では、障害理由に関する追加情報が提供されます。

ID ソース順序

ID ソース順序は、Cisco ISE がそれぞれ異なるデータベース内でユーザ クレデンシャルを検索する順序を定義します。Cisco ISE では次の ID ソースがサポートされます。

- 内部ユーザ
- ゲスト ユーザ
- Active Directory
- LDAP
- RSA
- RADIUS トークン サーバ
- 証明書認証プロファイル

Cisco ISE に接続されている 2 つ以上のデータベースにユーザ情報がある場合、Cisco ISE でこれらの ID ソース内の情報を検索する順序を定義できます。一致が見つかり、Cisco ISE はそれ以上の検索を行いませんが、クレデンシャルを評価し、ユーザに結果を返します。このポリシーは最初の一一致ポリシーです。

ID ソース順序の作成

始める前に

Cisco ISE に外部 ID ソースを設定していることを確認します。

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ゲスト ユーザがローカル WebAuth を使用して認証できるようにするには、ゲスト ポータル認証ソースと ID ソース順序に同じ ID ストアが含まれるように設定する必要があります。

ステップ 1 [管理 (Administration)] > [ID の管理 (Identity Management)] > [ID ソース順序 (Identity Source Sequences)] > [追加 (Add)] を選択します。

ステップ 2 ID ソース順序の名前を入力します。また、任意で説明を入力できます。

ステップ 3 [証明書認証プロファイル (Certificate Authentication Profile)] チェックボックスをオンにし、証明書ベースの認証のための証明書認証プロファイルを選択します。

ステップ 4 [選択済み (Selected)] リスト ボックスの ID ソース順序に含めるデータベースを選択します。

ステップ 5 Cisco ISE がデータベースを検索する順序に [選択済み (Selected)] リストのデータベースを並べ替えます。

ステップ 6 [高度な検索リスト (Advanced Search List)] 領域で、次のいずれかのオプションを選択します。

- [順序内の他のストアにアクセスせず、AuthenticationStatus 属性を ProcessError に設定 (Do not access other stores in the sequence and set the AuthenticationStatus attribute to ProcessError)] : 最初に選択された ID ソースでユーザが見つからないとき、Cisco ISE が検索を中止する場合。
- [ユーザが見つからなかったとして処理し、順序内の次のストアに進む (Treat as if the user was not found and proceed to the next store in the sequence)] : 最初に選択された ID ソースでユーザが見つからないとき、Cisco ISE が順序内の他の選択された ID ソースの検索を続行する場合。

Cisco ISE では、要求の処理中にこれらの ID ソースが順番に検索されます。[選択済み (Selected)] リストに、Cisco ISE が ID ソースを検索する順序で ID ソースが表示されていることを確認します。

ステップ 7 [送信 (Submit)] をクリックして ID ソース順序を作成すると、その後この ID ソース順序をポリシーで使用できます。

ID ソース順序の削除

ポリシーで今後使用しない ID ソース順序を削除できます。

始める前に

- 削除する ID ソース順序がいずれの認証ポリシーでも使用されていないことを確認してください。
- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 [管理 (Administration)] > [ID の管理 (Identity Management)] > [ID ソース順序 (Identity Source Sequences)] を選択します。

ステップ 2 削除する ID ソース順序の隣にあるチェックボックスをオンにし、[削除 (Delete)] をクリックします。

ステップ 3 [OK] をクリックして ID ソース順序を削除します。

レポートでの ID ソースの詳細

Cisco ISE は認証ダッシュレットおよび ID ソース レポートで ID ソースに関する情報を提供します。

[認証 (Authentications)] ダッシュレット

[認証 (Authentications)] ダッシュレットから、障害の理由などの詳細情報にドリルダウンできます。

[操作 (Operations)] > [RADIUS ライブログ (RADIUS LiveLog)] の順に選択して、リアルタイムで認証の概要を表示します。RADIUS ライブ ログの詳細については、[RADIUS ライブ ログ \(1451 ページ\)](#) を参照してください。

図 36: RADIUS ライブ ログ

Time	Status	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy
Aug 30, 2015 07:31:28.134 ...	✓			utente_3671839	00:00:01:42:45:58			Default
Aug 30, 2015 07:31:28.134 ...	✓			ユーザが_3324527	00:00:06:95:19:19			Default
Aug 30, 2015 07:31:28.134 ...	✓			사용자_3477996	00:00:07:24:56:11			Default
Aug 30, 2015 07:31:28.134 ...	✓			user_112043	00:00:09:90:33:85			Default
Aug 30, 2015 07:31:28.134 ...	✓			usuário_5642394	00:00:03:30:02:26			Default
Aug 30, 2015 07:31:28.134 ...	✓			пользователь_7569692	00:00:01:13:62:36			Default
Aug 30, 2015 07:31:28.134 ...	✓			usuario_3181739	00:00:07:19:75:11			Default
Aug 30, 2015 07:31:28.134 ...	✗			ユーザが_1943238	00:00:29:78:57:25			
Aug 30, 2015 07:31:28.134 ...	✗			사용자_7062289	00:00:29:78:57:25			
Aug 30, 2015 07:31:28.134 ...	✗			user_8498049	00:00:29:78:57:25			
Aug 30, 2015 07:31:28.134 ...	✓			user_4251097	00:00:00:06:38:51			Q LAN

ID ソース レポート

Cisco ISE は ID ソースに関する情報を含むさまざまなレポートを提供します。これらのレポートの詳細については、「使用可能なレポート」の項を参照してください。



第 16 章

ゲスト アクセスの設定

- [Cisco ISE ゲスト サービス \(521 ページ\)](#)
- [ゲスト アカウントとスポンサー アカウント \(522 ページ\)](#)
- [ゲスト ポータル \(538 ページ\)](#)
- [スポンサー ポータル \(556 ページ\)](#)
- [ゲストとスポンサーのアクティビティのモニタ \(572 ページ\)](#)
- [ゲスト アクセス Web 認証オプション \(574 ページ\)](#)

Cisco ISE ゲスト サービス

Cisco Identity Services Engine (ISE) ゲストサービスを使用すると、ビジター、請負業者、コンサルタント、顧客などのゲストにセキュアなネットワーク アクセスを提供することができます。Cisco ISE の Base ライセンスを持つゲストをサポートでき、会社のインフラストラクチャと機能の要件に応じて複数の展開オプションから選択できます。

Cisco ISE は、企業のネットワークおよび内部リソースとサービスへのゲストおよび従業員のオンボーディングを行う Web ベースのモバイル ポータルを提供します。

管理者ポータルで、ゲスト ポータルおよびスポンサー ポータルの作成と編集、ゲスト タイプの定義によるゲストアクセス権限の設定、ゲストアカウントの作成と管理のためのスポンサー権限の割り当てを行うことができます。

- [ゲスト ポータル \(538 ページ\)](#)
- [ゲスト タイプおよびユーザ ID グループ \(523 ページ\)](#)
- [スポンサー ポータル \(556 ページ\)](#)
- [スポンサー グループ \(559 ページ\)](#)

ISE コミュニティ リソース

ISE ゲストおよび Web 認証に関する ISE コミュニティ リソースのリストについては、「[ISE Guest Access - ISE Guest and Web Authentication](#)」を参照してください。

分散環境のエンドユーザのゲスト ポータルとスポンサー ポータル

Cisco ISE のエンドユーザ Web ポータルは、管理ペルソナ、ポリシー サービス ペルソナ、およびモニタリング ペルソナに基づき、設定、セッション サポート、およびレポート作成を提供します。

- **管理ノード**：ユーザ、デバイス、およびエンドユーザ ポータルが管理ノードに書き込まれる構成の変更。
- **ポリシー サービス ノード**：エンドユーザ ポータルはポリシー サービス ノードで実行する必要があります。ここでは、ネットワーク アクセス、クライアント プロビジョニング、ゲスト サービス、ポスチャ、およびプロファイリングを含むすべてのセッション トラフィックが処理されます。ポリシー サービス ノードがノード グループに含まれる場合、1 つのノードで障害が発生すると、他のノードが障害を検出し、保留中のセッションをリセットします。
- **モニタリング ノード**：モニタリング ノードは、デバイス ポータル、スポンサー ポータル、およびゲスト ポータルでのエンドユーザおよびデバイスのアクティビティについて、データを収集、集約、およびレポートします。プライマリ モニタリング ノードで障害が発生した場合は、セカンダリ モニタリング ノードが自動的にプライマリ モニタリング ノードになります。

ゲスト アカウントとスポンサー アカウント

- **ゲストアカウント**：ゲストとは、通常、ネットワークへの一時アクセスを必要とする承認ユーザ、担当者、顧客、その他のユーザを表します。いずれかのゲスト展開シナリオを使用して、従業員のネットワーク アクセスを許可する場合は、従業員用のゲスト アカウントを使用することもできます。スポンサー ポータルにアクセスして、スポンサーおよびアカウント登録ゲストによって作成されたゲスト アカウントを表示できます。
- **スポンサー アカウント**：スポンサー ポータルを使用して、承認ユーザ用の一時アカウントを作成し、企業ネットワークまたはインターネットにセキュアにアクセスできるようにします。ゲスト アカウントを作成した後、スポンサー ポータルを使用してそれらのアカウントを管理し、ゲストにアカウントの詳細を提供できます。

次のユーザがゲスト アカウントを作成できます。

- **スポンサー**：管理者ポータルで、ゲスト アカウントを作成し管理するスポンサー ポータルにアクセスできる、スポンサーのアクセス権限と機能のサポートを定義できます。
- **ゲスト**：ゲストは、アカウント登録ゲストポータルに自分自身を登録することによって、独自のアカウントを作成することもできます。これらのアカウント登録ゲストは、ポータル設定に基づいて、ログインクレデンシャルを受け取る前にスポンサーの承認が必要になる場合があります。

ゲストは、ホットスポット ゲスト ポータルを使用してネットワークにアクセスすることもできます。このポータルでは、ゲストアカウントやユーザ名およびパスワードなどのログイン クレデンシャルを作成する必要はありません。

- **従業員** : ID ストア (Active Directory、LDAP、内部ユーザなど) に含まれている従業員は、クレデンシャルを持つゲスト ポータル (Sponsored-Guest ポータルおよびアカウント登録ゲストポータル) が設定されている場合には、これを使用してアクセスすることもできます。

ゲスト アカウントが作成されると、ゲストは Sponsored-Guest ポータルを使用してネットワークにログインおよびアクセスできます。

ゲスト タイプおよびユーザ ID グループ

各ゲストアカウントをゲストタイプに関連付ける必要があります。ゲストタイプを使用して、スポンサーは、ゲストアカウントに対して、さまざまなレベルのアクセス権や、さまざまなネットワーク接続時間を割り当てることができます。これらのゲストタイプは、特定のネットワーク アクセス ポリシーに関連付けられます。Cisco ISE には、次のデフォルト ゲスト タイプが含まれます。

- **担当者** : 長い期間 (最大 1 年)、ネットワークへのアクセスを必要とするユーザ。
- **日次** : 1 ~ 5 日間の短期間に、ネットワーク リソースへのアクセスを必要とするゲスト。
- **週次** : 2 ~ 3 週間の間、ネットワークへのアクセスを必要とするユーザ。

ゲスト アカウントを作成する場合、特定のスポンサー グループを特定のゲスト タイプを使用するように制限することができます。このようなグループのメンバーは、そのゲストタイプに指定された機能のみを持つゲストを作成できます。たとえば、スポンサー グループ ALL_ACCOUNTS は担当者ゲスト タイプのみを使用するように設定でき、スポンサー グループ OWN_ACCOUNTS および GROUP_ACCOUNTS は日次または週次ゲスト タイプを使用するように設定できます。また、通常、アカウント登録ゲストポータルを使用するアカウント登録ゲストは、1 日のみのアクセスを必要とするため、これらのゲストには日次ゲストタイプを割り当てることができます。

ゲスト タイプは、ゲストのユーザ ID グループを定義します。

詳細については、以下を参照してください。

- [ユーザ ID グループ \(362 ページ\)](#)
- [ユーザ ID グループの作成 \(369 ページ\)](#)

ゲスト タイプの作成または編集

新しいゲスト タイプの作成に加えて、デフォルトのゲスト タイプのデフォルトのアクセス権限および設定を編集できます。ユーザが行った変更は、このゲストタイプを使用して作成された既存のゲスト アカウントに適用されます。ログインしているゲスト ユーザは、ログアウト

して再度ログインするまで、これらの変更を確認できません。また、ゲスト タイプを複製して、同じアクセス権限を持つ追加のゲスト タイプを作成できます。

各ゲスト タイプに名前、説明、およびこのゲスト タイプでゲスト アカウントを作成できるスポンサー グループのリストがあります。ゲスト タイプに対して、アカウント登録ゲストにのみ使用すること、（任意のスポンサー グループによる）ゲスト アカウントの作成には使用しないこと、などを指定できます。

次のフィールドを入力します。

- **[ゲストタイプ名 (Guest type name)]** : このゲスト タイプを他のゲスト タイプと区別する名前（1 ～ 256 文字）を指定します。
- **[説明 (Description)]** : このゲスト タイプの推奨される使用方法に関する追加情報（最大 2000 文字）を指定します。たとえば、アカウント登録ゲスト用。ゲスト アカウントの作成に使用しない、など。
- **[言語ファイル (Language File)]** : このフィールドでは、サポート対象のすべての言語で、電子メールの件名、電子メール メッセージ、および SMS メッセージの内容を含む言語ファイルをエクスポートおよびインポートできます。これらの言語とコンテンツは、アカウントが期限切れになった旨の通知に使用され、このゲスト タイプに割り当てられているゲストに送信されます。新しいゲスト タイプを作成すると、ゲスト タイプを保存するまではこの機能は無効です。言語ファイルの編集の詳細については、[ポータル言語のカスタマイズ \(648 ページ\)](#) を参照してください。
- **[追加データを収集 (Collect Additional Data)]** : **[カスタムフィールド... (Custom Fields...)]** ボタンをクリックして、このゲスト タイプを使用しているゲストから追加データを収集するために使用するカスタム フィールドを選択します。

カスタム フィールドを管理するには、**[ワークセンター (Work Centers)]** > **[ゲストアクセス (Guest Access)]** > **[設定 (Settings)]** > **[カスタムフィールド (Custom Fields)]** を選択します。

• 最大アクセス時間 (Maximum Access Time)

- **[アカウント期間の開始 (Account duration starts)]** : **[最初のログインから (From first login)]** を選択した場合、アカウントの開始時間は、ゲストユーザがゲストポータルに最初にログインしたときに開始され、終了時間は指定された期間に相当します。ゲストユーザがログインしなければ、アカウントがゲスト アカウント消去ポリシーによって削除されるまで、アカウントは *Awaiting first login* 状態のままになります。

値は、1 から 999 日、時間、または分です。

アカウント登録ユーザのアカウントは、ユーザがアカウントを作成し、自分のアカウントにログインしたときに開始されます。

[スポンサーが指定した日付から (From sponsor-specified date)] を選択した場合は、このゲスト タイプのゲストがネットワークにアクセスして接続を保持できる最大日数、時間数、または分数を入力します。

この設定を変更した場合、変更内容はこのゲスト タイプを使用して作成された既存のゲスト アカウントには適用されません。

- [最大アカウント期間 (Maximum account duration)] : このゲスト タイプが割り当てられているゲストがログインできる期間 (日数、時間数、または分数) を入力します。

(注) アカウント消去ポリシーにより期限切れのゲストアカウントが確認され、期限切れ通知が送信されます。このポリシーは 20 分ごとに実行されるため、アカウント期間を 20 分未満に設定すると、アカウントの消去前に期限切れ通知が送信されることがあります。

[アクセスを許可する日付と時刻 (Allow access only on these days and times)] オプションを使用して、このゲスト タイプのゲストにアクセスを提供する期間や曜日を指定できます。

- 選択した曜日によって、スポンサーのカレンダーで選択できる日付へのアクセスが制限されます。
- スポンサーが期間と日付を選択すると、スポンサー ポータルで最大アカウント期間が適用されます。

ここで設定するアクセス時刻の設定は、ゲストアカウントの作成時にスポンサー ポータルで使用できる時刻設定に影響します。詳細については、[スポンサーに対して使用可能な時間設定項目の設定 \(570 ページ\)](#) を参照してください。

• ログイン オプション

- [最大同時ログイン数 (Maximum simultaneous logins)] : このゲスト タイプに割り当てられたユーザが同時に実行できる最大ユーザセッション数を入力します。
- [ゲストが制限を超えた場合 (When guest exceeds limit)] : [最大同時ログイン数 (Maximum simultaneous logins)] を選択した場合は、その最大ログイン数に到達した後でユーザが接続したときに実行するアクションも選択する必要があります。

• 最も古い接続を切断 (Disconnect the oldest connection)

- [最も新しい接続を切断 (Disconnect the newest connection)] : [エラーメッセージを示すポータルページにユーザをリダイレクトする (Redirect user to a portal page showing an error message)] をオプションで選択 : 特定の時間にわたってエラー メッセージが表示され、その後セッションが切断されてユーザがゲストポータルにリダイレクトされます。エラーメッセージが表示される時間は設定可能です。エラー ページの内容は、[メッセージ (Messages)] > [エラーメッセージ (Error Messages)] ページの [ポータルページのカスタマイズ (Portal Page Customization)] ダイアログで設定します。

- [ゲストが登録できるデバイスの最大数 (Maximum devices guests can register)] : 各ゲストに登録できるデバイスの最大数を入力します。そのゲスト タイプのゲストに登録済みの値より小さい値を最大数として設定できます。この値は、新しく作成されたゲストアカウントにのみ適用されます。
- [ゲストデバイス登録のためのエンドポイントIDグループ (Endpoint identity group for guest device registration)] : ゲストのデバイスに割り当てるエンドポイント ID グループを選択します。Cisco ISE はデフォルトとして使用する **GuestEndpoints** のエンドポイント ID グループを提供します。デフォルトを使用しない場合、追加のエンドポイント ID グループを作成することもできます。

- [ゲストに対しゲストポータルのバイパスを許可する (Allow guest to bypass the Guest portal)] : クレデンシアルを持つゲスト タイプのキャプティブ ポータル (Web 認証ページ) をバイパスし、有線およびワイヤレス (dot1x) サプリカントまたは VPN クライアントに認証情報を提供することでネットワークにアクセスすることをユーザに許可します。ゲスト アカウントは、AUP が必要な場合でも、[初期ログインを待機 (Awaiting Initial Login)] 状態と AUP ページをバイパスして [アクティブ (Active)] 状態になります。

この設定を有効にしない場合、ユーザは初めにクレデンシアルを持つゲストのキャプティブ ポータルを使用してログインしないと、ネットワークの他の部分にアクセスできません。

• アカウント有効期限通知

- [アカウント有効期限の __ 日前にアカウント有効期限通知を送信する (Send account expiration notification __ days before account expires)] : アカウントが期限切れになる前にゲストに通知を送信します。有効期限前の日数、時間数、または分数を指定します。
- [メッセージ表示原語 (View messages in)] : 電子メールまたは SMS 通知の表示言語を指定します。
- [電子メール (Email)] : アカウント有効期限通知を電子メールで送信します。
- [次のポータルのカスタマイズを使用する (Use customization from)] : 選択したポータルに対して設定した同一のカスタマイズ内容をこのゲスト タイプのアカウント有効期限メールに適用します。
- [テキストのコピー元 (Copy text from)] : 別のゲスト タイプのアカウント有効期限メールに、作成した電子メール テキストを再利用します。
- **テスト電子メールの送信先 (Send test email to me at)**
- [SMS] : アカウント有効期限通知を SMS で送信します。

SMS の設定は、電子メール通知の設定と同一ですが、[テスト SMS の送信 (Send test SMS to me)] の SMS ゲートウェイを選択する点が異なります。

- [スポンサーグループ (Sponsor Groups)] : このゲスト タイプを使用してメンバーがゲストアカウントを作成できるスポンサーグループを指定します。このゲスト タイプにアクセスできないようにするスポンサー グループは削除します。

次のタスク

- このゲスト タイプを使用するスポンサー グループを作成または変更します。詳細については、[スポンサー グループ \(559 ページ\)](#) を参照してください。
- 該当する場合は、アカウント登録ゲスト ポータルで、このゲスト タイプをアカウント登録ゲストに割り当てます。詳細については、[アカウント登録ゲストポータルの作成 \(549 ページ\)](#) を参照してください。

ゲスト タイプの無効化

ゲスト アカウントで使用されているゲスト タイプのうち、最後に残ったゲスト タイプは削除できません。使用されているゲスト タイプを削除するには、最初にそのゲスト タイプが使用できなくなることを確認します。ゲスト タイプをディセーブルにしても、そのゲスト タイプで作成したゲスト アカウントには影響しません。

次の手順で、ターゲット ゲスト タイプを準備および無効にする方法を説明します。

- ステップ 1** ターゲットゲストタイプを使用して、スポンサーがゲストを作成するのを許可しているスポンサーグループを識別します。[ワークセンター (Work Centers)] > [ゲストアクセス (Guest Access)] > [ポータルとコンポーネント (Portals and Components)] > [スポンサーグループ (Sponsor Groups)] を選択し、各スポンサーグループを開いて、[このスポンサーグループはこれらのゲストタイプを使用してアカウントを作成できません (This sponsor group can create accounts using these guest types)] リストを調べます。
- ステップ 2** ターゲット ゲスト タイプを割り当てるアカウント登録ポータルを識別します。[ワークセンター (Work Center)] > [ゲストアクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [ゲストポータル (Guest Portals)] を選択します。各アカウント登録ゲストポータルを開きます。ポータルが特定のゲストタイプを使用している場合、[ポータル設定 (Portal Settings)] を展開し、[ゲストとしてこのポータルを使用する従業員のログインオプションの継承元 (Employees using this portal as guests inherit login options from)] フィールドに割り当てられたゲストタイプを変更します。
- ステップ 3** 削除するゲストタイプを開き、前の手順で識別したすべてのスポンサーグループを削除します。この操作により、効果的に、すべてのスポンサーがこのゲストタイプの新しいゲストアカウントの作成を使用できなくします。[ワークセンター (Work Center)] > [ゲストアクセス (Guest Access)] > [ポータルとコンポーネント (Portals and Components)] > [ゲストタイプ (Guest Type)] を選択します。

これで完了です。実際にゲストタイプは削除できません。将来的にすべてのポータルで使用しないことを確認します。

ゲスト アカウント属性の変更

ゲスト アカウントが作成されると、属性はゲスト タイプによってそのアカウントに設定されます。

ゲスト タイプに変更を加えた場合、アクティブなゲスト アカウントは、デフォルトのアクセス時刻、日付、期間など、更新されたゲストタイプのすべての属性を引き受けます。それらは後で編集できます。さらに、元のゲストタイプからカスタムフィールドが更新されたゲストタイプにコピーされます。

スポンサーは、期限切れになる前にアカウント有効期間を延長することもできます。

エンドポイント ユーザの最大同時ログイン数の設定

ゲストに許可される同時ログインの最大数を設定できます。

ユーザがゲストポータルにログインし、正常に認証されると、ユーザがすでにログインの最大数に達しているかどうかを確認するために、ユーザの既存のログイン数がチェックされます。達していた場合、ゲストユーザはエラーページにリダイレクトされます。エラーページが表示され、セッションが停止します。そのユーザがインターネットに再度アクセスしようとする、ユーザの接続はゲストポータルのログインページにリダイレクトされます。

始める前に

このポータルの許可ポリシーで使用している許可プロファイルで [アクセス タイプ (Access Type)] が *Access_Accept* に設定されていることを確認します。[アクセスタイプ (Access Type)] が *Access_Reject* に設定されている場合は、最大同時ログイン数は機能しません。

ステップ 1 [ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [ゲスト タイプ (Guest Type)] の順に選択し、[ログイン オプション (Login Options)] の下で次の操作を実行します。

- a) [最大同時ログイン数 (Maximum simultaneous logins)] を有効にします。これは、デフォルトのゲストタイプですすでに有効になっています。
- b) [ゲストが制限を超えた場合 (When guest exceeds limit)] の下で、[最も新しい接続を切断 (Disconnect the newest connection)] を選択します。
- c) [エラーメッセージを示すポータルページにユーザをリダイレクトする (Redirect user to a portal page showing an error message)] を選択して、許可する同時ログインの最大数を選択します。

ステップ 2 [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] を選択して認証プロファイルを作成します。

- a) [共通タスク (Common Tasks)] で、[Webリダイレクション (Web Redirection)] をチェックし、次の操作を実行します。
 - 最初のドロップダウンで、[中央集中Web認証 (Centralized Web Auth)] を選択します。
 - 前提条件の一部として作成した **ACL** を入力します。
 - [値 (Value)] の場合、リダイレクト先のゲストポータルを選択します。
- b) [一般的なタスク (Common Tasks)] でスクロールダウンして、[再認証 (Reauthentication)] をチェックして、次を行います。
 - [タイマー (Timer)] に、ユーザがゲストポータルにリダイレクトされる前にエラーページが表示される時間を入力します。
 - [再認証中に接続を維持 (Maintain Connectivity During Reauthentication)] で、[デフォルト (Default)] を選択します。

ステップ 3 [ポリシー (Policy)] > [認証 (Authorization)] を選択して、属性 `NetworkAccess.SessionLimitExceeded` が `true` の場合にユーザがポータルにリダイレクトされるように、許可ポリシーを作成します。

次のタスク

[ポータルページのカスタマイズ (Portal Page Customization)] タブでエラー ページのテキストをカスタマイズするには、[メッセージ (Messages)] || [エラーメッセージ (ErrorMessages)] タブで、エラーメッセージキー `ui_max_login_sessions_exceeded_error` のテキストを変更します。

期限切れのゲスト アカウントを消去するスケジューリング設定

アクティブなまたは一時停止されたゲストアカウントがアカウント有効期間（スポンサーがアカウントを作成するときに定義）の終了に達すると、そのアカウントは失効します。ゲストアカウントが期限切れになった場合、影響を受けるゲストはネットワークにアクセスできません。スポンサーは、期限切れになったアカウントを、消去される前に延長することができます。ただし、アカウントが消去された場合、スポンサーは、新しいアカウントを作成する必要があります。

期限切れになったゲストアカウントが消去された場合、関連するエンドポイントおよびレポート情報とログイン情報は保持されます。

Cisco ISE は、デフォルトで 15 日ごとに期限切れになったゲストアカウントを自動的に消去します。[次回消去日 (Date of next purge)] は、次の消去の発生時期を示します。次のことも実行できます。

- X 日ごとに消去が行われるようにスケジュール設定します。最初の消去は X 日後の **消去の時刻**に行われ、その後消去は X 日ごとに行われます。
- X 週間ごとに特定の曜日に消去が行われるようにスケジュール設定します。最初の消去は次のその曜日の **消去の時刻**に行われ、その後消去は設定された週数おきにその曜日と時刻に行われます。たとえば、月曜日に、5 週間おきに木曜日に消去が行われるように設定したとします。次の消去は、今から 5 週間後の木曜日ではなく、その週の木曜日に行われます。
- [今すぐ消去 (Purge Now)] をクリックして、ただちに消去を行います。

消去が実行されるようにスケジュールされているときに Cisco ISE サーバがダウンした場合は、消去は行われません。消去プロセスは、サーバがその時点で動作していれば、次にスケジュールされている消去時刻に再度実行されます。

ステップ 1 [ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [設定 (Settings)] > [ゲスト アカウント消去ポリシー (Guest Account Purge Policy)] の順に選択します。

ステップ 2 次のオプションのいずれかを選択します。

- 期限切れのゲスト アカウント レコードを即時に消去するには、[今すぐ消去 (Purge Now)] をクリックします。
- 消去をスケジュールするには、[期限切れのゲスト アカウントの消去のスケジュール (Schedule purge of expired guest accounts)] をオンにします。

(注) 各消去の完了後に、[次回消去日 (Date of next purge)] が次にスケジュールされている消去に合わせてリセットされます。

- ステップ 3** LDAP および Active Directory ユーザ用に Cisco ISE データベースに保持されているユーザに固有のポータルレコードが、非アクティブの状態で何日経過すると消去されるかを指定します。
- ステップ 4** [経過後にポータル ユーザ情報を期限切れにする (Expire portal-user information after)] で、ユーザを期限切れにするための非アクティブ日数を指定します。この設定により、使用されていない LDAP および Active Directory アカウントが ISE データベースに無期限に残ることを防ぎます。
- ステップ 5** [保存 (Save)] をクリックします。設定の更新を保存しない場合は、[リセット (Reset)] をクリックして、最後に保存した値に戻します。

ゲスト アカウント作成用のカスタム フィールドの追加

ゲスト アクセスを提供する場合、名前、電子メールアドレス、電話番号以外の情報をゲストから収集する必要がある場合があります。Cisco ISE には、会社のニーズに固有の、ゲストに関する追加情報の収集に使用できるカスタム フィールドが用意されています。ゲスト タイプ およびアカウント登録ゲスト ポータルとスポンサー ポータルにカスタム フィールドを関連付けることができます。Cisco ISE はデフォルトのカスタム フィールドを提供しません。

- ステップ 1** すべてのゲスト ポータルとスポンサー ポータルのカスタム フィールドを追加、編集、または削除するには、[ゲスト アクセス (Guest Access)] > [設定 (Settings)] > [カスタム フィールド (Custom Fields)] を選択します。
- ステップ 2** [カスタム フィールド名 (Custom Field Name)] に入力し、ドロップダウンリストからデータ タイプを選択し、カスタム フィールドに関する追加情報を提供するのに役立つヒントテキストを入力します。たとえば、Date of Birth と入力し、[Date-MDY] を選択して、日付形式に関するヒントとして MM/DD/YYYY を入力します。
- ステップ 3** [追加 (Add)] をクリックします。
- カスタム フィールドがリストにアルファベット順またはソート順序のコンテキストで表示されます。
- ステップ 4** [保存 (Save)] をクリックします。設定の更新を保存しない場合は、[リセット (Reset)] をクリックして、最後に保存した値に戻します。
- (注) カスタム フィールドを削除すると、ゲスト タイプの [カスタム フィールド (Custom Fields)] リスト、およびアカウント登録ゲスト ポータルとスポンサー ポータルの設定で選択できなくなります。フィールドが使用されている場合、[削除 (Delete)] は無効になります。

次のタスク

目的のカスタム フィールドを含めることが可能です。

- そのゲスト タイプで作成されたアカウントにこの情報が含まれるようにゲスト タイプを定義する場合。 [ゲスト タイプの作成または編集 \(523 ページ\)](#) を参照してください。

- ゲストアカウントの作成時にスポンサーが使用するスポンサー ポータルを設定する場合。[#unique_688](#)を参照してください。
- アカウント登録ゲストポータルを使用してアカウント登録ゲストからの情報を要求する場合。[アカウント登録ゲスト ポータルの作成 \(549 ページ\)](#)を参照してください。

電子メールでの通知用の電子メール アドレスおよび SMTP サーバの指定

Cisco ISE では、スポンサーおよびゲストに、情報と手順を通知する電子メールを送信できます。これらの電子メールでの通知を配信するように SMTP サーバを設定できます。また、ゲストに通知を送信する電子メール アドレスを指定できます。



(注) ゲスト通知には、UTF-8 に互換性がある電子メール クライアントが必要です。

シングルクリック スポンサーの承認機能を使用するには、HTML 対応の電子メール クライアント（機能を有効にする）が必要です。

- ステップ 1** 電子メール設定を指定し、すべてのゲストポータルおよびスポンサーポータルの SMTP サーバを設定するには、[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [設定 (Settings)] > [ゲスト電子メールの設定 (Guest Email Settings)] の順に選択します。
- ステップ 2** [ゲストへの電子メール通知を有効にする (Enable email notifications to guests)] はデフォルトでオンになっています。この設定を無効にした場合、ゲストは、ゲストポータルとスポンサーポータルの設定中に有効にした他の設定に関係なく、電子メールでの通知を受信しません。
- ステップ 3** ゲストに電子メールでの通知を送信するために指定されている[デフォルトの送信元メールアドレス (Default "From" email address)]を入力します。たとえば、`donotreply@yourcompany.com` と入力します。
- ステップ 4** 次のいずれかを実行します。
- ゲストのアカウントを作成したスポンサーからの通知をゲストが受信するようにする場合は、[スポンサーの電子メールアドレスから通知を送信する (スポンサーの場合) (Send notifications from sponsor's email address (if sponsored))] をオンにします。アカウント登録ゲストは、デフォルトの電子メールアドレスから通知を受信します。
 - ゲストがスポンサーかアカウント登録かに関係なく通知を受信するようにする場合は、[常にデフォルトの電子メールアドレスから通知を送信する (Always send notifications from the default email address)] をオンにします。
- ステップ 5** [保存 (Save)] をクリックします。設定の更新を保存しない場合は、[リセット (Reset)] をクリックして、最後に保存した値に戻します。

ゲストのロケーションおよび SSID の割り当て

ゲスト ロケーションはタイム ゾーンの名前を定義し、ゲストにログインした時間関連設定を適用するために ISE によって使用されます。ゲスト ロケーションは、ゲスト アカウントを作成するスポンサー、およびアカウント登録ゲストによってゲスト アカウントに割り当てられます。デフォルトのゲスト ロケーションは **San Jose** です。他のゲスト ロケーションが追加されていない場合、すべてのアカウントにこのゲスト ロケーションが割り当てられます。1 つ以上の新しいロケーションを作成しないと、**San Jose** のゲスト ロケーションは削除できません。すべてのゲストが **San Jose** と同じタイムゾーンにいる場合を除き、必要なタイムゾーンで少なくとも 1 つのゲスト ロケーションを作成します。



- (注) ゲスト アクセスの時間は、ゲスト ロケーションのタイム ゾーンに基づきます。ゲスト ロケーションのタイム ゾーンがシステムのタイム ゾーンと一致しないと、ゲスト ユーザはログインできなくなることがあります。この場合、ゲスト ユーザには「認証に失敗しました (Authentication Failed)」エラーが表示されることがあります。デバッグレポートに「ゲストのアクティブ時間はまだ開始していません (Guest active time period not yet started)」というエラー メッセージが表示されることがあります。回避策として、[アカウントの管理 (Manage Accounts)] オプションを使用して、ゲスト ユーザのローカルタイム ゾーンに一致するようにゲストのアクセス開始時刻を調整できます。

ここで追加する SSID はスポンサー ポータルで使用できるため、スポンサーは接続する SSID をゲストに伝えることができます。

ゲスト ロケーションまたは SSID がスポンサー ポータルで設定されている場合、またはゲスト アカウントに割り当てられている場合は、削除できません。

ステップ 1 ゲスト ポータルおよびスポンサー ポータルのゲスト ロケーションと SSID を追加、編集、または削除するには、[ワーク センター (Work Centers)] > [ポータルとコンポーネント (Portals & Components)] > [設定 (Settings)] > [ゲスト ロケーションおよび SSID (Guest Locations and SSIDs)] を選択します。

ステップ 2 [ゲスト ロケーション (Guest Locations)] :

- サポートが必要な各タイムゾーンに対し、[ロケーション名 (Location name)] に入力し、ドロップダウン リストから [タイムゾーン (Time zone)] を選択します。
 - [追加 (Add)] をクリックします。
- (注) ゲスト ロケーションでは、場所の名前、タイム ゾーンの名前、および GMT オフセットはスタティックであり、これらを変更できません。GMT オフセットは夏時間の変更によって変更されません。GMT オフセットは、リストに表示されているオフセットとは逆です。たとえば、*Etc/GMT+3* は実際には GMT-3 です。
- (注) 初回ログインのゲスト タイプの場合、[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [ゲスト タイプ (Guest Types)] ページでアクセス時間制限を設定する場合にのみ、ゲスト ロケーション (タイム ゾーン) を設定することを確認してください。

ステップ 3 [ゲスト SSID (Guest SSIDs)] :

- a) ゲスト ロケーションでゲストが使用できるネットワークの **SSID** 名を入力します。
- b) [追加 (Add)] をクリックします。

ステップ 4 [保存 (Save)] をクリックします。最後に保存した値に戻すには、[リセット (Reset)] をクリックします。

次のタスク

新しいゲスト ロケーションまたは **SSID** を追加すると、次のことが可能になります。

- スポンサーがゲスト アカウントを作成するときに使用できる **SSID** を提供します。 [スポンサー ポータルのポータル設定 \(1314 ページ\)](#) を参照してください。
- スポンサー グループにゲスト ロケーションを追加して、ゲスト アカウントの作成時にそのグループに割り当てられたスポンサーが使用できるようにします。 [スポンサー グループの設定 \(560 ページ\)](#) を参照してください。
- アカウント登録ゲスト ポータルを使用してアカウント登録ゲストに使用可能なゲスト ロケーションを割り当てます。 [アカウント登録ゲストポータルの作成 \(549 ページ\)](#) を参照してください。
- 既存のゲスト アカウントの場合は、アカウントを手動で編集して **SSID** またはロケーションを追加します。

ゲストパスワード ポリシーのルール

Cisco ISE には、ゲスト ユーザパスワードについて次の組み込みルールがあります。

- ゲストパスワードポリシーは、スポンサー ポータル、アカウント登録ポータル、CSV ファイルでアップロードされたアカウント、ERS API を使用して作成されたパスワード、およびユーザが作成したパスワードに適用されます。
- ゲストパスワードポリシーに対する変更は、ゲストパスワードの期限が切れて変更が必要になるまで、既存のアカウントに影響しません。
- パスワードは大文字・小文字の区別をします。(Unable to authenticate using the domain name, user name, and password that you specified. Please check the values that you entered and try again. Passwords are case sensitive.)」
- 特殊文字<、>、/、および%は使用できません。
- 最小長および最小必須文字数は、すべてのパスワードに適用されます。
- パスワードとユーザ名を同じにすることはできません。
- 新規パスワードと既存パスワードを同じにすることはできません。
- ゲストアカウントの期限切れとは異なり、ゲストはパスワードが期限切れになる前に通知を受信しません。ゲストパスワードが期限切れになった場合は、スポンサーがパスワード

をランダム パスワードにリセットするか、ゲストが現在のログイン クレデンシャルを使用してログインしてからパスワードを変更することができます。



(注) ゲストのデフォルトユーザ名は4文字の英字からなり、パスワードは4文字の数字からなりません。短期間のゲストには、短く覚えやすいユーザ名とパスワードが適切です。必要に応じてISEでユーザ名とパスワードの長さを変更できます。

ゲストパスワードポリシーと有効期限の設定

すべてのゲストポータルのパスワードポリシーを定義できます。ゲストパスワードポリシーは、すべてのゲストアカウントのパスワードの生成方法を決定します。パスワードはアルファベット、数字、特殊文字を組み合わせて作成することができます。また、ゲストパスワードが期限切れになるまでの日数を設定し、ゲストにパスワードのリセットを要求することができます。

ゲストパスワードポリシーは、スポンサーポータル、アカウント登録ポータル、CSVファイルでアップロードされたアカウント、ERS APIを使用して作成されたパスワード、およびユーザが作成したパスワードに適用されます。

ステップ 1 [ゲスト アクセス (Guest Access)] > [設定 (Settings)] > [ゲストパスワードポリシー (Guest Password Policy)] を選択します。

ステップ 2 ゲストパスワードの [最小パスワード長 (Minimum password length)] (文字数) を入力します。

ステップ 3 パスワードの作成にゲストが使用できる各文字セットの文字を指定します。

[許可される文字数と最小値 (Allowed Characters and Minimums)] で次のいずれか 1 つのオプションを選択して、ゲスト用のパスワードポリシーを指定します。

- 各文字セットのすべての文字を使用します。
- 特定の文字の使用を防止するには、ドロップダウンメニューから [カスタム (Custom)] を選択し、その文字を事前定義済みの完全なセットから削除します。

ステップ 4 各セットから、使用する最小文字数を入力します。

4つの文字セットの必須文字数の合計が、全体の**最小パスワード長**を超えないようにする必要があります。

ステップ 5 [パスワードの有効期限 (Password Expiration)] で、次のオプションのいずれかを選択します。

- 最初にログインしてからゲストがパスワードを変更する必要がある頻度 (日数) を指定します。期限切れになる前にゲストがパスワードをリセットしないと、次回に元のログインクレデンシャルを使用してネットワークにログインするときに、パスワードを変更するように促されます。
- パスワードを無期限に設定します。

ステップ 6 [保存 (Save)] をクリックします。設定の更新を保存しない場合は、[リセット (Reset)] をクリックして、最後に保存した値に戻します。

次のタスク

パスワード要件を提示するためのパスワード ポリシーに関連したエラー メッセージをカスタマイズする必要があります。

1. [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [Sponsored-Guest ポータル (Sponsored-Guest Portals)] または [アカウント登録ゲストポータル (Self-Registered Guest Portals)] > [編集 (Edit)] > [ポータルページのカスタマイズ (Portal Page Customization)] > [エラーメッセージ (Error Messages)] を選択します。
2. キーワード「policy」を検索します。

ゲスト ユーザ名ポリシーのルール

Cisco ISE には、ゲスト ユーザ名ポリシーについて次の組み込みルールがあります。

- ゲスト ユーザ名ポリシーに対する変更は、ゲスト アカウントの期限が切れて変更が必要になるまで、既存のアカウントに影響しません。
- 特殊文字 <, >, /, および % は使用できません。
- 最小長および最小必須文字数は、電子メールアドレスに基づいたユーザ名を含め、すべてのシステム生成ユーザ名に適用されます。
- パスワードとユーザ名を同じにすることはできません。

ゲスト ユーザ名ポリシーの設定

ゲストユーザ名の作成方法に関するルールを設定できます。生成されるユーザ名は、電子メールアドレスに基づいて、またはゲストの姓と名に基づいて作成できます。またスポンサーは、ランダムな数のゲストアカウントを作成し、複数のゲストを作成する場合、またはゲストの名前と電子メールアドレスが利用できない場合に時間を短縮することもできます。ランダムに生成されたゲストユーザ名は、アルファベット、数字、および特殊文字の組み合わせから成ります。これらの設定は、すべてのゲストに影響します。

-
- ステップ 1** すべてのゲスト ポータルとスポンサー ポータルのゲスト ユーザ名ポリシーを定義するには、[ワーク センター (Work Centers)] > [ポータルとコンポーネント (Portals & Components)] > [設定 (Settings)] > [ゲスト ユーザ名ポリシー (Guest Username Policy)] の順に選択します。
 - ステップ 2** ゲスト ユーザ名の [ユーザ名の最小長 (Minimum username length)] (文字数) を入力します。
 - ステップ 3** [既知のゲストのユーザ名基準 (Username Criteria for Known Guests)] で次のいずれか 1 つのオプションを選択して、既知のゲストのユーザ名を作成するためのポリシーを指定します。
 - ステップ 4** [ランダムに生成されるユーザ名で利用できる文字 (Characters Allowed in Randomly-Generated Usernames)] で次のいずれか 1 つのオプションを選択して、ゲストのランダム ユーザ名を作成するためのポリシーを指定します。
 - 各文字セットのすべての文字を使用します。

- 特定の文字の使用を防止するには、ドロップダウンメニューから[カスタム (Custom)]を選択し、その文字を事前定義済みの完全なセットから削除します。

ステップ 5 各セットから、使用する最小文字数を入力します。

3つの文字セットからの合計文字数は、[ユーザ名の最小長 (Minimum username length)]に指定されている数を超えないようにする必要があります。

ステップ 6 [保存 (Save)]をクリックします。設定の更新を保存しない場合は、[リセット (Reset)]をクリックして、最後に保存した値に戻します。

次のタスク

ユーザ名要件を提示するためのユーザ名ポリシーに関連したエラーメッセージをカスタマイズする必要があります。

1. [ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [Sponsored-Guest ポータル (Sponsored-Guest Portal)]、[アカウント登録ゲスト ポータル (Self-Registered Guest Portals)]、[スポンサー ポータル (Sponsor Portals)]、または [デバイス ポータル (My Devices Portals)] > [編集 (Edit)] > [ポータル ページのカスタマイズ (Portal Page Customization)] > [エラー メッセージ (Error Messages)] の順に選択します。
2. キーワード「policy」を検索します。

SMS プロバイダーおよびサービス

SMS サービスは、ユーザおよびスポンサーがクレデンシャルを持つゲスト ポータルを使用しているゲストに SMS 通知を送信する場合に必要となります。可能な限り、会社の経費を削減するために、無料の SMS サービス プロバイダーを設定および提供します。

Cisco ISE は、加入者に無料の SMS サービスを提供するさまざまなセルラー サービス プロバイダーをサポートします。Cisco ISE でサービス契約とアカウント クレデンシャルを設定せずに、これらのプロバイダーを使用できます。セルラー サービス プロバイダーには、ATT、Orange、Sprint、TMobile、Verizon などがあります。

また、無料の SMS サービスを提供するその他のセルラー サービス プロバイダー、または Click-A-Tell などのグローバル SMS サービス プロバイダーも追加できます。デフォルトのグローバル SMS サービス プロバイダーには、サービス契約が必要です。また、Cisco ISE のアカウント クレデンシャルを設定する必要があります。

- アカウント登録ゲストがアカウント登録フォームで無料 SMS サービス プロバイダーを選択すると、SMS 通知がログイン クレデンシャルとともに無料で送信されます。SMS サービス プロバイダーを選択しない場合は、会社が契約したデフォルトのグローバル SMS サービス プロバイダーが SMS 通知の送信に使用されます。
- 自分が作成したゲスト アカウントに対してスポンサーが SMS 通知を送信できるようにする場合は、スポンサー ポータルをカスタマイズして、スポンサーが使用できる適切な SMS サービス プロバイダーをすべて選択する必要があります。スポンサー ポータル用の SMS

サービスプロバイダーを選択しない場合は、会社が契約したデフォルトのグローバル SMS サービス プロバイダーが SMS サービスを提供します。

SMS プロバイダーは、ISE の SMS ゲートウェイとして設定されます。ISE からの電子メールは SMS ゲートウェイにより SMS に変換されます。SMS ゲートウェイはプロキシサーバの背後に配置できます。

関連トピック

[ゲストに SMS 通知を送信するための SMS ゲートウェイの設定](#) (537 ページ)

[SMS ゲートウェイ設定 \(SMS Gateway Settings\)](#) (1198 ページ)

ゲストに SMS 通知を送信するための SMS ゲートウェイの設定

次のことができるようにするには、Cisco ISE で SMS ゲートウェイを設定する必要があります。

- ログインクレデンシアルおよびパスワードリセット手順に関する SMS 通知をスポンサーがゲストに手動で送信します。
- ゲストが、自分自身の登録に成功した後、自分のログイン資格情報が含まれた SMS 通知を自動的に受信します。
- ゲスト アカウントの期限が切れる前に実行するアクションに関する SMS 通知をゲストが自動的に受信します。

情報をフィールドに入力するときは、[USERNAME]、[PASSWORD]、[PROVIDER_ID] など、[] 内のすべてのテキストを、SMS プロバイダーのアカウントに固有の情報で更新する必要があります。

始める前に

[SMS 電子メール ゲートウェイ (SMS Email Gateway)] オプションに使用するデフォルト SMTP サーバを設定します。

ステップ 1 [管理 (Administration)]>[システム (System)]>[設定 (Settings)]>[SMS ゲートウェイ (SMS Gateway)] を選択します。

ステップ 2 [追加 (Add)] をクリックします。

ステップ 3 [SMS ゲートウェイ プロバイダー名 (SMS Gateway Provider Name)] を入力します。

ステップ 4 [プロバイダー インターフェイス タイプ (Provider Interface Type)] を選択し、必要な情報を入力します。

- [SMS 電子メール ゲートウェイ (SMS Email Gateway)] : 電子メール サーバ経由で SMS を送信する場合。
- [SMS HTTP API] : HTTP API を介して SMS を送信する場合 (GET または POST 方式) 。

SMS 電子メール ゲートウェイおよび SMS HTTP API ゲートウェイの設定に関する詳細については、[SMS ゲートウェイ設定 \(SMS Gateway Settings\)](#) (1198 ページ) を参照してください。

ステップ 5 [長いメッセージを複数に分割する (Break up long message into multiple parts)] をオンにして、Cisco ISE で 140 バイトを超えるメッセージを複数のメッセージに分割できるようにします。

ほとんどの SMS プロバイダーは、長い SMS メッセージを自動的に複数に分割します。MMS メッセージは SMS メッセージよりも長くなる可能性があります。

ステップ 6 [送信 (Submit)] をクリックします。

次のタスク

新しい SMS ゲートウェイを追加すると、次のことが可能になります。

- 期限切れのアカウントに関する SMS 通知をゲストに送信するときに、SMS サービス プロバイダーを選択します。[ゲスト タイプの作成または編集 \(523 ページ\)](#) を参照してください。
- [アカウント登録 (Self-Registration)] フォームでアカウント登録ゲストに示される選択肢として、SMS プロバイダーのうちのどれを表示するかを指定します。[アカウント登録ゲスト ポータルの作成 \(549 ページ\)](#) を参照してください。

ゲスト ポータル

企業の訪問者が企業のネットワークを使用してインターネットまたはネットワーク上のリソースおよびサービスにアクセスしようとしている場合、ゲスト ポータルを使用してネットワーク アクセスを提供することができます。設定すると、従業員はゲスト ポータルを使用して会社のネットワークにアクセスできます。

3 つのデフォルトのゲスト ポータルがあります。

- ホットスポット ゲスト ポータル：ネットワーク アクセスはクレデンシアルを必要とせずに許可されます。通常、ネットワーク アクセスを許可する前にユーザ ポリシーの認可 (AUP) が承認される必要があります。
- Sponsored-Guest ポータル：ゲストのアカウントを作成したスポンサーによりネットワーク アクセスが許可され、ゲストにログイン クレデンシアルが提供されます。
- アカウント登録ゲスト ポータル：ゲストは各自のアカウント クレデンシアルを作成できます。ネットワーク アクセスが付与される前に、スポンサー承認が必要となることがあります。

Cisco ISE は、事前に定義されたデフォルト ポータルなど、複数のゲスト ポータルをホストすることができます。

デフォルトのポータル テーマには、管理者ポータルからカスタマイズできる標準のシスコ ブランドが適用されています。

Wireless Setup には独自のデフォルト テーマ (CSS) があります。ロゴ、バナー、背景画像、色、フォントなどの基本的な設定の一部を変更できます。ISE では、他の設定を変更することによって、保護されたネットワーク アクセスを提供します。ゲストがこれらのクレデンシャルの 1 つまたは組み合わせを使用してログインすることを要求できます。

ゲスト ポータルのクレデンシャル

Cisco ISE では、ゲストにさまざまなタイプのクレデンシャルを使用したログインを要求することによって、保護されたネットワーク アクセスを提供します。ゲストがこれらのクレデンシャルの 1 つまたは組み合わせを使用してログインすることを要求できます。

- ユーザ名：必須。エンドユーザ ポータル (ホットスポット ゲスト ポータルを除く) を使用するすべてのゲストに適用され、ユーザ名ポリシーから取得されます。ユーザ名ポリシーはシステムによって生成されたユーザ名のみに適用され、ゲスト API プログラミング インターフェイスまたはアカウント登録プロセスを使用して指定されたユーザ名には適用されません。[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [設定 (Settings)] > [ゲスト ユーザ名ポリシー (Guest Username Policy)] で、ユーザ名に適用するポリシーを設定できます。ゲストは、電子メール、SMS、または印刷形式で、ユーザ名の通知を受け取ることができます。
- パスワード：必須。エンドユーザ ポータル (ホットスポット ゲスト ポータルを除く) を使用するすべてのゲストに適用され、パスワードポリシーから取得されます。[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [設定 (Settings)] > [ゲスト パスワード ポリシー (Guest Password Policy)] で、パスワードに適用するポリシーを設定できます。ゲストは、電子メール、SMS、または印刷形式で、パスワードの通知を受け取ることができます。
- アクセス コード：オプション。ホットスポット ゲスト ポータルおよびクレデンシャルを持つゲスト ポータルを使用するゲストに適用されます。アクセス コードは、物理的に存在するゲストに対して指定される、主にローカルで認識されるコードです (ホワイトボードによって視覚的に、またはロビーアンバサダーにより口頭で)。ネットワークにアクセスするために、屋外にいる誰かに知られたり使用されたりすることはありません。アクセス コードの設定を有効にした場合、次のようになります。
 - スポンサー付きゲストは、[ログイン (Login)] ページで (ユーザ名およびパスワードとともに) これを入力するよう求められます。
 - ホットスポット ゲスト ポータルを使用するゲストは、[利用規定 (Acceptable Use Policy (AUP))] ページでこれを入力するよう求められます。
- 登録コード：オプション。アカウント登録ゲストに適用され、アカウント登録ゲストに提供される方法においてアクセスコードと似ています。登録コード設定が有効な場合、アカウント登録ゲストはアカウント登録フォームでこれを入力するよう求められます。

ユーザ名とパスワードは、社内のスポンサーが (スポンサー付きゲストに対して) 提供できます。または、ゲストが自分自身を登録してこれらのクレデンシャルを取得できるように、クレデンシャルを持つゲスト ポータルを設定できます。

関連トピック

[ユーザ認証ポリシーの設定](#) (1225 ページ)

[ゲスト タイプおよびユーザ ID グループ](#) (523 ページ)

ホットスポット ゲスト ポータルを使用したゲスト アクセス

Cisco ISE にはネットワーク アクセス機能があり、その機能には「ホットスポット」が含まれています。これは、アクセスポイントで、ゲストはこれを使用してログインにクレデンシャルを必要とすることなくインターネットにアクセスできます。ゲストがコンピュータまたは Web ブラウザを搭載した任意のデバイスでホットスポット ネットワークに接続して、Web サイトに接続しようとする、自動的にホットスポット ゲスト ポータルにリダイレクトされます。この機能では、有線接続と無線接続 (Wi-Fi) の両方がサポートされます。

ホットスポット ゲスト ポータルは代替となるゲスト ポータルで、これを使用すると、ゲストにユーザ名とパスワードを要求することなく、ネットワークアクセスを提供することができ、ゲストアカウントを管理する必要性が軽減されます。代わりに、ゲストデバイスにネットワークアクセスを直接提供するために、Cisco ISE はネットワークアクセスデバイス (NAD) およびデバイス登録 Web 認証 (デバイス登録 WebAuth) とともに動作します。場合によって、ゲストは、アクセスコードを使用してログインするよう要求されることがあります。通常、これは社内に物理的に存在しているゲストにローカルに提供されるコードです。

ホットスポット ゲスト ポータルをサポートしている場合：

- ホットスポット ゲスト ポータルの設定に基づいて、ゲスト アクセスの条件を満たしている場合、ゲストにネットワーク アクセスが付与されます。
- Cisco ISE によってデフォルトのゲスト ID グループ GuestEndpoints が提供され、これを使用して、ゲスト デバイスを一元的に追跡できます。

クレデンシャルを持つゲスト ポータルを使用したゲスト アクセス

クレデンシャルを持つゲスト ポータルを使用して、外部ユーザの内部ネットワークおよびサービスと、インターネットへの一時アクセスを識別し許可することができます。スポンサーは、ポータルの [ログイン (Login)] ページでこれらのクレデンシャルを入力することによって、ネットワークにアクセスできる承認ユーザの一時的なユーザ名およびパスワードを作成できます。

次のように取得したユーザ名とパスワードを使用してゲストがログインできるように、クレデンシャルを持つゲスト ポータルを設定できます。

- スポンサーから付与されます。このゲストフローでは、ゲストは、社内に入って個人のゲストアカウントで設定されたとき、ロビー アンバサダーなどのスポンサーによるグリーティングを受け取ります。
- オプションの登録コードまたはアクセスコードを使用して自分自身を登録した後に付与されます。このゲストフローでは、ゲストは人間の介入なしでインターネットにアクセスで

き、これらのゲストにコンプライアンスに使用可能な一意の識別子があることが Cisco ISE によって保証されます。

- オプションの登録コードまたはアクセスコードを使用して自分自身を登録した後に付与されます。ただし、ゲストアカウントの要求がスポンサーによって承認された後のみです。このゲストフローでは、ゲストにネットワークへのアクセスが提供されますが、追加のスクリーニング レベルが実行された後でのみ提供されます。

また、ログイン時にユーザに新しいパスワードを入力するよう強制できます。

Cisco ISE では、複数のクレデンシャルを持つゲスト ポータルを作成し、これを使用してさまざまな基準に基づいてゲストアクセスを許可することができます。たとえば、日次訪問者に使用されるポータルとは別の、月次担当者向けのポータルを設定できます。

クレデンシャルを持つゲスト ポータルを使用した従業員アクセス

従業員は、そのポータルに設定された ID ソース順序でクレデンシャルにアクセスできれば、従業員クレデンシャルを使用してサインインすることによって、クレデンシャルを持つゲストポータルを使用してネットワークにアクセスすることもできます。

ゲスト デバイスのコンプライアンス

ゲストおよび非ゲストがクレデンシャルを持つゲストポータルを介してネットワークにアクセスした場合、アクセスを許可する前に、そのデバイスのコンプライアンスをチェックすることができます。ゲストおよび非ゲストを [クライアントプロビジョニング (Client Provisioning)] ページにルーティングして、最初にポスチャエージェントをダウンロードするよう要求することができます。このエージェントは、ポスチャプロファイルをチェックし、デバイスが準拠しているかどうかを検証します。これは、クレデンシャルを持つゲストポータルで、[ゲストデバイスのコンプライアンス設定 (Guest Device Compliance Settings)] のオプションを有効にすることで実行できます。これによって、[クライアントプロビジョニング (Client Provisioning)] ページがゲストフローの一部として表示されます。

クライアントプロビジョニングサービスでは、ゲストのポスチャ評価および修復が提供されます。クライアントプロビジョニングポータルは、中央 Web 認証 (CWA) のゲスト展開でのみ使用できます。ゲストログインフローによって CWA が実行され、クレデンシャルを持つゲストポータルは、利用規定やパスワード変更のチェックを実行した後、クライアントプロビジョニングポータルにリダイレクトされます。いったんポスチャが評価されると、ポスチャサブシステムはネットワークアクセスデバイスに対して許可変更 (CoA) を実行し、クライアント再接続を再認証します。

ゲスト ポータルの設定タスク

デフォルトポータルと、証明書、エンドポイント ID グループ、ID ソース順序、ポータルテーマ、イメージ、および Cisco ISE によって提供されるその他の詳細などのデフォルト設定を使用できます。デフォルト設定を使用しない場合は、新しいポータルを作成するか、必要性に合

うように既存の設定を編集する必要があります。同じ設定で複数のポータルを作成する場合は、ポータルを複製できます。

新しいポータルを作成したり、デフォルトポータルを編集した後は、ポータルの使用を承認する必要があります。いったんポータルの使用を承認すると、後続の設定変更はただちに有効になります。

ポータルを削除する場合は、関連付けられている許可ポリシールールおよび許可プロファイルを先に削除するか、別のポータルを使用するように変更する必要があります。

さまざまなゲストポータルの設定に関連するタスクについては、この表を参照してください。

タスク	ホットスポットゲストポータル	Sponsored-Guest ポータル	アカウント登録ゲストポータル
ポリシーサービスの有効化 (543 ページ)	必須 (Required)	必須 (Required)	必須 (Required)
ゲストポータルの証明書の追加 (543 ページ)	必須 (Required)	必須 (Required)	必須 (Required)
外部 ID ソースの作成 (543 ページ)	N/A	必須 (Required)	必須 (Required)
ID ソース順序の作成 (545 ページ)	N/A	必須 (Required)	必須 (Required)
エンドポイント ID グループの作成 (815 ページ)	必須 (Required)	不要 (ゲストタイプによって定義される)	不要 (ゲストタイプによって定義される)
ホットスポットゲストポータルの作成 (546 ページ)	必須 (Required)	N/A	N/A
Sponsored-Guest ポータルの作成 (547 ページ)	N/A	必須 (Required)	N/A
アカウント登録ゲストポータルの作成 (549 ページ)	N/A	N/A	必須 (Required)
ポータルの許可 (554 ページ)	必須 (Required)	必須 (Required)	必須 (Required)
ゲストポータルのカスタマイズ (556 ページ)	オプション	オプション	オプション

ポリシー サービスの有効化

Cisco ISE エンドユーザ Web ポータルをサポートするには、ホストするノードでポータル ポリシー サービスを有効にする必要があります。

-
- ステップ 1 [管理 (Administration)] > [システム (System)] > [展開 (Deployment)] を選択します。
 - ステップ 2 ノードをクリックして、[編集 (Edit)] をクリックします。
 - ステップ 3 [全般設定 (General Settings)] タブで、[ポリシー サービス (Policy Service)] をオンにします。
 - ステップ 4 [セッション サービスの有効化 (Enable Session Services)] オプションをオンにします。
 - ステップ 5 [保存 (Save)] をクリックします。
-

ゲスト ポータルの証明書の追加

デフォルトの証明書を使用しない場合は、有効な証明書を追加して、証明書グループ タグに割り当てることができます。すべてのエンドユーザ Web ポータルに使用されるデフォルトの証明書グループ タグは [デフォルト ポータル証明書グループ (Default Portal Certificate Group)] です。

-
- ステップ 1 [管理 (Administration)] > [システム (System)] > [証明書 (Certificates)] > [システム証明書 (System Certificates)] を選択します。
 - ステップ 2 システム証明書を追加し、ポータルに使用する証明書グループ タグに割り当てます。
この証明書グループ タグは、ポータルを作成または編集するときに選択できるようになります。
 - ステップ 3 [ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [ゲスト ポータル (Guest Portals)] > [作成または編集 (Create or Edit)] > [ポータル設定 (Portal Settings)] の順に選択します。
 - ステップ 4 新しく追加された証明書に関連付けられた [証明書グループ タグ (Certificate group tag)] ドロップダウン リストから特定の証明書グループ タグを選択します。
-

外部 ID ソースの作成

Cisco ISE では、Active Directory、LDAP、RADIUS トークン、RSA SecurID サーバなどの外部 ID ソースに接続して、認証/許可のユーザ情報を取得できます。外部 ID ソースには、証明書ベースの認証に必要な証明書認証プロファイルも含まれています。



-
- (注) 認証済みユーザ ID を受信して共有できるようにするパッシブ ID サービスを使用するには、[その他のパッシブ ID サービスプロバイダー \(433 ページ\)](#) を参照してください。
-

ステップ 1 [管理 (Administration)] > [ID の管理 (Identity Management)] > [外部 ID ソース (External Identity Sources)] を選択します。

ステップ 2 次のオプションのいずれかを選択します。

- [証明書認証プロファイル (Certificate Authentication Profile)] : 証明書ベースの認証の場合。
- [Active Directory] : 外部 ID ソースとして Active Directory に接続する場合 (詳細は [外部 ID ソースとしての Active Directory \(379 ページ\)](#) を参照)。
- [LDAP] : LDAP ID ソースを追加する場合 (詳細は [LDAP \(482 ページ\)](#) を参照)。
- [RADIUS トークン (RADIUS Token)] : RADIUS トークン サーバを追加する場合 (詳細は [RADIUS トークン ID ソース \(499 ページ\)](#) を参照)。
- [RSA SecurID] : RSA SecurID サーバを追加する場合 (詳細は [RSA ID ソース \(504 ページ\)](#) を参照)。
- [SAML ID プロバイダー (SAML Id Providers)] : Oracle Access Manager などの ID プロバイダー (IdP) を追加する場合 (詳細は [外部 ID ソースとしての ID プロバイダ \(14 ページ\)](#) を参照)。

認証用の SAML IDP ポータルにリダイレクトするためのゲスト ポータルの設定

ゲスト ポータルを設定して、ユーザが認証のために SAML IDP ポータルにリダイレクトされるようにすることができます。

ゲスト ポータルで [ログインに次の ID プロバイダ ゲスト ポータルの使用を許可 (Allow the following identity-provider guest portal to be used for login)] を設定することで、そのポータルで新しいログインエリアが有効になります。ユーザがそのログインオプションを選択した場合、代替 ID ポータルにリダイレクトされてから (表示されません)、認証のために SAML IDP ログオン ポータルにリダイレクトされます。

たとえば、ゲストポータルには従業員ログインのためのリンクがある場合があります。既存のポータルにログインする代わりに、ユーザは従業員ログオンリンクをクリックし、SAML IDP シングルサインオンポータルにリダイレクトされます。従業員はこの SAML IDP による最後のログオンからのトークンを使用して再接続されるか、その SAML サイトでログインします。これにより、同じポータルでシングル SSID からゲストと従業員の両方を扱うことができます。

次の手順は、SAML IDP を認証用に使用するように設定されている別のポータルを呼び出すゲストポータルを設定する方法を示しています。

ステップ 1 外部 ID ソースを設定します。詳細については、『ISE Administrators Guide』の「[SAMLv2 Identity Provider as an External Identity Source](#)」を参照してください。

ステップ 2 SAML プロバイダーのゲストポータルを作成します。ポータル設定で [認証方式 (Authentication method)] を SAML プロバイダーに設定します。ユーザにはこのポータルは表示されず、これは単にユーザを SAML IDP ログオン ページにつなぐためのプレースホルダです。次に説明するように、他のポータルをこのサブポータルにリダイレクトするように設定できます。

ステップ 3 作成したばかりの SAML プロバイダーポータルのゲストポータルにリダイレクトするためのオプションを備えたゲストポータルを作成します。これはメインポータルで、サブポータルにリダイレクトします。

SAML プロバイダーに見えるように、このポータルの外観をカスタマイズする場合があります。

- a) メイン ポータルの [ログイン ページの設定 (Login Page Settings)] で、[ログインに次の ID プロバイダ ゲスト ポータルの使用を許可 (Allow the following identity-provider guest portal to be used for login)] にマークを付けます。
- b) SAML プロバイダーと使用するために設定したゲスト ポータルを選択します。

ID ソース順序の作成

始める前に

Cisco ISE に外部 ID ソースを設定していることを確認します。

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ゲスト ユーザがローカル WebAuth を使用して認証できるようにするには、ゲスト ポータル認証ソースと ID ソース順序に同じ ID ストアが含まれるように設定する必要があります。

ステップ 1 [管理 (Administration)] > [ID の管理 (Identity Management)] > [ID ソース順序 (Identity Source Sequences)] > [追加 (Add)] を選択します。

ステップ 2 ID ソース順序の名前を入力します。また、任意で説明を入力できます。

ステップ 3 [証明書認証プロファイル (Certificate Authentication Profile)] チェックボックスをオンにし、証明書ベースの認証のための証明書認証プロファイルを選択します。

ステップ 4 [選択済み (Selected)] リスト ボックスの ID ソース順序に含めるデータベースを選択します。

ステップ 5 Cisco ISE がデータベースを検索する順序に [選択済み (Selected)] リストのデータベースを並べ替えます。

ステップ 6 [高度な検索リスト (Advanced Search List)] 領域で、次のいずれかのオプションを選択します。

- [順序内の他のストアにアクセスせず、AuthenticationStatus 属性を ProcessError に設定 (Do not access other stores in the sequence and set the AuthenticationStatus attribute to ProcessError)] : 最初に選択された ID ソースでユーザが見つからないとき、Cisco ISE が検索を中止する場合。
- [ユーザが見つからなかったとして処理し、順序内の次のストアに進む (Treat as if the user was not found and proceed to the next store in the sequence)] : 最初に選択された ID ソースでユーザが見つからないとき、Cisco ISE が順序内の他の選択された ID ソースの検索を続行する場合。

Cisco ISE では、要求の処理中にこれらの ID ソースが順番に検索されます。[選択済み (Selected)] リストに、Cisco ISE が ID ソースを検索する順序で ID ソースが表示されていることを確認します。

ステップ 7 [送信 (Submit)] をクリックして ID ソース順序を作成すると、その後この ID ソース順序をポリシーで使用できます。

エンドポイント ID グループの作成

Cisco ISE では、検出したエンドポイントを、対応するエンドポイント ID グループにグループ化します。Cisco ISE では、システム定義された複数のエンドポイントの ID グループが事前に

用意されています。[エンドポイント ID グループ (Endpoint Identity Groups)] ページで追加のエンドポイント ID グループを作成することもできます。作成したエンドポイント ID グループを編集または削除できます。システム定義されたエンドポイント ID グループの説明のみを編集できます。これらのグループの名前を編集したり、これらのグループを削除したりすることはできません。

-
- ステップ 1** [管理 (Administration)] > [ID の管理 (Identity Management)] > [グループ (Groups)] > [エンドポイント ID グループ (Endpoint Identity Groups)] を選択します。
- ステップ 2** [追加 (Add)] をクリックします。
- ステップ 3** 作成するエンドポイント ID グループの名前を入力します (エンドポイント ID グループの名前にスペースを入れないでください)。
- ステップ 4** 作成するエンドポイント ID グループの説明を入力します。
- ステップ 5** [親グループ (Parent Group)] ドロップダウン リストをクリックして、新しく作成したエンドポイント ID グループを関連付けるエンドポイント ID グループを選択します。
- ステップ 6** [送信 (Submit)] をクリックします。
-

ホットスポット ゲスト ポータルの作成

ホットスポット ゲスト ポータルを提供して、ゲストが、ログインにユーザ名とパスワードを要求されずにネットワークに接続できるようにすることができます。ログイン時にアクセスコードが必要な場合があります。

新しいホットスポット ゲスト ポータルを作成するか、既存のものを編集または複製できます。Cisco ISE によって提供されているデフォルトのポータルを含むすべてのホットスポット ゲスト ポータルを削除できます。

[ポータルの動作およびフローの設定 (Portal Behavior and Flow Settings)] タブのページ設定に加えた変更は、ゲストフロー図のグラフィカルフローに反映されます。AUP ページなどのページを有効にすると、そのページがフローに表示され、ゲストはポータルで使えるようになります。無効にすると、フローから削除され、次に有効なページがゲストに表示されます。

[認証成功の設定 (Authentication Success Settings)] を除くすべてのページ設定は、任意です。

始める前に

- このポータルで使用するために、必要な証明書とエンドポイント ID グループが設定されていることを確認します。
- ゲストがホットスポット ポータルのために接続する WLC が ISE でサポートされていることを確認します。リリースの『**Cisco Identity Services Engine Network Component Compatibility**』ガイド (http://www.cisco.com/c/en/us/td/docs/security/ise/2-1/compatibility/ise_sdt.html など) を参照してください。

-
- ステップ 1** [ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [ゲスト ポータル (Guest Portals)] > [作成、編集または複製 (Create, Edit or Duplicate)] の順に選択します。
- ステップ 2** 新しいポータルを作成する場合は、[ゲスト ポータルの作成 (Create Guest Portal)] ダイアログ ボックスで、ポータル タイプとして [ホットスポット ゲスト ポータル (Hotspot Guest Portal)] を選択し、[続行 (Continue)] をクリックします。
- ステップ 3** ポータルの一意の [ポータル名 (Portal Name)] および [説明 (Description)] を指定します。
ここで使用するポータル名が他のエンドユーザ ポータルに使用されていないことを確認します。
- ステップ 4** [言語ファイル (Language File)] ドロップダウン メニューを使用して、ポータルで使用する言語ファイルをエクスポートおよびインポートします。
- ステップ 5** [ポータルの設定 (Portal Settings)] でポート、イーサネット インターフェイス、証明書グループ タグ、エンドポイント ID グループなどのデフォルト値を更新し、ポータル全体に適用する動作を定義します。
- ステップ 6** 特定のページのそれぞれに適用される次の設定を更新してください。
- [利用規定 (AUP) ページ設定 (Acceptable Use Policy (AUP) Page Settings)] : 利用規定に同意することをゲストに要求します。
 - [ポストログイン バナーページの設定 (Post-Login Banner Page Settings)] : 必要に応じて、ゲストにアクセス ステータスおよびその他の追加アクションを通知します。
 - [VLAN DHCP リリース ページの設定 (VLAN DHCP Release Page Settings)] : ゲスト デバイスの IP アドレスをゲスト VLAN から解放し、ネットワークの他の VLAN にアクセスするように更新します。
 - [認証成功の設定 (Authentication Success Settings)] : 認証されたゲストに対する表示内容を指定します。
 - [サポート情報ページの設定 (Support Information Page Settings)] : ネットワーク アクセスの問題のトラブルシューティングのためにヘルプデスクによって使用される情報をゲストが提供するのを支援します。
- ステップ 7** [保存 (Save)] をクリックします。システム生成の URL がポータル テスト URL として表示されます。この URL を使用して、ポータルにアクセスし、テストすることができます。
-

次のタスク

ポータルを使用するには、そのポータルを許可する必要があります。ポータルを使用できるように許可する前または後に、ポータルをカスタマイズすることもできます。

Sponsored-Guest ポータルの作成

Sponsored-Guest ポータルを提供して、指定されたスポンサーがゲストにアクセスを許可できるようにすることができます。

新しい Sponsored-Guest ポータルを作成するか、既存のものを編集または複製できます。Cisco ISEによって提供されているデフォルトのポータルを含む、任意の Sponsored-Guest ポータルを削除できます。

[ポータルの動作およびフローの設定 (Portal Behavior and Flow Settings)] タブのページ設定に加えた変更は、ゲストフロー図のグラフィカルフローに反映されます。AUPページなどのページを有効にすると、そのページがフローに表示され、ゲストはポータルで使えるようになります。無効にすると、フローから削除され、次に有効なページがゲストに表示されます。

次のすべてのページ設定によって、ゲスト用の利用規定 (AUP) を表示し、その同意を要求することができます。

- ログイン ページの設定 (Login Page Settings)
- 利用規定 (AUP) ページ設定 (Acceptable Use Policy (AUP) Page Settings)
- BYOD 設定 (BYOD Settings)

始める前に

このポータルで使用するために、必要な証明書、外部 ID ソース、および ID ソース順序が設定されていることを確認します。

-
- ステップ 1** [ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [設定 (Configure)] > [ゲスト ポータル (Guest Portals)] > [作成、編集または複製 (Create, Edit or Duplicate)] の順に選択します。
- ステップ 2** 新しいポータルを作成する場合は、[ゲスト ポータルの作成 (Create Guest Portal)] ダイアログ ボックスで、ポータルタイプとして [Sponsored-Guest ポータル (Sponsored-Guest Portal)] を選択し、[続行 (Continue)] をクリックします。
- ステップ 3** ポータルの一意の [ポータル名 (Portal Name)] および [説明 (Description)] を指定します。
ここで使用するポータル名が他のエンドユーザ ポータルに使用されていないことを確認します。
- ステップ 4** [言語ファイル (Language File)] ドロップダウン メニューを使用して、ポータルで使用する言語ファイルをエクスポートおよびインポートします。
- ステップ 5** [ポータル設定 (Portal Settings)] でポート、イーサネット インターフェイス、証明書グループ タグ、ID ソース順序、認証方式などのデフォルト値を更新し、ポータル全体に適用する動作を定義します。
- ステップ 6** 特定のページのそれぞれに適用される次の設定を更新してください。

- [ログイン ページの設定 (Login Page Settings)] : ゲスト クレデンシャルおよびログイン ガイドラインを指定します。[ゲストが自分のアカウントを作成することを許可する (Allow guests to create their accounts)] オプションを選択した場合、ユーザは独自のゲスト アカウントを作成できます。このオプションが選択されていない場合は、スポンサーがゲスト アカウントを作成する必要があります。

(注) [認証方式 (Authentication Method)] フィールドで ID プロバイダー IdP) を選択している場合は、[ログイン ページ設定 (Login Page Settings)] オプションは無効です。

- [利用規定 (AUP) ページ設定 (Acceptable Use Policy (AUP) Page Settings)] : 別の AUP ページを追加し、クレデンシャルを持つゲスト ポータルを使用する従業員を含むゲスト用の利用規定の動作を定義します。
- [従業員のパスワード変更の設定 (Employee Change Password Settings)] : ゲストに、初めてログインした後にパスワードを変更するように指示します。

- [ゲスト デバイス登録の設定 (Guest Device Registration Settings)] : Cisco ISE に自動的にゲスト デバイスが登録されるようにするか、またはゲストが手動でこれらのデバイスを登録できるページを表示するかどうかを選択します。
- [BYOD 設定 (BYOD Settings)] : 従業員が自分のパーソナル デバイスを使用してネットワークにアクセスすることを許可します。
- [ポストログイン バナーページの設定 (Post-Login Banner Page Settings)] : ネットワーク アクセスを許可する前にゲストに追加情報を通知します。
- [ゲスト デバイスのコンプライアンス設定 (Guest Device Compliance Settings)] : ゲストを [クライアント プロビジョニング (Client Provisioning)] ページにルーティングし、最初にポスチャ エージェントをダウンロードするように要求します。
- [VLAN DHCP リリース ページの設定 (VLAN DHCP Release Page Settings)] : ゲスト デバイスの IP アドレスをゲスト VLAN から解放し、ネットワークの他の VLAN にアクセスするように更新します。
- [認証成功の設定 (Authentication Success Settings)] : 認証されたゲストに対する表示内容を指定します。
- [サポート情報ページの設定 (Support Information Page Settings)] : ネットワーク アクセスの問題のトラブルシューティングのためにヘルプ デスクによって使用される情報をゲストが提供するのを支援します。

ステップ 7 [保存 (Save)] をクリックします。システム生成の URL がポータル テスト URL として表示されます。この URL を使用して、ポータルにアクセスし、テストすることができます。

次のタスク



- (注) テスト ポータルは RADIUS セッションをサポートしていないため、すべてのポータルに対するポータル フローの全体は表示されません。BYOD およびクライアント プロビジョニングは RADIUS セッションに依存するポータルの例です。たとえば、外部 URL へのリダイレクションは機能しません。

ポータルを使用するには、そのポータルを許可する必要があります。ポータルを使用できるように許可する前または後に、ポータルをカスタマイズすることもできます。

アカウント登録ゲスト ポータルの作成

アカウント登録ゲストポータルを提供して、ゲストが自分自身を登録し、自分のアカウントを作成して、ネットワークにアクセスできるようにすることができます。これらのアカウントに対しては、その後も、アクセスを許可する前に、スポンサーによる承認を要求できます。

新しいアカウント登録ゲストポータルを作成するか、既存のものを編集または複製できます。Cisco ISE によって提供されているデフォルトのポータルを含むすべてのアカウント登録ゲストポータルを削除できます。

[ポータルの動作およびフローの設定 (Portal Behavior and Flow Settings)] タブのページ設定に加えた変更は、ゲストフロー図のグラフィカルフローに反映されます。AUP ページなどのペー

ジを有効にすると、そのページがフローに表示され、ゲストはポータルで使えるようになります。無効にすると、フローから削除され、次に有効なページがゲストに表示されます。

次のすべてのページ設定によって、ゲスト用の利用規定（AUP）を表示し、その同意を要求することができます。

- ログイン ページの設定（Login Page Settings）
- アカウント登録ページの設定（Self-Registration Page Settings）
- アカウント登録成功ページの設定（Self-Registration Success Page Settings）
- 利用規定（AUP） ページ設定（Acceptable Use Policy (AUP) Page Settings）
- BYOD 設定（BYOD Settings）

始める前に

このポータルに必要な証明書、外部 ID ソース、および ID ソース順序が設定されていることを確認します。

-
- ステップ 1** [ワーク センター（Work Centers）] > [ゲスト アクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [ゲスト ポータル（Guest Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] の順に選択します。
- ステップ 2** 新しいポータルを作成する場合は、[ゲスト ポータルの作成（Create Guest Portal）] ダイアログ ボックスで、ポータル タイプとして [アカウント登録ゲスト ポータル（Self-Registered Guest Portal）] を選択し、[続行（Continue）] をクリックします。
- ステップ 3** ポータルの一意の [ポータル名（Portal Name）] および [説明（Description）] を指定します。
ここで使用するポータル名が他のエンドユーザ ポータルに使用されていないことを確認します。
- ステップ 4** [言語ファイル（Language File）] ドロップダウン メニューを使用して、ポータルで使用する言語ファイルをエクスポートおよびインポートします。
- ステップ 5** [ポータル設定（Portal Settings）] で、ポート、イーサネット インターフェイス、証明書グループ タグ、ID ソース シーケンス、認証方式、およびこのポータルの動作を定義するその他の設定のデフォルト値を更新します。
ポータル設定フィールドの詳細については、[クレデンシャルを持つゲスト ポータルのポータル設定（1296 ページ）](#) を参照してください。
- ステップ 6** 特定のページのそれぞれに適用される次の設定を更新してください。
- [ログイン ページの設定（Login Page Settings）] : ゲスト クレデンシャルおよびログイン ガイドラインを指定します。詳細については、[クレデンシャルを持つゲスト ポータルのログイン ページ設定（1299 ページ）](#) を参照してください。
 - [アカウント登録ページの設定（Self-Registration Page Settings）] : ゲストが [アカウント登録（Self-Registration）] フォームを送信した後のゲストエクスペリエンス以外に、アカウント登録ゲストが読み取る情報、および [アカウント登録（Self-Registration）] フォームに入力する必要がある情報を指定します。

- [利用規定 (AUP) ページ設定 (Acceptable Use Policy (AUP) Page Settings)] : 別の AUP ページを追加し、クレデンシャルを持つゲスト ポータルを使用する従業員を含むゲスト用の利用規定の動作を定義します。詳細については、[クレデンシャルを持つゲスト ポータルの利用規定 \(AUP\) ページ設定 \(1305 ページ\)](#) を参照してください。
- [従業員のパスワード変更の設定 (Employee Change Password Settings)] : ゲストに、初めてログインした後にパスワードを変更するように指示します。
- [ゲスト デバイス登録の設定 (Guest Device Registration Settings)] : Cisco ISE に自動的にゲスト デバイスが登録されるようにするか、またはゲストが手動でこれらのデバイスを登録できるページを表示するかどうかを選択します。
- [BYOD 設定 (BYOD Settings)] : 従業員が自分のパーソナル デバイスを使用してネットワークにアクセスすることを許可します。詳細については、[クレデンシャルを持つゲスト ポータルの BYOD 設定 \(1307 ページ\)](#) を参照してください。詳細については、[クレデンシャルを持つゲスト ポータルの BYOD 設定 \(1307 ページ\)](#) を参照してください。
- [ポストログイン バナー ページ設定 (Post-Login Banner Page Settings)] : ユーザが正常にログインした後、ネットワーク アクセスを付与される前に追加情報を表示します。
- [ゲスト デバイスのコンプライアンス設定 (Guest Device Compliance Settings)] : ポスチャ アセスメントのためにゲストを [クライアント プロビジョニング (Client Provisioning)] ページにリダイレクトします。詳細については、[クレデンシャルを持つゲスト ポータルのゲスト デバイスのコンプライアンス設定 \(1309 ページ\)](#) を参照してください。
- [VLAN DHCP リリース ページの設定 (VLAN DHCP Release Page Settings)] : ゲスト デバイスの IP アドレスをゲスト VLAN から解放し、ネットワークの他の VLAN にアクセスするように更新します。詳細については、[クレデンシャルを持つゲスト ポータルの BYOD 設定 \(1307 ページ\)](#) を参照してください。
- 認証成功の設定 (Authentication Success Settings) : 認証後のゲストの宛先を指定します。認証後に外部 URL にゲストをリダイレクトする場合、URL アドレスを解決して、セッションがリダイレクトされるまでに遅延が生じることがあります。詳細については、[ゲスト ポータルの認証成功の設定 \(1311 ページ\)](#) を参照してください。
- [サポート情報ページの設定 (Support Information Page Settings)] : ネットワーク アクセスの問題のトラブルシューティングのためにヘルプデスクによって使用される情報をゲストが提供するのを支援します。

ステップ 7 [保存 (Save)] をクリックします。システム生成の URL がポータル テスト URL として表示されます。この URL を使用して、ポータルにアクセスし、テストすることができます。

次のタスク



- (注) テスト ポータルは RADIUS セッションをサポートしていないため、すべてのポータルに対するポータル フローの全体は表示されません。BYOD およびクライアント プロビジョニングは RADIUS セッションに依存するポータルの例です。たとえば、外部 URL へのリダイレクションは機能しません。

ポータルを使用するには、そのポータルを許可する必要があります。ポータルを使用できるように許可する前または後に、ポータルをカスタマイズすることもできます。

電子メールによるアカウント登録のアカウントの承認

登録ゲストにはアカウントの承認が必要であると設定されている場合、[アカウント登録ページの設定 (Self-Registration Page Settings)] で設定されているスポンサーに対して電子メールが送信されます。このメールには、アカウントを拒否または承認するためのリンクが含まれています。



(注) 古いバージョンの Cisco ISE から Cisco ISE 2.2 にデータベースをアップグレードまたは復元する場合は、承認/拒否のリンクを手動で挿入する必要があります。承認/拒否のリンクを手動で挿入するには、次の手順に従います。

1. [アカウント登録ゲスト ポータル (Self-Registered Guest Portal)] を選択します。
2. [ポータルページのカスタマイズ (Portal Page Customizations)] をクリックします。
3. [承認要求の電子メール (Approval Request Email)] セクションで [承認/拒否のリンクを挿入する (Insert Approve/Deny link)] をクリックします。

承認/拒否リンクを含む承認要求の電子メールの設定については、[アカウント承認メール リンクの設定 \(553 ページ\)](#) を参照してください。

たとえば、スポンサーが電子メールを開いて [承認 (Approve)] リンクをクリックすると実行されるアクションは、承認者の設定方法に応じて異なります。

[承認要求電子メール送信先 (Email approval request to)] が次のいずれかに設定されている場合について説明します。

• [訪問先担当者 (person being visited)]

- ゲスト アカウントに認証が**不要**な場合、1 回のクリックでアカウントが承認されます。
- ゲスト アカウントに承認が**必要**な場合、スポンサーに対し、スポンサー ポータルの特別なページが表示されます。このページでは、アカウントの承認前にスポンサーがクレデンシャルを入力する必要があります。

- [下に示すスポンサーの電子メールアドレス (sponsor email addresses listed below)] : 指定されるすべての電子メールアドレスに承認リンクが電子メールで送信されます。これらのスポンサーのいずれかが承認リンクまたは拒否リンクをクリックすると、スポンサー ポータルが表示されます。スポンサーは、検証済みのクレデンシャルを提供します。スポンサーが所属するスポンサー グループで、スポンサーによるゲスト アカウントの承認が許可されている場合、アカウントは承認されます。クレデンシャルが失敗すると、スポンサー ポータルにログインしてアカウントを手動で承認する指示がスポンサーに対して示されます。

説明

- Active Directory と LDAP を使用するスポンサー ポータルだけがサポートされています。
- [訪問先担当者 (person being visited)] を選択した場合、アカウント登録ゲストがそのフィールドに入力する内容は、スポンサーの電子メールアドレスでなければなりません。アカウント登録ポータルをカスタマイズし、そのフィールド名を「スポンサーの電子メールアドレス」のような名前に変更することを推奨します。ゲストの訪問先担当者を取得するため、必要に応じて新しいフィールドを作成できます。ユーザが [登録 (Register)] ボタンをクリックすると、ISEにより、訪問先担当者が有効なスポンサーであり、電子メールアドレスがあることが確認されます。ISE が ID ソースでそのスポンサーの電子メールアドレスを見つけない場合、ISEはエラーメッセージを表示し、アカウント登録が失敗します。
- スポンサーのリストが設定されている場合、1 番目のポータルが、スポンサーがログインするポータルではない場合でも、1 番目のポータルのカスタマイズ内容が使用されます。

アカウント承認メール リンクの設定

アカウント登録ゲストを承認するための承認リンクをスポンサーに電子メールで送信する方法の詳細については、[電子メールによるアカウント登録のアカウントの承認 \(552 ページ\)](#) を参照してください。

ステップ 1 [ワーク センター (Work Centers)] > [ゲスト (Guest)] > [設定 (Configure)] > [ゲスト ポータル (Guest Portals)] に移動し、メール アカウント承認リンクを設定するアカウント登録ポータルを選択します。

ステップ 2 [アカウント登録ページの設定 (Self Registration Page Settings)] タブを展開します。

ステップ 3 3.[アカウント登録ゲストの承認が必要である (Require self-registered guests to be approved)] をオンにします。これにより、[承認/拒否のリンクの設定 (Approve/Deny Link Settings)] セクションがタブ エリアの下部に表示されます。また、[承認要求メール (Approval Request Email)] の電子メール設定に、承認リンクと拒否リンクが取り込まれます。

[アカウント登録ページの設定 (Self Registration Page Settings)] を選択すると表示されるすべてのフィールドを以下に示します。

- [アカウント登録ゲストが承認される必要がある (Require self-registered guests to be approved)] : このポータルを使用するアカウント登録ゲストは、ゲストのクレデンシャルを受信する前にスポンサーによる承認が必要であることを指定します。このオプションをクリックすると、スポンサーがアカウント登録ゲストを承認する方法に関する追加のオプションが表示されます。詳細については、[電子メールによるアカウント登録のアカウントの承認 \(552 ページ\)](#) を参照してください。
- [承認要求電子メール送信先 (Email approval request to)] : 次のいずれかを選択します。
 - [下に示すスポンサーの電子メールアドレス (sponsor email addresses listed below)] : 承認者として指名されたスポンサーの 1 つ以上の電子メールアドレス、またはすべてのゲストの承認要求の送信先となるメール ソフトウェアを入力します。
 - [訪問先担当者 (person being visited)] : [スポンサーに承認用クレデンシャルの入力を求める (Require sponsor to provide credentials for authentication)] フィールドが表示され、[含めるフィー

ルド (Fields to include)] の [必須 (Required)] オプションが有効になります (以前は無効だった場合)。これらのフィールドはアカウント登録フォームに表示され、アカウント登録ゲストからこの情報を要求します。

- [承認/拒否のリンクの設定 (Approve/Deny Link Settings)] : このセクションでは次の内容を設定できます。
 - [リンクの有効期間 (Links are valid for)] : アカウント承認リンクの有効期間を設定できます。
 - [スポンサーに承認用クレデンシャルの入力を求める (Require sponsor to provide credentials for authentication)] : このセクションの設定でスポンサーによるアカウント承認用のクレデンシャルの入力が必須ではない場合にも、スポンサーにこの情報を入力させるには、このフィールドをオンにします。このフィールドは、[アカウント登録ゲストが承認される必要がある (Require self-registered guests to be approved)] が [訪問先担当者 (person being visited)] に設定されている場合にだけ表示されます。
 - [承認権限を検証するためスポンサーがスポンサー ポータルと照合される (Sponsor is matched to a Sponsor Portal to verify approval privileges)] : [詳細 > (Details >)] をクリックして、スポンサーが有効なシステムユーザであり、スポンサーグループのメンバーであり、そのスポンサーグループのメンバーにアカウント承認権限があることを確認するために検索されるポータルを選択します。各スポンサーポータルには、スポンサーを識別するために使用される ID ソース シーケンスがあります。ポータルはリストされている順序で使用されます。リストの 1 番目のポータルは、スポンサー ポータルで使用されているスタイルとカスタマイズ内容を決定します。

ポータルの許可

ポータルを許可するときは、ネットワークアクセス用のネットワーク許可プロファイルおよびルールを設定します。

始める前に

ポータルを許可する前にポータルを作成する必要があります。

ステップ 1 ポータルの特別な許可プロファイルを設定します。

ステップ 2 プロファイルの許可ポリシー ルールを作成します。

許可プロファイルの作成

各ポータルには、特別な許可プロファイルを設定する必要があります。

始める前に

デフォルトのポータルを使用しない場合は、許可プロファイルとポータル名を関連付けることができるように、最初にポータルを作成する必要があります。

-
- ステップ 1** [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] > [許可 (Authorization)] > [許可プロファイル (Authorization Profiles)] を選択します。
- ステップ 2** 使用を許可するポータル名を使用して許可プロファイルを作成します。
-

次のタスク

新しく作成される許可プロファイルを使用するポータル許可ポリシールールを作成する必要があります。

ホットスポット ポータルおよび MDM ポータル用の許可ポリシー ルールの作成

ユーザ（ゲスト、スポンサー、従業員）のアクセス要求への応答に使用するポータルのリダイレクション URL を設定するには、そのポータル用の許可ポリシー ルールを定義します。

url-redirect は、ポータル タイプに基づいて次の形式になります。

ip:port = IP アドレスとポート番号

PortalID = 一意のポータル名

ホットスポット ゲスト ポータル :

<https://ip:port/guestportal/gateway?sessionId=SessionIdValue&portal=PortalID&action=cwa&type=drw>

モバイル デバイス管理 (MDM) ポータル :

<https://ip:port/mdmportal/gateway?sessionId=SessionIdValue&portal=PortalID&action=mdm>

- ステップ 1** [ポリシー (Policy)] > [認証 (Authorization)] を選択して、[標準 (Standard)] ポリシーで新しい許可ポリシー ルールを作成します。

ポリシー セットをイネーブルにした場合は、[ポリシー (Policy)] > [ポリシー セット (Policy Set)] を選択し、このポータルに使用するポリシー セットを選択して、[承認ポリシー (Authorization Policy)] を展開し、新しいルールを追加します。

- ステップ 2** [条件 (Conditions)] には、ポータルの検証に使用するエンドポイント ID グループを選択します。たとえば、ホットスポット ゲスト ポータルの場合は、デフォルトの [GuestEndpoints] エンドポイント ID グループを選択し、MDM、ポータルの場合は、デフォルトの [RegisteredDevices] エンドポイント ID グループを選択します。

(注) ホットスポット ゲスト ポータルは、Termination CoA だけを発行するため、ゲスト許可ポリシーの検証条件の 1 つとして [Network Access:UseCase EQUALS Guest Flow] を使用しないでください。代わりに、エンドポイントが属する ID グループに照合して検証を行います。次の例を参考にしてください。

- "GuestEndpoint" + Wireless MAB の場合は Permit Access
- Wireless MAB の場合は HotSpot Redirect

ステップ 3 [権限 (Permissions)] には、作成したポータル許可プロファイルを選択します。

ゲスト ポータルのカスタマイズ

ポータルの外観およびユーザ（必要に応じてゲスト、スポンサー、または従業員）エクスペリエンスをカスタマイズするには、ポータルテーマをカスタマイズし、ポータルページの UI 要素を変更して、ユーザに表示されるエラーメッセージと通知を編集します。ポータルのカスタマイズの詳細については、[エンドユーザ Web ポータルのカスタマイズ \(613 ページ\)](#) を参照してください。

定期的な AUP 受け入れの設定

[ポリシー (Policy)] > [認証 (Authorization)] [ポリシー (Policy)] > [ポリシー セット (Policy Sets)] を参照し、AUP の期限が切れた場合にゲストユーザをクレデンシャルを持つポータルにリダイレクトする新しい許可ルールをリストの上部に作成します。LastAUPAcceptanceHours を目的の最大時間と比較するには条件を使用します（たとえば LastAUPAcceptanceHours > 8）。時間の範囲 8 ～ 999 をチェックできます。

次のタスク

エンドポイントが AUP 設定を受信したことを確認するには、次の手順を実行します。

1. [管理 (Administration)] > [ID (Identities)] > [エンドポイント (EndPoints)] を選択します。
2. AUP が最後に受け入れられた時刻を確認するエンドポイントをクリックします (AUPAcceptedTime)。

スポンサー ポータル

スポンサー ポータルは、Cisco ISE ゲスト サービスの主要コンポーネントの 1 つです。スポンサー ポータルを使用して、スポンサーは承認ユーザ用の一時アカウントを作成および管理し、企業ネットワークまたはインターネットにセキュアにアクセスできるようにします。ゲストアカウントを作成した後、スポンサーは、スポンサー ポータルを使用して、印刷、電子メール送

信、または携帯電話による送信を行ってゲストにアカウントの詳細を提供することもできます。アカウント登録ゲストに企業ネットワークへのアクセス権を提供する前に、スポンサーはゲスト アカウントを承認するように電子メールで要求されることがあります。

スポンサー ポータルでのゲスト アカウントの管理

スポンサー ポータルのログオンのフロー

スポンサー グループにより、スポンサー ユーザに割り当てることができる権限のセットが指定されます。スポンサー ユーザがスポンサー ポータルにログインすると、次の処理が行われます。

1. ISE がユーザのクレデンシャルを検証します。
2. ユーザの認証が成功すると、次にそのスポンサーユーザに一致するスポンサー グループ、つまりそのユーザが属するスポンサー グループを見つけるため、使用可能なすべてのスポンサー グループが検索されます。次の両方の条件を満たしている場合は、ユーザがスポンサー グループに一致しているか、属しています。
 - ユーザは、設定されているいずれかのメンバー グループのメンバーである。
 - [その他の条件 (Other Conditions)] を使用している場合は、そのユーザについてすべての条件が `true` である。
3. スポンサー ユーザがスポンサー グループに属している場合、スポンサー ユーザはそのグループの権限を取得します。ユーザは複数のスポンサー グループに属することができます。この場合、属しているすべてのグループの権限が組み合わせられます。ユーザがどのスポンサー グループにも属していない場合、スポンサー ポータルへのログインは失敗します。

スポンサー グループとその権限は、スポンサー ポータルから独立しています。スポンサーがログインするスポンサー ポータルに関係なく、スポンサー グループの照合には同一アルゴリズムが適用されます。

スポンサー ポータルの使用

スポンサー ポータルを使用して、承認された訪問者が企業ネットワークまたはインターネットにセキュアにアクセスできるようにする一時ゲスト アカウントを作成します。ゲスト アカウントを作成したら、スポンサー ポータルを使用してこれらのアカウントを管理し、アカウントの詳細情報をゲストに提供することができます。

スポンサー ポータルでは、スポンサーが新しいゲスト アカウントを個別に作成するか、またはファイルからユーザ グループをインポートすることができます。



- (注) Active Directory などの外部 ID ストアから承認された ISE 管理者は、スポンサー グループに所属できます。ただし、内部管理者アカウント（デフォルトの「admin」アカウントなど）はスポンサー グループに含めることができません。

スポンサー ポータルを開く方法はいくつかあります。

- 管理者コンソールで [アカウントの管理 (Manage Accounts)] リンクを使用する：管理者コンソールで [ゲストアクセス (Guest Access)] をクリックし、[アカウントの管理 (Manage Accounts)] をクリックします。[アカウントの管理 (Manage Accounts)] をクリックすると、ALL_ACCOUNTS にアクセスできるデフォルトのスポンサー グループに割り当てられます。新しいゲストアカウントを作成できますが、ゲストに対して通知することはできません。これは、ゲストからのアカウント アクティベーション リクエストを受信するための電子メールアドレスがないためです。同じ権限を持ち、スポンサー ポータルにログインしてこれらのアカウントを検索するスポンサーは、通知を送信できます。

このステップでは、スポンサー ポータルの [ポータルの動作およびフローの設定 (Portal Behavior and Flow Settings)] ページで設定した FQDN が DNS サーバに存在している必要があります。

- 管理者コンソールのスポンサー ポータル設定ページから、次の操作を実行します。[ゲストアクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [スポンサー ポータル (Sponsor Portals)] をクリックし、スポンサー ポータルを開き、[説明 (Description)] フィールドの右側にある [ポータルテスト URL (Portal Test URL)] リンクをクリックします。
- ブラウザで、スポンサー ポータルの [ポータル設定 (Portal Settings)] ページで設定した URL (FQDN) を開きます。この URL (FQDN) は DNS サーバで定義されている必要があります。

次の作業

スポンサー ポータルの使い方については、『Sponsor Portal User Guide for Cisco Identity Services Engine』（http://www.cisco.com/c/en/us/td/docs/security/ise/2-2/sponsor_guide/b_sponsorPortalUserGuide_22.html）を参照してください。

スポンサー アカウントの管理

スポンサーは、スポンサー ポータルからゲスト ユーザ アカウントを作成および管理する組織の従業員または請負業者となります。Cisco ISE は、ローカル データベースあるいは外部の Lightweight Directory Access Protocol (LDAP)、Microsoft Active Directory、または SAML ID ストア経由でスポンサーを認証します。外部ソースを使用しない場合、スポンサー用の内部ユーザ アカウントを作成する必要があります。

スポンサー グループ

スポンサー グループは、スポンサー ポータルの使用時にスポンサーに付与される権限を制御します。スポンサーがスポンサー グループのメンバーである場合、スポンサーにはグループに定義されている権限が付与されます。

スポンサーは、次の両方が当てはまる場合にスポンサー グループのメンバーであると見なされます。

1. スポンサーが、スポンサー グループで定義されているメンバー グループの少なくとも 1 つに属している。メンバー グループは、ユーザ ID グループか、Active Directory などの外部 ID ソースから選択されたグループです。
2. スポンサーが、スポンサー グループで指定されているすべてのその他の条件を満たしている。オプションのその他の条件は、ディクショナリ属性で定義される条件です。これらの条件は、許可ポリシーで使用されるものと動作が似ています。

スポンサーは、複数のスポンサー グループのメンバーにすることができます。その場合、スポンサーにはそれらすべてのグループから次のように組み合わせられた権限が付与されます。

- いずれかのグループで有効になっている場合、「ゲストのアカウントの削除」などの個々の権限が付与されます。
- スポンサーは、任意のグループでゲスト タイプを使用してゲストを作成できます。
- スポンサーは、任意のグループの場所にゲストを作成できます。
- バッチ サイズ制限などの数値は、グループの最大値が使用されます。

スポンサーがいずれかのスポンサー グループのメンバーでない場合、そのスポンサーはスポンサー ポータルにログインできません。

- ALL_ACCOUNTS : スポンサーは、すべてのゲスト アカウントを管理できます。
- GROUP_ACCOUNTS : スポンサーは、同じスポンサー グループのスポンサーが作成したゲスト アカウントを管理できます。
- OWN_ACCOUNTS : スポンサーは、自分が作成したゲスト アカウントのみを管理できます。

特定のスポンサー グループで使用可能な機能をカスタマイズでき、それによりスポンサー ポータルの機能を制限または拡張できます。次に例を示します。

関連トピック

[スポンサー ポータル](#) (556 ページ)

スポンサー アカウントの作成およびスポンサー グループへの割り当て

内部スポンサー ユーザ アカウントを作成し、スポンサー ポータルを使用できるスポンサーを指定するには、次の手順を実行します。

ステップ 1 [管理 (Administration)] > [ID の管理 (Identity Management)] > [ID (Identities)] > [ユーザ (Users)] を選択します。適切なユーザ ID グループに内部スポンサー ユーザ アカウントを割り当てます。

(注) デフォルトのスポンサー グループには、デフォルトの ID グループ `Guest_Portal_Sequence` が割り当てられています。

ステップ 2 [ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [スポンサー グループ (Sponsor Groups)] > [作成、編集または複製 (Create, Edit or Duplicate)] の順に選択し、[メンバー (Members)] をクリックします。スポンサー ユーザ ID グループをスポンサー グループにマッピングします。

次のタスク

スポンサーで使用するために、追加で組織に固有のユーザ ID グループを作成することもできます。[管理 (Administration)] > [ID の管理 (Identity Management)] > [グループ (Groups)] > [ユーザ ID グループ (User Identity Groups)] を選択します。

スポンサー グループの設定

シスコはデフォルトのスポンサー グループを提供します。デフォルト オプションを使用しない場合、新しいスポンサー グループを作成するか、またはデフォルトのスポンサー グループを編集して設定を変更できます。スポンサー グループを複製して、同じ設定と権限を持つスポンサー グループをさらに作成することもできます。

スポンサー グループを無効にすることができます。無効になったグループのメンバーはスポンサー ポータルにログインできなくなります。Cisco ISE によって提供されているデフォルトのスポンサー グループ以外のスポンサー グループを削除できます。

ステップ 1 [ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals and Components)] > [スポンサー グループ (Sponsor Groups)] > [作成、編集または複製 (Create, Edit or Duplicate)] の順に選択します。

ステップ 2 [スポンサーグループ名 (Sponsor group name)] と [説明 (Description)] に入力します。

ステップ 3 [一致基準 (Matching Criteria)] : このセクションの設定により、スポンサーがこのグループのメンバーかどうかが判別されます。

- **メンバー グループ (Member Groups)** : メンバーをクリックして 1 つ以上のユーザ (ID) グループおよび外部 ID ソースのグループを選択し、それらのグループを追加します。ユーザがこのスポンサー グループのメンバーになるためには、少なくとも 1 つの設定済みグループに属している必要があります。
- **その他の条件 (Other conditions)** : [新しい条件の作成 (Create New Condition)] をクリックして、このスポンサー グループに含まれるためにスポンサーが満たす必要がある条件を 1 つ以上構築します。Active Directory、LDAP、SAML、ODBC の ID ストアからの認証属性を使用できますが、RADIUS トークンまたは RSA SecurID ストアは使用できません。内部ユーザ属性も使用できます。条件には、属性、演算子、値があります。

- ディクショナリ属性 *Name* を使用して条件を作成するには、ID グループ名の前にユーザ ID グループを付けます。次に例を示します。

InternalUser:Name EQUALS bsmith

この場合、「bsmith」という名前の内部ユーザだけがこのスポンサー グループに所属できます。

- Active Directory インスタンスの *ExternalGroups* 属性を使用して条件を作成するには、一致させるスポンサー ユーザの AD 「プライマリ グループ」を選択します。たとえば、ユーザの名前が Smith の場合は *AD1:LastName EQUALS Smith* になります。

1 つ以上の設定されたメンバー グループとの一致に加えて、スポンサーはここで作成する**すべての**条件に一致する必要があります。認証しているスポンサーユーザが複数のスポンサー グループの一致基準を満たす場合には、そのユーザには次のようにアクセス許可が付与されます。

- ゲストのアカウントの削除などの個々の権限は、一致するグループのいずれかで有効になっている場合に付与されます。
- スポンサーは、一致するグループのいずれかのゲスト タイプを使用してゲストを作成することができます。
- スポンサーは、一致するグループのいずれかのゲスト タイプを使用してゲストを作成することができます。
- スポンサーは、一致するグループのいずれかの場所でゲストを作成することができます。
- バッチ サイズ制限などの数値については、一致するグループの最も大きな値が使用されます。

[メンバー グループ (Member Groups)] のみが指定されている一致基準、または [その他の条件 (Other Conditions)] のみが指定されている一致基準を作成できます。[その他の条件 (Other Conditions)] のみを指定する場合、スポンサー グループのスポンサーのメンバーシップは、一致するディクショナリ属性のみに基づいて決定されます。

- ステップ 4** このスポンサー グループに基づくスポンサーによって作成できるゲスト タイプを指定するには、[このスポンサーグループはこれらのゲストタイプを使用してアカウントを作成可能 (This sponsor group can create accounts using these guest types)] でボックス内をクリックして、1 つ以上のゲスト タイプを選択します。

[次の場所にゲストタイプを作成 (Create Guest Types at)] の下のリンクをクリックして、このスポンサーグループに割り当てるゲストタイプをさらに作成できます。新しいゲストタイプを作成した後、その新しいゲストタイプを選択するには、スポンサー グループを保存して閉じ、再度開いてください。

- ステップ 5** [ゲストが訪問するロケーションを選択 (Select the locations that guests will be visiting)] を使用して、ゲストアカウントの作成時にスポンサー グループのスポンサーが選択できるロケーション (ゲストの時間帯の設定に使用) を指定します。

[次の場所にゲストロケーションを設定 (Configure guest locations at)] の下のリンクをクリックして、ゲストロケーションを追加することで、選択できるロケーションをさらに追加できます。新しいゲストロケーションを作成した後、その新しいゲストロケーションを選択するには、スポンサー グループを保存して閉じ、再度開いてください。

これによって、ゲストが他のロケーションからログインできなくなることはありません。

ステップ 6 スポンサーがユーザの作成後に [通知 (Notify)] をクリックする操作を行わずにすむようにするには、[自動ゲスト通知 (Automatic guest notification)] の下の [電子メール アドレスが使用可能な場合はアカウント作成時にゲストに電子メールを自動的に送信する (Automatically email guests upon account creation if email address is available)] をオンにします。これにより、電子メールが送信されたことを示すウィンドウが表示されます。また、このオプションをオンにすると、[ゲスト通知は自動送信されました (Guest notifications are sent automatically)] というヘッダーがスポンサー ポータルに追加されます。

ステップ 7 [スポンサー作成可能 (Sponsor Can Create)] で、このグループ内のスポンサーがゲスト アカウントを作成するために使用できるオプションを設定します。

- 特定のゲストに割り当てられた複数のゲスト アカウント (インポート) (Multiple guest accounts assigned to specific guests (Import)) : スポンサーは、ファイルから姓名などのゲストの詳細をインポートすることによって、複数のゲスト アカウントを作成できます。

このオプションが有効である場合、[インポート (Import)] ボタンがスポンサー ポータルの [アカウントの作成 (Create Accounts)] ページに表示されます。[インポート (Import)] オプションは、Internet Explorer、Firefox、Safari などのデスクトップ ブラウザだけで使用可能です (モバイルは不可)

- バッチ処理の制限 (Limit to batch of) : このスポンサー グループが複数のアカウントを同時に作成できる場合、単一のインポート操作で作成可能なゲスト アカウントの数を指定します。

スポンサーは最大 10,000 個のアカウントを作成できますが、潜在的なパフォーマンスの問題があるため、作成するアカウントの数を制限することを推奨します。

- [ゲストへの複数のゲスト アカウントの割り当て (ランダム) (Multiple guest accounts to be assigned to any guests (Random))] : スポンサーが、未知のゲストのプレースホルダとして複数のランダム ゲスト アカウントを作成するか、または、または複数のアカウントをすばやく作成することができるようにします。

このオプションが有効である場合、[ランダム (Random)] ボタンがスポンサー ポータルの [アカウントの作成 (Create Accounts)] ページに表示されます。

- デフォルト ユーザ名プレフィックス (Default username prefix) : スポンサーが複数のランダムなゲスト アカウントを作成する場合に使用できるユーザ名プレフィックスを指定します。指定した場合、このプレフィックスはランダムなゲスト アカウントを作成するときにスポンサー ポータルに表示されます。また、[スポンサーにユーザ名プレフィックスの指定を許可 (Allow sponsor to specify a username prefix)] の設定により、次のようになります。

- 有効 : スポンサーは、スポンサー ポータルでデフォルトのプレフィックスを編集できます。
- 無効 : スポンサーは、スポンサー ポータルでデフォルトのプレフィックスを編集できません。

ユーザ名プレフィックスを指定しないか、またはスポンサーにユーザ名プレフィックスの指定を許可しない場合、スポンサーはスポンサー ポータルでユーザ名プレフィックスを割り当てるできません。

- スポンサーにユーザ名プレフィックスの指定を許可 (Allow sponsor to specify a username prefix) : このスポンサー グループが複数のアカウントを同時に作成できる場合、単一のインポート操作で作成可能なゲスト アカウントの数を指定します。

スポンサーは最大 10,000 個のアカウントを作成できますが、潜在的なパフォーマンスの問題があるため、作成するアカウントの数を制限することを推奨します。

ステップ 8 [スポンサーが管理可能 (Sponsor Can Manage)] で、このスポンサー グループのメンバーが表示および管理できるゲスト アカウントを制限できます。

- スポンサーが作成したアカウントのみ (Only accounts sponsor has created) : このグループのスポンサーは、スポンサーの電子メールアカウントに基づいて、スポンサーが作成したゲストアカウントのみを表示および管理できます。
- このスポンサー グループのメンバーによって作成されたアカウント (Accounts created by members of this sponsor group) : このグループのスポンサーは、このスポンサー グループ内のスポンサーが作成したゲスト アカウントを表示および管理できます。
- すべてのゲスト アカウント (All guest accounts) : スポンサーはすべての保留中のゲスト アカウントを表示および管理できます。

ステップ 9 [スポンサーの権限 (Sponsor Can)] で、このスポンサー グループのメンバーに、ゲストのパスワードおよびアカウントに関連する追加の権限を提供できます。

- ゲストの連絡先情報 (電子メール、電話番号) の更新 (Update guests' contact information (email, Phone Number)) : スポンサーは、自分が管理できるゲスト アカウントについて、ゲストの連絡先情報を変更できます。
- ゲストのパスワードの表示/印刷 (View/print guests' passwords) : これをオンにすると、スポンサーはゲストのパスワードを印刷することができます。スポンサーは [アカウントの管理 (Manage Accounts)] ページおよびゲストの詳細で、ゲストのパスワードを表示できます。これがオフの場合、スポンサーはパスワードを印刷できませんが、ユーザは電子メールまたは SMS (設定済みの場合) を介してパスワードを取得できます。
- ゲストのクレデンシャルを含む SMS 通知の送信 (Send SMS notifications with guests' credentials) : スポンサーは、自分が管理できるゲストアカウントについて、アカウントの詳細とログインクレデンシャルとともにゲストに SMS (テキスト) 通知を送信できます。
- ゲストアカウントパスワードのリセット (Reset guest account passwords) : スポンサーは、自分が管理できるゲストアカウントについて、そのパスワードを Cisco ISE によって生成されたランダムなパスワードにリセットできます。
- ゲストのアカウントの延長 (Extend guests' accounts) : スポンサーは、自分が管理できるゲストアカウントについて、その有効期限を延長できます。スポンサーは、アカウントの有効期限に関してゲストに送信される電子メール通知に自動的にコピーされます。
- ゲストのアカウントの削除 (Delete guests' accounts) : スポンサーは、自分が管理できるゲストアカウントについて、アカウントを削除し、ゲストが企業のネットワークにアクセスすることを防ぐことができます。

- ゲストのアカウントの一時停止 (Suspend guests' accounts) : スポンサーは、自分が管理できるゲスト アカウントについて、アカウントを一時停止してゲストが一時的にログインすることを防ぐことができます。
- また、このアクションは、許可変更 (CoA) 終了を発行して、一時停止されていたゲストをネットワークから排除できます。
- スポンサーに理由の入力を求める (Require sponsor to provide a reason) : ゲスト アカウントの一時停止に対する説明の入力をスポンサーに求めます。
- アカウント登録ゲストからの要求の承認および表示 (Approve and view requests from self-registering guests) : このスポンサー グループに含まれているスポンサーは、(承認が必要な) アカウント登録ゲストからのすべての保留中のアカウント要求を表示するか、アクセス先の担当者としてユーザがスポンサーの電子メール アドレスを入力した要求のみを表示できます。この機能では、アカウント登録ゲストによって使用されるポータルで[アカウント登録ゲストが承認される必要がある (Require self-registered guests to be approved)] にマークが付けられていて、スポンサーの電子メールが連絡先の担当者としてリストされている必要があります。
- [保留中のすべてのアカウント (Any pending accounts)] : このグループに所属するスポンサーは、他のスポンサーによって作成されたアカウントを承認およびレビューします。
- [このスポンサーに割り当てられている保留中のアカウントのみ (Only pending accounts assigned to this sponsor)] : このグループに所属するスポンサーは、スポンサー自身が作成したアカウントだけを表示および承認できます。
- プログラムによるインターフェイス (Guest REST API) を使用した Cisco ISE ゲスト アカウントへのアクセス (Access Cisco ISE guest accounts using the programmatic interface (Guest REST API)) : スポンサーは、自分が管理できるゲスト アカウントについて、Guest REST API プログラミング インターフェイスを使用してゲスト アカウントにアクセスできます。

ステップ 10 [保存 (Save)] をクリックし、[閉じる (Close)] をクリックします。

スポンサー アカウント作成のためのアカウント コンテンツの設定

ゲストとスポンサーが新しいゲスト アカウントの作成時に指定する必要があるユーザ データのタイプを設定できます。ISE アカウントを識別するために必要なフィールドがありますが、その他のフィールドを削除し、独自のカスタム フィールドを追加することができます。

スポンサーによるアカウント作成用のフィールドを設定するには、次の手順に従います。

1. ISE で [ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [スポンサー ポータル (Sponsor Portals)] を選択し、スポンサー ポータルを編集します。
2. [ポータル ページのカスタマイズ (Portal Page Customization)] タブを選択します。
3. 下にスクロールして [既知のゲストのアカウント作成 (Create Account for Known Guests)] を選択します。

4. 右側の [プレビュー (Preview)] 表示で [設定 (Settings)] を選択します。

これらの設定により、スポンサー ポータルでのゲスト アカウントの作成時に表示される、ゲスト アカウントに必要なフィールドが決定します。この設定は、ゲスト タイプ [既知 (Known)]、[ランダム (Random)]、および [インポート (Imported)] に適用されます。新しいユーザをインポートするためにスポンサーがダウンロードするテンプレートは動的に作成されるので、[既知のゲスト (Known Guests)] で設定したフィールドだけが含まれます。

アカウントのユーザ名とパスワードのインポート

スポンサーはユーザ名とパスワードをインポートできますが、スポンサーが CSV テンプレートをダウンロードするときにはこれらの行がテンプレートに追加されません。スポンサーはこれらのヘッダーを追加できます。ISE が列を認識できるように、ヘッダーの名前が正しく設定されている必要があります。

- [ユーザ名 (Username)] : *User Name* または *UserName* です。
- [パスワード (Password)] : **password** である必要があります。

スポンサー ポータル フローの設定

デフォルト ポータルと、証明書、エンドポイント ID グループ、ID ソース順序、ポータルテーマ、イメージ、および Cisco ISE によって提供されるその他の詳細などのデフォルト設定を使用できます。デフォルト設定を使用しない場合は、新しいポータルを作成するか、必要性に合うように既存の設定を編集する必要があります。同じ設定で複数のポータルを作成する場合は、ポータルを複製できます。

会社の営業所やその小売の場所にさまざまなブランディングがある場合、会社にはさまざまな製品ブランドがある場合、または市役所が火災、警察、およびその他の部門で異なるテーマのポータルを必要とする場合は、複数のスポンサー ポータルを作成することもできます。

これらは、スポンサー ポータルの設定に関連するタスクです。

始める前に

[スポンサー グループの設定 \(560 ページ\)](#) の説明に従い、サイトの既存のスポンサー グループを設定または編集します。

-
- ステップ 1 [ポリシー サービスの有効化 \(566 ページ\)](#)。
 - ステップ 2 [ゲスト サービスの証明書の追加 \(566 ページ\)](#)。
 - ステップ 3 [外部 ID ソースの作成 \(566 ページ\)](#)。
 - ステップ 4 [ID ソース順序の作成 \(567 ページ\)](#)。
 - ステップ 5 [スポンサー ポータルの作成 \(568 ページ\)](#)。
 - ステップ 6 (任意) [スポンサー ポータルのカスタマイズ \(569 ページ\)](#) [c_CustomizingSponsorPortals.xml](#)。
-

ポリシー サービスの有効化

Cisco ISE エンドユーザ Web ポータルをサポートするには、ホストするノードでポータル ポリシー サービスを有効にする必要があります。

-
- ステップ 1 [管理 (Administration)] > [システム (System)] > [展開 (Deployment)] を選択します。
 - ステップ 2 ノードをクリックして、[編集 (Edit)] をクリックします。
 - ステップ 3 [全般設定 (General Settings)] タブで、[ポリシー サービス (Policy Service)] をオンにします。
 - ステップ 4 [セッション サービスの有効化 (Enable Session Services)] オプションをオンにします。
 - ステップ 5 [保存 (Save)] をクリックします。
-

ゲスト サービスの証明書の追加

デフォルトの証明書を使用しない場合は、有効な証明書を追加して、証明書グループタグに割り当てることができます。すべてのエンドユーザ Web ポータルに使用されるデフォルトの証明書グループタグは [デフォルト ポータル証明書グループ (Default Portal Certificate Group)] です。

-
- ステップ 1 [管理 (Administration)] > [システム (System)] > [証明書 (Certificates)] > [システム証明書 (System Certificates)] を選択します。
 - ステップ 2 システム証明書を追加し、ポータルに使用する証明書グループタグに割り当てます。
この証明書グループタグは、ポータルを作成または編集するときに選択できるようになります。
 - ステップ 3 [ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [スポンサー ポータル (Sponsor Portals)] > [作成または編集 (Create or Edit)] > [ポータル設定 (Portal Settings)] を選択します。
 - ステップ 4 新しく追加された証明書に関連付けられた [証明書グループタグ (Certificate Group Tag)] ドロップダウンリストから特定の証明書グループタグを選択します。
-

外部 ID ソースの作成

Cisco ISE では、Active Directory、LDAP、RADIUS トークン、RSA SecurID サーバなどの外部 ID ソースに接続して、認証/許可のユーザ情報を取得できます。外部 ID ソースには、証明書ベースの認証に必要な証明書認証プロファイルも含まれています。



-
- (注) 認証済みユーザ ID を受信して共有できるようにするパッシブ ID サービスを使用するには、[その他のパッシブ ID サービスプロバイダー \(433 ページ\)](#) を参照してください。
-

ステップ 1 [管理 (Administration)] > [ID の管理 (Identity Management)] > [外部 ID ソース (External Identity Sources)] を選択します。

ステップ 2 次のオプションのいずれかを選択します。

- [証明書認証プロファイル (Certificate Authentication Profile)] : 証明書ベースの認証の場合。
- [Active Directory] : 外部 ID ソースとして Active Directory に接続する場合 (詳細は [外部 ID ソースとしての Active Directory \(379 ページ\)](#) を参照)。
- [LDAP] : LDAP ID ソースを追加する場合 (詳細は [LDAP \(482 ページ\)](#) を参照)。
- [RADIUS トークン (RADIUS Token)] : RADIUS トークン サーバを追加する場合 (詳細は [RADIUS トークン ID ソース \(499 ページ\)](#) を参照)。
- [RSA SecurID] : RSA SecurID サーバを追加する場合 (詳細は [RSA ID ソース \(504 ページ\)](#) を参照)。
- [SAML ID プロバイダー (SAML Id Providers)] : Oracle Access Manager などの ID プロバイダー (IdP) を追加する場合 (詳細は [外部 ID ソースとしての ID プロバイダ \(14 ページ\)](#) を参照)。

ID ソース順序の作成

始める前に

Cisco ISE に外部 ID ソースを設定していることを確認します。

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ゲスト ユーザがローカル WebAuth を使用して認証できるようにするには、ゲスト ポータル認証ソースと ID ソース順序に同じ ID ストアが含まれるように設定する必要があります。

ステップ 1 [管理 (Administration)] > [ID の管理 (Identity Management)] > [ID ソース順序 (Identity Source Sequences)] > [追加 (Add)] を選択します。

ステップ 2 ID ソース順序の名前を入力します。また、任意で説明を入力できます。

ステップ 3 [証明書認証プロファイル (Certificate Authentication Profile)] チェックボックスをオンにし、証明書ベースの認証のための証明書認証プロファイルを選択します。

ステップ 4 [選択済み (Selected)] リスト ボックスの ID ソース順序に含めるデータベースを選択します。

ステップ 5 Cisco ISE がデータベースを検索する順序に [選択済み (Selected)] リストのデータベースを並べ替えます。

ステップ 6 [高度な検索リスト (Advanced Search List)] 領域で、次のいずれかのオプションを選択します。

- [順序内の他のストアにアクセスせず、AuthenticationStatus 属性を ProcessError に設定 (Do not access other stores in the sequence and set the AuthenticationStatus attribute to ProcessError)] : 最初に選択された ID ソースでユーザが見つからないとき、Cisco ISE が検索を中止する場合。
- [ユーザが見つからなかったとして処理し、順序内の次のストアに進む (Treat as if the user was not found and proceed to the next store in the sequence)] : 最初に選択された ID ソースでユーザが見つからないとき、Cisco ISE が順序内の他の選択された ID ソースの検索を続行する場合。

Cisco ISE では、要求の処理中にこれらの ID ソースが順番に検索されます。[選択済み (Selected)] リストに、Cisco ISE が ID ソースを検索する順序で ID ソースが表示されていることを確認します。

ステップ 7 [送信 (Submit)] をクリックして ID ソース順序を作成すると、その後この ID ソース順序をポリシーで使用できます。

スポンサー ポータルの作成

スポンサー ポータルを提供して、ネットワークに接続してインターネットと内部リソースおよびサービスにアクセスするゲストのアカウントをスポンサーが作成、管理、および承認できるようにすることができます。

Cisco ISE では、別のポータルを作成する必要なく使用できるデフォルトのスポンサー ポータルが用意されています。ただし、新しいスポンサー ポータルを作成するか、既存のものを編集または複製できます。デフォルトのスポンサー ポータル以外のすべてのポータルを削除できます。

[ポータルの動作およびフローの設定 (Portal Behavior and Flow Settings)] タブの [ページ設定 (Page Settings)] で行った変更は、スポンサー フロー図のグラフィカル フローに反映されます。[AUP] ページなどのページを有効にすると、そのページがフローに表示され、スポンサーはポータルでそれを確認します。無効にした場合は、そのページがフローから削除され、次に有効にされたページがスポンサーに表示されます。

始める前に

このポータルで使用するために、必要な証明書、外部 ID ソース、および ID ソース順序が設定されていることを確認します。

-
- ステップ 1** [スポンサー ポータルのポータル設定 \(1314 ページ\)](#) の説明に従って、[ポータル設定 (Portal Settings)] ページを設定します。
- ここで使用するポータル名が他のエンドユーザ ポータルに使用されていないことを確認します。
- ステップ 2** [スポンサー ポータルのログイン設定 \(1318 ページ\)](#) の説明に従って、[ログイン設定 (Login Settings)] ページを設定します。
- ステップ 3** [スポンサー ポータルの利用規定 \(AUP\) 設定 \(1318 ページ\)](#) の説明に従って、[利用規定 (AUP) ページ設定 (Acceptable Use Policy (AUP) Page Settings)] ページを設定します。
- ステップ 4** [ゲスト パスワード ポリシーと有効期限の設定 \(534 ページ\)](#) と [ゲスト パスワード ポリシーのルール \(533 ページ\)](#) の説明に従って、[スポンサーのパスワード変更設定 (Sponsor Change Password Settings)] ページを設定します。
- ステップ 5** [スポンサー ポータルのポストログインバナー設定 \(1319 ページ\)](#) の説明に従って、[ポストログインバナー ページ設定 (Post-Login Banner Page Settings)] ページを設定します。
- ステップ 6** [スポンサーポータルアプリケーションの設定 (Sponsor Portal Application Settings)] では、ポータルをカスタマイズする場合は [ポータルのカスタマイズ (Portal Customization)] タブを参照します。

ステップ7 [保存 (Save)] をクリックします。

スポンサー ポータルのカスタマイズ

ポータルの外観およびユーザ エクスペリエンスをカスタマイズするには、ポータル テーマをカスタマイズし、ポータル ページの UI 要素を変更して、ユーザに表示されるエラー メッセージと通知を編集します。ポータルのカスタマイズの詳細については、[エンドユーザ Web ポータルのカスタマイズ \(613 ページ\)](#) を参照してください。

スポンサー アカウント作成のためのアカウント コンテンツの設定

ゲストとスポンサーが新しいゲスト アカウントの作成時に指定する必要があるユーザ データのタイプを設定できます。ISE アカウントを識別するために必要なフィールドがありますが、その他のフィールドを削除し、独自のカスタム フィールドを追加することができます。

スポンサーによるアカウント作成用のフィールドを設定するには、次の手順に従います。

1. ISE で [ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [スポンサー ポータル (Sponsor Portals)] を選択し、スポンサー ポータルを編集します。
2. [ポータル ページのカスタマイズ (Portal Page Customization)] タブを選択します。
3. 下にスクロールして [既知のゲストのアカウント作成 (Create Account for Known Guests)] を選択します。
 - 右側の [プレビュー (Preview)] 表示で [設定 (Settings)] を選択します。

これらの設定により、スポンサー ポータルでのゲストアカウントの作成時に表示される、ゲスト アカウントに必要なフィールドが決定します。

この設定は、ゲスト タイプ [既知 (Known)]、[ランダム (Random)]、および [インポート (Imported)] に適用されます。新しいユーザをインポートするためにスポンサーがダウンロードするテンプレートは動的に作成されるので、[既知のゲスト (Known Guests)] で設定したフィールドだけが含まれます。

スポンサーによるアカウントのユーザ名とパスワードのインポート

スポンサーはユーザ名とパスワードをインポートできますが、スポンサーがテンプレートをダウンロードするときにはこれらの行はテンプレートに追加されません。スポンサーはこれらのヘッダーを追加できます。ISE が列を認識できるように、ヘッダーの名前が正しく設定されている必要があります。

- **ユーザ名** : **User Name** または **UserName** のいずれかを指定します。
- **[パスワード (Password)]** : **password** である必要があります。

スポンサーに対して使用可能な時間設定項目の設定

スポンサーは新しいゲストアカウントを作成するときに、アカウントがアクティブである期間を設定します。スポンサーが使用できるオプションを設定して、スポンサーがアカウントの期間と、開始時刻および終了時刻を設定できるようにすることができます。これらのオプションはゲスト タイプ別に設定されます。スポンサーに対し、[アクセス情報 (Access Information)] というヘッダーの下に結果が表示されます。

スポンサーのポータル アカウント期間オプションを制御する [ゲスト タイプ (Guest Type)] 設定は、[最大アクセス時間 (Maximum Access Time)] ヘッダーの下にあります。この設定について次に説明します。

- [初回ログインから (From-First-Login)] : スポンサー ポータルには [期間 (Duration)] フィールドが表示され、その下に [初回ログインから (From-First-Login)] が表示されます。

Access Information

Duration:*

90

Days (Maximum:365)

FromFirst Login

Create

ゲスト タイプ設定の [最大アカウント期間 (Maximum account duration)] により、スポンサーがその期間として入力できる値が決定されます。

- [スポンサーが指定した日付から (From sponsor-specified date)] (該当する場合はアカウント登録の日付) : スポンサーは、期間を [営業日の終わり (End of business day)] として設定するか、または [営業日の終わり (End of business day)] フィールドをオフにして、期間、開始時刻、および終了時刻を設定するかを選択できます。

Access Information

☒ End of business day

23:59

Duration:*

90

Days (Maximum:365)

From Date (yyyy-mm-dd) *

2017-02-08

From Time *

10:52

To Date (yyyy-mm-dd) *

2017-05-09

To Time *

11:52

Create

期間と有効な日付を制御するゲストタイプ設定は、[アクセスを許可する日付と時刻（Allow access only on these days and times）] ヘッダーの下にあります。

- 選択した曜日により、スポンサーのカレンダーで選択できる日付が制限されます。
- 期間と日付を選択すると、スポンサー ポータルで最大アカウント期間が適用されます。

スポンサーがスポンサー ポータルにログインできない

問題

次のエラー メッセージは、スポンサーがスポンサー ポータルにログインしようとしたときに表示されます。

"Invalid username or password. Please try again."

原因

- スポンサーが無効なクレデンシャルを入力しました。
- スポンサーは、ユーザレコードがデータベース（内部ユーザまたは Active Directory）にないため無効です。
- スポンサーが属するスポンサー グループは無効です。
- スポンサーのユーザ アカウントがアクティブな/有効なスポンサー グループのメンバーではありません。これは、スポンサー ユーザの ID グループがいずれのスポンサー グループのメンバーでもないことを意味します。

- スポンサーの内部ユーザ アカウントは無効（一時停止中）です。

ソリューション

- ユーザのクレデンシャルを確認します。
- スポンサー グループを有効にします。
- ユーザ アカウントが無効になっている場合は復元します。
- スポンサー ユーザの ID グループをスポンサー グループのメンバーとして追加します。

ゲストとスポンサーのアクティビティのモニタ

Cisco ISE は、エンドポイントおよびユーザ管理情報、およびゲストとスポンサーのアクティビティを参照できるさまざまなレポートとログを提供します。Cisco ISE 1.2 レポートの一部は廃止されましたが、情報は他のレポートで表示できます。

オン デマンドまたはスケジュール ベースでこれらのレポートを実行できます。

ステップ 1 [操作 (Operations)] > [レポート (Reports)] を選択します。

ステップ 2 レポート セレクタで、[ゲスト アクセス レポート (Guest Access Reports)] および [エンドポイントとユーザ (Endpoints and Users)] 選択を展開し、さまざまなゲスト、スポンサー、およびエンドポイントに関するレポートを表示します。

ステップ 3 レポートを選択し、[フィルタ (Filters)] ドロップダウン リストを使用して、検索するデータを選択します。

ユーザ名、ポータル名、デバイス名、エンドポイント ID グループ、および他のデータについてフィルタを使用できます。

ステップ 4 データを表示する [時間範囲 (Time Range)] を選択します。

ステップ 5 [実行 (Run)] をクリックします。

メトリック ダッシュボード

Cisco ISE では、Cisco ISE ホーム ページに表示されるメトリック ダッシュボードで、ネットワークの [認証されたゲスト (Authenticated Guests)] と [アクティブ エンドポイント (Active Endpoints)] を一目で確認できます。



(注) ホットスポット フローの場合、[認証されたゲスト (Authenticated Guests)] ダッシュレットにエンドポイントが表示されません。

AUP 受け入れステータス レポート

AUP 受け入れステータス レポートには、すべてのゲスト ポータルからの、ゲストによる利用規定（AUP）の受け入れのステータスが示されます。このレポートは、**[操作（Operations）]>[レポート（Reports）]>[ゲスト アクセス レポート（Guest Access Reports）]>[AUP 受け入れステータス（AUP Acceptance Status）]** から使用できます。

レポートを使用して、特定の期間のすべての許可および拒否された AUP 接続を追跡できます。

ゲスト アカウンティング レポート

ゲスト アカウンティング レポートは、指定された期間のゲスト ログイン履歴を表示します。このレポートは、**[操作（Operations）]>[レポート（Reports）]>[ゲスト アクセス レポート（Guest Access Reports）]>[ゲスト アカウンティング（Guest Accounting）]** で利用できます。

マスター ゲスト レポート

マスター ゲスト レポートは、さまざまなレポートからのデータを単一のビューへ結合して、複数の異なるレポート ソースからデータをエクスポートできるようにします。データ カラムをさらに追加したり、表示またはエクスポートしないデータ カラムを削除したりできます。このレポートは、**[操作（Operations）]>[レポート（Reports）]>[ゲスト アクセス レポート（Guest Access Reports）]>[マスター ゲスト（Master Guest）]** で利用できます。このレポートには、非推奨のゲスト アクティビティ レポートに含まれていた情報も含まれるようになりました。

このレポートはすべてのゲスト アクティビティを収集し、ゲスト ユーザがアクセスした Web サイトに関する詳細を提供します。このレポートをセキュリティ監査の目的で使用して、ゲスト ユーザがいつネットワークにアクセスして、何を行ったかを確認できます。アクセスした Web サイトの URL などのゲストのインターネット アクティビティを表示するには、初めに次の操作を行う必要があります。

- 成功した認証のロギング カテゴリを有効にします。**[管理（Administration）]>[システム（System）]>[ロギング（Logging）]>[ロギング カテゴリ（Logging Categories）]** を選択して、**[成功した認証（Passed authentications）]** を選択します。
- ゲスト トラフィックで使用するファイアウォールで次のオプションを有効にします。
 - HTTP トラフィックを検査し、Cisco ISE モニタリング ノードにデータを送信します。Cisco ISE はゲスト アクティビティ レポートに対して IP アドレスおよびアクセスした URL だけを必要とするため、可能な場合は、この情報だけが含まれるようにデータを制限します。
 - Cisco ISE モニタリング ノードに syslog を送信します。

スポンサーのログインおよび監査レポート

スポンサー ログインおよび監査レポートは、次を追跡する統合レポートです。

- スポンサー ポータルでのスポンサーによるログイン アクティビティ。
- スポンサー ポータルでスポンサーが実行したゲスト関連の操作。

このレポートは、[操作 (Operations)] > [レポート (Reports)] > [ゲスト アクセス レポート (Guest Access Reports)] > [スポンサー ログインおよび監査 (Sponsor Login and Audit)] で使用できます。

ゲストおよびスポンサー ポータルの監査ロギング

ゲスト ポータルおよびスポンサー ポータルで特定のアクションが実行されると、基礎となる監査システムに監査ログ メッセージが送信されます。デフォルトでは、これらのメッセージは、/opt/CSCOCpm/logs/localStore/iseLocalStore.log ファイルに記録されます。

これらのメッセージを syslog によってモニタリング/トラブルシューティング システムおよびログ コレクタに送信するように設定することができます。モニタリング サブシステムによって、適切なスポンサー、デバイス監査ログ、およびゲストのアクティビティ ログにこの情報が示されます。

ゲスト ログイン フローは、ゲスト ログインが成功したか失敗したかにかかわらず、監査ログに記録されます。

ゲスト アクセス Web 認証オプション

Cisco ISE では、Cisco ISE ゲスト サービスと Web 認証サービスを使用したセキュアなゲスト アクセスを有効にするための複数の展開オプションがサポートされています。ローカルまたは中央 Web 認証とデバイス登録 Web 認証を使用した有線または無線のゲスト接続を提供することができます。

- [中央 Web 認証 (Central WebAuth)] : すべてのゲスト ポータルに適用されます。Web 認証は、有線および無線の両方の接続要求に対して、中央 Cisco ISE RADIUS サーバによって実行されます。ゲスト デバイスの認証は、ゲストが、ホットスポット ゲスト ポータルで任意のアクセス コードを入力し、クレデンシャルを持つゲスト ポータルでユーザ名とパスワードを入力した後、実行されます。



(注) ユーザ資格情報用のブラウザへのリダイレクト (CWA) を使用する場合、起動時に複数のタブを開くブラウザを使用しているユーザはサポートされません。リダイレクト中にブラウザで複数のタブが開かれる場合、ISE はすべてのタブにリダイレクトします。ユーザはポータルにログインできるものの ISE はセッションを正しく承認しないため、ユーザはアクセスできません。

この問題を回避するには、ユーザがブラウザ上で 1 つを除くすべてのタブを閉じる必要があります。

- ローカル Web 認証 (ローカル WebAuth) : クレデンシャルを持つゲスト ポータルに適用されます。ゲストへの Web ページの提供は、有線接続の場合にはスイッチなどのネットワーク アクセス デバイス (NAD) で、無線接続の場合にはワイヤレス LAN コントローラ (WLC) によって、ローカルに実行されます。ゲスト デバイスの認証は、ゲストが、クレデンシャルを持つゲスト ポータルでユーザ名とパスワードを入力した後、実行されます。
- デバイス登録 Web 認証 (デバイス登録 WebAuth) : ホットスポット ゲスト ポータルにのみ適用されます。Web 認証は、Cisco ISE によってデバイスが登録され、使用が許可された後、実行されます。ゲストは、有線または無線接続で (ユーザ名またはパスワードを入力しないで) ネットワークにアクセスできるホットスポット ゲスト ポータルに誘導されます。

ISE Community Resource

ゲスト アクセスを提供するように Cisco ISE と Cisco ワイヤレス コントローラを設定する方法については、「[How-To_93_ISE_20_Wireless_Guest_Setup_Guide](#)」を参照してください。

ISE テクニカル ノートも参照してください。 <http://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/115732-central-web-auth-00.html>

中央 WebAuth プロセス対応の NAD

このシナリオでは、ネットワーク アクセス デバイス (NAD) で、不明なエンドポイント接続から Cisco ISE RADIUS サーバへの新しい認証要求を作成します。これで、エンドポイントは Cisco ISE への URL-redirect を受け取ります。



(注) webauth-vrf-aware コマンドは、IOS XE 3.7E、IOS 15.2(4)E 以降のバージョンでのみサポートされています。その他のスイッチでは、Virtual Route Forwarding (VRF) 環境での WebAuth URL リダイレクトはサポートされていません。このような場合、回避策として、トラフィックを VRF に戻すためのルートをグローバル ルーティング テーブルに追加できます。

ゲストデバイスが NAD に接続されている場合、ゲストサービスのインタラクションは、ゲストポータルの中央 WebAuth のログインにつながる MAC 認証バイパス (MAB) 要求の形式を取ります。無線と有線の両方のネットワーク アクセス デバイスに適用される後続の中央 Web 認証 (中央 WebAuth) プロセスの概要は、次のとおりです。

1. ゲストデバイスは、有線接続によって NAD に接続します。ゲストデバイス上に 802.1X サプリカントはありません。
2. MAB のサービス タイプを扱う認証ポリシーにより、MAB が引き続き失敗し、中央 WebAuth ユーザインターフェイスの URL-redirect を含む制限付きネットワーク プロファイルが返されます。
3. NAD は、Cisco ISE RADIUS サーバに対して MAB 要求を認証するように設定されています。
4. Cisco ISE RADIUS サーバで MAB 要求が処理されますが、ゲスト デバイスのエンドポイントが見つかりません。

この MAB の失敗により、制限付きネットワーク プロファイルが適用され、プロファイル内の URL-redirect 値が access-accept で NAD に返されます。この機能をサポートするには、許可ポリシーが存在し、適切な有線または無線 MAB (複合条件下で) と、任意で「Session:Posture Status=Unknown」条件が備わっていることを確認します。NAD では、この値に基づいて、デフォルト ポート 8443 のすべてのゲスト HTTPS トラフィックが URL-redirect 値にリダイレクトされます。

この場合の標準の URL 値は次のとおりです。

<https://ip:port/guestportal/gateway?sessionId=NetworkSessionId&portal=<PortalID>&action=cwa>

5. ゲスト デバイスが、Web ブラウザから URL をリダイレクトするための HTTP 要求を開始します。
6. NAD により、最初の access-accept から返された URL-redirect 値に要求がリダイレクトされます。
7. CWA をアクションとしたゲートウェイ URL 値は、ゲストポータル ログイン ページにリダイレクトされます。
8. ゲストはログイン クレデンシャルを入力してログイン フォームを送信します。
9. ゲスト サーバはログイン クレデンシャルを認証します。
10. フローのタイプに応じて、次の処理が実行されます。

- クライアントプロビジョニングを実行するようにゲストポータルが設定されていない非ポスチャ フロー (これ以上の検証がない認証) の場合、ゲストサーバは CoA を NAD に送信します。この CoA により、NAD は Cisco ISE RADIUS サーバを使用してゲストデバイスを再認証します。設定されたネットワークアクセスとともに新しい access-accept が NAD に返されます。クライアントプロビジョニングが未設定で、VLAN を変更する必要がある場合、ゲストポータルで VLAN IP の更新が行われます。ゲストはログイン クレデンシャルを再入力する必要はありません。初回ログイン時に入力したユーザ名とパスワードが自動的に使用されます。

- クライアントプロビジョニングを実行するようにゲストポータルが設定されているポスチャフローの場合、ゲストデバイスの Web ブラウザに、ポスチャ エージェントのインストールおよびコンプライアンスのための [クライアント プロビジョニング (Client Provisioning)] ページが表示されます。（必要に応じて、クライアント プロビジョニング リソース ポリシーに「NetworkAccess:UseCase=GuestFlow」条件を含めることもできます）。

Linux 向けのクライアントプロビジョニングやポスチャエージェントは存在しないため、ゲストポータルはクライアントプロビジョニングポータルにリダイレクトされ、クライアントプロビジョニングポータルは元のゲスト認証サブレットにリダイレクトされます。この認証サブレットで、必要に応じて IP リリース/更新が行われてから、CoA が実行されます。

クライアントプロビジョニングポータルへのリダイレクションを使用して、クライアントプロビジョニングサービスはゲストデバイスに非永続的 Web エージェントをダウンロードし、デバイスのポスチャチェックを実行します（必要に応じて、ポスチャポリシーに「NetworkAccess:UseCase=GuestFlow」条件を含めることもできます）。

ゲストデバイスが非準拠の場合、「NetworkAccess:UseCase=GuestFlow」条件および「Session:Posture Status=NonCompliant」条件を備えた許可ポリシーが設定済みであることを確認してください。

ゲストデバイスが準拠している場合は、設定した許可ポリシーに「NetworkAccess:UseCase=GuestFlow」条件および「Session:Posture Status=Compliant」条件が含まれていることを確認してください。ここから、クライアントプロビジョニングサービスによって NAD に対して CoA が発行されます。この CoA により、NAD は Cisco ISE RADIUS サーバを使用してゲストを再認証します。設定されたネットワークアクセスとともに新しい access-accept が NAD に返されます。



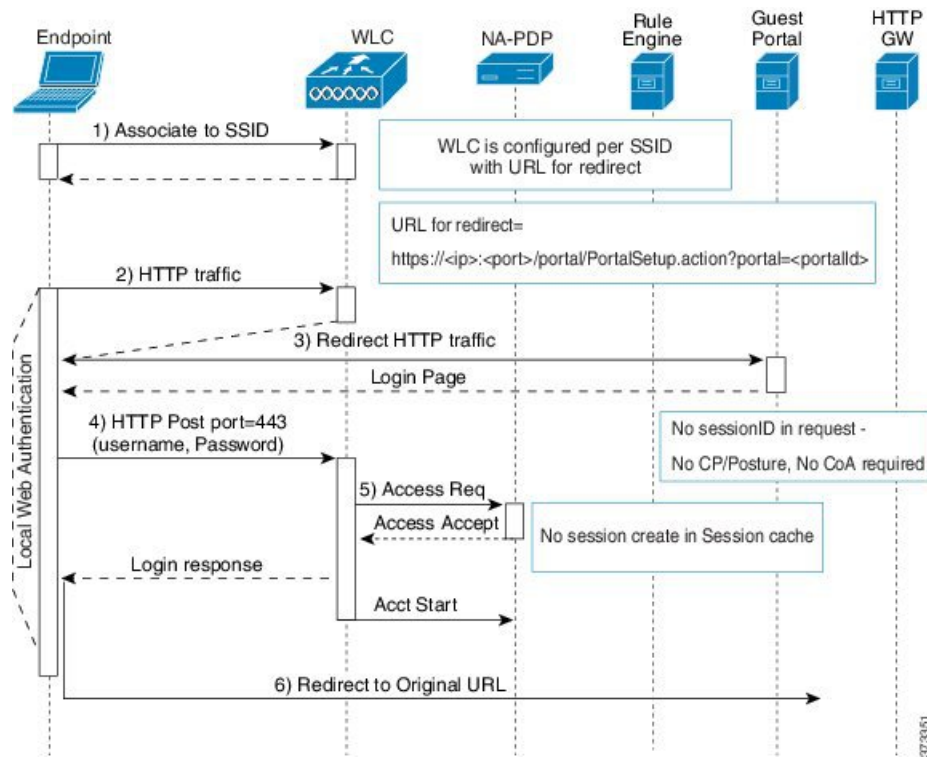
(注) 「NetworkAccess: UseCase=GuestFlow」は、ゲストとしてログインする Active Directory (AD) および LDAP ユーザにも適用できます。

ローカル WebAuth プロセス対応のワイヤレス LAN コントローラ

このシナリオでは、ゲストがログインすると、ワイヤレス LAN コントローラ (WLC) に転送されます。その後、WLC はゲストをゲストポータルにリダイレクトします。ゲストポータルでは、ログインクレデンシャルの入力を求められ、必要に応じて利用規定 (AUP) の受け入れやパスワードの変更を実行することもできます。完了したら、ゲストデバイスのブラウザは WLC にリダイレクトされ、POST 経由でログインクレデンシャルが提供されます。

WLC は、Cisco ISE RADIUS サーバ経由でゲストのログイン処理を行うことができます。その処理が完了したら、WLC はゲストデバイスのブラウザを元の URL の宛先にリダイレクトします。ゲストポータルの元の URL リダイレクトをサポートするためのワイヤレス LAN コントローラ (WLC) とネットワークアクセスデバイス (NAD) の要件は、リリース IOS-XE 3.6.0.E および 15.2(2)E が動作する WLC 5760 および Cisco Catalyst 3850、3650、2000、3000、および 4000 シリーズ アクセス スイッチです。

図 37: ローカル WebAuth 対応 WLC の Non-Posture フロー



ローカル WebAuth プロセス対応の有線 NAD

このシナリオでは、ゲスト ポータルにより、ゲストのログイン要求がスイッチ（有線 NAD）にリダイレクトされます。ログイン要求は、スイッチにポストされる HTTPS URL の形式になり、ログイン クレデンシャルが含まれます。スイッチにゲスト ログイン要求が届くと、設定済みの Cisco ISE RADIUS サーバを使用してゲストの認証が行われます。

1. Cisco ISE により、HTML リダイレクトを含む login.html ファイルを NAD にアップロードするよう要求されます。HTTPS 要求が発生すると、この login.html ファイルがゲストデバイスのブラウザに返されます。
2. ゲストデバイスのブラウザがゲスト ポータルにリダイレクトされます。ここで、ゲストのログイン クレデンシャルが入力されます。
3. 利用規定（AUP）とパスワード変更が処理された後（両方ともオプションです）、ゲスト ポータルにより、ログイン クレデンシャルをポストするゲストデバイスのブラウザが NAD にリダイレクトされます。
4. NAD により、Cisco ISE RADIUS サーバに対して RADIUS 要求が発行され、ゲストの認証と許可が行われます。

Login.html ページに必要な IP アドレスおよびポートの値

login.html ページの次の HTML コードで、IP アドレスとポートの値を Cisco ISE ポリシー サービス ノードと同じ値に変更する必要があります。デフォルトポートは 8443 ですが、この値を変更できます。そのため、スイッチに割り当てた値が Cisco ISE の設定と一致していることを確認してください。

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML>
<head>
<title>ISE Guest Portal</title>
<meta Http-Equiv="Cache-Control" Content="no-cache">
<meta Http-Equiv="Pragma" Content="no-cache">
<meta Http-Equiv="Expires" Content="0">
<meta http-equiv="content-type" content="text/html; charset=ISO-8859-1">

<meta http-equiv="REFRESH"
content="0;url=https://ip:port/portal/PortalSetup.action?switch_url=wired">

</HEAD>
<BODY>

<center>
Redirecting ... Login
<br>
<br>
<a href="https://ip:port/portal/PortalSetup.action?switch_url=wired">ISE Guest Portal</a>
</center>

</BODY>
</HTML>
```

カスタム ログイン ページはパブリック Web フォームであるため、次のガイドラインに従ってください。

- ログイン フォームは、ユーザによるユーザ名とパスワードの入力を受け付け、これらを **uname** および **pwd** として示す必要があります。
- カスタム ログイン ページは、ページ タイムアウト、パスワード非表示、冗長送信の防止など、Web フォームに対するベスト プラクティスに従う必要があります。

NAD での HTTPS サーバの有効化

Web ベース認証を使用するには、**ip http secure-server** コマンドを使用してスイッチ内で HTTPS サーバを有効にする必要があります。

NAD 上でのカスタマイズされた認証プロキシ Web ページのサポート

成功、失効、失敗に関するカスタム ページを NAD にアップロードできます。Cisco ISE では特定のカスタマイズは必要ないため、NAD に付属する標準の設定手順を使用して、これらのページを作成できます。

NAD の Web 認証の設定

デフォルトの HTML ページをカスタム ファイルで置き換えて、NAD における Web 認証を完了する必要があります。

始める前に

Web ベースの認証中、スイッチのデフォルト HTML ページの代わりに使用する 4 つの代替 HTML ページを作成します。

ステップ 1 カスタム認証プロキシ Web ページを使用するように指定するには、最初にカスタム HTML ファイルをスイッチのフラッシュ メモリに格納します。スイッチのフラッシュ メモリに HTML ファイルをコピーするには、スイッチで次のコマンドを実行します。

copy tftp/ftp flash

ステップ 2 スイッチに HTML ファイルをコピーした後、グローバル コンフィギュレーション モードで次のコマンドを実行します。

a.	ip admission proxy http login page file device:login-filename	スイッチのメモリ ファイルシステム内で、デフォルトのログイン ページの代わりに使用するカスタム HTML ファイルの場所を指定します。device: はフラッシュ メモリです。
b.	ip admission proxy http success page file device:success-filename	デフォルトのログイン成功ページの代わりに使用するカスタム HTML ファイルの場所を指定します。
c.	ip admission proxy http failure page file device:fail-filename	デフォルトのログイン失敗ページの代わりに使用するカスタム HTML ファイルの場所を指定します。
d.	ip admission proxy http login expired page file device:expired-filename	デフォルトのログイン失効ページの代わりに使用するカスタム HTML ファイルの場所を指定します。

ステップ 3 スイッチによって提供されるガイドラインに従って、カスタマイズされた認証プロキシ Web ページを設定します。

ステップ 4 次の例に示すように、カスタム認証プロキシ Web ページの設定を確認します。

```
Switch# show ip admission configuration
Authentication proxy webpage
Login page           : flash:login.htm
```

```
Success page      : flash:success.htm
Fail Page        : flash:fail.htm
Login expired Page : flash:expired.htm

Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication global init state time is 2 minutes
Authentication Proxy Session ratelimit is 100
Authentication Proxy Watch-list is disabled
Authentication Proxy Auditing is disabled
Max Login attempts per user is 5
```

デバイス登録 WebAuth プロセス

デバイス登録 Web 認証（デバイス登録 WebAuth）およびホットスポット ゲスト ポータルを使用すると、ユーザ名とパスワードを要求しないで、プライベートネットワークへの接続をゲスト デバイスに許可できます。

このシナリオでは、ゲストは無線接続でネットワークに接続します。デバイス登録 WebAuth プロセス フローの例については、[図 38: ワイヤレス デバイス登録 Web 認証フロー](#)を参照してください。後続のデバイス登録 WebAuth プロセスの概要を次に説明します。無線接続と有線接続の両方で同様のプロセスとなります。

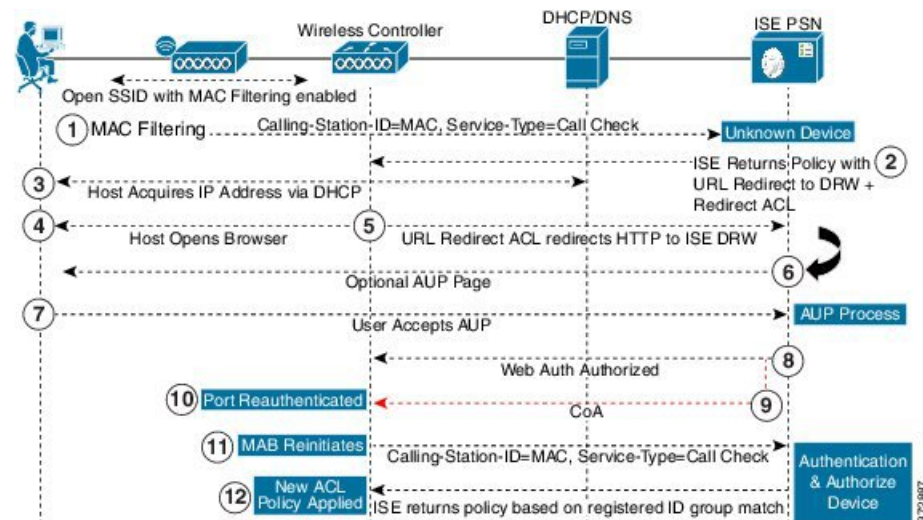
1. ネットワーク アクセス デバイス（NAD）がホットスポット ゲスト ポータルにリダイレクトを送信します。
2. ゲスト デバイスの MAC アドレスがいずれのエンドポイント ID グループにも含まれていないか、利用規定（AUP）accepted 属性が true に設定されていない場合、Cisco ISE は許可プロファイルに指定された URL リダイレクションを使用して応答します。
3. ゲストが何らかの URL にアクセスしようとする、URL リダイレクションによって AUP ページ（有効な場合）が表示されます。
 - ゲストが AUP を受け入れると、デバイスの MAC アドレスに関連付けられたエンドポイントが、設定されたエンドポイント ID グループに割り当てられます。ゲストによる AUP の受け入れを追跡できるよう、この時点で、このエンドポイントの AUP accepted 属性は true に設定されます。
 - ゲストが AUP を受け入れない場合、または、エンドポイントの作成中や更新中などにエラーが発生した場合、エラー メッセージが表示されます。
4. ホットスポット ゲスト ポータルの設定に基づいて、追加情報を含むポスト アクセス バナー ページが表示される場合があります（有効な場合）。
5. エンドポイントが作成または更新された後、許可変更（CoA）終了が NAD に送信されます。
6. CoA の後、NAD は MAC 認証バイパス（MAB）の新しい要求でゲスト接続を再認証します。新規認証では、エンドポイントとそれに関連付けられているエンドポイント ID グループが検索され、設定されているアクセスが NAD に返されます。

7. ホットスポットゲストポータルの設定に基づいて、ゲストは、アクセスを要求した URL、管理者が指定したカスタム URL、または認証の成功ページに誘導されます。

有線とワイヤレスのどちらの場合も、CoA タイプは Termination CoA です。VLAN DHCP リリース（および更新）を実行するようにホットスポットゲストポータルを設定し、それによって、有線と無線の両方の CoA タイプを許可変更に再許可できます。

VLAN DHCP リリースのサポートは、デスクトップデバイスの Mac OS と Windows でのみ使用可能です。モバイルデバイスでは利用できません。登録するデバイスがモバイルで、[VLAN DHCP リリース (VLAN DHCP Release)] オプションが有効の場合、ゲストは手動で IP アドレスを更新することを要求されます。モバイルデバイスのユーザの場合は、VLAN を使用するよりも、WLC でアクセス コントロール リスト (ACL) を使用することを推奨します。

図 38: ワイヤレス デバイス登録 Web 認証フロー





第 17 章

デバイス アクセスのサポート

- [企業ネットワークのパーソナル デバイス \(BYOD\) \(583 ページ\)](#)
- [パーソナル デバイス ポータル \(585 ページ\)](#)
- [ネイティブ サプリカントを使用したデバイス登録のサポート \(592 ページ\)](#)
- [デバイス ポータルの設定タスク \(593 ページ\)](#)
- [従業員が追加するパーソナル デバイスの管理 \(610 ページ\)](#)
- [デバイス ポータルおよびエンドポイント アクティビティのモニタ \(611 ページ\)](#)

企業ネットワークのパーソナル デバイス (BYOD)

企業ネットワーク上のパーソナル デバイスをサポートする場合は、ユーザ（従業員、請負業者、およびゲスト）とそのデバイスを認証および許可することで、ネットワーク サービスおよび企業データを保護する必要があります。Cisco ISE は、従業員が企業ネットワーク上でパーソナル デバイスを安全に使用できるようにするために必要なツールを提供します。

ゲストは、ゲストポータルへのログイン時に、自動的に自分のデバイスを登録することができます。ゲストは、ゲストタイプに定義されている最大数まで追加デバイスを登録できます。これらのデバイスは、ポータル構成に基づいてエンドポイント ID グループに登録されます。

ゲストは、ネイティブ サプリカント プロビジョニング (Network Setup Assistant) を実行するか、またはデバイスを [デバイス (My Devices)] ポータルに追加して、パーソナル デバイスをネットワークに追加できます。オペレーティングシステムに基づいて、使用する適切なネイティブ サプリカント プロビジョニング ウィザードを決定するネイティブ サプリカント プロファイルを作成できます。

ネイティブ サプリカント プロファイルはすべてのデバイスで利用できるわけではないため、ユーザはデバイスポータルを使用してこれらのデバイスを手動で追加することができます。または、これらのデバイスを登録するように BYOD ルールを設定できます。

ISE コミュニティ リソース

[How To: ISE and BYOD - Onboarding, Registering, and Provisioning](#)

[How To: ISE and BYOD - Using Certificates for Differentiated Access](#)

分散環境のエンドユーザのデバイス ポータル

Cisco ISE のエンドユーザ Web ポータルは、管理ペルソナ、ポリシー サービス ペルソナ、およびモニタリング ペルソナに基づき、設定、セッション サポート、およびレポート作成を提供します。

- **管理ノード**：ユーザ、デバイス、およびエンドユーザ ポータルが管理ノードに書き込まれる構成の変更。
- **ポリシー サービス ノード**：エンドユーザ ポータルはポリシー サービス ノードで実行する必要があります。ここでは、ネットワーク アクセス、クライアント プロビジョニング、ゲスト サービス、ポスチャ、およびプロファイリングを含むすべてのセッション トラフィックが処理されます。ポリシー サービス ノードがノード グループに含まれる場合、1 つのノードで障害が発生すると、他のノードが障害を検出し、保留中のセッションをリセットします。
- **モニタリング ノード**：モニタリング ノードは、デバイス ポータル、スポンサー ポータル、およびゲスト ポータルでのエンドユーザおよびデバイスのアクティビティについて、データを収集、集約、およびレポートします。プライマリ モニタリング ノードで障害が発生した場合は、セカンダリ モニタリング ノードが自動的にプライマリ モニタリング ノードになります。

デバイス ポータルのグローバル設定

[ワーク センター (Work Centers)] > [BYOD] > [設定 (Settings)] > [従業員が登録するデバイス (Employee Registered Devices)] または [管理 (Administration)] > [デバイス ポータルの管理 (Device Portal Management)] > [設定 (Settings)] を選択します。

BYOD ポータルおよびデバイス ポータルの次の一般設定を設定できます。

- [従業員が登録するデバイス (Employee Registered Devices)] : [従業員を制限 (Restrict employees to)] に、従業員が登録できるデバイスの最大数を入力します。デフォルトでは、この値は 5 デバイスに設定されています。
- [再試行 URL (Retry URL)] : デバイスを Cisco ISE にリダイレクトするために使用できる URL を [オンボードのための再試行 URL (Retry URL for onboarding)] に入力します。

これらの一般的な設定値を設定したら、これらの設定は会社を設定したすべて BYOD ポータルおよびデバイス ポータルに適用されます。

関連トピック

[従業員が登録するパーソナル デバイス数の制限](#)

[BYOD 登録に再接続する URL の提供](#) (593 ページ)

[分散環境のエンドユーザのデバイス ポータル](#) (584 ページ)

パーソナル デバイス ポータル

Cisco ISE では、従業員が所有するパーソナル デバイスをサポートするために複数の Web ベース ポータルが提供されています。これらのデバイス ポータルは、ゲスト ポータル フローまたはスポンサー ポータル フローには関与しません。

次のポータルを使用します。

- **ブラックリスト ポータル**：「ブラックリスト」に掲載されているためネットワーク アクセスには使用できないパーソナル デバイスに関する情報を提供します。
- **BYOD ポータル**：従業員がネイティブ サプリカント プロビジョニング機能を使用して自分のパーソナル デバイスを登録できるようにします。
- **証明書プロビジョニング ポータル**：管理者および従業員が BYOD フローを通過できないデバイスについてユーザ/デバイス証明書を要求できるようにします。
- **クライアントプロビジョニングポータル**：コンプライアンスをチェックするポスチャエージェントを自分のデバイスにダウンロードするよう従業員に強制します。
- **MDM ポータル**：従業員が外部のモバイル デバイス管理 (MDM) システムに自分のモバイル デバイスを登録できるようにします。
- **デバイス ポータル**：従業員がパーソナル デバイス (ネイティブ サプリカント プロビジョニングをサポートしないデバイスを含む) を追加および登録し、管理できるようにします。

Cisco ISE には、事前定義済みのデフォルト ポータルのセットを含む複数のデバイス ポータルを Cisco ISE サーバでホストする機能が用意されています。デフォルトのポータル テーマには、管理者ポータルからカスタマイズできる標準のシスコブランドが適用されています。組織に固有のイメージ、ロゴ、およびカスケーディング スタイルシート (CSS) ファイルをアップロードして、ポータルをさらにカスタマイズすることもできます。

デバイス ポータルへのアクセス

ステップ 1 デバイス ポータルへのアクセスには、次のいずれかを実行します。

- **[管理 (Administration)] > [デバイスポータル管理 (Device Portal Management)]** をクリックします。
[デバイス ポータルの設定およびカスタマイズ (Configure and Customize Device Portals)] ページには、サポートされるデバイス ポータルのリストが表示されます。
- **[管理 (Administration)] > [デバイス ポータル管理 (Device Portal Management)]** を選択します。ドロップダウン メニューにサポートされるデバイス ポータルが表示されます。

ステップ 2 設定する特定のデバイス ポータルを選択します。

ブラックリスト ポータル

従業員は、このポータルに直接アクセスするのではなく、このポータルにリダイレクトされます。

従業員が自分のパーソナル デバイスを紛失したり盗まれたりした場合、デバイス ポータルでデバイスのステータスを更新して、ブラックリスト エンドポイント ID グループにデバイスを追加できます。これにより、不正なネットワーク アクセスにデバイスが使用されることを防ぎます。誰かがこれらのデバイスの1つを使用してネットワークに接続しようとする、ブラックリスト ポータルにリダイレクトされ、デバイスがネットワークへのアクセスを拒否することが通知されます。デバイスが見つかった場合、従業員はデバイス ポータルでデバイスを復元し、デバイスを再登録せずにネットワークアクセスを回復できます。デバイスの盗難か紛失かによっては、デバイスをネットワークに接続する前に、追加のプロビジョニングが必要になる場合があります。

ブラックリスト ポータルのポート設定（デフォルトはポート 8444）を設定できます。ポート番号を変更する場合は、別のエンドユーザポータルで使用されていないことを確認してください。

ブラックリスト ポータルの設定については、[ブラックリストポータルの編集（598ページ）](#)を参照してください。

証明書プロビジョニング ポータル

従業員は、証明書プロビジョニング ポータルに直接アクセスできます。

証明書プロビジョニング ポータルでは、従業員はオンボーディング フローを通過できないデバイスについて証明書を要求することができます。たとえば、販売時点管理端末などのデバイスは、BYOD フローを通過できず、証明書を手動で発行する必要があります。証明書プロビジョニングポータルで、権限のある一連のユーザは、そのようなデバイスに対する証明書要求をアップロードし、キー ペアを生成し（必要に応じて）、証明書をダウンロードできます。

従業員は、このポータルにアクセスして、1つの証明書について要求を行うか、または CSV ファイルを使用して一括証明書要求を行うことができます。

ISE コミュニティ リソース

Identity Services Engine 証明書プロビジョニングポータルの機能と設定については、「[ISE 2.0: Certificate Provisioning Portal](#)」を参照してください。

個人所有デバイスの持ち込みポータル

従業員は、このポータルに直接アクセスしません。

従業員は、ネイティブ サプリカントを使用してパーソナル デバイスを登録すると、個人所有デバイスの持ち込み（BYOD）ポータルにリダイレクトされます。従業員がパーソナルデバイスを使用して初めてネットワークにアクセスを試みると、手動でNetwork Setup Assistant（NSA）ウィザードをダウンロードして起動するように求められ、ネイティブサプリカントの登録および

びインストールに進む場合があります。デバイスを登録すると、デバイス ポータルを使用して、それを管理できます。



- (注) BYOD フローは、デバイスが AnyConnect Network Access Manager (NAM) を使用してネットワークに接続すると、サポートされません。

関連トピック

[BYOD ポータルの作成](#) (600 ページ)

[企業ネットワークのパーソナル デバイス \(BYOD\)](#) (583 ページ)

クライアント プロビジョニング ポータル

従業員は、このポータルに直接アクセスするのではなく、このポータルにリダイレクトされます。

クライアント プロビジョニング システムでは、企業ネットワークにアクセスしようとしているデバイスのポスチャ評価および修復を行います。従業員がデバイスを使用してネットワークアクセスを要求したときに、クライアント プロビジョニング ポータルにルーティングして、最初にポスチャ エージェントをダウンロードするように要求できます。ポスチャ エージェントは、デバイスにアンチウイルス ソフトウェアがインストールされていることや、オペレーティングシステムがサポートされていることの確認など、コンプライアンスに関するデバイスのスキャンを行います。

関連トピック

[クライアント プロビジョニング ポータルの作成](#) (603 ページ)

モバイル デバイス 管理ポータル

従業員は、このポータルに直接アクセスするのではなく、このポータルにリダイレクトされます。

数多くの会社で、従業員のモバイル デバイスを管理するために、モバイル デバイス管理 (MDM) システムを使用しています。

Cisco ISE では外部 MDM システムとの統合が許可されており、従業員はこれを使用して、モバイルデバイスを登録し、企業ネットワークにアクセスすることができます。シスコでは、従業員がデバイスを登録し、ネットワークに接続するために使用できる外部 MDM インターフェイスを提供しています。

MDM ポータルを使用することで、従業員は外部 MDM システムに登録できます。

従業員は、デバイス ポータルを使用して、PIN コードでのデバイスのロック、工場出荷時のデフォルト設定へのデバイスのリセット、デバイス登録時にインストールされていたアプリケーションおよび設定の削除など、モバイル デバイスの管理を行うことができます。

Cisco ISE では、すべての外部 MDM システム用に単一の MDM ポータルを、または個々の MDM システムごとに 1 つのポータルを使用できます。

MDM サーバを ISE とともに動作するように設定する方法については、[MDM ポータルの作成 \(605 ページ\)](#) を参照してください。

デバイス ポータル

従業員は、デバイス ポータルに直接アクセスできます。

ネットワーク アクセスが必要な一部のネットワーク デバイスは、ネイティブ サプリカント プロビジョニングでサポートされていないため、BYOD ポータルを使用して登録することができません。ただし、従業員は、オペレーティング システムがサポートされていないか、Web ブラウザが搭載されていないパーソナル デバイス（プリンタ、インターネット ラジオ、その他のデバイスなど）を、デバイス ポータルを使用して追加および登録することができます。

従業員は、デバイスの MAC アドレスを入力して、新しいデバイスを追加および管理できます。従業員が、デバイス ポータルを使用してデバイスを追加すると、Cisco ISE はそのデバイスを **RegisteredDevices** エンドポイント ID グループのメンバーとして、[エンドポイント (Endpoints)] ページに追加します（別のエンドポイント ID グループに、すでに静的に割り当てられている場合を除く）。デバイスは、Cisco ISE の他のエンドポイントと同様にプロファイリングされ、ネットワーク アクセスのための登録プロセスが行われます。

1 つのデバイスからの 2 つの MAC アドレスがユーザによりデバイス ポータルに入力されると、それらが同じホスト名を持ち、ISE で 1 つのエントリとして統合されていることがプロファイリングによって設定されます。たとえば、ユーザは有線および無線のアドレスでラップトップを登録します。そのデバイス上での削除などの操作は、両方のアドレスで機能します。

登録済みデバイスがポータルから削除されると、デバイス登録状態属性と BYOD 登録状態属性は、それぞれ [未登録 (NotRegistered)] および [いいえ (No)] に変更されます。ただし、これらの属性は、従業員のデバイス登録時にのみ使用される BYOD 属性であるため、ゲスト（従業員以外）がクレデンシャルを持つゲストポータルの [ゲストデバイス登録 (Guest Device Registration)] ページを使用してデバイスを登録した場合は、変更されずそのままになります。

従業員は、BYOD またはデバイス ポータルを使用して自分のデバイスを登録しているかどうかに関係なく、デバイス ポータルを使用してそれらを管理できます。



(注) 管理者ポータルがダウンしている場合、デバイス ポータルは使用できません。

関連トピック

[デバイス ポータルの作成 \(607 ページ\)](#)

BYOD の展開オプションとステータス ワークフロー

パーソナルデバイスをサポートする BYOD 展開フローは、次の要因によって若干異なります。

- シングルまたはデュアル SSID：シングル SSID の場合は、証明書の登録、プロビジョニング、およびネットワーク アクセスに同じ WLAN が使用されます。デュアル SSID 展開では、2 つの SSID があります。1 つは登録およびプロビジョニングを提供し、もう 1 つはセキュアなネットワーク アクセスを提供します。
- Windows、MacOS、iOS、または Android デバイス：ネイティブ サプリカントのフローは、サポートされているパーソナル デバイスを利用する従業員を BYOD ポータルにリダイレクトしてこれらのデバイス情報を確認することによって、デバイスのタイプに関係なく、同様に開始します。プロセスはデバイス タイプに応じて分岐します。

従業員がネットワークに接続する

1. 従業員のクレデンシャルが認証される：Cisco ISE は、社内 Active Directory または社内の他の ID ストアと照合して従業員を認証し、許可ポリシーを提供します。
2. デバイスが BYOD ポータルにリダイレクトされる：デバイスが BYOD ポータルにリダイレクトされます。デバイスの [MAC アドレス (MAC address)] フィールドは自動的に事前設定されます。ユーザはデバイス名と説明を追加できます。
3. ネイティブ サプリカントが設定される (MacOS、Windows、iOS、Android)：ネイティブ サプリカントが設定されます。ただしこのプロセスはデバイスに応じて異なります。
 - MacOS および Windows デバイス：従業員が BYOD ポータルで [登録 (Register)] をクリックして、サプリカントプロビジョニングウィザード (Network Setup Assistant) をダウンロードしてインストールします。このウィザードではサプリカントが設定され、EAP-TLS 証明書ベース認証に使用する証明書が (必要に応じて) 提供されます。デバイスの MAC アドレスと従業員のユーザ名が発行済み証明書に組み込まれます。



(注) Network Setup Assistant は、そのデバイスのユーザが管理者権限を持っていない限り、Windows デバイスにダウンロードすることはできません。エンドユーザに管理者権限を与えることができない場合は、BYOD フローを使用するのではなく、GPO を使用して証明書をユーザのデバイスにプッシュします。

- iOS デバイス：Cisco ISE ポリシー サーバは Apple の iOS ワイヤレス機能を使用して新しいプロファイルを IOS デバイスに送信します。このプロファイルには次の情報が含まれます。
 - 発行済み証明書 (設定されている場合) には iOS デバイスの MAC アドレスと従業員のユーザ名が組み込まれます。
 - 802.1X 認証の EAP-TLS の使用を強制できる Wi-Fi サプリカント プロファイル。
- Android デバイス：Cisco ISE は、従業員に Google Play ストアから Cisco Network Setup Assistant (NSA) をダウンロードするように要求し、ルーティングします。アプリのインストール後に、従業員は NSA を開いてセットアップウィザードを開始できます。

このウィザードでは、サブリカントの設定と、デバイスの設定に使用される発行済み証明書が生成されます。

4. **認可変更が発行される**：ユーザがオンボーディング フローを通過すると、Cisco ISE は認可変更 (CoA) を開始します。これにより、MacOS X、Windows、および Android デバイスはセキュアな 802.1X ネットワークに再接続します。シングル SSID の場合、iOS デバイスも自動的に接続されますが、デュアル SSID の場合、ウィザードは iOS ユーザに手動で新しいネットワークに接続するように要求します。



- (注) サブリカントを使用しない BYOD フローを設定できます。Cisco ISE コミュニティの資料 (<https://supportforums.cisco.com/blog/12705471/ise-byod-registration-only-without-native-supplciant-or-certificate-provisioning>) を参照してください。



- (注) [ターゲットネットワークが非表示になっている場合に有効にする (Enable if Target Network is Hidden)] チェック ボックスをオンにするのは、実際の Wi-Fi ネットワークが非表示の場合に限ります。そうしないと、特にシングル SSID フロー (同じ Wi-Fi ネットワーク/SSID がオンボーディングと接続の両方に使用されている) の特定の iOS デバイスに対して Wi-Fi ネットワーク設定が適切にプロビジョニングされない場合があります。

BYOD セッション エンドポイント属性

エンドポイント属性 *BYODRegistration* の状態は、BYOD フローにおいて次の状態に変化します。

- *Unknown*：デバイスが BYOD フローを通過していません。
- *Yes*：デバイスは BYOD フローを通過し、登録されました。
- *No*：デバイスが BYOD フローを通過しましたが、登録されていません。つまり、デバイスは削除されています。

デバイス登録ステータスのエンドポイント属性

エンドポイント属性 *DeviceRegistrationStatus* の状態は、デバイス登録中に次の状態に変化します。

- *Registered*：デバイスは BYOD フローを通過し、登録されました。この属性が *Pending* から *Registered* になるまでに 20 分の遅れがあります。
- *Pending*：デバイスは BYOD フローを通過し、登録されました。ただし、ISE はネットワーク上でこのデバイスを認識していません。

- *Not Registered* : デバイスが BYOD フローを通過していません。これは、この属性のデフォルト状態です。
- *Stolen* : ユーザがデバイス ポータルにログインし、現在オンボーディングされているデバイスを *Stolen* としてマークしました。この状況が発生した場合は次のような処理が行われます。
 - 証明書とプロファイルをプロビジョニングしてデバイスのオンボーディングが行われた場合、ISE はそのデバイスに対してプロビジョニングされた証明書を失効させ、デバイスの MAC アドレスを **ブラックリスト ID グループ**に割り当てます。そのデバイスはネットワークにアクセスできなくなります。
 - (証明書は含めず) プロファイルのみをプロビジョニングしてデバイスのオンボーディングが行われた場合、ISE はそのデバイスを **ブラックリスト エンドポイント ID グループ**に割り当てます。この状況に対応する許可ポリシーを作成していない場合は、デバイスは引き続きネットワークにアクセスできます。たとえば、**IF Endpoint Identity Group is Blacklist AND BYOD_is_Registered THEN DenyAccess** となります。

管理者は、さまざまなデバイスに対してネットワーク アクセスを無効にするアクション (証明書の削除や失効など) を行います。

ユーザが盗まれたデバイスを復元すると、ステータスは *not registered* に戻ります。ユーザはそのデバイスを削除してからもう一度追加する必要があります。これにより、オンボーディング プロセスが開始されます。

- *Lost* : ユーザがデバイス ポータルにログオンし、現在オンボーディングされているデバイスを *Lost* としてマークしました。これにより、次のアクションが実行されます。
 - そのデバイスは **ブラックリスト ID グループ**に割り当てられます。
 - デバイスに対してプロビジョニングされた証明書は失効します。
 - デバイスのステータスが *Lost*. に更新されます。
 - 「BYODRegistration」が *No* に更新されます。

紛失デバイスをブロックする許可ポリシーを作成していない場合、紛失デバイスは引き続きネットワークにアクセスできます。ルールで **ブラックリスト ID グループ**または **endpoint:BYODRegistration** 属性を使用できます。たとえば、**IF Endpoint Identity Group is Blacklist AND EndPoints:BYODRegistrations Equals No THEN BYOD** と指定できます。きめ細かなアクセスを設定するには、**NetworkAccess:EAPAuthenticationMethod Equals PEAP or EAP-TLS or EAP-FAST**” , **InternalUser:IdentityGroup Equals <<group>>** をルールの IF 部分に追加することもできます。

ネイティブ サプリカントを使用したデバイス登録のサポート

ネイティブ サプリカント プロファイルを作成して、Cisco ISE ネットワークでパーソナル デバイスをサポートできます。ユーザの許可要件に関連付けるプロファイルに基づいて、Cisco ISE はネットワークにアクセスするユーザのパーソナル デバイスをセットアップするために必要な サプリカント プロビジョニング ウィザードを提供します。

従業員がパーソナル デバイスを使用して初めてネットワークへのアクセスを試みると、登録および サプリカントの設定の手順が自動的に示されます。デバイスを登録した後、デバイス ポータルを使用してデバイスを管理できます。

ネイティブ サプリカントがサポートするオペレーティング システム

ネイティブ サプリカントは、次のオペレーティング システムでサポートされます。

- Android (Amazon Kindle、B&N Nook を除く)
- Mac OS X (Apple Mac コンピュータの場合)
- Apple iOS デバイス (Apple iPod、iPhone、および iPad)
- Microsoft Windows 7、8 (RT を除く)、Vista、および 10

クレデンシャルを持つゲスト ポータルを使用したパーソナル デバイスの登録を従業員に許可

クレデンシャルを持つゲスト ポータルを利用している従業員は、自分のパーソナル デバイスを登録できます。BYOD ポータルによって提供されるセルフプロビジョニングフローにより、従業員は Windows、MacOS、iOS および Android デバイスで使用可能なネイティブ サプリカントを使用してネットワークにデバイスを直接接続できます。

始める前に

ネイティブ サプリカント プロファイルを作成する必要があります。

-
- ステップ 1** [ワーク センター (Work Center)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [ゲスト ポータル (Guest Portals)] を選択します。
- ステップ 2** 従業員がネイティブ サプリカントを使用して自分のデバイスを登録するために使用できるクレデンシャルを持つゲスト ポータルを選択し、[編集 (Edit)] をクリックします。
- ステップ 3** [ポータルの動作およびフローの設定 (Portal Behavior and Flow Settings)] タブおよび [BYOD 設定 (BYOD Settings)] で、[従業員にネットワークでのパーソナル デバイスの使用を許可する (Allow employees to use personal devices on the network)] をオンにします。

ステップ 4 [保存 (Save)] をクリックし、[閉じる (Close)] をクリックします。

BYOD 登録に再接続する URL の提供

BYOD ポータルを使用してパーソナル デバイスを登録中に問題が発生した従業員に、登録プロセスへの再接続を可能にする情報を提供できます。

ステップ 1 [管理 (Administration)] > [デバイス ポータル管理 (Device Portal Management)] > [設定 (Settings)] > [再試行 URL (Retry URL)] を選択します。

ステップ 2 IP アドレスを変更するか、またはデバイスを Cisco ISE にリダイレクトするために使用できる URL を [オンボードのための再試行 URL (Retry URL for onboarding)] に入力します。

登録プロセス中に従業員のデバイスに問題が発生した場合、デバイスはインターネットに自動的に再接続しようとします。この時点で、ここに入力する IP アドレスまたはドメイン名がデバイスを Cisco ISE にリダイレクトし、オンボーディングプロセスが再開されます。デフォルト値は 1.1.1.1 です。

ステップ 3 [保存 (Save)] をクリックします。設定の更新を保存しない場合は、[リセット (Reset)] をクリックして、最後に保存した値に戻します。

デバイス ポータルの設定タスク

デフォルトポータルと、証明書、エンドポイント ID グループ、ID ソース順序、ポータルテーマ、イメージ、および Cisco ISE によって提供されるその他の詳細などのデフォルト設定を使用できます。デフォルト設定を使用しない場合は、新しいポータルを作成するか、必要性に合うように既存の設定を編集する必要があります。同じ設定で複数のポータルを作成する場合は、ポータルを複製できます。

新しいポータルを作成したり、デフォルトポータルを編集した後は、ポータルの使用を承認する必要があります。いったんポータルの使用を承認すると、後続の設定変更はただちに有効になります。

デバイス ポータルを使用するための許可は必要ありません。

ポータルを削除する場合は、関連付けられている許可ポリシールールおよび許可プロファイルを先に削除するか、別のポータルを使用するように変更する必要があります。

この表を使用して、異なるデバイス ポータルの設定に関連するタスクを確認できます。

タスク	ブラックリスト ポータル	BYOD ポータル	クライアント プロビジョニング ポータル	MDM ポータル	デバイス ポータル
ポリシー サービスの有効化 (595 ページ)	必須 (Required)	必須 (Required)	必須 (Required)	必須 (Required)	必須 (Required)
証明書の追加 (595 ページ)	必須 (Required)	必須 (Required)	必須 (Required)	必須 (Required)	必須 (Required)
外部 ID ソースの作成 (596 ページ)	不要	不要	不要	不要	必須 (Required)
ID ソース順序の作成 (596 ページ)	不要	不要	不要	不要	必須 (Required)
エンドポイント ID グループの作成 (597 ページ)	不要	必須 (Required)	不要	必須 (Required)	必須 (Required)
ブラックリスト ポータルの編集 (598 ページ)	必須 (Required)	N/A	N/A	N/A	N/A
BYOD ポータルの作成 (600 ページ)	N/A	必須 (Required)	N/A	N/A	N/A
クライアント プロビジョニング ポータルの作成 (603 ページ)	N/A	N/A	必須 (Required)	N/A	N/A
MDM ポータルの作成 (605 ページ)	N/A	N/A	N/A	必須 (Required)	N/A
デバイス ポータルの作成 (607 ページ)	N/A	N/A	N/A	N/A	必須 (Required)

タスク	ブラックリスト ポータル	BYOD ポータル	クライアント プロビジョニング ポータル	MDM ポータル	デバイス ポータル
許可プロファイルの作成 (608 ページ)	N/A	必須 (Required)	必須 (Required)	必須 (Required)	不要
デバイス ポータルのカスタマイズ (610 ページ)	オプション	オプション	オプション	オプション	オプション

ポリシー サービスの有効化

Cisco ISE エンドユーザ Web ポータルをサポートするには、ホストするノードでポータル ポリシー サービスを有効にする必要があります。

-
- ステップ 1** [管理 (Administration)] > [システム (System)] > [展開 (Deployment)] を選択します。
- ステップ 2** ノードをクリックして、[編集 (Edit)] をクリックします。
- ステップ 3** [全般設定 (General Settings)] タブで、[ポリシー サービス (Policy Service)] をオンにします。
- ステップ 4** [セッション サービスの有効化 (Enable Session Services)] オプションをオンにします。
- ステップ 5** [保存 (Save)] をクリックします。
-

証明書の追加

デフォルトの証明書を使用しない場合は、有効な証明書を追加して、証明書グループタグに割り当てることができます。すべてのエンドユーザ Web ポータルに使用されるデフォルトの証明書グループタグは [デフォルト ポータル証明書グループ (Default Portal Certificate Group)] です。

-
- ステップ 1** [管理 (Administration)] > [システム (System)] > [証明書 (Certificates)] > [システム証明書 (System Certificates)] を選択します。
- ステップ 2** システム証明書を追加し、ポータルに使用する証明書グループタグに割り当てます。
この証明書グループタグは、ポータルを作成または編集するときに選択できるようになります。
- ステップ 3** [管理 (Administration)] > [デバイス ポータル管理 (Device Portal Management)] > (任意のポータル) > [作成または編集 (Create or Edit)] > [ポータル設定 (Portal Settings)] を選択します。

ステップ 4 新しく追加された証明書に関連付けられた [証明書グループ タグ (Certificate Group Tag)] ドロップダウンリストから特定の証明書グループ タグを選択します。

外部 ID ソースの作成

Cisco ISE では、Active Directory、LDAP、RADIUS トークン、RSA SecurID サーバなどの外部 ID ソースに接続して、認証/許可のユーザ情報を取得できます。外部 ID ソースには、証明書ベースの認証に必要な証明書認証プロファイルも含まれています。



(注) 認証済みユーザ ID を受信して共有できるようにするパッシブ ID サービスを使用するには、[その他のパッシブ ID サービスプロバイダー \(433 ページ\)](#) を参照してください。

ステップ 1 [管理 (Administration)] > [ID の管理 (Identity Management)] > [外部 ID ソース (External Identity Sources)] を選択します。

ステップ 2 次のオプションのいずれかを選択します。

- [証明書認証プロファイル (Certificate Authentication Profile)] : 証明書ベースの認証の場合。
- [Active Directory] : 外部 ID ソースとして Active Directory に接続する場合 (詳細は [外部 ID ソースとしての Active Directory \(379 ページ\)](#) を参照)。
- [LDAP] : LDAP ID ソースを追加する場合 (詳細は [LDAP \(482 ページ\)](#) を参照)。
- [RADIUS トークン (RADIUS Token)] : RADIUS トークン サーバを追加する場合 (詳細は [RADIUS トークン ID ソース \(499 ページ\)](#) を参照)。
- [RSA SecurID] : RSA SecurID サーバを追加する場合 (詳細は [RSA ID ソース \(504 ページ\)](#) を参照)。
- [SAML ID プロバイダー (SAML Id Providers)] : Oracle Access Manager などの ID プロバイダー (IdP) を追加する場合 (詳細は [外部 ID ソースとしての ID プロバイダ \(14 ページ\)](#) を参照)。

ID ソース順序の作成

始める前に

Cisco ISE に外部 ID ソースを設定していることを確認します。

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ゲスト ユーザがローカル WebAuth を使用して認証できるようにするには、ゲスト ポータル認証ソースと ID ソース順序に同じ ID ストアが含まれるように設定する必要があります。

ステップ 1 [管理 (Administration)] > [ID の管理 (Identity Management)] > [ID ソース順序 (Identity Source Sequences)] > [追加 (Add)] を選択します。

ステップ 2 ID ソース順序の名前を入力します。また、任意で説明を入力できます。

ステップ 3 [証明書認証プロファイル (Certificate Authentication Profile)] チェックボックスをオンにし、証明書ベースの認証のための証明書認証プロファイルを選択します。

ステップ 4 [選択済み (Selected)] リスト ボックスの ID ソース順序に含めるデータベースを選択します。

ステップ 5 Cisco ISE がデータベースを検索する順序に [選択済み (Selected)] リストのデータベースを並べ替えます。

ステップ 6 [高度な検索リスト (Advanced Search List)] 領域で、次のいずれかのオプションを選択します。

- [順序内の他のストアにアクセスせず、AuthenticationStatus 属性を ProcessError に設定 (Do not access other stores in the sequence and set the AuthenticationStatus attribute to ProcessError)] : 最初に選択された ID ソースでユーザが見つからないとき、Cisco ISE が検索を中止する場合。
- [ユーザが見つからなかったとして処理し、順序内の次のストアに進む (Treat as if the user was not found and proceed to the next store in the sequence)] : 最初に選択された ID ソースでユーザが見つからないとき、Cisco ISE が順序内の他の選択された ID ソースの検索を続行する場合。

Cisco ISE では、要求の処理中にこれらの ID ソースが順番に検索されます。[選択済み (Selected)] リストに、Cisco ISE が ID ソースを検索する順序で ID ソースが表示されていることを確認します。

ステップ 7 [送信 (Submit)] をクリックして ID ソース順序を作成すると、その後この ID ソース順序をポリシーで使用できます。

エンドポイント ID グループの作成

Cisco ISE では、検出したエンドポイントを、対応するエンドポイント ID グループにグループ化します。Cisco ISE では、システム定義された複数のエンドポイントの ID グループが事前に用意されています。[エンドポイント ID グループ (Endpoint Identity Groups)] ページで追加のエンドポイント ID グループを作成することもできます。作成したエンドポイント ID グループを編集または削除できます。システム定義されたエンドポイント ID グループの説明のみを編集できます。これらのグループの名前を編集したり、これらのグループを削除したりすることはできません。

ステップ 1 [管理 (Administration)] > [ID の管理 (Identity Management)] > [グループ (Groups)] > [エンドポイント ID グループ (Endpoint Identity Groups)] を選択します。

ステップ 2 [追加 (Add)] をクリックします。

ステップ 3 作成するエンドポイント ID グループの名前を入力します (エンドポイント ID グループの名前にスペースを入れないでください)。

ステップ 4 作成するエンドポイント ID グループの説明を入力します。

ステップ 5 [親グループ (Parent Group)] ドロップダウン リストをクリックして、新しく作成したエンドポイント ID グループを関連付けるエンドポイント ID グループを選択します。

ステップ 6 [送信 (Submit)] をクリックします。

ブラックリスト ポータルの編集

Cisco ISE では、Cisco ISE でブラックリストに登録されている紛失したり、盗難にあったりしたデバイスが企業ネットワークへのアクセスを試行した場合に、情報が表示される単一のブラックリスト ポータルが提供されます。

デフォルトのポータル設定を編集し、ポータルについて表示されるデフォルトのメッセージをカスタマイズすることのみができます。新しいブラックリストポータルを作成することはできず、デフォルト ポータルを複製または削除することもできません。

始める前に

このポータルで使用するために、必要な証明書が設定されていることを確認します。

ステップ 1 [管理 (Administration)] > [デバイス ポータル管理 (Device Portal Management)] > [ブラックリスト ポータル (Blacklist Portal)] > [編集 (Edit)] を選択します。

ステップ 2 ポータルの一意の [ポータル名 (Portal Name)] および [説明 (Description)] を指定します。
ここで使用するポータル名が他のエンドユーザ ポータルに使用されていないことを確認します。

ステップ 3 ポータルで使用する言語ファイルをエクスポートおよびインポートするには、[言語 (Languages)] メニューを使用します。

ステップ 4 [ポータルの設定 (Portal Settings)] で証明書グループ タグ、言語などのデフォルト値を更新し、ポータル全体に適用する動作を定義します。

- [HTTPS ポート (HTTPS port)] : 8000 ~ 8999 の範囲のポート値を入力します。デフォルト値はすべてのデフォルト ポータルで 8443 です。ただし、ブラックリスト ポータルは 8444 です。この範囲外のポート値を使用してアップグレードした場合は、このページで変更を加えるまで維持されます。このページを変更する場合は、この制限に従うようにポート設定を更新します。

ゲスト ポータルに非ゲスト ポータル (マイ デバイスなど) によって使用されるポートを割り当てると、エラー メッセージが表示されます。

ポスチャ評価と修復についてのみ、クライアントプロビジョニング ポータルはポート 8905 および 8909 も使用します。それ以外の場合は、ゲスト ポータルへの割り当てと同じポートを使用します。

同じ HTTPS ポートに割り当てられたポータルは、同じギガビット イーサネット インターフェイスまたは別のインターフェイスを使用できます。これらのポータルが同じポートとインターフェイスの組み合わせを使用している場合、同じ証明書グループ タグを使用する必要があります。次に例を示します。

- スポンサー ポータルを例として使用した有効な組み合わせを次に示します。
 - スポンサー ポータル : ポート **8443**、インターフェイス **0**、証明書タグ **A**、およびデバイス ポータル : ポート **8443**、インターフェイス **0**、証明書グループ **A**
 - スポンサー ポータル : ポート **8443**、インターフェイス **0**、証明書グループ **A**、およびデバイス ポータル : ポート **8445**、インターフェイス **0**、証明書グループ **B**

- スポンサー ポータル：ポート **8444**、インターフェイス **1**、証明書グループ **A**、およびブラックリスト ポータル：ポート **8444**、インターフェイス **0**、証明書グループ **B**
 - 無効な組み合わせには次が含まれます。
 - スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**、およびデバイス ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **B**
 - スポンサー ポータル：ポート **8444**、インターフェイス **0**、証明書タグ **A**、およびブラックリスト ポータル：ポート **8444**、インターフェイス **0**、証明書グループ **A**
 - [使用可能インターフェイス (Allowed interfaces)]：PANがポータルの実行に使用できる PSN インターフェイスを選択します。ポータルを開く要求が PAN で行われると、PAN は PSN で使用可能なポートを探します。異なるサブネット上の IP アドレスを使用してイーサネットインターフェイスを設定する必要があります。
- これらのインターフェイスは、ポリシー サービスがオンになっているすべての PSN (VM ベースを含む) で使用可能である必要があります。これは、これらのすべての PSN がゲストセッションの開始時にリダイレクトに使用される可能性があるため、必須要件です。
- イーサネット インターフェイスは、異なるサブネット上の IP アドレスを使用する必要があります。
 - ここで有効にするインターフェイスは、ポリシー サービスがオンになっているときの VM ベースのものを含む、すべての PSN で使用できるものでなければなりません。これは、これらのすべての PSN がゲストセッションの開始時にリダイレクトに使用される可能性があるため必須です。
 - ポータルの証明書のサブジェクト名とサブジェクトの代替名はインターフェイス IP に解決する必要があります。
 - ISE CLI で **ip host x.x.x.x yyy.domain.com** を設定して、セカンダリ インターフェイス IP を FQDN にマッピングします。これは、証明書のサブジェクト名とサブジェクトの代替名と一致させるために使用されます。
 - ボンディングされた NIC のみが選択されている場合：PSN がポータルを設定しようとする、最初にボンディング インターフェイスを設定しようとします。これが成功しない場合、おそらくは、その PSN でボンディングが設定されていないために、PSN でエラーが記録されて終了します。PSN は物理インターフェイスでのポータルの開始を試みません。
 - **NIC チーミング**またはボンディングは、高可用性 (耐障害性) のために 2 つの個別の NIC を設定できる、O/S 設定オプションです。どちらかの NIC に障害が発生すると、ボンディングされた接続の一部であるもう一方の NIC は、接続を続行します。1 つの NIC がポータル設定に基づきポータルに対して選択されます。
 - 物理 NIC と対応するボンディングされた NIC の両方が設定されている場合：PSN がポータルを設定しようとする、最初にボンディング インターフェイスへ接続しようとします。これが成功しない場合、その PSN にボンドセットアップがなかったことが原因である可能性があるため、PSN は物理インターフェイスでポータルを開始しようとします。

- [証明書グループ タグ (Certificate group tag)] : ポータルの HTTPS トラフィックに使用する証明書を指定する証明書グループ タグを選択します。

- 表示言語

- [ブラウザのロケールを使用する (Use browser locale)] : クライアントブラウザのロケール設定で指定された言語をポータルの表示言語として使用します。ブラウザ ロケールの言語が ISE でサポートされていない場合は、フォールバック言語が言語ポータルとして使用されます。
- [フォールバック言語 (Fallback language)] : ブラウザ ロケールから言語を取得できない場合、またはブラウザ ロケール言語が ISE でサポートされていない場合に使用する言語を選択します。
- [常に使用 (Always use)] : ポータルに使用する表示言語を選択します。この設定は、ユーザのブラウザのロケール オプションを上書きします。

[スポンサーに使用可能な SSID (SSIDs available to sponsors)] : ゲストの訪問にあたり、スポンサーが正しい接続先ネットワークとしてゲストに通知できる、ネットワークの名前または SSID (セッション サービス識別子) を入力します。

ステップ 5 [ポータル ページのカスタマイズ (Portal Page Customization)] タブで、許可されていないデバイスがネットワークへのアクセスの取得を試行した場合にポータルに表示されるページタイトルおよびメッセージテキストをカスタマイズします。

ステップ 6 [保存 (Save)] をクリックし、[閉じる (Close)] をクリックします。

BYOD ポータルの作成

個人所有デバイスの持ち込み (BYOD) ポータルを提供して、ネットワークへのアクセスの許可の前に登録とサブリカント設定を行うことができるように、従業員がパーソナルデバイスを登録できるようにすることができます。

新しい BYOD ポータルを作成するか、既存のものを編集または複製できます。Cisco ISE によって提供されているデフォルトのポータルを含むすべての BYOD ポータルを削除できます。

[ポータルの動作およびフローの設定 (Portal Behavior and Flow Settings)] タブのページ設定に加えた変更は、デバイス ポータルフロー図のグラフィカルフローに反映されます。[サポート情報 (Support Information)] ページなどのページを有効にすると、そのページがフローに表示され、従業員はポータルで使用できるようになります。無効にすると、フローから削除されます。

始める前に

このポータルで使用するために、必要な証明書とエンドポイント ID グループが設定されていることを確認します。

- ステップ 1** [管理 (Administration)] > [デバイス ポータル管理 (Device Portal Management)] > [BYOD ポータル (BYOD Portals)] > [作成、編集または複製 (Create, Edit or Duplicate)] を選択します。
- ステップ 2** ポータルの一意の [ポータル名 (Portal Name)] および [説明 (Description)] を指定します。
ここで使用するポータル名が他のエンドユーザ ポータルに使用されていないことを確認します。
- ステップ 3** [言語ファイル (Language File)] ドロップダウン メニューを使用して、ポータルで使用する言語ファイルをエクスポートおよびインポートします。
- ステップ 4** [ポータルの設定 (Portal Settings)] でポート、証明書グループタグ、エンドポイント ID グループなどのデフォルト値を更新し、ポータル全体に適用する動作を定義します。
- ステップ 5** ネットワークアクセスの問題のトラブルシューティングのためにヘルプデスクが使用する情報を従業員が提供するのに役立つように、[サポート情報ページの設定 (Support Information Page Settings)] を更新します。
- ステップ 6** [ポータル ページのカスタマイズ (Portal Page Customization)] タブで、プロビジョニング プロセス時に次のページに表示される [コンテンツ領域 (Content Area)] メッセージテキストをカスタマイズします。
- [BYOD ウェルカム (BYOD Welcome)] ページ：
 - [デバイス設定が必要 (Device Configuration Required)] : デバイスが BYOD ポータルに初めてリダイレクトされ、証明書のプロビジョニングが必要な場合。
 - [証明書の更新が必要 (Certificate Needs Renewal)] : 前の証明書が更新される必要がある場合。
 - [BYOD デバイス情報 (BYOD Device Information)] ページ：
 - [最大デバイス数に到達 (Maximum Devices Reached)] : 従業員が登録できるデバイスの最大数に到達した場合。
 - [必要なデバイス情報 (Required Device Information)] : 従業員がデバイスを登録できるようにするために必要なデバイス情報を要求している場合。
 - [BYOD インストール (BYOD Installation)] ページ：
 - [デスクトップ インストール (Desktop Installation)] : デスクトップ デバイス用のインストール情報を提供する場合。
 - [iOS インストール (iOS Installation)] : iOS モバイル デバイス用のインストールの指示を提供する場合。
 - [Android インストール (Android Installation)] : Android モバイル デバイス用のインストールの指示を提供する場合。
 - [BYOD 成功 (BYOD Success)] ページ：
 - [成功 (Success)] : デバイスが設定され、自動的にネットワークに接続される場合。
 - [成功：手動手順 (Success: Manual Instructions)] : デバイスが正常に設定され、従業員がネットワークに手動で接続する必要がある場合。

- [成功：サポート対象外のデバイス (Success: Unsupported Device)]：サポート対象外のデバイスがネットワークに接続できる場合。

ステップ 7 [保存 (Save)] をクリックし、[閉じる (Close)] をクリックします。

次のタスク

ポータルを使用するには、そのポータルを許可する必要があります。ポータルを使用できるように許可する前または後に、ポータルをカスタマイズすることもできます。

クライアント プロビジョニング ポータルの作成

Cisco ISE では証明書プロビジョニング ポータルが提供され、そこではオンボーディング フローを通過できないデバイスについて証明書を要求することができます。たとえば、販売時点管理端末などのデバイスがあります。1つの証明書について要求を行うか、またはCSVファイルを使用して一括証明書要求を行うことができます。

デフォルトのポータル設定を編集し、ポータルに表示されるメッセージをカスタマイズすることができます。また、証明書プロビジョニング ポータルを作成、複製、および削除することもできます。

証明書プロビジョニング ポータルにアクセスできるユーザには2つのタイプがあります。

- 管理者権限を持つ内部または外部のユーザ：自分自身と他人に対し証明書を生成できます。
- 他のすべてのユーザ：自分自身にのみ証明書を生成できます。

スーパー管理ロールまたは ERS 管理ロールを割り当てられたユーザ（ネットワーク アクセス ユーザ）はこのポータルにアクセスでき、他人のために証明書を要求できます。ただし、新しい内部管理ユーザを作成し、スーパー管理ロールまたは ERS 管理ロールを割り当てると、内部管理ユーザはこのポータルにアクセスできません。最初にネットワーク アクセス ユーザを作成し、それからユーザをスーパー管理グループまたは ERS 管理グループに追加する必要があります。スーパー管理グループまたは ERS 管理グループに追加されている既存のネットワーク アクセス ユーザは、このポータルにアクセスできます。

証明書プロビジョニング ポータルにアクセスするための管理者アカウントを作成するには、次の手順を実行します。

1. 内部ユーザを追加します ([管理 (Administration)] > [IDの管理 (Identity Management)] > [ID (Identities)] > [ユーザ (Users)] > [追加 (Add)])。
2. ユーザをスーパー管理グループまたは ERS 管理グループに追加します ([管理 (Administration)] > [管理者アクセス (Admin Access)] > [管理者 (Administrators)] > [管理ユーザ (Admin Users)] > [追加 (Add)] > [既存のネットワークアクセスユーザから選択 (Select from existing network access user)])。これでユーザが内部ネットワーク アクセス ユーザとスーパー管理ユーザまたは ERS 管理ユーザの両方になりました。

他のユーザがポータルにアクセスし、自分自身の証明書を生成できるようにするには、証明書プロビジョニング ポータルの設定を行います（[管理（Administration）]>[デバイスポータル管理（Device Portal Management）]>[証明書プロビジョニングポータル（Certificate Provisioning Portal）]>[作成、編集または複製（Create, Edit or Duplicate）]>[ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）]>[ポータル設定（Portal Settings）]）。[認証方式（Authentication Method）]で適切な ID ソースまたは ID ソース順序を選択し、[承認済みグループの設定（Configure Authorized Groups）]でユーザ グループを選択します。選択したグループに属するすべてのユーザが、ポータルにアクセスし、自分自身の証明書を生成できるようになります。

始める前に

このポータルで使用するために、必要な証明書が設定されていることを確認します。

-
- ステップ 1** [管理（Administration）]>[デバイスポータル管理（Device Portal Management）]>[証明書プロビジョニングポータル（Certificate Provisioning Portal）]>[作成（Create）]の順に選択します。
- ここで使用するポータル名が他のエンドユーザ ポータルに使用されていないことを確認します。
- ステップ 2** ポータルの一意の [ポータル名（Portal Name）] および [説明（Description）] を指定します。
- ステップ 3** [言語ファイル（Language File）] メニューを使用して、ポータルで使用する言語ファイルをエクスポートおよびインポートします。
- ステップ 4** [ポータルの設定（Portal Settings）] で証明書グループ タグ、言語などのデフォルト値を更新し、ポータル全体に適用する動作を定義します。
- ステップ 5** [ポータルページのカスタマイズ（Portal Page Customization）] タブで、ポータルに表示されるページタイトルおよびメッセージテキストをカスタマイズします。
- ステップ 6** [保存（Save）] をクリックし、[閉じる（Close）] をクリックします。
-

クライアント プロビジョニング ポータルの作成

クライアント プロビジョニング ポータルを提供して、ネットワークへのアクセスを許可する前に、デバイスのポスチャ コンプライアンスを確認する Cisco AnyConnect ポスチャ コンポーネントまたは Cisco NAC Agent を従業員がダウンロードできるようにすることができます。

新しいクライアント プロビジョニング ポータルを作成するか、既存のものを編集または複製できます。Cisco ISE によって提供されているデフォルトのポータルを含むすべてのクライアント プロビジョニング ポータルを削除できます。

スーパー管理ロールまたは ERS 管理ロールを割り当てられたユーザ（ネットワーク アクセスユーザ）はこのポータルにアクセスできます。ただし、新しい内部管理ユーザを作成し、スーパー管理ロールまたは ERS 管理ロールを割り当てると、内部管理ユーザはこのポータルにアクセスできません。最初にネットワーク アクセスユーザを作成し、それからユーザをスーパー管理グループまたは ERS 管理グループに追加する必要があります。スーパー管理グループま

または ERS 管理グループに追加されている既存のネットワーク アクセス ユーザは、このポータルにアクセスできます。

クライアント プロビジョニング ポータルにアクセスするための管理者アカウントを作成するには、次の手順を実行します。

1. 内部ユーザを追加します ([管理 (Administration)] > [ID の管理 (Identity Management)] > [ID (Identities)] > [ユーザ (Users)] > [追加 (Add)])。
2. ユーザをスーパー管理グループまたは ERS 管理グループに追加します ([管理 (Administration)] > [管理者アクセス (Admin Access)] > [管理者 (Administrators)] > [管理ユーザ (Admin Users)] > [追加 (Add)] > [既存のネットワーク アクセス ユーザから選択 (Select from existing network access user)])。これでユーザが内部ネットワーク アクセス ユーザとスーパー管理ユーザまたは ERS 管理ユーザの両方になりました。

他のユーザがポータルにアクセスし、自分自身の証明書を生成できるようにするには、クライアント プロビジョニング ポータルの設定を行います ([管理 (Administration)] > [デバイス ポータル管理 (Device Portal Management)] > [クライアント プロビジョニング (Client Provisioning)] > [作成、編集または複製 (Create, Edit or Duplicate)] > [ポータルの動作およびフローの設定 (Portal Behavior and Flow Settings)] > [ポータル設定 (Portal Settings)])。[認証方式 (Authentication Method)] で適切な ID ソースまたは ID ソース順序を選択し、[承認済みグループの設定 (Configure Authorized Groups)] でユーザ グループを選択します。選択したグループに属するすべてのユーザが、ポータルにアクセスできるようになります。

[ポータルの動作およびフローの設定 (Portal Behavior and Flow Settings)] タブのページ設定に加えた変更は、デバイス ポータルフロー図のグラフィカルフローに反映されます。[サポート情報 (Support Information)] ページなどのページを有効にすると、そのページがフローに表示され、従業員はポータルで使えるようになります。無効にすると、フローから削除されます。

始める前に

このポータルで使用するために設定されている必要な証明書とクライアント プロビジョニング ポリシーがあることを確認します。

-
- ステップ 1** [管理 (Administration)] > [デバイス ポータル管理 (Device Portal Management)] > [クライアント プロビジョニング ポータル (Client Provisioning Portals)] > [作成、編集または複製 (Create, Edit or Duplicate)] を選択します。
- ステップ 2** ポータルの一意の [ポータル名 (Portal Name)] および [説明 (Description)] を指定します。
ここで使用するポータル名が他のエンドユーザ ポータルに使用されていないことを確認します。
- ステップ 3** [言語ファイル (Language File)] ドロップダウン メニューを使用して、ポータルで使用する言語ファイルをエクスポートおよびインポートします。
- ステップ 4** [ポータルの設定 (Portal Settings)] でポート、証明書グループタグ、エンドポイント ID グループなどのデフォルト値を更新し、ポータル全体に適用する動作を定義します。
- ステップ 5** ネットワーク アクセスの問題のトラブルシューティングのためにヘルプデスクが使用する情報を従業員が提供するのに役立つように、[サポート情報ページの設定 (Support Information Page Settings)] を更新します。

ステップ 6 [ポータル ページのカスタマイズ (Portal Page Customization)] タブで、プロビジョニング プロセス時にクライアント プロビジョニング ポータルに表示される [コンテンツ領域 (Content Area)] メッセージ テキストをカスタマイズします。

a) [クライアント プロビジョニング (Client Provisioning)] ページ :

- [確認、スキャン、および準拠 (Checking, Scanning and Compliant)] : ポスチャ エージェントが正常にインストールされ、デバイスがポスチャ要件に準拠していることを確認、スキャン、および検証する場合。
- [非準拠 (Non-compliant)] : ポスチャ エージェントが、デバイスがポスチャ要件に準拠していないと判断した場合。

b) [クライアント プロビジョニング (エージェントが見つかりませんでした) (Client Provisioning (Agent Not Found))] ページ :

- [エージェントが見つかりませんでした (Agent Not Found)] : ポスチャ エージェントがデバイスで検出されない場合。
- [手動インストールの手順 (Manual Installation Instructions)] : デバイスに Java または Active X ソフトウェアがインストールされていない場合の、ポスチャ エージェントを手動でダウンロードし、インストールする方法の手順。
- [インストール、Java/ActiveX なし (Install, No Java/ActiveX)] : デバイスに Java または Active X ソフトウェアがインストールされていない場合の、手動で Java プラグインをダウンロードし、インストールする方法の手順。
- [エージェント インストール済み (Agent Installed)] : ポスチャ エージェントがデバイスで検出された場合の、ポスチャ エージェントを開始する方法の手順。これにより、デバイスがポスチャ要件に準拠するかどうかを確認される。

ステップ 7 [保存 (Save)] をクリックし、[閉じる (Close)] をクリックします。

次のタスク

ポータルを使用するには、そのポータルを許可する必要があります。ポータルを使用できるように許可する前または後に、ポータルをカスタマイズすることもできます。

関連トピック

[ポータルの許可](#) (554 ページ)

[デバイス ポータルのカスタマイズ](#) (610 ページ)

MDM ポータルの作成

モバイル デバイス管理 (MDM) ポータルを提供して、従業員が、企業ネットワークでの使用のために登録されたモバイル デバイスを管理できるようにすることができます。

新しい MDM ポータルを作成するか、既存のものを編集または複製できます。すべての MDM システムに対して 1 つの MDM ポータルを設定できます。または、各システムに対し 1 つのポータルを作成できます。Cisco ISE によって提供されているデフォルトのポータルを含むすべての MDM ポータルを削除できます。デフォルトのポータルは、サードパーティの MDM プロバイダー用です。

新しい MDM ポータルを作成するか、既存のものを編集または複製できます。Cisco ISE によって提供されているデフォルトのポータルを含むすべての MDM ポータルを削除できます。デフォルトのポータルは、サードパーティの MDM プロバイダー用です。

[ポータルの動作およびフローの設定 (Portal Behavior and Flow Settings)] タブのページ設定に加えた変更は、デバイスポータルフロー図のグラフィカルフローに反映されます。[サポート情報 (Support Information)] ページなどのページを有効にすると、そのページがフローに表示され、従業員はポータルで使えるようになります。無効にすると、フローから削除されます。

始める前に

このポータルで使用するために、必要な証明書とエンドポイント ID グループが設定されていることを確認します。

ステップ 1 [管理 (Administration)] > [デバイスポータル管理 (Device Portal Management)] > [MDM ポータル (MDM Portals)] > [作成、編集または複製 (Create, Edit or Duplicate)] を選択します。

ステップ 2 ポータルの一意の [ポータル名 (Portal Name)] および [説明 (Description)] を指定します。
ここで使用するポータル名が他のエンドユーザポータルに使用されていないことを確認します。

ステップ 3 [言語ファイル (Language File)] ドロップダウンメニューを使用して、ポータルで使用する言語ファイルをエクスポートおよびインポートします。

ステップ 4 [ポータルの設定 (Portal Settings)] でポート、証明書グループタグ、エンドポイント ID グループなどのデフォルト値を更新し、ポータル全体に適用する動作を定義します。

ステップ 5 特定のページのそれぞれに適用される次の設定を更新してください。

- [従業員のモバイルデバイス管理の設定 (Employee Mobile Device Management Settings)] では、サードパーティの MDM プロバイダーを設定するために提供されているリンクにアクセスし、MDM ポータルを使用して従業員の受信ポリシーによる動作を定義します。
- ネットワークアクセスの問題のトラブルシューティングのためにヘルプデスクによって使用される情報をゲストが提供するのに役立つように、[サポート情報ページの設定 (Support Information Page Settings)] を更新します。

ステップ 6 [ポータルページのカスタマイズ (Portal Page Customization)] タブで、デバイス登録プロセス時に MDM ポータルに表示される [コンテンツ領域 (Content Area)] メッセージをカスタマイズします。

- [到達不能 (Unreachable)] : 選択された MDM システムにアクセスできない場合。
- [非準拠 (Non-compliant)] : 登録されるデバイスが MDM システムの要件に準拠していない場合。
- [続行 (Continue)] : 接続に問題がある場合にデバイスがネットワークへの接続を試行する必要がある場合。

- [登録 (Enroll)] : デバイスが MDM エージェントを必要とし、かつそのデバイスを MDM システムに登録する必要がある場合。

ステップ 7 [保存 (Save)] をクリックし、[閉じる (Close)] をクリックします。

次のタスク

ポータルを使用するには、そのポータルを許可する必要があります。ポータルを使用できるように許可する前または後に、ポータルをカスタマイズすることもできます。また、次のトピックを参照してください。

- [証明書の追加 \(595 ページ\)](#)
- [エンドポイント ID グループの作成 \(597 ページ\)](#)
- [許可プロファイルの作成 \(608 ページ\)](#)
- [デバイス ポータルのカスタマイズ \(610 ページ\)](#)

デバイス ポータルの作成

デバイス ポータルを提供して、従業員が、ネイティブ サプリカントをサポートせず、個人所有デバイスの持ち込み (BYOD) を使用して追加できないパーソナルデバイスを追加および登録できるようにすることができます。デバイス ポータルを使用して、いずれかのポータルを使用して追加されたすべてのデバイスを管理できます。

新しいデバイス ポータルを作成するか、既存のものを編集または複製できます。Cisco ISE によって提供されているデフォルトのポータルを含むすべてのデバイス ポータルを削除できます。

[ポータルの動作およびフローの設定 (Portal Behavior and Flow Settings)] タブのページ設定に加えた変更は、デバイス ポータルフロー図のグラフィカルフローに反映されます。[サポート情報 (Support Information)] ページなどのページを有効にすると、そのページがフローに表示され、従業員はポータルで使用できるようになります。無効にすると、フローから削除されます。

始める前に

このポータルで使用するために、必要な証明書、外部 ID ストア、ID ソース順序、およびエンドポイント ID グループが設定されていることを確認します。

ステップ 1 [管理 (Administration)] > [デバイス ポータル管理 (Device Portal Management)] > [デバイス ポータル (My Devices Portals)] > [作成、編集または複製 (Create, Edit or Duplicate)] を選択します。

ステップ 2 ポータルの一意の [ポータル名 (Portal Name)] および [説明 (Description)] を指定します。

ここで使用するポータル名が他のエンドユーザ ポータルに使用されていないことを確認します。

ステップ 3 [言語ファイル (Language File)] ドロップダウン メニューを使用して、ポータルで使用する言語ファイルをエクスポートおよびインポートします。

ステップ 4 [ポータルの設定 (Portal Settings)] でポート、証明書グループ タグ、ID ソース順序、エンドポイント ID グループなどのデフォルト値を更新し、ポータル全体に適用する動作を定義します。

ステップ 5 特定のページのそれぞれに適用される次の設定を更新してください。

- [ログイン ページの設定 (Login Page Settings)] : 従業員クレデンシャルおよびログイン ガイドラインを指定します。
- [利用規定 (AUP) ページ設定 (Acceptable Use Policy (AUP) Page Settings)] : 別の AUP ページを追加し、従業員の利用規定の動作を定義します。
- [ポストログインバナーページの設定 (Post-Login Banner Page Settings)] : ポータルへのログイン後に、従業員に追加情報を通知します。
- [従業員のパスワード変更の設定 (Employee Change Password Settings)] : 従業員の自身のパスワードの変更を許可します。このオプションは、従業員が内部ユーザデータベースの一部である場合にのみ有効になります。

ステップ 6 [ポータル ページのカスタマイズ (Portal Page Customization)] タブで、登録および管理時にデバイス ポータルに表示される次の情報をカスタマイズします。

- タイトル、コンテンツ、フィールド、およびボタン ラベル
- エラー メッセージおよび通知メッセージ

ステップ 7 [保存 (Save)] をクリックし、[閉じる (Close)] をクリックします。

次のタスク

ポータルの外観を変更する場合は、ポータルをカスタマイズできます。参照先

関連トピック

[デバイス ポータルのカスタマイズ](#) (610 ページ)

[デバイス ポータル](#) (588 ページ)

[従業員が追加したデバイスの表示](#) (610 ページ)

許可プロファイルの作成

ポータルを許可するときは、ネットワークアクセス用のネットワーク許可プロファイルおよびルールを設定します。

始める前に

ポータルを許可する前にポータルを作成する必要があります。

ステップ 1 ポータルの特別な許可プロファイルを設定します。

ステップ 2 プロファイルの許可ポリシー ルールを作成します。

許可プロファイルの作成

各ポータルには、特別な許可プロファイルを設定する必要があります。

始める前に

デフォルトのポータルを使用しない場合は、許可プロファイルとポータル名を関連付けることができるように、最初にポータルを作成する必要があります。

ステップ 1 [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] > [許可 (Authorization)] > [許可プロファイル (Authorization Profiles)] を選択します。

ステップ 2 使用を許可するポータル名を使用して許可プロファイルを作成します。

次のタスク

新しく作成される許可プロファイルを使用するポータル許可ポリシールールを作成する必要があります。

許可ポリシー ルールの作成

ユーザ（ゲスト、スポンサー、従業員）のアクセス要求への応答に使用するポータルのリダイレクション URL を設定するには、そのポータル用の許可ポリシー ルールを定義します。

url-redirect は、ポータル タイプに基づいて次の形式になります。

ip:port = IP アドレスとポート番号

PortalID = 一意のポータル名

ホットスポット ゲスト ポータル :

<https://ip:port/guestportal/gateway?sessionID=SessionIdValue&portal=PortalID&action=cwa&type=drw>

モバイル デバイス管理 (MDM) ポータル :

<https://ip:port/mdmportal/gateway?sessionID=SessionIdValue&portal=PortalID&action=mdm>

ステップ 1 [ポリシー (Policy)] > [認証 (Authorization)] を選択して、[標準 (Standard)] ポリシーで新しい許可ポリシー ルールを作成します。

ポリシー セットをイネーブルにした場合は、[ポリシー (Policy)] > [ポリシー セット (Policy Set)] を選択し、このポータルに使用するポリシーセットを選択して、[承認ポリシー (Authorization Policy)] を展開し、新しいルールを追加します。

ステップ 2 [条件 (Conditions)] には、ポータルの検証に使用するエンドポイント ID グループを選択します。たとえば、ホットスポット ゲスト ポータルの場合は、デフォルトの [GuestEndpoints] エンドポイント ID グループ

を選択し、MDM、ポータルの場合は、デフォルトの [RegisteredDevices] エンドポイント ID グループを選択します。

(注) ホットスポット ゲスト ポータルは、Termination CoA だけを発行するため、ゲスト許可ポリシーの検証条件の1つとして [Network Access:UseCase EQUALS Guest Flow] を使用しないでください。代わりに、エンドポイントが属する ID グループに照合して検証を行います。次の例を参考にしてください。

- "GuestEndpoint" + Wireless MAB の場合は Permit Access
- Wireless MAB の場合は HotSpot Redirect

ステップ 3 [権限 (Permissions)] には、作成したポータル許可プロファイルを選択します。

デバイス ポータルのカスタマイズ

ポータルの外観およびユーザ（必要に応じてゲスト、スポンサー、または従業員）エクスペリエンスをカスタマイズするには、ポータルテーマをカスタマイズし、ポータルページの UI 要素を変更して、ユーザに表示されるエラーメッセージと通知を編集します。ポータルのカスタマイズの詳細については、[エンドユーザ Web ポータルのカスタマイズ \(613 ページ\)](#) を参照してください。

従業員が追加するパーソナル デバイスの管理

従業員が個人所有デバイスの持ち込み (BYOD) またはデバイス ポータルを使用してデバイスを登録すると、デバイスはエンドポイントリストに表示されます。従業員はデバイスを削除して自分のアカウントからデバイスを切り離すことができますが、デバイスは Cisco ISE データベースに残ります。この結果、従業員は、デバイスの使用時に発生するエラーの解決に管理者の支援を必要とする場合があります。

従業員が追加したデバイスの表示

[エンドポイント (Endpoints)] リスト ページに表示される [ポータル ユーザ (Portal User)] フィールドを使用して、特定の従業員が追加したデバイスを特定できます。これは、特定のユーザが登録したデバイスを削除する必要がある場合に役立つことがあります。デフォルトでは、このフィールドは表示されないため、検索する前に最初に有効にする必要があります。

ステップ 1 [ワーク センター (Work Centers)] > [ネットワーク アクセス (Network Access)] > [ID (Identities)] > [エンドポイント (Endpoints)] を選択します。

ステップ 2 [設定 (Settings)] アイコンをクリックし、[カラム (Columns)] を選択します。

ステップ 3 [ポータルユーザ (Portal User)] を選択して、[エンドポイント (Endpoints)] リストに情報を表示します。

ステップ 4 [表示 (Show)] ドロップダウンリストをクリックし、[クイック フィルタ (Quick Filter)] を選択します。

ステップ5 [ポータル ユーザ (Portal User)] フィールドにユーザの名前を入力して、その特定のユーザに割り当てられたエンドポイントのみを表示します。

デバイスをデバイス ポータルに追加するときのエラー

従業員は、別の従業員がすでに追加したサービスを追加することはできません。デバイスは引き続きエンドポイント データベースに含まれます。

Cisco ISE データベースにすでに存在しているデバイスを従業員が追加しようとした場合：

- さらに、デバイスがネイティブサブスクリプションプロビジョニングをサポートしている場合、BYOD ポータルからデバイスを追加することを推奨します。この場合、デバイスがネットワークに最初に追加されたときに作成された登録詳細がすべて上書きされます。
- デバイスがプリンタなどのMAC認証バイパス (MAB) デバイスである場合、デバイスの所有権を最初に解決する必要があります。必要に応じて、管理者ポータルを使用してエンドポイントデータベースからデバイスを削除できます。これにより、新しい所有者は、デバイス ポータルを使用して正常にデバイスを追加できます。



(注) 管理者ポータルがダウンしている場合、デバイス ポータルは使用できません。

デバイス ポータルから削除されたデバイスはエンドポイント データベースに残っている

従業員がデバイス ポータルからデバイスを削除すると、そのデバイスは従業員の登録済みデバイスのリストから削除されますが、Cisco ISE エンドポイント データベースに残っており、エンドポイント リストに表示されます。

[エンドポイント (Endpoints)] ページからデバイスを完全に削除するには、[ワーク センター (Work Centers)] > [ネットワーク アクセス (Network Access)] > [ID (Identities)] > [エンドポイント (Endpoints)] を選択します。

デバイスポータルおよびエンドポイントアクティビティのモニタ

Cisco ISE は、エンドポイントおよびユーザ管理情報、およびゲストとスポンサーのアクティビティを参照できるさまざまなレポートとログを提供します。Cisco ISE 1.2 レポートの一部は廃止されましたが、情報は他のレポートで表示できます。

オン デマンドまたはスケジュール ベースでこれらのレポートを実行できます。

ステップ 1 [操作 (Operations)] > [レポート (Reports)] を選択します。

ステップ 2 レポート セレクタで、[ゲスト アクセス レポート (Guest Access Reports)] および [エンドポイントとユーザ (Endpoints and Users)] 選択を展開し、さまざまなゲスト、スポンサー、およびエンドポイントに関するレポートを表示します。

ステップ 3 レポートを選択し、[フィルタ (Filters)] ドロップダウン リストを使用して、検索するデータを選択します。

ユーザ名、ポータル名、デバイス名、エンドポイント ID グループ、および他のデータについてフィルタを使用できます。

ステップ 4 データを表示する [時間範囲 (Time Range)] を選択します。

ステップ 5 [実行 (Run)] をクリックします。

デバイス ログインおよび監査レポート

デバイス ログインおよび監査レポートは、次のものを追跡する統合レポートです。

- デバイス ポータルでの従業員によるログイン アクティビティ。
- デバイス ポータルで従業員が実行したデバイス関連の操作。

このレポートは、[操作 (Operations)] > [レポート (Reports)] > [ゲスト アクセス レポート (Guest Access Reports)] > [デバイス ログインおよび監査レポート (My Devices Login and Audit)] で使用できます。

登録済みエンドポイント レポート

[登録済みエンドポイント レポート (Registered Endpoints report)] には、従業員によって登録されたすべてのエンドポイントに関する情報が表示されます。このレポートは、[操作 (Operations)] > [レポート (Reports)] > [エンドポイントとユーザ (Endpoints and Users)] > [登録済みエンドポイント (Registered Endpoints)] で使用できます。ID、エンドポイント ID、アイデンティティプロファイルなどに対してクエリーを実行し、レポートを生成できます。サブリカント プロビジョニング統計情報および関連データの詳細については、クライアント プロビジョニング レポートの表示に関する説明を参照してください。

エンドポイントデータベースに対するクエリーを実行して、RegisteredDevices エンドポイント ID グループに割り当て済みのエンドポイントの情報を取得することができます。また、[ポータルユーザ (Portal User)] 属性がヌル以外の値に設定されている特定のユーザについてレポートを生成することもできます。

[登録済みエンドポイント レポート (Registered Endpoints Report)] には、特定のユーザによって指定の期間内にデバイス登録ポータルから登録されたエンドポイントのリストに関する情報が表示されます。



第 18 章

エンドユーザ Web ポータルのカスタマイズ

- エンドユーザ ポータル (613 ページ)
- エンドユーザ Web ポータルのカスタマイズ (613 ページ)
- ポータル コンテンツのタイプ (616 ページ)
- ポータルの基本的なカスタマイズ (617 ページ)
- ポータルの高度なカスタマイズ (627 ページ)
- ポータル言語のカスタマイズ (648 ページ)
- ゲスト通知、承認、およびエラー メッセージのカスタマイズ (651 ページ)

エンドユーザ ポータル

Cisco ISE では、Web ベースのポータルをエンドユーザの 3 つのプライマリ セットに対して提供しています。

- ゲスト ポータル (ホットスポットとクレデンシャルを持つゲスト ポータル) を使用して企業ネットワークに一時的にアクセスする必要があるゲスト。
- スポンサー ポータルを使用してゲスト アカウントを作成および管理できるスポンサーとして指定されている従業員。
- 個人所有デバイスの持ち込み (BYOD)、モバイル デバイス管理 (MDM)、デバイス ポータルなどのさまざまな非ゲストポータルを使用して、企業ネットワークでパーソナル デバイスを使用している従業員。

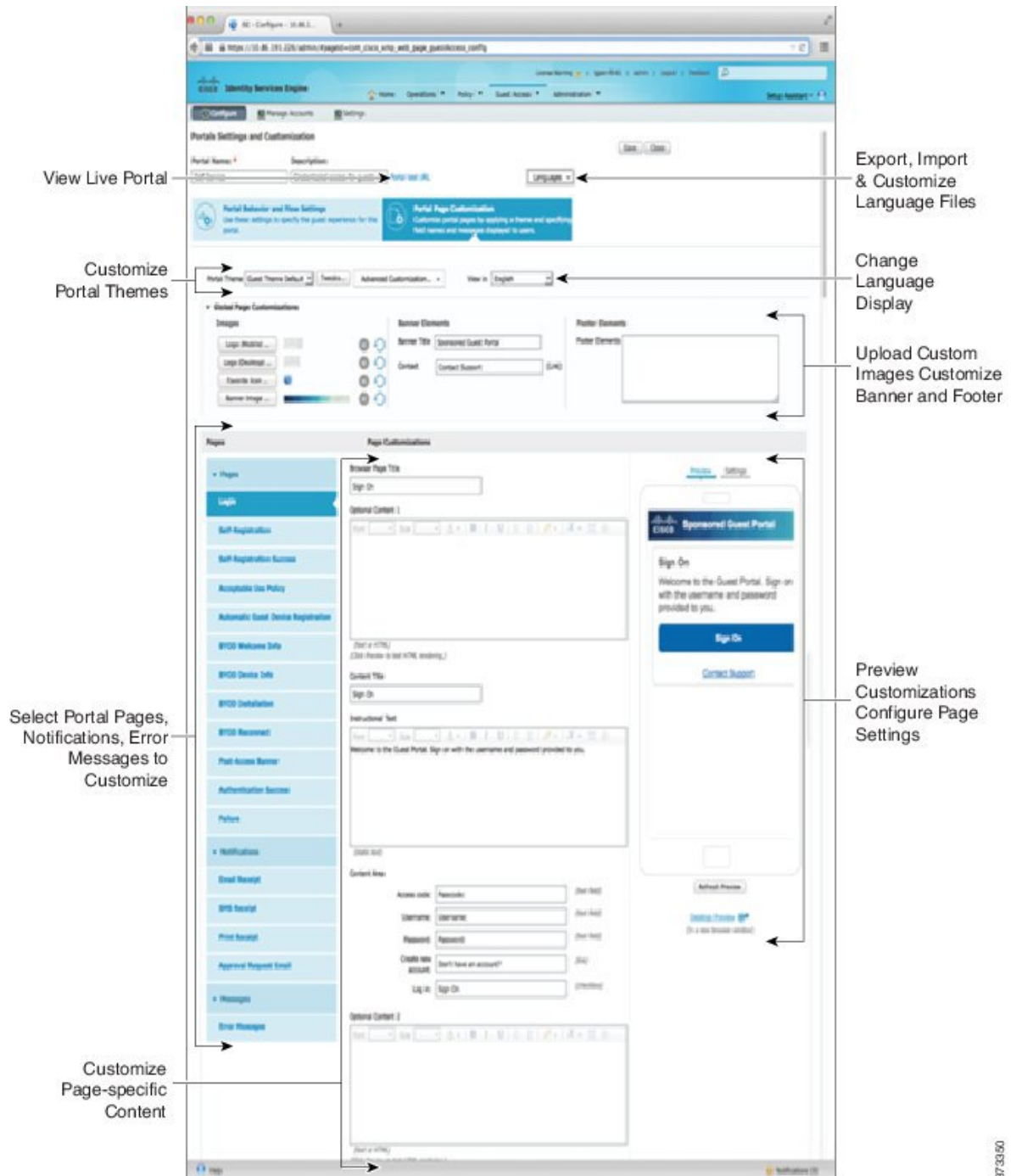
エンドユーザ Web ポータルのカスタマイズ

さまざまなデフォルトポータルが用意されており、これらを編集および複製したり、追加ポータルを作成したりすることができます。ポータルの外観を完全にカスタマイズし、その結果として、ポータルのエクスペリエンスをカスタマイズすることもできます。他のポータルへの影響なく、各ポータルを個別にカスタマイズできます。

ポータル全体またはポータルの特定のページに適用される、次のようなポータルインターフェイスのさまざまな側面をカスタマイズできます。

- テーマ、イメージ、色、バナー、およびフッター
- ポータル テキスト、エラー メッセージ、および通知の表示に使用される言語
- タイトル、コンテンツ、手順、およびフィールドとボタンのラベル
- 電子メール、SMS、およびプリンタでゲストに送信される通知（アカウント登録ゲストポータルとスポンサー ポータルにのみ該当）
- ユーザに表示されるエラー メッセージと情報メッセージ
- 特定の必要によってゲスト情報を収集するカスタム フィールド（アカウント登録ゲストポータルとスポンサー ポータルにのみ該当）

図 39: カスタマイズ用のポータル ページのレイアウト



ISE コミュニティ リソース

Web ポータルのカスタマイズの詳細については、「[ISE Portal Builder](#)」および「[HowTo: ISE Web Portal Customization Options](#)」を参照してください。

カスタマイズ方法

エンドユーザのポータルページをカスタマイズする方法は複数あり、それぞれ異なるレベルの知識が必要です。

- 基本：すべての変更はポータル カスタマイズ ページで行われます。このページでは次の操作を実行できます。
 - バナーとロゴのアップロード。
 - 一部の色の変更（ボタンを除く）。
 - 画面のテキスト、およびポータル全体で使用される言語の変更。
- 中間（Intermediate）
 - ミニ エディタを使用した HTML および Javascript の追加。
 - jQuery mobile theme roller を使用したすべてのページ要素の色の変更。
- 詳細設定（Advanced）
 - プロパティおよび CSS ファイルの手動による変更。

ポータルをカスタマイズした後、それを複製して（同じタイプの）複数のポータルを作成できます。たとえば、1つの業務エンティティのホットスポットゲストポータルをカスタマイズした場合、それを複製し、少し変更して他の業務エンティティのカスタム ホットスポット ゲスト ポータルを作成することができます。

ミニ エディタを使用してポータルをカスタマイズするためのヒント

- ミニエディタのボックス内のワードが長いと、ポータルの画面領域のスクロールがオフになる場合があります。これを防ぐには、HTML 段落属性 `style="word-wrap: break-word"` を使用します。次に例を示します。

```
<p style="word-wrap:break-word">
```

```
thisisaverylonglineoftextthatwillexceedthewidthoftheplacethatyouwanttoputitsousethisstructure
```

```
</p>
```

- HTML または javascript を使用してポータル ページをカスタマイズする場合は、必ず有効な構文を使用してください。ミニエディタに入力するタグおよびコードはISEによって検証されません。無効な構文が原因でポータルフロー時に問題が発生する場合があります。

ポータル コンテンツのタイプ

Cisco ISE では、「そのまま」使用するか、または新しいカスタム ファイルを作成するためのモデルとして既存の CSS ファイルを使用することでカスタマイズできる、ポータル テーマの

デフォルト セットが提供されます。ただし、カスタマイズされた CSS ファイルを使用しないでポータルの外観を変更することもできます。

たとえば、独自の企業ロゴやバナーイメージを使用する場合は、単にこれらの新しいイメージ ファイルをアップロードして使用することができます。ポータルのさまざまな要素および領域の色を変更することによって、デフォルトのカラースキームをカスタマイズできます。カスタム変更時に、カスタム変更を表示する言語を選択することもできます。

ロゴおよびバナーを置き換えるための画像を設計するときは、画像のサイズを次のピクセル サイズに可能な限り近づけてください。

バナー	1724 X 133
デスクトップのロゴ	86 X 45
モバイルのロゴ	80 X 35

ISE はポータルに合わせて画像のサイズを変更しますが、画像が小さすぎるとサイズ変更後に正しく表示されない場合があります。

高度なカスタマイズ（ページ レイアウトの変更、ポータル ページへのビデオ クリップや広告の追加など）を行うには、独自のカスタム CSS ファイルを使用できます。

特定のポータルでのこのようなタイプの変更は、そのポータルのすべてのページにグローバルに適用されます。ページ レイアウトの変更は、ポータル内にグローバルに、または特定の 1 ページのみに適用することができます。

ポータル ページのタイトル、コンテンツ、およびラベル

エンドユーザ Web ポータル ページでゲストに表示されるタイトル、テキスト ボックス、手順、フィールドとボタンのラベル、その他の視覚要素をカスタマイズすることができます。ページをカスタマイズするときには、ページ設定を動的に編集することができます。

これらの変更は、カスタマイズしている特定のページにのみ適用されます。

ポータルの基本的なカスタマイズ

ニーズに最適な事前定義済みテーマを選択し、デフォルト設定のほとんどを使用します。その後、次のような基本的なカスタマイズが可能です。

- [ポータルのテーマ カラーの変更（618 ページ）](#)
- [ポータルのアイコン、イメージ、およびロゴの変更（619 ページ）](#)
- [ポータルのバナーおよびフッター要素の更新（620 ページ）](#)
- [ポータルの表示言語の変更（619 ページ）](#)
- [タイトル、手順、ボタン、およびラベル テキストの変更（621 ページ）](#)
- [テキスト ボックスの内容のフォーマットおよびスタイル（621 ページ）](#)



ヒント 更新するときに、[カスタマイズの参照（626 ページ）](#)を行うことができます。

ポータルのテーマ カラーの変更

デフォルト ポータル テーマのデフォルト カラー スキームをカスタマイズして、ポータルのさまざまな要素と領域の色を変更できます。これらの変更は、カスタマイズしているポータル全体に適用されます。

ポータルの色を変更する場合は、次のことに注意してください。

- このオプションを使用して、このポータルで使用するためにインポートしたカスタム ポータル テーマのカラー スキームを変更することはできません。その色の設定を変更するには、カスタム テーマ CSS ファイルを編集する必要があります。
- ポータルのテーマ カラーを変更した後で、[ポータル テーマ (Portal Theme)] ドロップダウン メニューから別のポータルのテーマを選択した場合、元のポータル テーマの変更は失われ、デフォルト カラーに戻ります。
- 変更済みのカラー スキームを使用してポータルのテーマ カラーを調整し、保存する前に色をリセットした場合、カラー スキームはデフォルト カラーに戻り、前の変更はすべて失われます。

ステップ 1 次のポータルに移動します。

- ゲスト ポータルの場合、[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [設定 (Configure)] > [ゲスト ポータル (Guest Portals)] > [編集 (Edit)] > [ポータル ページのカスタマイズ (Portal Page Customization)] を選択します。
- スポンサー ポータルの場合、ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [スポンサー ポータル (Guest Portals)] > [編集 (Edit)] > [ポータル ページのカスタマイズ (Portal Page Customization)] を選択します。
- デバイス ポータル。[管理 (Administration)] > [デバイス ポータル管理 (Device Portal Management)] > (任意のポータル) > [編集 (Edit)] > [ポータル ページのカスタマイズ (Portal Page Customization)] を選択します。

ステップ 2 [ポータル テーマ (Portal Theme)] ドロップダウン リストからデフォルト テーマの 1 つを選択します。

ステップ 3 [調整 (Tweaks)] をクリックして、選択したデフォルト ポータル テーマの色の設定の一部を上書きします。

- a) バナーとページ背景、テキスト、およびラベルの色の設定を変更します。
- b) テーマのデフォルト カラー スキームに戻す場合は、[色のリセット (Reset Colors)] をクリックします。
- c) [プレビュー (Preview)] で色の変更を確認する場合は、[OK] をクリックします。

ステップ 4 [保存 (Save)] をクリックします。

ポータルの表示言語の変更

カスタム変更を加えるときに、変更内容を表示する言語を選択できます。この変更は、カスタマイズしているポータル全体に適用されます。

ステップ 1 次のポータルに移動します。

- ゲスト ポータルの場合、[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [ゲスト ポータル (Guest Portals)] > [編集 (Edit)] > [ポータル ページのカスタマイズ (Portal Page Customization)] > [グローバルなカスタマイズ (Global Customization)] を選択します。
- スポンサー ポータルの場合、[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [スポンサー ポータル (Sponsor Portals)] > [編集 (Edit)] > [ポータル ページのカスタマイズ (Portal Page Customization)] > [グローバルなカスタマイズ (Global Customization)] を選択します。
- デバイス ポータル。[管理 (Administration)] > [デバイス ポータル管理 (Device Portal Management)] > (任意のポータル) > [編集 (Edit)] > [ポータル ページのカスタマイズ (Portal Page Customization)] > [グローバルなカスタマイズ (Global Customization)] を選択します。

ステップ 2 [表示 (View In)] ドロップダウン リストから、ページをカスタマイズするときにテキストを表示する言語を選択します。

ドロップダウン リストには、特定のポータルに関連付けられた言語ファイルにあるすべての言語が含まれています。

次のタスク

ポータル ページをカスタマイズするときに選択した言語に加えた変更が、サポート対象のすべての言語プロパティ ファイルで更新されていることを確認します。

ポータルのアイコン、イメージ、およびロゴの変更

独自の企業ロゴ、アイコン、およびバナー イメージを使用する場合は、カスタム イメージをアップロードするだけで既存のイメージを置き換えることができます。サポートされている画像形式は、.gif、.jpg、.jpeg、.png です。これらの変更は、カスタマイズしているポータル全体に適用されます。

始める前に

ポータルのフッター (たとえば、アドバタイズメント) にイメージを含めるには、そのイメージがある外部サーバにアクセスする必要があります。

ステップ 1 次のポータルに移動します。

- ゲスト ポータルの場合、[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [ゲスト ポータル (Guest Portals)] > [編集 (Edit)] > [ポータル ページのカスタマイズ (Portal Page Customization)] を選択します。
- スポンサー ポータルの場合、[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [設定 (Configure)] > [スポンサー ポータル (Guest Portals)] > [編集 (Edit)] > [ポータル ページのカスタマイズ (Portal Page Customization)] を選択します。
- デバイス ポータル。[管理 (Administration)] > [デバイス ポータル管理 (Device Portal Management)] > (任意のポータル) > [編集 (Edit)] > [ポータル ページのカスタマイズ (Portal Page Customization)] を選択します。

ステップ 2 [イメージ (Images)] で、ロゴ、アイコン、イメージのボタンをクリックし、カスタム イメージをアップロードします。

ステップ 3 [保存 (Save)] をクリックします。

ポータルのバナーおよびフッター要素の更新

ポータルの各ページのバナーおよびフッターセクションに表示される情報をカスタマイズできます。これらの変更は、カスタマイズしているポータル全体に適用されます。

ステップ 1 次のポータルに移動します。

- ゲスト ポータルの場合、[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [ゲスト ポータル (Guest Portals)] > [編集 (Edit)] > [ポータル ページのカスタマイズ (Portal Page Customization)] を選択します。
- スポンサー ポータルの場合、[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [スポンサー ポータル (Guest Portals)] > [編集 (Edit)] > [ポータル ページのカスタマイズ (Portal Page Customization)] を選択します。
- デバイス ポータル。[管理 (Administration)] > [デバイス ポータル管理 (Device Portal Management)] > (任意のポータル) > [編集 (Edit)] > [ポータル ページのカスタマイズ (Portal Page Customization)] を選択します。

ステップ 2 各ポータル ページに表示される [バナー タイトル (Banner title)] を変更します。

ステップ 3 ポータルを使用するゲスト用に次のリンクを含めます。

- [ヘルプ (Help)] : オンライン ヘルプ (スポンサーおよびデバイス ポータルにのみ提供します)。
- [連絡先 (Contact)] : テクニカルサポート (このことができるようにするには、[サポート情報 (Support Information)] ページを設定します)。

ステップ 4 各ポータル ページの下部に表示される [フッター要素 (Footer Elements)] に利用規約または著作権表示を追加します。

ステップ5 [保存 (Save)] をクリックします。

タイトル、手順、ボタン、およびラベル テキストの変更

ポータルに表示されるすべてのテキストを更新できます。カスタマイズするページの各 UI 要素に、入力できる文字数の最小範囲および最大範囲があります。テキストブロックの一部が使用可能な場合、ミニエディタを使用して表示スタイルをテキストに適用できます。これらの変更は、カスタマイズしている特定のポータルページにだけ適用されます。これらのページ要素は、電子メール、SMS、印刷通知ごとに異なります。

ステップ1 次のポータルに移動します。

- ゲスト ポータルの場合、[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [設定 (Configure)] > [ゲスト ポータル (Guest Portals)] > [編集 (Edit)] > [ポータル ページのカスタマイズ (Portal Page Customization)] を選択します。
- スポンサー ポータルの場合、[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [スポンサー ポータル (Guest Portals)] > [編集 (Edit)] > [ポータル ページのカスタマイズ (Portal Page Customization)] を選択します。
- デバイス ポータル。[管理 (Administration)] > [デバイス ポータル管理 (Device Portal Management)] > (任意のポータル) > [編集 (Edit)] > [ポータル ページのカスタマイズ (Portal Page Customization)] を選択します。

ステップ2 [ページ (Pages)] で、変更するページを選択します。

ステップ3 [ページのカスタマイズ (Page Customizations)] で、表示された UI 要素を更新します。すべてのページに [ブラウザ ページ タイトル (Browser Page Title)]、[コンテンツ タイトル (Content Title)]、[説明テキスト (Instructional Text)]、[コンテンツ (Content)]、および2つの [任意のコンテンツ (Optional Content)] の各テキスト ブロックが含まれています。[コンテンツ (Content)] 領域のフィールドはすべてのページに固有です。

テキスト ボックスの内容のフォーマットおよびスタイル

テキストの基本的な書式設定を行うには、[説明テキスト (Instructional Text)]、[オプションの内容1 (Optional Content 1)]、および[オプションの内容2 (Optional Content 2)] テキスト ボックスにあるミニエディタを使用します。これらの変更は、カスタマイズしている特定のポータル ページにだけ適用されます。

[全画面表示の切り替え (Toggle Full Screen)] ボタンを使用して、作業しているテキスト ボックスのサイズを拡大および縮小します。

ステップ1 次のポータルに移動します。

- ゲスト ポータルの場合、[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [ゲスト ポータル (Guest Portals)] > [編集 (Edit)] > [ポータル ページのカスタマイズ (Portal Page Customization)] を選択します。
- スポンサー ポータルの場合、[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [スポンサー ポータル (Guest Portals)] > [編集 (Edit)] > [ポータル ページのカスタマイズ (Portal Page Customization)] を選択します。
- デバイス ポータル。[管理 (Administration)] > [デバイス ポータル管理 (Device Portal Management)] > (任意のポータル) > [編集 (Edit)] > [ポータル ページのカスタマイズ (Portal Page Customization)] を選択します。

ステップ 2 [ページ (Pages)] で、変更するページを選択します。

ステップ 3 [ページのカスタマイズ (Page Customizations)] の、[説明テキスト (Instructional Text)] および [オプションの内容 (Optional Content)] テキスト ボックスで、次の操作を実行できます。

- テキストのフォント、色、サイズを変更します。
- テキストに太字、イタリック体、下線のスタイルを設定します。
- 箇条書きおよび番号付きリストを作成します。

ミニエディタを使用してフォーマットしたテキストに適用された HTML タグを見るために [HTML ソースの切り替え (Toggle HTML Source)] ボタンを使用することもできます。

ポータル ページのカスタマイズ用の変数

これらのポータル ページ テキスト ボックスへのナビゲーション パス:

- ゲスト ポータルの場合、[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [ゲスト ポータル (Guest Portals)] > [編集 (Edit)] > [ポータル ページのカスタマイズ (Portal Page Customization)] > [ページ (Pages)] を選択します。
- スポンサー ポータルの場合、[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [スポンサー ポータル (Guest Portals)] > [編集 (Edit)] > [ポータル ページのカスタマイズ (Portal Page Customization)] > [ページ (Pages)] を選択します。
- デバイス ポータル。[管理 (Administration)] > [デバイス ポータル管理 (Device Portal Management)] > (任意のポータル) > [編集 (Edit)] > [ポータル ページのカスタマイズ (Portal Page Customization)] > [ページ (Pages)] を選択します。

ポータルユーザ (ゲスト、スポンサーおよび従業員) に表示される情報の一貫性を維持するために、ポータルコンテンツおよびゲスト通知用のテンプレートを作成するときにこれらの変数を使用します。[説明テキスト (Instructional Text)]、[オプションコンテンツ 1 (Optional Content

1)]、および [オプション コンテンツ 2 (Optional Content 2)] テキスト ボックスで、各ポータルのテキストを次に示す変数名と置き換えます。

表 33: ゲスト ポータルの変数のリスト

[表示名 (Display Name)]	変数名による代替
アクセス コード 電子メール、テキストまたは印刷物の通知を使用して、ゲストにアクセス コードを提供するためのテキスト。	ui_access_code
BYOD IOS SSID デュアル SSID フローに入った後にデバイスが接続する必要があるネットワークを指定するために使用します。	ui_byod_success_ios_ssid
クライアントプロビジョニングエージェントのタイプ (Client Provisioning Agent Type) AnyConnect エージェントや NAC エージェントなど、クライアントプロビジョニングポリシーで現在設定されているエージェントを指定するために使用します。	ui_client_provision_agent_type
クライアントプロビジョニングエージェントの URL (Client Provisioning Agent URL) ポスチャエージェントのダウンロード URL を指定するために使用します。	ui_client_provision_agent_url
クライアントプロビジョニングエージェントインストール分数 (Client Provisioning agent install minutes) ゲストに、クライアントプロビジョニングページでインストール手順を完了する必要がある制限時間 (修復タイマーにより設定) を通知するために使用します。タイマーが時間切れになる前にゲストがインストール手順を完了しなかった場合、ゲストはブラウザ ページをリフレッシュして、ログイン プロセスをやり直す必要があります。	ui_client_provision_install_agent_mins
会社	ui_company
電子メール アドレス (Email address)	ui_email_address
終了日時 (End date and time)	ui_end_date_time

[表示名 (Display Name)]	変数名による代替
名 (First name)	ui_first_name
姓 (Last name)	ui_last_name
ロケーション名	ui_location_name
最大登録デバイス数 (Maximum registered devices)	ui_max_reg_devices
最大同時ログイン数 (Maximum simultaneous logins)	ui_max_siml_login
[パスワード (Password)]	ui_password
訪問先担当者 (電子メール) (Person being visited (email))	ui_person_visited
電話番号 (Phone number)	ui_phone_number
訪問の理由 (Reason for visit)	ui_reason_visit
SMS プロバイダー (SMS Provider)	ui_sms_provider
SSID ゲストがネットワークに接続するために使用できるワイヤレス ネットワークを指定するために使用します。	ui_ssid
開始日時 (Start date and time)	ui_start_date_time
残り時間 (Time left)	ui_time_left
[ユーザ名 (Username)]	ui_user_name

表 34: スポンサー ポータルの変数のリスト

[表示名 (Display Name)]	変数名による代替
ゲスト - 会社 (Guest - Company)	ui_guest_company
ゲスト - 電子メールアドレス (Guest - Email address)	ui_guest_email_address
ゲスト - 終了日時 (Guest - End date and time)	ui_guest_end_date_time
ゲスト - 名 (Guest - First name)	ui_guest_first_name
ゲスト - 姓 (Guest - Last name)	ui_guest_last_name

[表示名 (Display Name)]	変数名による代替
ゲスト - ロケーション名 (Guest - Location name)	ui_guest_location_name
ゲスト - 最大登録デバイス数 (Guest - Maximum registered devices)	ui_guest_max_reg_devices
ゲスト - 最大同時ログイン数 (Guest - Maximum simultaneous logins)	ui_guest_max_siml_login
ゲスト - パスワード (Guest - Password)	ui_guest_password
ゲスト - 訪問先担当者 (電子メール) (Guest - Person being visited (email))	ui_guest_person_visited
ゲスト - 電話番号 (Guest - Phone number)	ui_guest_phone_number
ゲスト - 訪問の理由 (Guest - Reason for visit)	ui_guest_reason_visit
ゲスト - SMS プロバイダー (Guest - SMS Provider)	ui_guest_sms_provider
ゲスト - SSID (Guest - SSID) ゲストがネットワークに接続するために使用できるワイヤレス ネットワークを指定するために使用します。	ui_guest_ssid
ゲスト - 開始日時 (Guest - Start date and time)	ui_guest_start_date_time
ゲスト - 残り時間 (Guest - Time left)	ui_guest_time_left
ゲスト - ユーザ名 (Guest - Username)	ui_guest_user_name
[ユーザ名 (Username)] ポータルにログインしたユーザのユーザ名を指定するために使用します。	ui_sponsor_user_name

表 35: MDM ポータルの変数のリスト

[表示名 (Display Name)]	変数名による代替
MDM - ベンダー名 (MDM - Vendor Name)	ui_mdm_vendor_name

表 36: デバイス ポータルの変数のリスト

[表示名 (Display Name)]	変数名による代替
デバイス - ログイン失敗の頻度制限 (MyDevices - Login Failure Rate Limit)	\$user_login_failure_rate_limit\$
デバイス - 最大登録デバイス数 (MyDevices - Max Devices to Register)	ui_max_register_devices
デバイス - ユーザ名 (MyDevices - User Name) ポータルにログインしたユーザのユーザ名を 指定するために使用します。	\$session_username\$

カスタマイズの参照

カスタマイズがポータルユーザ（ゲスト、スポンサー、従業員）にどのように表示されるかを確認できます。

手順

- [ポータルテストURL (Portal test URL)] をクリックして、変更を表示します。



(注) テスト ポータルは RADIUS セッションをサポートしていないため、すべてのポータルに対するポータル フローの全体は表示されません。BYOD およびクライアント プロビジョニングは RADIUS セッションに依存するポータルの例です。

- 変更がさまざまなデバイスでどのように表示されるかを動的に確認するには、[プレビュー (Preview)] をクリックします。
 - モバイル デバイス : [プレビュー (Preview)] で変更を確認します。
 - デスクトップ デバイス : [プレビュー (Preview)] をクリックし、[デスクトッププレビュー (Desktop Preview)] をクリックします。新しいタブが開いて、すべての変更がこのタブに表示されます。

変更が表示されない場合は、[プレビューのリフレッシュ (Refresh Preview)] をクリックします。表示されるポータルは、変更を確認するためだけのものです。ボタンをクリックしたり、データを入力したりすることはできません。

カスタム ポータル ファイル

カスタム ポータル ファイル メニューでは、ISE サーバに独自のファイルをアップロードすることができ、ゲストおよび BYOD ポータルのカスタマイズに使用できます。アップロードしたファイルは PSN に保存され、すべての PSN で同期されます。

サポートされるファイル タイプは次のとおりです。

- .png、.gif、.jpg、.jpeg、.ico : 背景、お知らせ、広告用
- .htm、.html、.js、.json、.css、.m4a、.m4v、.mp3、.mp4、.mpeg、.ogg、.wav : 高度なカスタマイズ用、たとえば、ポータル ビルダー

ファイルのサイズは限定されます：

- ファイルあたり 20 MB
- すべてのファイルの合計が 200 MB

ファイルのリストのパス列には、このサーバ上のファイルの URL が表示されます。この URL は、ミニエディタ外部でそのファイルを参照する場合に使用できます。イメージファイルの場合、リンクをクリックすると、新しいウィンドウが開き、イメージが表示されます。

アップロードされたファイルは、ポータル ページのカスタマイズの下でミニ エディタで、管理者用ポータルを除くすべてのポータル タイプにより参照できます。ミニ エディタにファイルを挿入するには、ツールバーの [ファイルを挿入 (insert file)] ボタンをクリックします。[HTML ソース (HTML Source)] ビューに切り替えます。挿入されたファイルが適切な HTML タグで囲まれていることがわかります。

テストのために、表示可能なアップロードファイルを ISE の外部からブラウザで表示することもできます。URL は `https://ise_ip:8443/portal/customFiles/filename` です。

ポータルの高度なカスタマイズ

Cisco ISE から提供されるデフォルトのポータル テーマの 1 つを使用しない場合、ニーズに合わせてポータルをカスタマイズできます。そのためには、CSS および Javascript ファイルと jQuery Mobile ThemeRoller アプリケーションの使用経験が必要です。

デフォルトのポータル テーマを変更することはできませんが、次の操作を実行できます。

- [ポータルのデフォルトテーマ CSS ファイルのエクスポート \(633 ページ\)](#)、およびカスタム ポータル テーマを作成する基本として使用できます。
- [カスタム ポータルテーマ CSS ファイルの作成 \(634 ページ\)](#)、デフォルトのポータルテーマを編集し、新規ファイルとして保存することによって可能になります。
- [カスタム ポータルテーマ CSS ファイルのインポート \(646 ページ\)](#)、ポータルに適用できます。

専門知識と要件の範囲に基づいて、事前定義済み変数の使用など、さまざまなタイプの高度なカスタマイズを実行できます。これにより、表示される情報の整合性の実現、ポータルページへのアドバタイズメントの追加、HTML、CSS、および Javascript コードを使用した内容のカスタマイズ、ポータル ページのレイアウト変更が可能になります。

ポータルのカスタマイズの設定

Cisco ISE では、[ポータルページのカスタマイズ (Portal Page Customization)] に表示されているさまざまなページのテキストボックスで HTML および Javascript コードを使用して、エンドユーザ ポータルに表示される内容をカスタマイズすることができます。

-
- ステップ 1** [管理 (Administration)] > [システム (System)] > [管理者アクセス (Admin Access)] > [設定 (Settings)] > [ポータルのカスタマイズ (Portal Customization)] を選択します。
- ステップ 2** [HTML を使用したポータルのカスタマイズの有効化 (Enable portal customization with HTML)] がデフォルトでオンになっていることを確認します。この設定によって、[説明テキスト (Instructional Text)]、[オプションの内容 1 (Optional Content 1)]、および [オプションの内容 2 (Optional Content 2)] テキストボックスに HTML タグを含めることができます。
- ステップ 3** [説明テキスト (Instructional Text)]、[オプションの内容 1 (Optional Content 1)]、および [オプションの内容 2 (Optional Content 2)] テキストボックスに `<script>` タグを含めることによって、高度な JavaScript カスタマイゼーションを行う場合は、[HTML と Javascript を使用したポータルのカスタマイズの有効化 (Enable portal customization with HTML and Javascript)] をオンにします。
-

次のタスク

さまざまなポータルにアクセスし、ここで有効にしたオプションに基づいてテキストボックスに HTML および JavaScript コードを入力できます。

ポータル テーマと構造 CSS ファイル

CSS ファイルの使用に関する経験がある場合、デフォルトのポータル テーマ CSS ファイルをカスタマイズして、ポータル プレゼンテーションを変更し、ページ レイアウト、色、フォントなどの要素を操作できます。CSS ファイルをカスタマイズすると、プレゼンテーションの特性の指定における柔軟性と制御が向上し、複数のページでフォーマットを共有することが可能になり、構造化されたコンテンツの複雑さと繰り返しが削減されます。

Cisco ISE エンドユーザ ポータルは、種類が異なる 2 つの CSS ファイル (structure.css および theme.css) を使用します。ポータル テーマごとに独自の theme.css ファイルがありますが、ポータル タイプにつき structure.css ファイルは 1 つのみです (例: ゲスト ポータルの場合は guest.structure.css、スポンサー ポータルの場合は sponsor.structure.css、デバイス ポータルの場合は mydevices.structure.css)。

structure.css では、ページ レイアウトと構造のスタイルを指定しています。これには各ページの要素の位置が定義され、jQuery Mobile 構造のスタイルも含まれています。structure.css ファイルは表示のみ可能で、編集することはできません。ただし、theme.css ファイル内のページ レイアウトを変更し、これらのファイルをポータルにインポートして適用すると、最新の変更が structure.css のスタイルよりも優先されます。

theme.css ファイルは、フォント、ボタンの色、ヘッダーの背景などのスタイルを指定します。theme.css ファイルをエクスポートし、テーマ設定を変更してインポートし、ポータルのカスタ

ム テーマとして使用できます。 *theme.css* ファイルに対するページ レイアウト スタイルの変更は、 *structure.css* ファイルで定義されるスタイルよりも優先されます。

シスコが提供するデフォルトのポータル *theme.css* ファイルは変更できません。ただし、ファイル内の設定を編集して、新しいカスタム *theme.css* ファイルに保存できます。カスタム *theme.css* ファイルをさらに編集することはできますが、Cisco ISE に再度インポートする場合は、最初に使用されていたのと同じテーマ名にしてください。同じ *theme.css* ファイルに 2 つの異なるテーマ名を使用することはできません。

たとえば、デフォルトの *green theme.css* ファイルを使用して新しいカスタム *blue theme.css* ファイルを作成し、*Blue* と名付けることができます。その後、*blue theme.css* ファイルを編集できますが、これを再度インポートする場合は、同じテーマ名の *Blue* を再利用する必要があります。Cisco ISE はファイル名やその名前とテーマ名の一意性の関係を確認するため、そのファイルを *Red* という名前にすることはできません。ただし、*blue theme.css* ファイルを編集し、*red theme.css* として保存し、新規ファイルをインポートして *Red* と名付けることは可能です。

jQuery Mobile によるテーマ カラーの変更について

シスコのエンドユーザ ポータルのカラー スキームは、jQuery ThemeRoller と互換性があります。ThemeRoller Web サイトを使用して、ポータル全体の色を簡単に編集できます。

ThemeRoller の色の「見本」にはそれぞれ独自のカラー スキームがあります。それらのスキームによって、主要 UI 要素（ツールバー、コンテンツ ブロック、ボタン、リスト項目、フォントのテキストシャドウなど）の色、テキスト、フォントの設定が定義されます。さらに、ボタンのさまざまな操作状態（通常時、マウスオーバー時、押された時）の設定も定義されます。

シスコでは、次の 3 つの見本が使用されます。

- スイッチ A：デフォルトのスイッチ。
- スイッチ B：強調する要素を定義します（例：[承認（Accept）] ボタンなど）。
- スイッチ C：重要な要素を定義します（例：アラート、エラー メッセージ、無効な入力フィールド、削除ボタンなど）。

スイッチを新たに追加して適用する場合は、そのスイッチを使用する要素を含む HTML コードを（オプションコンテンツなどに）追加しない限り、追加したスイッチを適用できません。

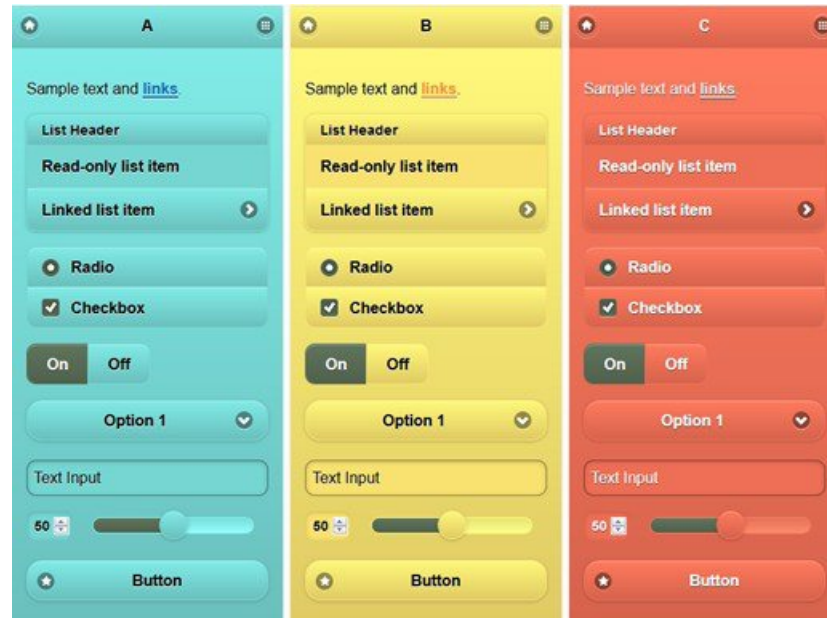
シスコ提供のデフォルトの CSS ファイルを編集するか、またはデフォルトのテーマに定義されている CSS クラスおよび構造に基づいて新しいファイルを作成するには、[jQuery Mobile ThemeRoller（リリース 1.3.2）](#) の必要なバージョンを使用してください。

jQuery Mobile ThemeRoller のスウォッチおよびテーマの詳細情報については、『[Creating a Custom Theme with ThemeRoller](#)』の「Theming Overview」を参照してください。jQuery Mobile ThemeRoller のオンライン ヘルプを使用して、カスタム テーマをダウンロード、インポート、および共有する方法を学習します。

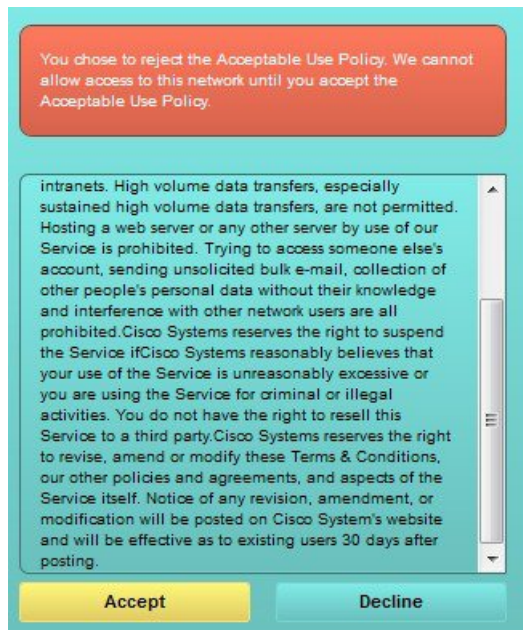
HTML、CSS、および Javascript コードを使用して、ポータル ページに表示されるテキストおよびコンテンツをカスタマイズする方法のチュートリアルについては、[Code Academy](#) にアクセスしてください。

シスコの見本を示すテーマの例

見本がどのように使用されるかを示すために、ゲスト ポータルのデフォルト テーマが色の違いを示すように ThemeRoller で編集されました。



次の画面は、ユーザ（見本B）からのアクションを取るボタンとともにゲストポータルのログインエラー（見本C）を示し、画面の残りは見本Aです。



jQuery Mobile によるテーマ カラーの変更

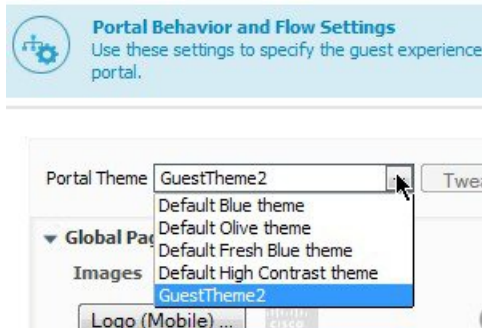
始める前に

jQuery Mobile ThemeRoller のバージョン 1.3.2 を使用していることを確認します。ご使用のバージョンが次のように画面の左上隅に表示されます。



- ステップ 1** ポータルで [設定 (Configuration)] タブをクリックして、[高度なカスタマイズ (Advanced Customization)] > [テーマのエクスポート/インポート (Export/Import Themes)] をクリックし、ポータルから変更する既存のテーマをエクスポートします。
- ステップ 2** [カスタムテーマ (Custom Theming)] ダイアログで、更新するテーマをエクスポートします。
- ステップ 3** テキスト エディタでそのテーマを開き、すべてを選択してコピーします。
- ステップ 4** jQuery Web サイトの [テーマのインポート (Import Theme)] ボックスにテキスト (CSS) を貼り付けます。
- ステップ 5** jQuery Mobil Web ベースのアプリケーションで変更を行います。
- ステップ 6** jQuery Web サイトから更新されたテーマをエクスポートします (エクスポート形式は zip)。
- ステップ 7** 更新されたテーマを解凍し、テーマフォルダ内の更新されたテーマを PC に展開します。テーマの名前は、jQuery Web サイトで指定した名前です。
- ステップ 8** ポータル設定ページの [カスタムテーマ (Custom Theming)] ダイアログで、展開した CSS テーマ ファイルをポータルにインポートします。

ポータル設定ページの [ポータルテーマ (Portal Theme)] ドロップダウンをクリックすることで、古いテーマと新しいテーマを切替えることができます。



ロケーションに基づくカスタマイズ

ゲストアカウントが作成されるときに、それらをロケーションに関連付けて **Service Set Identifier (SSID)** 属性を指定することができます。ロケーションと **SSID** のどちらも、**CSS クラス** として使用することができます。これを使用すると、ゲストのロケーションと **SSID** に基づいて、それぞれ異なる **CSS スタイル** をポータル ページに適用できます。



(注) この情報は、クレデンシアルを持つゲストポータルにのみ、ゲストがログインした後に適用されます。

次に例を示します。

- **ゲスト ロケーション** : ロケーションとして *San Jose* または *Boston* を持つアカウント付きゲストがクレデンシアルを持つゲストポータルにログインした場合、**guest-location-san-jose** または **guest-location-boston** のいずれかのクラスをすべてのポータル ページで使用できます。
- **ゲスト SSID** : *Coffee Shop Wireless* という名前の **SSID** の場合、すべてのポータル ページで **guest-ssid-coffee-shop-wireless** という **CSS クラス** を使用できます。この **SSID** は、ゲストアカウントに指定した **SSID** であり、ログイン時にゲストが接続した **SSID** ではありません。

スイッチやワイヤレス LAN コントローラ (WLC) などのデバイスをネットワークに追加するときに、ロケーションも指定できます。このロケーションも **CSS クラス** として使用することができ、これを使用すると、ネットワークデバイスのロケーションに応じて、それぞれ異なる **CSS スタイル** をポータル ページに適用できます。

たとえば、WLC が *Seattle* に割り当てられ、ゲストが *Seattle-WLC* から Cisco ISE にリダイレクトされた場合、すべてのポータル ページで **device-location-my-locations-usa-seattle** という **CSS クラス** を使用できます。

関連トピック

[ゲスト ロケーションに基づいたグリーティングのカスタマイズ](#) (641 ページ)

ユーザ デバイス タイプに基づくカスタマイズ

Cisco ISE は、クライアント デバイスのタイプ（ゲスト、スポンサー、または従業員）を検出し、企業のネットワークまたはエンドユーザ Web ポータル（ゲスト、スポンサーおよびデバイス）にアクセスします。タイプは、モバイル デバイス（Android、iOS など）またはデスクトップ デバイス（Windows、MacOS など）のいずれかとして検出されます。デバイス タイプは、CSS クラスとして利用できます。このクラスは、ユーザのデバイス タイプに基づいてポータル ページに異なる CSS スタイルを適用するために使用できます。

ユーザは Cisco ISE のエンドユーザ Web ポータルにログインすると、それらのポータル ページで **cisco-ise-mobile** クラスまたは **cisco-ise-desktop** クラスを使用できます。

関連トピック

[ユーザ デバイス タイプに基づいたグリーティングのカスタマイズ](#) (642 ページ)

ポータルのデフォルト テーマ CSS ファイルのエクスポート

シスコが提供するデフォルトのポータルテーマをダウンロードし、ニーズに合わせてカスタマイズできます。それを高度なカスタマイズを実行するための基本として使用できます。

ステップ 1 次のポータルに移動します。

- ゲスト ポータルの場合、[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [ゲスト ポータル (Guest Portals)] > [編集 (Edit)] > [ポータル ページのカスタマイズ (Portal Page Customization)] > [ページ (Pages)] を選択します。
- スポンサー ポータルの場合、[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [スポンサー ポータル (Guest Portals)] > [編集 (Edit)] > [ポータル ページのカスタマイズ (Portal Page Customization)] > [ページ (Pages)] を選択します。
- デバイス ポータル。[管理 (Administration)] > [デバイス ポータル管理 (Device Portal Management)] > (任意のポータル) > [編集 (Edit)] > [ポータル ページのカスタマイズ (Portal Page Customization)] > [ページ (Pages)] を選択します。

ステップ 2 [高度なカスタマイズ (Advanced Customization)] ドロップダウン リストから [テーマのエクスポート/インポート (Export/Import Themes)] を選択します。

ステップ 3 [カスタム テーマ (Custom Theming)] ダイアログボックスで、ドロップダウン リストを使用してカスタマイズするテーマを選択します。

ステップ 4 [テーマ CSS のエクスポート (Export Theme CSS)] をクリックして、カスタマイズするデフォルトの *theme.css* ファイルをダウンロードします。

ステップ 5 [保存 (Save)] をクリックしてファイルをデスクトップに保存します。

カスタム ポータル テーマ CSS ファイルの作成

カスタム ポータルテーマを作成するには、既存のデフォルト ポータルテーマをカスタマイズして、新規ポータルの *theme.css* ファイルに変更を保存します。デフォルト テーマの設定および見本を変更して、選択したポータルへのグローバルな変更を行うことができます。

始める前に

- カスタマイズするポータルから *theme.css* ファイルをデスクトップにダウンロードします。
- このタスクには、HTML、CSS、および Javascript コードの使用経験が必要です。
- jQuery Mobile ThemeRoller のリリース 1.3.2 を使用します。

ステップ 1 ダウンロードしたポータルの *theme.css* ファイルのコンテンツを jQuery Mobile ThemeRoller ツールにインポートします。

ヒント 変更時に、[カスタマイズの参照 \(647 ページ\)](#) を行うことができます。

ステップ 2 (任意) [ポータル コンテンツに組み込まれたリンク \(634 ページ\)](#)

ステップ 3 (任意) [動的なテキスト更新の変数の挿入 \(635 ページ\)](#)

ステップ 4 (任意) [テキストをフォーマットし、リンクを含めるソース コードの使用 \(636 ページ\)](#)

ステップ 5 (任意) [アドバタイズメントとしてのイメージの追加 \(638 ページ\)](#)

ステップ 6 (任意) [ゲスト ロケーションに基づいたグリーティングのカスタマイズ \(641 ページ\)](#)

ステップ 7 (任意) [ユーザ デバイス タイプに基づいたグリーティングのカスタマイズ \(642 ページ\)](#)

ステップ 8 (任意) [カルーセル アドバタイジングの設定 \(639 ページ\)](#)

ステップ 9 (任意) [ポータル ページのレイアウトの変更 \(643 ページ\)](#)

ステップ 10 カスタマイズされたファイルを新しい *theme.css* ファイルとして保存します。

(注) デフォルト CSS テーマファイルに編集内容を保存することはできません。編集を使用して新しいカスタム ファイルを作成することのみができます。

ステップ 11 新しい *theme.css* ファイルは、準備を整えた後、Cisco ISE にインポートできます。

ポータル コンテンツに組み込まれたリンク

リンクを追加して、ゲストがポータル ページからさまざまな Web サイトにアクセスできるようにすることができます。これらの変更は、カスタマイズしている特定のポータル ページにだけ適用されます。

[全画面表示の切り替え (Toggle Full Screen)] ボタンを使用して、作業しているテキスト ボックスのサイズを拡大および縮小します。

ステップ 1 次のポータルに移動します。

- ゲスト ポータルの場合、[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals and Components)] > [ゲスト ポータル (Guest Portals)] > [編集 (Edit)] > [ポータル ページのカスタマイズ (Portal Page Customization)] を選択します。
- スポンサー ポータルの場合、[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals and Components)] > [スポンサー ポータル (Guest Portals)] > [編集 (Edit)] > [ポータル ページのカスタマイズ (Portal Page Customization)] を選択します。
- デバイス ポータル。[管理 (Administration)] > [デバイス ポータル管理 (Device Portal Management)] > (任意のポータル) > [編集 (Edit)] > [ポータル ページのカスタマイズ (Portal Page Customization)] を選択します。
- 証明書プロビジョニング ポータル。[管理 (Administration)] > [デバイス ポータル管理 (Device Portal Management)] > [証明書プロビジョニング (Certificate Provisioning)] > [編集 (Edit)] > [ポータル ページのカスタマイズ (Portal Page Customization)] を選択します。

ステップ 2 [ページ (Pages)] で、更新するページを選択します。

ステップ 3 [ページのカスタマイズ (Page Customizations)] で、[オプションの内容 (Optional Content)] テキスト ブロックで提供されるミニエディタを使用して、ポータル ページへのリンクを追加します。

ステップ 4 [リンクの作成 (Create Link)] ボタンをクリックします。
[リンク プロパティ (Link Properties)] ダイアログボックスが表示されます。

ステップ 5 [URL] の [説明 (Description)] ウィンドウに、ハイパーリンクする URL およびテキストを入力します。
リンクが正しく機能するように、URL にプロトコル識別子を含めます。たとえば、www.cisco.com ではなく http://www.cisco.com を使用します。

ステップ 6 [設定 (Set)] をクリックし、[保存 (Save)] をクリックします。

ミニエディタを使用してフォーマットしたテキストに適用された HTML タグを見るために [HTML ソースの切り替え (Toggle HTML Source)] ボタンを使用できます。

動的なテキスト更新の変数の挿入

内容を動的に更新する事前定義済みの変数 (\$variable\$) を代わりに使用することによって、ポータルに表示されるテキストのテンプレートを作成することもできます。これにより、ゲストに表示するテキストと情報の一貫性が維持されます。これらの変更は、カスタマイズしている特定のポータル ページにだけ適用されます。

[全画面表示の切り替え (Toggle Full Screen)] ボタンを使用して、作業しているテキスト ボックスのサイズを拡大および縮小します。

ステップ 1 次のポータルに移動します。

- ゲスト ポータルの場合、[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals and Components)] > [ゲスト ポータル (Guest Portals)] > [編集 (Edit)] > [ポータル ページのカスタマイズ (Portal Page Customization)] を選択します。
- スポンサー ポータルの場合、[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals and Components)] > [スポンサー ポータル (Guest Portals)] > [編集 (Edit)] > [ポータル ページのカスタマイズ (Portal Page Customization)] を選択します。
- デバイス ポータル。[管理 (Administration)] > [デバイス ポータル管理 (Device Portal Management)] > (任意のポータル) > [編集 (Edit)] > [ポータル ページのカスタマイズ (Portal Page Customization)] を選択します。

ステップ 2 [ページ (Pages)] で、更新するページを選択します。

ステップ 3 [ページのカスタマイズ (Page Customizations)] で、[説明テキスト (Instructional Text)]、[オプションの内容 1 (Optional Content 1)]、および [オプションの内容 2 (Optional Content 2)] テキスト ボックスで提供されるミニエディタを使用して、ポータル ページのテキスト テンプレートを作成します。

たとえば、複数のゲスト用に単一の初期メッセージテンプレートを作成し、正常にログインしてネットワークに接続した後にゲストに表示するメッセージをカスタマイズできます。

ステップ 4 通常どおりにテキスト ボックスに情報を入力します。

たとえば、ポータル用の初期メッセージを入力することができます。

Welcome to our company's Guest portal,

ステップ 5 テキストの代わりに変数を使用するポイントで、[変数の挿入 (Insert Variable)] ボタンをクリックします。変数のリストがポップアップ メニューに表示されます。

ステップ 6 テキストの代わりに使用する変数を選択します。

この例では、初期メッセージに各ゲストの名を表示する [名 (First name)] を選択します。変数 **\$ui_first_name\$** がカーソル位置に挿入されます。

Welcome to our company's Guest portal,\$ui_first_name\$.

これは John という名のゲストのポータルの初期ページに表示される初期メッセージです。当社のゲストポータルへようこそ、John (Welcome to our company's Guest portal, John)。

ステップ 7 テキスト ボックスに情報を入力し終えるまで、必要に応じて続けて変数のリストを使用します。

ステップ 8 [保存 (Save)] をクリックします。

ミニエディタを使用してフォーマットしたテキストに適用された HTML タグを見るために [HTML ソースの切り替え (Toggle HTML Source)] ボタンを使用できます。

テキストをフォーマットし、リンクを含めるソース コードの使用

ミニエディタのフォーマットとプレーンテキスト付きリンクアイコンの使用に加えて、HTML、CSS、および Javascript コードを使用して、ポータル ページに表示されるテキストをカスタマイズすることもできます。これらの変更は、カスタマイズしている特定のポータルページにだけ適用されます。

[全画面表示の切り替え (Toggle Full Screen)] ボタンを使用して、作業しているテキスト ボックスのサイズを拡大および縮小します。

始める前に

[管理 (Administration)] > [システム (System)] > [管理者アクセス (Admin Access)] > [設定 (Settings)] > [ポータルのカスタマイズ (Portal Customization)] で [HTML を使用したポータルのカスタマイズの有効化 (Enable portal customization with HTML)] がデフォルトで有効になっていることを確認します。

ステップ 1 次のポータルに移動します。

- ゲスト ポータルの場合、[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [ゲスト ポータル (Guest Portals)] > [編集 (Edit)] > [ポータル ページのカスタマイズ (Portal Page Customization)] を選択します。
- スポンサー ポータルの場合、[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [スポンサー ポータル (Guest Portals)] > [編集 (Edit)] > [ポータル ページのカスタマイズ (Portal Page Customization)] を選択します。
- デバイス ポータル。[管理 (Administration)] > [デバイス ポータル管理 (Device Portal Management)] > (任意のポータル) > [編集 (Edit)] > [ポータル ページのカスタマイズ (Portal Page Customization)] を選択します。

ステップ 2 [ページ (Pages)] で、更新するページを選択します。

ステップ 3 [ページのカスタマイズ (Page Customizations)] で、[説明テキスト (Instructional Text)]、[任意のコンテンツ 1 (Optional Content 1)]、および [任意のコンテンツ 2 (Optional Content 2)] テキスト ボックスで提供されるミニエディタを使用して、ソース コードを入力および表示します。

ステップ 4 [HTML ソースの切り替え (Toggle HTML Source)] ボタンをクリックします。

ステップ 5 ソース コードを入力します。

たとえば、テキストに下線を引くには、次のように入力します。

```
<p style="text-decoration:underline;">Welcome to Cisco!</p>
```

たとえば、HTML コードを使用してリンクを含めるには、次のように入力します。

```
<a href="http://www.cisco.com">Cisco</a>
```

重要 外部 URL を HTML コードで挿入する場合は、「http」または「https」を含む絶対 (全体的な) URL パスを入力することを確認します。

ステップ 6 [保存 (Save)] をクリックします。

関連トピック

[ポータルのカスタマイズの設定 \(628 ページ\)](#)

アドバタイズメントとしてのイメージの追加

ポータルページの特定の領域に表示されるイメージおよびアドバタイズメントを含めることができます。

[全画面表示の切り替え (Toggle Full Screen)] ボタンを使用して、作業しているテキスト ボックスのサイズを拡大および縮小します。

始める前に

[管理 (Administration)] > [システム (System)] > [管理アクセス (Admin Access)] > [設定 (Settings)] > [ポータルのカスタマイズ (Portal Customization)] で [HTML を使用したポータルのカスタマイズの有効化 (Enable portal customization with HTML)] が有効になっていることを確認します。

ステップ 1 次のポータルに移動します。

- ゲスト ポータルの場合、[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [ゲスト ポータル (Guest Portals)] > [編集 (Edit)] > [ポータル ページのカスタマイズ (Portal Page Customization)] を選択します。
- スポンサー ポータルの場合、[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [スポンサー ポータル (Guest Portals)] > [編集 (Edit)] > [ポータル ページのカスタマイズ (Portal Page Customization)] を選択します。
- デバイス ポータル。[管理 (Administration)] > [デバイス ポータル管理 (Device Portal Management)] > (任意のポータル) > [編集 (Edit)] > [ポータル ページのカスタマイズ (Portal Page Customization)] を選択します。

ステップ 2 [ページ (Pages)] で、更新するページを選択します。

ステップ 3 [ページのカスタマイズ (Page Customizations)] で、[説明テキスト (Instructional Text)]、[任意のコンテンツ 1 (Optional Content 1)]、および [任意のコンテンツ 2 (Optional Content 2)] テキスト ボックスで提供されるミニエディタを使用して、ソース コードを入力および表示します。

ステップ 4 [HTML ソースの切り替え (Toggle HTML Source)] ボタンをクリックします。

ステップ 5 ソース コードを入力します。

たとえば、ホットスポット ゲスト ポータル ポスト アクセス バナーに HTML コードを使用して製品アドバタイズメントおよびそのイメージを含めるには、このコードを [ポスト アクセス バナー (Post-Access Banner)] ページの [任意のコンテンツ 1 (Optional Content 1)] テキスト ボックスに入力します。

```
<p style="text-decoration:underline;">Optimized for 10/40/100 Campus Services!</p>

```

(注) 外部 URL を HTML コードで挿入する場合は、「http」または「https」を含む絶対 (全体的な) URL パスを入力することを確認します。

図 40: アドバタイズメントのサンプル イメージ



ステップ 6 [保存 (Save)] をクリックします。

カルーセル アドバタイジングの設定

カルーセルアドバタイジングは、複数の製品イメージまたは説明テキストが表示され、バナー内で循環して繰り返されるアドバタイズメントの形式です。ゲスト ポータルでカルーセル アドバタイジングを使用して、複数の関連製品や、会社が提供するさまざまな製品を宣伝します。

[全画面表示の切り替え (Toggle Full Screen)] ボタンを使用して、作業しているテキスト ボックスのサイズを拡大および縮小します。

始める前に

[管理 (Administration)] > [システム (System)] > [管理者アクセス (Admin Access)] > [設定 (Settings)] > [ポータルのカスタマイズ (Portal Customization)] を選択し、[HTML と Javascript を使用したポータルのカスタマイズの有効化 (Enable portal customization with HTML and Javascript)] をオンにします。

ステップ 1 次のポータルに移動します。

- ゲスト ポータルの場合、[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [ゲスト ポータル (Guest Portals)] > [編集 (Edit)] > [ポータル ページのカスタマイズ (Portal Page Customization)] を選択します。
- スポンサー ポータルの場合、[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [スポンサー ポータル (Guest Portals)] > [編集 (Edit)] > [ポータル ページのカスタマイズ (Portal Page Customization)] を選択します。

- デバイス ポータル。[管理 (Administration)] > [デバイス ポータル管理 (Device Portal Management)] > (任意のポータル) > [編集 (Edit)] > [ポータル ページのカスタマイズ (Portal Page Customization)] を選択します。

ステップ 2 [ページ (Pages)] で、更新するページを選択します。

ステップ 3 [ページのカスタマイズ (Page Customizations)] で、[説明テキスト (Instructional Text)]、[任意のコンテンツ 1 (Optional Content 1)]、および [任意のコンテンツ 2 (Optional Content 2)] テキスト ボックスで提供されるミニエディタを使用して、ソース コードを入力および表示します。

ステップ 4 [HTML ソースの切り替え (Toggle HTML Source)] ボタンをクリックします。

ステップ 5 ソース コードを入力します。

たとえば、ゲスト ポータルで製品イメージを使用してカルーセル アドバタイジングを実装するには、[ポスト アクセス バナー (Post-Access Banner)] (ホットスポット ポータルの場合) または [ポスト ログイン バナー (Post Login Banner)] (クレデンシアルを持つゲスト ポータルの場合) ページの [オプションの内容 1 (Optional Content 1)] テキスト ボックスに次の HTML および Javascript コードを入力します。

```
<script>
var currentIndex = 0;
setInterval(changeBanner, 5000);

function changeBanner(){
var bannersArray = ["<img src='http://www.cisco.com/c/en/us/products/routers/index/_jcr_content/
content_parsys/overview/layout-overview/gd12v2/gd12v2-left/n21v1_cq/
n21v1DrawerContainer.img.jpg/1379452035953.jpg' width='100%' />",
"<img src='http://www.cisco.com/c/en/us/products/routers/index/_jcr_content/
content_parsys/overview/layout-overview/gd12v2/gd12v2-left/n21v1_cq_0/
n21v1DrawerContainer.img.jpg/1400748629549.jpg' width='100%' />",
"<img src='http://www.cisco.com/c/en/us/products/routers/index/_jcr_content/
content_parsys/overview/layout-overview/gd12v2/gd12v2-left/n21v1_cq_1/
n21v1DrawerContainer.img.jpg/1376556883237.jpg' width='100%' />"];

};
var div = document.getElementById("image-ads");
if(div){
    currentIndex = (currentIndex<2) ? (currentIndex+1) : 0;
    div.innerHTML = bannersArray[currentIndex];
}
}
</script>
<style>
.grey{
color: black;
background-color: lightgrey;
}
</style>
<div class="grey" id="image-ads">
<img src='http://www.cisco.com/c/en/us/products/routers/index/_jcr_content/
content_parsys/overview/layout-overview/gd12v2/gd12v2-left/n21v1_cq/
n21v1DrawerContainer.img.jpg/1379452035953.jpg' />
</div>
```

たとえば、ゲスト ポータルで製品の説明テキストを使用してカルーセル アドバタイジングを実装するには、[ポスト アクセス バナー (Post-Access Banner)] (ホットスポット ポータルの場合) または [ポスト ログイン バナー (Post Login Banner)] (クレデンシアルを持つゲスト ポータルの場合) ページの [オプションの内容 2 (Optional Content 2)] テキスト ボックスに次の HTML および Javascript コードを入力します。

```

<script>
var currentIndex = 0;
setInterval(changeBanner, 2000);

function changeBanner(){
var bannersArray = ["Optimize branch services on a single platform while delivering an optimal
application experience across branch and WAN infrastructure", "Transform your Network Edge to
deliver high-performance, highly secure, and reliable services to unite campus, data center,
and branch networks", "Differentiate your service portfolio and increase revenues by delivering
end-to-end scalable solutions and subscriber-aware services"];

var colorsArray = ["grey", "blue", "green"];
var div = document.getElementById("text-ads");
if(div){
    currentIndex = (currentIndex<2) ? (currentIndex+1) : 0;
    div.innerHTML = bannersArray[currentIndex];
    div.className = colorsArray[currentIndex];
}
}
</script>
<style>
.grey{
color: black;
background-color: lightgrey;
}
.blue{
color: black;
background-color: lightblue;
}
.green{
color: black;
background-color: lightgreen;
}
</style>
<div class="grey" id="text-ads">
Optimize branch services on a single platform while delivering an optimal application
experience across branch and WAN infrastructure
</div>

```

(注) 外部 URL を HTML コードで挿入する場合は、「http」または「https」を含む絶対（全体的な）URL パスを入力する必要があります。

ステップ 6 [保存 (Save)] をクリックします。

ゲスト ロケーションに基づいたグリーティングのカスタマイズ

次の例に、ゲストがクレデンシャルを持つゲストポータル（ホットスポットではない）にログインした後に表示される正常なログインメッセージを、ゲストタイプに設定されたロケーションに基づいてカスタマイズする方法を示します。

[全画面表示の切り替え (Toggle Full Screen)] ボタンを使用して、作業しているテキストボックスのサイズを拡大および縮小します。

ステップ 1 次のポータルのいずれかに移動します。

- ゲスト ポータルの場合、[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [ゲスト ポータル (Guest Portals)] > [編集 (Edit)] > [ポータル ページのカスタマイズ (Portal Page Customization)] を選択します。
- スポンサー ポータルの場合、[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [スポンサー ポータル (Guest Portals)] > [編集 (Edit)] > [ポータル ページのカスタマイズ (Portal Page Customization)] を選択します。

ステップ 2 [ページ (Pages)] で、[認証成功 (Authentication Success)] ページを選択します。

ステップ 3 [ページのカスタマイズ (Page Customizations)] で、[オプションの内容 1 (Optional Content 1)] テキスト ボックスで提供されるミニエディタを使用して、HTML ソース コードを入力および表示します。

ステップ 4 [HTML ソースの切り替え (Toggle HTML Source)] ボタンをクリックします。

ステップ 5 ソース コードを入力します。

たとえば、ロケーションベースのグリーティングを含めるには、[オプションコンテンツ1 (Optional Content 1)] に次のコードを入力します。

```
<style>
  .custom-greeting {
    display: none;
  }
  .guest-location-san-jose .custom-san-jose-greeting {
    display: block;
  }
  .guest-location-boston .custom-boston-greeting {
    display: block;
  }
</style>
<div class="custom-greeting custom-san-jose-greeting">
  Welcome to The Golden State!
</div>
<div class="custom-greeting custom-boston-greeting">
  Welcome to The Bay State!
</div>
```

正常なログイン後に、特定のロケーションに応じて異なるメッセージがゲストに表示されます。

ユーザ デバイス タイプに基づいたグリーティングのカスタマイズ

ユーザが Cisco ISE エンドユーザ Web ポータル (ゲスト、スポンサーおよびデバイス) のいずれかにログインした後に、ユーザに送信するグリーティングを、クライアント デバイス タイプ (モバイルまたはデスクトップ) に基づいてカスタマイズできます。

[全画面表示の切り替え (Toggle Full Screen)] ボタンを使用して、作業しているテキスト ボックスのサイズを拡大および縮小します。

ステップ 1 次のポータルに移動します。

- ゲスト ポータルの場合、[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [ゲスト ポータル (Guest Portals)] > [編集 (Edit)] > [ポータル ページのカスタマイズ (Portal Page Customization)] を選択します。

- スポンサー ポータルの場合、[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [スポンサー ポータル (Guest Portals)] > [編集 (Edit)] > [ポータル ページのカスタマイズ (Portal Page Customization)] を選択します。
- デバイス ポータル。[管理 (Administration)] > [デバイス ポータル管理 (Device Portal Management)] > (任意のポータル) > [編集 (Edit)] > [ポータル ページのカスタマイズ (Portal Page Customization)] を選択します。

ステップ 2 [ページ (Pages)] で、更新するページを選択します。

ステップ 3 [ページのカスタマイズ (Page Customizations)] で、[オプションの内容 1 (Optional Content 1)] テキスト ボックスで提供されるミニエディタを使用して、HTML ソース コードを入力および表示します。

ステップ 4 [HTML ソースの切り替え (Toggle HTML Source)] ボタンをクリックします。

ステップ 5 ソース コードを入力します。

たとえば、AUP ページにデバイス タイプベースのメッセージを含めるには、[AUP] ページの [オプションの内容 1 (Optional Content 1)] テキスト ボックスに次のコードを入力します。

```
<style>
  .custom-greeting {
    display: none;
  }
  .cisco-ise-desktop .custom-desktop-greeting {
    display: block;
  }
  .cisco-ise-mobile .custom-mobile-greeting {
    display: block;
  }
</style>
<div class="custom-greeting custom-mobile-greeting">
  Try our New Dark French Roast! Perfect on the Go!
</div>
<div class="custom-greeting custom-desktop-greeting">
  We brought back our Triple Chocolate Muffin!
  Grab a seat and dig in!
</div>
```

ユーザがネットワークまたはポータルへのアクセスを取得するために使用したデバイスに応じて、[AUP] ページに異なるグリーティングが表示されます。

ポータル ページのレイアウトの変更

ページの全体的なレイアウトを操作できます。たとえば、追加情報や情報へのリンクを提供するサイドバーを AUP ページに追加できます。

ステップ 1 作成し、ポータルに適用するカスタム *theme.css* ファイルの末尾に次の CSS コードを追加します。これにより、[オプションの内容 1 (Optional Content 1)] テキスト ボックスが次のように表示されるように AUP ページのレイアウトが変更されます。

- デスクトップ デバイス モードのサイド バー
- モバイル デバイス モードのサイド バー

```
#page-aup .cisco-ise-optional-content-1 {
    margin-bottom: 5px;
}
@media all and ( min-width: 60em ) {
    #page-aup .cisco-ise-optional-content-1 {
        float: left;
        margin-right: 5px;
        width: 150px;
    }
    #page-aup .cisco-ise-main-content {
        float: left;
        width: 800px;
    }
    #page-aup .cisco-ise-main-content h1,
    #page-aup .cisco-ise-main-content p {
        margin-right: auto;
        margin-left: -200px;
    }
}
```

次に、ポータルの AUP ページの [オプションの内容1 (Optional Content 1)] テキスト ボックスで HTML コードを使用して、リンクを追加できます。

ステップ 2 次のポータルに移動します。

- ゲスト ポータルの場合、[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portal & Components)] > [ゲスト ポータル (Guest Portals)] > [編集 (Edit)] > [ポータル ページのカスタマイズ (Portal Page Customization)] を選択します。
- スポンサー ポータルの場合、[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portal & Components)] > [スポンサー ポータル (Guest Portals)] > [編集 (Edit)] > [ポータル ページのカスタマイズ (Portal Page Customization)] を選択します。
- デバイス ポータル。[管理 (Administration)] > [デバイス ポータル管理 (Device Portal Management)] > (任意のポータル) > [編集 (Edit)] > [ポータル ページのカスタマイズ (Portal Page Customization)] を選択します。

ステップ 3 [ページ (Pages)] で、サイドバーを追加するページを選択します。

ステップ 4 [ページのカスタマイズ (Page Customizations)] で、[オプションの内容 1 (Optional Content 1)] テキスト ボックスで提供されるミニエディタを使用して、ソース コードを入力および表示します。

ステップ 5 [HTML ソースの切り替え (Toggle HTML Source)] ボタンをクリックします。

ステップ 6 ソース コードを入力します。

たとえば、AUP ページにサイドバーを含めるには、AUP ページの [オプションの内容 1 (Optional Content 1)] テキスト ボックスにこのコードを入力します。

```
<ul data-role="listview">
  <li>Rent a Car</li>
  <li>Top 10 Hotels</li>
  <li>Free Massage</li>
  <li>Zumba Classes</li>
</ul>
```

図 41: サンプル AUP ページのサイドバーのビュー (デスクトップ デバイス)

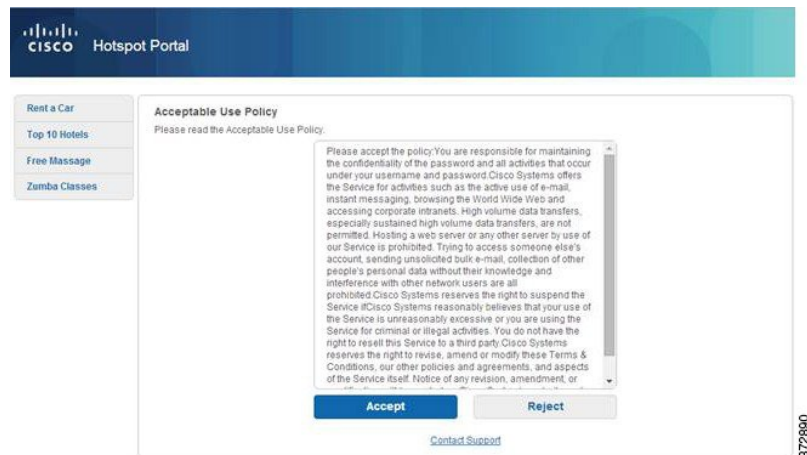
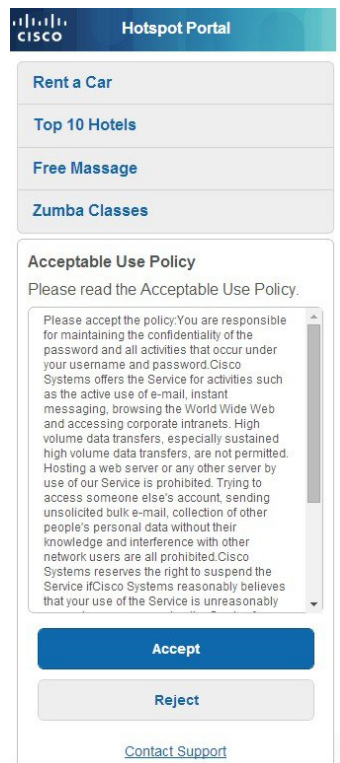


図 42: サンプル AUP ページのサイドバーのビュー (モバイル デバイス)



ステップ 7 [保存 (Save)] をクリックします。

次のタスク

[オプションの内容 (Optional Content)] テキスト ボックスに別のテキストまたは HTML コードを入力して、他のページをカスタマイズできます。

カスタム ポータル テーマ CSS ファイルのインポート

作成したカスタム *theme.css* ファイルをアップロードし、エンドユーザ ポータルに適用できます。これらの変更は、カスタマイズしているポータル全体に適用されます。

カスタム *theme.css* ファイルを編集し、Cisco ISE に再度インポートする場合は、最初に使用したテーマ名を使用するように注意してください。同じ *theme.css* ファイルに 2 つの異なるテーマ名を使用することはできません。

ステップ 1 次のポータルに移動します。

- ゲスト ポータルの場合、[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [設定 (Configure)] > [ゲスト ポータル (Guest Portals)] > [編集 (Edit)] > [ポータル ページのカスタマイズ (Portal Page Customization)] を選択します。
- スポンサー ポータルの場合、[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [スポンサー ポータル (Guest Portals)] > [編集 (Edit)] > [ポータル ページのカスタマイズ (Portal Page Customization)] を選択します。
- デバイス ポータル。[管理 (Administration)] > [デバイス ポータル管理 (Device Portal Management)] > (任意のポータル) > [編集 (Edit)] > [ポータル ページのカスタマイズ (Portal Page Customization)] を選択します。

ステップ 2 [高度なカスタマイズ (Advanced Customization)] ドロップダウン リストから [テーマのエクスポート/インポート (Export/Import Themes)] を選択します。

ステップ 3 [カスタム テーマ (Custom Theming)] ダイアログボックスで、新しい *theme.css* ファイルを検索するには、[参照 (Browse)] をクリックします。

ステップ 4 新しいファイルの [テーマ名 (Theme Name)] を入力します。

ステップ 5 [保存 (Save)] をクリックします。

次のタスク

カスタマイズするポータルにこのカスタム ポータル テーマを適用できます。

1. ポータル全体に適用する更新されたテーマを [ポータル テーマ (Portal Themes)] ドロップダウン リストから選択します。
2. [保存 (Save)] をクリックします。

カスタム ポータル テーマの削除

Cisco ISE にインポートしたカスタム ポータル テーマは、いずれかのポータルで使用されていない場合に削除できます。Cisco ISE によって提供されているデフォルトのテーマを削除することはできません。

始める前に

他のポータルで使用されているポータル テーマを削除することはできません。

ステップ 1 次のポータルに移動します。

- ゲスト ポータルの場合、[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [ゲスト ポータル (Guest Portals)] > [編集 (Edit)] > [ポータル ページのカスタマイズ (Portal Page Customization)] を選択します。
- スポンサー ポータルの場合、[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [スポンサー ポータル (Guest Portals)] > [編集 (Edit)] > [ポータル ページのカスタマイズ (Portal Page Customization)] を選択します。
- デバイス ポータル。[管理 (Administration)] > [デバイス ポータル管理 (Device Portal Management)] > (任意のポータル) > [編集 (Edit)] > [ポータル ページのカスタマイズ (Portal Page Customization)] を選択します。

ステップ 2 [高度なカスタマイズ (Advanced Customization)] ドロップダウン リストから [テーマの削除 (Delete Themes)] を選択します。

ステップ 3 [テーマ名 (Theme Name)] ドロップダウン リストから削除するポータル テーマを選択します。

ステップ 4 [削除 (Delete)] をクリックし、[保存 (Save)] をクリックします。

カスタマイズの参照

カスタマイズがポータルユーザ (ゲスト、スポンサー、従業員) にどのように表示されるかを確認できます。

手順

- [ポータルテストURL (Portal test URL)] をクリックして、変更を表示します。



(注) テスト ポータルは RADIUS セッションをサポートしていないため、すべてのポータルに対するポータル フローの全体は表示されません。BYOD およびクライアント プロビジョニングは RADIUS セッションに依存するポータルの例です。

- 変更がさまざまなデバイスでどのように表示されるかを動的に確認するには、[プレビュー (Preview)] をクリックします。
 - モバイル デバイス : [プレビュー (Preview)] で変更を確認します。
 - デスクトップ デバイス : [プレビュー (Preview)] をクリックし、[デスクトップ プレビュー (Desktop Preview)] をクリックします。新しいタブが開いて、すべての変更がこのタブに表示されます。

変更が表示されない場合は、[プレビューのリフレッシュ (Refresh Preview)] をクリックします。表示されるポータルは、変更を確認するためのものです。ボタンをクリックしたり、データを入力したりすることはできません。

ポータル言語のカスタマイズ

ゲスト、スポンサー、デバイスおよびクライアントプロビジョニングの各ポータルは、サポートされているすべての言語およびロケールにローカライズされています。ローカライズには、テキスト ラベル、メッセージ、フィールド名およびボタン ラベルが含まれます。クライアントブラウザが Cisco ISE テンプレートにマッピングされていないロケールを要求した場合、ポータルは英語のテンプレートを使用して内容を表示します。

管理者ポータルを使用して、各言語のゲスト、スポンサー、デバイスの各ポータルで使用されるフィールドを個別に変更できます。また、言語を追加することも可能です。現在、クライアントプロビジョニングポータルについては、これらのフィールドはカスタマイズできません。

デフォルトでは、各タイプのポータルでは15言語がサポートされています。[ポータルページのカスタマイズ (Portal Page Customization)] ページで、ポータルで使用する言語を選択し、オプションで選択した言語でページのコンテンツを更新します。ある言語に合わせてページのフォントとコンテンツを変更しても、他の言語へこの変更は反映されません。[ポータルページのカスタマイズ (Portal Page Customization)] 画面で行った変更は、次回に言語ファイルをエクスポートするときに組み込まれます。



(注) NAC および MAC エージェントのインストーラおよび WebAgent ページはローカライズされていません。

ポータルで使用する言語の編集

1. 編集するポータルを開きます。
2. [ポータルページのカスタマイズ (Portal Page Customization)] タブで、ページの最上部近くにある [表示(view in)] ドロップダウンから、編集する言語を選択します。
3. 必要に応じてコンテンツ、ヘッダー、フォントを変更します。
4. ポータル設定を保存し、更新する次の言語でこのフローを繰り返します。

言語ファイルを編集するには

各 [ポータルページのカスタマイズ (Portal Page Customization)] ページでは言語ファイルも提供されます。言語ファイルとは、属性ファイルが含まれている ZIP です。これらの属性ファイルは、ポータルフローの一部であるテキストやヘッダーのカスタマイズには使用できませんが、[ポータルページのカスタマイズ (Portal Page Customization)] ページのカスタマイズには使用できません。

言語ファイルには、特定のブラウザ ロケール設定（例：フランス語の場合は fr、fr-fr、fr-ca）へのマッピングと、その言語でのポータル全体のすべての文字列設定が含まれています。1 つの言語用のブラウザ ロケール設定を変更した場合、変更内容は他のすべてのエンドユーザ Web ポータルに適用されます。たとえば、ホットスポット ゲスト ポータルの French.properties ブラウザ ロケールを fr,fr-fr,fr-ca から fr,fr-fr に変更すると、この変更内容がデバイス ポータルにも適用されます。

zip 形式の言語ファイルをエクスポートし、新規言語の追加や不要な既存言語の削除などを行って更新することができます。

言語ファイルの更新手順については、次を参照してください。

- [言語ファイルのエクスポート（649 ページ）](#)
- [言語ファイルでの言語の追加または削除（650 ページ）](#)
- [更新された言語ファイルのインポート（650 ページ）](#)

言語ファイルのエクスポート

各ポータルタイプに使用できる言語ファイルをエクスポートして、そのファイルで指定された既存の値を編集およびカスタマイズし、言語を追加または削除できます。



(注) 言語プロパティ ファイル内の一部のディクショナリ キーだけが値（テキスト）で HTML をサポートしています。

ステップ 1 次のポータルに移動します。

- ゲスト ポータルの場合、[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [編集 (Edit)] を選択します。
- スポンサー ポータルの場合、[ワーク センター (Work Centers)] > [設定 (Configure)] > [ポータルとコンポーネント (Portals & Components)] > [スポンサー ポータル (Sponsor Portals)] > [編集 (Edit)] を選択します。
- デバイス ポータルの場合、[管理 (Administration)] > [デバイス ポータル管理 (Device Portal Management)] > (任意のポータル) > [編集 (Edit)] を選択します。

ステップ 2 [言語ファイル (Language File)] をクリックし、ドロップダウン リストから [エクスポート (Export)] を選択します。

ステップ 3 デスクトップに zip 形式の言語ファイルを保存します。例：Hotspot.zip、Self-Registered.zip など。

言語ファイルでの言語の追加または削除

ポータル タイプに使用したい言語が言語ファイルにない場合は、新しい言語プロパティ ファイルを作成し、zip 形式の言語ファイルに追加できます。不要な言語がある場合、その言語プロパティ ファイルを削除できます。

始める前に

言語プロパティ ファイルを追加または削除するには、各ポータルタイプで使用可能な zip 形式の言語ファイルをエクスポートします。

ステップ 1 UTF-8 を表示するエディタ（Notepad ++ など）を使用して、言語を追加または削除するポータル タイプ用の定義済み言語ファイルを開きます。

複数のポータル タイプの言語を追加または削除するには、該当するすべてのポータル プロパティ ファイルを使用します。

ステップ 2 新しい言語を追加するには、既存の言語プロパティ ファイルを他のファイルと同じ命名規則を使用する新しい言語プロパティ ファイルとして zip 形式の言語ファイルに保存します。たとえば、新しい日本語の言語プロパティ ファイルを作成するには、ファイルを `Japanese.properties` (`LanguageName.properties`) として保存します。

ステップ 3 新しい言語プロパティ ファイルの最初の行にブラウザ ロケール値を指定して、ブラウザ ロケールに新しい言語を関連付けます。たとえば、`LocaleKeys=ja,ja-jp` (`LocaleKeys=browser locale value`) を `Japanese.properties` ファイルの最初の行に入力する必要があります。

ステップ 4 新しい言語プロパティ ファイルでディクショナリ キーのすべての値（テキスト）を更新します。

ディクショナリ キーは変更できません。キーの値だけを変更できます。

（注） 一部のディクショナリ キーだけが、値（テキスト）に HTML をサポートしています。

次のタスク

1. すべてのプロパティ ファイル（新規および既存）を zip 形式で圧縮し、新しい zip 形式の言語ファイルを作成します。フォルダやディレクトリは含めないでください。
2. zip 形式の言語ファイルには新しい名前または元の名前を使用します。
3. エクスポート元の特定のポータルに zip 形式の言語ファイルをインポートします。

更新された言語ファイルのインポート

言語プロパティ ファイルを追加または削除したり、既存のプロパティ ファイルのテキストを更新してカスタマイズした編集済み言語ファイルをインポートできます。



- (注) Word ファイルからカスタマイズした内容をコピーして貼り付けることはできません。代わりに [ファイル (File)] > [名前を付けて保存 (Save As)] を選択し、Word ファイルを HTML 形式で保存します。その後、この HTML ファイルからカスタマイズした内容をコピーして貼り付けることができます。

ステップ 1 次のポータルに移動します。

- ゲスト ポータルの場合、[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [ゲスト ポータル (Guest Portals)] > [編集 (Edit)] を選択します。
- スポンサー ポータルの場合、[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [スポンサー ポータル (Sponsor Portals)] > [編集 (Edit)] を選択します。
- デバイス ポータル。[管理 (Administration)] > [デバイス ポータル管理 (Device Portal Management)] > (任意のポータル) > [編集 (Edit)] を選択します。

ステップ 2 [言語ファイル (Language)] をクリックし、ドロップダウン リストから [インポート (Import)] を選択します。

ステップ 3 デスクトップを参照して新しい zip 形式の言語ファイルを見つけます。

ステップ 4 エクスポートしたポータル タイプに再度インポートします。

次のタスク

変更したテキストまたは追加した新しい言語を表示するには、[表示 (View In)] ドロップダウン リストから特定の言語を選択します。

ゲスト通知、承認、およびエラーメッセージのカスタマイズ

各ポータルで内で、ゲストが電子メール、SMS テキスト メッセージ、および印刷物で通知を受け取る方法をカスタマイズできます。これらの通知を使用して、次の場合にログインクレデンシアルを電子メール送信、テキスト送信、または印刷します。

- ゲストがアカウント登録ゲスト ポータルを使用し、自分自身の登録に成功した場合。
- スポンサーがゲスト アカウントを作成し、ゲストに詳細を提供する場合。スポンサー グループ作成時にスポンサーによる SMS 通知の使用を許可するかどうかを指定できます。これらの機能を利用できる場合は、常に電子メール通知および印刷通知を使用できます。

ネットワークにアクセスしようとするアカウント登録ゲストを承認するよう要求するスポンサー宛電子メール通知をカスタマイズすることもできます。また、ゲストとスポンサーに表示されるデフォルトのエラーメッセージをカスタマイズできます。

電子メールでの通知のカスタマイズ

電子メールでゲストに送信される情報をカスタマイズできます。

始める前に

- 電子メールでの通知を有効にするように SMTP サーバを設定します。[管理 (Administration)] > [システム (System)] > [設定 (Settings)] > [SMTP サーバ (SMTP Server)] を選択します。
- ゲストへの電子メールでの通知のサポートを設定します。[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [設定 (Settings)] > [ゲスト電子メールの設定 (Guest Email Settings)] を選択します。[ゲストへの電子メール通知を有効にする (Enable email notifications to guests)] をオンにします。
- [管理 (Administration)] > [システム (System)] > [管理者アクセス (Admin Access)] > [設定 (Settings)] > [ポータルのカスタマイズ (Portal Customization)] で [HTML を使用したポータルのカスタマイズの有効化 (Enable portal customization with HTML)] がデフォルトで有効になっていることを確認します。

-
- ステップ 1** 自己登録スポンサー ポータルの場合、[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [スポンサー ポータル (Sponsor Portals)] > [編集 (Edit)] > [ポータル ページのカスタマイズ (Portal Page Customization)] > [ゲストへの通知 (Notify Guests)] > [電子メール通知 (Email Notification)] を選択します。
- ステップ 2** [グローバル ページのカスタマイズ (Global Page Customizations)] で指定されたデフォルトの [ロゴ (電子メール) (Logo (Email))] を変更できます。
- ステップ 3** [件名 (Subject)] および [電子メール本文 (Email body)] を指定します。電子メール メッセージに含まれる、ゲストアカウント情報を指定するには、事前定義済みの変数を使用します。テキストをカスタマイズするには、ミニエディタと HTML タグを使用します。
- ステップ 4** [設定 (Settings)] では、次のことが可能です。
- 異なる電子メールで [ユーザ名とパスワードを個別に送信する (Send username and password separately)]。このオプションを選択すると、**ユーザ名電子メール通知**と**パスワード電子メール通知**をカスタマイズするための 2 つのタブが [ページのカスタマイズ (Page Customizations)] に表示されます。
 - 電子メール アドレスへの [テスト電子メールの送信 (Send Test Email)]。すべてのデバイスでカスタマイズをプレビューし、適切に表示されることを確認します。
- ステップ 5** [保存 (Save)] をクリックし、[閉じる (Close)] をクリックします。
-

SMS テキスト メッセージ通知のカスタマイズ

SMS テキスト メッセージでゲストに送信される情報をカスタマイズできます。

始める前に

- SMS ゲートウェイに電子メールを送信して、SMS テキスト メッセージを配信するために使用される SMTP サーバを設定します。[管理 (Administration)] > [システム (System)] > [設定 (Settings)] > [SMTP サーバ (SMTP Server)] を選択します。
- SMS テキスト通知をサポートするようにスポンサー グループを設定します。
- サードパーティ SMS ゲートウェイでアカウントを設定します。[管理 (Administration)] > [システム (Systems)] > [設定 (Settings)] > [SMS ゲートウェイ (SMS Gateway)] を選択します。Cisco ISE では、テキスト メッセージが電子メールとしてゲートウェイに送信され、SMS プロバイダー経由で指定したユーザにメッセージが転送されます。
- [管理 (Administration)] > [システム (System)] > [管理者アクセス (Admin Access)] > [設定 (Settings)] > [ポータルのカスタマイズ (Portal Customization)] で [HTML を使用したポータルのカスタマイズの有効化 (Enable portal customization with HTML)] がデフォルトで有効になっていることを確認します。

ステップ 1 アカウント登録ゲストポータルおよびスポンサーポータルの場合は、[ワークセンター (Work Centers)] > [ゲストアクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [ゲストポータルまたはスポンサーポータル (Guest or Sponsor Portals)] > [編集 (Edit)] > [ポータルページのカスタマイズ (Portal Page Customization)] > [SMS 受信または SMS 通知 (SMS Receipt or SMS Notification)] を選択します。

ステップ 2 [メッセージテキスト (Message Text)] をカスタマイズするには、ミニエディタと HTML タグを使用します。SMS テキスト メッセージに含まれる、ゲストアカウント情報を指定するには、事前定義済みの変数を使用します。

ステップ 3 [設定 (Settings)] では、次のことが可能です。

- 異なるテキスト メッセージで [ユーザ名とパスワードを個別に送信する (Send username and password separately)]。このオプションを選択すると、**ユーザ名メッセージとパスワードメッセージ**をカスタマイズするための 2 つのタブが [ページのカスタマイズ (Page Customizations)] に表示されます。
- 携帯電話への [テストメッセージの送信 (Send Test Message)]。カスタマイズをプレビューし、情報が適切に表示されることを確認します。サポートされる電話番号の形式には、+1 ### ### ####、###-###-####、(###) ### ####、#####、1##### があります。

ステップ 4 [保存 (Save)] をクリックし、[閉じる (Close)] をクリックします。

印刷通知のカスタマイズ

ゲスト用に印刷される情報をカスタマイズできます。



(注) 各ポータル内では、印刷通知ロゴは、電子メール通知ロゴの設定から継承されます。

始める前に

[管理 (Administration)] > [システム (System)] > [管理者アクセス (Admin Access)] > [設定 (Settings)] > [ポータルのカスタマイズ (Portal Customization)] で [HTML を使用したポータルのカスタマイズの有効化 (Enable portal customization with HTML)] がデフォルトで有効になっていることを確認します。

- ステップ 1** アカウント登録ゲストポータルおよびスポンサーポータルの場合は、[ワークセンター (Work Centers)] > [ゲストアクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [ゲストポータルまたはスポンサーポータル (Guest or Sponsor Portals)] > [編集 (Edit)] > [ポータルページのカスタマイズ (Portal Page Customization)] > [印刷受け取りまたは印刷通知 (Print Receipt or Print Notification)] を選択します。
- ステップ 2** [印刷説明テキスト (Print Introduction Text)] を指定します。電子メールメッセージに含まれる、ゲストアカウント情報を指定するには、事前定義済みの変数を使用します。テキストをカスタマイズするには、ミニエディタと HTML タグを使用します。
- ステップ 3** サムネールで、または [印刷プレビュー (Print Preview)] をクリックして、カスタマイズをプレビューします。サムネールでは、HTML のカスタマイズを表示できません。
[印刷プレビュー (Print Preview)] オプションを選択した場合、アカウントの詳細を印刷できるウィンドウが表示され、そこで適切に表示されることを確認します。
- ステップ 4** [保存 (Save)] をクリックし、[閉じる (Close)] をクリックします。

承認要求の電子メールでの通知のカスタマイズ

アカウント登録ゲストのアカウントが作成され、そのゲストがログインクレデンシャルを取得する前に、アカウント登録ゲストを承認するようスポンサーに要求できます。電子メールでスポンサーに送信される、承認を要求する情報をカスタマイズできます。この通知は、ネットワークアクセスを許可する前にアカウント登録ゲストポータルを使用するアカウント登録ゲストを承認する必要があると指定した場合にのみ表示されます。

始める前に

- 電子メールでの通知を有効にするように SMTP サーバを設定します。[管理 (Administration)] > [システム (Systems)] > [設定 (Settings)] > [SMTP サーバ (SMTP Server)] を選択します。
- ゲストへの電子メールでの通知のサポートを設定します。[ワークセンター (Work Centers)] > [ゲストアクセス (Guest Access)] > [設定 (Settings)] > [ゲスト電子メールの設定 (Guest Email Settings)] を選択します。[ゲストへの電子メール通知を有効にする (Enable email notifications to guests)] をオンにします。

- スポンサーに自己登録アカウントの要求を承認させるには、[ポータルの動作およびフローの設定 (Portal Behavior and Flow Settings)] タブの [アカウント登録ページの設定 (Self-Registration Page Settings)] で、[アカウント登録ゲストが承認される必要がある (Require self-registered guests to be approved)] をオンにします。それによって、[ポータルページのカスタマイズ (Portal Page Customization)] の [通知 (Notifications)] の下の [承認要求の電子メール (Approval Request Email)] タブが有効になり、スポンサーに送られる電子メールをカスタマイズできます。

ステップ 1 [ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [設定 (Configure)] > [アカウント登録ゲスト ポータル (Self-Registered Guest Portals)] > [編集 (Edit)] > [ポータル ページのカスタマイズ (Portal Page Customization)] > [承認要求 電子メール (Approval Request Email)] を選択します。ここでは次を実行できます。

- a) [グローバル ページのカスタマイズ (Global Page Customizations)] で指定されたデフォルトの [ロゴ (Logo)] を変更します。
- b) [件名 (Subject)] および [電子メール本文 (Email body)] を指定します。電子メール メッセージに含まれる、ゲスト アカウント情報を指定するには、事前定義済みの変数を使用します。テキストをカスタマイズするには、ミニエディタと HTML タグを使用します。たとえば、リクエスト承認の電子メールにスポンサー ポータルへのリンクを含めるには、[リンクを作成 (Create a Link)] ボタンをクリックして、スポンサー ポータルに FQDN を追加します。
- c) [テスト電子メールの送信 (Send Test Email)] を使用してすべてのデバイスでカスタマイズをプレビューし、適切に表示されることを確認します。
- d) 忘れずに [保存 (Save)] をクリックしてから、[閉じる (Close)] をクリックしてください。

ステップ 2 スポンサーが送信する承認電子メールの内容をカスタマイズします。[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [スポンサー ポータル (Sponsor Portals)] の順に選択し、[ポータル ページのカスタマイズ (Portal Page Customization)] を選択してから、[メール通知 (Email Notification)] タブを選択します。

エラー メッセージの編集

ゲスト、スポンサー、および従業員に表示される [失敗 (Failure)] ページに表示されるエラー メッセージを完全にカスタマイズできます。[失敗 (Failure)] ページは、ブラックリスト ポータルを除くすべてのエンドユーザ Web ポータルで利用可能です。

ステップ 1 次のいずれかを実行します。

- ゲスト ポータルの場合は、[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [ゲスト ポータル (Guest Portals)] > [編集 (Edit)] > [ポータル ページのカスタマイズ (Portal Page Customization)] > [メッセージ (Messages)] > [エラー メッセージ (Error Messages)] の順に選択します。
- スポンサー ポータルの場合は、[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [スポンサー ポータル (Sponsor

Portals)] > [編集 (Edit)] > [ポータル ページのカスタマイズ (Portal Page Customization)] > [メッセージ (Messages)] > [エラー メッセージ (Error Messages)] の順に選択します。

- デバイス ポータルの場合は、[管理 (Administration)] > [デバイス ポータル管理 (Device Portal Management)] > (任意のポータル) > [編集 (Edit)] > [ポータル ページのカスタマイズ (Portal Page Customization)] > [メッセージ (Messages)] > [エラー メッセージ (Error Messages)] を選択します。

ステップ 2 [表示言語 (View In)] ドロップダウンから、メッセージのカスタマイズ時にテキストを表示する言語を選択します。

このドロップダウンリストには、特定のポータルに関連付けられた言語ファイルのすべての言語が含まれています。ポータルページのカスタマイズ時に行った変更でサポート対象の言語プロパティファイルを更新します。

ステップ 3 エラー メッセージ テキストを更新します。特定のエラー メッセージを検索するには、エラー メッセージに関連付けられた AUP を検索する **aup** などのキーワードを入力します。

ステップ 4 [保存 (Save)] をクリックし、[閉じる (Close)] をクリックします。



第 **V** 部

Cisco ISE サービスの有効化および設定

- [ポリシー条件の設定 \(659 ページ\)](#)
- [認証ポリシーの管理 \(675 ページ\)](#)
- [許可ポリシーおよびプロファイルの管理 \(717 ページ\)](#)
- [脅威中心型 NAC サービスの設定 \(737 ページ\)](#)
- [スマート ライセンス サービスおよび Smart Call Home サービスの設定 \(761 ページ\)](#)
- [Cisco ISE エンドポイント プロファイリング ポリシー \(769 ページ\)](#)
- [クライアント プロビジョニングの設定 \(857 ページ\)](#)
- [クライアント ポスチャ ポリシーの設定 \(931 ページ\)](#)
- [Cisco TrustSec ポリシーの設定 \(971 ページ\)](#)



第 19 章

ポリシー条件の設定

- [ポリシー条件 \(659 ページ\)](#)
- [単純条件と複合条件 \(659 ページ\)](#)
- [ポリシー評価 \(660 ページ\)](#)
- [単純条件の作成 \(661 ページ\)](#)
- [複合条件の作成 \(661 ページ\)](#)
- [プロファイラ条件 \(662 ページ\)](#)
- [ポストチャ条件 \(663 ページ\)](#)
- [パッチ管理条件の作成 \(668 ページ\)](#)
- [ディスク暗号化条件の作成 \(669 ページ\)](#)
- [ネットワーク条件 \(669 ページ\)](#)
- [時刻と日付の条件の作成 \(672 ページ\)](#)

ポリシー条件

Cisco ISE はポリシー ベースのネットワーク アクセス制御ソリューションで、ネットワーク アクセス、ゲスト、ポストチャ、クライアントプロビジョニング、プロファイラの各種サービスを提供します。Cisco ISE の設定時に、認証、許可、ゲスト、ポストチャ、およびプロファイラのポリシーを作成します。ポリシー条件は、ポリシーの基本的な構成要素です。ポリシー条件には、単純条件と複合条件の 2 種類のポリシー条件があります。

この章では、ポリシー条件と、Cisco ISE が提供するさまざまなサービス用にこれらを作成する方法について説明します。

単純条件と複合条件

Cisco ISE は、ネットワーク アクセス、プロファイラ、ポストチャ、ゲスト サービスを提供するために、ルールベースのポリシーを使用します。これらのルールベースのポリシーは、条件で構成されたルールで構成されます。Cisco ISE では、個別の再利用可能なポリシー要素として条件を作成でき、これらの条件は別のルールベースのポリシーから参照することが可能です。条件には次の 2 種類があります。

- 単純条件：単純条件は、オペランド（属性）、演算子（equal to、not equal to、greater than など）、および値で構成されています。単純条件を保存して、他のルールベースのポリシーで使用できます。

単純条件は、A オペランド B の形式をとります。ここで、A は Cisco ISE ディクショナリ内の任意の属性とすることができ、B は属性 A がとり得るいずれかの値とすることができ、デバイス タイプは、すべてのネットワーク デバイスの属性として使用され、値としてすべてのデバイス タイプを含めることができます。次の形式で、A Equals B を意味します。

DEVICE:Device Type Equals All Device Types

- 複合条件：複合条件は、1 つ以上の単純条件で構成され、AND または OR 演算子で接続されます。複合条件は、単純条件に基づいて構成されます。複合条件を保存して、他のルールベースのポリシーで再利用できます。

複合条件は、次のいずれかの形式にできます。

- (X オペランド Y) AND (A オペランド B) AND (X オペランド Z) AND (以下同様)
- (X オペランド Y) OR (A オペランド B) OR (X オペランド Z) OR (以下同様)

ここで、X および A はユーザ名やデバイス タイプなどの Cisco ISE ディクショナリの属性です。

次に、複合条件の例を示します。

[DEVICE]:[モデル名 (Model Name)] [一致 (Matches)] [Catalyst6K] [AND] [ネットワークへのアクセス (Network Access)] [使用例 (Use Case)] [等しい (Equals)] [ホストルックアップ (Host Lookup)]。

ポリシーで使用されているか、または複合条件の一部である条件を削除できません。

ポリシー評価

ポリシーはルールで構成され、各ルールは満たされるべき条件で構成され、この条件によって、ネットワーク リソースへのアクセスなどのアクションの実行が許可されます。ルールベースの条件は、ポリシーの基盤、つまり要求を評価するときに使用するルールのセットを形成します。

実行時に、Cisco ISE はポリシー条件を評価し、ポリシー評価が true または false 値のどちらを返すかに応じて、定義されている結果を適用します。

ポリシー条件の評価時に、Cisco ISE は属性と値を比較します。ポリシー条件で指定された属性に、要求内で割り当てられた値が含まれていない場合があります。このとき、比較に使用されている演算子が「not equal to」である場合、この条件は true と評価されます。その他の場合、この条件は false と評価されます。

たとえば、「Radius.Calling_Station_ID Not Equal to 1.1.1.1」という条件で RADIUS 要求に Calling Station ID が存在しない場合、この条件は true と評価されます。この評価は RADIUS ディクショナリに特有なものではなく、「Not Equal to」演算子の使用に起因して発生します。

ISE では、[ポリシー セット (Policy Sets)] テーブルには、現在システムに設定されているすべてのポリシー セットのリストが表示されます。有効なポリシー セットの順序によって、エンドポイントがアクセスを要求するたびにシステムが関連するポリシー セットを検索する順序が決まります。[ポリシー (Policy)] ページの最後の行は、他の設定されたポリシー セットのいずれかの要求と一致するルールが 1 つもない場合に適用されるデフォルト ポリシーです。デフォルト ポリシー セットでは許可されたプロトコルと ID ソースの選択を編集できますが、削除することはできません。

単純条件の作成

単純条件を作成し、認証ポリシー、許可ポリシー、またはゲストポリシーの定義時に再利用できます。

始める前に

次のタスクを実行するには、スーパー管理者またはポリシー管理者である必要があります。

- ステップ 1 [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [条件 (Conditions)] を選択します。
- ステップ 2 [認証 (Authentication)]、[許可 (Authorization)]、または [ゲスト (Guest)] の隣の矢印をクリックして、[単純条件 (Simple Conditions)] をクリックします。
- ステップ 3 [追加 (Add)] をクリックします。
- ステップ 4 [名前 (Name)]、[説明 (Description)]、[属性 (Attribute)]、[演算子 (Operator)]、および [値 (Value)] フィールドに適切な値を入力します。

単純条件で ID グループを指定する場合、これらを次のように必ず FQDN 形式で表記してください。

(InternalUser:IdentityGroup) : Equal : (UserIdentityGroups: Identity Group Name)

Cisco ISE では、(InternalUser:IdentityGroup) : Equal : (Identity Group Name) 形式の ID グループ エントリを正確に解決できません。

- ステップ 5 [送信 (Submit)] をクリックして、条件を保存します。

関連トピック

[ポリシー評価](#) (660 ページ)

[単純条件と複合条件](#) (659 ページ)

複合条件の作成

複合条件を作成し、認証ポリシーの定義時に再利用できます。

始める前に

- Cisco ISEには、最も一般的な使用例の一部に関する事前定義された複合条件が含まれています。これらの事前定義された条件を要件に合わせて編集できます。
- 次のタスクを実行するには、スーパー管理者またはポリシー管理者である必要があります。

-
- ステップ 1** [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [条件 (Conditions)] を選択します。
- ステップ 2** [認証 (Authentication)]、[許可 (Authorization)]、または[ゲスト (Guest)]の隣の矢印をクリックして、[複合条件 (Compound Conditions)] をクリックします。
- ステップ 3** [追加 (Add)] をクリックします。
- ステップ 4** 複合条件の名前を入力します。任意で説明を入力できます。
- ステップ 5** [既存の条件をライブラリから選択 (Select Existing Condition from Library)] をクリックして既存の単純条件を選択するか、[新しい条件の作成 (Create New Condition)] をクリックして、式ビルダーから属性、演算子、および値を選択します。
- ステップ 6** 条件をさらに追加するには、この行の末尾の[操作 (action)] アイコンをクリックします。
- ステップ 7** [属性/値の追加 (Add Attribute/Value)] をクリックして新しい条件を作成するか、[条件をライブラリから追加 (Add Condition from Library)] をクリックして既存の単純条件を追加します。
- ステップ 8** ドロップダウンリストから、オペランドを選択します。[AND] または [OR] を選択できます。この複合条件のすべての条件間で同じオペランドが使用されます。
- ステップ 9** [送信 (Submit)] をクリックして複合条件を作成します。
-

関連トピック

[ポリシー評価 \(660 ページ\)](#)

[単純条件と複合条件 \(659 ページ\)](#)

プロファイラ条件

プロファイラ条件はポリシー要素であり、他の条件とほとんど同じです。ただし、認証、許可、およびゲスト条件とは異なり、プロファイリング条件は限られた数の属性に基づいています。[プロファイラ条件 (Profiler Conditions)] ページに Cisco ISE で使用できる属性とその説明が表示されます。

プロファイラ条件は次のとおりです。

- シスコ提供：Cisco ISE には展開時に事前定義されたプロファイリング条件が含まれており、[プロファイラ条件 (Profiler Conditions)] ページでシスコ提供の条件として識別されます。シスコ提供のプロファイリング条件を削除することはできません。
- [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [ディクショナリ (Dictionaries)] > [システム (System)] からアクセスできる場所にあるシステムプロファイラディクショナリにもシスコ提供条件があります。

たとえば、MAC ディクショナリです。一部の製品では、OUI（固有識別子情報）がデバイスの製造組織を識別するために最初に使用できる固有属性です。これはデバイスの MAC アドレスのコンポーネントです。MAC ディクショナリには、MACAddress および OUI 属性が含まれています。

- 管理者作成：ユーザが Cisco ISE の管理者として作成するプロファイラ条件、複製された事前定義済みのプロファイリング条件は管理者作成として識別されます。[プロファイラ条件（Profiler Conditions）] ページでプロファイラ ディクショナリを使用して、DHCP、MAC、SNMP、IP、RADIUS、NetFlow、CDP、LLDP、および NMAP タイプのプロファイラ条件を作成できます。

プロファイリング ポリシーの数の推奨上限は 1000 ですが、最高 2000 までプロファイリング ポリシーを拡張できます。

プロファイラ条件の作成

Cisco ISE のエンドポイント プロファイリング ポリシーを使用すると、ネットワーク上で検出されたエンドポイントを分類し、特定のエンドポイント ID グループに割り当てることができます。これらのエンドポイント プロファイリング ポリシーは、エンドポイントを分類し、グループ化するために Cisco ISE が評価するプロファイリング条件から構成されます。

始める前に

次のタスクを実行するには、スーパー管理者またはポリシー管理者である必要があります。

-
- ステップ 1 [ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [プロファイリング（Profiling）] > [追加（Add）] を選択します。
 - ステップ 2 [エンドポイントプロファイリングポリシーの設定（1358ページ）](#) の説明に従って、フィールドに値を入力します。
 - ステップ 3 [送信（Submit）] をクリックして、プロファイラ条件を保存します。
 - ステップ 4 さらに多くの条件を作成するには、この手順を繰り返します。
-

関連トピック

[プロファイラ条件](#)（662 ページ）

ポスチャ条件

ポスチャ条件は次の単純条件のいずれかになります。ファイル、レジストリ、アプリケーション、サービス、またはディクショナリ条件。これらの単純条件のうちの1つ以上の条件によって複合条件が形成され、複合条件はポスチャ要件と関連付けることができます。

ネットワークに Cisco ISE を初めて展開する場合は、Web からポスチャ更新をダウンロードできます。このプロセスは、初期ポスチャ更新と呼ばれます。

初期ポスチャ更新の後、Cisco ISE はシスコ定義の単純および複合条件も作成します。シスコ定義の単純条件はプレフィクスとして `pc_` が付けられ、複合条件はプレフィクスとして `pr_` が付けられています。

ダイナミック ポスチャ更新の結果としてシスコ定義の条件を Web を介してダウンロードするように Cisco ISE を設定することもできます。シスコ定義のポスチャ条件を削除または編集することはできません。

ユーザ定義の条件やシスコ定義の条件には、単純条件と複合条件の両方が含まれます。

単純ポスチャ条件

ポスチャ ナビゲーション ペインを使用して、次の単純条件を管理できます。

- ファイル条件：ファイルの存在、ファイルの日付、およびクライアントのファイルバージョンを確認する条件。
- レジストリ条件：レジストリ キーの存在またはクライアントのレジストリ キーの値を確認する条件。
- アプリケーション条件：アプリケーション（プロセス）がクライアント上で実行されているかまたは実行されていないかを確認する条件。
- サービス条件：サービスがクライアント上で実行されているかまたは実行されていないかを確認する条件。
- ディクショナリ条件：ディクショナリ属性と値を確認する条件。
- USB 条件：USB マス ストレージ デバイスの有無をチェックする条件。

関連トピック

[ファイル条件の設定](#)（1369 ページ）

[レジストリ条件の設定](#)（1377 ページ）

[アプリケーション条件の設定](#)

[サービス条件の設定](#)（1381 ページ）

[ディクショナリ単純条件の設定](#)（1393 ページ）

[USB 条件の設定](#)（1399 ページ）

単純ポスチャ条件の作成

ポスチャポリシーまたは他の複合条件で使用できる、ファイル、レジストリ、アプリケーション、サービス、およびディクショナリ単純条件を作成できます。

始める前に

次のタスクを実行するには、スーパー管理者またはポリシー管理者である必要があります。

-
- ステップ 1** [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [条件 (Conditions)] > [ポスチャ (Posture)] を選択します。
- ステップ 2** [ファイル (File)]、[レジストリ (Registry)]、[アプリケーション (Application)]、[サービス (Service)]、または[ディクショナリ単純条件 (Dictionary Simple Condition)] のいずれかを選択します。
- ステップ 3** [追加 (Add)] をクリックします。
- ステップ 4** フィールドに適切な値を入力します。
- ステップ 5** [送信 (Submit)] をクリックします。
-

複合ポスチャ条件

複合条件は、1つ以上の単純条件、または複合条件で構成されます。ポスチャ ポリシーを定義する場合、次の複合条件を使用できます。

- 複合条件：1つ以上の単純条件、またはタイプがファイル、レジストリ、アプリケーション、またはサービス条件の複合条件が含まれます
- アンチウイルス複合条件：1つ以上の AV 条件、または AV 複合条件が含まれます
- アンチスパイウェア複合条件：1つ以上の AS 条件、または AS 複合条件が含まれます
- ディクショナリ複合条件：1つ以上のディクショナリ単純条件またはディクショナリ複合条件が含まれます
- マルウェア対策条件：1つ以上の AM 条件が含まれます

Windowsクライアントでの自動アップデートを有効にするためのシスコ事前定義の条件

pr_AutoUpdateCheck_Ruleはシスコによって事前定義された条件であり、[複合条件 (Compound Conditions)] ページにダウンロードされます。この条件を使用すると、Windows クライアント上で自動アップデート機能が有効になっているかどうかを確認することができます。Windows クライアントがこの要件を満たさない場合、ネットワークアクセスコントロール (NAC) エージェントによって、Windows クライアントの自動アップデート機能が強制的に有効になります (修復)。この修復後、Windows クライアントはポスチャ準拠になります。自動アップデート機能が Windows クライアント上で有効になっていない場合は、ポスチャ ポリシーで関連付けた Windows Update 修復で Windows 管理者設定を上書きします。

シスコ事前設定済みアンチウイルスおよびアンチスパイウェア条件

Cisco ISE の [AV 複合条件 (AV Compound Condition)] および [AS 複合条件 (AS Compound Condition)] ページには、アンチウイルスとアンチスパイウェアの事前設定済みの複合条件がロードされます。これらの条件は、Windows および Macintosh オペレーティング システムのアンチウイルスおよびアンチスパイウェアサポート表で定義されます。これらの複合条件では、指定されたアンチウイルスとアンチスパイウェア製品がすべてのクライアント上に存在するか

どうかを確認できます。Cisco ISE で新しいアンチウイルスとアンチスパイウェアの複合条件を作成することもできます。

アンチウイルスとアンチスパイウェア サポート表

Cisco ISE は、各ベンダー製品の最新バージョンおよび定義ファイルの日付を提供するアンチウイルスとアンチスパイウェアサポート表を使用します。ユーザは頻繁にアンチウイルスとアンチスパイウェアサポート表をポーリングする必要があります。アンチウイルスとアンチスパイウェアのベンダーはアンチウイルスとアンチスパイウェア定義ファイルを頻繁に更新するため、各ベンダー製品の最新バージョンおよび定義ファイルの日付を検索します。

新しいアンチウイルスとアンチスパイウェアのベンダー、製品、リリースのサポートを反映するようにアンチウイルスとアンチスパイウェア サポート表が更新されるたびに、NAC Agent は新しいアンチウイルスとアンチスパイウェア ライブラリを受け取ります。これは、NAC Agent がより新しい追加機能をサポートするのに役立ちます。NAC Agent がこのサポート情報を取得すると、定期的に更新される `se-checks.xml` ファイル（`se-templates.tar.gz` アーカイブで `se-rules.xml` ファイルとともに公開される）で最新の定義情報をチェックし、クライアントがポリシーに準拠しているかどうかを決定します。特定のアンチウイルスまたはアンチスパイウェア製品のアンチウイルスとアンチスパイウェアライブラリによってサポートされている機能に応じて、適切な要件が NAC Agent に送信され、ポストチャ検証中にクライアント上でそれらの存在、および特定のアンチウイルスおよびアンチスパイウェア製品のステータスが検証されます。

アンチウイルスとアンチスパイウェア サポート表は、[Cisco.com](https://www.cisco.com) で参照できます。

コンプライアンス モジュール

コンプライアンス モジュールには、ベンダー名、製品バージョン、製品名、および Cisco ISE のポストチャ条件をサポートする OPSWAT が提供する属性などのフィールドのリストが含まれています。

ベンダーは頻繁に製品バージョンや定義ファイルの日付を更新するので、頻繁にアップデートのコンプライアンス モジュールをポーリングすることで、各ベンダーの製品の最新バージョンおよび定義ファイルの日付を調べる必要があります。新しいベンダー、製品、およびリリースのサポートを反映してコンプライアンス モジュールが更新されるたびに、AnyConnectのエージェントは新しいライブラリを受信します。これは、AnyConnectのエージェントがより新しい追加機能をサポートするのに役立ちます。AnyConnectのエージェントがこのサポート情報を取得すると、定期的に更新される `se-checks.xml` ファイル（`se-templates.tar.gz` アーカイブで `se-rules.xml` ファイルとともに公開される）で最新の定義情報をチェックし、クライアントがポリシーに準拠しているかどうかを決定します。特定のアンチウイルス、アンチスパイウェア、マルウェア対策、ディスク暗号化またはパッチ管理製品のライブラリによってサポートされている機能に応じて、適切な要件が AnyConnect エージェントに送信され、ポストチャ検証中にクライアント上でそれらの存在、およびクライアントでの特定の製品のステータスが検証されます。

コンプライアンス モジュールは、[Cisco.com](https://www.cisco.com) で入手可能です。

ISE ポスチャポリシーをサポートするまたはしない OPSWAT API バージョンを次に示します。バージョン3および4をサポートするエージェントごとに異なるポリシールールがあります。

ポスチャ条件	コンプライアンス モジュールのバージョン
OPSWAT	
アンチウイルス	3.x 以前
スパイウェア対策	3.x 以前
マルウェア対策	4.x 以降
ディスク暗号化	3.x 以前および 4.x 以降
パッチ管理	3.x 以前および 4.x 以降
USB	4.x 以降
非 OPSWAT	
ファイル (File)	すべてのバージョン
Application	すべてのバージョン
複合	すべてのバージョン
レジストリ	すべてのバージョン
サービス	すべてのバージョン



- (注) 上記のバージョンのいずれかがインストールされた可能性のあるクライアントを予測して、バージョン 3.x 以前およびバージョン 4.x 以降用に別個のポスチャ ポリシーを作成する必要があります。



- (注) OESIS バージョン 4 のサポートはコンプライアンス モジュール 4.x および Cisco AnyConnect 4.3 以降に提供されます。しかし、AnyConnect 4.3 は OESIS バージョン 3 とバージョン 4 のポリシーの両方をサポートします。



- (注) バージョン 4 コンプライアンス モジュールは、ISE 2.1 以降でサポートされています。

複合ポスチャ条件の作成

ポスチャ評価と検証のポスチャ ポリシーで使用できる複合条件を作成できます。

始める前に

次のタスクを実行するには、スーパー管理者またはポリシー管理者である必要があります。

-
- ステップ 1** [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [条件 (Conditions)] > [ポスチャ (Posture)] > [複合条件 (Compound Conditions)] > [追加 (Add)] を選択します。
- ステップ 2** フィールドに適切な値を入力します。
- ステップ 3** 条件を検証するために [式の確認 (Validate Expression)] をクリックします。
- ステップ 4** [送信 (Submit)] をクリックします。
-

関連トピック

[ポスチャ条件](#) (663 ページ)

[単純ポスチャ条件](#) (664 ページ)

[複合ポスチャ条件](#) (665 ページ)

[Windows クライアントでの自動アップデートを有効にするためのシスコ事前定義の条件](#) (665 ページ)

[シスコ事前設定済みアンチウイルスおよびアンチスパイウェア条件](#) (665 ページ)

パッチ管理条件の作成

選択したベンダーのパッチ管理製品のステータスを確認するポリシーを作成できます。

たとえば、Microsoft System Center Configuration Manager (SCCM)、クライアントバージョン 4.x ソフトウェア製品がエンドポイントにインストールされているかどうかを確認する条件を作成できます。



(注) Cisco ISE および AnyConnect のサポート対象バージョンは次のとおりです。

- Cisco ISE バージョン 1.4 以降
 - AnyConnect バージョン 4.1 以降
-

始める前に

次のタスクを実行するには、スーパー管理者またはポリシー管理者である必要があります。

-
- ステップ 1** [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [条件 (Conditions)] > [ポスチャ (Posture)] > [パッチ管理条件 (Patch Management Condition)] を選択します。
- ステップ 2** [追加 (Add)] をクリックします。
- ステップ 3** [パッチ管理条件 (Patch Management Condition)] ページで、フィールドに適切な値を入力します。
-

ステップ 4 [送信 (Submit)] をクリックします。

関連トピック

[パッチ管理条件の設定](#) (1395 ページ)

[パッチ管理修復の追加](#) (953 ページ)

ディスク暗号化条件の作成

エンドポイントが指定されたデータ暗号化ソフトウェアに準拠しているかどうかを確認するポリシーを作成できます。

たとえば、C: ドライブがエンドポイントで暗号化されているかどうかを確認する条件を作成できます。C: ドライブが暗号化されていない場合、エンドポイントはコンプライアンス違反通知を受信し、ISE はメッセージをログに記録します。

始める前に

次のタスクを実行するには、スーパー管理者またはポリシー管理者である必要があります。AnyConnect ISE ポスチャ エージェントを使用している場合にのみ、ポスチャ要件とディスク暗号化条件を関連付けることができます。

ステップ 1 [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [条件 (Conditions)] > [ポスチャ (Posture)] > [ディスク暗号化条件 (Disk Encryption Condition)] を選択します。

ステップ 2 [追加 (Add)] をクリックします。

ステップ 3 [ディスク暗号化条件 (Disk Encryption Condition)] ページで、フィールドに適切な値を入力します。

ステップ 4 [送信 (Submit)] をクリックします。

ネットワーク条件

ポリシーは、一連の条件と結果で構成されています。ポリシー条件は、オペランド（属性）、演算子（equal to、not equal to、greater than など）、および値で構成されています。複合条件は、1 つ以上の単純条件で構成され、それぞれの条件が AND または OR 演算子で結合されています。実行時に、Cisco ISE はポリシー条件を評価し、ポリシー評価が true または false 値のどちらを返すかに応じて、定義された結果を適用します。

各ネットワーク条件は、オブジェクトのリストを定義します。このリストはポリシー条件に含めることができ、これにより、要求で示される定義と照合される定義セットになります。

演算子 EQUALS true を使用して、ネットワーク条件が true であるかどうか（要求に指定されている値がネットワーク条件の 1 つ以上のエントリと一致しているかどうか）を確認するか、または EQUALS false を使用して、ネットワーク条件が false であるかどうか（ネットワーク条件のどのエントリとも一致しないかどうか）を確認することができます。

ネットワーク条件を作成して名前を付けたら、ネットワーク条件ディクショナリからこのネットワーク条件を選択して、さまざまなルールやポリシーでこの条件を繰り返し使用できます。次に例を示します。

```
Network Conditions.MyNetworkCondition EQUALS true
```

次のネットワーク条件を作成してネットワークへのアクセスを制限することができます。

- エンドステーション ネットワーク条件 (Endstation Network Conditions) : 接続が開始および終了されるエンドステーションに基づきます。

Cisco ISE はリモート アドレスの [TO] フィールド (TACACS+ 要求または RADIUS 要求であるかに基づいて取得) を評価し、これがエンドポイントの IP アドレス、MAC アドレス、発信側回線 ID (CLI)、または着信番号識別サービス (DNIS) のいずれであるかを確認します。

RADIUS 要求では、この ID は属性 31 (Calling-Station-Id) で使用できます。

TACACS+ 要求では、リモート アドレスにスラッシュ (/) が含まれている場合、スラッシュより前の部分は [FROM] の値として見なされ、スラッシュより後の部分は [TO] 値として見なされます。たとえば、要求に CLI/DNIS と指定されている場合、CLI は [FROM] の値と見なされ、DNIS は [TO] の値と見なされます。スラッシュが含まれていない場合は、リモート アドレス全体が [FROM] の値として見なされます (IP アドレス、MAC アドレス、CLI いずれの場合でも)。

- デバイス ネットワーク条件 (Device Network Conditions) : 要求を処理する AAA クライアントに基づきます。

ネットワーク デバイスは、IP アドレス、ネットワーク デバイス リポジトリで定義されているデバイス名、またはネットワーク デバイス グループによって識別されます。

RADIUS 要求では、属性 4 (NAS-IP-Address) が指定されている場合、Cisco ISE はこの属性から IP アドレスを取得します。属性 32 (NAS-Identifier) が存在する場合、Cisco ISE は属性 32 から IP アドレスを取得します。これらの属性が存在しない場合は、受信したパケットから IP アドレスを取得します。

デバイスディクショナリ (NDGディクショナリ) にはネットワーク デバイス グループ属性 (Location、Device Type、または NDG を表すその他の動的に作成された属性など) が含まれています。これらの属性には、現在のデバイスに関連するグループが含まれています。

- [デバイス ポート ネットワーク条件 (Device Port Network Conditions)] : デバイスの IP アドレス、名前、NDG、およびポート (エンドポイントが接続しているデバイスの物理ポート) に基づきます。

RADIUS 要求では、属性 5 (NAS-Port) が要求内に存在する場合、Cisco ISE はこの属性から値を取得します。属性 87 (NAS-Port-Id) が要求内に存在する場合、Cisco ISE は属性 87 から要求を取得します。

TACACS+ 要求では、Cisco ISE はその ID を (すべてのフェーズの) 開始要求のポート フィールドから取得します。

エンドステーション ネットワーク条件の設定

ステップ 1 [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [条件 (Conditions)] > [ネットワーク条件 (Network Conditions)] > [エンドステーション ネットワーク条件 (Endstation Network Conditions)] の順に選択します。

ステップ 2 [追加 (Add)] をクリックします。

ステップ 3 ネットワーク条件の名前と説明を入力します。

ステップ 4 次の詳細を入力します。

- **IP アドレス** : IP アドレスまたはサブネットの一覧を、1 行に 1 つ追加できます。IP アドレス/サブネットは IPv4 または Ipv6 形式で指定できます。
- **MAC アドレス** : カンマ区切りのエンドステーション MAC アドレスと宛先 MAC アドレスの一覧を入力できます。各 MAC アドレスには 12 桁の 16 進数を含め、次の形式のいずれかで指定してください。
nn.nn.nn.nn.nn.nn、nn-nn-nn-nn-nn-nn、nnnn.nnnn.nnnn、nnnnnnnnnnnnnn。
エンドステーション MAC または宛先 MAC が必要でない場合は、代わりにトークン「-ANY-」を使用します。
- **CLI/DNIS** : カンマ区切りの発信者 ID (CLI) および受信者 ID (DNIS) の一覧を追加できます。発信者 ID (CLI) または受信者 ID (DNIS) が必要でない場合は、代わりにトークン「-ANY-」を使用します。

ステップ 5 [送信 (Submit)] をクリックします。

デバイス ネットワーク条件の設定

ステップ 1 [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [条件 (Conditions)] > [ネットワーク条件 (Network Conditions)] > [デバイス ネットワーク条件 (Device Network Conditions)] の順に選択します。

ステップ 2 [追加 (Add)] をクリックします。

ステップ 3 ネットワーク条件の名前と説明を入力します。

ステップ 4 次の詳細を入力します。

- **IP アドレス** : IP アドレスまたはサブネットの一覧を、1 行に 1 つ追加できます。IP アドレス/サブネットは IPv4 または Ipv6 形式で指定できます。
- **デバイス名 (Device Name)** : デバイス名の一覧を、1 行に 1 つ追加することができます。ネットワーク デバイス オブジェクトで設定されているものと同じデバイス名を入力する必要があります。
- **[デバイス グループ (Device Groups)]** : ルート NDG、カンマ、(ルート NDG 配下の) NDG の順でタプル一覧を追加できます。タプルは、1 行に 1 つにする必要があります。

ステップ 5 [送信 (Submit)] をクリックします。

デバイス ポート ネットワーク条件の設定

ステップ 1 [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [条件 (Conditions)] > [ネットワーク条件 (Network Conditions)] > [デバイス ポート ネットワーク条件 (Device Port Network Conditions)] の順に選択します。

ステップ 2 [追加 (Add)] をクリックします。

ステップ 3 ネットワーク条件の名前と説明を入力します。

ステップ 4 次の詳細を入力します。

- IP アドレス (IP Addresses) : 次の順序で詳細を入力します。IP アドレスまたはサブネット、カンマ、(デバイスによって使用される) ポート。タプルは、1 行に 1 つにする必要があります。
- デバイス (Devices) : 次の順序で詳細を入力します。デバイス名、カンマ、ポート。タプルは、1 行に 1 つにする必要があります。ネットワーク デバイス オブジェクトで設定されているものと同じデバイス名を入力する必要があります。
- デバイス グループ (Device Groups) : 次の順序で詳細を入力します。ルート NDG、カンマ、(ルート下の) NDG、ポート。タプルは、1 行に 1 つにする必要があります。

ステップ 5 [送信 (Submit)] をクリックします。

時刻と日付の条件の作成

[ポリシー要素条件 (Policy Elements Conditions)] ページを使用して、時刻と日付のポリシー要素条件を表示、作成、変更、削除、複製、および検索します。ポリシー要素は、設定した特定の時刻と日付の属性設定に基づく条件を定義する共有オブジェクトです。

時刻と日付の条件を使用すると、Cisco ISE システム リソースにアクセスする権限を、作成した属性設定で指定された特定の時刻と日付に設定または制限できます。

始める前に

次のタスクを実行するには、スーパー管理者またはポリシー管理者である必要があります。

ステップ 1 [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [条件 (Conditions)] > [時刻と日付 (Time and Date)] > [追加 (Add)] を選択します。

ステップ 2 フィールドに適切な値を入力します。

- [標準設定 (Standard Settings)] 領域で、アクセスを提供する日時を指定します。

- [例外 (Exceptions)] 領域で、アクセスを制限する日時の範囲を指定します。

ステップ 3 [送信 (Submit)] をクリックします。



第 20 章

認証ポリシーの管理

- [Cisco ISE 認証ポリシー \(675 ページ\)](#)
- [簡易認証ポリシー \(678 ページ\)](#)
- [ルールベースの認証ポリシー \(681 ページ\)](#)
- [認証用の プロトコルの設定 \(686 ページ\)](#)
- [ネットワーク アクセス サービス \(691 ページ\)](#)
- [ネットワーク アクセス ワーク センター \(695 ページ\)](#)
- [RADIUS プロキシ サーバとして機能する Cisco ISE \(696 ページ\)](#)
- [TACACS+ プロキシ クライアントとして機能する Cisco ISE \(698 ページ\)](#)
- [ロケーションに基づく認証 \(702 ページ\)](#)
- [ポリシー モード \(704 ページ\)](#)
- [簡易認証ポリシーの設定 \(706 ページ\)](#)
- [ルールベースの認証ポリシーの設定 \(707 ページ\)](#)
- [ポリシー セット \(708 ページ\)](#)
- [認証ポリシーの組み込み設定 \(711 ページ\)](#)
- [認証結果の表示 \(714 ページ\)](#)

Cisco ISE 認証ポリシー

認証ポリシーは、Cisco ISE がネットワーク デバイスと通信するために使用するプロトコルを定義します。また、認証に使用するソースを特定します。ポリシーは、一連の条件と結果で構成されています。ポリシー条件は、オペランド（属性）、演算子（equal to、not equal to、greater than など）、および値で構成されています。複合条件は、1 つ以上の単純条件で構成され、それぞれの条件が AND または OR 演算子で結合されています。実行時に、Cisco ISE はポリシー条件を評価し、ポリシー評価が true または false 値のどちらを返すかに応じて、定義された結果を適用します。

認証ポリシーは次の要素で構成されています。

- ネットワーク アクセス サービス：このサービスは次のいずれかとなります。
 - 許可されるプロトコル サービス。初期要求およびプロトコル ネゴシエーションを処理するためのプロトコルを選択します。

- プロキシサービス。外部RADIUSサーバが処理を行うように要求をプロキシします。
- ID ソース：認証に使用する ID ソースまたは ID ソース順序。

インストール後に、認証に使用される Cisco ISE でデフォルトの ID 認証ポリシーが使用できません。認証ポリシーを更新すると、デフォルトの設定が上書きされます。

関連トピック

- [ポリシー条件の評価](#) (676 ページ)
- [サポートされている認証 プロトコル](#) (676 ページ)
- [サポートされる認証タイプおよびデータベース](#) (677 ページ)
- [認証失敗のタイプ：フェイルオーバー](#) (677 ページ)
- [認証ポリシーの用語](#) (678 ページ)

ポリシー条件の評価

ポリシー条件の評価時に、Cisco ISE は属性と値を比較します。ポリシー条件で指定された属性に、要求内で割り当てられた値が含まれていない場合があります。このとき、比較に使用されている演算子が「not equal to」である場合、この条件は **true** と評価されます。その他の場合、この条件は **false** と評価されます。

たとえば、「Radius.Calling_Station_ID Not Equal to 1.1.1.1」という条件の場合に RADIUS 要求に Calling Station ID が存在しない場合、この条件は **true** と評価されます。この評価は RADIUS デictionary に特有なものではなく、「NotEqual to」演算子の使用に起因して発生します。

サポートされている認証 プロトコル

認証 ポリシーの定義時に選択可能なプロトコルを次に示します。

- Password Authentication Protocol (PAP)
- Protected Extensible Authentication Protocol (PEAP)
- Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAPv2)
- Extensible Authentication Protocol-Message Digest 5 (EAP-MD5)
- Extensible Authentication Protocol-Transport Layer Security (EAP-TLS)
- Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST)
- Extensible Authentication Protocol-Tunneled Transport Layer Security (EAP-TTLS; 拡張認証プロトコル - トンネル方式トランスポート層セキュリティ)
- Protected Extensible Authentication Protocol-Transport Layer Security (PEAP-TLS)

関連トピック

- [サポートされる認証タイプおよびデータベース](#) (677 ページ)

[認証ポリシーの用語](#) (678 ページ)

[簡易認証ポリシー](#) (678 ページ)

[ルールベースの認証ポリシー](#) (681 ページ)

サポートされる認証タイプおよびデータベース

認証タイプは、選択されたプロトコルに基づきます。認証タイプはパスワードベースです。認証は、要求内に存在するユーザ名とパスワードを使用してデータベースに対して実行されます。

認証ポリシーの結果である ID 特定方法は、次のいずれかになります。

- アクセスを拒否：ユーザへのアクセスは拒否され、認証は実行されません。
- ID データベース：次のいずれかの単一の ID データベース。
 - 内部ユーザ
 - ゲスト ユーザ
 - 内部エンドポイント
 - Active Directory
 - Lightweight Directory Access Protocol (LDAP) データベース
 - RADIUS トークン サーバ (RSA または SafeWord サーバ)
 - 証明書認証プロファイル
- ID ソース順序：認証に使用する ID データベースの順序。

デフォルトでは、Cisco ISE がユーザ情報の検索に使用する ID ソースは、内部ユーザ データベースです。

認証失敗のタイプ：フェイルオーバー

識別方法としてアクセス拒否を選択した場合、要求への応答として拒否メッセージが送信されます。ID データベースまたは ID ソース順序を選択して、認証が成功した場合、処理は許可ポリシーに対して続行されます。一部の認証は失敗し、その場合次のように分類されます。

- 認証の失敗：クレデンシャルが正しくない、無効なユーザであることなどが原因で認証が失敗したことを示す明確な応答を受信します。アクションのデフォルト コースは拒否です。
- ユーザが見つからない：どの ID データベースでもこのユーザが見つかりませんでした。アクションのデフォルト コースは拒否です。
- 処理の失敗：ID データベース（複数の場合もある）にアクセスできません。アクションのデフォルト コースはドロップです。

Cisco ISE では、認証失敗に対して次のアクションのコースのいずれかを設定することができます。

- [拒否 (Reject)] : 拒否応答が送信されます。
- [ドロップ (Drop)] : 応答は送信されません。
- [続行 (Continue)] : 許可ポリシーに従って Cisco ISE を継続します。

[続行 (Continue)] オプションを選択した場合でも、使用されているプロトコルの制限により Cisco ISE が要求の処理を実行できない場合があります。PEAP、LEAP、EAP-FAST、EAP-TLS、または RADIUS MSCHAP を使用した認証では、認証に失敗したり、ユーザが見つからなかったときには、要求の処理を続行することはできません。

認証に失敗した場合、PAP/ASCII または MAC 認証バイパス (MAB またはホスト ルックアップ) の許可ポリシーの処理を続行できます。その他のすべての認証プロトコルの場合、認証に失敗すると、次のいずれかの状態となります。

- 認証の失敗 : 拒否応答が送信されます。
- ユーザまたはホストが見つからない : 拒否応答が送信されます。
- 処理に問題が発生 : 応答は送信されず、要求はドロップされます。

認証ポリシーの用語

以下は認証ポリシー ページの一般用語の一部です。

- 許可されるプロトコル : 許可されるプロトコルは、ネットワーク リソースへのアクセスを要求するデバイスとの通信に Cisco ISE が使用できるプロトコルのセットを定義します。
- アイデンティティ ソース : Cisco ISE データベースがユーザ情報に使用する ID ソースを定義します。データベースは内部データベースの場合や、Active Directory または LDAP などの外部 ID ソースの場合もあります。一連のデータベースを ID ソース順序に加えて、この順序をポリシー内で ID ソースとしてリストできます。Cisco ISE は、リストされている順序でデータベース内のクレデンシャルを検索します。
- フェールオーバー オプション : 認証に失敗した、ユーザが見つからない、または処理に失敗した場合に Cisco ISE が取るべきアクションのコースを指定できます。

簡易認証ポリシー

簡易認証ポリシーでは、Cisco ISE が通信に使用する、許可されるプロトコルおよび ID ソースまたは ID ソース順序を静的に定義できます。単純なポリシーでは条件を定義できません。Cisco ISE ではすべての条件が満たされていると想定され、次の定義を使用して結果が決まります。

- 常に使用する必要がある許可されるプロトコルおよび ID ソースを静的に定義でき、条件のチェックが必要ない環境では、単純なポリシーを作成できます。

- プロキシ サービスベースの単純なポリシーを作成することもできます。Cisco ISE は、ポリシー サーバに要求をプロキシして、ユーザ認証に使用する ID ソースを決定します。要求が別のポリシー サーバにプロキシされた場合、プロトコル ネゴシエーションは発生しません。ポリシーサーバはどのIDソースを認証に使用するべきかを評価し、応答を Cisco ISE に返します。

関連トピック

[簡易認証ポリシーのフロー](#) (680 ページ)

[簡易認証ポリシー設定のガイドライン](#) (681 ページ)

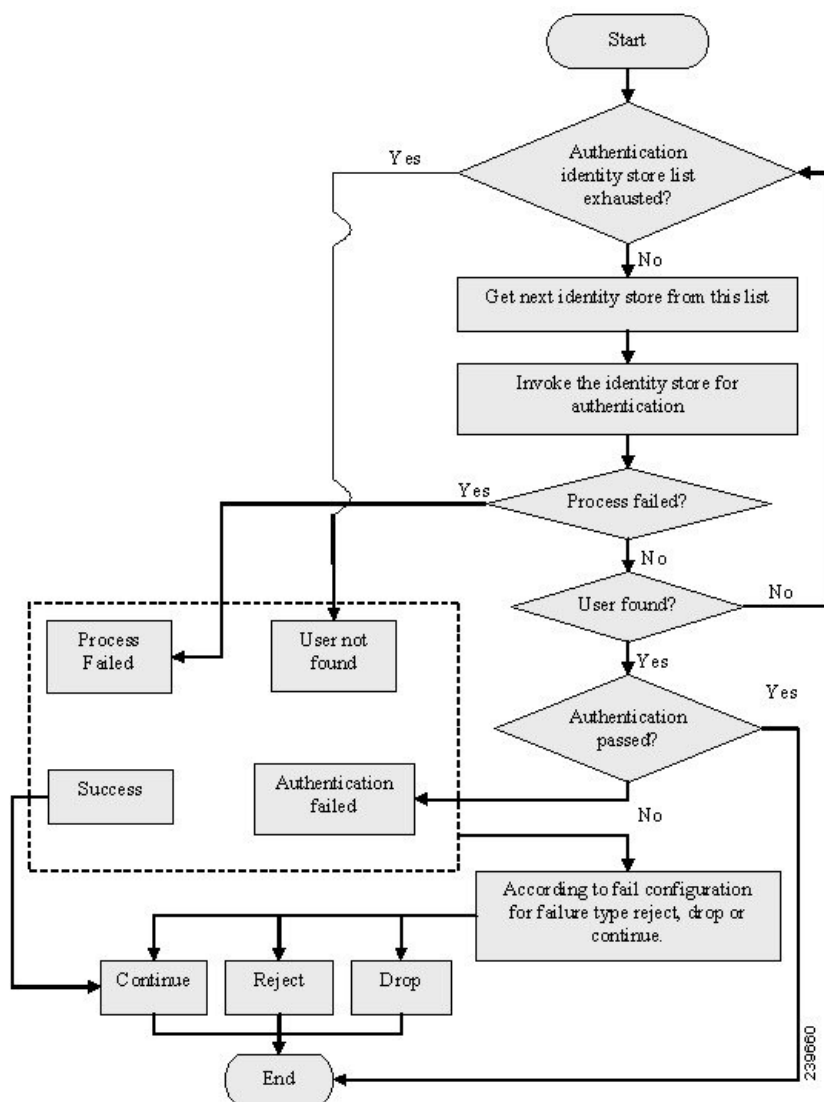
[ネットワーク アクセスの許可されるプロトコルの定義](#) (691 ページ)

[簡易認証ポリシーの設定](#) (706 ページ)

[ルールベースの認証ポリシー](#) (681 ページ)

簡易認証ポリシーのフロー

図 43: 簡易認証ポリシーのフロー



単純なポリシーの結果は、次のいずれかとなります。

- 認証に成功しました
- 認証に失敗しました

認証は次のいずれかの原因で失敗することがあります。

- 正しくないクレデンシャルまたは無効なユーザです。
- ユーザが見つかりません。
- 認証プロセスが失敗しました。

簡易認証ポリシー設定のガイドライン

簡易認証ポリシーを設定するときは、次のガイドラインに従ってください。

- RADIUS サーバ順序を使用する場合は、このアクセスサービスを定義してからポリシーを定義する必要があります。
- ユーザが外部 ID ソースで定義されている場合、ポリシーを定義する前に Cisco ISE でこれらの ID ソースが設定されていることを確認してください。
- ID ソース順序を使用してユーザを認証する場合、ポリシーを定義する前に、ID ソース順序が作成済みであることを確認してください。
- 単純なポリシーとルールベースのポリシーを切り替える場合、最初に設定したポリシーは失われます。たとえば、単純な認証ポリシーを設定した後でルールベースの認証ポリシーに移動すると、単純な認証ポリシーは失われます。また、ルールベースの認証ポリシーから簡易認証ポリシーに移動した場合は、ルールベースの認証ポリシーは失われます。
- ホスト認証は、MAC アドレスのみを使用して実行されます（MAB）。

関連トピック

[RADIUS プロキシ サーバとして機能する Cisco ISE](#)（696 ページ）

ルールベースの認証ポリシー

ルールベースの認証ポリシーは、属性ベースの条件で構成されています。この条件により、要求の処理に使用される許可されるプロトコルおよび ID ソースまたは ID ソース順序が決定されます。単純な認証ポリシーでは、許可されるプロトコルおよび ID ソースを静的に定義できます。ルールベースのポリシーでは、条件を定義することによって、Cisco ISE は許可されるプロトコルおよび ID ソースを動的に選択できるようになります。複数の条件を、Cisco ISE ディクショナリ内の任意の属性を使用して定義できます。

Cisco ISE では、個別の再利用可能なポリシー要素として条件を作成でき、これらの条件は別のルールベースのポリシーから参照することが可能です。ポリシー作成ページ内で条件を作成することも可能です。条件には 2 種類あります。

- 単純条件
- 複合条件

関連トピック

[ディクショナリによってサポートされる属性](#)（683 ページ）

[ルールベースの認証ポリシーの設定](#)（707 ページ）

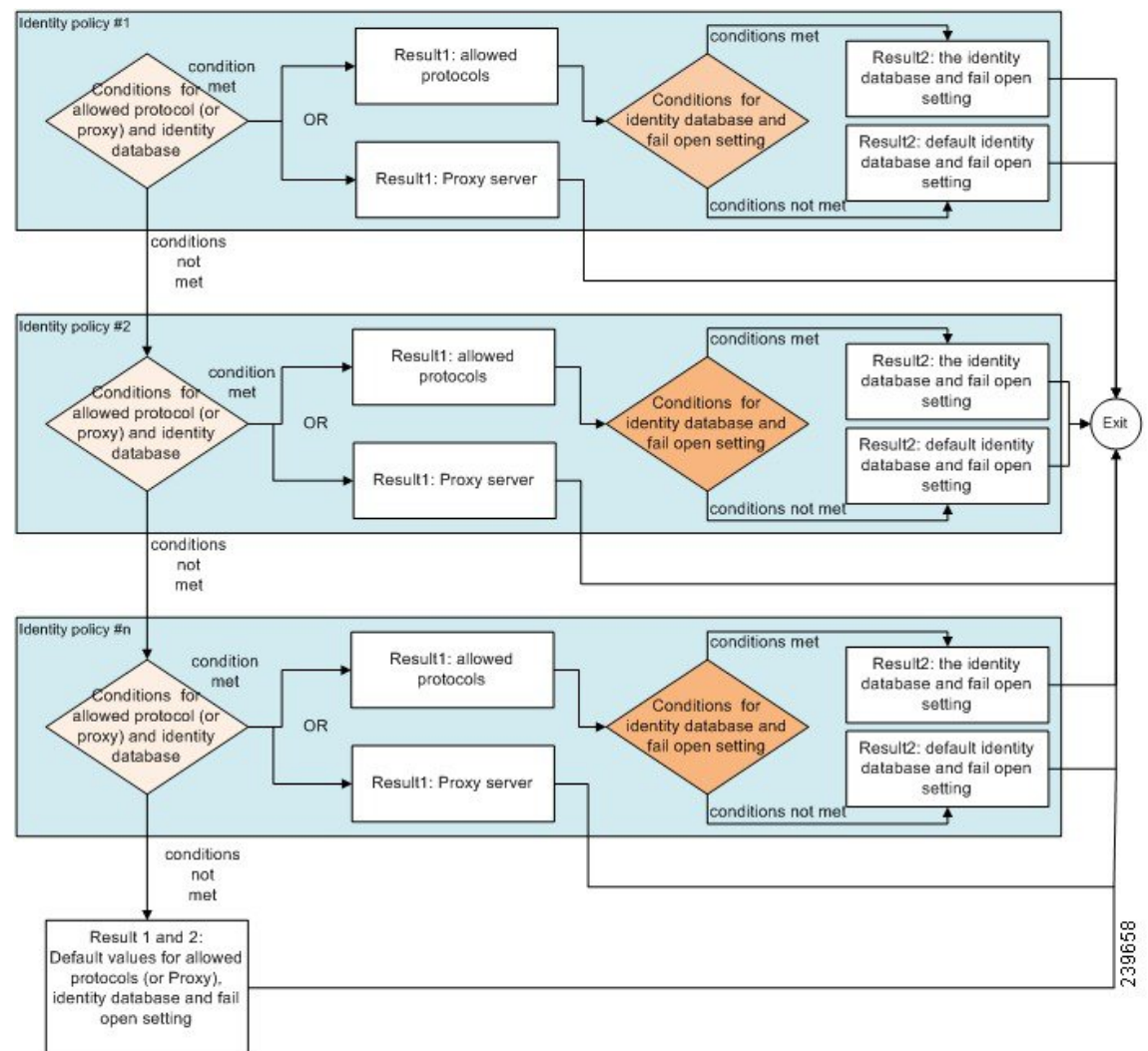
ルールベースの認証ポリシー

ルールベースのポリシーでは、複数のルールを定義できます。ID データベースは、基準に一致する最初のルールに基づいて選択されます。

異なるデータベースで構成される ID ソース順序を定義することもできます。Cisco ISE がデータベースを検索する順序を定義できます。Cisco ISE は、認証が成功するまで指定された順序でこれらのデータベースにアクセスします。1 つの外部データベースに同一ユーザの複数のインスタンスが存在する場合、認証は失敗します。1 つの ID ソース内で、ユーザ レコードは重複できません。

ID ソース順序には、3 つのデータベース、または多くとも 4 つのデータベースを使用することを推奨します。

図 44: ルールベースの認証ポリシー



ルールベースの認証ポリシーのサポート ディクショナリ

Cisco ISE は次のディクショナリをサポートします。

- システム定義されたディクショナリ
 - CERTIFICATE
 - DEVICE
 - RADIUS
- RADIUS ベンダー ディクショナリ
 - Airespace
 - Cisco
 - Cisco-BBSM
 - Cisco-VPN3000
 - Microsoft
 - Network Access

ディクショナリによってサポートされる属性

表に、ディクショナリでサポートされる固定属性を示します。これらの属性をポリシー条件内で使用できます。作成する条件のタイプによっては、使用できない属性もあります。

たとえば、認証ポリシー内でアクセス サービスを選択する条件を作成する場合、使用できるネットワーク アクセス属性は、Device IP Address、ISE Host Name、Network Device Name、Protocol、および Use Case のみです。

次の表に示す属性をポリシー条件に使用できます。

ディクショナリ	属性 (Attributes)	許可されるプロトコルのルールおよびプロキシ	ID ルール
Device	Device Type (定義済みのネットワーク デバイス グループ)	○	○
	Device Location (定義済みのネットワーク デバイス グループ)		
	Other Custom Network Device Group		
	ソフトウェア バージョン (Software Version)		
	モデル名 (Model Name)		

■ ディクショナリによってサポートされる属性

ディクショナリ	属性 (Attributes)	許可されるプロトコルのルールおよびプロキシ	ID ルール
RADIUS	すべての属性	○	○
Network Access	ISE Host Name	○	○
	AuthenticationMethod	なし	○
	AuthenticationStatus	[いいえ (No)]	[いいえ (No)]
	CTSDeviceID	[いいえ (No)]	[いいえ (No)]
	Device IP Address (デバイス IP アドレス)	○	○
	EapAuthentication (マシンのユーザの認証時に使用される EAP 方式)	なし	○
	EapTunnel (トンネルの確立に使用される EAP 方式)	なし	○
	プロトコル	○	○
	UseCase	○	○
	UserName	なし	○
	WasMachineAuthenticated	[いいえ (No)]	[いいえ (No)]

ディクショナリ	属性 (Attributes)	許可されるプロトコルのルールおよびプロキシ	ID ルール
証明書	Common Name	なし	○
	国 (Country)		
	E-mail		
	LocationSubject		
	Organization		
	Organization Unit		
	シリアル番号 (Serial Number)		
	State or Province		
	Subject		
	Subject Alternative Name		
	Subject Alternative Name - DNS		
	Subject Alternative Name - E-mail		
	Subject Alternative Name - Other Name		
	Subject Serial Number		
	発行元 (Issuer)		
	Issuer - Common Name		
	Issuer - Organization		
	Issuer - Organization Unit		
	Issuer - Location		
	Issuer - Country		
	Issuer - Email		
	Issuer - Serial Number		
	Issuer - State or Province		
	Issuer - Street Address		
	Issuer - Domain Component		
	Issuer - User ID		

認証用の プロトコルの設定

これらのプロトコルを使用して認証要求を処理するポリシーセットを作成、保存、実装する前に、Cisco ISE でグローバル プロトコル設定を定義する必要があります。[プロトコル設定 (Protocol Settings)] ページを使用して、ネットワーク内の他のデバイスと通信する Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST)、Extensible Authentication Protocol-Transport Layer Security (EAP-TLS)、および Protected Extensible Authentication Protocol (PEAP) の各プロトコルのグローバル オプションを定義できます。

関連トピック

[認証プロトコルとして EAP-FAST を使用するためのガイドライン](#) (686 ページ)

[EAP-FAST の設定](#) (687 ページ)

[EAP-FAST の PAC の生成](#) (687 ページ)

[EAP-TLS の設定](#) (689 ページ)

[PEAP の設定](#) (689 ページ)

[RADIUS の設定](#) (689 ページ)

認証プロトコルとして EAP-FAST を使用するためのガイドライン

EAP-FAST を認証プロトコルとして使用する場合は、次のガイドラインに従ってください。

- EAP-FAST 受信クライアント証明書が認証されたプロビジョニングで有効な場合は、EAP-TLS 内部方式を有効にすることを強く推奨します。認証されたプロビジョニングの EAP-FAST 受信クライアント証明書は別の認証方式ではなく、ユーザを認証するのと同じ証明書のクレデンシャルのタイプを使用した略式のクライアント証明書認証ですが、内部方式を実行する必要がありません。
- PAC なしの完全なハンドシェイクおよび認定 PAC プロビジョニングとの認証プロビジョニング作業に対するクライアント証明書を受け入れます。PAC なしのセッション再開、匿名 PAC プロビジョニング、PAC ベース認証には動作しません。
- EAP 属性は、認証の順序とは関係なく、ID ごとにモニタリング ツールの認証詳細に、まずユーザ順、次にマシン順に表示されます（したがって EAP チェーニングは 2 回表示されます）。
- EAP-FAST 認可 PAC が使用される場合、ライブ ログに表示される EAP 認証方式は完全認証に使用される認証方式と同じ（PEAP のように）であり、参照としてではありません。
- EAP チェーン モードでは、トンネル PAC が期限切れになると、ISE がプロビジョニングにフォールバックし、AC 要求ユーザおよびマシン認可 PAC（マシン許可 PAC）はプロビジョニングできません。後続の PAC ベースの認証通信で AC が要求したときにプロビジョニングされます。
- Cisco ISE がチェーンに、AC がシングルモードに設定されている場合は、AC は IdentityType TLV で ISE に応答しますが、2 番目の ID 認証は失敗します。この通信から、クライ

アノンのチェーニング実行は適切であるが、現在はシングルモードで構成されていることがわかります。

- Cisco ISE は AD にのみチェーニングしている EAP-FAST のマシンとユーザの両方の属性およびグループをサポートします。LDAP および内部 DB ISE に対しては、最新の ID 属性のみを使用します。



(注) Sierra MAC OSX 高性能デバイスに EAP-FAST 認証プロトコルを使用すると、「EAP-FAST 暗号化バインドの検証に失敗しました (EAP-FAST cryptobinding verification failed)」というメッセージが表示される場合があります。Sierra MAC OSX 高性能デバイスに EAP-FAST を使用する代わりに PEAP または EAP-TLS を使用するよう、[許可プロトコル (Allowed Protocols)] ページの [優先 EAP プロトコル (Preferred EAP Protocol)] フィールドを設定することをお勧めします。

EAP-FAST の設定

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

- ステップ 1 [管理 (Administration)] > [システム (System)] > [設定 (Settings)] > [プロトコル (Protocols)] > [EAP-FAST] > [EAP-FAST の設定 (EAP-FAST Settings)] を選択します。
- ステップ 2 EAP-FAST プロトコルの定義に必要な詳細を入力します。
- ステップ 3 以前に生成されたマスター キーおよび PAC をすべて失効させるには、[失効 (Revoke)] をクリックします。
- ステップ 4 EAP-FAST 設定を保存するには、[保存 (Save)] をクリックします。

関連トピック

[EAP-FAST の PAC の生成](#) (687 ページ)

EAP-FAST の PAC の生成

Cisco ISE の [PAC の生成 (Generate PAC)] オプションを使用して、EAP-FAST プロトコルのトンネル PAC またはマシン PAC を生成できます。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

- ステップ 1 [管理 (Administration)] > [システム (System)] > [設定 (Settings)] を選択します。

ステップ 2 左側の [設定 (Settings)] ナビゲーション ペインの [プロトコル (Protocols)] をクリックします。

ステップ 3 [EAP-FAST] > [PAC の生成 (Generate PAC)] を選択します。

ステップ 4 EAP-FAST プロトコルのマシン PAC を生成する場合に必要な詳細を入力します。

ステップ 5 [PAC の生成 (Generate PAC)] をクリックします。

認証プロトコルとしての EAP-TTLS の使用

EAP-TTLS は、EAP-TLS プロトコルの機能を拡張する 2 フェーズ プロトコルです。フェーズ 1 では、セキュアなトンネルを構築し、フェーズ 2 で使用するセッション キーを導出し、サーバとクライアント間で属性および内部方式データを安全にトンネリングします。フェーズ 2 中では、トンネリングされた属性を使用して、多数のさまざまなメカニズムを使用する追加認証を実行できます。

Cisco ISE は、次のようなさまざまな TTLS サプリカントから認証を処理できます。

- Windows 上の AnyConnect Network Access Manager (NAM)
- Windows 8.1 ネイティブ サプリカント
- セキュア W2 (MultiOS で JoinNow と呼ばれます)
- MAC OS X ネイティブ サプリカント
- IOS ネイティブ サプリカント
- Android ベースのネイティブ サプリカント
- Linux WPA サプリカント



(注) 暗号化バインドが必要な場合は、内部方式として EAP-FAST を使用する必要があります。

EAP-TLS の設定

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 [管理 (Administration)] > [システム (System)] > [設定 (Settings)] > [プロトコル (Protocols)] > [EAP-TTLS] を選択します。

ステップ 2 [EAP-TTLS 設定 (EAP-TTLS Settings)] ページに必要な詳細を入力します。

ステップ 3 [保存 (Save)] をクリックします。

関連トピック

[EAP-TTLS 設定](#) (1188 ページ)

EAP-TLS の設定

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

-
- ステップ 1** [管理 (Administration)] > [システム (System)] > [設定 (Settings)] > [プロトコル (Protocols)] > [EAP-TLS] を選択します。
- ステップ 2** EAP-TLS プロトコルの定義に必要な詳細を入力します。
- ステップ 3** EAP-TLS 設定を保存するには、[保存 (Save)] をクリックします。
-

PEAP の設定

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

-
- ステップ 1** [管理 (Administration)] > [システム (System)] > [設定 (Settings)] を選択します。
- ステップ 2** 左側の [設定 (Settings)] ナビゲーション ペインの [プロトコル (Protocols)] をクリックします。
- ステップ 3** [PEAP] を選択します。
- ステップ 4** PEAP プロトコルの定義に必要な詳細を入力します。
- ステップ 5** PEAP 設定を保存するには、[保存 (Save)] をクリックします。
-

RADIUS の設定

認証に失敗、または認証成功のレポートの繰り返しの抑制に失敗したクライアントを検出するように RADIUS 設定を設定することができます。

-
- ステップ 1** [管理 (Administration)] > [システム (System)] > [設定 (Settings)] を選択します。
- ステップ 2** [設定 (Settings)] ナビゲーション ペインで [プロトコル (Protocols)] をクリックします。
- ステップ 3** [RADIUS] を選択します。
- ステップ 4** RADIUS 設定の定義に必要な詳細を入力します。

ステップ 5 [保存 (Save)] をクリックして、設定を保存します。

セキュリティ設定の構成

セキュリティ設定を構成するには、次の手順を実行します。

ステップ 1 [管理 (Administration)] > [システム (System)] > [設定 (Settings)] > [プロトコル (Protocols)] > [セキュリティ設定 (Security Settings)] を選択します。

ステップ 2 [セキュリティ設定 (Security Settings)] ページで、次の必須オプションを選択します。

- レガシー サーバで TLS 1.0 を許可する (Allow TLS 1.0 for Legacy Servers) : レガシー サーバのみで TLS 1.0 を有効にする場合は、このチェックボックスをオンにします。このオプションは、デフォルトで有効です。

次のワークフローはこのオプションの影響を受けます。

- Cisco ISE は、HTTPS またはセキュア LDAP サーバから CRL をダウンロードします。
- Cisco ISE は、セキュアな syslog クライアントとして設定されます。
- Cisco ISE は、セキュアな LDAP クライアントとして設定されます。

(注) セキュリティを強化するために、TLS の上位バージョンを使用するようにサーバでネゴシエートすることをお勧めします。

- レガシーサーバで SHA-1 を許可する (Allow SHA-1 for Legacy Servers) : レガシーサーバのみで SHA-1 暗号スイートを実効にする場合は、このチェックボックスをオンにします。このオプションは、デフォルトで有効です。

次のワークフローはこのオプションの影響を受けます。

- Cisco ISE は、HTTPS またはセキュア LDAP サーバから CRL をダウンロードします。
- Cisco ISE は、セキュアな syslog クライアントとして設定されます。
- Cisco ISE は、セキュアな LDAP クライアントとして設定されます。

セキュリティを強化するために、SHA-256 または SHA-384 暗号方式を使用することを推奨します。

- TLS 再ネゴシエーションを許可する (Allow TLS Renegotiation) : パラメータの再ネゴシエーションと新しいキーの生成を許可するには、このチェックボックスをオンにします。このオプションは、デフォルトで有効です。
- ISE セキュア クライアントで 3DES/DES/DSS/RC4 暗号方式を許可する (Allow 3DES/DES/DSS/RC4 ciphers for ISE secure clients) : このオプションを実効にすると、次のワークフローのピアとの通信で 3DES、DES、DSS、および RC4 暗号方式が許可されます。
 - Cisco ISE は、HTTPS またはセキュア LDAP サーバから CRL をダウンロードします。

- Cisco ISE は、セキュアな syslog クライアントとして設定されます。
- Cisco ISE は、セキュアな LDAP クライアントとして設定されます。

このオプションは、デフォルトで有効です。

ステップ 3 [保存 (Save)] をクリックします。

次のワークフローはセキュリティ設定の影響を受けません。

- Cisco ISE は、クライアントを認証する EAP-TLS、EAP-TTLS、PEAP、または EAP-FAST サーバとして動作し、ネットワークへのアクセス権を提供します。



(注) Cisco ISE 2.2 パッチ 2 以上では、[セキュリティ設定 (Security Settings)] ページのオプションが変更されています。詳細については、『[Release Notes for the Cisco Identity Services Engine, Release 2.2](#)』を参照してください。

ネットワーク アクセス サービス

ネットワーク アクセス サービスには、要求に対する認証ポリシー条件が含まれています。たとえば有線 802.1X や有線 MAB など、さまざまな用途向けに個別のネットワーク アクセス サービスを作成することができます。ネットワーク アクセス サービスを作成するには、許可されているプロトコルまたはサーバ順序を設定します。

関連トピック

[ネットワーク アクセスの許可されるプロトコルの定義](#) (691 ページ)

[RADIUS プロキシ サーバとして機能する Cisco ISE](#) (696 ページ)

[簡易認証ポリシー](#) (678 ページ)

[ルールベースの認証ポリシーの設定](#) (707 ページ)

ネットワーク アクセスの許可されるプロトコルの定義

許可されるプロトコルは、ネットワーク リソースへのアクセスを要求するデバイスとの通信に Cisco ISE が使用できるプロトコルのセットを定義します。許可されるプロトコル アクセス サービスは、認証ポリシーを設定する前に作成する必要がある独立したエントリです。許可されるプロトコル アクセス サービスは、特定の使用例に対して選択されたプロトコルが含まれているオブジェクトです。

[許可されるプロトコル サービス (Allowed Protocols Services)] ページには、作成した許可されるプロトコル サービスがすべて表示されます。Cisco ISE で事前に定義されたデフォルトのネットワーク アクセス サービスが存在します。

始める前に

この手順を開始する前に、認証に使用するプロトコルサービスの基本を理解している必要があります。

- この章の「Cisco ISE 認証ポリシー」の項を参照して、さまざまなデータベースでサポートされる認証タイプおよびプロトコルについて理解します。
- 「PAC オプション」を確認して、各プロトコル サービスの機能とオプションを理解し、使用しているネットワークに最適な選択ができるようにしてください。
- 手順を進める前に、グローバル プロトコル設定を必ず定義してください。

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] > [認証 (Authentication)] > [許可されるプロトコル (Allowed Protocols)] を選択します。

Cisco ISE が FIPS モードで動作するように設定されている場合は、一部のプロトコルがデフォルトで無効になり、それらのプロトコルを設定できません。

ステップ 2 [追加 (Add)] をクリックします。

ステップ 3 必要な情報を入力します。

ステップ 4 ネットワークに適切な認証プロトコルとオプションを選択します。

ステップ 5 PAC の使用を選択した場合、適切な選択を行います。

匿名 PAC プロビジョニングを有効にするには、内部方式として EAP-MSCHAPv2 と Extensible Authentication Protocol-Generic Token Card (EAP-GTC) の両方を選択する必要があります。また Cisco ISE では、マシン認証の外部 ID ソースとしては Active Directory だけがサポートされる点に注意してください。

ステップ 6 [送信 (Submit)] をクリックして、許可されるプロトコル サービスを保存します。

許可されるプロトコルサービスは、単純な認証ポリシーおよびルールベースの認証ポリシーのページで独立したオブジェクトとして表示されます。このオブジェクトは異なるルールに使用できます。

これで、単純な認証ポリシーおよびルールベースの認証ポリシーを作成できるようになります。

内部方式として EAP-MSCHAP を無効にし、PEAP または EAP-FAST の EAP-GTC と EAP-TLS 内部方式を有効にすると、ISE は内部方式のネゴシエーション中に EAP-GTC 内部方式を開始します。最初の EAP-GTC メッセージがクライアントに送信される前に、ISE は ID 選択のポリシーを実行して、ID ストアから GTC パスワードを取得します。このポリシーの実行中、EAP 認証は EAP-GTC と同じです。EAP-GTC 内部方式がクライアントによって拒否され、EAP-TLS がネゴシエートされても、ID ストア ポリシーが再び実行されることはありません。ID ストア ポリシーが EAP 認証属性に基づいている場合、本当の EAP 認証は EAP-TLS でありながら ID ポリシー評価後に設定されたため、予期しない結果になることがあります。

関連トピック

[Cisco ISE 認証ポリシー \(675 ページ\)](#)

[認証用のプロトコルの設定 \(686 ページ\)](#)

シスコ以外のデバイスからの MAB の有効化

次の設定を順番に設定して、シスコ以外のデバイスから MAB を設定します。

ステップ 1 認証されたエンドポイントの MAC アドレスが、エンドポイント データベースで使用可能なことを確認します。プロファイラ サービスによって、これらのエンドポイントを追加したり、自動的にプロファイリングしたりできます。

ステップ 2 シスコ以外のデバイス（PAP、CHAP、EAP-MD5）で使用される MAC 認証のタイプに基づいて、ネットワーク デバイス プロファイルを作成します。

- a) [管理 (Administration)] > [ネットワーク リソース (Network Resources)] > [ネットワーク デバイス プロファイル (Network Device Profiles)] の順に選択します。
- b) [追加 (Add)] をクリックします。
- c) ネットワーク デバイス プロファイルの名前と説明を入力します。
- d) [ベンダー (Vendor)] ドロップダウン リストからベンダー名を選択します。
- e) デバイスがサポートするプロトコルのチェックボックスをオンにします。デバイスが RADIUS をサポートする場合は、ネットワーク デバイスで使用する RADIUS ディクショナリを選択します。
- f) [認証/許可 (Authentication/Authorization)] セクションを展開し、フロータイプ、属性エイリアシング、およびホスト ルックアップに関するデバイスのデフォルト設定を行います。
- g) [ホスト ルックアップ (MAB) (Host Lookup (MAB))] セクションで、次を実行します。

- [ホスト ルックアップの処理 (Process Host Lookup)] : ネットワーク デバイス プロファイルで使用するホスト ルックアップ用のプロトコルを定義するには、このチェックボックスをオンにします。

さまざまなベンダーからのネットワーク デバイスは、MAB 認証を異なる方法で実行します。デバイス タイプに応じて、使用しているプロトコルの [パスワードを確認 (Check Password)] チェックボックスまたは [Calling-Station-Id が MAC アドレスと等しいかを確認 (Checking Calling-Station-Id equals MAC Address)] チェックボックス、またはその両方をオンにします。

- [PAP/ASCII 経由 (Via PAP/ASCII)] : ホスト ルックアップ要求としてネットワーク デバイス プロファイルからの PAP 要求を検出するように Cisco ISE を設定するには、このチェックボックスをオンにします。
- [CHAP 経由 (Via CHAP)] : ホスト ルックアップ要求としてネットワーク デバイスからのこのタイプの要求を検出するように Cisco ISE を設定するには、このチェックボックスをオンにします。
- [EAP-MD5 経由 (Via EAP-MD5)] : ネットワーク デバイス プロファイルに EAP ベースの MD5 ハッシュ認証を有効にするには、このチェックボックスをオンにします。

- h) [アクセス許可 (Permissions)]、[認可変更 (CoA) (Change of Authorization (CoA))]、[リダイレクト (Redirect)] のセクションに必要な詳細を入力して、[送信 (Submit)] をクリックします。

カスタム NAD プロファイルを作成する方法については、『[Network Access Device Profiles with Cisco Identity Services Engine](#)』を参照してください。

ステップ 3 [管理 (Administration)] > [ネットワーク リソース (Network Resources)] > [ネットワーク デバイス (Network Devices)] の順に選択します。

ステップ 4 MAB を有効にするデバイスを選択して、[編集 (Edit)] をクリックします。

ステップ 5 [ネットワーク デバイス (Network Device)] ページの [デバイス プロファイル (Device Profile)] ドロップダウン リストから、手順 2 で作成したネットワーク デバイス プロファイルを選択します。

ステップ 6 [保存 (Save)] をクリックします。



(注) Cisco NAD では、MAB および Web/ユーザ認証に使用する Service-Type 値は異なります。これにより、Cisco NAD を使用する場合に、ISE は MAB と Web 認証を区別できます。シスコ以外の一部の NAD では、MAB と Web/ユーザ認証に同じ値の Service-Type 属性を使用しています。この場合、アクセスポリシーでセキュリティ上の問題につながる場合があります。シスコ以外のデバイスで MAB を使用する場合は、ネットワークセキュリティが侵害されないように、追加の許可ポリシールールを設定することを推奨します。たとえば、プリンタで MAB を使用する場合は、ACL のプリンタ プロトコル ポートに制限する許可ポリシー ルールを設定できます。

関連トピック

[ネットワーク アクセスの許可されるプロトコルの定義](#) (691 ページ)

[ルールベースの認証ポリシーの設定](#) (707 ページ)

シスコ デバイスからの MAB の有効化

次の設定を順番に設定して、シスコ デバイスから MAB を設定します。

ステップ 1 認証されたエンドポイントの MAC アドレスが、エンドポイント データベースで使用可能なことを確認します。プロファイラ サービスによって、これらのエンドポイントを追加したり、自動的にプロファイリングしたりできます。

ステップ 2 シスコ デバイス (PAP、CHAP、EAP-MD5) で使用される MAC 認証のタイプに基づいて、ネットワーク デバイス プロファイルを作成します。

- a) [管理 (Administration)] > [ネットワーク リソース (Network Resources)] > [ネットワーク デバイス プロファイル (Network Device Profiles)] の順に選択します。
- b) [追加 (Add)] をクリックします。
- c) ネットワーク デバイス プロファイルの名前と説明を入力します。
- d) デバイスがサポートするプロトコルのチェックボックスをオンにします。デバイスが RADIUS をサポートする場合は、ネットワーク デバイスで使用する RADIUS ディクショナリを選択します。
- e) [認証/許可 (Authentication/Authorization)] セクションを展開し、フロータイプ、属性エイリアシング、およびホストルックアップに関するデバイスのデフォルト設定を行います。
- f) [ホストルックアップ (MAB) (Host Lookup (MAB))] セクションで、次を実行します。

- [ホスト ルックアップの処理 (Process Host Lookup)] : ネットワーク デバイス プロファイルで使用するホスト ルックアップ用のプロトコルを定義するには、このチェックボックスをオンにします。
デバイス タイプに応じて、使用しているプロトコルの [パスワードを確認 (Check Password)] チェックボックスまたは [Calling-Station-Id が MAC アドレスと等しいかを確認 (Checking Calling-Station-Id equals MAC Address)] チェックボックス、またはその両方をオンにします。
- [PAP/ASCII 経由 (Via PAP/ASCII)] : ホスト ルックアップ要求としてネットワーク デバイス プロファイルからの PAP 要求を検出するように Cisco ISE を設定するには、このチェックボックスをオンにします。
- [CHAP 経由 (Via CHAP)] : ホスト ルックアップ要求としてネットワーク デバイスからのこのタイプの要求を検出するように Cisco ISE を設定するには、このチェックボックスをオンにします。
- [EAP-MD5 経由 (Via EAP-MD5)] : ネットワーク デバイス プロファイルに EAP ベースの MD5 ハッシュ認証を有効にするには、このチェックボックスをオンにします。

g) [アクセス許可 (Permissions)]、[認可変更 (CoA) (Change of Authorization (CoA))]、[リダイレクト (Redirect)] のセクションで必要な詳細を入力して、[送信 (Submit)] をクリックします。

カスタム NAD プロファイルを作成する方法については、『[Network Access Device Profiles with Cisco Identity Services Engine](#)』を参照してください。

ステップ 3 [管理 (Administration)] > [ネットワーク リソース (Network Resources)] > [ネットワーク デバイス (Network Devices)] の順に選択します。

ステップ 4 MAB を有効にするデバイスを選択して、[編集 (Edit)] をクリックします。

ステップ 5 [ネットワーク デバイス (Network Device)] ページの [デバイス プロファイル (Device Profile)] ドロップダウンリストから、手順 2 で作成したネットワーク デバイス プロファイルを選択します。

ステップ 6 [保存 (Save)] をクリックします。

ISE コミュニティ リソース

IP フォンの認証機能については、「[Phone Authentication Capabilities](#)」を参照してください。

関連トピック

[ネットワーク アクセスの許可されるプロトコルの定義](#) (691 ページ)

[ルールベースの認証ポリシーの設定](#) (707 ページ)

ネットワーク アクセス ワーク センター

ネットワーク アクセスに関するオプションは、[ネットワーク アクセス ワーク センター (Network Access Work Center)] メニュー ([ワーク センター (Work Centers)] > [ネットワーク アクセス (Network Access)]) で、管理者が 1 つの場所で簡単にネットワーク アクセスに関連するすべてのオプションにアクセスできるようにグループ化されます。

[ネットワーク アクセス ワーク センター (Network Access Work Center)] から次のタスクを実行できます。

- ユーザとデバイスの認証プロセスで使用する外部 ID ストアを設定します。次の外部 ID ストアを設定できます：Active Directory、LDAP、ODBC、RADIUS、RSA、および SAML ID プロバイダです。
- 認証および許可ポリシーで使用するポリシーの要素を定義します。
- Cisco ISE によって制御されているすべてのネットワーク デバイスを追加します。デバイスはタイプおよびロケーション別にグループ化することができます。
- 必要に応じて、ユーザおよびネットワーク デバイスの認証と許可ポリシーを定義します。
- クライアントのプロビジョニング、プロトコル設定、およびプロキシ設定に対するデフォルト ネットワーク アクセス設定を確認します。
- RADIUS ライブログを使用してネットワーク イベントを監視します。
- ネットワーク アクセス レポートを実行して、アクセスおよび許可の結果を確認します。
- 診断ツールを使用してネットワーク アクセスの問題のトラブルシューティングを行います。

RADIUS プロキシ サーバとして機能する Cisco ISE

Cisco ISE は、RADIUS サーバおよび RADIUS プロキシ サーバとして機能できます。プロキシ サーバとして機能する場合、Cisco ISE はネットワーク アクセス サーバ (NAS) から認証要求およびアカウンティング要求を受信し、これらの要求を外部 RADIUS サーバに転送します。Cisco ISE は要求の結果を受け取り、NAS に返します。

Cisco ISE は、同時に複数の外部 RADIUS サーバへのプロキシ サーバとして動作できます。RADIUS サーバ順序で設定した外部 RADIUS サーバを使用できます。次に説明する [外部 RADIUS サーバ (External RADIUS Server)] ページには、Cisco ISE で定義した外部 RADIUS サーバがすべて表示されます。フィルタ オプションを使用して、名前または説明、またはその両方に基づいて特定の RADIUS サーバを検索することができます。単純な認証ポリシーとルールベースの認証ポリシーの両方で、RADIUS サーバ順序を使用して要求を RADIUS サーバにプロキシできます。

RADIUS サーバ順序は、RADIUS-Username 属性からドメイン名を抜き取り (ストリッピング) 、RADIUS 認証に使用します。このドメイン ストリッピングは EAP 認証には使用できません。EAP 認証では EAP-Identity 属性が使用されます。RADIUS プロキシ サーバは RADIUS-Username 属性からユーザ名を取得し、RADIUS サーバ順序の設定時に指定した文字列からユーザ名を抜き取ります。EAP 認証の場合は、RADIUS プロキシ サーバはユーザ名を EAP-Identity 属性から取得します。RADIUS サーバ順序を使用する EAP 認証は、EAP-Identity 値と RADIUS-Username 値が同一である場合のみ成功します。

外部 RADIUS サーバの設定

Cisco ISE で外部 RADIUS サーバを設定して、要求を外部 RADIUS サーバに送信できるようにする必要があります。タイムアウト時間および接続試行回数を定義できます。

始める前に

- この項で作成した外部 RADIUS サーバは、それだけでは使用できません。RADIUS サーバ順序を作成して、この項で作成した RADIUS サーバを使用するように設定する必要があります。これにより、RADIUS サーバ順序を認証ポリシーで使用できるようになります。
- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 [管理 (Administration)] > [ネットワーク リソース (Network Resources)] > [外部 RADIUS サーバ (External RADIUS Servers)] を選択します。

[RADIUS サーバ (RADIUS Servers)] ページが表示され、Cisco ISE で定義された外部 RADIUS サーバのリストが示されます。

ステップ 2 外部 RADIUS サーバを追加するには、[追加 (Add)] をクリックします。

ステップ 3 必要に応じて値を入力します。

ステップ 4 [送信 (Submit)] をクリックして、外部 RADIUS サーバの設定を保存します。

関連トピック

[RADIUS サーバの順序](#)

RADIUS サーバ順序の定義

Cisco ISE の RADIUS サーバ順序を使用すると、NAD からの要求を外部 RADIUS サーバにプロキシできます。外部 RADIUS サーバは要求を処理して結果を Cisco ISE に返し、Cisco ISE はその応答を NAD に転送します。

[RADIUS サーバ順序 (RADIUS Server Sequences)] ページに、Cisco ISE で定義したすべての RADIUS サーバの順序が表示されます。このページを使用して、RADIUS サーバの作成、編集、または複製が可能です。

始める前に

- この手順を開始する前に、プロキシサービスの基本を理解し、関連リンクの最初のエントリのタスクを正常に完了している必要があります。
- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

- ステップ 1 [管理 (Administration)] > [ネットワーク リソース (Network Resources)] > [RADIUS サーバ順序 (RADIUS Server Sequences)] を選択します。
- ステップ 2 [追加 (Add)] をクリックします。
- ステップ 3 必要に応じて値を入力します。
- ステップ 4 [送信 (Submit)] をクリックして、ポリシーに使用する RADIUS サーバ順序を保存します。

関連トピック

- [外部 RADIUS サーバの設定](#) (697 ページ)
- [ルールベースの認証ポリシーの設定](#) (707 ページ)
- [RADIUS サーバの順序](#)

TACACS+ プロキシクライアントとして機能する Cisco ISE

Cisco ISE は、外部 TACACS+ サーバへのプロキシクライアントとして機能できます。プロキシクライアントとして機能する場合、Cisco ISE はネットワーク アクセス サーバ (NAS) から認証要求、許可要求およびアカウンティング要求を受信し、これらの要求を外部 TACACS+ サーバに転送します。Cisco ISE は要求の結果を受け取り、NAS に返します。

[TACACS+外部サーバ (TACACS+ External Servers)] ページには、Cisco ISE で定義した外部 TACACS+ サーバがすべて表示されます。フィルタ オプションを使用して、名前または説明、またはその両方に基づいて特定の TACACS+ サーバを検索することができます。

Cisco ISE は、同時に複数の外部 TACACS+ サーバへのプロキシクライアントとして動作できます。複数の外部サーバを設定するには、[TACACS+サーバの順序 (TACACS+ server sequence)] ページを使用できます。詳細については、「[TACACS+ サーバ順序の設定](#)」ページを参照してください。

関連トピック

- [TACACS+ 外部サーバの設定](#) (698 ページ)
- [外部 TACACS+ サーバの設定](#) (700 ページ)
- [TACACS+ サーバ順序の設定](#) (700 ページ)
- [TACACS+ サーバ順序の定義](#) (702 ページ)

TACACS+ 外部サーバの設定

次の表では、[TACACS外部サーバ (TACACS External Servers)] ページのフィールドについて説明します。ナビゲーションパスは、[ワークセンター (Work Centers)] > [デバイス管理 (Device Administration)] > [ネットワークリソース (Network Resources)] > [TACACS外部サーバ (TACACS External Servers)] ページです。

表 37: TACACS+ 外部サーバの設定

フィールド	使用上のガイドライン
[名前 (Name)]	TACACS+ 外部サーバの名前を入力します。
説明	TACACS+ 外部サーバ設定の説明を入力します。
ホスト名/アドレス (Host IP)	リモート TACACS+ 外部サーバの IP アドレスを入力します。
接続ポート (Connection Port)	リモート TACACS+ 外部サーバのポート番号を入力します。ポート番号は 49 です。
Timeout	ISE が外部 TACACS+ サーバからの応答を待機する秒数を入力します。デフォルトは 5 秒です。有効な値は 1 ～ 120 です。
共有秘密鍵 (Shared Secret)	TACACS+ 外部サーバとの接続を保護するのに使用するテキスト文字列。正しく設定されていない場合、接続は TACACS+ 外部サーバによって拒否されます。
シングル接続を使用 (Use Single Connect)	<p>TACACS プロトコルは、接続にセッションを関連付けるための 2 つのモード、シングル接続と非シングル接続をサポートしています。シングル接続モードは、クライアントが開始する可能性がある多数の TACACS+ セッションに対し、単一の TCP 接続を再使用します。非シングル接続では、クライアントが開始するすべての TACACS+ セッションに対し、新しい TCP 接続が開かれます。TCP 接続は、各セッションの後に閉じられます。</p> <p>トラフィックが多い環境では、[シングル接続を使用 (Use Single Connect)]チェックボックスをオンにし、トラフィックが少ない環境ではオフにできます。</p>

関連トピック

[TACACS+ 外部サーバの設定](#) (698 ページ)[外部 TACACS+ サーバの設定](#) (700 ページ)[TACACS+ サーバ順序の設定](#) (700 ページ)[TACACS+ サーバ順序の定義](#) (702 ページ)

外部 TACACS+ サーバの設定

Cisco ISE で外部 TACACS サーバを設定して、要求を外部 TACACS サーバに送信できるようにする必要があります。タイムアウト時間および接続試行回数を定義できます。

始める前に

- この項で作成した外部 TACACS サーバは、ポリシーに直接使用できません。TACACS サーバ順序を作成して、この項で作成した TACACS サーバを使用するように設定する必要があります。これにより、TACACS サーバ順序をポリシー セットで使用できるようになります。
- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 [ワークセンター (Work Centers)] > [デバイス管理 (Device Administration)] > [ネットワークリソース (Network Resources)] > [TACACS 外部サーバ (TACACS External Servers)] の順に選択します。
[TACACS 外部サーバ (TACACS External Servers)] ページが表示され、Cisco ISE で定義された外部 TACACS サーバのリストが示されます。

ステップ 2 外部 TACACS サーバを追加するには、[追加 (Add)] をクリックします。

ステップ 3 必要に応じて値を入力します。

ステップ 4 [送信 (Submit)] をクリックして、外部 TACACS サーバの設定を保存します。

関連トピック

- [TACACS+ 外部サーバの設定](#) (698 ページ)
- [外部 TACACS+ サーバの設定](#) (700 ページ)
- [TACACS+ サーバ順序の設定](#) (700 ページ)
- [TACACS+ サーバ順序の定義](#) (702 ページ)

TACACS+ サーバ順序の設定

次の表では、[TACACS サーバ順序 (TACACS Server Sequence)] ページのフィールドについて説明します。ナビゲーションパスは、[ワークセンター (Work Centers)] > [デバイス管理 (Device Administration)] > [ネットワークリソース (Network Resources)] > [TACACS サーバ順序 (TACACS Server Sequence)] ページです。

表 38: TACACS+ サーバ順序の設定

フィールド	使用上のガイドライン
[名前 (Name)]	TACACS プロキシ サーバ順序の名前を入力します。

フィールド	使用上のガイドライン
説明	TACACS プロキシ サーバ 順序の説明を入力します。
サーバ リスト (Server List)	[使用可能 (Available)] リストから必要な TACACS プロキシ サーバ を選択します。[使用可能 (Available)] リストには、[TACACS 外部 サービス (TACACS External Services)] ページで設定されている TACACS プロキシ サーバ のリストが含まれています。
ロギング制御 (Logging Control)	ロギング制御を有効にするにはオンにします。 <ul style="list-style-type: none"> ローカル アカウンティング：アカウンティング メッセージは、デバイスからの要求を処理するサーバによってログに記録されます。 リモート アカウンティング：アカウンティング メッセージは、デバイスからの要求を処理するプロキシ サーバによってログに記録されます。
ユーザ名の除去 (Username Stripping)	ユーザ名のプレフィックス/サフィックスの除去 <ul style="list-style-type: none"> [プレフィックスの除去 (Prefix Strip)]：プレフィックスからユーザ名を取り除く場合にオンにします。たとえば、サブジェクト名が <code>acme\smith</code>、区切り文字が <code>\</code> の場合、ユーザ名は <code>smith</code> になります。デフォルトの区切り文字は <code>\</code> です。 [サフィックスの除去 (Suffix Strip)]：サフィックスからユーザ名を取り除く場合にオンにします。たとえば、サブジェクト名が <code>smith@acme.com</code>、区切り文字が <code>@</code> の場合、ユーザ名は <code>smith</code> になります。デフォルトの区切り文字は <code>@</code> です。

関連トピック

[TACACS+ 外部サーバの設定](#) (698 ページ)

[外部 TACACS+ サーバの設定](#) (700 ページ)

[TACACS+ サーバ順序の設定](#) (700 ページ)

[TACACS+ サーバ順序の定義](#) (702 ページ)

TACACS+ サーバ順序の定義

Cisco ISE の TACACS+ サーバ順序を使用すると、NAD からの要求を外部 TACACS+ サーバにプロキシできます。外部 TACACS+ サーバは要求を処理して結果を Cisco ISE に返し、Cisco ISE はその応答を NAD に転送します。[TACACS+サーバ順序 (TACACS+ Server Sequences)] ページに、Cisco ISE で定義したすべての TACACS+ サーバの順序が表示されます。このページを使用して、TACACS+ サーバ順序の作成、編集、または複製が可能です。

始める前に

- プロキシ サービス、Cisco ISE 管理者グループ、アクセス レベル、権限、および制限の基本を理解している必要があります。
- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。
- TACACS+ サーバ順序で使用する外部 TACACS+ サーバがすでに定義されていることを確認します。

ステップ 1 [ワークセンター (Work Centers)] > [デバイス管理 (Device Administration)] > [ネットワークリソース (Network Resources)] > [TACACS外部サーバ順序 (TACACS External Server Sequence)] の順に選択します。

ステップ 2 [追加 (Add)] をクリックします。

ステップ 3 必要な値を入力します。

ステップ 4 [送信 (Submit)] をクリックして、ポリシーに使用する TACACS+ サーバ順序を保存します。

関連トピック

[TACACS+ 外部サーバの設定](#) (698 ページ)

[外部 TACACS+ サーバの設定](#) (700 ページ)

[TACACS+ サーバ順序の設定](#) (700 ページ)

[TACACS+ サーバ順序の定義](#) (702 ページ)

ロケーションに基づく認証

Cisco ISE は、Cisco モビリティ サービス エンジン (MSE) と統合し、物理ロケーションベースの認証を導入します。Cisco ISE は、MSE からの情報を使用して、MSE によって報告されるユーザの実際の位置に基づいて差別化されたネットワーク アクセスを提供します。

この機能を使用すると、エンドポイントのロケーション情報を使用して、ユーザが適切なゾーンにいる場合にネットワークアクセスを提供できます。また、エンドポイントのロケーションをポリシーの追加属性として追加して、デバイスのロケーションに基づいてより詳細なポリシー許可のセットを定義することもできます。次のように、ロケーションベースの属性を使用する許可ルール内で条件を設定できます。

MSE.Location Equals LND_Campus1:Building1:Floor2:SecureZone

ロケーション階層（キャンパス/ビルディング/フロア構造）を定義して、Cisco Prime Infrastructure のアプリケーションを使用してセキュアおよび非セキュアのゾーンを設定できます。ロケーション階層を定義した後、ロケーション階層データを MSE サーバと同期する必要があります。

Cisco Prime Infrastructure の詳細については、<http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/products-user-guide-list.html> を参照してください。

1 つまたは複数の MSE インスタンスを追加して、MSE ベースのロケーション データを許可プロセスに統合できます。これらの MSE からロケーション階層データを取得し、このデータを使用してロケーション ベースの許可ルールを設定できます。

エンドポイントの移動を追跡するには、許可プロファイルの作成時に [移動の追跡 (Track Movement)] チェックボックスをオンにします。Cisco ISE は、5 分ごとにエンドポイント ロケーションの関連 MSE にクエリを行い、ロケーションが変更されたかどうかを確認します。



(注) 複数のユーザを追跡すると、頻繁な更新によってパフォーマンスに影響します。[移動の追跡 (Track Movement)] オプションは、上位のセキュリティ ロケーションに使用できます。

ロケーション ツリーは、MSE インスタンスから取得されたロケーション データを使用して作成されます。ロケーション ツリーを使用して、許可ポリシーに公開するロケーション エントリを選択できます。



(注) ロケーション サービスを使用するには、ISE Plus ライセンスが必要です。

MSE サーバの追加

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

- ステップ 1** [管理 (Administration)] > [ネットワークリソース (Network Resources)] > [ロケーションサービス (Location Services)] > [ロケーションサーバ (Location Servers)] を選択します。
- ステップ 2** [追加 (Add)] をクリックします。
- ステップ 3** サーバ名、ホスト名/IP アドレス、パスワードなど、MSE サーバの詳細を入力します。
- ステップ 4** 指定したサーバの詳細を使用して MSE の接続性をテストするには、[テスト (Test)] をクリックします。
- ステップ 5** (任意) エンドポイントがこの MSE に現在接続されているかどうかを確認するには、[ロケーション検索 (Find Location)] フィールドにエンドポイントの MAC アドレスを入力し、[検索 (Find)] をクリックします。

エンドポイントのロケーションが見つかった場合は、*Campus:Building:Floor:Zone* の形式で表示されます。ロケーションの階層およびゾーンの設定によっては、複数のエントリが表示される場合があります。たと

例えば、*Campus1* という名前のキャンパス内のビルディング (*building1*) のすべてのフロアが非セキュアゾーンとして定義され、最初のフロアのラボエリアがセキュアゾーンとして定義されている場合、エンドポイントがそのラボエリアにある場合は、次のエントリが表示されます。

見つかった場所：

Campus1#building1#floor1#LabArea

Campus1#building1#floor1#NonSecureZone

ステップ 6 [送信 (Submit)] をクリックします。

新しい MSE を追加したら、[ロケーションツリー (Location Tree)] ページに移動し、[更新の取得 (Get Update)] をクリックして、ロケーション階層を取得し、それをロケーション ツリーに追加します。このツリーで定義されたフィルタがある場合、これらのフィルタは新しい MSE エントリにも適用されます。

ロケーション ツリー

ロケーション ツリーは、MSE インスタンスから取得されたロケーション データを使用して作成されます。ロケーション ツリーを表示するには、[管理 (Administration)] > [ネットワーク リソース (Network Resources)] > [ロケーションサービス (Location Services)] > [ロケーション ツリー (Location Tree)] を選択します。

1 つのビルディングに複数の MSE がある場合、Cisco ISE はすべての MSE からロケーションの詳細を照合し、単一のツリーとして表示します。

ロケーション ツリーを使用して、許可ポリシーに公開するロケーション エントリを選択できます。また、要件に基づいて特定のロケーションを非表示にすることもできます。ロケーションを非表示にする前にロケーション ツリーを更新することを推奨します。非表示にされたロケーションは、ツリーが更新されても非表示のままになります。

許可ルールに関連するロケーション エントリが変更または削除された場合は、影響を受けるルールをディセーブルにし、これらのロケーションを[不明 (Unknown)] として設定するか、または影響を受ける各ルールに代替ロケーションを選択する必要があります。変更を適用したり更新をキャンセルする前に新しいツリー構造を確認する必要があります。

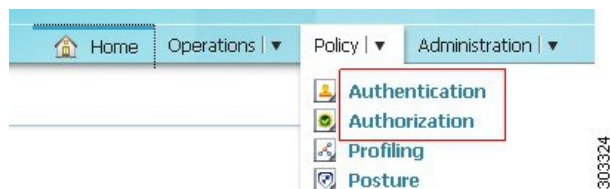
すべての MSE から最新のロケーション階層構造を取得するには、[更新の取得 (Get Update)] をクリックします。新しいツリー構造を確認したら、[保存 (Save)] をクリックして変更を適用します。

ポリシー モード

Cisco ISE には、簡易モードとポリシー セット モードの 2 種類のポリシー モードがあります。2 種類のうちのどちらかのモードを選択して、認証ポリシーと許可ポリシーを設定します。ポリシー モードを変更すると、Cisco ISE インターフェイスに再度ログインするように促されます。ポリシー セット モードから簡易モードに切り替えた場合、すべてのポリシー セットのデータがデフォルト ポリシーを除いて削除されます。[ポリシー (Policy)] メニュー オプションはポリシー モードの選択に基づいて変化します。

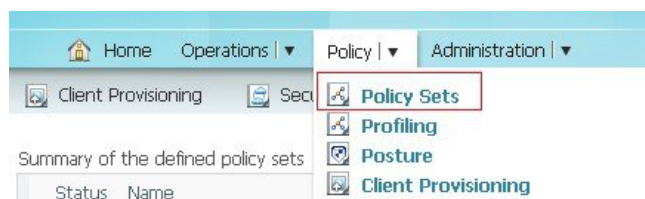
- 簡易モード：簡易モードを選択した場合は、[ポリシー（Policy）]メニューで認証ポリシーと許可ポリシーを別々に定義できます。

図 45:簡易モードの [ポリシー（Policy）]メニュー



- ポリシーセットモード：ポリシーセットモードを選択した場合は、ポリシーセットを作成して、認証と許可を論理的に同一グループにグループ化できます。必要に応じて複数のグループを作成できます。

図 46:ポリシーセットモードの [ポリシー（Policy）]メニュー



関連トピック

[ポリシー モード変更のガイドライン](#)

[ポリシー モードの変更](#)（705 ページ）

[簡易認証ポリシー](#)（678 ページ）

[ルールベースの認証ポリシーの設定](#)（707 ページ）

[ポリシーセット](#)（708 ページ）

ポリシー モードの変更

ポリシー モード変更のためのガイドラインは、次のとおりです。

- Cisco ISE、リリース 1.1 から新たにインストールまたは更新すると、簡易モードポリシーモデルがデフォルトで選択されます。
- 簡易モードからポリシーセットモードに切り替えると、認証および許可ポリシーはデフォルトポリシーセットに移行されます。
- ポリシーセットモードから簡易モードに切り替えると、デフォルトポリシーセットの認証および許可が認証および認可ポリシーに移行されます。その他のすべてのポリシーセットポリシーは削除されます。

ステップ 1 [管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポリシーセット（Policy Sets）] を選択します。

ステップ 2 ポリシー セット モードを有効または無効にします。

ステップ 3 [保存 (Save)] をクリックします。

新しいポリシー モードを有効にするために、もう一度ログインするよう促されます。

関連トピック

[簡易認証ポリシー](#) (678 ページ)

[ルールベースの認証ポリシー](#) (681 ページ)

[ポリシー セット](#) (708 ページ)

簡易認証ポリシーの設定

単純な認証ポリシーの設定手順には、許可されるプロトコルサービスの定義および単純な認証ポリシーの設定が含まれます。

始める前に

- RADIUS サーバを使用して簡易認証ポリシーを設定するには、さまざまなデータベースがサポートする認証タイプとプロトコルの理解のために、Cisco ISE 認証ポリシーおよびプロキシ サービスの基本を理解する必要があります。
- 許可されるプロトコル アクセス サービスや RADIUS サーバ順序を定義する必要があります。
- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

このプロセスにより、RADIUS サーバ順序を使用した簡易ポリシーの設定も可能です。

ステップ 1 [ポリシー (Policy)] > [認証 (Authentication)] を選択します。

ステップ 2 メッセージが表示されたら、[OK] をクリックします。

ステップ 3 必要に応じて値を入力します。

ステップ 4 [保存 (Save)] をクリックして、設定した単純な認証ポリシーを保存します。

関連トピック

[Cisco ISE 認証ポリシー](#) (675 ページ)

[ネットワーク アクセスの許可されるプロトコルの定義](#) (691 ページ)

[RADIUS サーバの順序](#)

[RADIUS プロキシ サーバとして機能する Cisco ISE](#) (696 ページ)

ルールベースの認証ポリシーの設定

ルールベースのポリシーでは、条件を定義することによって、Cisco ISE は許可されるプロトコルおよび ID ソースを動的に選択できるようになります。複数の条件を、Cisco ISE ディクショナリ内の任意の属性を使用して定義できます。



ヒント

ルールベースの認証ポリシーを作成する前に、許可されるプロトコル アクセス サービス、条件、および ID ソース順序を作成することを推奨します。RADIUS サーバ順序を使用する場合、ポリシーを作成する前に RADIUS サーバ順序を定義できます。

始める前に

- ルールベースの認証ポリシー、ネットワーク アクセスに許可される定義済みのプロトコル、作成された ID ソース順序、および RADIUS サーバ順序（許可されるプロトコル アクセス サービスの代わりに RADIUS サーバ順序を使用する場合）の基本的な理解が必要です。
- Cisco ISE では、有線 802.1X、無線 802.1X、および有線 MAB を使用する場合の標準的なルールベースの認証ポリシーが事前に用意されています。
- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。
- ユーザが外部の ID ソースで定義されている場合、Cisco ISE でこれらの ID ソースが設定されていることを確認してください。



(注)

単純なポリシーとルールベースのポリシーを切り替える場合、最初に設定したポリシーは失われます。たとえば、単純な認証ポリシーを設定した後でルールベースの認証ポリシーに移動すると、単純な認証ポリシーは失われます。また、ルールベースの認証ポリシーから簡易認証ポリシーに移動した場合は、ルールベースの認証ポリシーは失われます。

ステップ 1 [ポリシー (Policy)] > [認証 (Authentication)] を選択します。

ステップ 2 [ルールベース (Rule-Based)] オプション ボタンをクリックします。

ステップ 3 メッセージが表示されたら、[OK] をクリックします。

ステップ 4 アクション アイコンをクリックして、新しいポリシーを表示するリスト上の位置に応じて [新しい行を上 に挿入 (Insert new row above)] または [新しい行を下に挿入 (Insert new row below)] をクリックします。ポリシーは、順序に従って評価されます。

このルールベースのポリシーのページ内の各行は、単純な認証ポリシーと同等です。各行には、許可されるプロトコルおよび ID ソースを決定する一連の条件が含まれています。

ステップ 5 必要に応じて新しい認証ポリシーを作成するための値を入力します。

ステップ 6 [保存 (Save)] をクリックして、作成したルールベースの認証ポリシーを保存します。

EAP-FAST クライアント証明書が外部の TLS ネゴシエーションで送信される場合の認証ポリシーを設定するときに、「Username」属性は指定できません。「CN」や「SAN」などの証明書フィールドを使用することをお勧めします。

Active Directory のアカウントが logon hours、locked-out、workstations のいずれかの属性を使用してユーザまたはマシンを拒否するように設定されている場合、ISE は Active Directory に対してユーザまたはマシンの EAP-TLS 認証を制限しません。これらの属性を使用して、EAP-TLS 認証のユーザまたはマシンを制限しないでください。

関連トピック

[ルールベースの認証ポリシー](#) (681 ページ)

[ルールベースの認証ポリシーの設定](#) (707 ページ)

[ネットワーク アクセスの許可されるプロトコルの定義](#) (691 ページ)

[RADIUS サーバの順序](#)

[認証ポリシーの組み込み設定](#) (711 ページ)

[ディクショナリによってサポートされる属性](#) (683 ページ)

[RADIUS プロキシサーバとして機能する Cisco ISE](#) (696 ページ)

[Cisco ISE 認証ポリシー](#) (675 ページ)

デフォルトの認証ポリシー

認証ポリシーページの最後の行は、どのルールも要求と一致しない場合に適用されるデフォルトポリシーです。このデフォルトのポリシーの許可されるプロトコルおよび ID ソースを編集できます。

他のいかなる作成済みポリシーにも要求が一致しない場合のデフォルトのポリシーで、ID ソースとして [アクセスを拒否 (Deny Access)] を選択することを推奨します。

ポリシー セット

ポリシーセットでは、論理的に同じセット内の認証および許可ポリシーをグループ化することができます。ロケーション、アクセス タイプ、類似パラメータに基づくポリシー セットなどの領域に基づいて、複数のポリシー セットを作成できます。

ポリシーセットは最初に一致したポリシーです。各ポリシーには簡易または複合条件のどちらかがあり、次のサポート ディクショナリがあります。

- Airspace

- Cisco
- Cisco-BBSM
- Cisco-VPN3000
- Device、Microsoft
- NetworkAccess
- RADIUS

ポリシーセットが一致し選択されたら、認証および許可ポリシーが評価されます。さらに、ポリシーセット モデルの一部として、グローバル許可例外ポリシーを利用できます。

常時 1 つのポリシー セットが定義されています。それがデフォルト ポリシー セットです。

関連トピック

[ポリシー セットの評価フロー](#) (709 ページ)

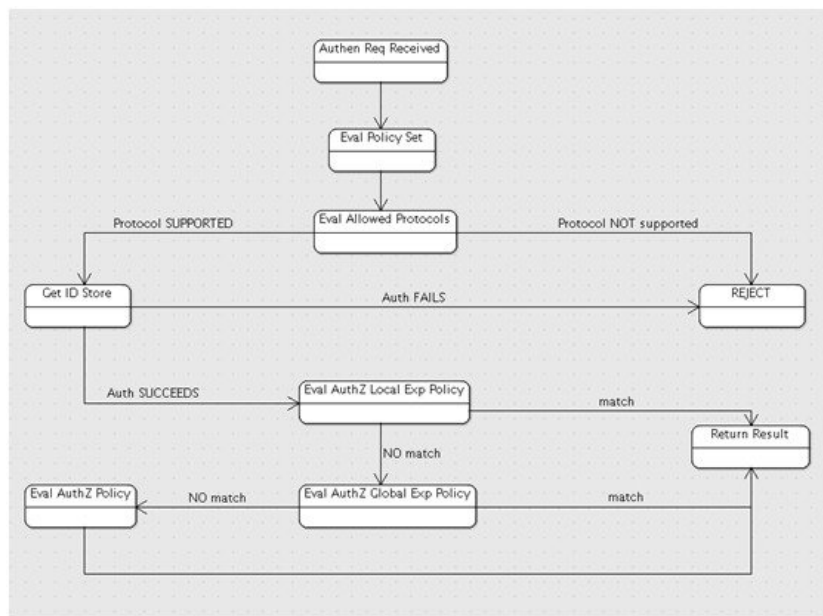
[ポリシー セットの作成のガイドライン](#) (710 ページ)

[グローバル許可例外ポリシー](#) (710 ページ)

[ポリシー セットの設定](#) (710 ページ)

ポリシー セットの評価フロー

図 47: ポリシー セットの認証および許可の評価フロー



ポリシー セットの順序および認証と許可の評価フローは、次のとおりです。

1. ポリシーセットを評価します（ポリシーセットの条件を評価する）。その結果、ポリシーセットが 1 つ選択されます。

2. 選択したポリシーセットの許可されたプロトコルルールを評価します。
 3. 選択したポリシーセットの ID ストアルールを評価します。
 4. 次のパラダイムに基づいて、選択したポリシーセットの許可ルールを評価します。
 - ローカル例外ポリシーが定義されている場合は、これを評価する
 - 上記手順 1 で一致がない場合、定義されていればグローバル例外ポリシーを評価する
 - 上記手順 2 で一致がない場合、許可ルールを評価する
- どのポリシーセットにも一致しない場合は、デフォルトのポリシーセットが選択されます。

ポリシーセットの作成のガイドライン

ポリシーセット作成のためのガイドラインは、次のとおりです。

- ルールは、名前、条件、結果を使用して設定されます。ポリシーセットを実装するには、認証ルールと許可ルールを定義する必要があります。作成した新しいポリシーセットと同様に、ISE で自動的にインストールされるデフォルトの事前設定済みポリシーセットは、既存のデフォルトの認証および許可ポリシールールで自動的に作成され、その後編集または補足できます。
- 同じルールタイプ（認証または許可のいずれか）で、同じポリシーセット内でのみルールを複製できます。
- 異なるポリシーセットはルールを共有できません。各ポリシーセットには独自のルールがあります。ただし、条件ライブラリを使用している場合は、条件を共有することができます。

グローバル許可例外ポリシー

グローバル許可例外ポリシーにより、すべてのポリシーセットに適用するルールを定義できます。グローバル許可例外ポリシーは、すべてのポリシーセットのすべての許可ポリシーに追加されます。グローバル許可例外ポリシーは、ポリシーセットのリストからグローバル例外オプションを選択することによって更新できます。

各許可ポリシーには、ローカル例外規則、グローバル例外規則、通常ルールがあります。ローカル許可例外ルールを設定すると、（ある許可ポリシー用の）グローバル例外許可ルールが、ローカル許可例外ルールと並んで読み取り専用モードで表示されます。ローカル許可例外ルールは、グローバル例外ルールに優先します。許可ルールは、許可ポリシーのローカル例外規則、グローバル例外規則、通常ルールの順番で処理されます。

ポリシーセットの設定

このページを使用して、ポリシーセットを設定できます。

始める前に

ポリシー セットが設定できるように、ポリシー モードをポリシー セットとして選択しておく必要があります。これを行うには、[管理 (Administration)] > [システム (System)] > [設定 (Settings)] > [ポリシー セット (Policy Sets)] に移動します。

-
- ステップ 1** [ポリシー (Policy)] > [ポリシー セット (Policy Sets)] を選択します。
- ステップ 2** [デフォルト (Default)] ポリシーをクリックします。デフォルト ポリシーが右側に表示されます。
- ステップ 3** 上部のプラス (+) 記号をクリックして、[上を作成 (Create Above)] を選択します。
- ステップ 4** このグループ ポリシーの名前、説明、条件を入力します。
- ステップ 5** 認証ポリシーを定義します。
- ステップ 6** 許可ポリシーを定義します。
- ステップ 7** [送信 (Submit)] をクリックします。ポリシー セットの設定後、Cisco ISE からログアウトされます。管理者ポータルにアクセスするために再度ログインする必要があります。
-

関連トピック

- [ポリシー モードの変更 \(705 ページ\)](#)
- [ルールベースの認証ポリシーの設定 \(707 ページ\)](#)
- [ポリシー セットの評価フロー \(709 ページ\)](#)
- [ポリシー セットの作成のガイドライン \(710 ページ\)](#)
- [グローバル許可例外ポリシー \(710 ページ\)](#)

認証ポリシーの組み込み設定

Cisco ISE には、一部の一般的な用途に対応した、さまざまなデフォルト設定が含まれています。

表 39: 認証ポリシー設定のデフォルト

[名前 (Name)]	ユーザインターフェイスのパス	説明	その他の情報
ネットワークアクセスのデフォルトの許可されるプロトコルアクセス サービス	[ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [設定 (Configuration)] > [許可されるプロトコル (Allowed Protocols)]	このデフォルトは、認証ポリシーに使用されるネットワークアクセスの組み込みの許可されるプロトコルサービスです。	このアクセスサービスは、有線および無線の 802.1X、および有線 MAB の認証ポリシーに使用できます。

[名前 (Name)]	ユーザインターフェイスのパス	説明	その他の情報
有線 802.1X 複合条件	[ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [認証 (Authentication)] > [ゲスト (Guest)] > [複合条件 (Compound Conditions)] を選択します。	この複合条件は次の属性と値をチェックします。 <ul style="list-style-type: none"> • RADIUS:Service-Type equals Framed • RADIUS:NAS-Port-Type equals Ethernet 	この複合条件は、有線 802.1X 認証ポリシーに使用できます。このポリシーに指定された基準に一致するすべての要求は、有線 802.1X 認証ポリシーに基づいて評価されます。
無線 802.1X 複合条件	[ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [認証 (Authentication)] > [ゲスト (Guest)] > [複合条件 (Compound Conditions)] を選択します。	この複合条件は次の属性と値をチェックします。 <ul style="list-style-type: none"> • RADIUS:Service-Type equals Framed • RADIUS:NAS-Port-Type equals Wireless-IEEE802.11 	この複合条件は、無線 802.1X 認証ポリシーに使用できます。このポリシーに指定された基準に一致するすべての要求は、無線 802.1X 認証ポリシーに基づいて評価されます。
有線 MAB 複合条件	[ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [認証 (Authentication)] > [ゲスト (Guest)] > [複合条件 (Compound Conditions)] を選択します。	この複合条件は次の属性と値をチェックします。 <ul style="list-style-type: none"> • RADIUS:Service-Type は Call-Check • RADIUS:NAS-Port-Type equals Ethernet 	この複合条件は、有線 MAB 認証ポリシーに使用できます。このポリシーに指定された基準に一致するすべての要求は、有線 MAB 認証ポリシーに基づいて評価されます。
Catalyst スイッチのローカル Web 認証複合条件	[ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [認証 (Authentication)] > [ゲスト (Guest)] > [複合条件 (Compound Conditions)] を選択します。	この複合条件は次の属性と値をチェックします。 <ul style="list-style-type: none"> • RADIUS:Service-Type equals Outbound • RADIUS:NAS-Port-Type equals Ethernet 	この複合条件を使用するには、この条件を確認する認証ポリシーを作成する必要があります。また、要件に基づいてアクセスサービスを定義するか、このポリシーのデフォルトネットワークアクセス許可プロトコルサービスを利用できます。

[名前 (Name)]	ユーザインターフェイスのパス	説明	その他の情報
ワイヤレス LAN コントローラ (WLC) ローカル Web 認証複合条件 (Wireless Lan Controller (WLC) Local Web Authentication Compound Condition)	[ポリシー (Policy)]> [ポリシー要素 (Policy Elements)]> [認証 (Authentication)]> [ゲスト (Guest)]> [複合条件 (Compound Conditions)]を選択します。	この複合条件は次の属性と値をチェックします。 <ul style="list-style-type: none"> • RADIUS:Service-Type equals Outbound • RADIUSNAS-Port-Type equals Wireless-IEEE802.11 	この複合条件を使用するには、この条件を確認する認証ポリシーを作成する必要があります。また、要件に基づいてアクセスサービスを定義するか、このポリシーのデフォルトネットワークアクセス許可プロトコルサービスを利用できます。
有線 802.1X 認証ポリシー	[ポリシー (Policy)]> [認証 (Authentication)]> [ルールベース (Rule-Based)]	このポリシーは、有線 802.1X 複合条件およびデフォルトのネットワークアクセスの許可されるプロトコルサービスを使用します。このポリシーは、有線 802.1X 複合条件で指定された基準に一致する要求を評価します。	このデフォルト ポリシーは ID ソースとして内部エンドポイントデータベースを使用します。このポリシーを編集して、あらゆる ID ソース順序やアイデンティティソースを必要に応じて設定できます。
無線 802.1X 認証ポリシー	[ポリシー (Policy)]> [認証 (Authentication)]> [ルールベース (Rule-Based)]	このポリシーは、無線 802.1X 複合条件およびデフォルトのネットワークアクセスの許可されるプロトコルサービスを使用します。このポリシーは、無線 802.1X 複合条件で指定された基準に一致する要求を評価します。	このデフォルト ポリシーは ID ソースとして内部エンドポイントデータベースを使用します。このポリシーを編集して、あらゆる ID ソース順序やアイデンティティソースを必要に応じて設定できます。

[名前 (Name)]	ユーザインターフェイスのパス	説明	その他の情報
有線 MAB 認証ポリシー	[ポリシー (Policy)] > [認証 (Authentication)] > [ルールベース (Rule-Based)]	このポリシーは、有線 MAB 複合条件およびデフォルトのネットワーク アクセスの許可されるプロトコルサービスを使用します。このポリシーは、有線 MAB 複合条件で指定された基準に一致する要求を評価します。	このデフォルト ポリシーは ID ソースとして内部エンドポイントデータベースを使用します。

関連トピック

[ネットワーク アクセス サービス \(691 ページ\)](#)

[ルールベースの認証ポリシーの設定 \(707 ページ\)](#)

認証結果の表示

Cisco ISE にはリアルタイムで認証の概要を表示するさまざまな方法があります。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 [操作 (Operations)] > [RADIUS ライブログ (RADIUS LiveLog)] を選択して、リアルタイムで認証の概要を表示します。

ステップ 2 認証の概要を表示するには、次のような方法があります。

- [ステータス (Status)] アイコンの上にマウスカーソルを移動すると、認証の結果と概要を表示できます。ステータスの詳細とともにポップアップが表示されます。
- 結果をフィルタリングするには、リストの最上部に表示される 1 つ以上の任意のテキストボックスに検索条件を入力して **Enter** を押します。
- 詳細レポートを表示するには、[詳細 (Details)] カラムにある虫眼鏡アイコンをクリックします。

(注) 認証概要レポートまたはダッシュボードが失敗または成功した認証に対応する最新のデータを収集して表示するため、レポートの内容は数分の遅延の後に表示されます。

認証ダッシュレット

Cisco ISE のダッシュボードには、ネットワークとデバイスに対し行われたすべての認証の概要が表示されます。これには、認証ダッシュレットにある認証および許可の失敗についての概要情報が表示されます。

RADIUS 認証ダッシュレットには、Cisco ISE が処理した認証に関する次の統計情報が表示されます。

- 認証成功、認証失敗、同一ユーザによる同時ログインなど、Cisco ISE が処理した RADIUS 認証要求の総数。
- Cisco ISE が処理した、失敗した RADIUS 認証要求の総数。

また、TACACS+ 認証の概要を表示することもできます。TACACS+ 認証ダッシュレットには、デバイス認証の統計情報が表示されます。

デバイス管理認証の詳細については、[TACACS ライブ ログ \(1459 ページ\)](#) を参照してください。RADIUS ライブ ログ設定の詳細については、[RADIUS ライブ ログ \(1451 ページ\)](#) を参照してください。

ISE コミュニティ リソース

認証と許可の失敗のトラブルシューティング方法については、「[How To: Troubleshoot ISE Failed Authentications & Authorizations](#)」を参照してください。

認証レポートおよびトラブルシューティング ツール

認証の詳細の他に、Cisco ISE では、ネットワークの効率的な管理に使用できるさまざまなレポートおよびトラブルシューティング ツールが提供されます。

ネットワーク内の認証の傾向およびトラフィックを把握するために実行できるさまざまなレポートがあります。現在のデータに加えて履歴のレポートを生成できます。認証レポートのリストは次のとおりです。

- AAA の診断
- RADIUS アカウンティング (RADIUS Accounting)
- RADIUS 認証
- 認証概要 (Authentication Summary)



第 21 章

許可ポリシーおよびプロファイルの管理

- [Cisco ISE の許可ポリシー](#) (717 ページ)
- [Cisco ISE の許可プロファイル](#) (717 ページ)
- [デフォルトの許可ポリシー、ルール、プロファイルの設定](#) (722 ページ)
- [許可ポリシーの設定](#) (728 ページ)
- [許可プロファイルの権限](#) (732 ページ)
- [ダウンロード可能 ACL \(Downloadable ACLs\)](#) (733 ページ)
- [Active Directory ユーザ許可のためのマシン アクセス制限](#) (734 ページ)

Cisco ISE の許可ポリシー

許可ポリシーは、Cisco ISE ネットワーク許可サービスのコンポーネントです。このサービスを使用して、ネットワーク リソースにアクセスする特定のユーザおよびグループの許可ポリシーを定義し、許可プロファイルを設定することができます。

許可ポリシーには条件付きの要件を含めることができ、この要件では、1つ以上の許可プロファイルを返すことができる許可チェックを含む複合条件を使用して、1つ以上の ID グループを組み合わせます。また、特定の ID グループを使用しない条件付きの要件が存在する場合があります（デフォルトの「Any」の使用など）。

許可ポリシーは、Cisco Identity Services Engine (Cisco ISE) で許可プロファイルを作成する場合に使用されます。許可ポリシーは許可ルールで構成されます。許可ルールには、名前、属性、および権限の3つの要素があります。権限要素は、許可プロファイルにマッピングする要素です。

Cisco ISE の許可プロファイル

許可ポリシーは、特定のユーザおよびグループの ID にルールを関連付け、対応するプロファイルを作成します。これらのルールが設定された属性と一致する場合は、常に、権限を付与する、対応する許可プロファイルがポリシーによって返され、ネットワーク アクセスがこれに応じて許可されます。

たとえば、許可プロファイルには、次のタイプに含まれるさまざまな権限を含めることができます。

- 標準プロファイル
- 例外プロファイル
- デバイススペースのプロファイル

プロファイルは、利用可能なベンダー ディクショナリのいずれかに保存されているリソース セットから選択された属性で構成され、特定の許可ポリシーの複合条件が一致したときに返されます。許可ポリシーには単一のネットワーク サービス ルールにマッピングする複合条件を含めることができるため、許可チェックのリストを含めることもできます。

単純なシナリオでは、すべての許可チェックがルール内で AND ブール演算子を使用して作成されます。高度なシナリオでは、任意のタイプの許可確認式を使用できますが、これらの許可確認は、返される許可プロファイルに準拠する必要があります。許可確認は、通常、ライブラリに追加できるユーザ定義名を含む1つ以上の条件から構成され、他の許可ポリシーで再利用できます。

関連トピック

[許可ポリシーの用語](#) (718 ページ)

[許可ポリシーとサポートされているディクショナリ](#) (720 ページ)

[許可ポリシーの設定](#) (728 ページ)

[許可プロファイルの権限](#) (732 ページ)

[ダウンロード可能 ACL に対する権限の設定](#) (734 ページ)

許可ポリシーの用語

Cisco ISE ネットワークやリソースにアクセスするユーザの、ネットワーク許可用の許可プロファイルおよびポリシーを定義できます。Cisco ISE は、ダウンロード可能 ACL (DACL) も使用します。

ネットワーク許可

ネットワーク許可は、ネットワークおよびそのリソースへのユーザアクセスならびに各ユーザがシステム上でこれらのリソースに対して実行できることを制御します。読み取り、書き込み、および実行権限を許可する権限セットを定義して、Cisco ISE からネットワーク許可をアクティブにします。Cisco ISE では、ネットワークのニーズに合わせて、多数のさまざまな許可ポリシーを作成できます。このリリースでは、Cisco ISE ネットワークとリソースへの RADIUS アクセスだけをサポートします。

ポリシー要素

ポリシー要素は許可ポリシーを定義するコンポーネントであり、次のものがあります。

- ルール名

- ID グループ
- 条件 (Conditions)
- 権限 (Permissions)

これらのポリシー要素は、ポリシールールを作成したときに参照され、条件および属性の選択によって、特定のタイプの許可プロファイルを作成できます。

許可プロファイル

許可プロファイルは、多数の特定の権限によって一連のネットワークサービスへのアクセスが許可されるコンテナとして機能します。許可プロファイルには、ネットワークアクセス要求に付与される権限セットを定義し、次のものを含めることができます。

- プロファイル名
- プロファイルの説明
- 関連 DACL
- 関連 VLAN
- 関連 SGACL
- 任意の数の他のディクショナリベースの属性

許可ポリシー

許可ポリシーは、ユーザ定義の単一のルールまたはルールのセットで構成できます。これらのルールは、特定のポリシーを作成するために機能します。たとえば、標準ポリシーは、ID グループ用に入力した値と特定の条件または属性をリンクする If-Then 表記法を使用するルール名を含め、一意の許可プロファイルを作成する特定の権限セットを生成できます。設定できる許可ポリシー オプションは 2 つあります。

- 最初に一致したルールの適用 (First Matched Rules Apply)
- 複数の一致するルールの適用 (Multiple Matched Rule Applies)

これら 2 つのオプションは、ユーザの権限セットと一致したときに、標準ポリシーテーブルにリストされている最初に一致したルール タイプの使用または複数の一致したルール タイプの使用のいずれかを Cisco ISE に指示します。設定できる許可ポリシーには、次の 2 つのタイプがあります。

- 標準：標準ポリシーは、長期間有効なままにし、ユーザ、デバイス、またはグループの大規模なグループに適用し、特定またはすべてのネットワークエンドポイントへのアクセスを許可するために作成されるポリシーです。標準ポリシーは変更しないようにし、権限の共通セットを共有するユーザ、デバイス、グループの大規模なグループに適用します。

標準ポリシーは、特定の条件または権限を使用する特定の ID グループに使用するために変更したり、新しい事業部門、ユーザグループ、デバイス、ネットワークグループのニー

ズを満たすための別のタイプの標準ポリシーを作成したりするためのテンプレートとして使用できます。

- 例外：これとは対照的に、例外ポリシーは、標準ポリシーの例外として機能するタイプのポリシーであるため、適切な名前を付けられます。例外ポリシーは、短期間のポリシー期間、特定のタイプのネットワーク デバイス、ネットワーク エンドポイントまたはグループ、特別な条件や権限を満たすニーズ、あるいは即時要件などのさまざまな要因に基づく制限されたアクセスを許可することを目的としています。

例外ポリシーは、制限された数のユーザ、デバイス、またはグループにネットワーク リソースへのアクセスを許可するなどの、即時または短期間のニーズを満たすために作成します。例外ポリシーを使用すると、1 人のユーザまたはユーザのサブセットに合わせて調整された、ID グループ、条件、または権限に対する、カスタマイズされた値の特定のセットを作成できます。これにより、さまざまな、またはカスタマイズされたポリシーを作成し、企業、グループ、またはネットワークのニーズを満たすことができます。

アクセスコントロール リスト

Cisco ISE システムのアクセス コントロール リスト (ACL) は、特定のオブジェクトまたはネットワーク リソースに接続する権限のリストです。ACL は、いずれのユーザまたはグループがオブジェクトへのアクセス権を付与されるか、および指定されたオブジェクトまたはネットワーク リソースでどの操作が許可されるかを指定します。一般的な ACL の各エントリは、サブジェクトおよび操作を指定するか、または状態（許可または拒否など）を提供します。

許可ポリシーとサポートされているディクショナリ

許可ポリシータイプの場合、確認は、返される許可プロファイルに準拠する必要があります。

確認には、通常、ライブラリに追加して他のポリシーで再利用できるユーザ定義名を含む 1 つ以上の条件が含まれます。条件は、Cisco ISE ディクショナリからの属性を使用して条件を定義します。ディクショナリには、次のものがあります。

- システム定義されたディクショナリ：
 - RADIUS
- RADIUS ベンダー ディクショナリ
 - Airespace
 - Cisco
 - Cisco-BBSM
 - Cisco-VPN3000
 - Microsoft

許可ポリシーおよびプロファイルの設定のガイドライン

許可ポリシーおよびプロファイルを管理または運用する場合、次のガイドラインに従ってください。

- 作成するルール名は、サポートされている次の文字のみを使用する必要があります。
 - 記号：プラス (+)、ハイフン (-)、アンダースコア (_)、ピリオド (.)、およびスペース ()。
 - アルファベット文字：A ～ Z、a ～ z。
 - 数字：0 ～ 9。
- ID グループのデフォルトは「Any」です（このグローバル デフォルトを使用してすべてのユーザに適用できます）。
- 条件では、1 つ以上のポリシー値を設定することが許可されています。ただし、条件はオプションであり、許可ポリシーを作成する場合に必須ではありません。条件の作成には 2 つの方法があります。
 - 選択肢の対応するディクショナリから既存の条件または属性を選択します。
 - 推奨値を選択またはテキストボックスを使用してカスタム値を入力できるカスタム条件を作成します。
- 作成する条件名は、サポートされている次の文字のみを使用する必要があります。
 - 記号：ハイフン (-)、アンダースコア (_)、およびピリオド (.)。
 - アルファベット文字：A ～ Z、a ～ z。
 - 数字：0 ～ 9。
- 権限は、ポリシーに使用する許可プロファイルを選択するときに重要です。権限は、特定のリソースへのアクセス権を付与したり、特定のタスクの実行を可能にしたりできます。たとえば、あるユーザが特定の ID グループ（デバイス管理者など）に属しており、そのユーザが定義済みの条件（サイトがボストンにあるなど）を満たしている場合、このユーザは、そのグループに関連付けられた権限（特定のネットワーク リソースのセットへのアクセス権、デバイスへの特定の操作を実行する権限など）を付与されます。
- 必ず[保存 (Save)] をクリックして、新規または変更したポリシーやプロファイルを Cisco ISE データベースに保存します。

デフォルトの許可ポリシー、ルール、プロファイルの設定

Cisco ISE ソフトウェアには、共通設定を提供する多数のデフォルトの条件、ルール、プロファイルが事前インストールされているため、Cisco ISE の許可ポリシーおよびプロファイルに必要なルールおよびポリシーを容易に作成できます。

表に、Cisco ISE で指定された値が含まれている組み込み設定のデフォルトを示します。

表 40: 許可ポリシー、プロファイル、およびルールの設定のデフォルト

[名前 (Name)]	ユーザインターフェイスのパス	説明	その他の情報
許可ポリシーのデフォルト			
許可ポリシーのデフォルトの複合条件	[ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [条件 (Conditions)] > [許可 (Authorization)]	これらは、許可ポリシーで使用される条件、ルール、およびプロファイルの事前インストールされた設定のデフォルトです。	許可ポリシーを作成するために、次の関連属性を使用できます。 <ul style="list-style-type: none"> • 有線 802.1x • 有線 MAB • 無線 802.1x • Catalyst スイッチ ローカル Web 認証 • WLC Web 認証
有線 MAB 複合条件	[ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [条件 (Conditions)] > [許可 (Authorization)] > [複合条件 (Compound Conditions)]	この複合条件は次の属性と値をチェックします。 <ul style="list-style-type: none"> • RADIUS:Service-Type = Call-Check • RADIUS:NAS-Port-Type = Ethernet 	この複合条件は、有線 MAB 許可ポリシーで使用されます。このポリシーで指定された基準に一致する要求は、有線 MAB 許可ポリシーに基づいて評価されます。

[名前 (Name)]	ユーザインターフェイスのパス	説明	その他の情報
無線 802.1X 複合条件	[ポリシー (Policy)]>[ポリシー要素 (Policy Elements)]>[条件 (Conditions)]>[許可 (Authorization)]>[複合条件 (Compound Conditions)]	この複合条件は次の属性と値をチェックします。 <ul style="list-style-type: none"> • RADIUS:Service-Type = Framed • RADIUSNAS-Port-Type = Wireless-IEEE802.11 	この複合条件は、無線 802.1X 許可ポリシーで使用されます。 このポリシーで指定された基準に一致する要求は、無線 802.1X 許可ポリシーに基づいて評価されます。
許可プロファイル設定のデフォルト			
Blacklist_Access	[ポリシー (Policy)]>[ポリシー要素 (Policy Elements)]>[結果 (Results)]>[許可プロファイル (Authorization Profiles)]>[Blacklist_Access]	この許可プロファイルは、ブラックリストに登録されているデバイスへのアクセスを拒否します。ブラックリストに登録されているデバイスはすべて、次の URL にリダイレクトされます。 http://10.10.10.10:8080/	このデフォルトの許可プロファイルは、デバイスポータルで「失われた」として宣言されているすべてのエンドポイントに適用されます。
Cisco_IP_Phones	[ポリシー (Policy)]>[ポリシー要素 (Policy Elements)]>[結果 (Results)]>[許可プロファイル (Authorization Profiles)]>[Cisco_IP_Phones]	この許可プロファイルでは、次の値の設定デフォルトプロファイルを使用します。 <ul style="list-style-type: none"> • [名前 (Name)] : [Cisco IP Phone] • [DACL] : [PERMIT_ALL_TRAFFIC] • [VSA] : [compulsary-voice] <p>このプロファイルは、このプロファイルで指定された基準に一致する要求を評価します。</p>	このデフォルトの許可プロファイルは、DACL およびベンダー固有属性 (VSA) を使用して、すべての「音声」トラフィックを許可します (PERMIT_ALL_TRAFFIC) 。
許可ポリシーのデフォルト			

[名前 (Name)]	ユーザインターフェイスのパス	説明	その他の情報
有線 802.1X 複合条件	[ポリシー (Policy)]>[ポリシー要素 (Policy Elements)]>[条件 (Conditions)]>[許可 (Authorization)]>[複合条件 (Compound Conditions)]	この複合条件は次の属性と値をチェックします。 <ul style="list-style-type: none"> • RADIUS:Service-Type = Framed • RADIUS:NAS-Port-Type = Ethernet 	この複合条件は、有線 802.1X 許可ポリシーで使用されます。 このポリシーで指定された基準に一致する要求は、有線 802.1X 許可ポリシーに基づいて評価されます。
Catalyst スイッチのローカル Web 認証複合条件	[ポリシー (Policy)]>[ポリシー要素 (Policy Elements)]>[条件 (Conditions)]>[許可 (Authorization)]>[複合条件 (Compound Conditions)]	この複合条件は次の属性と値をチェックします。 <ul style="list-style-type: none"> • RADIUS:Service-Type = Outbound • RADIUS:NAS-Port-Type = Ethernet 	この複合条件を使用するには、この条件を確認する許可ポリシーを作成する必要があります。
ワイヤレス LAN コントローラ (WLC) ローカル Web 認証複合条件 (Wireless Lan Controller (WLC) Local Web Authentication Compound Condition)	[ポリシー (Policy)]>[ポリシー要素 (Policy Elements)]>[条件 (Conditions)]>[許可 (Authorization)]>[複合条件 (Compound Conditions)]	この複合条件は次の属性と値をチェックします。 <ul style="list-style-type: none"> • RADIUS:Service-Type = Outbound • RADIUS:NAS-Port-Type = Wireless-IEEE802.11 	この複合条件を使用するには、この条件を確認する許可ポリシーを作成する必要があります。

[名前 (Name)]	ユーザインターフェイスのパス	説明	その他の情報
ブラックリストのデフォルトの許可ルール	[ポリシー (Policy)]> [許可ポリシー (Authorization Policy)]	<p>この許可ポリシーでは、次の値の設定デフォルトルールを使用します。</p> <ul style="list-style-type: none">• [ルール名 (Rule Name)] : [ブラックリストのデフォルト (Black List Default)]• [エンドポイント ID グループ (Endpoint Identity Group)] : [ブラックリスト (Blacklist)]• 条件 : すべて• 権限/許可プロファイル : Blacklist_Access	このデフォルトルールは、「失われた」ユーザデバイスがシステムから削除されるか、または「復元される」まで、このようなデバイスを適切にプロビジョニングするように設計されています。

[名前 (Name)]	ユーザインターフェイスのパス	説明	その他の情報
プロファイリングされた Cisco IP Phone 許可ルール	[ポリシー (Policy)]> [許可ポリシー (Authorization Policy)]	<p>この許可ポリシーでは、次の値の設定デフォルトルールを使用します。</p> <ul style="list-style-type: none"> • [ルール名 (Rule Name)] : [プロファイリングされた Cisco IP Phone (Profiled Cisco IP Phones)] • [エンドポイント ID グループ (Endpoint Identity Group)] : [Cisco-IP-Phones] • 条件 : すべて • [権限/許可プロファイル (Permissions/Authorization Profile)] : [Cisco_IP_Phones] 	このデフォルトルールは、デフォルトのエンドポイント ID グループとして Cisco IP Phone を使用し、このテーブルにリストされている値を使用します。
許可ルール設定のデフォルト			

[名前 (Name)]	ユーザインターフェイスのパス	説明	その他の情報
デフォルトの許可ルール	[ポリシー (Policy)]> [許可ポリシー (Authorization Policy)]	<p>この許可ポリシーでは、次の値の設定デフォルトルールを使用します。</p> <ul style="list-style-type: none"> • [ルール名 (Rule Name)] : [デフォルト (Default)] • [エンドポイント ID グループ (Endpoint Identity Group)] : [任意 (Any)] • 条件 : すべて • [許可プロファイル (Authorization Profile)] : [PermitAccess] 	このデフォルトルールは、デフォルトのエンドポイント ID グループとして [任意 (Any)] を使用し、このテーブルにリストされている値を使用します。

デフォルトの許可ルール

Cisco ISE ソフトウェアには、より簡単に許可ポリシーおよびプロファイルを作成できるようにする多数の事前設定済み許可ルールが付属しています。これらのルールは、デフォルトでは無効になっています。要件に基づいて、これらのルールを有効にできます。

表 41: 事前設定済み許可ルール

ルール名 (Rule Name)	説明	条件 (Conditions)	権限 (Permissions)
Basic_Authenticated_Access	認証されたユーザへのアクセスを可能にします。	Network_Access_Authentication_Passed	PermitAccess
Wi-Fi_Redirect_to_Guest_Login	ユーザを CWA ポータルにリダイレクトします。	Wireless_MAB	Cisco_WebAuth

ルール名 (Rule Name)	説明	条件 (Conditions)	権限 (Permissions)
Wi-Fi_Guest_Access	ゲスト ユーザが WebAuth から認証された後にゲスト アクセスを許可します。	(GuestType_Daily (デフォルト) または GuestType_Weekly (デフォルト) または GuestType_Contractor (デフォルト)) および (Wireless_MAB および Guest_Flow)	Guest および PermitAccess
Compliant_Devices_Access	対応デバイスのアクセスをイネーブルにします。	Compliant_Devices	PermitAccess
Employee_Onboarding	MSCHAPv2 を使用する無線 802.1X 認証がネイティブ サプリカント プロビジョニング プロセスにリダイレクトされます。	(Wireless_802.1X および EAP-MSCHAPv2)	NSP_Onboard および BYOD



(注) 事前設定済みの許可ルールは新規インストールでのみ利用可能です。これらのルールは、Cisco ISE の以前のバージョンからアップグレードした場合は使用できません。

許可ポリシーの設定

[許可ポリシー (Authorization Policy)] ページでは、許可ポリシーを表示、作成、複製/変更、削除できます。次の許可ポリシープロファイルの各項には、標準許可ポリシーで指示されるアクションの例が示されています。同じプロセスに従って例外許可ポリシーを管理できます。

始める前に

この手順を開始する前に、管理者ポータルで使用される管理およびルールベース条件、ID グループ、状態、権限の基本構成要素と利用方法の基本を理解している必要があります。

ステップ 1 [ポリシー (Policy)] > [許可 (Authorization)] > [標準 (Standard)] を選択します。

ステップ 2 右端にある下矢印をクリックし、[新規ルールを上挿入 (Insert New Rule Above)] または [新規ルールを下挿入 (Insert New Rule Below)] のどちらかを選択します。

ステップ 3 ルール名を入力し、許可ポリシーの ID グループ、条件、属性、および権限を選択します。

選択するすべての属性に「Equals」、「Not Equals」、「Matches」、「Starts With」、「Not Starts With」の演算子オプションが含まれているわけではありません。

「Matches」演算子は、ワイルドカードなしの正規表現 (REGEX) をサポートし、使用します。

- (注) 単純比較の場合は、「equals」演算子を使用する必要があります。「Contains」演算子は、複数值属性に使用できます。正規表現の比較には、「Matches」演算子を使用する必要があります。「Matches」演算子を使用すると、正規表現は静的値と動的値の両方について解釈されます。

ステップ 4 [完了 (Done)] をクリックします。

ステップ 5 [保存 (Save)] をクリックして、変更を Cisco ISE システム データベースに保存し、この新しい許可ポリシーを作成します。

関連トピック

- [単純条件の作成](#) (661 ページ)
- [複合条件の作成](#) (661 ページ)
- [単純条件と複合条件](#) (659 ページ)
- [許可ポリシーの設定](#) (1356 ページ)

許可ポリシーの属性および条件

許可ポリシー条件を作成するときに、有効な属性を再利用するには、サポートされている属性を含むディクショナリから選択します。たとえば、Cisco ISE は、AuthenticationIdentityStore という属性を提供しています。これは NetworkAccess ディクショナリにあります。この属性は、ユーザの認証中にアクセスされた最後の ID ソースを識別します。

- 認証中に単一の ID ソースが使用されると、この属性には認証が成功した ID ストアの名前が含まれます。
- 認証中に ID ソース順序を使用する場合、この属性にはアクセスされた最後の ID ソースの名前が含まれます。

AuthenticationStatus 属性を AuthenticationIdentityStore 属性と組み合わせて使用し、ユーザが正常に認証された ID ソースを識別する条件を定義できます。たとえば、許可ポリシーで LDAP ディレクトリ (LDAP13) を使用してユーザが認証された条件をチェックするために、次の再利用可能な条件を定義できます。

```
If NetworkAccess.AuthenticationStatus EQUALS AuthenticationPassed AND  
NetworkAccess.AuthenticationIdentityStore EQUALS LDAP13
```



- (注) AuthenticationIdentityStore は、条件にデータを入力できるテキストフィールドを表します。このフィールドには、名前を必ず正しく入力またはコピーします。ID ソースの名前が変更された場合は、ID ソースの変更と一致するように、この条件を変更する必要があります。

以前認証されたエンドポイント ID グループに基づく許可条件を定義するために、Cisco ISE では、エンドポイント ID グループ 802.1X 認証ステータスの間に定義された許可をサポートしています。Cisco ISE では、802.1X 認証を実行するとき、RADIUS 要求の「Calling-Station-ID」フィールドから MAC アドレスを抽出し、この値を使用して、デバイスのエンドポイント ID グループ（endpointIDgroup 属性として定義）のセッション キャッシュを検索して読み込みます。

このプロセスによって、許可ポリシー条件の作成に endpointIDgroup 属性を使用できるようになり、ユーザ情報に加えてこの属性を使用して、エンドポイント ID グループ情報に基づく許可ポリシーを定義できます。

エンドポイント ID グループの条件は、[許可ポリシー設定（authorization policy configuration）] ページの [ID グループ（ID Groups）] カラムで定義できます。ユーザ関連情報に基づく条件は、許可ポリシーの [その他の条件（Other Conditions）] のセクションで定義する必要があります。ユーザ情報が内部ユーザ属性に基づいている場合は、内部ユーザディクショナリの ID グループ属性を使用します。たとえば、「User Identity Group:Employee:US」のような値を使用して、ID グループに完全な値のパスを入力できます。

ISE コミュニティ リソース

SSID に基づく Cisco ISE での許可ポリシーの設定方法の例については、「[ISE Policies Based on SSID Configuration Example](#)」を参照してください。

時刻と日付の条件

[ポリシー要素条件（Policy Elements Conditions）] ページを使用して、時刻と日付のポリシー要素条件を表示、作成、変更、削除、複製、および検索します。ポリシー要素は、設定した特定の時刻と日付の属性設定に基づく条件を定義する共有オブジェクトです。

時刻と日付の条件を使用すると、Cisco ISE システム リソースにアクセスする権限を、作成した属性設定で指定された特定の時刻と日付に設定または制限できます。

関連トピック

[時刻と日付の条件の設定](#)（1399 ページ）

[時刻と日付の条件の作成](#)（672 ページ）

許可ポリシーでの IPv6 属性の使用

Cisco ISE では、エンドポイントからの IPv6 トラフィックを検出、管理、保護できます。

IPv6 対応エンドポイントが Cisco ISE ネットワークに接続すると、IPv6 ネットワーク経由でネットワーク アクセスデバイス（NAD）と通信します。NAD は、アカウントिंगおよびプロファイリングの情報をエンドポイント（IPv6 値を含む）から Cisco ISE に IPv4 ネットワークを介して伝達します。IPv6 属性を使用して、IPv6 対応エンドポイントからのそのような要求を処理し、エンドポイントが準拠していることを保証するための、許可プロファイルおよびポリシーを Cisco ISE で設定できます。

ワイルドカード文字は、IPv6 プレフィックスと IPv6 インターフェイスの値でサポートされています。たとえば、2001:db8:1234::/48 です。

サポートされている IPv6 アドレス形式は次のとおりです。

- 完全表記：コロンで区切られた 4 つの 16 進数桁の 8 つのグループ。たとえば、2001:0db8:85a3:0000:0000:8a2e:0370:7334 です。
- 短縮表記：1 つのグループ内にある先行ゼロは除きます。ゼロのグループを 2 つの連続するコロンに置き換えます。たとえば、2001:db8:85a3::8a2e:370:7334 です。
- ドット区切りの 4 つの表記（IPv4 対応付けおよび IPv4 互換性 IPv6 アドレス）：たとえば、::ffff:192.0.2.128 です。

サポートされている IPv6 属性は次のとおりです。

- NAS-IPv6-Address
- Framed-Interface-Id
- Framed-IPv6-Prefix
- Login-IPv6-Host
- Framed-IPv6-Route
- Framed-IPv6-Pool
- Delegated-IPv6-Prefix
- Framed-IPv6-Address
- DNS-Server-IPv6-Address
- Route-IPv6-Information
- Delegated-IPv6-Prefix-Pool
- Stateful-IPv6-Address-Pool

サポートされるシスコの属性と値のペアおよび対応する IETF 属性を次の表に示します。

シスコの属性と値のペア	IETF 属性
ipv6:addrv6=<ipv6 address>	Framed-ipv6-Address
ipv6:stateful-ipv6-address-pool=<name>	Stateful-IPv6-Address-Pool
ipv6:delegated-ipv6-pool=<name>	Delegated-IPv6-Prefix-Pool
ipv6:ipv6-dns-servers-addr=<ipv6 address>	DNS-Server-IPv6-Address

[RADIUSライブログ (RADIUS Live Logs)] ページ、RADIUS 認証レポート、RADIUS アカウ
ンティング レポート、現在アクティブなセッション レポート、RADIUS エラー レポート、設
定が誤っている NAS レポート、EPS 監査レポート、および設定が誤っているサブリカントレ
ポートは、IPv6 アドレスをサポートしています。[RADIUSライブログ (RADIUS Live Logs)]

ページ、またはこれらのレポートのいずれかから、これらのセッションの詳細を表示できます。IPv4、IPv6、または MAC アドレスに基づいてレコードをフィルタリングできます。



- (注) IPv6 対応の DHCPv6 ネットワークに Android デバイスを接続すると、そのデバイスは DHCP サーバからリンクローカルの IPv6 アドレスのみを受信します。したがって [ライブ ログ (Live Log)] と [エンドポイント (Endpoints)] ページ ([ワーク センター (Work Centers)] > [ネットワーク アクセス (Network Access)] > [ID (Identities)] > [エンドポイント (Endpoints)]) にはグローバル IPv6 アドレスは表示されません。

次の手順は、許可ポリシーに IPv6 属性を設定する方法を説明します。

始める前に

展開内の NAD が IPv6 による AAA をサポートしていることを確認します。NAD で IPv6 の AAA サポートをイネーブルにする方法については、『[AAA Support for IPv6](#)』を参照してください。

ステップ 1 [ポリシー (Policy)] > [認証 (Authorization)] > [標準 (Standard)] を選択します。

ステップ 2 右端にある下矢印をクリックし、[新規ルールを上挿入 (Insert New Rule Above)] または [新規ルールを下挿入 (Insert New Rule Below)] のどちらかを選択します。

ステップ 3 ルール名を入力し、条件を指定します。

RADIUS デictionary から、RADIUS IPv6 属性、演算子、および値を選択します。

ステップ 4 [完了 (Done)]

許可プロファイルの権限

許可プロファイルの権限設定を開始する前に、以下を確認します。

- 許可ポリシーおよび許可プロファイル間の関係を理解している
- 許可プロファイル ページをよく理解している
- ポリシーおよびプロファイルを設定する場合に必要な基本ガイドラインを知っている
- 許可プロファイルの権限の構成を理解している

許可プロファイルを使用するには、[ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] を選択します。左側のメニューから、[認証 (Authorization)] > [許可プロファイル (Authorization Profiles)] を選択します。

ネットワークでさまざまなタイプの許可プロファイルのポリシー要素権限を表示、作成、変更、削除、複製、または検索するプロセスの開始点として [結果 (Results)] ナビゲーション

ペインを使用します。[結果 (Results)] ペインには、最初 [認証 (Authentication)]、[許可 (Authorization)]、[プロファイリング (Profiling)]、[ポスチャ (Posture)]、[クライアントプロビジョニング (Client Provisioning)]、および [TrustSec] のオプションが表示されています。

許可プロファイルでは、RADIUS 要求が受け入れられたときに返される属性を選択できます。Cisco ISE では、[共通タスク (Common Tasks)] 設定を設定して共通に使用される属性をサポートできるメカニズムが提供されます。Cisco ISE が基盤となる RADIUS 値に変換する [共通タスク (Common Tasks)] 属性の値を入力する必要があります。

ISE コミュニティ リソース

802.1x サプリカント (Cisco AnyConnect Mobile Security) とオーセンティケータ (スイッチ) 間の Media Access Control Security (MACsec) 暗号化を設定する方法の例については、「[MACsec Switch-host Encryption with Cisco AnyConnect and ISE Configuration Example](#)」を参照してください。

関連トピック

- [許可ポリシーとサポートされているディクショナリ \(720 ページ\)](#)
- [許可ポリシーおよびプロファイルの設定のガイドライン \(721 ページ\)](#)
- [新しい標準許可プロファイルの権限の設定 \(733 ページ\)](#)
- [デフォルトの許可ポリシー、ルール、プロファイルの設定 \(722 ページ\)](#)
- [デフォルトの許可ルール \(727 ページ\)](#)

新しい標準許可プロファイルの権限の設定

- ステップ 1** [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] > [許可 (Authorization)] > [許可プロファイル (Authorization Profiles)] を選択します。
- ステップ 2** [追加 (Add)] をクリックします。
- ステップ 3** 必要に応じて値を入力して、新しい許可プロファイルを設定します。[名前 (name)] フィールドでサポートされる文字は次のとおりです：スペース、! # \$ % & ' () * + , - . / ; = ? @ _ { }。
- ステップ 4** [送信 (Submit)] をクリックして変更を Cisco ISE システム データベースに保存し、許可プロファイルを作成します。

関連トピック

- [許可プロファイルの設定 \(1421 ページ\)](#)

ダウンロード可能 ACL (Downloadable ACLs)

DACL を定義して、Access-Accept メッセージを返すことができます。ACL を使用して、ネットワークに不要なトラフィックが発生することを防止します。ACL では、RADIUS プロトコル

を使用して、送信元 IP アドレスと宛先 IP アドレス、トランスポートプロトコルなどをフィルタリングできます。

名前付き権限オブジェクトとして作成した DACL は、許可プロファイルに追加できます。その後、これらの許可プロファイルを許可ポリシーの結果として指定できます。

既存の DACL と同じか、または類似する新しい DACL を作成する場合は、ダウンロード可能 ACL を複製できます。

複製の完了後、各 DACL（元の DACL および複製された DACL）に個別にアクセスして、編集または削除します。



- (注) DACL 作成中は、キーワード **Any** が DACL のすべての ACE のソースである必要があります。DACL がプッシュされると、ソースの **Any** がスイッチに接続されているクライアントの IP アドレスで置き換えられます。

関連トピック

[ダウンロード可能 ACL に対する権限の設定](#) (734 ページ)

ダウンロード可能 ACL に対する権限の設定

- ステップ 1** [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] > [許可 (Authorization)] > [ダウンロード可能 ACL (Downloadable ACLs)] を選択します。
- ステップ 2** [操作 (Action)] アイコンをクリックし、[DACL の作成 (Create DACL)] を選択するか、[DACL 管理ページ (DACL Management)] ページにある [追加 (Add)] をクリックします。
- ステップ 3** DACL に値を入力します。[名前 (name)] フィールドでサポートされる文字は次のとおりです：スペース、! # \$ % & ' () * + , - . / ; = ? @ _ { }。
- ステップ 4** [送信 (Submit)] をクリックします。

Active Directory ユーザ許可のためのマシン アクセス制限

Cisco ISE には、Microsoft Active Directory 認証ユーザの許可を制御する追加の方法を提供する、マシン アクセス制限 (MAR) コンポーネントが含まれています。この形式の許可は、Cisco ISE ネットワークにアクセスするために使用されるコンピュータのマシン認証に基づきます。成功したマシン認証ごとに、Cisco ISE は、RADIUS Calling-Station-ID 属性 (属性 31) で受信した値を、成功したマシン認証の証拠としてキャッシュします。

Cisco ISE は、[Active Directory の設定 (Active Directory Settings)] ページの [存続可能時間 (Time to Live)] パラメータで設定された時間が失効になるまで各 Calling-Station-ID 属性値をキャッシュに保持します。失効したパラメータは、Cisco ISE によってキャッシュから削除されます。

ユーザをエンドユーザ クライアントから認証する場合、Cisco ISE は、成功したマシン認証の Calling-Station-ID 値のキャッシュを検索して、ユーザ認証要求で受信した Calling-Station-ID 値を見つけようとします。Cisco ISE が一致するユーザ認証 Calling-Station-ID 値をキャッシュで見つけた場合、これは、次の方法で認証を要求するユーザに Cisco ISE が権限を割り当てる方法に影響します。

- Calling-Station-ID 値が Cisco ISE キャッシュで見つかった値と一致する場合、成功した許可の許可プロファイルを割り当てます。
- Calling-Station-ID 値が Cisco ISE キャッシュの値と一致しないことがわかった場合、マシン認証のない成功したユーザ認証の許可プロファイルを割り当てます。



第 22 章

脅威中心型 NAC サービスの設定

- [脅威中心型 NAC サービス \(737 ページ\)](#)

脅威中心型 NAC サービス

脅威中心型ネットワークアクセスコントロール (TC-NAC) 機能により、脅威および脆弱性のアダプタから受信する脅威と脆弱性の属性に基づいて、許可ポリシーを作成できます。脅威の重大度レベルと脆弱性評価の結果は、エンドポイントまたはユーザのアクセスレベルを動的に制御するために使用できます。

忠実度の高い侵害の兆候 (IoC)、脅威検出イベント、および CVSS スコアを Cisco ISE に送信するように脆弱性および脅威のアダプタを設定できます。これにより、エンドポイントの権限とコンテキストを適宜変更するための脅威中心型アクセス ポリシーを作成できます。

Cisco ISE では次のアダプタがサポートされています。

- SourceFire FireAMP
- Cognitive Threat Analytics (CTA) アダプタ
- Qualys
- Rapid7 Nexpose
- Tenable Security Center

エンドポイントの脅威イベントが検出されたら、[侵害されたエンドポイント (Compromised Endpoints)] ページでエンドポイントの MAC アドレスを選択して ANC ポリシー (Quarantine など) を適用できます。Cisco ISE は、そのエンドポイントに対して CoA をトリガーし、対応する ANC ポリシーを適用します。ANC ポリシーが使用可能ではない場合、Cisco ISE はそのエンドポイントに対して CoA をトリガーし、元の許可ポリシーを適用します。[侵害されたエンドポイント (Compromised Endpoints)] ページの [脅威と脆弱性のクリア (Clear Threat and Vulnerabilities)] オプションを使用して、(Cisco ISE システム データベースから) エンドポイントに関連付けられている脅威と脆弱性をクリアできます。

脅威ディクショナリには次の属性がリストされます。

- CTA-Course_Of_Action (値は Internal Blocking、Eradication、または Monitoring です。)

- Qualys-CVSS_Base_Score
- Qualys-CVSS_Temporal_Score
- Rapid7 Nexpose-CVSS_Base_Score
- Tenable Security Center-CVSS_Base_Score
- Tenable Security Center-CVSS_Temporal_Score

Base Score 属性と Temporal Score 属性の有効な範囲は 0 ~ 10 です。

脆弱性イベントがエンドポイントに受信されると、Cisco ISE はそのエンドポイントの CoA をトリガーします。ただし、脅威イベントの受信時には CoA はトリガーされません。

脆弱性属性を使用して、属性の値に基づいて脆弱なエンドポイントを自動的に隔離する許可ポリシーを作成できます。次に例を示します。

```
Any Identity Group & Threat:Qualys-CVSS_Base_Score > 7.0 -> Quarantine
```

脅威中心型 NAC サービスを有効にする際には、次の点に注意してください。

- 脅威中心型 NAC サービスを使用するには、Apex ライセンスが必要です。
- 脅威中心型 NAC サービスは、展開内の 1 つのノードでのみ有効にできます。
- 脆弱性アセスメント サービスでは、ベンダーあたり 1 つのアダプタ インスタンスだけを追加できます。ただし、FireAMP アダプタ インスタンスは複数追加できます。
- 設定を失わずにアダプタを停止、再開できます。アダプタの設定後は、任意の時点でアダプタを停止できます。ISE サービスの再起動時でもアダプタはこの状態のままになります。アダプタを再起動するには、アダプタを選択して [再起動 (Restart)] をクリックします。



(注) アダプタが [停止 (Stopped)] 状態の場合、アダプタ インスタンスの名前だけを編集できます。アダプタ設定や詳細設定は編集できません。

[脅威中心型 NAC ライブ ログ (Threat Centric NAC Live Logs)] ページ ([操作 (Operations)] > [TC NAC ライブ ログ (TC NAC Live Log)]) には、脅威イベントと脆弱性イベントがすべて表示されます。エンドポイントのインシデントタイプ、アダプタ名、一致する許可ルール、許可プロファイル (新しいプロファイルと古いプロファイル) が表示されます。また、イベントの詳細情報も確認できます。

エンドポイントの脅威情報は次に示すページで確認できます。

- [ホーム (Home)] ページ > [脅威 (Threat)] ダッシュボード
- [コンテキストの可視性 (Context Visibility)] > [エンドポイント (Endpoints)] > [侵害されたエンドポイント (Compromised Endpoints)]

脅威中心型 NAC サービスによりトリガーされるアラームを次に示します。

- **Adapter not reachable** (syslog ID : 91002) : アダプタに到達できないことを示します。
- **Adapter Connection Failed** (syslog ID : 91018) : アダプタに到達できるが、アダプタとソースサーバの間の接続がダウンしていることを示します。
- **Adapter Stopped Due to Error** (syslog ID : 91006) : このアラームは、アダプタが必要な状態になっていない場合にトリガーされます。このアラームが表示されたら、アダプタ設定とサーバ接続を調べてください。詳細については、アダプタ ログを参照してください。
- **Adapter Error** (syslog ID : 91009) : Qualys アダプタが Qualys サイトとの接続を確立できないか、またはこのサイトから情報をダウンロードできないことを示します。

脅威中心型 NAC サービスで利用できるレポートを次に示します。

- **アダプタのステータス** : アダプタのステータスレポートには、脅威と脆弱性のアダプタのステータスが表示されます。
- **COA イベント** : エンドポイントの脆弱性イベントを受信すると、Cisco ISE はそのエンドポイントについて CoA をトリガーします。CoA イベントレポートには、これらの CoA イベントのステータスが表示されます。また、これらのエンドポイントの新旧の認証ルールとプロファイルの詳細が表示されます。
- **脅威イベント** : 脅威イベント レポートには、設定したさまざまなアダプタから Cisco ISE が受信した脅威イベントがすべて表示されます。脆弱性アセスメントのイベントは、このレポートには含まれません。
- **脆弱性アセスメント** : 脆弱性アセスメントレポートには、エンドポイントで実行中のアセスメントに関する情報が示されます。このレポートを表示して、設定されたポリシーに基づいてアセスメントが行われているかどうかを確認することができます。

[操作 (Operations)] > [レポート (Reports)] > [診断 (Diagnostics)] > [ISE カウンタ (ISE Counters)] > [しきい値カウンタのトレンド (Threshold Counter Trends)] で、次の情報を確認できます。

- 受信したイベントの総数
- 脅威イベントの総数
- 脆弱性イベントの総数
- (PSN に対して) 発行された CoA の総数

これらの属性の値は 5 分おきに収集されるため、この値は直近 5 分間の数を表します。

[脅威 (Threat)] ダッシュボードには次のダッシュレットが表示されます。

- [侵害されたエンドポイントの総数 (Total Compromised Endpoints)] ダッシュレットには、ネットワーク上で現在影響を受けているエンドポイント (接続エンドポイントと切断エンドポイントの両方) の総数が表示されます。

- [特定期間における侵害されたエンドポイント (Compromised Endpoints Over Time)] ダッシュレットには、指定された期間におけるエンドポイントへの影響の履歴ビューが表示されます。
- [上位の脅威 (Top Threats)] ダッシュレットには、影響を受けるエンドポイントの数と脅威の重大度に基づく上位の脅威が表示されます。
- [脅威ウォッチリスト (Threats Watchlist)] ダッシュレットを使用して、選択したイベントのトレンドを分析できます。

[上位の脅威 (Top Threats)] ダッシュレットでは、バブルのサイズが影響を受けるエンドポイントの数を示し、薄い影が付いているエリアが切断されているエンドポイントの数を示します。色と縦方向の目盛りで脅威の重大度を示します。脅威には、インディケータとインシデントという2つのカテゴリがあります。インディケータの重大度属性は「Likely_Impact」、インシデントの重大度属性は「Impact_Qualification」です。

[侵害されたエンドポイント (Compromised Endpoint)] ページには、影響を受けるエンドポイントのマトリックスビューと、各脅威カテゴリの影響の重大度が示されます。エンドポイントの詳細な脅威情報を表示するには、デバイスリンクをクリックします。

[実行されたアクション (Course Of Action)] チャートには、CTA アダプタから受信した CTA-Course_Of_Action 属性に基づき、脅威インシデントに対して実行されたアクション ([内部ブロック (Internal Blocking)]、[撲滅 (Eradication)]、または[モニタリング (Monitoring)]) が表示されます。

[ホーム (Home)] ページの [脆弱性 (Vulnerability)] ダッシュボードには、次のダッシュレットが表示されます。

- [脆弱なエンドポイントの総数 (Total Vulnerable Endpoints)] ダッシュレットには、指定された値よりも大きい CVSS スコアを持つエンドポイントの総数が表示されます。また、CVSS スコアが指定された値よりも大きい接続エンドポイントと切断エンドポイントの総数も表示されます。
- [上位の脆弱性 (Top Vulnerability)] ダッシュレットには、影響を受けるエンドポイントの数または脆弱性の重大度に基づく上位の脅威が表示されます。[上位の脆弱性 (Top Vulnerability)] ダッシュレットでは、バブルのサイズが影響を受けるエンドポイントの数を示し、薄い影が付いているエリアが切断されているエンドポイントの数を示します。色と縦方向の目盛りで脆弱性の重大度を示します。
- [脆弱性ウォッチリスト (Vulnerability Watchlist)] ダッシュレットを使用して、一定期間にわたる選択した脆弱性のトレンドを分析できます。ダッシュレットで検索アイコンをクリックし、ベンダー固有の ID (Qualys の ID 番号の場合は「qid」) を入力して、その ID 番号の傾向を選択して表示します。
- [特定期間における脆弱なエンドポイント (Vulnerable Endpoints Over Time)] ダッシュレットには、一定期間におけるエンドポイントへの影響の履歴ビューが表示されます。

[脆弱なエンドポイント (Vulnerable Endpoints)] ページの [CVSS 別エンドポイント数 (Endpoint Count By CVSS)] グラフには、影響を受けるエンドポイントの数とその CVSS スコアが表示されます。[脆弱なエンドポイント (Vulnerable Endpoints)] ページでは、影響を受けるエンドポ

イントのリストも表示されます。各エンドポイントの詳細な脆弱性情報を表示するには、デバイス リンクをクリックします。

脅威中心型 NAC サービス ログはサポート バンドルに含まれています ([Cisco ISE ログ ファイルのダウンロード \(1086 ページ\)](#)) を参照)。脅威中心型 NAC サービス ログは support/logs/TC-NAC/ にあります。

脅威中心型 NAC サービスの有効化

脆弱性と脅威のアダプタを設定するには、まず脅威中心型 NAC サービスを有効にする必要があります。このサービスは、導入内の 1 つのポリシー サービス ノードでのみ有効にできます。

-
- ステップ 1** [管理 (Administration)] > [システム (System)] > [展開 (Deployment)] を選択します。
- ステップ 2** 脅威中心型 NAC サービスを有効にする PSN の隣にあるチェック ボックスにマークを付けて、[編集 (Edit)] をクリックします。
- ステップ 3** [脅威中心型 NAC サービスの有効化 (Enable Threat Centric NAC Service)] チェック ボックスにマークを付けます。
- ステップ 4** [保存 (Save)] をクリックします。
-

SourceFire FireAMP アダプタの追加

始める前に

- SourceFire FireAMP のアカウントが必要です。
- すべてのエンドポイントの FireAMP クライアントを導入する必要があります。
- 脅威中心型 NAC サービスを展開ノードで有効にする必要があります ([脅威中心型 NAC サービスの有効化 \(741 ページ\)](#)) を参照)。
- FireAMP アダプタは REST API コール (AMP クラウドへ)、およびイベントを受信する AMQP に SSL を使用します。また、プロキシの使用をサポートしています。FireAMP アダプタは通信にポート 443 を使用します。

-
- ステップ 1** [管理 (Administration)] > [脅威中心型 NAC (Threat Centric NAC)] > [サードパーティ ベンダー (Third Party Vendors)] を選択します。
- ステップ 2** [追加 (Add)] をクリックします。
- ステップ 3** [ベンダー (Vendor)] ドロップダウン リストから [AMP : 脅威 (AMP : Threat)] を選択します。
- ステップ 4** アダプタ インスタンスの名前を入力します。
- ステップ 5** [保存 (Save)] をクリックします。

- ステップ 6** ベンダー インスタンスのリスト ページを更新します。ベンダー インスタンスのリスト ページでアダプタのステータスが [設定準備完了 (Ready to Configure)] に変更された後でのみ、アダプタを設定できます。
- ステップ 7** [設定準備完了 (Ready to Configure)] リンクをクリックします。
- ステップ 8** (オプション) すべてのトラフィックをルーティングするように SOCKS プロキシ サーバを設定した場合、プロキシサーバのホスト名とポート番号を入力します。
- ステップ 9** 接続するクラウドを選択します。US クラウドまたは EU クラウドを選択できます。
- ステップ 10** サブスクライブするイベント ソースを選択します。次のオプションを使用できます。
- [AMP イベントのみ (AMP events only)]
 - [CTA イベントのみ (CTA events only)]
 - [CTA と AMP のイベント (CTA and AMP events)]
- ステップ 11** FireAMP リンクをクリックし、admin として FireAMP にログインします。[アプリケーション (Applications)] ペインの [許可 (Allow)] をクリックして、ストリーミング イベント エクスポート 要求を許可します。
Cisco ISE にリダイレクトします。
- ステップ 12** 監視するイベントを選択します (たとえば、不審なダウンロード、疑わしいドメインへの接続、実行されたマルウェア、Java 侵害)。
- 詳細設定の変更またはアダプタの再設定時に、AMPクラウドに新しいイベントが追加されている場合、これらのイベントも [イベント リスト (Events Listing)] ページに表示されます。
- アダプタ用のログ レベルを選択できます。選択可能なオプションは、[エラー (Error)]、[情報 (Info)]、[デバッグ (Debug)] です。
- アダプタ インスタンスの設定の要約が [設定サマリー (Configuration Summary)] ページに表示されます。

Cognitive Threat Analytics アダプタの追加

始める前に

- 脅威中心型 NAC サービスを展開ノードで有効にする必要があります (脅威中心型 NAC サービスの有効化 (741 ページ) を参照)。
- <http://cognitive.cisco.com/login> から Cisco Cognitive Threat Analytics (CTA) ポータルにログインし、CTA STIX/TAXII サービスを要求します。詳細については、『Cisco ScanCenter Administrator Guide』を参照してください。
- Cognitive Threat Analytics (CTA) アダプタは、SSL とともに TAXII プロトコルを使用して、CTAクラウドをポーリングし、検出された脅威を確認します。また、プロキシの使用をサポートしています。

- 信頼できる証明書ストアにアダプタ証明書をインポートします。[管理 (Administration)] > [システム (System)] > [証明書 (Certificates)] > [信頼できる証明書 (Trusted Certificates)] > [インポート (Import)] の順に選択し、証明書をインポートします。

-
- ステップ 1** [管理 (Administration)] > [脅威中心型 NAC (Threat Centric NAC)] > [サードパーティ ベンダー (Third Party Vendors)] を選択します。
- ステップ 2** [追加 (Add)] をクリックします。
- ステップ 3** [ベンダー (Vendor)] ドロップダウン リストから [CTA : 脅威 (CTA : Threat)] を選択します。
- ステップ 4** アダプタ インスタンスの名前を入力します。
- ステップ 5** [保存 (Save)] をクリックします。
- ステップ 6** ベンダー インスタンスのリスト ページを更新します。ベンダー インスタンスのリスト ページでアダプタのステータスが [設定準備完了 (Ready to Configure)] に変更された後でのみ、アダプタを設定できます。
- ステップ 7** [設定準備完了 (Ready to Configure)] リンクをクリックします。
- ステップ 8** 次の詳細を入力します。
- [CTA STIX/TAXII サービスの URL (CTA STIX/TAXII service URL)] : CTA クラウド サービスの URL。デフォルトでは URL <https://taxii.cloudsec.sco.cisco.com/skym-taxii-ws/PollService/> が使用されます。
 - [CTA フィード名 (CTA feed name)] : CTA クラウド サービスのフィード名を入力します。
 - [CTA ユーザ名とパスワード (CTA username and password)] : CTA クラウド サービスのユーザ名とパスワードを入力します。
 - [プロキシホストとポート (Proxy host and port)] (オプション) すべてのトラフィックをルーティングするようにプロキシサーバを設定した場合、プロキシサーバのホスト名とポート番号を入力します。
 - [ポーリング間隔 (Polling interval)] : 各ポーリング間の間隔です。デフォルト値は 30 分です。
 - [最初のポーリング期間 (時間数) (First Poll Duration in hours)] : 最初のポーリングで取得されるデータの経過時間。デフォルト値は 2 時間です。最大値は 12 時間です。
 - [インシデント タイプ (Incident Type)] : 次のオプションを使用できます。
 - [CTA イベントのみ (CTA events only)]
 - [AMP イベントのみ (AMP events only)]
 - [CTA と AMP のイベント (CTA and AMP events)]
- ステップ 9** [Next] をクリックします。
- ステップ 10** 次のオプションを設定するには、[詳細設定 (Advanced Settings)] をクリックします。
- [影響の指定 (Impact Qualification)] : ポーリングするインシデントの重大度レベルを選択します。次のオプションを使用できます。

- [1 - 影響なし (1 - Insignificant)]
- [2 - 妨害 (2 - Distracting)]
- [3 - 困難 (3 - Painful)]
- [4 - 損害発生 (4 - Damaging)]
- [5 - 壊滅的 (5 - Catastrophic)]

[3 - 困難 (3 - Painful)] を選択した場合、重大度レベルが [3 - 困難 (3 - Painful)] またはそれ以上 (この場合 [4 - 損害発生 (4 - Damaging)] と [5 - 壊滅的 (5 - Catastrophic)]) のインシデントがポーリングされます。

- [ロギング レベル (Logging Level)] : アダプタのログ レベルを選択します。選択可能なオプションは、[エラー (Error)]、[情報 (Info)]、[デバッグ (Debug)] です。

ステップ 11 [終了 (Finish)] をクリックします。



(注) CTA は Web プロキシ ログに IP アドレスまたはユーザ名としてリストされているユーザ ID を処理します。具体的には、IP アドレスの場合、プロキシ ログで使用可能なデバイスの IP アドレスが、内部ネットワークの別のデバイスの IP アドレスと競合する可能性があります。たとえば AnyConnect 経由で接続するローミング ユーザと、インターネットに直接接続するスプリットトンネルが獲得するローカル IP 範囲アドレス (例 : 10.0.0.X) が、内部ネットワークで使用されている重複するプライベート IP 範囲のアドレスと競合することがあります。不一致のデバイスに隔離アクションが適用されることを防ぐポリシーを定義するときには、論理ネットワーク アーキテクチャを考慮することが推奨されます。

CTA アダプタの許可プロファイルの設定

脅威イベントごとに、CTA アダプタは Course of Action 属性の値「Internal Blocking」、 「Monitoring」、または「Eradication」のいずれかを返します。これらの値に基づいて許可プロファイルを作成できます。

ステップ 1 [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [許可 (Authorization)] > [許可プロファイル (Authorization Profiles)] を選択します。

ステップ 2 [追加 (Add)] をクリックします。

ステップ 3 許可プロファイルの名前および説明を入力します。

ステップ 4 アクセス タイプを選択します。

ステップ 5 必要な詳細を入力し、[送信 (Submit)] をクリックします。

Course of Action 属性を使用した許可ポリシーの設定

脅威イベントが報告されたエンドポイントに対して許可ポリシーを設定するには、CTA-Course_Of_Action 属性を使用できます。この属性は [脅威 (Threat)] ディレクトリで使用できます。

また、CTA-Course_Of_Action 属性に基づいて例外ルールを作成することもできます。

ステップ 1 [ポリシー (Policy)] > [許可 (Authorization)] を選択します。

許可ポリシー ページが表示されます。脅威イベントが発生したエンドポイントについて、既存のポリシールールを編集するか、または新しい例外ルールを作成することができます。

ステップ 2 CTA-Course_Of_Action 属性値を検査するための条件を作成し、適切な許可プロファイルを割り当てます。次に例を示します。

Network_Access_Authentication_Passed AND ThreatCTA-Course_Of_Action CONTAINS Internal Blocking then blocking (authorization profile)

(注) 「Internal Blocking」はエンドポイントの隔離に使用することが推奨される Course of Action 属性です。

ステップ 3 [保存 (Save)] をクリックします。

エンドポイントの脅威イベントを受信すると、Cisco ISE は、そのエンドポイントに一致する許可ポリシーがあるかどうかを調べ、エンドポイントがアクティブな場合にのみ CoA をトリガーします。エンドポイントがオフラインの場合、脅威イベントの詳細が脅威イベントレポートに追加されます ([操作 (Operations)] > [レポート (Reports)] > [脅威中心型 NAC (Threat Centric NAC)] > [脅威イベント (Threat Events)])。



(注) CTA が 1 つのインシデントで複数のリスクとそれらに関連付けられている Course of Action 属性を送信することがあります。たとえば 1 つのインシデントで「Internal Blocking」と「Monitoring」(Course of Action 属性)を送信することがあります。この場合、「equals」演算子を使用してエンドポイントを隔離する許可ポリシーが設定されていると、エンドポイントは隔離されません。次に例を示します。

CTA-Course_Of_Action EQUALS Internal Blocking then Quarantine_Systems (authorization profile)

この場合、エンドポイントを隔離するには許可ポリシーで「contains」演算子を使用する必要があります。次に例を示します。

CTA-Course_Of_Action CONTAINS Internal Blocking then Quarantine_Systems

Cisco ISE での脆弱性アセスメントのサポート

Cisco Identity Services Engine は次の脆弱性アセスメント (VA) エコシステム パートナーと連携し、Cisco ISE ネットワークに接続するエンドポイントの脆弱性アセスメント結果を取得します。

- **Qualys** : Qualys は、ネットワークに導入されているスキャナアプライアンスを使用するクラウドベースの評価システムです。Cisco ISE では、Qualys と通信して VA 結果を取得するアダプタを設定できます。管理者ポータルからアダプタを設定できます。アダプタを設定するには、スーパー管理者権限を持つ Cisco ISE 管理者アカウントが必要です。Qualys アダプタは、Qualys クラウドサービスとの通信に REST API を使用します。REST API にアクセスするには、Qualys でマネージャ権限が付与されたユーザアカウントが必要です。Cisco ISE は次の Qualys REST API を使用します。

- **Host Detection List API** : エンドポイントの最新スキャン結果を確認します。
- **Scan API** : エンドポイントのオンデマンド スキャンをトリガーします。

Qualys により、サブスクリプション ユーザが実行できる API コールの数に制限が適用されます。デフォルトのレート制限カウントは、24 時間あたり 300 です。Cisco ISE は Qualys API バージョン 2.0 を使用して Qualys に接続します。これらの API 機能の詳細については、『Qualys API V2 User Guide』を参照してください。

- **Rapid7 Nexpose** : Cisco ISE は脆弱性管理ソリューションである Rapid 7 Nexpose と連携して、脆弱性の検出を促進します。これにより、このような脅威に迅速に対応できるようになります。Cisco ISE は Nexpose から脆弱性データを受信し、ISE で設定したポリシーに基づいて、影響を受けるエンドポイントを隔離します。Cisco ISE ダッシュボードから、影響を受けるエンドポイントを確認し、適切なアクションを実行できます。

Cisco ISE は Nexpose リリース 6.4.1 でテスト済みです。

- **Tenable Security Center (Nessus スキャナ)** : Cisco ISE は Tenable SecurityCenter と連携し、(Tenable SecurityCenter により管理される) Tenable Nessus スキャナから脆弱性データを受信します。また、ISE で設定したポリシーに基づいて、影響を受けるエンドポイントを隔離します。Cisco ISE ダッシュボードから、影響を受けるエンドポイントを確認し、適切なアクションを実行できます。

Cisco ISE は Tenable SecurityCenter 5.3.2 でテスト済みです。

エコシステム パートナーからの結果は Structured Threat Information Expression (STIX) 表現に変換され、この値に基づき、必要に応じて認可変更 (CoA) がトリガーされ、適切なアクセスレベルがエンドポイントに付与されます。

エンドポイントの脆弱性に関する評価にかかる時間は、さまざまな要因に基づいて異なるため、VA をリアルタイムで実行することはできません。エンドポイントの脆弱性に関する評価にかかる時間に影響する要因を次に示します。

- 脆弱性アセスメント エコシステム
- スキャン対象の脆弱性のタイプ

- 有効なスキャンのタイプ
- エコシステムによりスキナ アプライアンスに割り当てられるネットワーク リソースとシステム リソース

このリリースの Cisco ISE では、IPv4 アドレスを持つエンドポイントのみが脆弱性を評価できます。

脆弱性アセスメント サービスの有効化と設定

Cisco ISE で脆弱性アセスメント サービスを有効にして設定するには、次の作業を行います。

ステップ 1 [脅威中心型 NAC サービスの有効化（741 ページ）](#)。

ステップ 2 次の設定を行います。

- Qualys アダプタ ([Qualys アダプタの設定（747 ページ）](#) を参照)。
- Nexpose アダプタ ([Nexpose アダプタの設定（751 ページ）](#) を参照)。
- Tenable アダプタ ([Tenable アダプタの設定（754 ページ）](#) を参照)。

ステップ 3 [認可プロファイルの設定（758 ページ）](#)。

ステップ 4 [脆弱なエンドポイントを隔離する例外ルールの設定（759 ページ）](#)。

脅威中心型 NAC サービスの有効化

脆弱性と脅威のアダプタを設定するには、まず脅威中心型 NAC サービスを有効にする必要があります。このサービスは、導入内の 1 つのポリシーサービス ノードでのみ有効にできます。

ステップ 1 [管理 (Administration)] > [システム (System)] > [展開 (Deployment)] を選択します。

ステップ 2 脅威中心型 NAC サービスを有効にする PSN の隣にあるチェック ボックスにマークを付けて、[編集 (Edit)] をクリックします。

ステップ 3 [脅威中心型 NAC サービスの有効化 (Enable Threat Centric NAC Service)] チェック ボックスにマークを付けます。

ステップ 4 [保存 (Save)] をクリックします。

Qualys アダプタの設定

Cisco ISE は、Qualys 脆弱性アセスメント エコシステムをサポートしています。Cisco ISE 用の Qualys アダプタを作成して、Qualys と通信し、VA 結果を取得する必要があります。

始める前に

- 次のユーザ アカウントを準備する必要があります。

- ベンダー アダプタを設定できる、スーパー管理者権限を持つ Cisco ISE の管理者ユーザ アカウント。
- 管理者権限を持つ Qualys のユーザ アカウント
- 適切な Qualys ライセンス サブスクリプションがあることを確認します。Qualys レポート センター、ナレッジベース (KBX)、API にアクセスする必要があります。詳細については、Qualys アカウント マネージャにお問い合わせください。
- Cisco ISE の信頼できる証明書ストアに Qualys サーバ証明書をインポートします ([管理 (Administration)] > [証明書 (Certificates)] > [証明書の管理 (Certificate Management)] > [信頼できる証明書 (Trusted Certificates)] > [インポート (Import)])。適切なルートと中間証明書が、Cisco ISE の信頼できる証明書ストアにインポートされている (または存在する) ことを確認します。
- Qualys API ガイドの次の設定を参照してください。
 - Qualys で CVSS スコアが有効になっていることを確認します ([レポート (Reports)] > [設定 (Setup)] > [CVSS スコア (CVSS Scoring)] > [CVSS スコアの有効化 (Enable CVSS Scoring)])。
 - Qualys にエンドポイントの IP アドレスとサブネット マスクが追加されていることを確認します ([アセット (Assets)] > [ホスト アセット (Host Assets)])。
 - Qualys オプションプロファイルの名前があることを確認します。オプションプロファイルは、Qualys がスキャンのために使用するスキャナ テンプレートです。認証されたスキャンを含むオプションプロファイルを使用することを推奨します (このオプションは、エンドポイントの MAC アドレスも確認します)。
- HTTPS/SSL (ポート 443) を介して Qualys と通信する Cisco ISE。

-
- ステップ 1** [管理 (Administration)] > [脅威中心型 NAC (Threat Centric NAC)] > [サードパーティ ベンダー (Third Party Vendors)] の順に選択します。
- ステップ 2** [追加 (Add)] をクリックします。
- ステップ 3** [ベンダー (Vendor)] ドロップダウン リストから、[Qualys:VA] を選択します。
- ステップ 4** アダプタ インスタンスの名前を入力します。たとえば、Qualys_Instance などです。
設定されているアダプタ インスタンスのリストを含むリスト ページが表示されます。
- ステップ 5** ベンダー インスタンスのリスト ページを更新します。新しく追加された Qualys_Instance アダプタのステータスが、[設定準備完了 (Ready to Configure)] に変化します。
- ステップ 6** [設定準備完了 (Ready to Configure)] リンクをクリックします。
- ステップ 7** Qualys の設定画面で次の値を入力し、[次へ (Next)] をクリックします。

フィールド	説明
REST API ホスト (REST API Host)	Qualys クラウドをホストするサーバのホスト名です。この情報については、Qualys の担当者にお問い合わせください。
REST API ポート (REST API Port)	443
[ユーザ名 (Username)]	管理者権限を持つ Qualys のユーザ アカウントです。
[パスワード (Password)]	Qualys ユーザ アカウントのパスワードです。
HTTP プロキシ ホスト (HTTP Proxy Host)	すべてのインターネット トラフィックをルーティングするように設定されたプロキシ サーバがある場合は、プロキシ サーバのホスト名を入力します。
HTTP プロキシ ポート (HTTP Proxy Port)	プロキシ サーバが使用するポート番号を入力します。

Qualys サーバへの接続が確立されると、Qualys スキャナのリストを含む [スキャナ マッピング (Scanner Mappings)] ページが表示されます。ネットワークからの Qualys スキャナがこのページに表示されます。

ステップ 8 Cisco ISE がオンデマンド スキャンに使用するデフォルトのスキャナを選択します。

ステップ 9 [スキャナ マッピングに対する PSN (PSN to Scanner Mapping)] エリアで、PSN ノードに対して 1 つ以上の Qualys スキャナ アプライアンスを選択し、[次へ (Next)] をクリックします。

[詳細設定 (Advanced Settings)] ページが表示されます。

ステップ 10 [詳細設定 (Advanced Settings)] ページに次の値を入力します。このページの設定は、オンデマンド スキャンがトリガーされるかどうかや、最後のスキャン結果が VA に使用されるかどうかを決定します。

フィールド	説明
オプション プロ ファイル (Option Profile)	Qualys がエンドポイントのスキャンのために使用するオプション プロファイルを選択します。デフォルト オプション プロファイルである、[初期オプション (Initial Options)] を選択できます。
最後のスキャン結果 - チェック設定	

フィールド	説明
分単位の最後のスキャン結果のチェック間隔 (Last scan results check interval in minutes)	(ホスト検出リスト API のアクセス レートに影響します) 経過後に最後のスキャン結果を再度チェックする必要がある、分単位の時間間隔です。有効な範囲は 1 ～ 2880 です。
最後のスキャン結果がチェックされる前の最大結果数 (Maximum results before last scan results are checked)	(ホスト検出リスト API のアクセス レートに影響します) キューに登録されたスキャン要求の数がここで指定された最大数を超えた場合、[分単位の最後のスキャン結果のチェック間隔 (Last scan results check interval in minutes)] フィールドで指定された時間間隔の前に最後のスキャン結果がチェックされます。有効な範囲は 1 ～ 1000 です。
MAC アドレスの確認 (Verify MAC address)	[はい (True)] または [いいえ (False)] です。[はい (True)] に設定した場合、Qualys からの最後のスキャン結果はエンドポイントの MAC アドレスを含む場合にのみ使用されます。
スキャンの設定	
分単位のスキャントリガー間隔 (Scan trigger interval in minutes)	(スキャン API のアクセス レートに影響します) 経過後にオンデマンドスキャンがトリガーされる、分単位の時間間隔です。有効な範囲は 1 ～ 2880 です。
スキャンがトリガーされる前の最大要求数 (Maximum requests before scan is triggered)	(スキャン API のアクセス レートに影響します) キューに登録されたスキャン要求の数がここで指定された最大数を超えた場合、[分単位のスキャントリガー間隔 (Scan trigger interval in minutes)] フィールドで指定された時間間隔の前にオンデマンドスキャンがトリガーされます。有効な範囲は 1 ～ 1000 です。
分単位のスキャンステータスのチェック間隔 (Scan status check interval in minutes)	経過後に Cisco ISE が Qualys と通信してスキャンのステータスをチェックする、分単位の時間間隔です。有効な範囲は 1 ～ 60 です。

フィールド	説明
同時にトリガーできるスキャン数 (Number of scans that can be triggered concurrently)	(このオプションは、[スキャナ マッピング (Scanner Mappings)] 画面で各 PSN にマッピングされているスキャナの数に依存しています) 各スキャナは同時に 1 つの要求のみを処理できます。PSN に複数のスキャナをマッピングしている場合は、選択したスキャナの数に基づいてこの値を増やすことができます。有効な範囲は 1 ～ 200 です。
分単位のスキャンタイムアウト (Scan timeout in minutes)	経過後にスキャン要求がタイムアウトする、分単位の時間です。スキャン要求がタイムアウトすると、アラームが生成されます。有効な範囲は 20 ～ 1440 です。
スキャナごとの送信される IP アドレスの最大数 (Maximum number of IP addresses to be submitted per scanner)	処理のために Qualys に送信される単一の要求にキュー登録できる要求の数を示します。有効な範囲は 1 ～ 1000 です。
アダプタ ログファイル用のログレベルの選択 (Choose the log level for adapter log files)	アダプタ用のログ レベルを選択します。使用できるオプションは、[エラー (ERROR)]、[情報 (INFO)]、[デバッグ (DEBUG)]、[トレース (TRACE)] です。

ステップ 11 [次へ (Next)] をクリックして、構成設定を確認します。

ステップ 12 [終了 (Finish)] をクリックします。

Nexpose アダプタの設定

Cisco ISE 用の Nexpose アダプタを作成して、Nexpose と通信し、VA 結果を取得する必要があります。

始める前に

- Cisco ISE で脅威中心型 NAC サービスを有効にしていることを確認します。
- Nexpose Security Console にログインし、ユーザアカウントを作成して次の権限をこのアカウントに付与します。
 - サイトの管理

- レポートの作成

- Cisco ISE の信頼できる証明書ストアに Nexpose サーバ証明書をインポートします ([管理 (Administration)] > [証明書 (Certificates)] > [証明書の管理 (Certificate Management)] > [信頼できる証明書 (Trusted Certificates)] > [インポート (Import)])。適切なルートと中間証明書が、Cisco ISE の信頼できる証明書ストアにインポートされている (または存在する) ことを確認します。
- HTTPS/SSL (ポート 3780) を介して Nexpose と通信する Cisco ISE。

ステップ 1 [管理 (Administration)] > [脅威中心型 NAC (Threat Centric NAC)] > [サードパーティ ベンダー (Third Party Vendors)] の順に選択します。

ステップ 2 [追加 (Add)] をクリックします。

ステップ 3 [ベンダー (Vendor)] ドロップダウンリストから [Rapid7 Nexpose:VA] を選択します。

ステップ 4 アダプタ インスタンスの名前を入力します。たとえば Nexpose と入力します。

設定されているアダプタ インスタンスのリストを含むリスト ページが表示されます。

ステップ 5 ベンダー インスタンスのリスト ページを更新します。新しく追加された Nexpose アダプタのステータスが、[設定準備完了 (Ready to Configure)] に変化します。

ステップ 6 [設定準備完了 (Ready to Configure)] リンクをクリックします。

ステップ 7 Nexpose の設定画面で次の値を入力し、[次へ (Next)] をクリックします。

フィールド	説明
[Nexpose ホスト (Nexpose Host)]	Nexpose サーバのホスト名。
[Nexpose ポート (Nexpose Port)]	3780。
[ユーザ名 (Username)]	Nexpose 管理者ユーザ アカウント。
[パスワード (Password)]	Nexpose 管理者ユーザ アカウントのパスワード。
HTTP プロキシ ホスト (HTTP Proxy Host)	すべてのインターネット トラフィックをルーティングするように設定されたプロキシ サーバがある場合は、プロキシ サーバのホスト名を入力します。
HTTP プロキシ ポート (HTTP Proxy Port)	プロキシ サーバが使用するポート番号を入力します。

ステップ 8 [次へ (Next)] をクリックして拡張設定を設定します。

ステップ 9 [詳細設定 (Advanced Settings)] ページに次の値を入力します。このページの設定は、オンデマンド スキャンがトリガーされるかどうかや、最後のスキャン結果が VA に使用されるかどうかを決定します。

フィールド	説明
最新スキャン結果のチェックの設定	
[最新スキャン結果をチェックする間隔 (分単位) (Interval between checking the latest scan results in minutes)]	最新スキャン結果を再度確認するまでの時間間隔 (分単位)。有効な範囲は 1 ～ 2880 です。
[最新スキャン結果を確認するトリガーとなる保留要求数 (Number of pending requests that can trigger checking the latest scan results)]	[最新スキャン結果をチェックする間隔 (分単位) (Interval between checking the latest scan results in minutes)] フィールドに指定した期間が経過していない場合でも、キューに登録されたスキャン要求の数がここで指定する最大数を超えると、最新スキャン結果が確認されます。有効な範囲は 1 ～ 1000 です。
MAC アドレスの確認 (Verify MAC address)	[はい (True)] または [いいえ (False)] です。[はい (True)] に設定した場合、Nexpose からの最後のスキャン結果はエンドポイントの MAC アドレスを含む場合にのみ使用されます。
スキャンの設定	
[各サイトのスキャン トリガー 間隔 (分単位) (Scan trigger interval for each site in minutes)]	スキャンがトリガーされるまでの時間間隔 (分単位)。有効な範囲は 1 ～ 2880 です。
[各サイトのスキャンのトリガーとなる保留要求の数 (Number of pending requests before a scan is triggered for each site)]	キューに登録されたスキャン要求の数がここで指定された最大数を超えた場合、[スキャン トリガー 間隔 (分単位) (Scan trigger interval in minutes)] フィールドで指定された時間間隔が経過する前にスキャンがトリガーされます。有効な範囲は 1 ～ 1000 です。

フィールド	説明
最新スキャン結果のチェックの設定	
分単位のスキャン タイムアウト (Scan timeout in minutes)	経過後にスキャン要求がタイムアウトする、分単位の時間です。スキャン要求がタイムアウトすると、アラームが生成されます。有効な範囲は 20 ～ 1440 です。
[スキャンを同時に トリガーできる サイトの数 (Number of sites for which scans could be triggered concurrently)]	スキャンを同時に実行できるサイトの数。有効な範囲は 1 ～ 200 です。
タイムゾーン (Timezone)	Nexpose サーバで設定されているタイム ゾーンに基づいてタイム ゾーンを選択します。
[HTTP タイムアウト (秒単位) (Http timeout in seconds)]	Cisco ISE が Nexpose からの応答を待機する時間間隔。有効な範囲は 5 ～ 1200 です。
アダプタ ログ ファイル用のログ レベルの選択 (Choose the log level for adapter log files)	アダプタ用のログ レベルを選択します。使用できるオプションは、[エラー (ERROR)]、[情報 (INFO)]、[デバッグ (DEBUG)]、[トレース (TRACE)] です。

ステップ 10 [次へ (Next)] をクリックして、構成設定を確認します。

ステップ 11 [終了 (Finish)] をクリックします。

Tenable アダプタの設定

Cisco ISE が Tenable SecurityCenter (Nessus スキャナ) と通信し、VA 結果を取得するためには、Tenable アダプタを作成する必要があります。

始める前に



(注) Cisco ISE で Tenable Adapter を設定する前に、Tenable SecurityCenter で次の項目を設定する必要があります。これらの設定については、Tenable SecurityCenter のマニュアルを参照してください。

- Tenable Security Center と Tenable Nessus Vulnerability Scanner がインストールされている必要があります。Tenable Nessus スキャナの登録時に、[登録 (Registration)] フィールドで [SecurityCenter で管理 (Managed by SecurityCenter)] を必ず選択します。
- Tenable SecurityCenter で Security Manager 権限を持つユーザ アカウントを作成します。
- SecurityCenter でリポジトリを作成します (管理者クレデンシャルを使用して Tenable SecurityCenter にログインし、[リポジトリ (Repository)] > [追加 (Add)] を選択します)。
- リポジトリにスキャン対象のエンドポイント IP 範囲を追加します。
- Nessus スキャナを追加します。
- スキャン ゾーンを作成し、作成したスキャン ゾーンと、これらのスキャン ゾーンにマッピングされているスキャナに、IP アドレスを割り当てます。
- ISE のスキャン ポリシーを作成します。
- アクティブなスキャンを追加し、ISE スキャン ポリシーに関連付けます。設定項目、ターゲット (IP/DNS 名) を設定します。
- システム証明書とルート証明書を Tenable SecurityCenter からエクスポートし、Cisco ISE の信頼できる証明書ストアにインポートします ([管理 (Administration)] > [証明書 (Certificates)] > [証明書の管理 (Certificate Management)] > [信頼できる証明書 (Trusted Certificates)] > [インポート (Import)])。適切なルートと中間証明書が、Cisco ISE の信頼できる証明書ストアにインポートされている (または存在する) ことを確認します。
- HTTPS/SSL (ポート 443) を介して Tenable SecurityCenter と通信する Cisco ISE。

- ステップ 1** [管理 (Administration)] > [脅威中心型 NAC (Threat Centric NAC)] > [サードパーティ ベンダー (Third Party Vendors)] の順に選択します。
- ステップ 2** [追加 (Add)] をクリックします。
- ステップ 3** [ベンダー (Vendor)] ドロップダウン リストから、[Tenable Security Center:VA] を選択します。
- ステップ 4** アダプタ インスタンスの名前を入力します。たとえば、Tenable。
設定されているアダプタ インスタンスのリストを含むリスト ページが表示されます。
- ステップ 5** ベンダー インスタンスのリスト ページを更新します。新しく追加された Tenable アダプタのステータスが、[設定準備完了 (Ready to Configure)] に変化します。
- ステップ 6** [設定準備完了 (Ready to Configure)] リンクをクリックします。

ステップ 7 Tenable SecurityCenter の設定画面で次の値を入力し、[次へ (Next)] をクリックします。

フィールド	説明
[Tenable SecurityCenter ホスト (Tenable SecurityCenter Host)]	Tenable SecurityCenter のホスト名。
[Tenable SecurityCenter ポート (Tenable SecurityCenter Port)]	443
[ユーザ名 (Username)]	Tenable SecurityCenter でセキュリティ マネージャ 権限を持つユーザ アカウントのユーザ名。
[パスワード (Password)]	Tenable SecurityCenter でセキュリティ マネージャ 権限を持つユーザ アカウントのパスワード。
HTTP プロキシ ホスト (HTTP Proxy Host)	すべてのインターネット トラフィックをルーティングするように設定されたプロキシ サーバがある場合は、プロキシ サーバのホスト名を入力します。
HTTP プロキシ ポート (HTTP Proxy Port)	プロキシ サーバが使用するポート番号を入力します。

ステップ 8 [Next] をクリックします。

ステップ 9 [詳細設定 (Advanced Settings)] ページに次の値を入力します。このページの設定は、オンデマンド スキャンがトリガーされるかどうかや、最後のスキャン結果が VA に使用されるかどうかを決定します。

フィールド	説明
リポジトリ (Repository)	Tenable SecurityCenter で作成したリポジトリを選択します。
[スキャン ポリシー (Scan Policy)]	Tenable SecurityCenter で、ISE 用に作成したスキャン ポリシーを選択します。
最新スキャン結果のチェックの設定	

フィールド	説明
[最新スキャン結果をチェックする間隔（分単位） （Interval between checking the latest scan results in minutes）]	最新スキャン結果を再度確認するまでの時間間隔（分単位）。有効な範囲は1～2880です。
[最新スキャン結果を確認するトリガーとなる保留要求数（Number of pending requests that can trigger checking the latest scan results）]	[最新スキャン結果をチェックする間隔（分単位）（Interval between checking the latest scan results in minutes）] フィールドに指定した期間が経過していない場合でも、キューに登録されたスキャン要求の数がここで指定された最大数を超えた場合、最新スキャン結果が確認されます。有効な範囲は1～1000です。デフォルトは10です。
MAC アドレスの確認（Verify MAC address）	[はい（True）] または [いいえ（False）] です。[はい（True）] に設定した場合、Tenable SecurityCenter からの最新スキャン結果は、エンドポイントの MAC アドレスを含む場合にのみ使用されます。
スキャンの設定	
[各サイトのスキャン トリガー 間隔（分単位） （Scan trigger interval for each site in minutes）]	オンデマンド スキャンがトリガーされるまでの時間間隔（分単位）。有効な範囲は1～2880です。
[スキャンのトリガーとなる保留要求の数（Number of pending requests before a scan is triggered）]	キューに登録されたスキャン要求の数がここで指定された最大数を超えた場合、[スキャン トリガー 間隔（分単位）（Scan trigger interval in minutes）] フィールドで指定された時間間隔が経過する前にオンデマンド スキャンがトリガーされます。有効な範囲は1～1000です。
分単位のスキャン タイムアウト （Scan timeout in minutes）	経過後にスキャン要求がタイムアウトする期間（分単位）です。スキャン要求がタイムアウトすると、アラームが生成されます。有効な範囲は20～1440です。

フィールド	説明
[並列実行可能なスキャンの数 (Number of scans that could run in parallel)]	同時に実行できるスキャンの数。有効な範囲は 1 ～ 200 です。
[HTTP タイムアウト (秒単位) (Http timeout in seconds)]	Cisco ISE が Tenable SecurityCenter からの応答を待機する時間間隔。有効な範囲は 5 ～ 1200 です。
アダプタ ログ ファイル用のログ レベルの選択 (Choose the log level for adapter log files)	アダプタ用のログ レベルを選択します。使用できるオプションは、[エラー (ERROR)]、[情報 (INFO)]、[デバッグ (DEBUG)]、[トレース (TRACE)] です。

ステップ 10 [次へ (Next)] をクリックして、構成設定を確認します。

ステップ 11 [終了 (Finish)] をクリックします。

認可プロファイルの設定

Cisco ISE の許可プロファイルに、脆弱性がないかエンドポイントをスキャンするオプションが含まれるようになりました。スキャンの定期的な実行を選択できます。また、これらのスキャンの時間間隔を指定することもできます。許可プロファイルを定義した後、既存の認可ポリシー ルールに適用するか、または新しい認可ポリシー ルールを作成できます。

始める前に

脅威中心型 NAC サービスを有効にし、ベンダー アダプタを設定する必要があります。

ステップ 1 [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [認証 (Authorization)] > [許可プロファイル (Authorization Profiles)] を選択します。

ステップ 2 新規の許可プロファイルを作成するか、既存のプロファイルを編集します。詳細については、[新しい標準許可プロファイルの権限の設定 \(733 ページ\)](#) を参照してください。

ステップ 3 [共通タスク (Common Tasks)] 領域で、[脆弱性を評価する (Assess Vulnerabilities)] チェックボックスをオンにします。

ステップ 4 [アダプタ インスタンス (Adapter Instance)] ドロップダウン リストから、設定したベンダー アダプタを選択します。たとえば、Qualys_Instance などです。

ステップ 5 最後のスキャンからの時間がテキストボックスよりも大きい場合は、トリガースキャンのスキャン間隔を時間単位で入力します。有効な範囲は 1 ～ 9999 です。

ステップ 6 [上の間隔を使用して定期的に評価する (Assess periodically using above interval)] チェックボックスをオンにします。

ステップ 7 [送信 (Submit)] をクリックします。

脆弱なエンドポイントを隔離する例外ルールの設定

例外ルールを設定し、脆弱なエンドポイントへのアクセスを制限するには、次の脆弱性アセスメント属性を使用できます。

- Threat:Qualys-CVSS_Base_Score
- Threat:Qualys-CVSS_Temporal_Score
- Rapid7 Nexpose-CVSS_Base_Score
- Tenable Security Center-CVSS_Base_Score
- Tenable Security Center-CVSS_Temporal_Score

これらの属性は [脅威 (Threat)] ディレクトリで使用できます。有効な値の範囲は 0 ～ 10 です。

エンドポイントの隔離、アクセスの制限 (別のポータルへのリダイレクト) 、または要求の拒否のいずれかを選択できます。

ステップ 1 [ポリシー (Policy)] > [承認 (Authorization)] を選択します。

許可ポリシー ページが表示されます。既存のポリシー ルールを編集するか、または VA 属性のチェックについて新しい例外ルールを作成します。

ステップ 2 Qualys スコアを確認して適切な許可プロファイルを割り当てるための条件を作成します。次に例を示します。

Any Identity Group & Threat:Qualys-CVSS_Base_Score > 5 -> Quarantine (authorization profile)

ステップ 3 [保存 (Save)] をクリックします。

脆弱性アセスメント ログ

Cisco ISE には、VA サービスのトラブルシューティングのための次のログがあります。

- **vaservice.log** : VA コア情報が含まれており、TC-NAC サービスを実行しているノードで使用可能です。
- **varuntime.log** : エンドポイントと VA フローに関する情報が含まれており、モニタリング ノードと、TC-NAC サービスを実行しているノードで使用可能です。
- **vaaggregation.log** : 1 時間ごとに収集されるエンドポイントの脆弱性に関する情報が含まれており、プライマリ管理ノードで使用可能です。



第 23 章

スマートライセンスサービスおよび Smart Call Home サービスの設定

- [Cisco ISE スマート ライセンス \(761 ページ\)](#)
- [Smart Call Home \(766 ページ\)](#)

Cisco ISE スマート ライセンス

シスコは、別々のライセンスを個別にインポートするのではなく、単一のトークン登録で ISE ソフトウェア ライセンスとエンドポイント ライセンスの消費を簡単かつ効率的にモニタできるようにする、スマートライセンスを提供しています。購入したシスコ製品とライセンスの詳細は Cisco Smart Software Manager (CSSM) と呼ばれる集中型データベースに保持され、ここからどのエンドポイント ライセンスが使用できるかと、消費の統計情報を簡単に追跡できます。

スマートライセンス トークンが ISE からアクティベートされ登録されている場合、製品ライセンスごとの各エンドポイントセッションによるライセンスの消費をモニタします。スマートライセンスは、ISE のシンプルな表レイアウトからエンドポイントセッションによるライセンスの消費について管理者に通知します。スマートライセンスは、有効な各ライセンスのピーク使用量を集中型データベースに毎日レポートします。ライセンスが使用できる状態で消費されていない場合、使用可能なライセンスについて管理者に通知され、使用量のモニタを継続できます。消費量が使用可能なライセンスの数を超えると、アラームが起動し、アラームと通知によって管理者に通知されます。

スマートライセンスでは、Base、Plus、Apex、TACACS などの、シスコのスマートアカウントを介して含まれているさまざまなライセンス権限を管理することもできます。ISE から、ライセンス権限ごとの基本的な消費統計情報をモニタできます。CSSM アカウントから、追加情報、統計情報、通知を表示することや、アカウントおよび権限に変更を加えることができます。



(注) Cisco スマート ソフトウェア マネージャ サテライトはサポートされていません。

ISE はライセンス消費の内部サンプルを 30 分ごとに取得し、コンプライアンスと消費がそれに
 応じて更新されます。[更新 (Refresh)] をクリックするだけで ISE の [ライセンス (Licenses)]
 テーブルにこの情報が表示されます。毎日午前 1:00 に、ISE は [ライセンス (Licenses)] テー
 ブルに同様に表示される [昨日のピーク数 (Yesterday's Peak Count)] データに基づき、有効な
 各ライセンスについて日々のピーク数を CSSM サーバにレポートします。ISE は、毎日の同期
 中に自動的に再承認される CSSM 証明書のローカル コピーを保存することで CSSM サーバと
 通信し、ユーザが [ライセンス (Licenses)] テーブルを手動で更新したときにも通信します。
 通常、証明書の有効期間は 6 ヶ月です。CSSM サーバと同期したときにコンプライアンスが変
 更された場合、[ライセンス (Licenses)] テーブルの [最後の認証 (Last Authorization)] 列がそ
 れに応じて更新されます。また、権限がコンプライアンスを満たさなくなった場合には、コン
 プライアンス外となっている日数が [コンプライアンス外の日数 (Days Out of Compliancy)] 列
 に表示されます。コンプライアンス違反は、[ライセンス (Licensing)] エリアの上部にある
 [通知 (Notifications)] と、[ライセンス警告 (License Warning)] リンクにある ISE ツールバー
 にも示されます。通知に加えて、アラームも確認できます。詳細については、[Cisco ISE アラーム \(1042 ページ\)](#) を参照してください。



(注) TACACS ライセンスは ISE が CSSM サーバと通信したときに承認されますが、セッションベ
 ースではないため、[ライセンス (Licenses)] テーブルで消費数は関連付けられません。

図 48: [ライセンス (Licenses)] テーブル

License	Status	Compliance	Yesterday's Peak Count	Consumption Count*	Days Out of Compliancy	Last Authorization
Base	Enabled	Released Entitlement	0	0	-	-
Plus	Enabled	Released Entitlement	0	0	-	-
Apex	Enabled	Released Entitlement	0	0	-	-
Tacacs	Enabled	In Compliance	Uncounted	Uncounted	-	May 19, 2016 5:25:55 PM

*Consumption Count Updated: May 19, 2016 17:00:00 IST

ISE でのスマート ライセンスの有効化および登録

始める前に

スマート ライセンスを有効化してから、CSSM アカウントを介してシスコ担当者によって発行
 されたトークンを使用して ISE から登録します。

Cisco Smart Software Manager (CSSM) アカウントで必要な ISE の権限があることを確認しま
 す。詳細については、<https://software.cisco.com/> を参照するか、シスコ担当者にお問い合わせく
 ださい。

ISE-PIC からアップグレードする場合は、この手順でスマート ライセンスを有効化する前に、
 まず ISE アップグレードライセンスをインストールしてから次の作業を行う必要があります。

- ISE Base ライセンスをインストールする。
- または、既存の ISE 展開に PIC インストールを移動する。
 1. 既存の ISE 展開から、ISE ノードを追加します。

2. 既存の ISE 管理ノードからセッションプロファイリングと pxGrid サービスを有効にします。



(注) ISE ノードの追加と設定の詳細については、[Cisco ISE ノードの設定 \(60 ページ\)](#) を参照してください。

ステップ 1 [管理 (Administration)] > [システム (System)] > [ライセンス (Licensing)] の順に選択して、ISE の [ライセンス (Licensing)] エリアにアクセスします。

ISE ボックスをインストールまたはアップグレードした後、スマート ライセンスを有効化する前に、ISE の [ライセンス (Licensing)] エリアに入ると、デフォルトで従来のライセンスが使用され、[ライセンス方式 (Licensing Method)] エリアの画面上部に表示されます。

図 49: 従来のライセンス

Licensing Method ⓘ

✓ **Traditional Licensing** is currently in use.

Click below to switch to **Cisco Smart Licensing** ⓘ

▶ **Cisco Smart Licensing**

ステップ 2 [ライセンス方式 (Licensing Method)] エリアの [Cisco Smart Licensing] リンクをクリックして [スマート ライセンス (Smart Licensing)] に切り替えます。

接続方式フィールドを持つ [Cisco Smart Licening] エリアが展開します。

図 50: スマート ライセンスの接続方式の詳細

Specify the method to use to connect to Cisco Smart Software Manager and then click Enable to get Started.

Connection Method

Optional Secondary administration node for high availability.

Secondary UDI

ⓘ Cisco cloud server information

Enable

Cancel

ステップ 3 [Cisco Smart Licensing] エリアの [セカンダリ UDI (Secondary UDI)] フィールドで、少なくとも 1 つの追加 ISE ボックスがネットワークで設定されている場合は、プライマリ ノードが使用できない場合に使用されるセカンダリ ノードを入力します。ISE ボックスから CSSM に接続するために使用される接続方式を [接

続方式 (Connection Method)] ドロップダウンリストから選択し、[有効化 (Enable)] をクリックします。
[接続方式 (Connection Method)] については、次のように選択します。

- a) インターネットに到達するために設定された直接接続がある場合には、[直接HTTPS (DirectHTTPS)] を選択します。
- b) 直接接続がなく、プロキシ経由で接続する必要がある場合には、[HTTPS プロキシ (HTTPS Proxy)] を選択します。
- c) [トランスポートゲートウェイ (Transport Gateway)] は、推奨される接続方式です。スマートライセンスを使用する場合、Smart Call Home (SCH) サービスも自動的に有効になり、Transport Gateway を設定できるようになります。接続方式として Transport Gateway を設定するには、まず管理ワーク センターの Smart Call Home 設定から設定する必要があります。これを行う方法と SCH および Transport Gateway に関する詳細については、[Smart Call Home \(766 ページ\)](#) を参照してください。

(注) スマートライセンスを有効にすると、すべてのライセンスが有効になる、90 日間の評価期間になります。この間に、スマートライセンスとすべての ISE 機能を試すことができます。ISE の使用を継続するには、次の手順に進んで評価期間が終了する前に有効なトークンを使用してスマートライセンスに登録する必要があります。

このエリアのフィールドはダイナミックです。接続の詳細を入力し、[有効化 (Enable)] をクリックすると、エリアが折りたたまれます。エリアを再度展開すると、今度は [Cisco Smart Licensing の登録 (Cisco Smart Licensing Registration)] が呼び出され、スマートライセンス トークンの詳細を入力することができます。

ステップ 4 ISE の [Cisco Smart Licensing の登録 (Cisco Smart Licensing Registration)] エリアから、スマートライセンス トークンを購入したときに受け取った [登録トークン (Registration Token)] を入力し、[登録 (Register)] をクリックします。CSSM アカountの ISE エリアに移動して [コピー (Copy)] をクリックすることで、いつでもトークンを取得できます。

また、チェックマークを外すことで、スマートライセンス トークンに含まれている任意のライセンスを無効にすることができます。ライセンスを無効にすると、スマートライセンス機能の一部として自動的に有効性がチェックされなくなります。

ISE のスマート ライセンスの管理

スマートライセンス トークンをアクティブ化して登録すると、ISE のライセンス権限を次の方法で管理することができます。

- ライセンス権限資格証明書の有効化、無効化、および更新。
- スマート ライセンスの登録の更新。
- 準拠および非準拠ライセンスの問題の特定。

始める前に

スマート ライセンス トークンをアクティブ化して登録していることを確認します。詳細については、[ISE でのスマート ライセンスの有効化および登録 \(762 ページ\)](#) を参照してください。

- ステップ 1** スマートライセンスを最初に起動すると、すべてのライセンス権限は評価期間の一部として自動的に有効になります。トークンを登録すると、CSSM アカウントに特定の権限が含まれず、登録時にそれらを無効にしていなかった場合は、非準拠通知が ISE に表示されます。それらの権限を CSSM アカウントに追加し（サポートが必要な場合は、Cisco アカウント担当者にお問い合わせください）、[ライセンス (Licenses)] テーブルから [更新 (Refresh)] をクリックし、非準拠通知を削除して、関連機能を使い続けます。承認を更新したら、ログアウトして、関連する削除する非準拠メッセージのために ISE に再度ログインします。
- ステップ 2** 毎日の自動承認が何らかの理由で成功しないと、非準拠メッセージが表示されることがあります。[更新 (Refresh)] をクリックして権限を再承認します。承認を更新したら、ログアウトして、関連する削除する非準拠メッセージのために ISE に再度ログインします。
- ステップ 3** スマートライセンスを最初に起動すると、すべてのライセンス権限は評価期間の一部として自動的に有効になります。トークンを登録すると、CSSM アカウントに特定の権限が含まれず、登録時にそれらを無効にしていなかった場合は、不必要な非準拠通知を回避するために、ISE のスマート ライセンスからそれらの権限を無効のままにすることができます。[ライセンス (Licenses)] テーブルから、トークンに含まれていないライセンス権限にチェックマークを付け、ツールバーから [無効 (Disabled)] をクリックします。ライセンス権限を無効にした後、ログアウトし、メニューから削除する関連機能および削除する非準拠メッセージのために ISE に再度ログインします。
- ステップ 4** アカウントに権限を追加したら、それらの権限を有効にします。[ライセンス (Licenses)] テーブルから、必要な無効化されたライセンスにチェックマークを付け、ツールバーから [有効 (Enable)] をクリックします。
- ステップ 5** まず 1 UDI だけのスマートライセンスを設定し、セカンダリ UDI を入力しない場合、後で情報を更新できます。[Cisco スマート ライセンス登録の詳細 (Cisco Smart Licensing Registration Details)] リンクをクリックして、エリアを開きます。トークンを再入力し、新しいセカンダリ UDI を入力して、[更新 (Update)] をクリックします。
- ステップ 6** 登録証明書は自動的に 6 ヶ月ごとに更新されます。手動でスマート ライセンス証明書登録を更新するには、[Cisco Smart Licensing] 領域の上部から [登録の更新 (Renew Registration)] をクリックします。
- ステップ 7** ISE ボックス登録 (UDI により示されます) をスマート アカウントから削除するが、評価期間の終了までスマートライセンスを引き続き使用するには、[Cisco Smart Licensing] 領域の上部から [登録解除 (Deregister)] をクリックします。たとえば、登録プロセスの一環として示した UDI を変更する必要がある場合に、これを行うことができます。まだ評価期間の残りの時間があれば、ISE はスマート ライセンスのままです。評価期間の残りの時間がない場合、ブラウザが更新されたときに通知が表示されます。登録解除したら、同一または別の UDI で登録するために登録プロセスを再度実行できます。スマートライセンスをアクティブにし、登録する方法の詳細については、[ISE でのスマート ライセンスの有効化および登録 \(762 ページ\)](#) を参照してください。
- ステップ 8** ISE ボックス登録 (UDI により示されます) をスマート アカウントから完全に削除し、従来のライセンスに戻すには、[Cisco Smart Licensing] 領域の上部から [無効 (Disabled)] をクリックします。たとえば、登録プロセスの一環として示した UDI を変更する必要がある場合に、これを行うことができます。無効にしたら、同一または別の UDI でアクティブ化および登録するために登録プロセスを再度実行できます。スマートライセンスをアクティブにし、登録する方法の詳細については、[ISE でのスマート ライセンスの有効化および登録 \(762 ページ\)](#) を参照してください。

Smart Call Home

Smart Call Home (SCH) 機能は、Smart Call Home ポータルで設定されている場合、ネットワーク内の Cisco ISE デバイスを監視し、重大なイベントに関して電子メールで知らせます。また、検出した問題への修復アドバイスを含むリアルタイムのアラートを提供します。SCH は環境の問題を監視し、イベント通知を送信します。

Cisco ISE のスマート ライセンスをアクティブにすると、SCH の機能はデフォルトで有効になります。それ以外の場合で、SCH を有効にするには、SCH サービス用に Cisco ISE を登録する必要があります。SCH 機能を有効にする方法の詳細については、[Smart Call Home サービスの登録 \(767 ページ\)](#) を参照してください。スマートライセンスを有効にするか、SCH サービスを登録すると、次のいずれかを選択することができます。

- 匿名レポートのみを有効にします。SCH の匿名レポート機能は、ネットワーク内の Cisco ISE デバイスの最小限の状態に関する情報を提供します。
- SCH が提供するすべての機能セットを有効にします。

SCH 機能の有効化については、[Smart Call Home サービスの登録 \(767 ページ\)](#) を参照してください。

Cisco ISE は、サテライトまたは Transport Gateway をサポートしています。組織のセキュリティポリシーがネットワークの ISE サーバと SCH サーバ間の通信を許可しない場合、SCH 通信のプロキシとして機能するオプションの Transport Gateway を使用できます。Transport Gateway ソフトウェアは Cisco.com からダウンロードでき、Linux サーバにインストールして維持することができます。RHEL サーバでの Transport Gateway ソフトウェアの導入方法については、『[Smart Call Home Deployment Guide](#)』を参照してください。

Smart Call Home プロファイル

Smart Call Home プロファイルは、デバイスでモニタされるイベントのタイプを決定します。Cisco ISE には、次のデフォルト プロファイルがあります。

- ciscotac-1 : 匿名レポートのために使用されます
- isesch-1 : Smart Call Home 機能のために使用されます

匿名レポートのために使用されるデフォルト プロファイル (ciscotac-1) を編集することはできません。

Anonymous Reporting

Cisco ISE は、ユーザの展開、ネットワーク アクセス デバイス、プロファイラ、およびその他に使用しているサービスに関する非機密情報を安全に収集します。このデータは、Cisco ISE の使用状況をより詳しく把握し、製品と製品が提供するさまざまなサービスを向上させる目的で収集されます。

デフォルトでは、anonymous reporting は有効になっています。anonymous reporting を使用不可にするには、ISE 管理者ポータル ([管理 (Administration)] > [システム (System)] > [設定 (Settings)] > [Smart Call Home]) で行うことができます。

Smart Call Home サービスの登録



(注) Cisco ISE のスマート ライセンスを有効にしている場合、Smart Call Home (SCH) サービスに登録する必要はありません。スマート ライセンスにより、SCH 機能はデフォルトで有効になっています。[Smart Call Home] ページの登録ステータスはアクティブになっています。匿名レポートのみを有効にすることや、SCH が提供する機能一式を有効にすることができます。

スマート ライセンスを使用せずに SCH サービスを有効にするには、まず SCH サービス用に Cisco ISE を登録する必要があります。これは、スタンドアロン ノードまたはプライマリ管理 ノードからのみ行うことができます。

ステップ 1 [管理 (Administration)] > [システム (System)] > [設定 (Settings)] > [Smart Call Home] の順に選択します。

ステップ 2 次のいずれかを実行します。

- SCH のすべての機能をオンにする (Turn on full SCH capability)
- デフォルト SCH テレメトリ設定を保持して匿名データのみを送信する (Keep the default SCH telemetry settings and send only anonymous data)
- すべて無効にする (Disable everything)

ステップ 3 ([SCH のすべての機能をオンにする (Turn on full SCH capability)] オプションを選択した場合のみ) [登録ステータス (Registration Status)] エリアに電子メールアドレスを入力します。

ステップ 4 (オプション) [Transport Gateway] チェックボックスをオンにして、Transport Gateway の URL を入力します。

ステップ 5 [保存 (Save)] をクリックします。

SCH のすべての機能を有効にしている場合は、アクティベーションリンクが記載された電子メールを受信します。アクティベーションリンクをクリックして記載されている指示に従い、登録を完了します。



第 24 章

Cisco ISE エンドポイント プロファイリング ポリシー

- [Cisco ISE プロファイリング サービス \(770 ページ\)](#)
- [Cisco ISE ノードでのプロファイリング サービスの設定 \(772 ページ\)](#)
- [プロファイリング サービスによって使用されるネットワーク プローブ \(773 ページ\)](#)
- [Cisco ISE ノードごとのプローブの設定 \(784 ページ\)](#)
- [CoA、SNMP RO コミュニティおよびエンドポイント属性フィルタの設定 \(784 ページ\)](#)
- [ISE データベースの持続性とパフォーマンスの属性フィルタ \(788 ページ\)](#)
- [IOS センサー組み込みスイッチからの属性の収集 \(791 ページ\)](#)
- [プロファイラ条件 \(793 ページ\)](#)
- [Cisco NAC アプライアンスとの Cisco ISE 統合 \(794 ページ\)](#)
- [プロファイラ条件の作成 \(796 ページ\)](#)
- [エンドポイント プロファイリング ポリシー ルール \(796 ページ\)](#)
- [エンドポイント プロファイリング ポリシーの作成 \(797 ページ\)](#)
- [事前定義されたエンドポイント プロファイリング ポリシー \(801 ページ\)](#)
- [エンドポイント プロファイリング ポリシーの論理プロファイルによるグループ化 \(805 ページ\)](#)
- [プロファイリング例外アクション \(806 ページ\)](#)
- [ポリシーおよび ID グループのスタティック割り当てによるエンドポイントの作成 \(807 ページ\)](#)
- [識別されたエンドポイント \(813 ページ\)](#)
- [プロファイラ レポート \(823 ページ\)](#)
- [エンドポイントの異常な動作の検出 \(824 ページ\)](#)
- [プロファイラ フィード サービス \(826 ページ\)](#)
- [プロファイラ レポート \(831 ページ\)](#)
- [エンドポイントの異常な動作の検出 \(832 ページ\)](#)
- [Cisco NAC アプライアンスとの Cisco ISE 統合 \(834 ページ\)](#)
- [ポリシーおよび ID グループのスタティック割り当てによるエンドポイントの作成 \(836 ページ\)](#)
- [識別されたエンドポイント \(842 ページ\)](#)

- [プロファイラ レポート \(852 ページ\)](#)
- [エンドポイントの異常な動作の検出 \(853 ページ\)](#)

Cisco ISE プロファイリング サービス

Cisco Identity Services Engine (ISE) のプロファイリングサービスは、ネットワークに接続されているデバイスおよびその場所を識別します。エンドポイントは Cisco ISE に設定されたエンドポイント プロファイリング ポリシーに基づいてプロファイリングされます。次に、Cisco ISE では、ポリシー評価の結果に基づいてネットワークのリソースにアクセスする権限がエンドポイントに付与されます。

プロファイリング サービス：

- IEEE 規格 802.1X ポートベースの認証アクセスコントロール、MAC 認証バイパス (MAB) 認証、およびネットワーク アドミッション コントロール (NAC) をさまざまな規模および複雑度の企業ネットワークに使用して、認証の効率的かつ効果的な展開および継続的な管理を容易にします。
- デバイス タイプにかかわらず、接続されたすべてのネットワーク エンドポイントの機能を特定、検索、および決定します。
- 一部のエンドポイントへのアクセスを誤って拒否しないようにします。

[ISE Community Resource](#)

[ISE Endpoint Profiles](#)

[How To: ISE Profiling Design Guide](#)

プロファイラ ワーク センター

[プロファイラ ワーク センター (Profiler Work Center)] メニュー ([ワーク センター (Work Centers)] > [プロファイラ (Profiler)]) には、すべてのプロファイラ ページが含まれ、ISE の管理者向けの単一の窓口として機能します。[プロファイラ ワーク センター (Profiler Work Center)] メニューには次のオプションがあります：[概要 (Overview)]、[外部 ID ストア (Ext ID Stores)]、[ネットワーク デバイス (Network Devices)]、[エンドポイント分類 (Endpoint Classification)]、[ノード設定 (Node Config)]、[フィード (Feeds)]、[手動スキャン (Manual Scans)]、[ポリシー要素 (ポリシーの要素)]、[プロファイリング ポリシー (Profiling Policies)]、[許可ポリシー (Authorization Policy)]、[トラブルシューティング (Troubleshoot)]、[レポート (Reports)]、[設定 (Settings)] および [ディクショナリ (Dictionaries)]。

[プロファイラ (Profiler)] ダッシュボード

[プロファイラ (Profiler)] ダッシュボード ([ワーク センター (Work Centers)] > [プロファイラ (Profiler)] > [エンドポイント分類 (Endpoint Classification)]) は、ネットワーク内のプロファイル、エンドポイント、アセットの集中型モニタリングツールです。このダッシュボード

には、グラフと表の形式でデータが表示されます。[プロファイル (Profiles)] ダッシュレットには、ネットワークで現在アクティブな論理プロファイルとエンドポイントプロファイルが表示されます。[エンドポイント (Endpoints)] ダッシュレットには、ネットワークに接続するエンドポイントの ID グループ、PSN、OS タイプが表示されます。[アセット (Assets)] ダッシュレットには、ゲスト、BYOD、企業などのフローが表示されます。表には接続されたさまざまなエンドポイントが表示され、新しいエンドポイントを追加することもできます。

プロファイリングサービスを使用したエンドポイントインベントリ

プロファイリングサービスを使用して、ネットワークに接続されたすべてのエンドポイントの機能を検出、特定、および決定することができます。デバイスのタイプに関係なく、エンドポイントの企業ネットワークへの適切なアクセスを、保障し、保持できます。

プロファイリングサービスでは、エンドポイントの属性をネットワークデバイスとネットワークから収集し、エンドポイントをそのプロファイルに従って特定のグループに分類します。一致したプロファイルを持つエンドポイントが Cisco ISE データベースに保存されます。プロファイリングサービスで処理されるすべての属性は、プロファイラ ディクショナリに定義されている必要があります。

プロファイリングサービスは、ネットワークの各エンドポイントを識別し、そのプロファイルに従ってシステム内の既存のエンドポイントの ID グループ、またはシステム内で作成できる新しいグループにそれらのエンドポイントをグループ化します。エンドポイントをグループ化して既存の ID グループにエンドポイントプロファイリングポリシーを適用することで、エンドポイントと対応するエンドポイントプロファイリングポリシーのマッピングを決定できます。

Cisco ISE プロファイラ キュー制限の設定

Cisco ISE プロファイラは、ネットワークから大量のエンドポイントデータを短時間で収集します。それにより、一部の遅い Cisco ISE コンポーネントがプロファイラによって生成されるデータを処理するときにバックログが蓄積されるため、Java 仮想マシン (JVM) のメモリ使用率が増大し、パフォーマンスの低下および安定性の問題が生じます。

プロファイラが JVM メモリ使用率を増やさず、また、JVM がメモリ不足になり、再起動しないように、プロファイラの次の内部コンポーネントに制限が適用されます。

- エンドポイントキャッシュ：内部キャッシュのサイズは制限され、サイズが制限を超えると定期的に消去する必要があります（最長時間未使用方式に基づく）。
- フォワーダ：プロファイラによって収集されたエンドポイント情報のメイン入力キュー。
- イベント ハンドラ：高速コンポーネントを接続解除する内部キューで、（通常、データベース クエリーに関連する）低速処理コンポーネントにデータを提供します。

エンドポイントキャッシュ

- maxEndpointsInLocalDb = 100000（キャッシュ内のエンドポイント オブジェクト）

- `endPointsPurgeIntervalSec = 300` (秒単位のエンドポイント キャッシュ消去スレッド間隔)
- `numberOfProfilingThreads = 8` (スレッド数)

制限は、すべてのプロファイラ内部イベント ハンドラに適用されます。キュー サイズ制限に達すると、モニタリング アラームがトリガーされます。

Cisco ISE プロファイラのキュー サイズの制限

- `forwarderQueueSize = 5000` (エンドポイント収集イベント)
- `eventHandlerQueueSize = 10000` (イベント)

イベント ハンドラ

- `NetworkDeviceEventHandler` : すでにキャッシュされているネットワーク アクセス デバイス (NAD) の重複 IP アドレスのフィルタリングのほか、ネットワーク デバイスのイベント用。
- `ARPCacheEventHandler` : ARP キャッシュのイベント用。

Cisco ISE ノードでのプロファイリング サービスの設定

Cisco ISE 対応のネットワークでネットワーク リソースを使用しているすべてのエンドポイントのコンテキスト インベントリを提供するプロファイリング サービスを設定できます。

デフォルトですべての管理、モニタリング、およびポリシー サービスのペルソナを担当する単一の Cisco ISE ノードで実行されるようにプロファイリング サービスを設定できます。

分散展開では、プロファイリング サービスは、ポリシー サービス ペルソナを担当する Cisco ISE ノードでのみ実行され、管理ペルソナとモニタリング ペルソナを担当する他の Cisco ISE ノードでは実行されません。

ステップ 1 [管理 (Administration)] > [システム (System)] > [展開 (Deployment)] を選択します。

ステップ 2 ポリシー サービス ペルソナを担当する Cisco ISE ノードを選択します。

ステップ 3 [展開ノード (Deployment Nodes)] ページで [編集 (Edit)] をクリックします。

ステップ 4 [全般設定 (General Settings)] タブで [ポリシー サービス (Policy Service)] チェックボックスをオンにします。[ポリシー サービス (Policy Service)] チェックボックスがオフになっている場合は、セッション サービスとプロファイリング サービスの両方のチェックボックスが無効になります。

ステップ 5 次の作業を実行します。

- [セッション サービスの有効化 (Enable Session Services)] チェックボックスをオンにして、ネットワーク アクセス セッション サービス、ポスチャ セッション サービス、ゲスト セッション サービス、およびクライアント プロビジョニング セッション サービスを実行します。
- [プロファイリング サービスの有効化 (Enable Profiling Service)] チェックボックスをオンにして、プロファイリング サービスを実行します。

- c) デバイス管理サービスを実行し、企業のネットワーク デバイスを制御および監査するには、[デバイス管理サービスの有効化 (Enable Device Admin Service)] チェックボックスをオンにします。

ステップ 6 [保存 (Save)] をクリックしてノード設定を保存します。

プロファイリング サービスによって使用されるネットワーク プローブ

ネットワークプローブは、ネットワーク上のエンドポイントから属性を収集するために使用される方法です。プローブを使用して、エンドポイントを Cisco ISE データベース内の一致するプロファイルで作成または更新できます。

Cisco ISE では、ネットワーク デバイスの動作を分析してデバイス タイプを決定する多数のネットワークプローブを使用して、デバイスをプロファイリングすることができます。ネットワークプローブは、ネットワーク可視性の向上に役立ちます。

IP アドレスと MAC アドレスのバインディング

エンドポイントを作成または更新するには、企業ネットワークの MAC アドレスのみを使用できます。ARP キャッシュにエントリが見つからない場合は、Cisco ISE で HTTP パケットの L2 MAC アドレスと NetFlow パケットの IN_SRC_MAC を使用してエンドポイントを作成または更新できます。エンドポイントが 1 ホップだけ離れている場合、プロファイリング サービスは L2 隣接関係に依存します。エンドポイントに L2 隣接関係がある場合、エンドポイントの IP アドレスと MAC アドレスはすでにマッピングされているため、IP-MAC キャッシュ マッピングは必要ありません。エンドポイントに L2 隣接関係が存在せず、エンドポイントが複数ホップ離れている場合、マッピングは信頼できない場合があります。収集する NetFlow パケットの既知の属性には、PROTOCOL、L4_SRC_PORT、IPV4_SRC_ADDR、L4_DST_PORT、IPV4_DST_ADDR、IN_SRC_MAC、OUT_DST_MAC、IN_SRC_MAC、OUT_SRC_MAC などがあります。エンドポイントに L2 隣接関係が存在せず、L3 ホップに関して複数ホップ離れている場合は、IN_SRC_MAC 属性で L3 ネットワーク デバイスの MAC アドレスのみが伝送されます。Cisco ISE で HTTP プローブが有効になっている場合は、HTTP 要求メッセージによってペイロードデータでエンドポイントの IP アドレスと MAC アドレスが伝送されないため、HTTP パケットの MAC アドレスを使用してのみエンドポイントを作成できます。Cisco ISE では、プロファイリング サービスで ARP キャッシュが実装されるため、エンドポイントの IP アドレスと MAC アドレスを確実にマッピングできます。ARP キャッシュを機能させるには、DHCP プローブまたは RADIUS プローブを有効にする必要があります。DHCP プローブと RADIUS プローブは、ペイロードデータでエンドポイントの IP アドレスと MAC アドレスを伝送します。DHCP プローブの dhcp-requested address 属性と RADIUS プローブの Framed-IP-address 属性によって、エンドポイントの IP アドレスがその MAC アドレスとともに伝送されます。これらのアドレスは、マッピングして ARP キャッシュに格納できます。

NetFlow プローブ

Cisco ISE プロファイラは Cisco IOS NetFlow Version 9 を実装しています。NetFlow Version 9 には、Cisco ISE プロファイリング サービスをサポートするためのプロファイラの拡張に必要な追加機能があるため、これを使用することを推奨します。

NetFlow Version 9 の属性を NetFlow 対応のネットワーク アクセス デバイスから収集して、エンドポイントを作成したり、Cisco ISE データベース内の既存のエンドポイントを更新できます。NetFlow Version 9 は、エンドポイントの送信元 MAC アドレスと宛先 MAC アドレスを割り当てて、更新するように設定できます。NetFlow 属性のディクショナリを作成して NetFlow ベースのプロファイリングに対応することもできます。

NetFlow Version 9 レコード フォーマットの詳細については、『NetFlow Version 9 Flow-Record Format』 マニュアルの表 6 「NetFlow Version 9 Field Type Definitions」を参照してください。

さらに、Cisco ISE は Version 5 以前の NetFlow バージョンをサポートします。ネットワークで NetFlow Version 5 を使用する場合は、Version 5 をアクセス レイヤのプライマリ ネットワーク アクセス デバイス (NAD) でのみ使用できます。他のデバイスでは動作しません。

Cisco IOS NetFlow Version 5 パケットには、エンドポイントの MAC アドレスが含まれません。NetFlow Version 5 から収集された属性は、Cisco ISE データベースに直接追加できません。IP アドレスを使用してエンドポイントを検出し、エンドポイントに NetFlow Version 5 の属性を付加できます。このことは、ネットワーク アクセス デバイスの IP アドレスと NetFlow Version 5 属性から抽出される IP アドレスを組み合わせることによって実行できます。ただし、これらのエンドポイントを RADIUS または SNMP プローブで事前に検出しておく必要があります。

NetFlow Version 5 以前のバージョンでは、MAC アドレスは IP フローの一部ではありません。このため、エンドポイントのキャッシュにあるネットワーク アクセス デバイスから収集された属性情報を関連付けることにより、エンドポイントの IP アドレスをプロファイリングすることが必要となります。

NetFlow Version 5 レコード フォーマットの詳細については、『NetFlow Services Solutions Guide』の表 2 「Cisco IOS NetFlow Flow Record and Export Format Content Information」を参照してください。

DHCP プローブ

Cisco ISE 展開のダイナミック ホスト コンフィギュレーション プロトコル プローブを有効にすると、Cisco ISE プロファイリング サービスで INIT-REBOOT および SELECTING メッセージ タイプの新しい要求だけに基づいてエンドポイントを再プロファイリングできます。

RENEWING や REBINDING などの他の DHCP メッセージ タイプは処理されますが、エンドポイントのプロファイリングには使用されません。DHCP パケットから解析された属性は、エンドポイント属性にマッピングされます。

INIT-REBOOT 状態中に生成された DHCPREQUEST メッセージ

DHCP クライアントが前に割り当てられてキャッシュされた設定を確認する場合、クライアントはサーバ識別子 (server-ip) オプションを入力できません。代わりに、前に割り当てられた

IP アドレスを要求された IP アドレス (requested-ip) オプションに入力する必要があります。また、DHCPREQUEST メッセージの Client IP Address (ciaddr) フィールドをゼロで埋める必要があります。要求された IP アドレスが正しくない場合、またはクライアントが誤ったネットワークに配置されている場合、DHCP サーバは DHCPNAK メッセージをクライアントに送信します。

SELECTING 状態中に生成された DHCPREQUEST メッセージ

DHCP クライアントは、サーバ識別子 (server-ip) オプションで選択された DHCP サーバの IP アドレスを挿入し、要求された IP アドレス (requested-ip) オプションにクライアントによって選択された DHCP OFFER の Your IP Address (yiaddr) フィールドの値を入力します。また、「ciaddr」フィールドをゼロで埋めます。

表 42: さまざまな状態からの DHCP クライアントメッセージ

—	INIT-REBOOT	SELECTING	RENEWING	REBINDING
ブロードキャスト/ユニキャスト	broadcast	broadcast	ユニキャスト	broadcast
server-ip	MUST NOT	MUST	MUST NOT	MUST NOT
requested-ip	MUST	MUST	MUST NOT	MUST NOT
ciaddr	zero	zero	IP アドレス	IP アドレス

DHCP ブリッジモードのワイヤレス LAN コントローラ設定

ダイナミック ホスト コンフィギュレーション プロトコル (DHCP) ブリッジモードでワイヤレス LAN コントローラ (WLC) を設定することを推奨します。このモードでは、ワイヤレスクライアントから Cisco ISE にすべての DHCP パケットを転送できます。WLC Web インターフェイスの [コントローラ (Controller)] > [詳細設定 (Advanced)] > [DHCP マスター コントローラ モード (DHCP Master Controller Mode)] > [DHCP パラメータ (DHCP Parameters)] で使用可能な [DHCP プロキシの有効化 (Enable DHCP Proxy)] チェックボックスをオフにする必要があります。DHCP IP ヘルパー コマンドが Cisco ISE ポリシー サービス ノードを指していることも確認する必要があります。

DHCP SPAN プローブ

DHCP スイッチド ポート アナライザ (SPAN) プローブは、Cisco ISE ノードで初期化されると、特定インターフェイス上のネットワークアクセスデバイスからのネットワークトラフィックをリッスンします。DHCP SPAN パケットを DHCP サーバから Cisco ISE プロファイラに転送するようにネットワークアクセスデバイスを設定する必要があります。プロファイラはこれらの DHCP SPAN パケットを受信して解析し、エンドポイントのプロファイリングに使用できるエンドポイント属性を取得します。

次に例を示します。

```
switch(config)# monitor session 1 source interface Gi1/0/4
switch(config)# monitor session 1 destination interface Gi1/0/2
```

HTTP プローブ

HTTP プローブでは、識別文字列が HTTP 要求ヘッダー フィールド **User-Agent** を使って転送されます。このフィールドは、IP タイプのプロファイリング条件の作成、および Web ブラウザ情報の確認に使用される属性です。プロファイラは Web ブラウザ情報を **User-Agent** 属性および要求メッセージの他の HTTP 属性から取得し、エンドポイント属性のリストに追加します。

Cisco ISE はポート 80 およびポート 8080 で Web ブラウザからの通信をリッスンします。Cisco ISE には、多くのデフォルトプロファイルが用意されています。これらのプロファイルはシステムに組み込まれ、**User-Agent** 属性に基づいてエンドポイントを識別します。

HTTP SPAN プローブ

Cisco ISE 展開の HTTP プローブをスイッチド ポート アナライザ (SPAN) プローブとともに有効にすると、プロファイラは指定されたインターフェイスからの HTTP パケットをキャプチャできます。SPAN 機能は、Cisco ISE サーバが Web ブラウザからの通信をリッスンするポート 80 で使用できます。

HTTP SPAN は、HTTP 要求ヘッダー メッセージの HTTP 属性を IP ヘッダー (L3 ヘッダー) の IP アドレスとともに収集し、L2 ヘッダーのエンドポイントの MAC アドレスに基づいてエンドポイントに関連付けることができます。この情報は、Apple デバイスやさまざまなオペレーティング システムのコンピュータなどの各種モバイルおよびポータブル IP 対応デバイスを識別するのに役立ちます。ゲスト ログインまたはクライアント プロビジョニング ダウンロード時に Cisco ISE サーバでキャプチャをリダイレクトするため、各種モバイルおよびポータブル IP 対応デバイスの識別の信頼性が向上しました。これにより、プロファイラは **User-Agent** 属性とその他の HTTP 属性を要求メッセージから取得し、Apple デバイスなどのデバイスを識別できます。

VMware で実行中の Cisco ISE の HTTP 属性の収集の無効化

Cisco ISE を ESX サーバ (VMware) に展開している場合、Cisco ISE プロファイラはダイナミック ホスト コンフィギュレーション プロトコル トラフィックを収集しますが、vSphere クライアント上の設定の問題により HTTP トラフィックを収集しません。VMware セットアップで HTTP トラフィックを収集するには、Cisco ISE プロファイラのために作成する仮想スイッチの無差別モードを **Accept** から **Reject** (デフォルト) に変更して、セキュリティを設定します。DHCP および HTTP のスイッチド ポート アナライザ (SPAN) プローブが有効になっている場合は、Cisco ISE プロファイラによって DHCP トラフィックと HTTP トラフィックの両方が収集されます。

RADIUS プローブ

Cisco ISE で認証に RADIUS を使用するように設定し、クライアントサーバトランザクションで利用できる共有秘密を定義できます。RADIUS サーバから RADIUS 要求および応答メッセージを受信すると、プロファイラはエンドポイントのプロファイリングに使用できる RADIUS 属性を収集できます。

Cisco ISE は RADIUS サーバおよび他の RADIUS サーバに対する RADIUS プロキシクライアントとして動作できます。プロキシクライアントとして動作する場合は、外部の RADIUS サーバを使用して RADIUS 要求および応答メッセージを処理します。

ネットワーク スキャン (NMAP) プローブ

NMAP プローブについて

Cisco ISE では、NMAP セキュリティ スキャナを使用して、サブネット内のデバイスを検出できます。プロファイリング サービスの実行が有効になっているポリシー サービス ノードで NMAP プローブをイネーブルにします。エンドポイント プロファイリング ポリシーでそのプロブからの結果を使用します。

NMAP の各手動サブネット スキャンには、エンドポイント ソース情報をそのスキャン ID で更新するために使用される一意の数値 ID があります。エンドポイント検出時に、エンドポイント ソース情報を更新して、ネットワーク スキャン プローブで検出されたことを示すこともできます。

NMAP の手動サブネット スキャンは、静的な IP アドレスが割り当てられたプリンタなど、常に Cisco ISE ネットワークに接続されているために、他のプロブで検出できないデバイスを検出する場合に便利です。

NMAP スキャンの制限

サブネットのスキャンには非常に多くのリソースを消費します。サブネットのスキャンは時間のかかるプロセスです。これは、サブネットのサイズや密度によって異なります。アクティブなスキャンの数は常に 1 つに制限されるため、同時にスキャンできるサブネットは 1 つだけです。また、サブネット スキャンの進行中にいつでもサブネット スキャンをキャンセルできます。[クリック (Click)] を使用して、最新のスキャン結果のリンクを表示できます。これにより、[ワーク センター (Work Centers)] > [プロファイラ (Profiler)] > [手動スキャン (Manual Scans)] > [手動 NMAP スキャンの結果 (Manual NMAP Scan Results)] に保存されている最新のネットワーク スキャン結果を表示できます。

手動 NMAP スキャン

次の NMAP コマンドを使用すると、サブネットがスキャンされ、nmapSubnet.log に出力が送信されます。

```
nmap -O -sU -p U:161,162 -oN /opt/CSCOcprm/logs/nmapSubnet.log  
--append-output -oX - <subnet>
```

表 43: 手動サブネット スキャンの NMAP コマンド

-O	OS 検出の有効化
-sU	UDP スキャン
-p <port ranges>	特定のポートのみスキャンします。たとえば、U:161, 162 と指定します。
oN	通常の出力
oX	XML 出力

NMAP の手動サブネット スキャンの SNMP 読み取り専用コミュニティ スtring

NMAP の手動サブネット スキャンは、エンドポイントで UDP ポート 161 が開かれ、その結果、より多くの属性が収集されることを検出したときには、SNMP クエリーで拡張されます。NMAP 手動サブネット スキャン中は、ネットワーク スキャンプローブによって、デバイスで SNMP ポート 161 が開いているかどうかを検出されます。ポートが開いている場合は、SNMP バージョン 2c のデフォルトのコミュニティ スtring (public) を使用して SNMP クエリがトリガーされます。デバイスで SNMP がサポートされ、デフォルトの読み取り専用コミュニティ スtring が public に設定されている場合は、デバイスの MAC アドレスを MIB 値「ifPhysAddress」から取得できます。さらに、[プロファイラ設定 (Profiler Configuration)] ページでは、NMAP の手動でのネットワーク スキャンのために、カンマで区切られた追加の SNMP 読み取り専用コミュニティ スtring を設定できます。また、[管理 (Administration)] > [システム (System)] > [設定 (Settings)] > [プロファイリング (Profiling)] では、SNMP バージョン 1 および 2c の SNMP MIB ウォーク用に新しい読み取り専用コミュニティ スtring を指定できます。

手動 NMAP スキャンの結果

最新のネットワーク スキャン結果は、[ワーク センター (Work Centers)] > [プロファイラ (Profiler)] > [手動スキャン (Manual Scans)] > [手動 NMAP スキャンの結果 (Manual NMAP Scan Results)] に保存されます。[手動 NMAP スキャンの結果 (Manual NMAP Scan Results)] ページには、任意のサブネットに対して手動でのネットワーク スキャンを実行し、その結果として検出された最新のエンドポイントのみが、関連付けられたエンドポイントプロファイル、MAC アドレス、およびスタティック割り当てステータスとともに表示されます。このページでは、必要に応じて、エンドポイントサブネットで検出されたポイントをより適切に分類するために編集できます。

Cisco ISE を使用すると、プロファイリングサービスの実行が有効になっている [ポリシー サービス (Policy Service)] ノードで手動でのネットワーク スキャンを実行できます。展開内のプライマリ管理 ISE ノードユーザインターフェイスでポリシー サービス ノードを選択し、そのポリシー サービス ノードで手動でのネットワーク スキャンを実行する必要があります。任意のサブネットに対する手動でのネットワーク スキャン時に、ネットワーク スキャンプローブにより、指定されたサブネット上のエンドポイントとそのオペレーティングシステムが検出され、SNMP サービス用の UDP ポート 161 および 162 がチェックされます。

その他の情報

手動での NMAP スキャンの結果に関する追加情報を以下に示します。

- 不明なエンドポイントを検出するには、NMAP が NMAP スキャンまたはサポートする SNMP スキャンを介して IP/MAC バインディングを学習する必要があります。
- ISE は、RADIUS 認証または DHCP プロファイリングを使用して、既知のエンドポイントの IP/MAC バインディングを学習します。
- IP/MAC バインディングは、展開内の PSN ノード間で複製されません。したがって、ローカル データベースに IP/MAC バインディングがある PSN（たとえば、MAC アドレスが最後に認証された PSN）から手動スキャンを開始する必要があります。
- NMAP スキャンの結果には、手動または自動にかかわらず、NMAP が以前にスキャンしたエンドポイントに関する情報は表示されません。

DNS プローブ

Cisco ISE 展開のドメイン ネーム サーバ (DNS) プローブを使用すると、プロファイラはエンドポイントを検索し、完全修飾名 (FQDN) を取得できます。Cisco ISE 対応のネットワークでエンドポイントが検出されたら、エンドポイント属性のリストが NetFlow、DHCP、DHCP SPAN、HTTP、RADIUS、または SNMP プローブから収集されます。

Cisco ISE をスタンドアロンで展開する場合、または初めて分散環境に展開する場合は、セットアップユーティリティを実行して Cisco ISE アプライアンスを設定するように求められます。セットアップユーティリティを実行するときに、ドメイン ネーム システム (DNS) ドメインとプライマリ ネームサーバ (プライマリ DNS サーバ) を設定します。設定時には、1 つ以上のネームサーバを設定できます。Cisco ISE の展開後に、CLI コマンドを使用して DNS ネームサーバを変更または追加することもできます。

DNS FQDN ルックアップ

DNS ルックアップを実行する前に、DHCP、DHCP SPAN、HTTP、RADIUS、または SNMP のいずれかのプローブを DNS プローブとともに起動する必要があります。これにより、プロファイラの DNS プローブは、Cisco ISE 展開に定義されている、指定されたネームサーバに対して逆引き DNS ルックアップ (FQDN ルックアップ) を実行できます。新しい属性がエンドポイントの属性リストに追加され、エンドポイント プロファイリング ポリシーの評価に使用できます。FQDN は、システム IP ディクショナリに存在する新しい属性です。エンドポイント プロファイリング条件を作成して、FQDN 属性およびそのプロファイリング用の値を検証できます。次は、DNS ルックアップ、およびこれらの属性を収集するプローブに必要な特定のエンドポイント属性です。

- dhcp-requested-address 属性 : DHCP プローブと DHCP SPAN プローブによって収集される属性
- SourceIP 属性 : HTTP プローブによって収集される属性
- Framed-IP-Address 属性 : RADIUS プローブによって収集される属性

- cdpCacheAddress 属性：SNMP プロープによって収集される属性

WLC Web インターフェイスでの呼出端末 ID タイプの設定

WLC Web インターフェイスを使用して、呼出端末 ID タイプ情報を設定できます。WLC Web インターフェイスの [セキュリティ (Security)] タブに移動すると、[RADIUS RADIUS 認証サーバ (Authentication Servers)] ページで発信側ステーション ID を設定できます。[MAC デリミタ (MAC Delimiter)] フィールドは、WLC ユーザインターフェイスのデフォルトでは、[コロン (Colon)] に設定されます。

WLC Web インターフェイスで設定する方法の詳細については、『Cisco Wireless LAN Controller Configuration Guide, Release 7.2』の第 6 章「Configuring Security Solutions」を参照してください。

config radius callStationIdType コマンドを使用して WLC CLI で設定する方法の詳細については、『Cisco Wireless LAN Controller Command Reference Guide, Release 7.2』の第 2 章「Controller Commands」を参照してください。

-
- ステップ 1 ワイヤレス LAN コントローラのユーザインターフェイスにログインします。
 - ステップ 2 [セキュリティ (Security)] をクリックします。
 - ステップ 3 [AAA] を展開して、[RADIUS] > [認証 (Authentication)] を選択します。
 - ステップ 4 [呼出端末 ID タイプ (Call Station ID Type)] ドロップダウンリストから [システム MAC アドレス (System MAC Address)] を選択します。
 - ステップ 5 FIPS モードで Cisco ISE を実行する場合は、[AES キー ラップ (AES Key Wrap)] チェックボックスをオンにします。
 - ステップ 6 [MAC 区切り文字 (MAC Delimiter)] ドロップダウンリストから [コロン (Colon)] を選択します。
-

SNMP クエリ プロープ

[ノードの編集 (Edit Node)] ページでの SNMP クエリー プロープの設定に加えて、[管理 (Administration)] > [ネットワーク リソース (Network Resources)] > [ネットワーク デバイス (Network Devices)] でその他の Simple Management Protocol 設定を行う必要があります。

[ネットワーク デバイス (Network Devices)] リスト ページで新しいネットワーク アクセス デバイス (NAD) の SNMP 設定を行うことができます。ネットワーク アクセス デバイスの SNMP クエリー プロープまたは SNMP 設定に指定したポーリング間隔で、NAD に定期的にクエリーを実行します。

次の設定に基づいて、特定の NAD の SNMP クエリーをオンおよびオフにすることができます。

- [リンクアップ時に SNMP クエリー (SNMP Query on Link up)] および [新しい MAC の通知 (New MAC notification)] のオンまたはオフ

- Cisco Discovery Protocol 情報の [リンクアップ時に SNMP クエリー (SNMP Query on Link up)] および [新しい MAC の通知 (New MAC notification)] のオンまたはオフ
- SNMP クエリー タイマーをデフォルトでスイッチごとに 1 時間に 1 回

iDevice および SNMP をサポートしないその他のモバイルデバイスでは、ARP テーブルによって MAC アドレスを検出でき、SNMP クエリー プローブによってネットワーク アクセス デバイスからクエリーを実行できます。

SNMP クエリに関する Cisco Discovery Protocol のサポート

ネットワーク デバイスで SNMP 設定を行う場合は、ネットワーク デバイスのすべてのポートで Cisco Discovery Protocol を有効 (デフォルト) にする必要があります。ネットワーク デバイスのいずれかのポートで Cisco Discovery Protocol を無効にすると、接続されているすべてのエンドポイントの Cisco Discovery Protocol 情報が失われるため、正しくプロファイリングを実行できなくなる可能性があります。ネットワーク デバイスで `cdp run` コマンドを使用して Cisco Discovery Protocol をグローバルに有効にし、ネットワーク アクセス デバイスのインターフェイスで `cdp enable` コマンドを使用して Cisco Discovery Protocol を有効にします。ネットワーク デバイスとインターフェイスで Cisco Discovery Protocol を無効にするには、コマンドの先頭に `no` キーワードを使用します。

SNMP クエリに関する Link Layer Discovery Protocol のサポート

Cisco ISE プロファイラは LLDP の属性を収集するために SNMP クエリーを使用します。RADIUS プローブを使用して、ネットワーク デバイ스에組み込まれている Cisco IOS センサーから LLDP 属性を収集することもできます。ネットワーク アクセス デバイスで LLDP グローバル コンフィギュレーション コマンドおよび LLDP インターフェイス コンフィギュレーション コマンドの設定に使用できるデフォルトの LLDP 構成設定を確認してください。

表 44: デフォルトの LLDP 設定

機能	機能
LLDP グローバル ステート	無効
LLDP ホールドタイム (廃棄までの時間)	120 秒
LLDP タイマー (パケット更新頻度)	30 秒
LLDP 再初期化遅延	2 秒
LLDP tlv-select	有効 (すべての TLV の送受信が可能)
LLDP インターフェイス ステート	[有効 (Enabled)]
LLDP 受信	[有効 (Enabled)]
LLDP 転送	[有効 (Enabled)]
LLDP med-tlv-select	有効 (すべての LLDP-MED TLV の送信が可能)

単一文字で表示される CDP および LLDP の機能コード

エンドポイントの属性リストには、lldpCacheCapabilities 属性と lldpCapabilitiesMapSupported 属性の 1 文字の値が表示されます。値は、CDP と LLDP を実行するネットワーク アクセス デバイスに対して表示される機能コードです。

例 1

```
lldpCacheCapabilities S
lldpCapabilitiesMapSupported S
```

例 2

```
lldpCacheCapabilities B;T
lldpCapabilitiesMapSupported B;T
```

例 3

```
Switch#show cdp neighbors
Capability Codes:
R - Router, T - Trans Bridge, B - Source Route Bridge, S - Switch, H - Host, I - IGMP,
r - Repeater, P - Phone, D - Remote, C - CVTA, M - Two-port Mac Relay
...
Switch#

Switch#show lldp neighbors
Capability codes:
(R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
(W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
...
Switch#
```

SNMP トラップ プローブ

SNMP トラップは、MAC 通知、linkup、linkdown、および informs をサポートする特定のネットワーク アクセスデバイスから情報を受信します。SNMP トラッププローブは、ポートがアップまたはダウンし、エンドポイントがネットワークから切断するか、またはネットワークに接続したときに、特定のネットワーク アクセス デバイスから情報を受信します。そのため、受信した情報は Cisco ISE にエンドポイントを作成するのに十分ではありません。

SNMP トラップを完全に機能させ、エンドポイントを作成するには、トラップを受信したときに SNMP クエリープローブがネットワーク アクセス デバイスの特定のポートでポーリングイベントをトリガーするように SNMP クエリーを有効にする必要があります。この機能を完全に動作させるには、ネットワーク アクセス デバイスと SNMP トラップを設定する必要があります。



(注) Cisco ISE では、ワイヤレス LAN コントローラ (WLC) とアクセス ポイント (AP) から受信した SNMP トラップはサポートされません。

Active Directory プローブ

AD のプローブ :

- Windows エンドポイントの OS 情報の明瞭度を向上させます。Microsoft AD はバージョンとサービス パックのレベルを含む、AD に参加しているコンピュータの OS の詳細情報を追跡します。AD のプローブは、AD のランタイム コネクタを使用してこの情報を直接取得し、クライアント OS 情報の信頼性の高いソースを提供します。
- 社内および社外の資産を区別するのに役立ちます。AD のプローブで使用される基本的ですが重要な属性は、エンドポイントが AD にあるかどうかです。この情報は AD に含まれるエンドポイントを管理対象デバイスまたは企業資産として分類するために使用できます。

[管理 (Administration)] > [システム (System)] > [展開 (Deployment)] > [プロファイリング設定 (Profiling Configuration)] ページで AD プローブを有効化できます。このプローブを有効にすると、ISE はホスト名を受信するとすぐに、新しいエンドポイントの AD 属性を取得します。ホスト名は通常 DHCP または DNS プローブから正常に学習されます。正常に取得すると、ISE は再スキャンがタイムアウトになるまで、同じエンドポイントに対し AD を再度問い合わせようとはしません。これにより属性の問い合わせに対する AD の負荷が制限されます。再スキャンタイマーは、[再スキャンまでの日数 (Days Before Rescan)] フィールド ([管理 (Administration)] > [システム (System)] > [展開 (Deployment)] > [プロファイリング設定 (Profiling Configuration)] > [Active Directory]) で設定できます。エンドポイントでの追加のプロファイリング アクティビティがあれば、AD はもう一度クエリーされます。

次の AD プローブの属性は ACTIVEDIRECTORY 条件を使用して、[ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [プロファイリング (Profiling)] でマッピングさせることができます。AD のプローブを使用して集められた AD 属性は、[コンテキストの可視性 (Context Visibility)] > [エンドポイント (Endpoints)] ページのエンドポイントの詳細にプレフィックス「AD」が付いて表示されます。

- AD-Host-Exists
- AD-Join-Point
- AD-Operating-System
- AD-OS-Version
- AD-Service-Pack

Cisco ISE ノードごとのプローブの設定

ポリシー サービス ペルソナを担当する展開の Cisco ISE ノードごとに、[プロファイリング設定 (Profiling Configuration)] タブで次のプローブを 1 つ以上設定できます。

- [スタンドアロン ノード (A standalone node)] : デフォルトですべての管理、モニタリング、およびポリシー サービスのペルソナを担当する単一のノードに Cisco ISE を展開した場合。
- [複数ノード (Multiple nodes)] : 展開でポリシー サービス ペルソナを担当するノードを複数登録した場合。

始める前に

Cisco ISE ノードごとのプローブは、管理ノードからのみ設定できます。管理ノードは、分散展開のセカンダリ管理ノードで使用できません。

-
- ステップ 1 [管理 (Administration)] > [システム (System)] > [展開 (Deployment)] を選択します。
 - ステップ 2 ポリシー サービス ペルソナを担当する Cisco ISE ノードを選択します。
 - ステップ 3 [展開ノード (Deployment Nodes)] ページで [編集 (Edit)] をクリックします。
 - ステップ 4 [全般設定 (General Settings)] タブで [ポリシー サービス (Policy Service)] チェックボックスをオンにします。[ポリシー サービス (Policy Service)] チェックボックスがオフになっている場合は、セッション サービスとプロファイリング サービスの両方のチェックボックスが無効になります。
 - ステップ 5 [プロファイリング サービスの有効化 (Enable Profiling Service)] チェックボックスをオンにします。
 - ステップ 6 [プロファイリング設定 (Profiling Configuration)] タブをクリックします。
 - ステップ 7 各プローブの値を設定します。
 - ステップ 8 [保存 (Save)] をクリックしてプローブ設定を保存します。
-

CoA、SNMP RO コミュニティおよびエンドポイント属性フィルタの設定

Cisco ISE では、グローバル コンフィギュレーションで、[プロファイラ設定 (Profiler Configuration)] ページで許可変更 (CoA) を発行し、プロファイリング サービスを有効にしてすでに認証されているエンドポイントに対する制御を拡張することができます。

さらに、[プロファイラ設定 (Profiler Configuration)] ページでは、NMAP の手動でのネットワーク スキャンのために、カンマで区切られた追加の SNMP 読み取り専用コミュニティ ストリングを設定できます。SNMPRO コミュニティ ストリングは、[現在のカスタム SNMP コミュニティ]

ニティ スtring (Current custom SNMP community strings)] フィールドに表示されるのと同じ順序で使用されます。

[プロファイラ設定 (Profiler Configuration)] ページでは、エンドポイント属性のフィルタリングを設定することもできます。

ステップ 1 [管理 (Administration)] > [システム (System)] > [設定 (Settings)] > [プロファイリング (Profiling)] を選択します。

ステップ 2 次のいずれかの設定を選択して、CoA タイプを設定します。

- [CoA なし (No CoA)] (デフォルト) : このオプションを使用して、CoA のグローバルコンフィギュレーションを無効にできます。この設定は、エンドポイントプロファイリングポリシーごとに設定された CoA を上書きします。
- [ポート バウンス (Port Bounce)] : スイッチ ポートのセッションが 1 つだけである場合は、このオプションを使用できます。ポートに複数のセッションがある場合は、[再認証 (Reauth)] オプションを使用します。
- [再認証 (Reauth)] : このオプションを使用して、すでに認証されているエンドポイントをプロファイリング時に再認証できます。

1 つのポートに複数のアクティブなセッションがある場合は、CoA に [ポート バウンス (Port Bounce)] オプションを設定しても、プロファイリング サービスによって [再認証 (Reauth)] オプションが指定された CoA が発行されます。この機能を使用すると、[ポート バウンス (Port Bounce)] オプションの場合のように他のセッションが切断されるのを回避できます。

ステップ 3 NMAP の手動でのネットワーク スキャンのために、カンマで区切られた新しい SNMP コミュニティ スtring を [カスタム SNMP コミュニティ スtring の変更 (Change custom SNMP community strings)] フィールドに入力し、[カスタム SNMP コミュニティ スtring の確認 (Confirm custom SNMP community strings)] フィールドに文字列を再入力します。

ステップ 4 [エンドポイント属性フィルタ (Endpoint Attribute Filter)] チェックボックスをオンにして、エンドポイント属性のフィルタリングを有効にします。

ステップ 5 [保存 (Save)] をクリックします。

認証されたエンドポイントに対する許可変更のグローバル設定

デフォルトの [CoA なし (No CoA)] オプションを使用して許可変更 (CoA) を無効にするか、ポート バウンスと再認証オプションを使用して CoA を有効にするグローバルコンフィギュレーション オプションを使用できます。Cisco ISE の CoA でポート バウンスを設定している場合は、「CoA 免除」の項で説明されているように、プロファイリング サービスにより他の CoA が発行されることがあります。

RADIUS プロブまたはモニタリング ペルソナの REST API を使用して、エンドポイントの認証できます。RADIUS プロブを有効にして、パフォーマンスを向上させることができます。CoA を有効にした場合は、Cisco ISE アプリケーションで CoA 設定と合わせて RADIUS プロブ

ブを有効にしてパフォーマンスを向上させることを推奨します。これにより、プロファイリングサービスは収集された RADIUS 属性を使用して、エンドポイントに適切な CoA を発行できます。

Cisco ISE アプリケーションで RADIUS プローブを無効にした場合は、モニタリング ペルソナの REST API を使用して CoA を発行できます。これにより、プロファイリングサービスは幅広いエンドポイントをサポートできます。分散展開では、モニタリング ペルソナの REST API を使用して CoA を発行するために、モニタリング ペルソナを担当する Cisco ISE ノードがネットワークに少なくとも 1 つ存在している必要があります。

プライマリおよびセカンダリ モニタリング ノードは同一のセッション ディレクトリ情報を持つため、Cisco ISE は、分散展開内の REST クエリーのデフォルトの宛先としてプライマリおよびセカンダリ モニタリング ノードを適宜指定します。

許可変更の発行の使用例

次の場合に、プロファイリングサービスによって許可変更が発行されます。

- エンドポイントが削除される：エンドポイントが[エンドポイント (Endpoints)] ページから削除され、そのエンドポイントがネットワークから接続解除または排除された場合。
- 例外アクションが設定される：エンドポイントに異常または許容できないイベントをもたらす例外アクションがプロファイルごとに設定されている場合。プロファイリングサービスは、CoA を発行して対応するスタティック プロファイルにエンドポイントを移動します。
- エンドポイントが初めてプロファイリングされる：エンドポイントがスタティックに割り当てられておらず、初めてプロファイリングされる場合（たとえば、プロファイルが不明プロファイルから既知のプロファイルに変更された場合）。
 - エンドポイント ID グループが変更される：エンドポイントが許可ポリシーで使用されるエンドポイント ID グループに対して追加または削除された場合。
 エンドポイント ID グループが変更され、エンドポイント ID グループが次のために許可ポリシーで使用されている場合、プロファイリングサービスは CoA を発行します。
 - 動的にプロファイリングされる場合のエンドポイントに対するエンドポイント ID グループの変更
 - ダイナミック エンドポイントに対してスタティック割り当てフラグが true に設定されている場合のエンドポイント ID グループの変更
- エンドポイントプロファイリングのポリシーが変更され、ポリシーが許可ポリシーで使われる：エンドポイント プロファイリング ポリシーが変更され、許可ポリシーで使われる論理的なプロファイルにそのポリシーが含まれる場合。エンドポイントプロファイリング ポリシーは、プロファイリング ポリシーの一致のため、または、エンドポイントが論理的なプロファイルに関連付けられたエンドポイント プロファイリング ポリシーにスタティックに割り当てられるときに、変更される場合があります。両方の場合で、エンド

ポイント プロファイリング ポリシーが許可ポリシーで使用される場合のみ、プロファイリング サービスは CoA を発行します。

許可変更の発行の免除

エンドポイント ID グループが変更され、スタティック割り当てがすでに true の場合、プロファイリング サービスは CoA を発行しません。

Cisco ISE は次の理由で CoA を発行しません。

- エンドポイントがネットワークから切断されている：ネットワークから切断されているエンドポイントが検出された場合。
- 有線（Extensible Authentication Protocol）EAP 対応エンドポイントが認証された：認証された有線 EAP 対応エンドポイントが検出された場合。
- ポートごとに複数のアクティブセッション：1つのポートに複数のアクティブなセッションがある場合は、CoA に [ポート バウンス（Port Bounce）] オプションを設定しても、プロファイリング サービスによって [再認証（Reauth）] オプションが指定された CoA が発行されます。
- ワイヤレス エンドポイント検出時のパケット オブ ディスコネクト CoA（セッションの終了）：エンドポイントがワイヤレスとして検出されて、パケット オブ ディスコネクト CoA（セッション終了）がポート バウンス CoA の代わりに送信された場合。この変更の利点は、ワイヤレス LAN コントローラ（WLC）CoA がサポートされていることです。
- エンドポイントがゲストデバイス登録フローによって作成された：エンドポイントがゲストのデバイス登録によって作成された場合。CoA が Cisco ISE でグローバルに有効になっても、プロファイリング サービスは、デバイス登録のフローに影響を与えないように CoA を発行しません。特に、ポートバウンス CoA のグローバル設定は、エンドポイント接続のフローを中断します。
- グローバルな [CoA なし（No CoA）] 設定がポリシー CoA を上書きする：グローバルな [CoA なし（No CoA）] は、エンドポイントプロファイリング ポリシーのすべての構成設定を上書きします。エンドポイントプロファイリングポリシーごとに設定された CoA に関係なく、Cisco ISE で CoA が発行されないためです。



(注) [CoA なし（No CoA）] および [再認証（Reauth）] CoA 設定は影響を受けません。また、プロファイラサービスは有線およびワイヤレス エンドポイントに同じ CoA の設定を適用します。

CoA 設定の各タイプに発行される許可変更

表 45: CoA 設定の各タイプに発行される許可変更

シナリオ	CoA なし設定	ポート バウンス 設定	再認証設定	その他の情報
Cisco ISE における CoA グローバル コンフィギュレーション (一般的な設定)	CoA なし (No CoA)	ポート バウンス	再認証 (Reauthentication)	—
エンドポイントがネットワークで検出された場合	CoA なし (No CoA)	CoA なし (No CoA)	CoA なし (No CoA)	許可変更は、RADIUS 属性の Acct -Status -Type 値 Stop で判別されます。
同じスイッチポートで複数のアクティブセッションと有線接続	CoA なし (No CoA)	再認証 (Reauthentication)	再認証 (Reauthentication)	再認証は、他のセッションの切断を回避します。
ワイヤレス エンドポイント	CoA なし (No CoA)	切断パケット CoA (セッション終了)	再認証 (Reauthentication)	ワイヤレス LAN コントローラに対するサポート。
不完全な CoA データ	CoA なし (No CoA)	CoA なし (No CoA)	CoA なし (No CoA)	原因は RADIUS 属性の欠落。

ISE データベースの持続性とパフォーマンスの属性フィルタ

Cisco ISE は、ダイナミック ホスト コンフィギュレーション プロトコル (DHCP ヘルパーと DHCPSPAN の両方)、HTTP、RADIUS、およびシンプルネットワーク管理プロトコルの各プローブのフィルタを実装しています。ただし、パフォーマンスの低下に対処するために NetFlow は除外されています。各プローブ フィルタには、一時的でエンドポイント プロファイルとは関係のない属性のリストが含まれ、これらの属性はプローブによって収集された属性から削除されます。

isebootstrap ログ (isebootstrap-yyyymmdd-xxxxxx.log) には、辞書からの属性がフィルタリングされた状態で、辞書の作成を処理するメッセージが含まれます。エンドポイントがフィルタリ

ング フェーズを通過するときに、フィルタリングが行われたことを示すデバッグ メッセージをログに記録するように設定することもできます。

Cisco ISE プロファイラは、次のエンドポイント属性フィルタを呼び出します。

- DHCP ヘルパーと DHCP SPAN の両方の DHCP フィルタには、不要なすべての属性が含まれ、これらの属性は DHCP パケットの解析後に削除されます。フィルタリング後の属性は、エンドポイントのエンドポイント キャッシュ内にある既存の属性とマージされます。
- HTTP フィルタは、HTTP パケットからの属性のフィルタリングに使用され、フィルタリング後の属性セットに大幅な変更はありません。
- RADIUS フィルタは、syslog 解析が完了すると使用され、エンドポイント属性がプロファイリングのためにエンドポイント キャッシュにマージされます。
- SNMP クエリー用の SNMP フィルタには、CDP および LLDP フィルタが含まれています。これらのフィルタはすべて SNMP クエリー プロンプトに使用されます。

ホワイトリストを使用してエンドポイント属性をフィルタリングするグローバル設定

収集ポイントで頻繁には変わらないエンドポイント属性の数を減らして、永続性イベントおよび複製イベントの数を減らすことができます。エンドポイント属性フィルタを有効にすると、Cisco ISE プロファイラは、重要な属性のみを保持し、その他の属性をすべて廃棄します。重要な属性とは、Cisco ISE システムによって使用される属性またはエンドポイント プロファイリング ポリシーやルールで明確に使用される属性です。

ホワイトリストは、カスタム エンドポイント プロファイリング ポリシー内でエンドポイントのプロファイリングに使用される属性のセットであり、許可変更 (CoA)、個人所有デバイスの持ち込み (BYOD)、デバイス登録 WebAuth (DRW) などが Cisco ISE で期待どおりに機能するために不可欠な属性のセットです。ホワイトリストは、無効になっている場合でも、エンドポイントの所有権が変わった場合に (属性が複数のポリシーのサービス ノードによって収集されている場合)、常に基準として使用されます。

デフォルトではホワイトリストは無効で、属性は、属性フィルタが有効になっている場合にのみドロップされます。ホワイトリストは、フィードからの変更など、エンドポイントプロファイリングポリシーが変更されると、プロファイリングポリシーに新しい属性を含めるように、動的に更新されます。ホワイトリストにない属性は収集時に即座にドロップされ、属性をプロファイリングエンドポイントに加えることはできません。バッファリングと組み合わせると、永続性イベントの数を減らすことができます。

ホワイトリストに次の2つのソースから決定された属性のセットが含まれていることを確認する必要があります。

- エンドポイントをプロファイルに適合させるためにデフォルトプロファイルで使用される属性のセット。
- 許可変更 (CoA)、個人所有デバイスの持ち込み (BYOD)、デバイス登録 WebAuth (DRW) などが Cisco ISE で期待どおりに機能するために不可欠な属性のセット。

表 46: ホワイトリストの属性

AAA-Server	BYODRegistration
Calling-Station-ID	Certificate Expiration Date
Certificate Issue Date	Certificate Issuer Name
Certificate Serial Number	説明
DestinationIPAddress	Device Identifier
デバイス名 (Device Name)	DeviceRegistrationStatus
EndPointPolicy	EndPointPolicyID
EndPointProfilerServer	EndPointSource
[FQDN]	FirstCollection
Framed-IP-Address	IdentityGroup
IdentityGroupID	IdentityStoreGUID
IdentityStoreName	L4_DST_PORT
LastNmapScanTime	MACAddress
MatchedPolicy	MatchedPolicyID
NADAddress	NAS-IP-Address
NAS-Port-Id	NAS-Port-Type
NmapScanCount	NmapSubnetScanID
OS Version	OUI
PolicyVersion	PortalUser
PostureApplicable	製品
RegistrationTimeStamp	—
StaticAssignment	StaticGroupAssignment
TimeToProfile	Total Certainty Factor
User-Agent	cdpCacheAddress
cdpCacheCapabilities	cdpCacheDeviceId
cdpCachePlatform	cdpCacheVersion
ciaddr	dhep-class-identifier

dhcp-requested-address	host-name
hrDeviceDescr	ifIndex
ip	lldpCacheCapabilities
lldpCapabilitiesMapSupported	lldpSystemDescription
operating-system	sysDescr
161-udp	—

IOS センサー組み込みスイッチからの属性の収集

IOS センサーの統合によって、Cisco ISE ランタイムと Cisco ISE プロファイラでスイッチから送信された任意またはすべての属性を収集できるようになりました。RADIUS プロトコルを使用して、DHCP、CDP、および LLDP 属性をスイッチから直接収集できます。DHCP、CDP、および LLDP について収集された属性は、解析され、次の場所のプロファイラディクショナリの属性にマッピングされます ([ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [ディクショナリ (Dictionaries)])。

デバイス センサー用にサポートされている Catalyst プラットフォームについては、<https://communities.cisco.com/docs/DOC-72932> を参照してください。

IOS センサー組み込みネットワーク アクセス デバイス

IOS センサー組み込みネットワーク アクセス デバイスと Cisco ISE の統合では、次のコンポーネントが含まれます。

- IOS センサー
- DHCP、CDP および LLDP のデータを収集するためにネットワーク アクセス デバイス（スイッチ）に組み込まれているデータ コレクタ
- データを処理し、エンドポイントのデバイス タイプを決定するアナライザ

アナライザを展開するには次の 2 つの方法がありますが、2 つを組み合わせることは想定されていません。

- アナライザを Cisco ISE に展開する
- アナライザをセンサーとしてスイッチに組み込む

IOS センサー組み込みネットワーク アクセス デバイスの設定チェックリスト

ここでは、スイッチから直接 DHCP、CDP、および LLDP の属性を収集するために、IOS センサー対応スイッチと Cisco ISE で設定する必要がある作業のリストの概要を説明します。

- RADIUS プローブが Cisco ISE で有効になっていることを確認します。
- ネットワーク アクセス デバイスで DHCP、CDP、および LLDP 情報を収集するための IOS センサーがサポートされていることを確認します。
- ネットワーク アクセス デバイスで、エンドポイントから CDP 情報と LLDP 情報を取得するために次の CDP コマンドと LLDP コマンドが実行されていることを確認します。

```
cdp enable
lldp run
```

- 標準の AAA コマンドと RADIUS コマンドを使用して、セッションアカウンティングが個別に有効になっていることを確認します。

コマンドの使用例を示します。

```
aaa new-model
aaa accounting dot1x default start-stop group radius

radius-server host <ip> auth-port <port> acct-port <port> key <shared-secret>
radius-server vsa send accounting
```

- IOS センサー固有のコマンドを実行していることを確認します。

- アカウンティング拡張の有効化

ネットワーク アクセス デバイスで IOS センサー プロトコル データを RADIUS アカウンティング メッセージに追加したり、新しいセンサー プロトコル データの検出時に追加のアカウンティング イベントを生成したりできるようにする必要があります。つまり、RADIUS アカウンティング メッセージには、すべての CDP、LLDP、および DHCP 属性が含まれている必要があります。

次のグローバル コマンドを入力します。

```
device-sensor accounting
```

- アカウンティング拡張の無効化

(アカウンティング機能がグローバルに有効になっている場合、) (アカウンティング) ネットワーク アクセス デバイスで、特定のポートでホストされているセッションについて IOS センサー プロトコル データを RADIUS アカウンティング メッセージに追加できないようにするには、適切なポートで次のコマンドを入力します。

```
no device-sensor accounting
```

- TLV 変更のトラッキング

デフォルトでは、サポートされている各ピアプロトコルでクライアント通知とアカウントティングイベントが生成されるのは、特定のセッションのコンテキストで前に受信したことの無いタイプ、長さ、値（TLV）が着信パケットに含まれている場合だけです。

新しい TLV が存在するか、または前に受信した TLV の値が異なる場合は、すべての TLV 変更に対するクライアント通知とアカウントティング イベントを有効にする必要があります。次のコマンドを入力します。

```
device-sensor notify all-changes
```

- ネットワーク アクセス デバイスで IOS Device Classifier（ローカル アナライザ）が無効になっていることを確認します。

次のコマンドを入力します。

```
no macro auto monitor
```



（注） このコマンドにより、ネットワーク アクセス デバイスは変更ごとに2つの同じ RADIUS アカウントティング メッセージを送信できなくなります。

プロファイラ条件

プロファイラ条件はポリシー要素であり、他の条件とほとんど同じです。ただし、認証、許可、およびゲスト条件とは異なり、プロファイリング条件は限られた数の属性に基づいています。[プロファイラ条件（Profiler Conditions）] ページに Cisco ISE で使用できる属性とその説明が表示されます。

プロファイラ条件は次のとおりです。

- シスコ提供：Cisco ISE には展開時に事前定義されたプロファイリング条件が含まれており、[プロファイラ条件（Profiler Conditions）] ページでシスコ提供の条件として識別されます。シスコ提供のプロファイリング条件を削除することはできません。

[ポリシー（Policy）]>[ポリシー要素（Policy Elements）]>[ディクショナリ（Dictionaries）]>[システム（System）] からアクセスできる場所にあるシステムプロファイラディクショナリにもシスコ提供条件があります。

たとえば、MAC ディクショナリです。一部の製品では、OUI（固有識別子情報）がデバイスの製造組織を識別するために最初に使用できる固有属性です。これはデバイスの MAC アドレスのコンポーネントです。MAC ディクショナリには、MACAddress および OUI 属性が含まれています。

- 管理者作成：ユーザが Cisco ISE の管理者として作成するプロファイラ条件、複製された事前定義済みのプロファイリング条件は管理者作成として識別されます。[プロファイラ

条件 (Profiler Conditions)] ページでプロファイラ ディクショナリを使用して、DHCP、MAC、SNMP、IP、RADIUS、NetFlow、CDP、LLDP、および NMAP タイプのプロファイラ条件を作成できます。

プロファイリング ポリシーの数の推奨上限は 1000 ですが、最高 2000 までプロファイリング ポリシーを拡張できます。

Cisco NAC アプライアンスとの Cisco ISE 統合

Cisco ISE は、Cisco Network Admission Control (NAC) アプライアンス リリース 4.9 との統合のみをサポートし、Cisco ISE に Advanced ライセンスまたは Wireless ライセンスをインストールした場合に使用できます。

Cisco ISE プロファイラは Cisco NAC 展開のエンドポイントを管理する Cisco Network Admission Control (NAC) プロファイラに似ています。この統合により、Cisco NAC 展開にインストールされている既存の Cisco NAC プロファイラを置き換えることができます。Cisco ISE プロファイラからのプロファイル名およびエンドポイント分類の結果を Cisco Clean Access Manager (CAM) と同期できます。

管理ノードでの Cisco Clean Access Manager の設定

Cisco ISE では、REST API 通信設定のために分散展開のプライマリ PAN で複数の Clean Access Manager (CAM) を登録できます。Cisco ISE に登録されている CAM のリストは、すべてのプロファイラ設定変更が通知されるリストです。プライマリ PAN は、Cisco ISE と Cisco NAC アプライアンス間のすべての通信を担当します。Cisco ISE では、CAM をプライマリ PAN でのみ設定できます。1 つ以上の CAM をプライマリ PAN で登録するときに使用されたクレデンシャルが CAM との接続の認証に使用されます。

Cisco ISE と Cisco NAC アプライアンス間の通信は、Secure Sockets Layer (SSL) 上で安全に行われます。Cisco ISE はプロファイラ設定の変更を CAM にプッシュし、CAM はエンドポイントの MAC アドレスと対応するプロファイルのリストおよびすべてのプロファイル名のリストを Cisco ISE から定期的にプルするため、通信は実際には双方向です。

Cisco ISE と CAM 間でセキュアな通信を適切に行えるように、[管理 (Administration)] > [Clean Access Manager] > [SSL] で X509 証明書の内容を Clean Access Manager からエクスポートし、それを [管理 (Administration)] > [システム (System)] > [証明書 (Certificates)] > [信頼できる証明書ストア (Trusted Certificates Store)] で Cisco ISE のプライマリ PAN にインポートする必要があります。

ハイアベイラビリティ用の CAM のペアを設定する方法の詳細については、次のリンクを参照してください。

Cisco ISE プロファイラと Cisco Clean Access Manager の通信

Cisco ISE プロファイラは、プロファイラ設定の変更をプライマリ PAN からすべての登録済み Clean Access Manager (CAM) に通知します。これにより、Cisco ISE 分散展開における通知の

重複が回避されます。Cisco ISE データベースでエンドポイントの追加や削除、およびエンドポイント プロファイリング ポリシーの変更が行われると、プロファイラ設定の変更を通知するために REST API が使用されます。エンドポイントのインポート時、Cisco ISE プロファイラはインポートの完了後にのみ CAM に通知します。

プロファイラ設定の変更を CAM にプッシュするために、次の REST API フローが実装されます。

Cisco ISE プロファイラ エンドポイント変更のプッシュ：Cisco ISE でエンドポイントがプロファイリングされ、エンドポイントのプロファイルに変更がある場合、Cisco ISE プロファイラは、エンドポイント プロファイルの変更をすべての登録済み CAM に通知します。

CAM で Cisco ISE を設定し、CAM の [同期設定 (Sync Settings)] に応じて CAM を Cisco ISE と同期することができます。ルールを作成し、Cisco ISE プロファイルのリストから 1 つ以上の一致するプロファイルを選択し、エンドポイントを CAM のいずれかのアクセス タイプにマッピングできます。CAM はエンドポイントと対応するプロファイル、およびすべてのプロファイル名のリストを Cisco ISE プロファイラから定期的に取得します。

プロファイラ設定の変更を Cisco ISE プロファイラからプルするために、次の REST API フローが実装されます。

- NAC Manager のエンドポイントプル：エンドポイントの MAC アドレスと既知のエンドポイントの対応するプロファイルのリストをプルします。
- NAC Manager のプロファイルプル：プロファイル名を Cisco ISE プロファイラからプルします。

Cisco ISE プロファイラは、Cisco ISE と Cisco NAC アプライアンス リリース 4.9 との統合のモニタとトラブルシューティングに使用できるすべてのイベントを Cisco ISE モニタリング ペルソナに通知します。

Cisco ISE プロファイラ ログには、統合のモニタリングとトラブルシューティングに関する次のイベントが取り込まれます。

- NAC 設定の変更 (情報)
- NAC 通知イベント障害 (エラー)

Cisco Clean Access Manager の追加

Cisco ISE を Cisco NAC アプライアンス リリース 4.9 と統合すると、Cisco NAC 展開で Cisco ISE プロファイリング サービスを利用できます。

[NAC Managers] ページでは、複数の Clean Access Manager (CAM) を設定でき、登録した CAM をフィルタリングするためのオプションを使用できます。このページには、CAM が名前、説明、IP アドレス、および CAM でエンドポイント通知が有効になっているかどうかを示すステータスとともに表示されます。

-
- ステップ 1** [管理 (Administration)] > [ネットワーク リソース (Network Resources)] > [NAC Managers] を選択します。
- ステップ 2** [追加 (Add)] をクリックします。
- ステップ 3** Cisco Access Manager の名前を入力します。
- ステップ 4** CAM への接続を認証する Cisco ISE プロファイラからの REST API 通信を有効にする場合は、[ステータス (Status)] チェックボックスをオンにします。
- ステップ 5** 0.0.0.0 および 255.255.255.255 の IP アドレス以外の CAM の IP アドレスを入力します。
- ステップ 6** CAM のユーザインターフェイスにログインするために使用する CAM 管理者のユーザ名とパスワードを入力します。
- ステップ 7** [送信 (Submit)] をクリックします。
-

プロファイラ条件の作成

Cisco ISE のエンドポイント プロファイリング ポリシーを使用すると、ネットワーク上で検出されたエンドポイントを分類し、特定のエンドポイント ID グループに割り当てることができます。これらのエンドポイント プロファイリング ポリシーは、エンドポイントを分類し、グループ化するために Cisco ISE が評価するプロファイリング条件から構成されます。

始める前に

次のタスクを実行するには、スーパー管理者またはポリシー管理者である必要があります。

-
- ステップ 1** [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [条件 (Conditions)] > [プロファイリング (Profiling)] > [追加 (Add)] を選択します。
- ステップ 2** [エンドポイントプロファイリングポリシーの設定 \(1358 ページ\)](#) の説明に従って、フィールドに値を入力します。
- ステップ 3** [送信 (Submit)] をクリックして、プロファイラ条件を保存します。
- ステップ 4** さらに多くの条件を作成するには、この手順を繰り返します。
-

関連トピック

[プロファイラ条件](#) (662 ページ)

エンドポイント プロファイリング ポリシー ルール

ルールを定義すると、すでにポリシー要素ライブラリに作成および保存されているライブラリから 1 つ以上のプロファイリング条件を選択し、確実度係数の整数値を各条件に関連付けるか、例外アクションまたはネットワーク スキャンアクションをその条件に関連付けることが

できます。例外アクションまたはネットワーク スキャンアクションは、Cisco ISE がエンドポイントの分類全体に関するプロファイリングポリシーを評価しているときに、設定可能なアクションをトリガーするために使用します。

特定のポリシー内のルールが OR 演算子で個別に評価されると、各ルールの確実度メトリックは、エンドポイント プロファイルからエンドポイント カテゴリを決定するための全体的な照合の計算に使用されます。エンドポイント プロファイリング ポリシーのルールが一致した場合、そのプロファイリングポリシーおよび一致するポリシーは、それらがネットワーク上で動的に検出された場合のエンドポイントと同じです。

ルール内で論理的にグループ化される条件

エンドポイントプロファイリングポリシー（プロファイル）には、単一の条件またはAND演算子やOR演算子を使用して論理的に結合された複数の単一条件の組み合わせが含まれ、これらの条件と照合して、ポリシー内の特定のルールについてエンドポイントをチェック、分類、およびグループ化することができます。

条件は、収集されたエンドポイント属性値をエンドポイントの条件に指定されている値と照合するために使用されます。複数の属性をマッピングする場合は、条件を論理的にグループ化して、ネットワーク上のエンドポイントの分類に使用できます。ルールで対応する確実度メトリック（定義済みの整数値）が関連付けられている1つ以上の条件とエンドポイントを照合するか、または、条件に関連付けられた例外アクション、または条件に関連付けられたネットワーク スキャンアクションをトリガーすることができます。

確実度係数

プロファイリングポリシーの最小確実度メトリックは、エンドポイントの一致するプロファイルの評価します。エンドポイント プロファイリング ポリシーの各ルールには、プロファイリング条件に関連付けられた最小確実度メトリック（整数値）があります。確実度メトリックは、エンドポイント プロファイリング ポリシー内のすべての有効ルールに対して追加される尺度で、エンドポイント プロファイリング ポリシー内の各条件がエンドポイントの全体的な分類の改善にどの程度役立つかを測定します。

各ルールの確実度メトリックは、エンドポイント プロファイルからエンドポイント カテゴリを決定するための全体的な照合の計算に使用されます。すべての有効なルールの確実度メトリックが合計され、照合の確実度が求められます。この値は、エンドポイントプロファイリングポリシーに定義されている最小の確実度係数を超過する必要があります。デフォルトでは、すべての新しいプロファイリングポリシー ルールおよび事前に定義されたプロファイリングポリシーで、最小の確実度係数は 10 です。

エンドポイント プロファイリング ポリシーの作成

[プロファイリングポリシー（Profiling Policies）] ページを使用して、Cisco ISE の管理者として作成したエンドポイントプロファイリングポリシーおよび展開時に Cisco ISE によって提供されるエンドポイントプロファイリングポリシーを管理できます。

新しいプロファイリングポリシーを作成して、エンドポイントをプロファイリングするには、[新しいプロファイラ ポリシー (New Profiler Policy)] ページで次のオプションを使用します。

- ポリシー有効 (Policy Enabled)
- [ID グループの作成 (Create an Identity Group)] : 一致するエンドポイント ID グループを作成するか、またはエンドポイント ID グループ階層を使用するポリシーの場合
- 親ポリシー (Parent Policy)
- 関連 CoA タイプ (Associated CoA Type)



(注) [プロファイリングポリシー (Profiling Policies)] ページでエンドポイントポリシーを作成する場合は、Web ブラウザの停止ボタンを使用しないでください。このアクションによって、[新しいプロファイラ ポリシー (New Profiler Policy)] ページでのロードが停止され、アクセス時にリスト ページ内のその他のリスト ページおよびメニューがロードされ、リスト ページ内のフィルタ メニュー以外のすべてのメニューでの操作を実行できなくなります。リスト ページ内ですべてのメニューの操作を実行するには、Cisco ISE からログアウトし、再度ログインする必要がある場合があります。

類似した特性のプロファイリングポリシーを作成するには、すべての条件を再定義して新しいプロファイリングポリシーを作成するのではなく、エンドポイントプロファイリングポリシーを複製して変更することができます。

- ステップ 1 [ポリシー (Policy)] > [プロファイリング (Profiling)] > [プロファイリングポリシー (Profiling Policies)] を選択します。
- ステップ 2 [追加 (Add)] をクリックします。
- ステップ 3 作成する新しいエンドポイント ポリシーの名前と説明を入力します。[ポリシー有効 (Policy Enabled)] チェックボックスはデフォルトでオンになっており、エンドポイントのプロファイリング時に検証するエンドポイントプロファイリング ポリシーが含まれます。
- ステップ 4 有効範囲 1 ~ 65535 の最小の確実度係数の値を入力します。
- ステップ 5 [例外アクション (Exception Action)] ドロップダウン リストの隣にある矢印をクリックして、例外アクションを関連付けるか、[ネットワーク スキャン (NMAP) アクション (Network Scan (NMAP) Actions)] ドロップダウンリストの隣にある矢印をクリックして、ネットワーク スキャンアクションを関連付けます。
- ステップ 6 [ポリシーの ID グループの作成 (Create an Identity Group for the policy)] で次のオプションのいずれか 1 つを選択します。
 - はい、一致する ID グループを作成します (Yes, create matching Identity Group)
 - いいえ、既存の ID グループ階層を使用します (No, use existing Identity Group hierarchy)

- ステップ 7** [親ポリシー (Parent Policy)] ドロップダウンリストの隣の矢印をクリックして、新しいエンドポイントポリシーに親ポリシーを関連付けます。
- ステップ 8** [関連付ける CoA タイプ (Associated CoA Type)] ドロップダウンリストで、関連付ける CoA タイプを選択します。
- ステップ 9** ルールをクリックし、条件を追加して、各条件の確実度係数の整数値を関連付けるか、エンドポイントの全体的な分類のその条件の例外アクションまたはネットワーク スキャンアクションを関連付けます。
- ステップ 10** [送信 (Submit)] をクリックしてエンドポイントポリシーを追加するか、または [新しいプロファイラポリシー (New Profiler Policy)] ページの [プロファイラ ポリシー リスト (Profiler Policy List)] リンクをクリックして [プロファイリング ポリシー (Profiling Policies)] ページに戻ります。

エンドポイント プロファイリング ポリシーごとの許可変更の設定

Cisco ISE の許可変更 (CoA) タイプのグローバル コンフィギュレーションに加えて、各エンドポイント プロファイリング ポリシーに関連付けられた特定のタイプの CoA も発行するように設定できます。

グローバル CoA なしタイプの設定は、エンドポイント プロファイリング ポリシーで設定された各 CoA タイプを上書きします。グローバル CoA タイプが CoA なしタイプ以外に設定されている場合、各エンドポイント プロファイリング ポリシーはグローバル CoA の設定を上書きできます。

CoA がトリガーされると、各エンドポイント プロファイリング ポリシーは、次のように実際の CoA タイプを決定できます。

- [全般設定 (General Settings)] : これは、グローバル コンフィギュレーションごとに CoA を発行するすべてのエンドポイント プロファイリング ポリシーのデフォルトの設定です。
- [CoA なし (No CoA)] : この設定はグローバル コンフィギュレーションを上書きし、そのプロファイルの CoA を無効にします。
- [ポート バウンス (Port Bounce)] : この設定は、グローバル ポート バウンスおよび再認証設定タイプを上書きし、ポート バウンス CoA を発行します。
- [再認証 (Reauth)] : この設定は、グローバル ポート バウンスおよび再認証設定タイプを上書きし、再認証 CoA を排出します。



(注) プロファイラ グローバル CoA 設定がポート バウンス (または再認証) に設定されている場合は、モバイル デバイスの BYOD フローが切断されないように、対応するエンドポイント プロファイリング ポリシーを [CoA なし (No CoA)]、[ポリシーごとの CoA (per-policy CoA)] オプションを指定して設定していることを確認します。

グローバルおよびエンドポイント プロファイリング ポリシー設定に基づいて各場合に発行されたすべての CoA タイプと実際の CoA タイプが組み合わされた設定については、次の概要を参照してください。

表 47: 設定のさまざまな組み合わせに発行された CoA タイプ

グローバル CoA タイプ	ポリシーごとに設定されたデフォルトの CoA タイプ	ポリシーごとの CoA なしタイプ	ポリシーごとのポート バウンス タイプ	ポリシーごとの再認証タイプ
CoA なし (No CoA)	CoA なし (No CoA)	CoA なし (No CoA)	CoA なし (No CoA)	CoA なし (No CoA)
ポート バウンス	ポート バウンス	CoA なし (No CoA)	ポート バウンス	再認証 (Re-Auth)
再認証 (Reauth)	再認証 (Reauth)	CoA なし (No CoA)	ポート バウンス	再認証 (Re-Auth)

エンドポイント プロファイリング ポリシーのインポート

エクスポート機能で作成できる同じ形式を使用して、XML ファイルからエンドポイント プロファイリング ポリシーをインポートできます。親ポリシーが関連付けられている、新しく作成されたプロファイリング ポリシーをインポートする場合は、子ポリシーを定義する前に親ポリシーを定義しておく必要があります。

インポート ファイルでは、エンドポイント プロファイリング ポリシーが階層構造になっており、最初に親ポリシー、次にポリシーに定義されているルールとチェックとともにインポートしたプロファイルが含まれます。

-
- ステップ 1** [ポリシー (Policy)] > [プロファイリング (Profiling)] > [プロファイリング (Profiling)] > [プロファイリング ポリシー (Profiling Policies)] を選択します。
- ステップ 2** [インポート (Import)] をクリックします。
- ステップ 3** [参照 (Browse)] をクリックして、前にエクスポートしてこれからインポートするファイルを特定します。
- ステップ 4** [送信 (Submit)] をクリックします。
- ステップ 5** [プロファイリング ポリシー (Profiling Policies)] ページに戻るには、[プロファイラ ポリシー リスト (Profiler Policy List)] リンクをクリックします。
-

エンドポイント プロファイリング ポリシーのエクスポート

他の Cisco ISE 展開にエンドポイント プロファイリング ポリシーをエクスポートできます。または、XML ファイルを独自のポリシーを作成するためのテンプレートとして使用してインポート

トできます。ファイルをシステムのデフォルトの場所にダウンロードして、後でインポートに使用することもできます。

エンドポイント プロファイリング ポリシーをエクスポートする際にダイアログが表示され、適切なアプリケーションで `profiler_policies.xml` を開くか、保存するように要求されます。これは XML 形式のファイルで、Web ブラウザまたは他の適切なアプリケーションで開くことができます。

ステップ 1 [ポリシー (Policy)] > [プロファイリング (Profiling)] > [プロファイリング (Profiling)] > [プロファイリング (Profiling Policies)] を選択します。

ステップ 2 [エクスポート (Export)] を選択し、次のいずれかを選択します。

- [選択済みをエクスポート (Export Selected)] : [プロファイリング ポリシー (Profiling Policies)] ページで選択済みのエンドポイント プロファイリングのポリシーだけをエクスポートできます。
- [選択済みとエンドポイントをエクスポート (Export Selected with Endpoints)] : 選択済みのエンドポイント プロファイリングポリシーと、選択済みのエンドポイント プロファイリングポリシーでプロファイリングされたエンドポイントをエクスポートできます。
- [すべてエクスポート (Export All)] : デフォルトでは、[プロファイリング ポリシー (Profiling Policies)] ページのすべてのプロファイリングポリシーをエクスポートできます。

ステップ 3 [OK] をクリックして、`profiler_policies.xml` ファイルのエンドポイント プロファイリングポリシーをエクスポートします。

事前定義されたエンドポイント プロファイリング ポリシー

Cisco ISE を展開するとき、Cisco ISE には事前定義されたデフォルトのプロファイリングポリシーが含まれます。その階層構造を使用して、ネットワーク上の識別されたエンドポイントを分類し、それらを一致するエンドポイント ID グループに割り当てることができます。エンドポイント プロファイリングポリシーは階層的であるため、[プロファイリング ポリシー (Profiling Policies)] ページにはデバイスの一般的な（親）ポリシーと、親ポリシーが [プロファイリング ポリシー (Profiling Policies)] リストページに関連付けられている子ポリシーが表示されます。

[プロファイリング ポリシー (Profiling Policies)] ページには、エンドポイント プロファイリングポリシーとともに、その名前、タイプ、説明、およびステータス（検証が有効になっているかどうか）が表示されます。

エンドポイント プロファイリングポリシータイプは、次のように分類されます。

- シスコ提供 : Cisco ISE で事前定義されたエンドポイント プロファイリングポリシーはシスコ提供タイプとして識別されます。

- 管理者による変更：事前定義されたエンドポイントプロファイリングポリシーを変更したときに、エンドポイントプロファイリングポリシーは管理者による変更タイプとして識別されます。Cisco ISE では、事前定義されたエンドポイントプロファイリングポリシーに行った変更がアップグレード時に上書きされます。

管理者によって変更されたポリシーは削除できますが、Cisco ISE によりシスコ提供のポリシーの最新バージョンで置き換えられます。

- 管理者作成：作成したエンドポイントプロファイリングポリシー、またはシスコ提供のエンドポイントプロファイリングポリシーを複製したときのエンドポイントプロファイリングポリシーは、管理者作成タイプとして識別されます。

一連のエンドポイントの一般的なポリシー（親）を作成して、その子がルールと条件を継承できるようにすることを推奨します。エンドポイントを分類する必要がある場合は、エンドポイントをプロファイリングするときに、まずエンドポイントプロファイルを親ポリシーと、次にその子孫（子）ポリシーと照合する必要があります。

たとえば、Cisco-Device は、すべてのシスコデバイスの一般的なエンドポイントプロファイリングのポリシーであり、シスコデバイスの他のポリシーは、Cisco-Device の子です。エンドポイントを Cisco-IP-Phone 7960 として分類する必要がある場合は、まずこのエンドポイントのエンドポイントプロファイルの親の Cisco-Device ポリシー、その子の Cisco-IP-Phone ポリシーと照合する必要があります、その後さらに分類するために Cisco-IP-Phone 7960 プロファイリングポリシーと照合します。

アップグレード中に上書きされる事前定義されたエンドポイントプロファイリングポリシー

[プロファイリングポリシー (Profiling Policies)] ページで既存のエンドポイントプロファイリングポリシーを編集できます。また、事前定義されたエンドポイントプロファイリングポリシーを変更するときは、事前定義されたエンドポイントプロファイルのコピーにすべての設定を保存する必要があります。

アップグレード時に、事前定義されたエンドポイントプロファイルに保存した設定が上書きされます。

エンドポイントプロファイリングポリシーを削除できない

[プロファイリングポリシー (Profiling Policies)] ページで選択したエンドポイントプロファイリングポリシーまたはすべてのエンドポイントプロファイリングポリシーを削除できます。デフォルトでは、[プロファイリングポリシー (Profiling Policies)] ページからすべてのエンドポイントプロファイリングポリシーを削除できます。[プロファイリングポリシー (Profiling Policies)] ページですべてのエンドポイントプロファイリングポリシーを選択して削除しようとしても、エンドポイントプロファイリングポリシーが他のエンドポイントプロファイリングポリシーにマッピングされた親ポリシーであるか、または許可ポリシーにマッピングされ、

かつ他のエンドポイント プロファイリング ポリシーの親ポリシーである場合、そのエンドポイント プロファイリング ポリシーは削除できません。

次の例を参考にしてください。

- シスコ提供のエンドポイント プロファイリング ポリシーは削除できません。
- エンドポイント プロファイルが他のエンドポイント プロファイルの親として定義されている場合は、[プロファイリング ポリシー (Profiling Policies)] ページで親プロファイルは削除できません。たとえば、Cisco-Device は、シスコ デバイスの他のエンドポイント プロファイリング ポリシーの親です。
- 許可ポリシーにマッピングされているエンドポイント プロファイルは削除できません。たとえば、Cisco-IP-Phone は Profiled Cisco IP Phones 許可ポリシーにマッピングされ、Cisco IP Phone の他のエンドポイント プロファイリング ポリシーの親です。

Draeger 医療機器用の事前定義済みプロファイリング ポリシー

Cisco ISE のデフォルトのエンドポイント プロファイルには、Draeger 医療機器用の一般的なポリシー、Draeger-Delta 医療機器用のポリシー、および Draeger-M300 医療機器用のポリシーが含まれます。両方の医療機器にポート 2050 と 2150 があるため、デフォルトの Draeger エンドポイント プロファイリング ポリシーを使用しても、Draeger-Delta 医療機器と Draeger-M300 医療機器を分類できません。

使用中の環境では、これらの Draeger デバイスにポート 2050 と 2150 があるため、デフォルトの Draeger-Delta and Draeger-M300 エンドポイント プロファイリング ポリシーでデバイスの宛先 IP アドレスのチェックに加えて、これらの医療機器を区別できるようにルールを追加する必要があります。

Cisco ISE には、Draeger 医療機器のエンドポイント プロファイリング ポリシーで使用される次のプロファイリング条件があります。

- ポート 2000 が含まれる Draeger-Delta-PortCheck1
- ポート 2050 が含まれる Draeger-Delta-PortCheck2
- ポート 2100 が含まれる Draeger-Delta-PortCheck3
- ポート 2150 が含まれる Draeger-Delta-PortCheck4
- ポート 1950 が含まれる Draeger-M300PortCheck1
- ポート 2050 が含まれる Draeger-M300PortCheck2
- ポート 2150 が含まれる Draeger-M300PortCheck3

不明なエンドポイントのエンドポイント プロファイリング ポリシー

既存のプロファイルに一致せず、Cisco ISE でプロファイリングできないエンドポイントは、不明なエンドポイントです。不明プロファイルは、エンドポイントについて収集された属性が

Cisco ISE の既存のプロファイルと一致しない場合にそのエンドポイントに割り当てられるデフォルトのシステム プロファイリング ポリシーです。

不明プロファイルは次のシナリオで割り当てられます。

- エンドポイントが Cisco ISE で動的に検出され、そのエンドポイントに一致するエンドポイントプロファイリング ポリシーがない場合、エンドポイントは不明プロファイルに割り当てられます。
- エンドポイントが Cisco ISE で静的に追加され、静的に追加されたエンドポイントに一致するエンドポイントプロファイリング ポリシーがない場合、エンドポイントは不明プロファイルに割り当てられます。

ネットワークにエンドポイントを静的に追加した場合、そのエンドポイントは Cisco ISE のプロファイリングサービスによってプロファイリングされません。不明プロファイルは適切なプロファイルに後で変更できます。割り当てたプロファイリングポリシーは、Cisco ISE によって再プロファイリングされることはありません。

静的に追加されたエンドポイントのエンドポイントプロファイリングポリシー

静的に追加されたエンドポイントをプロファイリングするために、プロファイリングサービスは、新しい **MATCHEDPROFILE** 属性をエンドポイントに追加することによって、エンドポイントのプロファイルを計算します。計算されたプロファイルは、そのエンドポイントが動的にプロファイリングされるときのエンドポイントの実際のプロファイルです。これにより、静的に追加されたエンドポイントの計算されたプロファイルと動的にプロファイリングされたエンドポイントに一致するプロファイルの間の不一致を見つけることができます。

スタティックIPデバイスのエンドポイントプロファイリングポリシー

静的に割り当てられた IP アドレスを持つエンドポイントがある場合、そのスタティック IP デバイスのプロファイルを作成できます。

スタティック IP アドレスが割り当てられているエンドポイントをプロファイリングするには、RADIUS プローブまたは SNMP クエリー プローブと SNMP トラップ プローブを有効にする必要があります。

エンドポイント プロファイリング ポリシーの一致

1つ以上のルールで定義されているプロファイリング条件がプロファイリングポリシーに一致する場合、Cisco ISE は、エンドポイント用に選択されたポリシーを、評価されたポリシーではなく、一致したポリシーであると常に見なします。ここで、そのエンドポイントのスタティック割り当てのステータスがシステムで **false** に設定されます。ただし、エンドポイントの編集時にスタティック割り当て機能を使用して、システム内の既存のプロファイリングポリシーに静的に再割り当てした後は、**true** に設定されることがあります。

次は、エンドポイントの一致したポリシーに適用されます。

- スタティックに割り当てられたエンドポイントでは、プロファイリング サービスは **MATCHEDPROFILE** を計算します。
- 動的に割り当てられたエンドポイントでは、**MATCHEDPROFILE** は一致するエンドポイント プロファイルと同じです。

ダイナミック エンドポイントに一致するプロファイリング ポリシーは、プロファイリング ポリシーで定義された1つ以上のルールを使用して特定できます。また、分類のために、必要に応じてエンドポイント ID グループを割り当てることができます。

エンドポイントが既存のポリシーにマッピングされる場合、プロファイリングサービスは、一連のポリシーが一致する最も近い親プロファイルをプロファイリング ポリシーの階層で検索し、エンドポイントを適切なエンドポイント ポリシーに割り当てます。

許可に使用するエンドポイント プロファイリング ポリシー

許可ルールにエンドポイント プロファイリング ポリシーを使用できます。このとき、エンドポイント プロファイリング ポリシーのチェックを含めるように属性として新しい条件を作成できます。属性値は、エンドポイント プロファイリング ポリシーの名前になります。エンドポイント プロファイリング ポリシーを、エンドポイント辞書から選択できます。エンドポイント プロファイリング ポリシーには、属性 **PostureApplicable**、**EndPointPolicy**、**LogicalProfile** および **BYODRegistration** が含まれています。

EndPointPolicy、**BYODRegistration** および ID グループの組み合わせを含む許可ルールを定義できます。

エンドポイント プロファイリング ポリシーの論理プロファイルによるグループ化

論理プロファイルは、エンドポイント プロファイリング ポリシーがシスコ提供か、管理者作成かに関係なく、プロファイルまたは関連付けられているプロファイルのカテゴリのコンテナです。エンドポイント プロファイリング ポリシーは、複数の論理プロファイルに関連付けることができます。

許可ポリシー条件で論理プロファイルを使用して、プロファイルのカテゴリでネットワーク全体のアクセス ポリシーの作成に役立てることができます。許可の単純条件を作成して、許可ルールに含めることができます。許可条件で使用できる属性と値のペアは、論理プロファイル（属性）および論理プロファイルの名前（値）であり、エンドポイント システム デictionary内にあります。

たとえば、カテゴリに一致するエンドポイント プロファイリング ポリシーを論理プロファイルに割り当てることによって、**Android**、**Apple iPhone**、**Blackberry** などのすべてのモバイルデバイスの論理プロファイルを作成できます。Cisco ISE には、すべての IP フォンのデフォルト

の論理プロファイルである IP-Phone が含まれ、IP-Phone には、IP-Phone、Cisco IP-Phone、Nortel-IP-Phone-2000-Series、および Avaya-IP-Phone プロファイルが含まれます。

論理プロファイルの作成

エンドポイントプロファイリング ポリシーのカテゴリをグループ化するために使用できる論理プロファイルを作成でき、それにより、プロファイルまたは関連付けられているプロファイルのカテゴリ全体を作成できます。エンドポイントプロファイリング ポリシーを割り当てられたセットから削除して、使用可能なセットに戻すこともできます。ロジカルプロファイルの詳細については、[エンドポイントプロファイリングポリシーの論理プロファイルによるグループ化（805 ページ）](#) を参照してください。

-
- ステップ 1 [ポリシー (Policy)] > [プロファイリング (Profiling)] > [プロファイリング (Profiling)] > [論理プロファイル (Logical Profiles)] を選択します。
 - ステップ 2 [追加 (Add)] をクリックします。
 - ステップ 3 [名前 (Name)] と [説明 (Description)] のテキストボックスに新しい論理プロファイルの名前と説明を入力します。
 - ステップ 4 [使用可能なポリシー (Available Policies)] からエンドポイントプロファイリング ポリシーを選択して、論理プロファイルに割り当てます。
 - ステップ 5 右矢印をクリックして、選択したエンドポイントプロファイリング ポリシーを [割り当てられたポリシー (Assigned Policies)] に移動します。
 - ステップ 6 [送信 (Submit)] をクリックします。
-

プロファイリング例外アクション

例外アクションは、エンドポイントプロファイリングポリシーで参照できる単一の設定可能なアクションであり、アクションに関連付けられている例外条件が満たされるとトリガーされます。

例外アクションのタイプは次のいずれかになります。

- シスコ提供：シスコ提供の例外アクションは削除できません。Cisco ISE では、Cisco ISE のエンドポイントのプロファイリングするときに、次の編集不能なプロファイリング例外アクションがトリガーされます。
 - 許可変更：エンドポイントが許可ポリシーで使用されるエンドポイント ID グループに対して追加または削除される場合、プロファイリングサービスは許可変更を発行します。
 - エンドポイント削除：エンドポイントが [エンドポイント (Endpoints)] ページでシステムから削除されるか、Cisco ISE ネットワーク上で編集ページから不明プロファイルに再割り当てされると、Cisco ISE で例外アクションがトリガーされ、CoA が発行されます。

- **FirstTimeProfiled** : エンドポイントが Cisco ISE で初めてプロファイリングされ、そのエンドポイントのプロファイルが不明プロファイルから既存のプロファイルに変更されて、そのエンドポイントが Cisco ISE ネットワーク上で認証に失敗すると、Cisco ISE で例外アクションがトリガーされ、CoA が発行されます。
- **管理者作成** : Cisco ISE では、作成したプロファイリング例外アクションがトリガーされます。

例外アクションの作成

1 つ以上の例外ルールを定義し、1 つのプロファイリング ポリシーに関連付けることができます。この関連付けにより、Cisco ISE でエンドポイントのプロファイリングする際にプロファイリング ポリシーが一致し、少なくとも 1 つの例外ルールが一致する場合、例外アクション（単一の設定可能なアクション）がトリガーされます。

-
- ステップ 1** [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] > [プロファイリング (Profiling)] > [例外アクション (Exception Actions)] を選択します。
- ステップ 2** [追加 (Add)] をクリックします。
- ステップ 3** [名前 (Name)] と [説明 (Description)] のテキスト ボックスに例外アクションの名前と説明を入力します。
- ステップ 4** [CoA アクション (CoA Action)] チェックボックスをオンにします。
- ステップ 5** [ポリシー割り当て (Policy Assignment)] ドロップダウン リストをクリックしてエンドポイント ポリシーを選択します。
- ステップ 6** [送信 (Submit)] をクリックします。
-

ポリシーおよびIDグループのスタティック割り当てによるエンドポイントの作成

[エンドポイント (Endpoints)] ページでエンドポイントの MAC アドレスを使用して、新しいエンドポイントを静的に作成できます。また、スタティック割り当ての [エンドポイント (Endpoints)] ページで、エンドポイント プロファイリング ポリシーおよび ID グループを選択できます。

通常のモバイルデバイス (MDM) エンドポイントは、[エンドポイント ID (Endpoints Identities)] リストに表示されます。リストページには、[ホスト名 (Hostname)]、[デバイスタイプ (Device Type)]、[デバイス ID (Device ID)] など、MDM エンドポイントの属性のカラムが表示されます。[スタティック割り当て (Static Assignment)]、[スタティック グループ割り当て (Static Group Assignment)] などのその他のカラムは、デフォルトでは表示されません。



(注) このページを使用して、MDM エンドポイントを追加、編集、削除、インポートまたはエクスポートすることはできません。

- ステップ 1** [ワーク センター (Work Centers)] > [ネットワーク アクセス (Network Access)] > [ID (Identities)] > [エンドポイント (Endpoints)] を選択します。
- ステップ 2** [追加 (Add)] をクリックします。
- ステップ 3** エンドポイントの MAC アドレスをコロンで区切られた 16 進表記で入力します。
- ステップ 4** [ポリシー割り当て (Policy Assignment)] ドロップダウン リストから一致するエンドポイント ポリシーを選択して、スタティック割り当てステータスをダイナミックからスタティックに変更します。
- ステップ 5** [スタティック割り当て (Static Assignment)] チェックボックスをオンにして、エンドポイントに割り当てられたスタティック割り当てのステータスをダイナミックからスタティックに変更します。
- ステップ 6** [ID グループ割り当て (Identity Group Assignment)] ドロップダウン リストから、新しく作成されたエンドポイントを割り当てるエンドポイント ID グループを選択します。
- ステップ 7** エンドポイント ID グループのダイナミック割り当てをスタティックに変更するには、[スタティック グループ割り当て (Static Group Assignment)] チェックボックスをオンにします。
- ステップ 8** [送信 (Submit)] をクリックします。

CSV ファイルからのエンドポイントのインポート

Cisco ISE テンプレートから作成した CSV ファイルからエンドポイントをインポートし、エンドポイントの詳細を使用して更新することができます。ISE からエクスポートされたエンドポイントには約 75 個の属性が含まれているため、別の ISE 展開に直接インポートすることはできません。インポートが許可されていない列が CSV ファイルにある場合は、列のリストを含むメッセージが表示されます。ファイルを再度インポートする前に、指定された列を削除する必要があります。



(注) エンドポイントのカスタム属性をインポートするには、正しいデータ タイプを使用して [管理 (Administration)] > [ID の管理 (Identity Management)] > [設定 (Settings)] > [エンドポイント カスタム属性 (Endpoint Custom Attributes)] ページで CSV ファイルと同じカスタム属性を作成する必要があります。これらのコマンドには、「CUSTOM.」というプレフィックスを付けてエンドポイント属性と区別する必要があります。

インポートできる属性は約 30 あります。このリストには、MACAddress、EndPointPolicy、IdentityGroup が含まれています。オプション属性は次のとおりです。

説明	PortalUser	LastName
PortalUser.GuestType	PortalUser.FirstName	EmailAddress

PortalUser.Location	デバイスタイプ (Device Type)	host-name
PortalUser.GuestStatus	StaticAssignment	参照先
PortalUser.CreationType	StaticGroupAssignment	MDMEnrolled
PortalUser.EmailAddress	User-Name	MDMOSVersion
PortalUser.PhoneNumber	DeviceRegistrationStatus	MDMServerName
PortalUser.LastName	AUPAccepted	MDMServerID
PortalUser.GuestSponsor	FirstName	BYODRegistration
CUSTOM.<custom attribute name>	—	—

ファイルヘッダーは、デフォルトのインポートテンプレートで指定されている形式にして、エンドポイントのリストが次の順序で表示されるようにする必要があります。MACAddress、EndpointPolicy、IdentityGroup、<オプション属性として上に記載されている属性のリスト>。次のファイルテンプレートを作成できます。

- MACAddress
- MACAddress, EndPointPolicy
- MACAddress, EndPointPolicy, IdentityGroup
- MACAddress, EndPointPolicy, IdentityGroup, <オプション属性として上に記載されている属性のリスト>

MAC アドレスを除くすべての属性値は、CSV ファイルからエンドポイントをインポートする際に省略可能です。特定の値のないエンドポイントをインポートする場合も、値はカンマで区切られます。

次の例を参考にしてください。

- MAC1, Endpoint Policy1, Endpoint Identity Group1
- MAC2
- MAC3, Endpoint Policy3
- MAC4, , Endpoint Identity Group4
- MAC5, , Endpoint Identity Group5, MyDescription, MyPortalUser, など

ステップ 1 [コンテキストの可視性 (Context Visibility)] > [エンドポイント (Endpoints)] > [インポート (Import)] の順に選択します。

ステップ 2 [ファイルからインポート (Import from File)] をクリックします。

ステップ 3 [参照 (Browse)] をクリックして、作成済みの CSV ファイルを見つけます。

ステップ 4 [送信 (Submit)] をクリックします。

エンドポイントで使用可能なデフォルトのインポート テンプレート

エンドポイントのインポートに使用できるエンドポイントを更新できるテンプレートを生成できます。デフォルトで、[テンプレートの生成 (Generate a Template)] リンクを使用して、Microsoft Office Excel アプリケーションで CSV ファイルを作成し、このファイルをシステム上にローカルに保存できます。ファイルは [コンテキストの可視性 (Context Visibility)] > [エンドポイント (Endpoints)] > [インポート (Import)] > [ファイルからインポート (Import from File)] にあります。[テンプレートの生成 (Generate a Template)] リンクを使用してテンプレートを作成でき、Cisco ISE サーバは、[template.csv を開く (Opening template.csv)] ダイアログを表示します。このダイアログを使用すると、デフォルトの template.csv ファイルを開いたり、template.csv ファイルをシステム上にローカルに保存できます。このダイアログで template.csv ファイルを開くことを選択した場合、このファイルは Microsoft Office Excel アプリケーションで開かれます。デフォルトの template.csv ファイルには、MAC アドレス、エンドポイント ポリシー、エンドポイント ID グループ、およびその他のオプション属性が表示されるヘッダー行が含まれています。

エンドポイントの MAC アドレス、エンドポイント プロファイリング ポリシー、エンドポイント ID グループを、インポートするオプションの属性値とともに更新し、新しいファイル名を使用してファイルを保存します。このファイルをエンドポイントのインポートのために使用できます。[テンプレートの生成 (Generate a Template)] リンクを使用したときに作成される template.csv ファイルのヘッダー行を参照してください。

表 48: CSV テンプレート ファイル

MAC	EndPointPolicy	IdentityGroup	その他のオプションの属性
11:11:11:11:11:11	Android	プロファイル済み	<Empty><Value>

インポート中の不明なエンドポイントの再プロファイリング

インポートに使用するファイルに、MAC アドレスを持つエンドポイントがあり、それらに割り当てられているエンドポイント プロファイリング ポリシーが不明プロファイルである場合、これらのエンドポイントはインポート中に Cisco ISE でただちに一致するエンドポイント プロファイリング ポリシーに再プロファイリングされます。ただし、不明プロファイルに静的に割り当てられることはありません。エンドポイントに割り当てられているエンドポイント プロファイリング ポリシーが CSV ファイルにない場合、これらのエンドポイントは不明プロファイルに割り当てられ、一致するエンドポイント プロファイリング ポリシーに再プロファイリングされます。次に、Cisco ISE が、インポート中に Xerox_Device プロファイルに一致する不明プロファイルをどのように再プロファイリングするか、および割り当てられていないエンドポイントをどのように再プロファイリングするかを示します。

表 49: 不明プロファイル：ファイルからのインポート

MAC アドレス	Cisco ISE でのインポート前に割り当てられたエンドポイントプロファイリングポリシー	Cisco ISE でのインポート後に割り当てられたエンドポイントプロファイリングポリシー
00:00:00:00:01:02	不明。	Xerox-Device
00:00:00:00:01:03	不明。	Xerox-Device
00:00:00:00:01:04	不明。	Xerox-Device
00:00:00:00:01:05	プロファイルがエンドポイントに割り当てられていない場合、そのエンドポイントは不明プロファイルに割り当てられ、一致するプロファイルに再プロファイリングされます。	Xerox-Device

インポートされない無効な属性を持つエンドポイント

CSV ファイルに存在するエンドポイントのいずれかに無効な属性がある場合、エンドポイントはインポートされず、エラー メッセージが表示されます。

たとえば、エンドポイントがインポートに使用されるファイル内で無効なプロファイルに割り当てられている場合、それらのエンドポイントは、Cisco ISE には一致するプロファイルがないためインポートされません。エンドポイントが CSV ファイル内の無効なプロファイルに割り当てられている場合、それらのエンドポイントがインポートされない仕組みを下に示します。

表 50: 無効なプロファイル：ファイルからのインポート

MAC アドレス (MAC Address)	Cisco ISE でのインポート前に割り当てられたエンドポイントプロファイリングポリシー	Cisco ISE でのインポート後に割り当てられたエンドポイントプロファイリングポリシー
00:00:00:00:01:02	不明。	Xerox-Device
00:00:00:00:01:05	00:00:00:00:01:05 などのエンドポイントが Cisco ISE 使用可能なプロファイル以外の無効なプロファイルに割り当てられている場合、Cisco ISE では、ポリシー名が無効で、エンドポイントがインポートされないことを示す警告メッセージが表示されます。	エンドポイントは、Cisco ISE 内に一致するプロファイルがないためインポートされません。

LDAP サーバからのエンドポイントのインポート

エンドポイントの MAC アドレス、関連するプロファイル、およびエンドポイント ID グループを LDAP サーバからセキュアにインポートできます。

始める前に

エンドポイントをインポートする前に、LDAP サーバがインストールされていることを確認します。

LDAP サーバからインポートするには、接続設定値およびクエリー設定値を設定する必要があります。接続設定値またはクエリー設定値が Cisco ISE で間違っていて設定されていると、「LDAP インポートが失敗： (LDAP import failed:)」エラー メッセージが表示されます。

ステップ 1 [コンテキストの可視性 (Context Visibility)] > [エンドポイント (Endpoints)] > [インポート (Import)] > [LDAP からのインポート (Import From LDAP)] の順に選択します。

ステップ 2 接続設定の値を入力します。

ステップ 3 クエリー設定の値を入力します。

ステップ 4 [送信 (Submit)] をクリックします。

カンマ区切り形式ファイルを使用したエンドポイントのエクスポート

選択したエンドポイントまたはすべてのエンドポイントを Cisco ISE サーバから CSV ファイルでエクスポートできます。このファイルで、エンドポイントは MAC アドレス、エンドポイント プロファイリング ポリシー、およびエンドポイント ID グループと、約 75 属性とともに一覧表示されます。Cisco ISE で作成されたカスタム属性は、CSV ファイルにエクスポートすることもでき、「CUSTOM.」というプレフィックスが付けられて、他のエンドポイント属性と区別できます。



(注) 1 つの導入からエクスポートされたエンドポイントのカスタム属性を別の導入にインポートするには、[管理 (Administration)] > [ID の管理 (Identity Management)] > [設定 (Settings)] > [エンドポイント カスタム属性 (Endpoint Custom Attributes)] ページで同じカスタム属性を作成し、最初の導入で指定したのと同じデータ タイプを使用する必要があります。

[すべてエクスポート (Export All)] では Cisco ISE のすべてのエンドポイントがエクスポートされ、[選択済みのみをエクスポート (Export Selected)] ではユーザが選択したエンドポイントのみがエクスポートされます。デフォルトでは、profiler_endpoints.csv が CSV ファイルであり、Microsoft Office Excel が CSV ファイルを開くデフォルトのアプリケーションです。

ステップ 1 [コンテキストの可視性 (Context Visibility)] > [エンドポイント (Endpoints)] を選択します。

ステップ 2 [エクスポート (Export)] をクリックし、次のいずれかを選択します。

- [選択済みをエクスポート (Export Selected)] : [エンドポイント (Endpoints)] ページで選択したエンドポイントだけをエクスポートできます。
- [すべてエクスポート (Export All)] : デフォルトで、[エンドポイント (Endpoints)] ページのすべてのエンドポイントをエクスポートできます。

ステップ 3 [OK] をクリックして、profiler_endpoints.csv ファイルを保存します。

識別されたエンドポイント

Cisco ISE では、ネットワークに接続してネットワーク リソースを使用する識別されたエンドポイントが、[エンドポイント (Endpoints)] ページに表示されます。エンドポイントは、通常、有線および無線のネットワーク アクセス デバイスと VPN を介してネットワークに接続するネットワーク対応デバイスです。エンドポイントとして、パーソナルコンピュータ、ラップトップ、IP Phone、スマートフォン、ゲームコンソール、プリンタ、ファクス機などがあります。

16進数形式で表したエンドポイントの MAC アドレスは、常にエンドポイントの一意の表現ですが、それらに関連付けられた属性と値のさまざまなセット（属性と値のペアと呼ばれる）でエンドポイントを識別することもできます。エンドポイントの属性のさまざまなセットは、エンドポイント機能、ネットワーク アクセス デバイスの機能と設定、およびこれらの属性の収集に使用する方法（プローブ）に基づいて収集できます。

動的にプロファイリングされるエンドポイント

エンドポイントは、ネットワークで検出されると、設定されているプロファイリングエンドポイントのプロファイリングポリシーに基づいて動的にプロファイリングされ、プロファイルに応じて一致するエンドポイント ID グループに割り当てられます。

静的にプロファイリングされるエンドポイント

MAC アドレスを使用してエンドポイントを作成し、Cisco ISE のエンドポイント ID グループとともにプロファイルをそのエンドポイントに割り当てると、エンドポイントを静的にプロファイリングすることができます。Cisco ISE では、静的に割り当てられたエンドポイントに対して、プロファイリングポリシーおよび ID グループを再割り当てしません。

不明なエンドポイント

エンドポイントに対して一致するプロファイリングポリシーがない場合、不明なプロファイリングポリシー（「不明」）を割り当てることで、エンドポイントを不明としてプロファイリングできます。不明なエンドポイント ポリシーにプロファイリングされたエンドポイントの場合、そのエンドポイントに対して収集された属性または属性セットを使用してプロファイルを作成する必要があります。いずれのプロファイルにも一致しないエンドポイントは、不明なエンドポイント ID グループにグループ化されます。

識別されたエンドポイントの、ポリシー サービス ノード データベースへのローカル保存

Cisco ISE は識別されたエンドポイントをポリシー サービス ノードのデータベースにローカルに書き込みます。エンドポイントをデータベースにローカル保存した後は、それらのエンドポイントは、重要な属性がエンドポイントで変更され、他のポリシーサービスノードデータベースに複製されているときにのみ、管理ノードデータベースで利用できる（リモート書き込み）ようになります。

重要な属性は次のとおりです。

- ip
- EndPointPolicy
- MatchedValue
- StaticAssignment
- StaticGroupAssignment
- MatchedPolicyID
- NmapSubnetScanID
- PortalUser
- DeviceRegistrationStatus
- BYODRegistration

Cisco ISE でエンドポイント プロファイル定義を変更した場合、すべてのエンドポイントを再プロファイリングする必要があります。エンドポイント属性を収集するポリシーサービスノードが、これらのエンドポイントの再プロファイリングを担当します。

あるポリシーサービスノードが、最初は別のポリシーサービスノードによって属性が収集されていたエンドポイントに関する属性を収集し始めると、エンドポイントの所有権が現在のポリシーサービスノードに移ります。新しいポリシーサービスノードは、前のポリシーサービスノードから最新の属性を取得して、すでに収集されている属性と調整します。

重要な属性がエンドポイントで変更されると、エンドポイントの属性は管理ノードデータベースに自動的に保存され、エンドポイントの最新の重要な変更を使用できます。エンドポイントを所有するポリシーサービスノードが何らかの理由で使用できない場合、管理 ISE ノードが所有者を失ったエンドポイントを再プロファイリングします。また、このようなエンドポイントに対して新しいポリシーサービスノードを設定する必要があります。

クラスタのポリシー サービス ノード

Cisco ISE では、ポリシーサービスノードグループをクラスタとして使用するため、クラスタ内の複数のノードが同じエンドポイントの属性を収集するときに、エンドポイント属性を交換できます。1つのロードバランサの背後に存在する、すべてのポリシーサービスノードに対するクラスタを作成することを推奨します。

現在のオーナー以外の別のノードが同じエンドポイントの属性を受信した場合、属性をマージし、所有権の変更が必要かどうかを決定するために、現在のオーナーから最新の属性を要求するメッセージをクラスタ全体に送信します。Cisco ISE でノード グループを定義していない場合は、すべてのノードが 1 つのクラスタ内にあると想定されます。

Cisco ISE でエンドポイントの作成と複製への変更は行われません。エンドポイントの所有権の変更のみが、プロファイリングに使用される、静的属性と動的属性から作成される属性のリスト（ホワイト リスト）に基づいて決定されます。

次のいずれかの属性が変更された場合、後続の属性の収集時に、エンドポイントは管理ノードで更新されます。

- ip
- EndPointPolicy
- MatchedValue
- StaticAssignment
- StaticGroupAssignment
- MatchedPolicyID
- NmapSubnetScanID
- PortalUser
- DeviceRegistrationStatus
- BYODRegistration

エンドポイントが管理ノードで編集および保存されている場合、この属性はエンドポイントの現在のオーナーから取得されます。

エンドポイント ID グループの作成

Cisco ISE では、検出したエンドポイントを、対応するエンドポイント ID グループにグループ化します。Cisco ISE では、システム定義された複数のエンドポイントの ID グループが事前に用意されています。[エンドポイント ID グループ (Endpoint Identity Groups)] ページで追加のエンドポイント ID グループを作成することもできます。作成したエンドポイント ID グループを編集または削除できます。システム定義されたエンドポイント ID グループの説明のみを編集できます。これらのグループの名前を編集したり、これらのグループを削除したりすることはできません。

ステップ 1 [管理 (Administration)] > [ID の管理 (Identity Management)] > [グループ (Groups)] > [エンドポイント ID グループ (Endpoint Identity Groups)] を選択します。

ステップ 2 [追加 (Add)] をクリックします。

ステップ 3 作成するエンドポイント ID グループの名前を入力します（エンドポイント ID グループの名前にスペースを入れないでください）。

ステップ 4 作成するエンドポイント ID グループの説明を入力します。

ステップ 5 [親グループ (Parent Group)] ドロップダウン リストをクリックして、新しく作成したエンドポイント ID グループを関連付けるエンドポイント ID グループを選択します。

ステップ 6 [送信 (Submit)] をクリックします。

識別されたエンドポイントの、エンドポイント ID グループでのグループ化

Cisco ISE では、エンドポイント プロファイリング ポリシーに基づいて、検出されたエンドポイントに対応するエンドポイント ID グループにグループ化します。プロファイリング ポリシーは階層構造になっており、Cisco ISE のエンドポイント ID グループ レベルで適用されます。エンドポイントを実エンドポイント ID グループにグループ化し、プロファイリング ポリシーを実エンドポイント ID グループに適用すると、Cisco ISE により、対応するエンドポイント プロファイリング ポリシーを確認してエンドポイント プロファイルへのエンドポイントのマッピングを決定できます。

Cisco ISE によってエンドポイント ID グループのセットがデフォルトで作成され、これを使用して、エンドポイントを動的または静的に割り当てできる独自の ID グループを作成できます。エンドポイント ID グループを作成し、システムが作成した ID グループの 1 つにその ID グループを関連付けることができます。また、自分が作成したエンドポイントをシステム内のいずれかの ID グループに静的に割り当てることができ、ID グループがプロファイリング サービスで再割り当てされることはありません。

エンドポイントに対して作成されるデフォルトのエンドポイント ID グループ

Cisco ISE は次の 5 つのエンドポイント ID グループをデフォルトで作成します。ブラックリスト、GuestEndpoints、プロファイル済み、RegisteredDevices、不明。さらに、プロファイル済み (親) ID グループに関連付けられている Cisco-IP-Phone やワークステーションなどの追加の 2 つの ID グループを作成します。親グループは、システムに存在するデフォルトの ID グループです。

Cisco ISE は次のエンドポイント ID グループを作成します。

- **ブラックリスト**：このエンドポイント ID グループには、Cisco ISE でこのグループに静的に割り当てられたエンドポイントおよびデバイス登録ポータルでブラックリストに記載されたエンドポイントが含まれます。許可プロファイルを Cisco ISE で定義して、このグループのエンドポイントへのネットワーク アクセスを許可または拒否できます。
- **GuestEndpoints**：このエンドポイント ID グループには、ゲストユーザが使用するエンドポイントが含まれます。
- **プロファイル済み**：このエンドポイント ID グループには、Cisco ISE の Cisco IP Phone およびワークステーションを除くエンドポイント プロファイリング ポリシーに一致するエンドポイントが含まれます。
- **登録済みデバイス**：このエンドポイント ID グループには、デバイス登録ポータルを介して従業員が追加した登録済みデバイスであるエンドポイントが含まれます。プロファイリング サービスは通常、これらのデバイスがこのグループに割り当てられている場合、これらのデバイスを引き続きプロファイリングします。エンドポイントは Cisco ISE のこのグループに静的に割り当てられ、プロファイリング サービスがこれらのエンドポイントを他

の ID グループに割り当てることはできません。これらのデバイスは、エンドポイント リストの他のエンドポイントと同様に表示されます。デバイス登録ポータルを介して追加されたこれらのデバイスに対して、Cisco ISE の [エンドポイント (Endpoints)] ページのエンドポイントリストで編集、削除およびブラックリストへの記載を実行できます。デバイス登録ポータルでブラックリストに記載されたデバイスは、ブラックリストエンドポイント ID グループに割り当てられ、Cisco ISE に存在する許可プロファイルは、ブラックリストに記載されたデバイスを URL (「無許可ネットワーク アクセス」と表示される、ブラックリストに記載されたデバイスのデフォルト ポータル ページ) にリダイレクトします。

- 不明：このエンドポイント ID グループには、Cisco ISE のプロファイルに一致しないエンドポイントが含まれます。

上記のシステムで作成されたエンドポイント ID グループに加えて、Cisco ISE ではプロファイル済み ID グループに関連付けられる次のエンドポイント ID グループが作成されます。

- Cisco-IP-Phone：ネットワーク上のすべてのプロファイル済み Cisco IP Phone が含まれる ID グループです。
- ワークステーション：ネットワーク上のすべてのプロファイル済みワークステーションが含まれる ID グループです。

一致するエンドポイント プロファイリング ポリシーに対して作成されるエンドポイント ID グループ

既存のポリシーと一致するエンドポイント ポリシーがある場合、プロファイリング サービスは一致するエンドポイント ID グループを作成できます。この ID グループは、プロファイル済みエンドポイント ID グループの子になります。エンドポイント ポリシーを作成する場合、[プロファイリング ポリシー (Profiling Policies)] ページの [一致する ID グループの作成 (Create Matching Identity Group)] チェックボックスをオンにして、一致するエンドポイント ID グループを作成できます。プロファイルのマッピングが削除されない限り、一致する ID グループは削除できません。

エンドポイント ID グループでの静的なエンドポイントの追加

エンドポイント ID グループの静的に追加されたエンドポイントを追加または削除できます。

[エンドポイント (Endpoints)] ウィジェットのエンドポイントのみを特定の ID グループに追加できます。エンドポイントを特定のエンドポイント ID グループに追加した場合、そのエンドポイントは、前に動的にグループ化されたエンドポイント ID グループから移動されます。

エンドポイントを最近追加したエンドポイント ID グループから削除すると、そのエンドポイントは、適切な ID グループに再プロファイリングされます。エンドポイントは、システムから削除されませんが、エンドポイントの ID グループからのみ削除されます。

-
- ステップ 1 [管理 (Administration)] > [ID の管理 (Identity Management)] > [グループ (Groups)] > [エンドポイント ID グループ (Endpoint Identity Groups)] を選択します。
 - ステップ 2 エンドポイント ID グループを選択して [編集 (Edit)] をクリックします。
 - ステップ 3 [追加 (Add)] をクリックします。

ステップ 4 [エンドポイント (Endpoints)] ウィジェットでエンドポイントを選択して、選択したエンドポイントをエンドポイント ID グループに追加します。

ステップ 5 [エンドポイント グループ リスト (Endpoint Group List)] リンクをクリックして、[エンドポイント ID グループ (Endpoint Identity Groups)] ページに戻ります。

ダイナミック エンドポイントの、ID グループへの追加または削除後の再プロファイリング

エンドポイント ID グループが静的に割り当てられていない場合、エンドポイント ID グループに追加した、またはエンドポイント ID グループから削除したエンドポイントは、再プロファイリングされます。ISE プロファイラにより動的に識別されたエンドポイントは、適切なエンドポイント ID グループに表示されます。動的に追加されたエンドポイントをエンドポイント ID グループから削除した場合、Cisco ISE では、エンドポイント ID グループからエンドポイントを正常に削除したが、それらのエンドポイントをエンドポイント ID グループに再プロファイリングして戻すことを示すメッセージが表示されます。

許可ルールで使用するエンドポイント ID グループ

エンドポイント ID グループを許可ポリシーで効率的に使用して、検出されたエンドポイントに適切なネットワークアクセス権限を付与することができます。たとえば、すべてのタイプの Cisco IP Phone 用の許可ルールが、デフォルトで、Cisco ISE の [ポリシー (Policy)] > [認証 (Authorization)] > [標準 (Standard)] > [ポリシー (Policy)] で使用できます。

エンドポイント プロファイリング ポリシーがスタンドアロン ポリシー (他のエンドポイント プロファイリング ポリシーの親でない) であるか、またはエンドポイント プロファイリング ポリシーの親ポリシーが無効でないことを確認する必要があります。

プロファイラ フィード サービス

プロファイラ条件、例外アクション、および NMAP スキャンアクションが、シスコ提供または管理者作成 (システム タイプ属性を参照) として分類されます。また、エンドポイント プロファイリング ポリシーは、シスコ提供、管理者作成、または管理者による変更 (システム タイプ属性を参照) として分類されます。

システムタイプ属性によって、プロファイラ条件、例外アクション、NMAP スキャンアクション、およびエンドポイント プロファイリング ポリシーに対して異なる操作を実行できます。シスコ提供の条件、例外アクション、NMAP スキャンアクションは編集または削除できません。シスコが提供するエンドポイントポリシーは削除できません。ポリシーが編集されると、管理者によって変更されたと思なされます。管理者によって変更されたポリシーが削除されると、それが基づいていたシスコ提供ポリシーの最新のバージョンに置き換えられます。

新規および更新されたエンドポイント プロファイリング ポリシーや更新された OUI データベースを、指定された Cisco フィード サーバからの、サブスクリプションを介した Cisco ISE へのフィードとして取得できます。また、適用、成功、および失敗メッセージに対して設定した、Cisco ISE の管理者としての電子メール アドレスに電子メール通知を受信できます。通知を受信するために追加の加入者情報も提供できます。レコードを維持するために加入者情報をシスコに送り返すことができ、それらは特権および機密として処理されます。

、Cisco ISE は毎日ローカル Cisco ISE サーバのタイム ゾーンの午前 1:00 にフィード サービス ポリシーと OUI データベースの更新をダウンロードします。Cisco ISE は、これらのダウンロードされたフィード サーバ ポリシーを自動的に適用し、また、これらの変更を以前の状態に復元できるように一連の変更を保存します。最後に適用した一連の変更から復元すると、新しく追加されたエンドポイント プロファイリング ポリシーは削除され、更新されたエンドポイント プロファイリング ポリシーは以前の状態に復元されます。さらに、プロファイラ フィード サービスは自動的に無効になります。

また、オフラインモードで手動でフィード サービスを更新することもできます。ISE 展開をシスコ フィード サービスに接続できない場合には、このオプションを使用して更新プログラムを手動でダウンロードすることができます。

更新が行われるとき、シスコ提供のプロファイリングポリシーと、以前の更新で変更されたエンドポイント プロファイリング ポリシーのみが更新されます。シスコ提供の無効のプロファイリングポリシーも更新されますが、無効のままです。管理者作成または管理者による変更のプロファイリング ポリシーは、上書きされません。管理者による変更のエンドポイント プロファイリング ポリシーをシスコ提供のエンドポイント プロファイリング ポリシーに復元する場合は、管理者による変更のエンドポイント プロファイリング ポリシーを削除するか、または管理者による変更のエンドポイント プロファイリング ポリシーを以前のシスコ提供のエンドポイント プロファイリング ポリシーに復元する必要があります。



(注) 60 日間のうち、ライセンスがコンプライアンス外 (OOC) となっている日数が 45 日間に達すると、フィード サービスからの更新が許可されなくなります。ライセンスがコンプライアンス外になるのは、ライセンスの有効期限が切れるか、または使用が許可されているセッション数を超えた時点です。

OUI フィード サービス

指定されたシスコ フィード サーバは、<http://standards.ieee.org/develop/regauth/oui/oui.txt> から更新済みの OUI データベースをダウンロードします。これは、MAC OUI に関連付けられたベンダーのリストです。更新された OUI データベースは、Cisco ISE が自身のデータベースにダウンロードするフィードとして、ISE 展開で使用できます。Cisco ISE はエンドポイントを更新してから、エンドポイントの再プロファイリングを始めます。

指定されたシスコ フィード サーバは、<https://ise.cisco.com:8443/feedserver/> にあります。サービスへのアクセスに問題がある場合は、(たとえば、ファイアウォールやプロキシサーバのような) ネットワーク セキュリティ コンポーネントで、この URL に対する直接アクセスが許可されていることを確認します。

プロファイラ フィード サービスの設定

プロファイラ フィード サービスは、Cisco フィード サーバから新規および更新されたエンドポイント プロファイリング ポリシーと MAC OUI データベース更新を取得します。フィード サービスが使用できない場合、またはその他のエラーが発生した場合は、操作監査レポートで報告されます。

フィード サービス使用レポートをシスコに返信するように Cisco ISE を設定できます。そのレポートでは、次の情報がシスコに送信されます。

- Hostname : Cisco ISE ホスト名
- MaxCount : エンドポイントの合計数
- ProfiledCount : プロファイリングされたエンドポイント カウント
- UnknownCount : 不明なエンドポイント カウント
- MatchSystemProfilesCount : シスコ提供のプロファイル カウント
- UserCreatedProfiles : ユーザ作成のプロファイル カウント

シスコから提供されるプロファイリング ポリシーの CoA タイプを変更できます。フィード サービスがそのポリシーを更新すると、CoA タイプは変更されませんが、そのポリシーの残りの属性は引き続き更新されます。

始める前に

分散展開またはスタンドアロン ISE ノードでは、Cisco ISE 管理者ポータルからのみプロファイラ フィード サービスを設定できます。

フィード更新について管理者ポータルから電子メール通知を送信する場合は、Simple Mail Transfer Protocol (SMTP) サーバを設定します ([管理 (Administration)] > [システム (System)] > [設定 (Settings)])。

フィード サービスをオンラインで更新するには、次の手順に従います。

- ステップ 1** [管理 (Administration)] > [証明書 (Certificates)] > [信頼できる証明書 (Trusted Certificates)] の順に選択し、Verisign Class 3 Public Primary Certification Authority および Verisign Class 3 Server CA - G3 が有効であることを確認します。
- ステップ 2** [ワーク センター (Work Centers)] > [プロファイラ (Profiler)] > [フィード (Feeds)] の順に選択します。
[管理 (Administration)] > [フィードサービス (FeedService)] > [プロファイラ (Profiler)] ページでこのオプションにアクセスすることもできます。
- ステップ 3** [オンライン サブスクリプションの更新 (Online Subscription Update)] タブをクリックします。
- ステップ 4** [フィードサービス接続のテスト (Test Feed Service Connection)] ボタンをクリックして、Cisco フィード サービスへの接続があり、証明書が有効であることを確認します。
- ステップ 5** [オンラインサブスクリプション更新の有効化 (Enable Online Subscription Update)] チェック ボックスをオンにします。
- ステップ 6** HH:MM 形式で時刻 (Cisco ISE サーバのローカル タイム ゾーン) を入力します。デフォルトでは、Cisco ISE フィード サービスは毎日午前 1 時にスケジュールされます。
- ステップ 7** [ダウンロードが行われたら管理者に通知 (Notify administrator when download occurs)] チェック ボックスをオンにして、[管理者の電子メールアドレス (Administrator email address)] テキストボックスに電子メールアドレスを入力します。Cisco ISE が非機密情報 (今後のリリースでよりよいサービスと追加機能を提供

するために使用される) を収集することを許可する場合、[プロファイリング精度を上げるために Cisco 匿名情報を提供する (Provide Cisco anonymous information to help improve profiling accuracy)] チェック ボックスをオンにします。

ステップ 8 [保存 (Save)] をクリックします。

ステップ 9 [今すぐ更新 (Update Now)] をクリックします。

最後のフィード サービス更新以降に作成された新規および更新されたプロファイルをチェックするために Cisco フィード サーバに連絡するように Cisco ISE に指示します。これによりシステム内のすべてのエンドポイントが再プロファイリングされ、システム負荷が増加する可能性があります。エンドポイント プロファイリング ポリシーの更新のため、現在 Cisco ISE に接続している一部のエンドポイントの許可ポリシーが変更される場合があります。

最後のフィード サービス以降に作成された新規および更新されたプロファイルを更新すると [今すぐ更新 (Update Now)] ボタンは無効になり、ダウンロードの完了後にのみ有効になります。[プロファイラ フィード サービス設定 (Profiler Feed Service Configuration)] ページから別の場所に移動し、このページに戻ります。

関連トピック

[オフラインでのプロファイラ フィード サービスの設定](#) (821 ページ)

オフラインでのプロファイラ フィード サービスの設定

Cisco ISE と Cisco フィード サーバが直接接続されていないときに、フィード サービスをオフラインで更新できます。Cisco フィード サーバからオフライン更新プログラムパッケージをダウンロードし、Cisco ISE にオフライン フィード更新プログラムを使用してアップロードできます。またフィードサーバに追加される新しいポリシーに関する電子メール通知を設定することもできます。

オフラインでのプロファイラ フィード サービス設定には、次のタスクが含まれます。

1. オフライン更新プログラム パッケージのダウンロード
2. オフライン フィード更新の適用

オフライン更新プログラム パッケージのダウンロード

オフライン更新プログラムパッケージをダウンロードするには、以下のステップに従います。

-
- ステップ 1** [ワーク センター (Work Centers)] > [プロファイラ (Profiler)] > [フィード (Feeds)] の順に選択します。
- [管理 (Administration)] > [フィードサービス (FeedService)] > [プロファイラ (Profiler)] ページでこのオプションにアクセスすることもできます。
- ステップ 2** [オフライン手動更新 (Offline Manual Update)] タブをクリックします。
- ステップ 3** [更新されているプロファイル ポリシーのダウンロード (Download Updated Profile Policies)] リンクをクリックします。フィード サービス パートナー ポータルにリダイレクトされます。

オフライン フィード更新の適用

また、ブラウザから <https://ise.cisco.com/partner/> にアクセスして、フィード サービス パートナー ポータルに直接アクセスすることもできます。

- ステップ 4** 初めてのユーザは、各種条件および契約に同意します。
要求を承認するフィードサービス管理者に電子メールが送信されます。承認されると、確認用の電子メールが届きます
- ステップ 5** Cisco.com のクレデンシャルを使用してパートナー ポータルにログインします。
- ステップ 6** [オフライン フィード (Offline Feed)] > [パッケージのダウンロード (Download Package)] の順に選択します。
- ステップ 7** [パッケージの生成 (Generate Package)] をクリックします。
- ステップ 8** [オフライン 更新プログラム パッケージの内容を表示するにはクリックしてください (Click to View the Offline Update Package contents)] リンクをクリックして、生成したパッケージに含まれるすべてのプロファイルと OUI を表示します。
- [フィード プロファイラ 1 (Feed Profiler 1)] と [フィード OUI (Feed OUI)] の下のポリシーは Cisco ISE の全バージョンにダウンロードされます。
 - [フィード プロファイラ 2 (Feed Profiler 2)] の下のポリシーは Cisco ISE リリース 1.3 以降のみにダウンロードされます。
 - [フィード プロファイラ 3 (Feed Profiler 2)] の下のポリシーは Cisco ISE リリース 2.1 以降のみにダウンロードされます。
- ステップ 9** [パッケージのダウンロード (Download Package)] をクリックして、ローカル システムにファイルを保存します。
保存したファイルを Cisco ISE サーバにアップロードして、ダウンロードしたパッケージのフィード更新プログラムを適用できます。

オフライン フィード更新の適用

ダウンロードしたオフライン フィード更新を適用するには：

始める前に

フィード更新を適用する前に、オフライン更新プログラムパッケージをダウンロードしている必要があります。

- ステップ 1** [ワーク センター (Work Centers)] > [プロファイラ (Profiler)] > [フィード (Feeds)] の順に選択します。
[管理 (Administration)] > [フィードサービス (FeedService)] > [プロファイラ (Profiler)] ページでこのオプションにアクセスすることもできます。
- ステップ 2** [オフライン手動更新 (Offline Manual Update)] タブをクリックします。
- ステップ 3** [参照 (Browse)] をクリックして、ダウンロードしたプロファイラ フィードパッケージを選択します。

ステップ 4 [更新の適用 (Apply Update)] をクリックします。

プロファイルと OUI の更新に関する電子メール通知の設定

プロファイルと OUI の更新通知を受信する電子メール アドレスを設定できます。

電子メール通知を設定するには、次の手順に従います。

ステップ 1 [オフライン更新プログラム パッケージのダウンロード](#) セクションの手順 1 ~ 5 を実行し、フィード サービス パートナー ポータルに移動します。

ステップ 2 [オフラインフィード (Offline Feed)] > [電子メール設定 (Email Preferences)] を選択します。

ステップ 3 通知を受信するには、[通知の有効化 (Enable Notifications)] チェック ボックスをオンにします。

ステップ 4 新しい更新通知を受信する頻度を設定するには、[日数 (days)] ドロップダウン リストから日数を選択します。

ステップ 5 電子メール アドレスまたはアドレスを入力し、[保存 (Save)] をクリックします。

フィード更新の取り消し

前回の更新で更新されたエンドポイント プロファイリング ポリシーに戻り、プロファイラ フィード サービスの前回の更新により新しく追加されたが、エンドポイント プロファイリング ポリシーおよび OUI を削除できます。

エンドポイント プロファイリング ポリシーは、フィード サーバからの更新後に変更された場合、システムで変更されません。

ステップ 1 [ワーク センター (Work Centers)] > [プロファイラ (Profiler)] > [フィード (Feeds)] の順に選択します。

ステップ 2 変更設定監査レポートで設定変更を表示する場合は、[更新レポート ページに移動 (Go to Update Report Page)] をクリックします。

ステップ 3 [最新を元に戻す (Undo Latest)] をクリックします。

プロファイラ レポート

Cisco ISE には、エンドポイント プロファイリングに関するさまざまなレポートと、ネットワークの管理に使用できるトラブルシューティングツールが用意されています。現在のデータに加えて履歴のレポートを生成できます。レポートの一部をドリルダウンして詳細を表示できます。大規模なレポートの場合、レポートをスケジュールし、さまざまな形式でダウンロードすることもできます。

[操作 (Operations)] > [レポート (Reports)] > [エンドポイントとユーザ (Endpoints and Users)] からエンドポイントに関する次のレポートを実行できます。

- エンドポイント セッション履歴
- プロファイリングされたエンドポイントの概要
- エンドポイント プロファイルの変更
- エンドポイントによる上位承認
- 登録済みエンドポイント

エンドポイントの異常な動作の検出

Cisco ISE により、不正な MAC アドレスの使用からネットワークが保護されます。ISE は MAC アドレススプーフィングに関与しているエンドポイントを検出し、疑わしいエンドポイントの権限を制限できます。

プロファイラ設定ページには、異常な動作に関する次の 2 つのオプションがあります。

- 異常な動作の検出を有効にする (Enable Anomalous Behavior Detection)
- 異常な動作の適用を有効にする (Enable Anomalous Behavior Enforcement)

異常な動作の検出を有効にすると、Cisco ISE はデータを調査し、NAS ポート タイプ、DHCP クラス ID、およびエンドポイント ポリシーに関連する属性の変更について、既存のデータとの矛盾がないかどうかを確認します。該当する場合、**AnomalousBehavior** 属性が True に設定され、エンドポイントに追加されます。これは、[可視性のコンテキスト (Visibility Context)] ページでエンドポイントをフィルタリングおよび表示する際に役立ちます。該当する MAC アドレスの監査ログも生成されます。

異常な動作の検出を有効にすると、Cisco ISE は、既存のエンドポイントの次の属性が変更されたかどうかを検査します。

1. ポートタイプ—エンドポイントのアクセス方式が変更されたかどうかを判断します。たとえば、有線 Dot1x で接続した MAC アドレスがワイヤレス Dot1x にも使用されているかどうか (あるいはその逆) を判断します。
2. DHCP クラス ID—エンドポイントのクライアントまたはベンダーのタイプが変更されたかどうかを判断します。これは、DHCP クラス ID 属性に特定の値が入力された後で別の値に変更された場合にのみ当てはまります。エンドポイントが静的 IP アドレスで構成されている場合、Cisco ISE での DHCP クラス ID 属性は空です。後で別のデバイスがこのエンドポイントの MAC アドレスをスプーフィングして DHCP を使用すると、クラス ID が空の値から特定の文字列に変更されます。これによって異常な動作の検出がトリガーされることはありません。
3. エンドポイントポリシー—重要なプロファイル変更があったかどうかを判断します。たとえば、エンドポイントのプロファイルが [電話 (Phone)] または [プリンタ (Printer)] から [ワークステーション (Workstation)] に変更されたかどうかを判断します。

異常な動作の適用を有効にすると、異常な動作が検出された時点で CoA が発行されます。これは、[プロファイラ設定 (Profiler Configuration)] ページで設定した許可ルールに基づいて、疑わしいエンドポイントを再許可するときに使用できます。

異常な動作に関する許可ポリシールールをエンドポイントに設定するには、「[異常な動作が発生しているエンドポイントに関する許可ポリシールールの設定 \(825 ページ\)](#)」を参照してください。

異常な動作が発生しているエンドポイントに関する許可ポリシールールの設定

異常な動作が発生しているエンドポイントに対して実行するアクションを選択するには、[許可ポリシー (Authorization Policy)] ページで対応するルールを設定します。

-
- ステップ 1 [ポリシー (Policy)] > [許可 (Authorization)] を選択します。
 - ステップ 2 既存のルールの [編集 (Edit)] ドロップダウン矢印をクリックし、[新規ルールを上挿入 (Insert New Rule Above)] または [新規ルールを下挿入 (Insert New Rule Below)] をクリックします。
 - ステップ 3 [ルール名 (Rule Name)] にルール名を入力します。
 - ステップ 4 [条件 (Conditions)] フィールドの追加アイコンをクリックし、[新しい条件の作成 (高度なオプション) (Create New Condition (Advance Option))] をクリックします。
 - ステップ 5 [属性の選択 (Select Attribute)] ドロップダウンから [エンドポイント (Endpoints)] > [異常な動作 (Anomalous Behavior)] を選択します。
 - ステップ 6 最後のフィールドに「true」と入力します。
 - ステップ 7 [権限 (Permissions)] 列の追加アイコンをクリックし、[項目の選択 (Select Item)] ドロップダウンリストから必要なアクションを選択します。

例：

攻撃者や疑わしいエンドポイントにアクセス権限を付与しない場合は、[項目の選択 (Select Item)] ドロップダウンリストから [標準 (Standard)] > [アクセス拒否 (Deny Access)] を選択します。

- ステップ 8 [完了 (Done)] をクリックします。
-

異常な動作が発生しているエンドポイントの表示

次のいずれかのオプションを使用して、異常な動作が発生しているエンドポイントを表示できます。

- [ホーム (Home)] > [概要 (Summary)] > [メトリック (Metrics)] から [異常な動作 (Anomalous Behavior)] をクリックします。この操作により、ページ下部のペインに [異常な動作 (Anomalous Behavior)] 列がある新しいタブが表示されます。

- [コンテキストの可視性 (Context Visibility)] > [エンドポイント (Endpoints)] > [エンドポイントの分類 (Endpoint Classification)] を選択します。ページ下部のペインで [異常な動作 (Anomalous Behavior)] 列を確認できます。
- 次の手順で説明するように、[コンテキストの可視性 (Context Visibility)] ページの [認証 (Authentication)] ビューまたは [侵害されたエンドポイント (Compromised Endpoints)] ビューで新しい [異常な動作 (Anomalous Behavior)] 列を作成できます。

-
- ステップ 1** [コンテキストの可視性 (Context Visibility)] > [エンドポイント (Endpoints)] > [認証 (Authentication)] または [コンテキストの可視性 (Context Visibility)] > [エンドポイント (Endpoints)] > [侵害されたエンドポイント (Compromised Endpoints)] を選択します。
- ステップ 2** ページ下部のペインにある [設定 (Settings)] アイコンをクリックし、[異常な動作 (Anomalous Behavior)] チェックボックスをオンにします。
- ステップ 3** [移動 (Go)] をクリックします。
[認証 (Authentication)] ビューまたは [侵害されたエンドポイント (Compromised Endpoints)] ビューで [異常な動作 (Anomalous Behavior)] 列を表示できます。
-

プロファイラ フィード サービス

プロファイラ条件、例外アクション、および NMAP スキャンアクションが、シスコ提供または管理者作成 (システム タイプ属性を参照) として分類されます。また、エンドポイント プロファイリング ポリシーは、シスコ提供、管理者作成、または管理者による変更 (システム タイプ属性を参照) として分類されます。

システムタイプ属性によって、プロファイラ条件、例外アクション、NMAP スキャンアクション、およびエンドポイント プロファイリング ポリシーに対して異なる操作を実行できます。シスコ提供の条件、例外アクション、NMAP スキャンアクションは編集または削除できません。シスコが提供するエンドポイントポリシーは削除できません。ポリシーが編集されると、管理者によって変更されたと見なされます。管理者によって変更されたポリシーが削除されると、それが基づいていたシスコ提供ポリシーの最新のバージョンに置き換えられます。

新規および更新されたエンドポイント プロファイリング ポリシーや更新された OUI データベースを、指定された Cisco フィード サーバからの、サブスクリプションを介した Cisco ISE へのフィードとして取得できます。また、適用、成功、および失敗メッセージに対して設定した、Cisco ISE の管理者としての電子メール アドレスに電子メール通知を受信できます。通知を受信するために追加の加入者情報も提供できます。レコードを維持するために加入者情報をシスコに送り返すことができ、それらは特権および機密として処理されます。

、Cisco ISE は毎日ローカル Cisco ISE サーバのタイム ゾーンの午前 1:00 にフィード サービスポリシーと OUI データベースの更新をダウンロードします。Cisco ISE は、これらのダウンロードされたフィード サーバポリシーを自動的に適用し、また、これらの変更を以前の状態に復元できるように一連の変更を保存します。最後に適用した一連の変更から復元すると、新しく追加されたエンドポイント プロファイリング ポリシーは削除され、更新されたエンドポイント

トプロファイリング ポリシーは以前の状態に復元されます。さらに、プロファイラ フィード サービスは自動的に無効になります。

また、オフラインモードで手動でフィードサービスを更新することもできます。ISE 展開をシスコ フィード サービスに接続できない場合には、このオプションを使用して更新プログラムを手動でダウンロードすることができます。

更新が行われるとき、シスコ提供のプロファイリングポリシーと、以前の更新で変更されたエンドポイント プロファイリング ポリシーのみが更新されます。シスコ提供の無効のプロファイリングポリシーも更新されますが、無効のままです。管理者作成または管理者による変更のプロファイリングポリシーは、上書きされません。管理者による変更のエンドポイント プロファイリング ポリシーをシスコ提供のエンドポイント プロファイリング ポリシーに復元する場合は、管理者による変更のエンドポイント プロファイリング ポリシーを削除するか、または管理者による変更のエンドポイント プロファイリング ポリシーを以前のシスコ提供のエンドポイント プロファイリング ポリシーに復元する必要があります。



(注) 60 日間のうち、ライセンスがコンプライアンス外 (OOC) となっている日数が 45 日間に達すると、フィードサービスからの更新が許可されなくなります。ライセンスがコンプライアンス外になるのは、ライセンスの有効期限が切れるか、または使用が許可されているセッション数を超えた時点です。

OUI フィード サービス

指定されたシスコ フィード サーバは、<http://standards.ieee.org/develop/regauth/oui/oui.txt> から更新済みの OUI データベースをダウンロードします。これは、MAC OUI に関連付けられたベンダーのリストです。更新された OUI データベースは、Cisco ISE が自身のデータベースにダウンロードするフィードとして、ISE 展開で使用できます。Cisco ISE はエンドポイントを更新してから、エンドポイントの再プロファイリングを始めます。

指定されたシスコ フィード サーバは、<https://ise.cisco.com:8443/feedserver/> にあります。サービスへのアクセスに問題がある場合は、(たとえば、ファイアウォールやプロキシサーバのような) ネットワーク セキュリティ コンポーネントで、この URL に対する直接アクセスが許可されていることを確認します。

プロファイラ フィード サービスの設定

プロファイラ フィード サービスは、Cisco フィード サーバから新規および更新されたエンドポイント プロファイリング ポリシーと MAC OUI データベース更新を取得します。フィード サービスが使用できない場合、またはその他のエラーが発生した場合は、操作監査レポートで報告されます。

フィード サービス使用レポートをシスコに返信するように Cisco ISE を設定できます。そのレポートでは、次の情報がシスコに送信されます。

- Hostname : Cisco ISE ホスト名

- MaxCount : エンドポイントの合計数
- ProfiledCount : プロファイリングされたエンドポイント カウント
- UnknownCount : 不明なエンドポイント カウント
- MatchSystemProfilesCount : シスコ提供のプロファイル カウント
- UserCreatedProfiles : ユーザ作成のプロファイル カウント

シスコから提供されるプロファイリング ポリシーの CoA タイプを変更できます。フィード サービスがそのポリシーを更新すると、CoA タイプは変更されませんが、そのポリシーの残りの属性は引き続き更新されます。

始める前に

分散展開またはスタンドアロン ISE ノードでは、Cisco ISE 管理者ポータルからのみプロファイラ フィード サービスを設定できます。

フィード更新について管理者ポータルから電子メール通知を送信する場合は、Simple Mail Transfer Protocol (SMTP) サーバを設定します ([管理 (Administration)] > [システム (System)] > [設定 (Settings)])。

フィード サービスをオンラインで更新するには、次の手順に従います。

-
- ステップ 1** [管理 (Administration)] > [証明書 (Certificates)] > [信頼できる証明書 (Trusted Certificates)] の順に選択し、Verisign Class 3 Public Primary Certification Authority および Verisign Class 3 Server CA - G3 が有効であることを確認します。
 - ステップ 2** [ワーク センター (Work Centers)] > [プロファイラ (Profiler)] > [フィード (Feeds)] の順に選択します。
[管理 (Administration)] > [フィードサービス (FeedService)] > [プロファイラ (Profiler)] ページでこのオプションにアクセスすることもできます。
 - ステップ 3** [オンライン サブスクリプションの更新 (Online Subscription Update)] タブをクリックします。
 - ステップ 4** [フィードサービス接続のテスト (Test Feed Service Connection)] ボタンをクリックして、Cisco フィード サービスへの接続があり、証明書が有効であることを確認します。
 - ステップ 5** [オンラインサブスクリプション更新の有効化 (Enable Online Subscription Update)] チェック ボックスをオンにします。
 - ステップ 6** HH:MM 形式で時刻 (Cisco ISE サーバのローカル タイム ゾーン) を入力します。デフォルトでは、Cisco ISE フィード サービスは毎日午前 1 時にスケジュールされます。
 - ステップ 7** [ダウンロードが行われたら管理者に通知 (Notify administrator when download occurs)] チェック ボックスをオンにして、[管理者の電子メールアドレス (Administrator email address)] テキストボックスに電子メールアドレスを入力します。Cisco ISE が非機密情報 (今後のリリースでよりよいサービスと追加機能を提供するために使用される) を収集することを許可する場合、[プロファイリング精度を上げるために Cisco 匿名情報を提供する (Provide Cisco anonymous information to help improve profiling accuracy)] チェック ボックスをオンにします。
 - ステップ 8** [保存 (Save)] をクリックします。

ステップ 9 [今すぐ更新 (Update Now)] をクリックします。

最後のフィード サービス更新以降に作成された新規および更新されたプロファイルをチェックするために Cisco フィード サーバに連絡するように Cisco ISE に指示します。これによりシステム内のすべてのエンドポイントが再プロファイリングされ、システム負荷が増加する可能性があります。エンドポイント プロファイリング ポリシーの更新のため、現在 Cisco ISE に接続している一部のエンドポイントの許可ポリシーが変更される場合があります。

最後のフィード サービス以降に作成された新規および更新されたプロファイルを更新すると [今すぐ更新 (Update Now)] ボタンは無効になり、ダウンロードの完了後にのみ有効になります。[プロファイラ フィード サービス設定 (Profiler Feed Service Configuration)] ページから別の場所へ移動し、このページに戻ります。

関連トピック

[オフラインでのプロファイラ フィード サービスの設定](#) (821 ページ)

オフラインでのプロファイラ フィード サービスの設定

Cisco ISE と Cisco フィード サーバが直接接続されていないときに、フィード サービスをオフラインで更新できます。Cisco フィード サーバからオフライン更新プログラムパッケージをダウンロードし、Cisco ISE にオフライン フィード更新プログラムを使用してアップロードできます。またフィード サーバに追加される新しいポリシーに関する電子メール通知を設定することもできます。

オフラインでのプロファイラ フィード サービス設定には、次のタスクが含まれます。

1. オフライン更新プログラム パッケージのダウンロード
2. オフライン フィード更新の適用

オフライン更新プログラム パッケージのダウンロード

オフライン更新プログラムパッケージをダウンロードするには、以下のステップに従います。

ステップ 1 [ワーク センター (Work Centers)] > [プロファイラ (Profiler)] > [フィード (Feeds)] の順に選択します。
[管理 (Administration)] > [フィードサービス (FeedService)] > [プロファイラ (Profiler)] ページでこのオプションにアクセスすることもできます。

ステップ 2 [オフライン手動更新 (Offline Manual Update)] タブをクリックします。

ステップ 3 [更新されているプロファイル ポリシーのダウンロード (Download Updated Profile Policies)] リンクをクリックします。フィード サービス パートナー ポータルにリダイレクトされます。
また、ブラウザから <https://ise.cisco.com/partner/> にアクセスして、フィード サービス パートナー ポータルに直接アクセスすることもできます。

ステップ 4 初めてのユーザは、各種条件および契約に同意します。

要求を承認するフィードサービス管理者に電子メールが送信されます。承認されると、確認用の電子メールが届きます

ステップ 5 Cisco.com のクレデンシアルを使用してパートナー ポータルにログインします。

ステップ 6 [オフライン フィード (Offline Feed)] > [パッケージのダウンロード (Download Package)] の順に選択します。

ステップ 7 [パッケージの生成 (Generate Package)] をクリックします。

ステップ 8 [オフライン 更新プログラム パッケージの内容を表示するにはクリックしてください (Click to View the Offline Update Package contents)] リンクをクリックして、生成したパッケージに含まれるすべてのプロファイルと OUI を表示します。

- [フィード プロファイラ 1 (Feed Profiler 1)] と [フィード OUI (Feed OUI)] の下のポリシーは Cisco ISE の全バージョンにダウンロードされます。
- [フィード プロファイラ 2 (Feed Profiler 2)] の下のポリシーは Cisco ISE リリース 1.3 以降のみにダウンロードされます。
- [フィード プロファイラ 3 (Feed Profiler 2)] の下のポリシーは Cisco ISE リリース 2.1 以降のみにダウンロードされます。

ステップ 9 [パッケージのダウンロード (Download Package)] をクリックして、ローカル システムにファイルを保存します。

保存したファイルを Cisco ISE サーバにアップロードして、ダウンロードしたパッケージのフィード更新プログラムを適用できます。

オフライン フィード更新の適用

ダウンロードしたオフライン フィード更新を適用するには：

始める前に

フィード更新を適用する前に、オフライン更新プログラムパッケージをダウンロードしている必要があります。

ステップ 1 [ワーク センター (Work Centers)] > [プロファイラ (Profiler)] > [フィード (Feeds)] の順に選択します。
[管理 (Administration)] > [フィードサービス (FeedService)] > [プロファイラ (Profiler)] ページでこのオプションにアクセスすることもできます。

ステップ 2 [オフライン手動更新 (Offline Manual Update)] タブをクリックします。

ステップ 3 [参照 (Browse)] をクリックして、ダウンロードしたプロファイラ フィード パッケージを選択します。

ステップ 4 [更新の適用 (Apply Update)] をクリックします。

プロファイルと OUI の更新に関する電子メール通知の設定

プロファイルと OUI の更新通知を受信する電子メール アドレスを設定できます。

電子メール通知を設定するには、次の手順に従います。

-
- ステップ 1 [オフライン更新プログラム パッケージのダウンロード](#) セクションの手順 1～5 を実行し、フィード サービス パートナー ポータルに移動します。
 - ステップ 2 [オフライン フィード (Offline Feed)] > [電子メール設定 (Email Preferences)] を選択します。
 - ステップ 3 通知を受信するには、[通知の有効化 (Enable Notifications)] チェック ボックスをオンにします。
 - ステップ 4 新しい更新通知を受信する頻度を設定するには、[日数 (days)] ドロップダウン リストから日数を選択します。
 - ステップ 5 電子メール アドレスまたはアドレスを入力し、[保存 (Save)] をクリックします。
-

フィード更新の取り消し

前回の更新で更新されたエンドポイント プロファイリング ポリシーに戻り、プロファイラ フィード サービスの前回の更新により新しく追加されたが、エンドポイント プロファイリング ポリシーおよび OUI を削除できます。

エンドポイント プロファイリング ポリシーは、フィード サーバからの更新後に変更された場合、システムで変更されません。

-
- ステップ 1 [ワーク センター (Work Centers)] > [プロファイラ (Profiler)] > [フィード (Feeds)] の順に選択します。
 - ステップ 2 変更設定監査レポートで設定変更を表示する場合は、[更新レポート ページに移動 (Go to Update Report Page)] をクリックします。
 - ステップ 3 [最新を元に戻す (Undo Latest)] をクリックします。
-

プロファイラ レポート

Cisco ISE には、エンドポイント プロファイリングに関するさまざまなレポートと、ネットワークの管理に使用できるトラブルシューティングツールが用意されています。現在のデータに加えて履歴のレポートを生成できます。レポートの一部をドリルダウンして詳細を表示できます。大規模なレポートの場合、レポートをスケジュールし、さまざまな形式でダウンロードすることもできます。

[操作 (Operations)] > [レポート (Reports)] > [エンドポイントとユーザ (Endpoints and Users)] からエンドポイントに関する次のレポートを実行できます。

- エンドポイント セッション履歴

- プロファイリングされたエンドポイントの概要
- エンドポイント プロファイルの変更
- エンドポイントによる上位承認
- 登録済みエンドポイント

エンドポイントの異常な動作の検出

Cisco ISE により、不正な MAC アドレスの使用からネットワークが保護されます。ISE は MAC アドレススプーフィングに関与しているエンドポイントを検出し、疑わしいエンドポイントの権限を制限できます。

プロファイラ設定ページには、異常な動作に関する次の 2 つのオプションがあります。

- 異常な動作の検出を有効にする (Enable Anomalous Behavior Detection)
- 異常な動作の適用を有効にする (Enable Anomalous Behavior Enforcement)

異常な動作の検出を有効にすると、Cisco ISE はデータを調査し、NAS ポート タイプ、DHCP クラス ID、およびエンドポイント ポリシーに関連する属性の変更について、既存のデータとの矛盾がないかどうかを確認します。該当する場合、**AnomalousBehavior** 属性が True に設定され、エンドポイントに追加されます。これは、[可視性のコンテキスト (Visibility Context)] ページでエンドポイントをフィルタリングおよび表示する際に役立ちます。該当する MAC アドレスの監査ログも生成されます。

異常な動作の検出を有効にすると、Cisco ISE は、既存のエンドポイントの次の属性が変更されたかどうかを検査します。

1. ポートタイプ—エンドポイントのアクセス方式が変更されたかどうかを判断します。たとえば、有線 Dot1x で接続した MAC アドレスがワイヤレス Dot1x にも使用されているかどうか（あるいはその逆）を判断します。
2. DHCP クラス ID—エンドポイントのクライアントまたはベンダーのタイプが変更されたかどうかを判断します。これは、DHCP クラス ID 属性に特定の値が入力された後で別の値に変更された場合にのみ当てはまります。エンドポイントが静的 IP アドレスで構成されている場合、Cisco ISE での DHCP クラス ID 属性は空です。後で別のデバイスがこのエンドポイントの MAC アドレスをスプーフィングして DHCP を使用すると、クラス ID が空の値から特定の文字列に変更されます。これによって異常な動作の検出がトリガーされることはありません。
3. エンドポイントポリシー—重要なプロファイル変更があったかどうかを判断します。たとえば、エンドポイントのプロファイルが [電話 (Phone)] または [プリンタ (Printer)] から [ワークステーション (Workstation)] に変更されたかどうかを判断します。

異常な動作の適用を有効にすると、異常な動作が検出された時点で CoA が発行されます。これは、[プロファイラ設定 (Profiler Configuration)] ページで設定した許可ルールに基づいて、疑わしいエンドポイントを再許可するときに使用できます。

異常な動作に関する許可ポリシールールをエンドポイントに設定するには、「[異常な動作が発生しているエンドポイントに関する許可ポリシールールの設定（825ページ）](#)」を参照してください。

異常な動作が発生しているエンドポイントに関する許可ポリシールールの設定

異常な動作が発生しているエンドポイントに対して実行するアクションを選択するには、[許可ポリシー（Authorization Policy）] ページで対応するルールを設定します。

-
- ステップ 1 [ポリシー（Policy）] > [許可（Authorization）] を選択します。
 - ステップ 2 既存のルールの [編集（Edit）] ドロップダウン矢印をクリックし、[新規ルールを上に入力（Insert New Rule Above）] または [新規ルールを下に入力（Insert New Rule Below）] をクリックします。
 - ステップ 3 [ルール名（Rule Name）] にルール名を入力します。
 - ステップ 4 [条件（Conditions）] フィールドの追加アイコンをクリックし、[新しい条件の作成（高度なオプション）（Create New Condition (Advance Option)）] をクリックします。
 - ステップ 5 [属性の選択（Select Attribute）] ドロップダウンから [エンドポイント（Endpoints）] > [異常な動作（Anomalous Behavior）] を選択します。
 - ステップ 6 最後のフィールドに「true」と入力します。
 - ステップ 7 [権限（Permissions）] 列の追加アイコンをクリックし、[項目の選択（Select Item）] ドロップダウンリストから必要なアクションを選択します。

例：

攻撃者や疑わしいエンドポイントにアクセス権限を付与しない場合は、[項目の選択（Select Item）] ドロップダウンリストから [標準（Standard）] > [アクセス拒否（Deny Access）] を選択します。

- ステップ 8 [完了（Done）] をクリックします。
-

異常な動作が発生しているエンドポイントの表示

次のいずれかのオプションを使用して、異常な動作が発生しているエンドポイントを表示できます。

- [ホーム（Home）] > [概要（Summary）] > [メトリック（Metrics）] から [異常な動作（Anomalous Behavior）] をクリックします。この操作により、ページ下部のペインに [異常な動作（Anomalous Behavior）] 列がある新しいタブが表示されます。
- [コンテキストの可視性（Context Visibility）] > [エンドポイント（Endpoints）] > [エンドポイントの分類（Endpoint Classification）] を選択します。ページ下部のペインで [異常な動作（Anomalous Behavior）] 列を確認できます。

- 次の手順で説明するように、[コンテキストの可視性 (Context Visibility)] ページの [認証 (Authentication)] ビューまたは [侵害されたエンドポイント (Compromised Endpoints)] ビューで新しい [異常な動作 (Anomalous Behavior)] 列を作成できます。

-
- ステップ 1** [コンテキストの可視性 (Context Visibility)] > [エンドポイント (Endpoints)] > [認証 (Authentication)] または [コンテキストの可視性 (Context Visibility)] > [エンドポイント (Endpoints)] > [侵害されたエンドポイント (Compromised Endpoints)] を選択します。
- ステップ 2** ページ下部のペインにある [設定 (Settings)] アイコンをクリックし、[異常な動作 (Anomalous Behavior)] チェックボックスをオンにします。
- ステップ 3** [移動 (Go)] をクリックします。
[認証 (Authentication)] ビューまたは [侵害されたエンドポイント (Compromised Endpoints)] ビューで [異常な動作 (Anomalous Behavior)] 列を表示できます。
-

Cisco NAC アプライアンスとの Cisco ISE 統合

Cisco ISE は、Cisco Network Admission Control (NAC) アプライアンス リリース 4.9 との統合のみをサポートし、Cisco ISE に Advanced ライセンスまたは Wireless ライセンスをインストールした場合に使用できます。

Cisco ISE プロファイラは Cisco NAC 展開のエンドポイントを管理する Cisco Network Admission Control (NAC) プロファイラに似ています。この統合により、Cisco NAC 展開にインストールされている既存の Cisco NAC プロファイラを置き換えることができます。Cisco ISE プロファイラからのプロファイル名およびエンドポイント分類の結果を Cisco Clean Access Manager (CAM) と同期できます。

管理ノードでの Cisco Clean Access Manager の設定

Cisco ISE では、REST API 通信設定のために分散展開のプライマリ PAN で複数の Clean Access Manager (CAM) を登録できます。Cisco ISE に登録されている CAM のリストは、すべてのプロファイラ設定変更が通知されるリストです。プライマリ PAN は、Cisco ISE と Cisco NAC アプライアンス間のすべての通信を担当します。Cisco ISE では、CAM をプライマリ PAN でのみ設定できます。1 つ以上の CAM をプライマリ PAN で登録するときに使用されたクレデンシャルが CAM との接続の認証に使用されます。

Cisco ISE と Cisco NAC アプライアンス間の通信は、Secure Sockets Layer (SSL) 上で安全に行われます。Cisco ISE はプロファイラ設定の変更を CAM にプッシュし、CAM はエンドポイントの MAC アドレスと対応するプロファイルのリストおよびすべてのプロファイル名のリストを Cisco ISE から定期的にプルするため、通信は実際には双方向です。

Cisco ISE と CAM 間でセキュアな通信を適切に行えるように、[管理 (Administration)] > [Clean Access Manager] > [SSL] で X509 証明書の内容を Clean Access Manager からエクスポートし、それを [管理 (Administration)] > [システム (System)] > [証明書 (Certificates)] > [信頼できる

証明書ストア (Trusted Certificates Store)] で Cisco ISE のプライマリ PAN にインポートする必要があります。

ハイアベイラビリティ用の CAM のペアを設定する方法の詳細については、次のリンクを参照してください。

Cisco ISE プロファイラと Cisco Clean Access Manager の通信

Cisco ISE プロファイラは、プロファイラ設定の変更をプライマリ PAN からすべての登録済み Clean Access Manager (CAM) に通知します。これにより、Cisco ISE 分散展開における通知の重複が回避されます。Cisco ISE データベースでエンドポイントの追加や削除、およびエンドポイントプロファイリングポリシーの変更が行われると、プロファイラ設定の変更を通知するために REST API が使用されます。エンドポイントのインポート時、Cisco ISE プロファイラはインポートの完了後にのみ CAM に通知します。

プロファイラ設定の変更を CAM にプッシュするために、次の REST API フローが実装されます。

Cisco ISE プロファイラ エンドポイント変更のプッシュ：Cisco ISE でエンドポイントがプロファイリングされ、エンドポイントのプロファイルに変更がある場合、Cisco ISE プロファイラは、エンドポイントプロファイルの変更をすべての登録済み CAM に通知します。

CAM で Cisco ISE を設定し、CAM の [同期設定 (Sync Settings)] に応じて CAM を Cisco ISE と同期することができます。ルールを作成し、Cisco ISE プロファイルのリストから 1 つ以上の一致するプロファイルを選択し、エンドポイントを CAM のいずれかのアクセスタイプにマッピングできます。CAM はエンドポイントと対応するプロファイル、およびすべてのプロファイル名のリストを Cisco ISE プロファイラから定期的に取得します。

プロファイラ設定の変更を Cisco ISE プロファイラからプルするために、次の REST API フローが実装されます。

- NAC Manager のエンドポイントプル：エンドポイントの MAC アドレスと既知のエンドポイントの対応するプロファイルのリストをプルします。
- NAC Manager のプロファイルプル：プロファイル名を Cisco ISE プロファイラからプルします。

Cisco ISE プロファイラは、Cisco ISE と Cisco NAC アプライアンス リリース 4.9 との統合のモニタとトラブルシューティングに使用できるすべてのイベントを Cisco ISE モニタリングペルソナに通知します。

Cisco ISE プロファイラ ログには、統合のモニタリングとトラブルシューティングに関する次のイベントが取り込まれます。

- NAC 設定の変更 (情報)
- NAC 通知イベント障害 (エラー)

Cisco Clean Access Manager の追加

Cisco ISE を Cisco NAC アプライアンス リリース 4.9 と統合すると、Cisco NAC 展開で Cisco ISE プロファイリング サービスを利用できます。

[NAC Managers] ページでは、複数の Clean Access Manager (CAM) を設定でき、登録した CAM をフィルタリングするためのオプションを使用できます。このページには、CAM が名前、説明、IP アドレス、および CAM でエンドポイント通知が有効になっているかどうかを示すステータスとともに表示されます。

-
- ステップ 1** [管理 (Administration)] > [ネットワーク リソース (Network Resources)] > [NAC Managers] を選択します。
- ステップ 2** [追加 (Add)] をクリックします。
- ステップ 3** Cisco Access Manager の名前を入力します。
- ステップ 4** CAM への接続を認証する Cisco ISE プロファイラからの REST API 通信を有効にする場合は、[ステータス (Status)] チェックボックスをオンにします。
- ステップ 5** 0.0.0.0 および 255.255.255.255 の IP アドレス以外の CAM の IP アドレスを入力します。
- ステップ 6** CAM のユーザインターフェイスにログインするために使用する CAM 管理者のユーザ名とパスワードを入力します。
- ステップ 7** [送信 (Submit)] をクリックします。
-

ポリシーおよび ID グループのスタティック割り当てによるエンドポイントの作成

[エンドポイント (Endpoints)] ページでエンドポイントの MAC アドレスを使用して、新しいエンドポイントを静的に作成できます。また、スタティック割り当ての [エンドポイント (Endpoints)] ページで、エンドポイントプロファイリング ポリシーおよび ID グループを選択できます。

通常のモバイルデバイス (MDM) エンドポイントは、[エンドポイント ID (Endpoints Identities)] リストに表示されます。リストページには、[ホスト名 (Hostname)]、[デバイス タイプ (Device Type)]、[デバイス ID (Device ID)] など、MDM エンドポイントの属性のカラムが表示されます。[スタティック割り当て (Static Assignment)]、[スタティック グループ割り当て (Static Group Assignment)] などのその他のカラムは、デフォルトでは表示されません。



-
- (注) このページを使用して、MDM エンドポイントを追加、編集、削除、インポートまたはエクスポートすることはできません。
-

- ステップ 1** [ワーク センター (Work Centers)] > [ネットワーク アクセス (Network Access)] > [ID (Identities)] > [エンドポイント (Endpoints)] を選択します。
- ステップ 2** [追加 (Add)] をクリックします。
- ステップ 3** エンドポイントの MAC アドレスをコロンで区切られた 16 進表記で入力します。
- ステップ 4** [ポリシー割り当て (Policy Assignment)] ドロップダウン リストから一致するエンドポイント ポリシーを選択して、スタティック割り当てステータスをダイナミックからスタティックに変更します。
- ステップ 5** [スタティック割り当て (Static Assignment)] チェックボックスをオンにして、エンドポイントに割り当てられたスタティック割り当てのステータスをダイナミックからスタティックに変更します。
- ステップ 6** [ID グループ割り当て (Identity Group Assignment)] ドロップダウン リストから、新しく作成されたエンドポイントを割り当てるエンドポイント ID グループを選択します。
- ステップ 7** エンドポイント ID グループのダイナミック割り当てをスタティックに変更するには、[スタティック グループ割り当て (Static Group Assignment)] チェックボックスをオンにします。
- ステップ 8** [送信 (Submit)] をクリックします。

CSV ファイルからのエンドポイントのインポート

Cisco ISE テンプレートから作成した CSV ファイルからエンドポイントをインポートし、エンドポイントの詳細を使用して更新することができます。ISE からエクスポートされたエンドポイントには約 75 個の属性が含まれているため、別の ISE 展開に直接インポートすることはできません。インポートが許可されていない列が CSV ファイルにある場合は、列のリストを含むメッセージが表示されます。ファイルを再度インポートする前に、指定された列を削除する必要があります。



- (注) エンドポイントのカスタム属性をインポートするには、正しいデータ タイプを使用して [管理 (Administration)] > [ID の管理 (Identity Management)] > [設定 (Settings)] > [エンドポイント カスタム属性 (Endpoint Custom Attributes)] ページで CSV ファイルと同じカスタム属性を作成する必要があります。これらのコマンドには、「CUSTOM.」というプレフィックスを付けてエンドポイント属性と区別する必要があります。

インポートできる属性は約 30 あります。このリストには、MACAddress、EndPointPolicy、IdentityGroup が含まれています。オプション属性は次のとおりです。

説明	PortalUser	LastName
PortalUser.GuestType	PortalUser.FirstName	EmailAddress
PortalUser.Location	デバイスタイプ (Device Type)	host-name
PortalUser.GuestStatus	StaticAssignment	参照先

PortalUser.CreationType	StaticGroupAssignment	MDMEnrolled
PortalUser.EmailAddress	User-Name	MDMOSVersion
PortalUser.PhoneNumber	DeviceRegistrationStatus	MDMServerName
PortalUser.LastName	AUPAccepted	MDMServerID
PortalUser.GuestSponsor	FirstName	BYODRegistration
CUSTOM.<custom attribute name>	—	—

ファイルヘッダーは、デフォルトのインポートテンプレートで指定されている形式にして、エンドポイントのリストが次の順序で表示されるようにする必要があります。MACAddress、EndpointPolicy、IdentityGroup、<オプション属性として上に記載されている属性のリスト>。次のファイルテンプレートを作成できます。

- MACAddress
- MACAddress, EndPointPolicy
- MACAddress, EndPointPolicy, IdentityGroup
- MACAddress, EndPointPolicy, IdentityGroup, <オプション属性として上に記載されている属性のリスト>

MAC アドレスを除くすべての属性値は、CSV ファイルからエンドポイントをインポートする際に省略可能です。特定の値のないエンドポイントをインポートする場合も、値はカンマで区切られます。

次の例を参考にしてください。

- MAC1, Endpoint Policy1, Endpoint Identity Group1
- MAC2
- MAC3, Endpoint Policy3
- MAC4, , Endpoint Identity Group4
- MAC5, , Endpoint Identity Group5, MyDescription, MyPortalUser, など

ステップ 1 [コンテキストの可視性 (Context Visibility)] > [エンドポイント (Endpoints)] > [インポート (Import)] の順に選択します。

ステップ 2 [ファイルからインポート (Import from File)] をクリックします。

ステップ 3 [参照 (Browse)] をクリックして、作成済みの CSV ファイルを見つけます。

ステップ 4 [送信 (Submit)] をクリックします。

エンドポイントで使用可能なデフォルトのインポート テンプレート

エンドポイントのインポートに使用できるエンドポイントを更新できるテンプレートを生成できます。デフォルトで、[テンプレートの生成 (Generate a Template)] リンクを使用して、Microsoft Office Excel アプリケーションで CSV ファイルを作成し、このファイルをシステム上にローカルに保存できます。ファイルは [コンテキストの可視性 (Context Visibility)] > [エンドポイント (Endpoints)] > [インポート (Import)] > [ファイルからインポート (Import from File)] にあります。[テンプレートの生成 (Generate a Template)] リンクを使用してテンプレートを作成でき、Cisco ISE サーバは、[template.csv を開く (Opening template.csv)] ダイアログを表示します。このダイアログを使用すると、デフォルトの template.csv ファイルを開いたり、template.csv ファイルをシステム上にローカルに保存できます。このダイアログで template.csv ファイルを開くことを選択した場合、このファイルは Microsoft Office Excel アプリケーションで開かれます。デフォルトの template.csv ファイルには、MAC アドレス、エンドポイント ポリシー、エンドポイント ID グループ、およびその他のオプション属性が表示されるヘッダー行が含まれています。

エンドポイントの MAC アドレス、エンドポイント プロファイリング ポリシー、エンドポイント ID グループを、インポートするオプションの属性値とともに更新し、新しいファイル名を使用してファイルを保存します。このファイルをエンドポイントのインポートのために使用できます。[テンプレートの生成 (Generate a Template)] リンクを使用したときに作成される template.csv ファイルのヘッダー行を参照してください。

表 51: CSV テンプレート ファイル

MAC	EndPointPolicy	IdentityGroup	その他のオプションの属性
11:11:11:11:11:11	Android	プロファイル済み	<Empty>/<Value>

インポート中の不明なエンドポイントの再プロファイリング

インポートに使用するファイルに、MAC アドレスを持つエンドポイントがあり、それらに割り当てられているエンドポイント プロファイリング ポリシーが不明プロファイルである場合、これらのエンドポイントはインポート中に Cisco ISE でただちに一致するエンドポイント プロファイリング ポリシーに再プロファイリングされます。ただし、不明プロファイルに静的に割り当てられることはありません。エンドポイントに割り当てられているエンドポイント プロファイリング ポリシーが CSV ファイルにない場合、これらのエンドポイントは不明プロファイルに割り当てられ、一致するエンドポイント プロファイリング ポリシーに再プロファイリングされます。次に、Cisco ISE が、インポート中に Xerox_Device プロファイルに一致する不明プロファイルをどのように再プロファイリングするか、および割り当てられていないエンドポイントをどのように再プロファイリングするかを示します。

表 52: 不明プロファイル：ファイルからのインポート

MAC アドレス	Cisco ISE でのインポート前に割り当てられたエンドポイントプロファイリングポリシー	Cisco ISE でのインポート後に割り当てられたエンドポイントプロファイリングポリシー
00:00:00:00:01:02	不明。	Xerox-Device
00:00:00:00:01:03	不明。	Xerox-Device
00:00:00:00:01:04	不明。	Xerox-Device
00:00:00:00:01:05	プロファイルがエンドポイントに割り当てられていない場合、そのエンドポイントは不明プロファイルに割り当てられ、一致するプロファイルに再プロファイリングされます。	Xerox-Device

インポートされない無効な属性を持つエンドポイント

CSV ファイルに存在するエンドポイントのいずれかに無効な属性がある場合、エンドポイントはインポートされず、エラー メッセージが表示されます。

たとえば、エンドポイントがインポートに使用されるファイル内で無効なプロファイルに割り当てられている場合、それらのエンドポイントは、Cisco ISE には一致するプロファイルがないためインポートされません。エンドポイントが CSV ファイル内の無効なプロファイルに割り当てられている場合、それらのエンドポイントがインポートされない仕組みを下に示します。

表 53: 無効なプロファイル：ファイルからのインポート

MAC アドレス (MAC Address)	Cisco ISE でのインポート前に割り当てられたエンドポイントプロファイリングポリシー	Cisco ISE でのインポート後に割り当てられたエンドポイントプロファイリングポリシー
00:00:00:00:01:02	不明。	Xerox-Device
00:00:00:00:01:05	00:00:00:00:01:05 などのエンドポイントが Cisco ISE 使用可能なプロファイル以外の無効なプロファイルに割り当てられている場合、Cisco ISE では、ポリシー名が無効で、エンドポイントがインポートされないことを示す警告メッセージが表示されます。	エンドポイントは、Cisco ISE 内に一致するプロファイルがないためインポートされません。

LDAP サーバからのエンドポイントのインポート

エンドポイントの MAC アドレス、関連するプロファイル、およびエンドポイント ID グループを LDAP サーバからセキュアにインポートできます。

始める前に

エンドポイントをインポートする前に、LDAP サーバがインストールされていることを確認します。

LDAP サーバからインポートするには、接続設定値およびクエリー設定値を設定する必要があります。接続設定値またはクエリー設定値が Cisco ISE で間違って設定されていると、「LDAP インポートが失敗：（LDAP import failed:）」エラー メッセージが表示されます。

-
- ステップ 1** [コンテキストの可視性 (Context Visibility)] > [エンドポイント (Endpoints)] > [インポート (Import)] > [LDAP からのインポート (Import From LDAP)] の順に選択します。
- ステップ 2** 接続設定の値を入力します。
- ステップ 3** クエリー設定の値を入力します。
- ステップ 4** [送信 (Submit)] をクリックします。
-

カンマ区切り形式ファイルを使用したエンドポイントのエクスポート

選択したエンドポイントまたはすべてのエンドポイントを Cisco ISE サーバから CSV ファイルでエクスポートできます。このファイルで、エンドポイントは MAC アドレス、エンドポイント プロファイリング ポリシー、およびエンドポイント ID グループと、約 75 属性とともに一覧表示されます。Cisco ISE で作成されたカスタム属性は、CSV ファイルにエクスポートすることもでき、「CUSTOM.」というプレフィックスが付けられて、他のエンドポイント属性と区別できます。



- (注) 1 つの導入からエクスポートされたエンドポイントのカスタム属性を別の導入にインポートするには、[管理 (Administration)] > [ID の管理 (Identity Management)] > [設定 (Settings)] > [エンドポイント カスタム属性 (Endpoint Custom Attributes)] ページで同じカスタム属性を作成し、最初の導入で指定したのと同じデータ タイプを使用する必要があります。

[すべてエクスポート (Export All)] では Cisco ISE のすべてのエンドポイントがエクスポートされ、[選択済みのみをエクスポート (Export Selected)] ではユーザが選択したエンドポイントのみがエクスポートされます。デフォルトでは、profiler_endpoints.csv が CSV ファイルであり、Microsoft Office Excel が CSV ファイルを開くデフォルトのアプリケーションです。

-
- ステップ 1** [コンテキストの可視性 (Context Visibility)] > [エンドポイント (Endpoints)] を選択します。
- ステップ 2** [エクスポート (Export)] をクリックし、次のいずれかを選択します。

- [選択済みをエクスポート (Export Selected)] : [エンドポイント (Endpoints)] ページで選択したエンドポイントだけをエクスポートできます。
- [すべてエクスポート (Export All)] : デフォルトで、[エンドポイント (Endpoints)] ページのすべてのエンドポイントをエクスポートできます。

ステップ 3 [OK] をクリックして、`profiler_endpoints.csv` ファイルを保存します。

識別されたエンドポイント

Cisco ISE では、ネットワークに接続してネットワーク リソースを使用する識別されたエンドポイントが、[エンドポイント (Endpoints)] ページに表示されます。エンドポイントは、通常、有線および無線のネットワーク アクセス デバイスと VPN を介してネットワークに接続するネットワーク対応デバイスです。エンドポイントとして、パーソナルコンピュータ、ラップトップ、IP Phone、スマートフォン、ゲームコンソール、プリンタ、ファクス機などがあります。

16 進数形式で表したエンドポイントの MAC アドレスは、常にエンドポイントの一意の表現ですが、それらに関連付けられた属性と値のさまざまなセット（属性と値のペアと呼ばれる）でエンドポイントを識別することもできます。エンドポイントの属性のさまざまなセットは、エンドポイント機能、ネットワーク アクセス デバイスの機能と設定、およびこれらの属性の収集に使用する方法（プローブ）に基づいて収集できます。

動的にプロファイリングされるエンドポイント

エンドポイントは、ネットワークで検出されると、設定されているプロファイリングエンドポイントのプロファイリングポリシーに基づいて動的にプロファイリングされ、プロファイルに応じて一致するエンドポイント ID グループに割り当てられます。

静的にプロファイリングされるエンドポイント

MAC アドレスを使用してエンドポイントを作成し、Cisco ISE のエンドポイント ID グループとともにプロファイルをそのエンドポイントに割り当てると、エンドポイントを静的にプロファイリングすることができます。Cisco ISE では、静的に割り当てられたエンドポイントに対して、プロファイリング ポリシーおよび ID グループを再割り当てしません。

不明なエンドポイント

エンドポイントに対して一致するプロファイリングポリシーがない場合、不明なプロファイリングポリシー（「不明」）を割り当てることで、エンドポイントを不明としてプロファイリングできます。不明なエンドポイント ポリシーにプロファイリングされたエンドポイントの場合、そのエンドポイントに対して収集された属性または属性セットを使用してプロファイルを作成する必要があります。いずれのプロファイルにも一致しないエンドポイントは、不明なエンドポイント ID グループにグループ化されます。

識別されたエンドポイントの、ポリシー サービス ノード データベースへのローカル保存

Cisco ISE は識別されたエンドポイントをポリシー サービス ノードのデータベースにローカルに書き込みます。エンドポイントをデータベースにローカル保存した後は、それらのエンドポイントは、重要な属性がエンドポイントで変更され、他のポリシーサービスノードデータベースに複製されているときにのみ、管理ノードデータベースで利用できる（リモート書き込み）ようになります。

重要な属性は次のとおりです。

- ip
- EndPointPolicy
- MatchedValue
- StaticAssignment
- StaticGroupAssignment
- MatchedPolicyID
- NmapSubnetScanID
- PortalUser
- DeviceRegistrationStatus
- BYODRegistration

Cisco ISE でエンドポイント プロファイル定義を変更した場合、すべてのエンドポイントを再プロファイリングする必要があります。エンドポイント属性を収集するポリシーサービスノードが、これらのエンドポイントの再プロファイリングを担当します。

あるポリシー サービス ノードが、最初は別のポリシー サービス ノードによって属性が収集されていたエンドポイントに関する属性を収集し始めると、エンドポイントの所有権が現在のポリシーサービスノードに移ります。新しいポリシーサービスノードは、前のポリシーサービスノードから最新の属性を取得して、すでに収集されている属性と調整します。

重要な属性がエンドポイントで変更されると、エンドポイントの属性は管理ノードデータベースに自動的に保存され、エンドポイントの最新の重要な変更を使用できます。エンドポイントを所有するポリシー サービス ノードが何らかの理由で使用できない場合、管理 ISE ノードが所有者を失ったエンドポイントを再プロファイリングします。また、このようなエンドポイントに対して新しいポリシー サービス ノードを設定する必要があります。

クラスタのポリシー サービス ノード

Cisco ISE では、ポリシー サービス ノードグループをクラスタとして使用するため、クラスタ内の複数のノードが同じエンドポイントの属性を収集するときに、エンドポイント属性を交換できます。1つのロード バランサの背後に存在する、すべてのポリシー サービス ノードに対するクラスタを作成することを推奨します。

現在のオーナー以外の別のノードが同じエンドポイントの属性を受信した場合、属性をマージし、所有権の変更が必要かどうかを決定するために、現在のオーナーから最新の属性を要求するメッセージをクラスタ全体に送信します。Cisco ISE でノード グループを定義していない場合は、すべてのノードが 1 つのクラスタ内にあると想定されます。

Cisco ISE でエンドポイントの作成と複製への変更は行われません。エンドポイントの所有権の変更のみが、プロファイリングに使用される、静的属性と動的属性から作成される属性のリスト（ホワイト リスト）に基づいて決定されます。

次のいずれかの属性が変更された場合、後続の属性の収集時に、エンドポイントは管理ノードで更新されます。

- ip
- EndPointPolicy
- MatchedValue
- StaticAssignment
- StaticGroupAssignment
- MatchedPolicyID
- NmapSubnetScanID
- PortalUser
- DeviceRegistrationStatus
- BYODRegistration

エンドポイントが管理ノードで編集および保存されている場合、この属性はエンドポイントの現在のオーナーから取得されます。

エンドポイント ID グループの作成

Cisco ISE では、検出したエンドポイントを、対応するエンドポイント ID グループにグループ化します。Cisco ISE では、システム定義された複数のエンドポイントの ID グループが事前に用意されています。[エンドポイント ID グループ (Endpoint Identity Groups)] ページで追加のエンドポイント ID グループを作成することもできます。作成したエンドポイント ID グループを編集または削除できます。システム定義されたエンドポイント ID グループの説明のみを編集できます。これらのグループの名前を編集したり、これらのグループを削除したりすることはできません。

ステップ 1 [管理 (Administration)] > [ID の管理 (Identity Management)] > [グループ (Groups)] > [エンドポイント ID グループ (Endpoint Identity Groups)] を選択します。

ステップ 2 [追加 (Add)] をクリックします。

ステップ 3 作成するエンドポイント ID グループの名前を入力します（エンドポイント ID グループの名前にスペースを入れないでください）。

ステップ 4 作成するエンドポイント ID グループの説明を入力します。

ステップ 5 [親グループ (Parent Group)] ドロップダウン リストをクリックして、新しく作成したエンドポイント ID グループを関連付けるエンドポイント ID グループを選択します。

ステップ 6 [送信 (Submit)] をクリックします。

識別されたエンドポイントの、エンドポイント ID グループでのグループ化

Cisco ISE では、エンドポイント プロファイリング ポリシーに基づいて、検出されたエンドポイントを対応するエンドポイント ID グループにグループ化します。プロファイリング ポリシーは階層構造になっており、Cisco ISE のエンドポイント ID グループ レベルで適用されます。エンドポイントを実エンドポイント ID グループにグループ化し、プロファイリング ポリシーを実エンドポイント ID グループに適用すると、Cisco ISE により、対応するエンドポイント プロファイリング ポリシーを確認してエンドポイント プロファイルへのエンドポイントのマッピングを決定できます。

Cisco ISE によってエンドポイント ID グループのセットがデフォルトで作成され、これを使用して、エンドポイントを動的または静的に割り当てできる独自の ID グループを作成できます。エンドポイント ID グループを作成し、システムが作成した ID グループの 1 つにその ID グループを関連付けることができます。また、自分が作成したエンドポイントをシステム内のいずれかの ID グループに静的に割り当てることができ、ID グループがプロファイリング サービスで再割り当てされることはありません。

エンドポイントに対して作成されるデフォルトのエンドポイント ID グループ

Cisco ISE は次の 5 つのエンドポイント ID グループをデフォルトで作成します。ブラックリスト、GuestEndpoints、プロファイル済み、RegisteredDevices、不明。さらに、プロファイル済み（親）ID グループに関連付けられている Cisco-IP-Phone やワークステーションなどの追加の 2 つの ID グループを作成します。親グループは、システムに存在するデフォルトの ID グループです。

Cisco ISE は次のエンドポイント ID グループを作成します。

- **ブラックリスト**：このエンドポイント ID グループには、Cisco ISE でこのグループに静的に割り当てられたエンドポイントおよびデバイス登録ポータルでブラックリストに記載されたエンドポイントが含まれます。許可プロファイルを Cisco ISE で定義して、このグループのエンドポイントへのネットワーク アクセスを許可または拒否できます。
- **GuestEndpoints**：このエンドポイント ID グループには、ゲストユーザが使用するエンドポイントが含まれます。
- **プロファイル済み**：このエンドポイント ID グループには、Cisco ISE の Cisco IP Phone およびワークステーションを除くエンドポイント プロファイリング ポリシーに一致するエンドポイントが含まれます。
- **登録済みデバイス**：このエンドポイント ID グループには、デバイス登録ポータルを介して従業員が追加した登録済みデバイスであるエンドポイントが含まれます。プロファイリング サービスは通常、これらのデバイスがこのグループに割り当てられている場合、これらのデバイスを引き続きプロファイリングします。エンドポイントは Cisco ISE のこのグループに静的に割り当てられ、プロファイリング サービスがこれらのエンドポイントを他

一致するエンドポイント プロファイリング ポリシーに対して作成されるエンドポイント ID グループ

の ID グループに割り当ててはできません。これらのデバイスは、エンドポイント リストの他のエンドポイントと同様に表示されます。デバイス登録ポータルを介して追加されたこれらのデバイスに対して、Cisco ISE の [エンドポイント (Endpoints)] ページのエンドポイントリストで編集、削除およびブラックリストへの記載を実行できます。デバイス登録ポータルでブラックリストに記載されたデバイスは、ブラックリストエンドポイント ID グループに割り当てられ、Cisco ISE に存在する許可プロファイルは、ブラックリストに記載されたデバイスを URL (「無許可ネットワークアクセス」と表示される、ブラックリストに記載されたデバイスのデフォルト ポータル ページ) にリダイレクトします。

- 不明：このエンドポイント ID グループには、Cisco ISE のプロファイルに一致しないエンドポイントが含まれます。

上記のシステムで作成されたエンドポイント ID グループに加えて、Cisco ISE ではプロファイル済み ID グループに関連付けられる次のエンドポイント ID グループが作成されます。

- Cisco-IP-Phone：ネットワーク上のすべてのプロファイル済み Cisco IP Phone が含まれる ID グループです。
- ワークステーション：ネットワーク上のすべてのプロファイル済みワークステーションが含まれる ID グループです。

一致するエンドポイント プロファイリング ポリシーに対して作成されるエンドポイント ID グループ

既存のポリシーと一致するエンドポイント ポリシーがある場合、プロファイリング サービスは一致するエンドポイント ID グループを作成できます。この ID グループは、プロファイル済みエンドポイント ID グループの子になります。エンドポイント ポリシーを作成する場合、[プロファイリング ポリシー (Profiling Policies)] ページの [一致する ID グループの作成 (Create Matching Identity Group)] チェックボックスをオンにして、一致するエンドポイント ID グループを作成できます。プロファイルのマッピングが削除されない限り、一致する ID グループは削除できません。

エンドポイント ID グループでの静的なエンドポイントの追加

エンドポイント ID グループの静的に追加されたエンドポイントを追加または削除できます。

[エンドポイント (Endpoints)] ウィジェットのエンドポイントのみを特定の ID グループに追加できます。エンドポイントを特定のエンドポイント ID グループに追加した場合、そのエンドポイントは、前に動的にグループ化されたエンドポイント ID グループから移動されます。

エンドポイントを最近追加したエンドポイント ID グループから削除すると、そのエンドポイントは、適切な ID グループに再プロファイリングされます。エンドポイントは、システムから削除されませんが、エンドポイントの ID グループからのみ削除されます。

ステップ 1 [管理 (Administration)] > [ID の管理 (Identity Management)] > [グループ (Groups)] > [エンドポイント ID グループ (Endpoint Identity Groups)] を選択します。

ステップ 2 エンドポイント ID グループを選択して [編集 (Edit)] をクリックします。

ステップ 3 [追加 (Add)] をクリックします。

- ステップ 4** [エンドポイント (Endpoints)] ウィジェットでエンドポイントを選択して、選択したエンドポイントをエンドポイント ID グループに追加します。
- ステップ 5** [エンドポイント グループ リスト (Endpoint Group List)] リンクをクリックして、[エンドポイント ID グループ (Endpoint Identity Groups)] ページに戻ります。

ダイナミック エンドポイントの、ID グループへの追加または削除後の再プロファイリング

エンドポイント ID グループが静的に割り当てられていない場合、エンドポイント ID グループに追加した、またはエンドポイント ID グループから削除したエンドポイントは、再プロファイリングされます。ISE プロファイラにより動的に識別されたエンドポイントは、適切なエンドポイント ID グループに表示されます。動的に追加されたエンドポイントをエンドポイント ID グループから削除した場合、Cisco ISE では、エンドポイント ID グループからエンドポイントを正常に削除したが、それらのエンドポイントをエンドポイント ID グループに再プロファイリングして戻すことを示すメッセージが表示されます。

許可ルールで使用されるエンドポイント ID グループ

エンドポイント ID グループを許可ポリシーで効率的に使用して、検出されたエンドポイントに適切なネットワーク アクセス権限を付与することができます。たとえば、すべてのタイプの Cisco IP Phone 用の許可ルールが、デフォルトで、Cisco ISE の [ポリシー (Policy)] > [認証 (Authorization)] > [標準 (Standard)] > [ポリシー (Policy)] で使用できます。

エンドポイント プロファイリング ポリシーがスタンドアロン ポリシー (他のエンドポイント プロファイリング ポリシーの親でない) であるか、またはエンドポイント プロファイリング ポリシーの親ポリシーが無効でないことを確認する必要があります。

プロファイラ フィード サービス

プロファイラ条件、例外アクション、および NMAP スキャンアクションが、シスコ提供または管理者作成 (システム タイプ属性を参照) として分類されます。また、エンドポイント プロファイリング ポリシーは、シスコ提供、管理者作成、または管理者による変更 (システム タイプ属性を参照) として分類されます。

システムタイプ属性によって、プロファイラ条件、例外アクション、NMAP スキャンアクション、およびエンドポイント プロファイリング ポリシーに対して異なる操作を実行できます。シスコ提供の条件、例外アクション、NMAP スキャンアクションは編集または削除できません。シスコが提供するエンドポイントポリシーは削除できません。ポリシーが編集されると、管理者によって変更されたと見なされます。管理者によって変更されたポリシーが削除されると、それが基づいていたシスコ提供ポリシーの最新のバージョンに置き換えられます。

新規および更新されたエンドポイント プロファイリング ポリシーや更新された OUI データベースを、指定された Cisco フィード サーバからの、サブスクリプションを介した Cisco ISE へのフィードとして取得できます。また、適用、成功、および失敗メッセージに対して設定した、Cisco ISE の管理者としての電子メール アドレスに電子メール通知を受信できます。通知を受信するために追加の加入者情報も提供できます。レコードを維持するために加入者情報をシスコに送り返すことができ、それらは特権および機密として処理されます。

、Cisco ISE は毎日ローカル Cisco ISE サーバのタイム ゾーンの午前 1:00 にフィード サービス ポリシーと OUI データベースの更新をダウンロードします。Cisco ISE は、これらのダウンロードされたフィード サービス ポリシーを自動的に適用し、また、これらの変更を以前の状態に復元できるように一連の変更を保存します。最後に適用した一連の変更から復元すると、新しく追加されたエンドポイント プロファイリング ポリシーは削除され、更新されたエンドポイント プロファイリング ポリシーは以前の状態に復元されます。さらに、プロファイラ フィード サービスは自動的に無効になります。

また、オフラインモードで手動でフィード サービスを更新することもできます。ISE 展開をシスコ フィード サービスに接続できない場合には、このオプションを使用して更新プログラムを手動でダウンロードすることができます。

更新が行われるとき、シスコ提供のプロファイリング ポリシーと、以前の更新で変更されたエンドポイント プロファイリング ポリシーのみが更新されます。シスコ提供の無効のプロファイリング ポリシーも更新されますが、無効のままです。管理者作成または管理者による変更のプロファイリング ポリシーは、上書きされません。管理者による変更のエンドポイント プロファイリング ポリシーをシスコ提供のエンドポイント プロファイリング ポリシーに復元する場合は、管理者による変更のエンドポイント プロファイリング ポリシーを削除するか、または管理者による変更のエンドポイント プロファイリング ポリシーを以前のシスコ提供のエンドポイント プロファイリング ポリシーに復元する必要があります。



- (注) 60 日間のうち、ライセンスがコンプライアンス外 (OOC) となっている日数が 45 日間に達すると、フィード サービスからの更新が許可されなくなります。ライセンスがコンプライアンス外になるのは、ライセンスの有効期限が切れるか、または使用が許可されているセッション数を超えた時点です。

OUI フィード サービス

指定されたシスコ フィード サーバは、<http://standards.ieee.org/develop/regauth/oui/oui.txt> から更新済みの OUI データベースをダウンロードします。これは、MAC OUI に関連付けられたベンダーのリストです。更新された OUI データベースは、Cisco ISE が自身のデータベースにダウンロードするフィードとして、ISE 展開で使用できます。Cisco ISE はエンドポイントを更新してから、エンドポイントの再プロファイリングを始めます。

指定されたシスコ フィード サーバは、<https://ise.cisco.com:8443/feedserver/> にあります。サービスへのアクセスに問題がある場合は、（たとえば、ファイアウォールやプロキシサーバのような）ネットワークセキュリティ コンポーネントで、この URL に対する直接アクセスが許可されていることを確認します。

プロファイラ フィード サービスの設定

プロファイラ フィード サービスは、Cisco フィード サーバから新規および更新されたエンドポイント プロファイリング ポリシーと MAC OUI データベース更新を取得します。フィード サービスが使用できない場合、またはその他のエラーが発生した場合は、操作監査レポートで報告されます。

フィード サービス使用レポートをシスコに返信するように Cisco ISE を設定できます。そのレポートでは、次の情報がシスコに送信されます。

- Hostname : Cisco ISE ホスト名
- MaxCount : エンドポイントの合計数
- ProfiledCount : プロファイリングされたエンドポイント カウント
- UnknownCount : 不明なエンドポイント カウント
- MatchSystemProfilesCount : シスコ提供のプロファイル カウント
- UserCreatedProfiles : ユーザ作成のプロファイル カウント

シスコから提供されるプロファイリング ポリシーの CoA タイプを変更できます。フィード サービスがそのポリシーを更新すると、CoA タイプは変更されませんが、そのポリシーの残りの属性は引き続き更新されます。

始める前に

分散展開またはスタンドアロン ISE ノードでは、Cisco ISE 管理者ポータルからのみプロファイラ フィード サービスを設定できます。

フィード更新について管理者ポータルから電子メール通知を送信する場合は、Simple Mail Transfer Protocol (SMTP) サーバを設定します ([管理 (Administration)] > [システム (System)] > [設定 (Settings)])。

フィード サービスをオンラインで更新するには、次の手順に従います。

-
- ステップ 1** [管理 (Administration)] > [証明書 (Certificates)] > [信頼できる証明書 (Trusted Certificates)] の順に選択し、Verisign Class 3 Public Primary Certification Authority および Verisign Class 3 Server CA - G3 が有効であることを確認します。
 - ステップ 2** [ワーク センター (Work Centers)] > [プロファイラ (Profiler)] > [フィード (Feeds)] の順に選択します。
[管理 (Administration)] > [フィードサービス (FeedService)] > [プロファイラ (Profiler)] ページでこのオプションにアクセスすることもできます。
 - ステップ 3** [オンライン サブスクリプションの更新 (Online Subscription Update)] タブをクリックします。
 - ステップ 4** [フィードサービス接続のテスト (Test Feed Service Connection)] ボタンをクリックして、Cisco フィード サービスへの接続があり、証明書が有効であることを確認します。
 - ステップ 5** [オンラインサブスクリプション更新の有効化 (Enable Online Subscription Update)] チェック ボックスをオンにします。
 - ステップ 6** HH:MM 形式で時刻 (Cisco ISE サーバのローカル タイム ゾーン) を入力します。デフォルトでは、Cisco ISE フィード サービスは毎日午前 1 時にスケジュールされます。
 - ステップ 7** [ダウンロードが行われたら管理者に通知 (Notify administrator when download occurs)] チェック ボックスをオンにして、[管理者の電子メールアドレス (Administrator email address)] テキストボックスに電子メールアドレスを入力します。Cisco ISE が非機密情報 (今後のリリースでよりよいサービスと追加機能を提供

するために使用される) を収集することを許可する場合、[プロファイリング精度を上げるために Cisco 匿名情報を提供する (Provide Cisco anonymous information to help improve profiling accuracy)] チェック ボックスをオンにします。

ステップ 8 [保存 (Save)] をクリックします。

ステップ 9 [今すぐ更新 (Update Now)] をクリックします。

最後のフィード サービス更新以降に作成された新規および更新されたプロファイルをチェックするために Cisco フィード サーバに連絡するように Cisco ISE に指示します。これによりシステム内のすべてのエンドポイントが再プロファイリングされ、システム負荷が増加する可能性があります。エンドポイント プロファイリング ポリシーの更新のため、現在 Cisco ISE に接続している一部のエンドポイントの許可ポリシーが変更される場合があります。

最後のフィード サービス以降に作成された新規および更新されたプロファイルを更新すると [今すぐ更新 (Update Now)] ボタンは無効になり、ダウンロードの完了後にのみ有効になります。[プロファイラ フィード サービス設定 (Profiler Feed Service Configuration)] ページから別の場所へ移動し、このページに戻ります。

関連トピック

[オフラインでのプロファイラ フィード サービスの設定](#) (821 ページ)

オフラインでのプロファイラ フィード サービスの設定

Cisco ISE と Cisco フィード サーバが直接接続されていないときに、フィード サービスをオフラインで更新できます。Cisco フィード サーバからオフライン更新プログラム パッケージをダウンロードし、Cisco ISE にオフライン フィード更新プログラムを使用してアップロードできます。またフィード サーバに追加される新しいポリシーに関する電子メール通知を設定することもできます。

オフラインでのプロファイラ フィード サービス設定には、次のタスクが含まれます。

1. オフライン更新プログラム パッケージのダウンロード
2. オフライン フィード更新の適用

オフライン更新プログラム パッケージのダウンロード

オフライン更新プログラム パッケージをダウンロードするには、以下のステップに従います。

ステップ 1 [ワーク センター (Work Centers)] > [プロファイラ (Profiler)] > [フィード (Feeds)] の順に選択します。

[管理 (Administration)] > [フィードサービス (FeedService)] > [プロファイラ (Profiler)] ページでこのオプションにアクセスすることもできます。

ステップ 2 [オフライン手動更新 (Offline Manual Update)] タブをクリックします。

ステップ 3 [更新されているプロファイル ポリシーのダウンロード (Download Updated Profile Policies)] リンクをクリックします。フィード サービス パートナー ポータルにリダイレクトされます。

また、ブラウザから <https://ise.cisco.com/partner/> にアクセスして、フィード サービス パートナー ポータルに直接アクセスすることもできます。

- ステップ 4** 初めてのユーザは、各種条件および契約に同意します。
要求を承認するフィード サービス管理者に電子メールが送信されます。承認されると、確認用の電子メールが届きます
- ステップ 5** Cisco.com のクレデンシャルを使用してパートナー ポータルにログインします。
- ステップ 6** [オフライン フィード (Offline Feed)] > [パッケージのダウンロード (Download Package)] の順に選択します。
- ステップ 7** [パッケージの生成 (Generate Package)] をクリックします。
- ステップ 8** [オフライン 更新プログラム パッケージの内容を表示するにはクリックしてください (Click to View the Offline Update Package contents)] リンクをクリックして、生成したパッケージに含まれるすべてのプロファイルと OUI を表示します。
- [フィード プロファイラ 1 (Feed Profiler 1)] と [フィード OUI (Feed OUI)] の下のポリシーは Cisco ISE の全バージョンにダウンロードされます。
 - [フィード プロファイラ 2 (Feed Profiler 2)] の下のポリシーは Cisco ISE リリース 1.3 以降のみにダウンロードされます。
 - [フィード プロファイラ 3 (Feed Profiler 2)] の下のポリシーは Cisco ISE リリース 2.1 以降のみにダウンロードされます。
- ステップ 9** [パッケージのダウンロード (Download Package)] をクリックして、ローカル システムにファイルを保存します。
保存したファイルを Cisco ISE サーバにアップロードして、ダウンロードしたパッケージのフィード更新プログラムを適用できます。

オフライン フィード更新の適用

ダウンロードしたオフライン フィード更新を適用するには：

始める前に

フィード更新を適用する前に、オフライン更新プログラムパッケージをダウンロードしている必要があります。

-
- ステップ 1** [ワーク センター (Work Centers)] > [プロファイラ (Profiler)] > [フィード (Feeds)] の順に選択します。
[管理 (Administration)] > [フィード サービス (FeedService)] > [プロファイラ (Profiler)] ページでこのオプションにアクセスすることもできます。
- ステップ 2** [オフライン手動更新 (Offline Manual Update)] タブをクリックします。
- ステップ 3** [参照 (Browse)] をクリックして、ダウンロードしたプロファイラ フィード パッケージを選択します。

ステップ 4 [更新の適用 (Apply Update)] をクリックします。

プロファイルと OUI の更新に関する電子メール通知の設定

プロファイルと OUI の更新通知を受信する電子メール アドレスを設定できます。

電子メール通知を設定するには、次の手順に従います。

ステップ 1 [オフライン更新プログラムパッケージのダウンロード](#) セクションの手順 1 ～ 5 を実行し、フィードサービス パートナー ポータルに移動します。

ステップ 2 [オフライン フィード (Offline Feed)] > [電子メール設定 (Email Preferences)] を選択します。

ステップ 3 通知を受信するには、[通知の有効化 (Enable Notifications)] チェック ボックスをオンにします。

ステップ 4 新しい更新通知を受信する頻度を設定するには、[日数 (days)] ドロップダウン リストから日数を選択します。

ステップ 5 電子メール アドレスまたはアドレスを入力し、[保存 (Save)] をクリックします。

フィード更新の取り消し

前回の更新で更新されたエンドポイントプロファイリング ポリシーに戻り、プロファイラ フィードサービスの前回の更新により新しく追加されたが、エンドポイントプロファイリング ポリシーおよび OUI を削除できます。

エンドポイントプロファイリング ポリシーは、フィード サーバからの更新後に変更された場合、システムで変更されません。

ステップ 1 [ワーク センター (Work Centers)] > [プロファイラ (Profiler)] > [フィード (Feeds)] の順に選択します。

ステップ 2 変更設定監査レポートで設定変更を表示する場合は、[更新レポート ページに移動 (Go to Update Report Page)] をクリックします。

ステップ 3 [最新を元に戻す (Undo Latest)] をクリックします。

プロファイラ レポート

Cisco ISE には、エンドポイントプロファイリングに関するさまざまなレポートと、ネットワークの管理に使用できるトラブルシューティングツールが用意されています。現在のデータに加えて履歴のレポートを生成できます。レポートの一部をドリルダウンして詳細を表示できます。大規模なレポートの場合、レポートをスケジュールし、さまざまな形式でダウンロードすることもできます。

[操作 (Operations)] > [レポート (Reports)] > [エンドポイントとユーザ (Endpoints and Users)] からエンドポイントに関する次のレポートを実行できます。

- エンドポイント セッション履歴
- プロファイリングされたエンドポイントの概要
- エンドポイント プロファイルの変更
- エンドポイントによる上位承認
- 登録済みエンドポイント

エンドポイントの異常な動作の検出

Cisco ISE により、不正な MAC アドレスの使用からネットワークが保護されます。ISE は MAC アドレススプーフィングに関与しているエンドポイントを検出し、疑わしいエンドポイントの権限を制限できます。

プロファイラ設定ページには、異常な動作に関する次の 2 つのオプションがあります。

- 異常な動作の検出を有効にする (Enable Anomalous Behavior Detection)
- 異常な動作の適用を有効にする (Enable Anomalous Behavior Enforcement)

異常な動作の検出を有効にすると、Cisco ISE はデータを調査し、NAS ポートタイプ、DHCP クラス ID、およびエンドポイント ポリシーに関連する属性の変更について、既存のデータとの矛盾がないかどうかを確認します。該当する場合、**AnomalousBehavior** 属性が True に設定され、エンドポイントに追加されます。これは、[可視性のコンテキスト (Visibility Context)] ページでエンドポイントをフィルタリングおよび表示する際に役立ちます。該当する MAC アドレスの監査ログも生成されます。

異常な動作の検出を有効にすると、Cisco ISE は、既存のエンドポイントの次の属性が変更されたかどうかを検査します。

1. ポートタイプ—エンドポイントのアクセス方式が変更されたかどうかを判断します。たとえば、有線 Dot1x で接続した MAC アドレスがワイヤレス Dot1x にも使用されているかどうか (あるいはその逆) を判断します。
2. DHCP クラス ID—エンドポイントのクライアントまたはベンダーのタイプが変更されたかどうかを判断します。これは、DHCP クラス ID 属性に特定の値が入力された後で別の値に変更された場合にのみ当てはまります。エンドポイントが静的 IP アドレスで構成されている場合、Cisco ISE での DHCP クラス ID 属性は空です。後で別のデバイスがこのエンドポイントの MAC アドレスをスプーフィングして DHCP を使用すると、クラス ID が空の値から特定の文字列に変更されます。これによって異常な動作の検出がトリガーされることはありません。
3. エンドポイントポリシー—重要なプロファイル変更があったかどうかを判断します。たとえば、エンドポイントのプロファイルが [電話 (Phone)] または [プリンタ (Printer)] から [ワークステーション (Workstation)] に変更されたかどうかを判断します。

異常な動作の適用を有効にすると、異常な動作が検出された時点で CoA が発行されます。これは、[プロファイラ設定 (Profiler Configuration)] ページで設定した許可ルールに基づいて、疑わしいエンドポイントを再許可するときに表示されます。

異常な動作に関する許可ポリシールールをエンドポイントに設定するには、「[異常な動作が発生しているエンドポイントに関する許可ポリシー ルールの設定 \(825 ページ\)](#)」を参照してください。

異常な動作が発生しているエンドポイントに関する許可ポリシー ルールの設定

異常な動作が発生しているエンドポイントに対して実行するアクションを選択するには、[許可ポリシー (Authorization Policy)] ページで対応するルールを設定します。

-
- ステップ 1** [ポリシー (Policy)] > [許可 (Authorization)] を選択します。
- ステップ 2** 既存のルールの [編集 (Edit)] ドロップダウン矢印をクリックし、[新規ルールを上へ挿入 (Insert New Rule Above)] または [新規ルールを下へ挿入 (Insert New Rule Below)] をクリックします。
- ステップ 3** [ルール名 (Rule Name)] にルール名を入力します。
- ステップ 4** [条件 (Conditions)] フィールドの追加アイコンをクリックし、[新しい条件の作成 (高度なオプション) (Create New Condition (Advance Option))] をクリックします。
- ステップ 5** [属性の選択 (Select Attribute)] ドロップダウンから [エンドポイント (Endpoints)] > [異常な動作 (Anomalous Behavior)] を選択します。
- ステップ 6** 最後のフィールドに「true」と入力します。
- ステップ 7** [権限 (Permissions)] 列の追加アイコンをクリックし、[項目の選択 (Select Item)] ドロップダウンリストから必要なアクションを選択します。
- 例：
- 攻撃者や疑わしいエンドポイントにアクセス権限を付与しない場合は、[項目の選択 (Select Item)] ドロップダウンリストから [標準 (Standard)] > [アクセス拒否 (Deny Access)] を選択します。
- ステップ 8** [完了 (Done)] をクリックします。
-

異常な動作が発生しているエンドポイントの表示

次のいずれかのオプションを使用して、異常な動作が発生しているエンドポイントを表示できます。

- [ホーム (Home)] > [概要 (Summary)] > [メトリック (Metrics)] から [異常な動作 (Anomalous Behavior)] をクリックします。この操作により、ページ下部のペインに [異常な動作 (Anomalous Behavior)] 列がある新しいタブが表示されます。

- [コンテキストの可視性 (Context Visibility)] > [エンドポイント (Endpoints)] > [エンドポイントの分類 (Endpoint Classification)] を選択します。ページ下部のペインで [異常な動作 (Anomalous Behavior)] 列を確認できます。
- 次の手順で説明するように、[コンテキストの可視性 (Context Visibility)] ページの [認証 (Authentication)] ビューまたは [侵害されたエンドポイント (Compromised Endpoints)] ビューで新しい [異常な動作 (Anomalous Behavior)] 列を作成できます。

-
- ステップ 1** [コンテキストの可視性 (Context Visibility)] > [エンドポイント (Endpoints)] > [認証 (Authentication)] または [コンテキストの可視性 (Context Visibility)] > [エンドポイント (Endpoints)] > [侵害されたエンドポイント (Compromised Endpoints)] を選択します。
- ステップ 2** ページ下部のペインにある [設定 (Settings)] アイコンをクリックし、[異常な動作 (Anomalous Behavior)] チェックボックスをオンにします。
- ステップ 3** [移動 (Go)] をクリックします。
[認証 (Authentication)] ビューまたは [侵害されたエンドポイント (Compromised Endpoints)] ビューで [異常な動作 (Anomalous Behavior)] 列を表示できます。
-

■ 異常な動作が発生しているエンドポイントの表示



第 25 章

クライアント プロビジョニングの設定

- [Cisco ISE でのクライアント プロビジョニングの設定 \(858 ページ\)](#)
- [クライアント プロビジョニン リソース \(859 ページ\)](#)
- [シスコからのクライアント プロビジョニング リソースの追加 \(860 ページ\)](#)
- [ローカルマシンからのシスコ提供のクライアント プロビジョニング リソースの追加 \(861 ページ\)](#)
- [ローカル マシンからの AnyConnect 用の顧客作成リソースの追加 \(862 ページ\)](#)
- [ネイティブ サプリカント プロファイルの作成 \(863 ページ\)](#)
- [各種ネットワークでの URL リダイレクトなしでのクライアント プロビジョニング \(865 ページ\)](#)
- [AMP イネーブラ プロファイルの設定 \(867 ページ\)](#)
- [Cisco ISE の Chromebook デバイスのオンボーディングのサポート \(872 ページ\)](#)
- [AnyConnect 設定の作成 \(885 ページ\)](#)
- [AnyConnect と Cisco NAC のエージェント プロファイルの作成 \(887 ページ\)](#)
- [エージェント プロファイル設定のガイドライン \(887 ページ\)](#)
- [クライアント IP アドレスのリフレッシュ設定 \(894 ページ\)](#)
- [ポストチャ プロトコル設定 \(897 ページ\)](#)
- [クライアント ログインセッションの基準 \(902 ページ\)](#)
- [Cisco NAC Agent MSI インストーラを使用したクライアント マシンのプロビジョニング \(903 ページ\)](#)
- [Cisco ISE ポスチャ エージェント \(904 ページ\)](#)
- [AnyConnect \(906 ページ\)](#)
- [Cisco NAC Agent XML ファイルのインストール ディレクトリ \(907 ページ\)](#)
- [Windows クライアント用 Cisco NAC Agent \(908 ページ\)](#)
- [Macintosh クライアント用 Cisco NAC Agent \(910 ページ\)](#)
- [Cisco Web Agent \(910 ページ\)](#)
- [Cisco NAC Agent ログ \(911 ページ\)](#)
- [Cisco NAC Agent のエージェント カスタマイズ ファイルの作成 \(911 ページ\)](#)
- [クライアント プロビジョニング リソース ポリシーの設定 \(925 ページ\)](#)
- [クライアント プロビジョニング レポート \(928 ページ\)](#)
- [クライアント プロビジョニング イベント ログ \(929 ページ\)](#)

Cisco ISE でのクライアント プロビジョニングの設定

クライアントプロビジョニングを有効にして、ユーザがクライアントプロビジョニングリソースをダウンロードし、エージェント プロファイルを設定できるようにします。Windows クライアント、Mac OS X クライアント、およびパーソナルデバイスのネイティブ サプリカント プロファイルのエージェント プロファイルを設定できます。クライアント プロビジョニングを無効にすると、ネットワークにアクセスしようとするユーザには、クライアントプロビジョニングリソースをダウンロードできないことを示す警告メッセージが表示されます。

始める前に

プロキシを使用していて、クライアントプロビジョニングリソースをリモートシステムでホスティングしている場合は、プロキシがクライアントにそのリモートロケーションへのアクセスを許可していることを確認します。

ステップ 1 [管理 (Administration)] > [システム (System)] > [設定 (Settings)] > [クライアント プロビジョニング (Client Provisioning)] の順に選択します。

ステップ 2 [プロビジョニングの有効化 (Enable Provisioning)] ドロップダウンリストから、**Enable** または **Disable** を選択します。

ステップ 3 [自動ダウンロードの有効化 (Enable Automatic Download)] **Enable Automatic Download** ドロップダウン リストから、[有効 (Enable)] **Enable** を選択します。

フィードのダウンロードには、すべての使用可能なクライアントプロビジョニングリソースが含まれています。これらのリソースの一部は、展開に関連していない場合があります。シスコでは、このオプションを設定する代わりに可能な限りリソースを手動でダウンロードすることを推奨します。

ステップ 4 [フィード URL の更新 (Update Feed URL)] : [フィード URL の更新 (Update Feed URL)] テキストボックスに、Cisco ISE で検索するシステム アップデートの URL を指定します。たとえば、クライアントプロビジョニングリソースをダウンロードするためのデフォルト URL は <https://www.cisco.com/web/secure/pmbu/provisioning-update.xml> です。

ネットワークで URL リダイレクション機能 (プロキシ サーバ経由など) を制限しているために、デフォルトの URL へのアクセスに問題がある場合は、Cisco ISE で URL <https://www.perfigo.com/ise/provisioning-update.xml> を指定してください。

ステップ 5 [ネイティブ サプリカントプロビジョニング ポリシーを使用できない (Native Supplcant Provisioning Policy Unavailable)] : デバイスに対するクライアントプロビジョニングリソースがない場合は、ここでフローの進め方を決定します。

- **Allow Network Access** : ユーザは、ネイティブ サプリカント ウィザードをインストールおよび起動せずに、デバイスをネットワークに登録することを許可されます。
- **Apply Defined Authorization Policy** : ユーザは、標準認証および (ネイティブ サプリカントプロビジョニング プロセスではない) 許可ポリシーを適用して Cisco ISE ネットワークへのアクセスを試みる必要があります。このオプションを有効にすると、ユーザ デバイスに対して、ユーザの ID に適用されたすべてのクライアント プロビジョニング ポリシーに従った標準登録が行われます。Cisco ISE ネットワーク

トワークにアクセスするためにユーザのデバイスが証明書を必要とする場合は、第15章の「End_User Web ポータルのセットアップとカスタマイズ」の「カスタム言語テンプレートの追加」の項の説明に従って、カスタマイズ可能なユーザ提示テキストフィールドを使用して有効な証明書を取得して適用する方法もユーザに詳細に指示する必要があります。

ステップ 6 [保存 (Save)] **Save** をクリックします。

次のタスク

クライアントプロビジョニングリソースポリシーを設定します。

関連トピック

[クライアントプロビジョニングリソース](#) (859 ページ)

クライアントプロビジョニングリソース

クライアントプロビジョニングリソースは、エンドポイントがネットワークに接続した後にエンドポイントにダウンロードされます。クライアントプロビジョニングリソースは、デスクトップの場合はコンプライアンスとポスチャエージェントで構成され、電話およびタブレットの場合はネイティブサブリカントプロファイルで構成されます。クライアントプロビジョニングポリシーによって、これらのプロビジョニングリソースがエンドポイントに割り当てられ、ネットワークセッションが開始します。

クライアントプロビジョニングリソースは、**[ポリシー要素 (Policy Elements)] > [結果 (Results)] > [クライアントプロビジョニング (Client Provisioning)] > [リソース (Resources)]** にリストされます。次のリソースタイプは、**[追加 (Add)]** ボタンをクリックすることでリストに追加できます。

- **[Ciscoサイトのエージェントリソース (Agent resources from Cisco Site)]** : クライアントプロビジョニングポリシーでできるようにする [NAC]、[AnyConnect] および [サブリカントプロビジョニング (Supplicant Provisioning)] ウィザードを選択します。シスコは、新しいリソースを追加したり既存のリソースを更新することで、定期的にこのリソースのリストを更新します。すべてのシスコのリソースおよびリソースの更新を自動的にダウンロードするようにISEを設定することもできます。詳細については、[Cisco ISE でのクライアントプロビジョニングの設定 \(858 ページ\)](#) を参照してください。
- **[ローカルディスクのエージェントリソース (Agent resources from local disk)]** : ISE にアップロードする PC 上のリソースを選択します。[ローカルマシンからのシスコ提供のクライアントプロビジョニングリソースの追加 \(861 ページ\)](#) を参照してください。
- **[AnyConnect設定 (AnyConnect Configuration)]** : クライアントプロビジョニングでできるようにする AnyConnect PC クライアントを選択します。詳細については、「[AnyConnect 設定の作成](#)」を参照してください。
- **[ネイティブサブリカントプロファイル (Native Supplicant Profile)]** : ネットワークの設定が含まれている電話とタブレット用のサブリカントプロファイルを設定します。詳細については、「[ネイティブサブリカントプロファイルの作成](#)」を参照してください。

- [NACエージェントまたはAnyConnect ISEポスチャプロファイル (NAC Agent or AnyConnect ISE Posture Profile)]: エージェント XML プロファイルを作成/配布しない場合は、ここで NAC エージェントと AnyConnect ISE ポスチャを設定します。AnyConnect ISE ポスチャエージェントの詳細については、『[AnyConnect Administrators Guide, ISE Posture Profile Editor](#)』を参照してください。NAC エージェントプロファイルの詳細については、[Cisco NAC Agent のエージェント カスタマイズ ファイルの作成 \(911 ページ\)](#) を参照してください。

クライアントプロビジョニングリソースを作成した後、エンドポイントにクライアントプロビジョニングリソースを適用するクライアントプロビジョニングポリシーを作成します。[クライアントプロビジョニングリソースポリシーの設定 \(925 ページ\)](#) を参照してください。

関連トピック

- [シスコからのクライアントプロビジョニングリソースの追加 \(860 ページ\)](#)
- [ローカルマシンからのシスコ提供のクライアントプロビジョニングリソースの追加 \(861 ページ\)](#)
- [ローカルマシンからの AnyConnect 用の顧客作成リソースの追加 \(862 ページ\)](#)
- [クライアントプロビジョニングリソースの自動ダウンロード](#)
- [クライアントプロビジョニングリソースポリシーの設定 \(925 ページ\)](#)

シスコからのクライアントプロビジョニングリソースの追加

Windows クライアントおよび MAC OS x クライアント用の AnyConnect および Cisco NAC Agent、および Cisco Web Agent のために Cisco.com からクライアントプロビジョニングリソースを追加できます。選択するリソースおよび使用できるネットワーク帯域幅によっては、Cisco ISE にクライアントプロビジョニングリソースをダウンロードするのに数秒から数分かかることがあります。

始める前に

- Cisco ISE で正しいプロキシ設定が設定されていることを確認します。
- Cisco ISE でクライアントプロビジョニングを有効にします。

-
- ステップ 1** [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] > [クライアントプロビジョニング (Client Provisioning)] > [リソース (Resources)] を選択します。
- ステップ 2** [追加 (Add)] > [Cisco サイトのエージェントリソース (Agent resources from Cisco site)] を選択します。
- ステップ 3** [ダウンロードリモートリソース (Download Remote Resources)] ダイアログボックスで選択可能なリストから必要なクライアントプロビジョニングリソースを 1 つ以上選択します。
- ステップ 4** [保存 (Save)] Save をクリックします。
-

次のタスク

Cisco ISE に正常にクライアント プロビジョニング リソースを追加したら、クライアント プロビジョニング リソース ポリシーの設定を開始します。

関連トピック

[クライアント プロビジョニン リソース](#) (859 ページ)

ローカルマシンからのシスコ提供のクライアントプロビジョニング リソースの追加

シスコから以前にダウンロードしたクライアント プロビジョニング リソースがあればローカル ディスクから追加できます。

始める前に

Cisco ISE には、必ず現行のサポートされているリソースのみをアップロードしてください。古いサポートされていないリソース（たとえば、Cisco NAC Agent の古いバージョン）を使用すると、クライアント アクセスで重大な問題が発生する場合があります。

Cisco.com からリソース ファイルを手動でダウンロードする場合は、リリース ノートの「Cisco ISE Offline Updates」の項を参照してください。

-
- ステップ 1 [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] > [クライアント プロビジョニング (Client Provisioning)] > [リソース (Resources)] を選択します。
 - ステップ 2 [追加 (Add)] > [ローカル ディスクのエージェント リソース (Agent resources from local disk)] を選択します。
 - ステップ 3 [カテゴリ (Category)] ドロップダウンから [シスコ提供パッケージ (Cisco Provided Packages)] を選択します。
 - ステップ 4 [参照 (Browse)] **Browse** をクリックし、Cisco ISE にダウンロードするリソース ファイルがあるローカルマシン上のディレクトリに移動します。
以前に Cisco サイトからローカル マシンにダウンロードした AnyConnect、Cisco NAC Agent、および Cisco Web Agent のリソースを追加できます。
 - ステップ 5 [送信 (Submit)] **Submit** をクリックします。
-

次のタスク

Cisco ISE に正常にクライアント プロビジョニング リソースを追加したら、クライアント プロビジョニング リソース ポリシーの設定を開始します。

関連トピック

[クライアント プロビジョニン リソース](#) (859 ページ)

ローカルマシンからの AnyConnect 用の顧客作成リソースの追加

AnyConnect カスタマイズパッケージ、AnyConnect ローカリゼーションパッケージ、AnyConnect プロファイルなどの顧客作成リソースをローカルマシンから Cisco ISE に追加します。

始める前に

AnyConnect の顧客作成リソースがローカルディスクに zip 形式のファイルで使用可能であることを確認します。

-
- ステップ 1** [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] > [クライアントプロビジョニング (Client provisioning)] > [リソース (Resources)] を選択します。
- ステップ 2** [追加 (Add)] をクリックします。
- ステップ 3** [ローカルディスクのエージェントリソース (Agent Resources from local disk)] を選択します。
- ステップ 4** [カテゴリ (Category)] ドロップダウンから [顧客作成のパッケージ (Customer Created Packages)] を選択します。
- ステップ 5** AnyConnect リソースの名前と説明を入力します。
- ステップ 6** [参照 (Browse)] をクリックし、Cisco ISE にダウンロードするリソースファイルがあるローカルマシン上のディレクトリに移動します。
- ステップ 7** Cisco ISE にアップロードする次の AnyConnect リソースを選択します。
- AnyConnect カスタマイゼーションバンドル
 - AnyConnect ローカリゼーションバンドル
 - AnyConnect プロファイル
 - 高度なマルウェア防御 (AMP) イネーブラプロファイル
- ステップ 8** [送信 (Submit)] をクリックします。
[アップロードされた AnyConnect リソース (Uploaded AnyConnect Resources)] 表に、Cisco ISE に追加する AnyConnect リソースが表示されます。
-

次のタスク

AnyConnect エージェントプロファイルの作成

関連トピック

[クライアントプロビジョニングリソース](#) (859 ページ)

ネイティブサブリカントプロファイルの作成

ネイティブサブリカントプロファイルを作成して、ユーザが独自のデバイスを Cisco ISE ネットワークに含めることができます。ユーザがサインインすると、Cisco ISE は、ユーザの承認要件に関連付けられたプロファイルを使用して、必要なサブリカントプロビジョニングウィザードを選択します。ウィザードは、ユーザのパーソナルデバイスを起動して設定し、ネットワークにアクセスします。



(注) プロビジョニングウィザードは、アクティブなインターフェイスのみを設定します。このため、有線接続ユーザと無線接続ユーザは、どちらもアクティブになっている場合を除き、両方のインターフェイスにはプロビジョニングされません。

始める前に

- リモートデバイス登録に TLS デバイスプロトコルを使用しようとしている場合、少なくとも 1 つの Simple Certificate Enrollment Protocol (SCEP) プロファイルを設定します。
- TCP ポート 8909 および UDP ポート 8909 を開き、Cisco NAC Agent、Cisco NAC Web Agent、およびサブリカントプロビジョニングウィザードのインストールを有効にします。ポートの使用法の詳細については、『Cisco Identity Services Engine Hardware Installation Guide』の付録「Cisco ISE Appliance Ports Reference」を参照してください。

ステップ 1 [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] > [クライアントプロビジョニング (Client Provisioning)] > [リソース (Resources)] を選択します。

ステップ 2 [追加 (Add)] > [ネイティブサブリカントプロファイル (Native Supplciant Profile)] を選択します。

ステップ 3 に示す説明を使用して、プロファイルを作成します。 [ネイティブサブリカントプロファイルの設定 \(863 ページ\)](#)

次のタスク

「複数ゲストポータルをサポート」の項の説明に従って、従業員が自分のパーソナルデバイスをネットワークに直接接続できるようにセルフプロビジョニング機能を有効にします。

ネイティブサブリカントプロファイルの設定

[ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] > [クライアントプロビジョニングリソース (Client Provisioning Resources)] の順に選択し、ネイティブサブリカントプロファイルを追加すると、次の設定が表示されます。

- [名前 (Name)] : 作成するネイティブ サプリカント プロファイルの名前。このプロファイルを適用するオペレーティングシステムを選択します。各プロファイルは、ISE がクライアントのネイティブ サプリカントに適用するネットワーク接続の設定を定義します。

ワイヤレス プロファイル

1 つ以上のワイヤレス プロファイルを設定します。クライアントで使用可能にする SSID ごとに 1 つを設定します。

- [SSID名 (SSID Name)] : クライアントが接続する SSID の名前。
- [プロキシ自動コンフィギュレーションファイルの URL (Proxy Auto-Config File URL)] : サプリカントのネットワーク設定を取得するためにクライアントがプロキシに接続する場合は、そのプロキシ サーバへの URL を入力します。
- プロキシホスト/IP (Proxy Host/IP)
- プロキシ ポート (Proxy Port)
- [セキュリティ (Security)] : WPA または WPA2 を使用するようにクライアントを設定します。
- [許可されているプロトコル (Allowed Protocol)] : クライアントが認証サーバに接続するのに使用するプロトコルを設定します (PEAP または EAP-TLS)。
- [証明書テンプレート (Certificate Template)] : TLS の場合は、[管理 (Administration)] > [システム証明書 (System Certificates)] > [認証局 (Certificate Authority)] > [証明書テンプレート (Certificate Templates)] で定義された証明書テンプレートのいずれかを選択します。

オプション設定は、「オプション設定 : *Windows* の場合」の項で説明します。

iOS 設定

- ターゲットネットワークが非表示になっている場合に有効にする (Enable if target network is hidden)

有線 プロファイル

- [許可されているプロトコル (Allowed Protocol)] : クライアントが認証サーバに接続するのに使用するプロトコルを設定します (PEAP または EAP-TLS)。
- [証明書テンプレート (Certificate Template)] : TLS の場合は、[管理 (Administration)] > [システム証明書 (System Certificates)] > [認証局 (Certificate Authority)] > [証明書テンプレート (Certificate Templates)] で定義された証明書テンプレートのいずれかを選択します。

オプション設定 : *Windows* の場合

[オプション (Optional)] を展開すると、Windows クライアントの場合は次のフィールドも使用できます。

- [認証モード (Authentication Mode)] : 許可のクレデンシャルとして、[ユーザ (User)]、[マシン (Machine)] またはその両方を使用するかを決定します。
- [自動的にログイン名とパスワード (およびもしあればドメイン) を使用する (Automatically use logon name and password (and domain if any))] : 認証モードで [ユーザ (User)] を選択すると、ユーザにプロンプトを表示することなくログインおよびパスワードを使用します (その情報が使用できる場合)。
- [高速再接続を有効にする (Enable Fast Reconnect)] : セッションの再開機能が PEAP プロトコル オプションで有効な場合 (これは、[管理 (Administration)] > [システム (System)] > [設定 (Settings)] > [プロトコル (Protocols)] > [PEAP] で設定されます)、PEAP セッションはユーザ クレデンシャルをチェックすることなく再開できます。
- [隔離チェックを有効にする (Enable Quarantine Checks)] : クライアントが隔離されたかどうかを確認します。
- [サーバが暗号化バインド TLV を示さない場合に切断する (Disconnect if server does not present cryptobinding TLV)] : 暗号化バインド TLV がネットワーク接続でサポートされていない場合に切断します。
- [新規サーバまたは信頼できる証明機関の承認をユーザに求めない (Do not prompt user to authorize new servers or trusted certification authorities)] : 自動的にユーザ証明書を受け入れ、ユーザにプロンプトを表示しません。
- [ネットワークが名前 (SSID) をブロードキャストしていなくても接続する (Connect even if the network is not broadcasting its name (SSID))] : ワイヤレス プロファイルの場合のみ。

各種ネットワークでの URL リダイレクトなしでのクライアント プロビジョニング

URL リダイレクトなしのクライアント プロビジョニングは、サードパーティの NAC で CoA がサポートされていない場合に必要です。クライアント プロビジョニングは、URL リダイレクトの有無にかかわらず実行できます。



(注) URL リダイレクションを使用するクライアント プロビジョニングの場合、クライアント マシンにプロキシ設定が構成されている場合は、ブラウザ設定の例外リストに Cisco ISE を追加してください。この設定は、URL リダイレクションを使用するすべてのフロー、BYOD、MDM、ゲスト、およびボスチャに適用されます。たとえば、Windows マシンでは、次の手順を実行します。

1. コントロール パネルから、[Internet Properties] をクリックします。
2. [Connections] タブを選択します。
3. [LAN settings] をクリックします。
4. [プロキシ サーバー] 領域から、[Advanced] をクリックします。
5. [Exceptions] ボックスに Cisco ISE ノードの IP アドレスを入力します。
6. [OK] をクリックします。

各種ネットワークでリダイレクトなしでエンドポイントをプロビジョニングする手順を次に示します。

Dot1X EAP-TLS

1. プロビジョニングされた認証を使用して Cisco ISE ネットワークに接続する
2. ブラウザ ウィンドウを開き、プロビジョニング URL (provisioning.cisco.com) を入力する。
3. 内部ユーザ、AD、LDAP、または SAML を介して CP ポータルにログインする。

AnyConnect がボスチャを実行する。エンドポイントがボスチャ コンプライアンスに基づいて正しいネットワークに移動する。

Dot1X PEAP

1. NSP 経由でユーザ名とパスワードを使用して Cisco ISE ネットワークに接続する
2. ブラウザ ウィンドウを開き、プロビジョニング URL (provisioning.cisco.com) を入力する。
3. 内部ユーザ、AD、LDAP、または SAML を介して CP ポータルにログインする

AnyConnect がボスチャを実行する。エンドポイントがボスチャ コンプライアンスに基づいて正しいネットワークに移動する。

MAB (有線ネットワーク)

1. Cisco ISE ネットワークに接続する。
2. ブラウザ ウィンドウを開き、プロビジョニング URL (provisioning.cisco.com) を入力する。
3. 内部ユーザ、AD、LDAP、または SAML を介して CP ポータルにログインする。

AnyConnect がボスチャを実行する。エンドポイントがボスチャ コンプライアンスに基づいて正しいネットワークに移動する。

MAB（ワイヤレス ネットワーク）

1. Cisco ISE ネットワークに接続する
2. ブラウザウィンドウを開き、プロビジョニング URL（provisioning.cisco.com）を入力する。
3. 内部ユーザ、AD、LDAP、または SAML を介して CP ポータルにログインする。
AnyConnect がポスチャを実行する。ポスチャはワイヤレス 802.1X の場合にのみ開始する。

AMP イネーブラ プロファイルの設定

次の表に、[高度なマルウェア防御（AMP）イネーブラプロファイル（Advanced Malware Protection (AMP) Enabler Profile）] ページのフィールドを示します。ナビゲーションパスは、[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [クライアント プロビジョニング（Client Provisioning）] > [リソース（Resources）] です。

[追加（Add）] ドロップダウン矢印をクリックし、[AMPイネーブラプロファイル（AMP Enabler Profile）] を選択します。

表 54: [AMPイネーブラプロファイル（AMP Enabler Profile）] ページ

フィールド	使用上のガイドライン
[名前（Name）]	ユーザが作成する AMP イネーブラ プロファイルの名前を入力します。
説明	AMP イネーブラ プロファイルの説明を入力します。

フィールド	使用上のガイドライン
AMPイネーブラのインストール (Install AMP Enabler)	<ul style="list-style-type: none"> • Windows インストーラ : Windows OS ソフトウェアの AMP をホストするローカルサーバの URL を指定します。AnyConnect モジュールはこの URL を使用して、エンドポイントに .exe ファイルをダウンロードします。ファイルサイズは約 25 MB です。 • Mac インストーラ : Mac OSX ソフトウェアの AMP をホストするローカルサーバの URL を指定します。AnyConnect モジュールはこの URL を使用して、エンドポイントに .pkg ファイルをダウンロードします。ファイルサイズは約 6 MB です。 <p>[オン (Check)] ボタンは、サーバと通信を行って URL が有効かどうかを確認します。URL が有効の場合は、「ファイルが見つかりました (File found) 」メッセージが表示され、有効でない場合はエラー メッセージが表示されます。</p>
AMPイネーブラのアンインストール (Uninstall AMP Enabler)	エンドポイントからエンドポイントソフトウェアの AMP をアンインストールします。
開始メニューへの追加 (Add to Start Menu)	エンドポイント ソフトウェアの AMP がエンドポイントにインストールされた後、エンドポイントの [開始 (Start)] メニューにエンドポイントソフトウェアの AMP のショートカットを追加します。
デスクトップへの追加 (Add to Desktop)	エンドポイント ソフトウェアの AMP がエンドポイントにインストールされた後、エンドポイントのデスクトップにエンドポイントソフトウェアの AMP のショートカットを追加します。
コンテキストメニューへの追加 (Add to Context Menu)	エンドポイント ソフトウェアの AMP がエンドポイントにインストールされた後、エンドポイントの右クリック コンテキストメニューに [今すぐスキャン (Scan Now)] オプションを追加します。

組み込みプロファイル エディタを使用した AMP イネーブラ プロファイルの作成

ISE 埋め込みプロファイル エディタまたはスタンドアロン エディタを使用して、AMP イネーブラ プロファイルを作成できます。

ISE 埋め込みプロファイル エディタを使用して AMP イネーブル プロファイルを作成するには、次の手順を実行します。

始める前に

- SOURCEfire ポータルからエンドポイント ソフトウェアの AMP をダウンロードし、ローカル サーバでホスティングします。
- [管理 (Administration)] > [証明書 (Certificates)] > [信頼できる証明書 (Trusted Certificates)] に移動して、エンドポイント ソフトウェアの AMP をホストするサーバの証明書を ISE 証明書ストアにインポートします。
- [AMPイネーブラ (AMP Enabler)] オプションが [AnyConnect設定 (AnyConnect Configuration)] ページ ([ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] > [クライアントプロビジョニング (Client provisioning)] > [リソース (Resources)] > [追加 (Add)] > [AnyConnect設定 (AnyConnect Configuration)] > [AnyConnectパッケージの選択 (Select AnyConnect Package)] の [AnyConnectモジュール選択 (AnyConnect Module Selection)] および [プロファイル選択 (Profile Selection)] セクションで選択されていることを確認します。
- SOURCEfire ポータルにログインして、エンドポイント グループのポリシーを作成し、エンドポイント ソフトウェアの AMP をダウンロードする必要があります。ソフトウェアには、選択したポリシーが事前設定されています。2つのイメージ、すなわち Windows OS の場合はエンドポイント ソフトウェアの AMP、Mac OSX の場合はエンドポイント ソフトウェアの AMP の再頒布可能なバージョンをダウンロードする必要があります。ダウンロードされたソフトウェアは、エンタープライズネットワークからアクセスできるサーバでホストされます。

ステップ 1 [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] > [クライアント プロビジョニング (Client Provision)] > [リソース (Resources)] を選択します。

ステップ 2 [追加 (Add)] ドロップダウンをクリックします。

ステップ 3 [AMPイネーブラプロファイル (AMP Enabler Profile)] を選択して、新しい AMP イネーブラ プロファイルを作成します。

ステップ 4 フィールドに適切な値を入力します。

ステップ 5 [送信 (Submit)] をクリックして、プロファイルを [リソース (Resources)] ページに保存します。

スタンドアロン エディタを使用した AMP イネーブラ プロファイルの作成

AnyConnect スタンドアロンエディタを使用して、AMP イネーブラ プロファイルを作成するには、次の手順を実行します。

始める前に

AnyConnect 4.1 スタンドアロン エディタを使用して、XML 形式のプロファイルをアップロードして AMP イネーブラ プロファイルを作成できます。

- Cisco.com から Windows および Mac OS の AnyConnect スタンドアロン プロファイル エディタをダウンロードします。
- スタンドアロン プロファイル エディタを起動し、[AMP イネーブラ プロファイルの設定 (AMP Enabler Profile Settings)] [AMP イネーブラ プロファイルの設定 \(867 ページ\)](#) で指定されているようにフィールドに入力します。
- プロファイルを XML ファイルとしてローカル ディスクに保存します。
- [AMP イネーブラ (AMP Enabler)] オプションが [AnyConnect 設定 (AnyConnect Configuration)] ページ ([ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] > [クライアントプロビジョニング (Client provisioning)] > [リソース (Resources)] > [追加 (Add)] > [AnyConnect 設定 (AnyConnect Configuration)] > [AnyConnect パッケージの選択 (Select AnyConnect Package)] の [AnyConnect モジュール選択 (AnyConnect Module Selection)] および [プロファイル選択 (Profile Selection)] セクションで選択されていることを確認します。

ステップ 1 [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] > [クライアントプロビジョニング (Client provisioning)] > [リソース (Resources)] を選択します。

ステップ 2 [追加 (Add)] をクリックします。

ステップ 3 [ローカルディスクのエージェントリソース (Agent resources from local disk)] を選択します。

ステップ 4 [カテゴリ (Category)] ドロップダウンから [顧客作成のパッケージ (Customer Created Packages)] を選択します。

ステップ 5 [タイプ (Type)] ドロップダウンから [AMP イネーブラ プロファイル (AMP Enabler Profile)] を選択します。

ステップ 6 [名前 (Name)] と [説明 (Description)] に入力します。

ステップ 7 [参照 (Browse)] をクリックして、ローカル ディスクから保存済みプロファイル (XML ファイル) を選択します。次に、カスタマイズされたインストール ファイルの例を示します。

```
<?xml version="1.0" encoding="UTF-8"?>
<FAProfile xsi:noNamespaceSchemaLocation="FAProfile.xsd"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <FAConfiguration>
    <Install>
      <WindowsConnectorLocation>
        https://fa_webserver/ACFA_Mac_FireAMPSetup.exe
```

```
</WindowsConnectorLocation>
<MacConnectorLocation>
https://fa_webserver/ACFA_Mac_FireAMPSetup.exe
</MacConnectorLocation>
<StartMenu>true</StartMenu>
<DesktopIcon>false</DesktopIcon>
<ContextIcon>true</ContextIcon>
</Install>
</FAConfiguration>
</FAProfile>
```

次に、カスタマイズされたアンインストール ファイルの例を示します。

```
<?xml version="1.0" encoding="UTF-8"?>
<FAProfile xsi:noNamespaceSchemaLocation="FAProfile.xsd"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <FAConfiguration>
    <Uninstall>
    </Uninstall>
  </FAConfiguration>
</FAProfile>
```

ステップ 8 [送信 (Submit)] をクリックします。

新しく作成された AMP イネーブラ プロファイルが [リソース (Resources)] ページに表示されます。

一般的な AMP イネーブラ インストール エラーのトラブルシューティング

[Windowsインストーラ (Windows Installer)] または [MACインストーラ (MAC Installer)] テキスト ボックスに SOURCEfire URL を入力して [オン (Check)] をクリックすると、次のエラーのいずれかが発生する場合があります。

- エラー メッセージ: 「MacまたはWindowsのインストーラファイルを含むサーバの証明書がISEによって信頼されていません。(The certificate for the server containing the Mac/Windows installer file is not trusted by ISE.) 信頼証明書を [管理 (Administration)] > [証明書 (Certificates)] > [信頼できる証明書 (Trusted Certificates)] に追加します。(Add a trust certificate to **Administration > Certificates > Trusted Certificates.**)」

このエラー メッセージは、Cisco ISE 証明書ストアに SOURCEfire の信頼できる証明書をインポートしていない場合に表示されます。SOURCEfire の信頼できる証明書を入手し、Cisco ISE の信頼できる証明書ストア ([管理 (Administration)] > [証明書 (Certificates)] > [信頼できる証明書 (Trusted Certificates)]) にインポートします。

- エラーメッセージ: 「インストーラファイルがこの場所で見つかりません。接続の問題である可能性があります。(The installer file is not found at this location, this may be due to a connection issue.) 有効なパスを [インストーラ (Installer)] テキスト ボックスに入力するか、または接続を確認します。(Enter a valid path in the Installer text box or check your connection.)」

このエラー メッセージは、エンドポイントソフトウェアの AMP をホストしているサーバがダウンした場合、または [Windowsインストーラ (Windows Installer)] または [MACインストーラ (MAC Installer)] テキスト ボックスに入力ミスがある場合に表示されます。

- エラーメッセージ：「[Windowsインストーラ（Windows Installer）]または[MACインストーラ（MAC Installer）]テキストボックスに有効なURLが含まれていません。（The Windows/Mac installer text box does not contain a valid URL.）」

このエラーメッセージは、構文的に正しくないURL形式を入力した場合に表示されます。

Cisco ISE の Chromebook デバイスのオンボーディングのサポート

Chromebook デバイスは他のデバイス（Apple、Windows、Android）とは異なり管理型デバイス（Google ドメインによって管理）で、オンボーディングサポートが制限されています。Cisco ISE はネットワークでの Chromebook デバイスのオンボーディングをサポートしています。オンボーディングとは、Cisco ISE による認証の後にネットワークに安全に接続できるように、エンドポイントに必要な設定とファイルを配送するプロセスのことです。このプロセスには、証明書のプロビジョニングやネイティブサブリカントのプロビジョニングが含まれています。ただし、Chromebook デバイスでは、証明書のプロビジョニングのみが実行できます。ネイティブサブリカントのプロビジョニングは、Google 管理コンソールで実行されます。

管理されていない Chromebook デバイスは、安全なネットワークへのオンボーディングができません。

Chromebook オンボーディング プロセスに関与するエンティティは次のとおりです。

- Google 管理者
- ISE 管理者
- Chromebook ユーザ/デバイス
- Google 管理コンソール（Google 管理者が管理）

Google 管理者：

- 次のライセンスの安全性を確保します。
 1. Google 管理コンソール設定のための Google Apps 管理者ライセンス。URL：
<https://admin.google.com>。Google 管理コンソールを使用して、管理者は組織内の人間のための Google サービスを管理できます。
 2. Chromebook のデバイス管理ライセンス。URL：
<https://support.google.com/chrome/a/answer/2717664?hl=en>。Chromebook のデバイス管理ライセンスは、特定の Chromebook デバイスに対して設定を行い、ポリシーを適用するために使用されます。ユーザアクセスの制御、機能のカスタマイズ、ネットワークアクセスの設定などのためのデバイス設定への Google 管理者アクセス権を提供します。
- Google デバイス ライセンスによる Chromebook デバイスのプロビジョニングと登録を促進します。

- Google 管理コンソールを通じて Chromebook デバイスを管理します。
- 各 Chromebook ユーザの Wi-Fi ネットワーク設定のセットアップと管理を行います。
- Chromebook デバイスでアプリケーションの設定と強制されている拡張機能のインストールを行い、Chromebook デバイスを管理します。Chromebook デバイスのオンボーディングには、Chromebook デバイスに Cisco Network Setup Assistant 拡張機能がインストールされている必要があります。これにより、Chromebook デバイスが Cisco ISE に接続し、ISE 証明書をインストールできるようになります。証明書のインストールの操作は管理対象デバイスにのみ許可されるため、この拡張機能は強制的にインストールされます。
- サーバの検証と安全な接続を実現するために、Cisco ISE 証明書が Google 管理コンソールにインストールされていることを確認します。Google 管理者が、証明書がデバイスに対して生成されるか、ユーザに対して生成されるかを決定します。Cisco ISE には次のオプションがあります。
 - Chromebook デバイスを共有しない単一のユーザ用に証明書を生成します。
 - 複数のユーザで共有される Chromebook デバイス用に証明書を生成します。必要な追加設定については、「[Google 管理コンソールでのネットワークの設定と拡張機能の強制](#)」セクションの手順 5 を参照してください。

ISE が Chromebook デバイスで証明書のプロビジョニングを実行するために信頼され、EAP-TLS 証明書ベースの認証が許可されるように、Google 管理者が ISE サーバ証明書をインストールします。Google Chrome バージョン 37 以降は、Chromebook デバイスの証明書ベースの認証をサポートしています。Google 管理者は Google 管理コンソールで ISE プロビジョニングアプリケーションをロードし、ISE から証明書を取得するために Chromebook デバイスで使えるようにする必要があります。

- 推奨される Google ホスト名が、SSL の安全な接続のために WLC で設定された ACL 定義リストのホワイトリストにあることを確認します。[Google サポート](#) ページの推奨されるホスト名のホワイトリストを参照してください。

ISE 管理者：

- 証明書テンプレートの構造を含む、Chromebook OS のネイティブ サプリカント プロファイルを定義します。
- Chromebook ユーザの Cisco ISE で必要な認証ルールとクライアント プロビジョニング ポリシーを作成します。

Chromebook ユーザ：

- Chromebook デバイスを消去し、Google ドメインに登録して、Google 管理者によって定義された適用ポリシーを保護します。
- Chromebook デバイス ポリシーと、Google 管理コンソールによってインストールされた、強制されている Cisco Network Setup Assistant 拡張機能を受信します。
- Google 管理者によって定義されているとおりにプロビジョニングされた SSID に接続して、ブラウザを開いて BYOD ページを表示し、オンボーディングプロセスを開始します。
- Cisco Network Setup Assistant が Chromebook デバイスにクライアント証明書をインストールし、これによりデバイスが EAP-TLS 証明書ベースの認証を行えるようになります。

Google 管理コンソール：

Google 管理コンソールは Chromebook デバイス管理をサポートし、安全なネットワークの設定と、Chromebook への Cisco Network Setup Assistant 証明書管理拡張機能のプッシュができます。この拡張機能は SCEP 要求を Cisco ISE に送信し、クライアント証明書をインストールして、安全な接続とネットワークへのアクセスを可能にします。

共有環境での Chromebook デバイスの使用のベスト プラクティス

Chromebook デバイスが学校や図書館などの共有環境で使用される場合、Chromebook デバイスはさまざまなユーザによって共有されます。シスコが推奨するベストプラクティスの一部は、次のとおりです。

- 特定のユーザ（学生または教授）の名前で Chromebook デバイスをオンボーディングする場合、ユーザの名前が証明書の [件名 (Subject)] フィールドの [共通名 (CN) (Common Name (CN))] に入力されます。また、共有 Chromebook がその特定のユーザの My Devices ポータルに表示されます。そのため、共有デバイスではオンボーディング時に共有クレデンシャルを使用し、特定のユーザの My Devices ポータルのリストにのみデバイスが表示されるようにすることを推奨します。共有アカウントは、個別のアカウントとして管理者または教授が管理し、共有デバイスを制御することができます。
- ISE 管理者は、共有 Chromebook デバイス用のカスタム証明書テンプレートを作成し、ポリシーで使用することができます。たとえば、[件名-共通名 (CN) (Subject-Common Name (CN))] 値に一致する標準の証明書テンプレートを使用する代わりに、証明書の名前 (chrome-shared-grp1 など) を指定して同じ名前を Chromebook デバイスに割り当てることができます。ポリシーは、Chromebook デバイスへのアクセスを許可または拒否するために、名前で一致させるように設計できます。
- ISE 管理者は、（アクセスが制限される必要があるデバイスの）Chromebook オンボーディングを経る必要があるすべての Chromebook デバイスの MAC アドレスを備えたエンドポイントグループを作成することができます。認証ルールは、デバイスタイプ Chromebook とともにこれを呼び出す必要があります。これにより、アクセスが NSP にリダイレクトされます。

Chromebook オンボーディング プロセス

Chromebook オンボーディング プロセスは、次の一連のステップを実行します。

-
- ステップ 1 [Google 管理コンソールでのネットワークの設定と拡張機能の強制](#)。
 - ステップ 2 [Chromebook オンボーディングのための ISE の設定](#)。
 - ステップ 3 [Chromebook デバイスのワイプ](#)。
 - ステップ 4 [Google 管理コンソールへの Chromebook の登録](#)。
 - ステップ 5 [BYOD オンボーディング用の Cisco ISE ネットワークへの Chromebook の接続](#)。
-

Google 管理コンソールでのネットワークの設定と拡張機能の強制

以下のステップは、Google 管理者が実行します。

ステップ 1 Google 管理コンソールにログインします。

- ブラウザで URL <https://admin.google.com> を入力します。
- 必要なユーザ名とパスワードを入力します。
- [Welcome to Admin Console] ページで、[Device Management] をクリックします。
- [Device Management] ページで、[Network] をクリックします。

ステップ 2 管理対象デバイスの Wi-Fi ネットワークをセットアップします。

- [Networks] ページで、[Wi-Fi] をクリックします。
- [Add Wi-Fi] をクリックして、必要な SSID を追加します。詳細については、「[Google 管理コンソール：Wi-Fi ネットワーク設定](#)」ページを参照してください。

MAB フローについては、2 つの SSID を作成し、1 つをオープン ネットワーク用、もう 1 つを証明書認証用にします。オープンネットワークに接続しているとき、Cisco ISE ACL はユーザをクレデンシャルを持つゲスト ポータルにリダイレクトし、認証後に BYOD ポータルにリダイレクトします。

- [追加 (Add)] をクリックします。

ステップ 3 強制拡張機能を作成します。

- [Device Management] ページの [Device Settings] 領域で、[Chrome Management] をクリックします。
- [User Settings] をクリックします。
- 下にスクロールして、[アプリケーションと拡張機能 (Apps and Extensions)] セクションの [強制的にインストールされたアプリケーションと拡張機能 (Force-Installed Apps and Extensions)] オプションで、[強制的にインストールされたアプリケーションの管理 (Manage Force-Installed Apps)] をクリックします。

ステップ 4 強制拡張機能をインストールします。

- [Force-Installed Apps and Extensions] ページで、[Chrome Web Store] をクリックします。
- [Search] テキスト ボックスに「Cisco Network Setup Assistant」と入力して、拡張機能を見つけます。

Chromebook デバイスの Cisco Network Setup Assistant 拡張機能は、Cisco ISE の証明書を要求し、Chromebook デバイスに ISE の証明書をインストールします。証明書のインストールアクションは管理対象デバイスに対してのみ許可されるため、この拡張機能は、強制的にインストールされるように設定する必要があります。登録プロセス中に Chromebook にこの拡張機能がインストールされていない場合は、Cisco ISE の証明書をインストールすることはできません。

拡張機能でサポートされている言語の詳細については、「[Cisco ISE 国際化およびローカリゼーション](#)」のトピックを参照してください。

- [Add] をクリックして、強制的にアプリをインストールします。
- [保存 (Save)] をクリックします。

ステップ 5 (オプション) 複数のユーザに共有されている Chromebook デバイスに証明書をインストールするには、コンフィギュレーション ファイルを定義します。

- a) メモ帳ファイルに次のコードをコピー アンド ペーストして、ローカル ディスクに保存します。

```
{
  "certType": {
    "Value": "system"
  }
}
```

- b) **[Device Management] > [Chromebook Management] > [App Management]** の順に選択します。
 c) **[Cisco Network Setup Assistant]** 拡張機能をクリックします。
 d) **[User Settings]** をクリックし、ドメインを選択します。
 e) **[Upload Configuration File]** をクリックし、ローカル ディスクに保存した .txt ファイルを選択します。

(注) Cisco Network Setup Assistant で複数のユーザが共有するデバイスの証明書を作成するには、このメモ帳ファイルを Google 管理コンソールに追加する必要があります。追加しないと、Cisco NSA はシングル ユーザ用の証明書を作成します。

- f) **[保存 (Save)]** をクリックします。

ステップ 6 (オプション) Chromebook デバイスを共有しないシングル ユーザの証明書をインストールします。

- a) **[Device Management] > [Network] > [Certificates]** の順に選択します。
 b) **[Certificates]** セクションで、**[Add Certificate]** をクリックして、Cisco ISE の証明書ファイルをアップロードします。

次のタスク

Chromebook オンボーディングのために ISE を設定します。

Chromebook オンボーディングのための ISE の設定

始める前に

ISE 管理者は、**[ポリシー (Policy)] > [認証 (Authorization)]** ページで必要なポリシーを作成する必要があります。

認証ポリシーの例を次に示します。

Rule Name: Full_Access_After_Onboarding, Conditions: If RegisteredDevices AND Wireless_802.1x AND Endpoints:BYODRegistration EQUALS Yes AND Certificate: Subject Alternative Name Equals RadiusCalling-Station-ID AND Network Access: EAP-Authentication EQUALS EAP-TLS Then CompliantNetworkAccess.

CompliantNetworkAccess は、**[ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] > [Authorization (認証)] > [認証プロファイル (Authorization Profiles)]** ページで設定されている認証結果です。

ステップ 1 Cisco ISE でネイティブ サプリカント プロファイル (NSP) を設定します。

- a) **[ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)]** の順に選択します。

- b) [クライアントプロビジョニング (Client Provisioning)] > [リソース (Resources)] の順にクリックします。

Chromebook デバイスが新規 Cisco ISE インストールの [クライアントプロビジョニング (Client Provisioning)] ページに表示されます。ただし、アップグレードの場合は、[管理 (Administration)] > [システム (System)] > [設定 (Settings)] > [ポスチャ (Posture)] > [更新 (Updates)] ページからポスチャの更新プログラムをダウンロードする必要があります。

- c) [追加 (Add)] > [ネイティブサプリカントプロファイル (Native Supplicant Profile)] の順にクリックします。
- d) [名前 (Name)] と [説明 (Description)] に入力します。
- e) [オペレーティングシステム (Operating System)] フィールドで、[Chrome OS すべて (Chrome OS All)] を選択します。
- f) [証明書テンプレート (Certificate Template)] フィールドで、必要な証明書テンプレートを選択します。
- g) [送信 (Submit)] をクリックします。SSID が Google 管理コンソールからプロビジョニングされていて、ネイティブサプリカントプロビジョニングフローからではないことを確認します。

ステップ 2 [クライアントプロビジョニング (Client Provisioning)] ページで NSP をマッピングします。

- a) [ポリシー (Policy)] > [クライアントプロビジョニング (Client Provisioning)] の順に選択します。
- b) 結果を定義します。
- クライアントプロビジョニングポリシーの [結果 (Results)] で組み込みのネイティブサプリカント設定 (Cisco-ISE-Chrome-NSP) を選択します。
 - または、新しいルールを作成し、Chromebook デバイス用に作成された [結果 (Result)] が選択されていることを確認します。

Chromebook デバイスのワイプ

Chromebook デバイスは、Google 管理コンソールが Google 管理者により設定された後でワイプされる必要があります。Chromebook ユーザはデバイスをワイプする必要があり、これは拡張を強制し、ネットワークを設定する一度だけの処理です。詳細については、次の URL <https://support.google.com/chrome/a/answer/1360642> を参照してください。

Chromebook ユーザは次の手順を実行します。

ステップ 1 **Esc**□**Refresh**□**Power** キーの組み合わせを押します。画面に黄色い感嘆符 (!) が表示されます。

ステップ 2 開発モードを開始するには、**Ctrl**□**D** キーの組み合わせを押してから、**Enter** キーを押します。画面に赤い感嘆符が表示されます。

ステップ 3 **Ctrl**□**D** キーの組み合わせを押します。Chromebook はローカルデータを削除して、初期状態に戻ります。この削除には約 15 分かかります。

ステップ 4 移行が完了したら、**Space** キーを押してから **Enter** キーを押して、確認モードに戻ります。

ステップ 5 サインインする前に Chromebook を登録します。

次のタスク

Google 管理コンソールに Chromebook を登録します。

Google 管理コンソールへの Chromebook の登録

Chromebook のデバイスをプロビジョニングするには、Chromebook ユーザは最初に Google 管理コンソールページに登録し、デバイスポリシーおよび強制拡張を受信する必要があります。

- ステップ 1 Chromebook のデバイスの電源を入れ、サインオン画面が表示されるまで、画面上の指示に従います。まだサインインしないでください。
- ステップ 2 Chromebook のデバイスにサインインする前に、**Ctrl + Alt + E** のキーの組み合わせを押します。[エンタープライズ登録 (Enterprise Enrolment)] 画面が表示されます。
- ステップ 3 E メールアドレスを入力し、[次へ (Next)] をクリックします。
次のメッセージが表示されます: 「デバイスは企業管理用に正しく登録されています (Your device has successfully been enrolled for enterprise management.)」。
- ステップ 4 [完了 (Done)] をクリックします。
- ステップ 5 Google 管理のようこそレターからのユーザ名とパスワード、または登録資格があるアカウントの既存の Google アプリケーション ユーザのユーザ名とパスワードを入力します。
- ステップ 6 [デバイスの登録 (Enroll Device)] をクリックします。デバイスが正常に登録されると、確認メッセージが表示されます。

Chromebook の登録の処理は一度だけであることに注意してください。

BYOD オンボーディング用の Cisco ISE ネットワークへの Chromebook の接続

この手順はデュアル SSID、EAP-TLS プロトコルを使用した Dot1x ネットワークへのオープンネットワーク用です。Chromebook ユーザは次の手順を実行します。



- (注) デュアル SSID、EAP-TLS ネットワークへの Dot1x PEAP を使用する場合、ネットワーク サブリカント (Web ブラウザではありません) にクレデンシャルを入力することで、ネットワークに接続する必要があります。

ステップ 1 Chromebook デバイスで [設定 (Settings)] をクリックします。

ステップ 2 [インターネット接続 (Internet Connection)] セクションで、[Wi-Fi ネットワークをプロビジョニングする (Provisioning Wi-Fi Network)] をクリックしてから、該当するネットワークをクリックします。

ステップ 3 クレデンシャルを持つゲスト ポータルにリダイレクトされます。

1. [サインオン (Sign On)] ページで、[ユーザ名 (Username)] と [パスワード (Password)] を入力します。
2. [サインオン (Sign-on)] をクリックします。

ステップ 4 BYOD のウェルカム ページで、[開始 (Start)] をクリックします。

ステップ 5 [デバイス情報 (Device Information)] フィールドにデバイスの名前と説明を入力します。たとえば、パーソナル デバイス : 学校で使用するジェーンの Chromebook、または共有デバイス : ライブラリ Chromebook #1 または教室 1 Chromebook #1。

ステップ 6 [続行 (Continue)] をクリックします。

ステップ 7 [Cisco Network Setup Assistant] ダイアログ ボックスで [はい (Yes)] をクリックして、セキュアなネットワークにアクセスするための証明書をインストールします。

セキュアな Wi-Fi が Google の管理者により設定されている場合、自動的に接続されます。ただし、接続されていない場合は、使用可能なネットワークからセキュアな SSID を選択します。

すでにドメインに登録され、Cisco Network Setup Assistant の拡張を取得済みの Chromebook デバイス ユーザは、自動更新を待たずに、拡張を更新できます。次の手順を実行して、拡張を更新できます。

1. Chromebook デバイスで、ブラウザを開き、次の URL を入力してください。 **chrome://Extensions**
2. [開発者モード (Developer Mode)] チェック ボックスをオンにします。
3. [今すぐ拡張を更新 (Update Extensions Now)] をクリックします。
4. Cisco Network Setup Assistant の拡張バージョンが 2.1.0.35 以上であることを確認します。

Google 管理コンソール : Wi-Fi ネットワーク設定

Wi-Fi ネットワークの設定を使用して、顧客ネットワークの SSID を設定するか、または証明書属性 (EAP-TLS 用) を使用して証明書を照合します。証明書が Chromebook にインストールされるときに、Google 管理設定と同期されます。接続は、定義された証明書属性のいずれかが SSID 設定と一致したときのみ確立されます。

以下に、EAP-TLS、PEAP およびオープン ネットワーク フローに特有な必須フィールドを示します。これらは、Google 管理コンソール ページで各 Chromebook ユーザに対し、Wi-Fi ネットワークを設定するように Google 管理者が設定します。([デバイス管理 (Device Administration)] > [ネットワーク (Network)] > [Wi-Fi] > [Wi-Fi の追加 (Add Wi-Fi)])。

フィールド	EAP-TLS	PEAP	オープン (Open)
[名前 (Name)]	ネットワーク接続の名前を入力します。	ネットワーク接続の名前を入力します。	ネットワーク接続の名前を入力します。

フィールド	EAP-TLS	PEAP	オープン (Open)
サービスセット識別子 (SSID)	SSID (たとえば、tls_ssid) を入力します。	SSID (たとえば、tls_ssid) を入力します。	SSID (たとえば、tls_ssid) を入力します。
この SSID はブロードキャストされません	オプションを選択します。	オプションを選択します。	オプションを選択します。
自動的に接続	オプションを選択します。	オプションを選択します。	オプションを選択します。
セキュリティ タイプ	WPA/WPA2 Enterprise (802.1x)	WPA/WPA2 Enterprise (802.1x)	オープン (Open)
Extensible Authentication Protocol	EAP-TLS	PEAP	—
内部プロトコル	—	<ul style="list-style-type: none"> • 自動 (Automatic) • MSCHAP v2 (オプションを選択) • MD5 • PAP • MSCHAP • GTC 	—
外部 ID	—	—	—
[ユーザ名 (Username)]	必要に応じて、固定値を設定するか、またはユーザログインから変数を使用します : \${LOGIN_ID} または \${LOGIN_EMAIL}。	ISE (内部 ISE ユーザ / AD / その他の ISE ID) とパスワードフィールドに対し認証する PEAP クレデンシャルを入力します。	—
サーバ認証局 (Server Certificate Authority)	ISE 証明書を選択します ([デバイス管理 (Device Administration)] > [ネットワーク (Network)] > [証明書 (Certificates)] からインポートされます)。	ISE 証明書を選択します ([デバイス管理 (Device Administration)] > [ネットワーク (Network)] > [証明書 (Certificates)] からインポートされます)。	—

フィールド	EAP-TLS	PEAP	オープン (Open)
プラットフォームによるこの Wi-Fi ネットワークへのアクセス制限	<ul style="list-style-type: none"> モバイル デバイスを選択します。 Chromebooks を選択します。 	<ul style="list-style-type: none"> モバイル デバイスを選択します。 Chromebooks を選択します。 	—
クライアントの登録 URL	登録されていないユーザに対して Chromebook デバイスのブラウザがリダイレクトされる先の URL を入力します。未登録のユーザをリダイレクトするために、ワイヤレス LAN コントローラの ACL を設定します。	—	—

フィールド	EAP-TLS	PEAP	オープン (Open)
発行者パターン	<p>証明書属性。少なくとも1つの属性を、インストールされた証明書属性に一致する、発行者パターンまたはサブジェクトパターンから選択してください。証明書を受け入れるように Chromebook デバイスに一致する証明書属性を指定します。</p> <ul style="list-style-type: none"> • 共通名：証明書のサブジェクトフィールド、またはノードのFQDNと一致している必要がある証明書のサブジェクトフィールドのワイルドカードドメインを参照します。 • 地域：証明書のサブジェクトに関連するテスト地域（市）を参照してください。 • 組織：証明書のサブジェクトに関連する組織名を参照します。 • 組織単位：証明書のサブジェクトに関連する組織単位の名前を参照します。 	—	—

フィールド	EAP-TLS	PEAP	オープン (Open)
サブジェクトパターン	<p>証明書属性。少なくとも 1 つの属性を、インストールされた証明書属性に一致する、発行者パターンまたはサブジェクトパターンから選択してください。証明書を受け入れるように Chromebook デバイスに一致する証明書属性を指定します。</p> <ul style="list-style-type: none"> • 共通名：証明書のサブジェクトフィールド、またはノードの FQDN と一致している必要がある証明書のサブジェクトフィールドのワイルドカードドメインを参照します。 • 地域：証明書のサブジェクトに関連するテスト地域（市）を参照してください。 • 組織：証明書のサブジェクトに関連する組織名を参照します。 • 組織単位：証明書のサブジェクトに関連する組織単位の名前を参照します。 	—	—

フィールド	EAP-TLS	PEAP	オープン (Open)
プロキシの設定	<ul style="list-style-type: none"> インターネットへの直接接続（選択済み） 手動でのプロキシ設定 自動でのプロキシ設定 	<ul style="list-style-type: none"> インターネットへの直接接続（選択済み） 手動でのプロキシ設定 自動でのプロキシ設定 	—
ネットワークの適用	By User	By User	—

Cisco ISE での Chromebook デバイス アクティビティのモニタ

Cisco ISE は Chromebook のデバイスの認証と認可に関する情報を表示するさまざまなレポートとログを提供します。オン デマンドまたは定期的にこれらのレポートを実行できます。[操作 (Operations)] > [RADIUS] > [ライブ ログ (Live Logs)] ページで、認証方法（たとえば、802.1x）と認証プロトコル（たとえば、EAP-TLS）を表示することができます。また、[ワーク センター (Work Center)] > [ネットワーク アクセス (Network Access)] > [ID (Identities)] > [エンドポイント (Endpoints)] ページに移動して、Chromebook デバイスとして分類されたエンドポイントの数も識別できます。

オンボーディング中の Chromebook デバイスのトラブルシューティング

このセクションでは、Chromebook デバイスのオンボーディング中に発生する可能性のある問題について説明します。

- エラー：webstore から拡張をインストールできない：webstore から拡張をインストールできません。これは、ネットワーク管理者によって Chromebook デバイスに自動的にインストールされます。
- エラー：証明書のインストールを完了したが、セキュアなネットワークに接続できない：管理コンソールで、インストールした証明書が定義された発行者とサブジェクトの属性パターンと一致していることを確認します。以下からインストールされた証明書に関する情報を得ることができます。<chrome://settings/certificates>
- エラー：Chromebook でセキュアなネットワークに手動で接続しようとして、「ネットワーク証明書の取得 (Obtain Network Certificate)」のエラー メッセージが表示される：[新しい証明書の取得 (Get New Certificate)] をクリックしてブラウザを開き、証明書をインストールする ISE BYOD にリダイレクトされます。ただし、セキュアなネットワークに接続できない場合は、管理コンソールで、インストールされた証明書が定義された発行者とサブジェクトの属性パターンと一致していることを確認します。

- エラー：[新しい証明書の取得 (Get New Certificate)] をクリックしたが、www.cisco.com に転送される：ユーザはISEにリダイレクトされ、証明書のインストールプロセスを開始するために、プロビジョニングする SSID に接続する必要があります。適切なアクセス リストがこのネットワーク用に定義されていることを確認します。
- エラー：エラーメッセージ「管理対象デバイスのみがこの拡張を使用できます。ヘルプデスクまたはネットワーク管理者にお問い合わせください (Only managed devices can use this extension. Contact helpdesk or network administrator)」が表示される：Chromebook は管理対象デバイスであり、デバイスで証明書をインストールするには、拡張は、Chrome OS API にアクセスするために強制インストールとして設定する必要があります。拡張は、Google Web ストアからダウンロードして手動でインストールすることもできますが、登録されていない Chromebook ユーザは証明書をインストールすることはできません。

登録されていない Chromebook デバイスは、ユーザがドメインユーザグループに属する場合に証明書を保護できます。拡張はデバイスのドメインユーザを追跡します。ただし、ドメイン ユーザは登録されていないデバイスのユーザ単位の認証キーを生成できます。

- エラー：Google の管理コンソールで SSID が接続された順番が不明：
 - いくつかの SSID (PEAP、および EAP-TLS) が Google の管理コンソールで設定された場合、証明書がインストールされ、属性が一致すると、Chrome OS は SSID が設定された順序にかかわらず、証明書ベースの認証を使用して SSID に自動的に接続します。
 - 2つの EAP-TLS SSID が同じ属性で一致した場合、接続は、信号強度や他のネットワークレベルの信号などの、ユーザまたは管理者で制御できないその他の要因に依存します。
 - 複数の EAP-TLS の証明書が Chromebook デバイスにインストールされ、そのすべてが管理コンソールで設定された証明書パターンと一致した場合、一番新しい証明書が接続に使用されます。

AnyConnect 設定の作成

AnyConnect 設定には、AnyConnect ソフトウェアおよび関連するコンフィギュレーションファイルが含まれます。この設定は、ユーザがクライアントで AnyConnect リソースをダウンロードしてインストールできるクライアントプロビジョニングポリシーで使用できます。AnyConnect を展開するために ISE および ASA を使用した場合、設定は両方のヘッドエンドで一致する必要があります。



- (注) VPNに接続するときにISE ポスチャ モジュールをプッシュするには、シスコの Adaptive Security Device Manager (ASDM) GUI ツールを使用する Cisco 適応型セキュリティ アプライアンス (ASA) を使用して AnyConnect エージェントをインストールすることをお勧めします。ASA は、VPN ダウンローダを使用してインストールを行います。ダウンロードでは、ISE ポスチャ プロファイルは ASA によってプッシュされ、後続のプロファイルのプロビジョニングに必要なホスト検出が利用可能になってから、ISE ポスチャ モジュールが ISE に接続します。その一方、ISE では、ISE ポスチャ モジュールは ISE が検出された後にのみプロファイルを取得し、これがエラーの原因になることがあります。したがって、VPN に接続するとき ASA を ISE ポスチャ モジュールにプッシュすることを推奨します。

始める前に

AnyConnect 設定オブジェクトを設定する前に AnyConnect パッケージ、コンプライアンス モジュール、プロファイル、およびオプションのカスタマイゼーションバンドルとローカリゼーションバンドルをアップロードする必要があります。

- ステップ 1 [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] > [クライアント プロビジョン (Client Provision)] > [リソース (Resources)] を選択します。
 - ステップ 2 [追加 (Add)] をクリックして、AnyConnect 設定を作成します。
 - ステップ 3 [AnyConnect 設定 (AnyConnect Configuration)] を選択します。
 - ステップ 4 以前にアップロードした AnyConnect パッケージを選択します。たとえば、AnyConnectDesktopWindows xxx.x.xxxxx.x を選択します。
 - ステップ 5 現在の AnyConnect 設定の名前を入力します。たとえば、AC Config xxx.x.xxxxx.x とします。
 - ステップ 6 以前にアップロードしたコンプライアンス モジュールを選択します。たとえば、AnyConnectComplianceModulewindows x.x.xxxx.x を選択します。
 - ステップ 7 1つ以上の AnyConnect モジュールのチェックボックスをオンにします。たとえば、ISE ポスチャ、VPN、ネットワーク アクセス マネージャ、Web セキュリティ、AMP イネーブラ、ASA ポスチャ、Start Before Log on (Windows OS のみ)、Diagnostic and Reporting Tool の中から、1つ以上のモジュールを選択します。
- (注) [AnyConnect モジュール選択 (AnyConnect Module Selection)] で VPN モジュールをオフにしても、プロビジョニングされたクライアントの VPN タイルは無効になりません。AnyConnect GUI の VPN タイルを無効にするには、VPNDisable_ServiceProfile.xml を設定する必要があります。AnyConnect がデフォルトの場所にインストールされているシステムでは、このファイルは C:\Program Files\Cisco にあります。AnyConnect が別の場所にインストールされている場合、このファイルは <AnyConnect がインストールされているパス>\Cisco にあります。
- ステップ 8 選択した AnyConnect モジュール用の AnyConnect プロファイルを選択します。たとえば、ISE ポスチャ、VPN、NAM および Web セキュリティを選択します。
 - ステップ 9 AnyConnect カスタマイズ バンドルおよびローカリゼーションバンドルを選択します。

ステップ 10 [送信 (Submit)] をクリックします。

関連トピック

[AnyConnect](#) (906 ページ)

AnyConnect と Cisco NAC のエージェント プロファイルの作成

AnyConnect や NAC ポスチャのエージェント プロファイルを作成するには、次の手順を実行します。このプロファイルでは、エージェントの動作を定義するパラメータ、クライアント IP アドレスをリフレッシュするかどうかに関連するパラメータ、およびポスチャプロトコルのパラメータを指定できます。

ステップ 1 [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] > [クライアント プロビジョニング (Client Provisioning)] > [リソース (Resources)] を選択します。

ステップ 2 [追加 (Add)] をクリックします。

ステップ 3 [NAC AnyConnect エージェント ポスチャ プロファイル (NAC AnyConnect Agent Posture Profile)] を選択します。

ステップ 4 [AnyConnect] または [NAC Agent] を選択します。

ステップ 5 次のパラメータを設定します。

- Cisco ISE ポスチャ エージェントの動作
- クライアント IP アドレスの変更
- Cisco ISE ポスチャ プロトコル

ステップ 6 [送信 (Submit)] をクリックします。

関連トピック

[エージェント プロファイル設定のガイドライン](#) (887 ページ)

エージェント プロファイル設定のガイドライン

シスコは、エージェント プロファイルを設定して、修復タイマー、ネットワーク遷移遅延タイマー、およびクライアントマシン上でログイン成功画面を自動的に閉じるために使用するタイマー制御し、これらの設定がポリシーベースになるようにすることを推奨します。ただし、クライアント プロビジョニング ポリシーと一致するように設定されたエージェント プロファイルがない場合、[管理 (Administration)] > [システム (System)] > [設定 (Settings)] > [ポスチャ (Posture)] > [全般設定 (General Settings)] の設定を使用して、同じ目的を達成できます。

ポリシー適用または他の方法でクライアント デバイスにエージェント プロファイルを設定してアップロードすると、そのエージェント プロファイルはクライアント上で維持され、他の何かに変更するまで、ログインおよび操作の動作に影響を及ぼします。したがって、エージェント プロファイルを Cisco ISE から削除しても、以前影響を受けたクライアントからその動作はなくなりません。ログインおよび操作の動作を変更するには、クライアント上の、既存のエージェント プロファイル パラメータの値を上書きする新しいエージェント プロファイルを定義し、これをポリシー適用によってアップロードする必要があります。

クライアントにあるものと異なるエージェント プロファイルが Cisco ISE にある場合（MD5 チェックサムを使用して判定）、Cisco ISE は、新しいエージェント プロファイルをクライアントにダウンロードします。Cisco ISE から送信されるエージェント カスタマイズ ファイルが異なる場合にも、Cisco ISE は新しいエージェント カスタマイズ ファイルをクライアントにダウンロードします。

エージェントの動作の設定

次の表に、ポスチャ エージェント（AnyConnect および Cisco NAC Agent）のパラメータを設定できる [NAC または AnyConnect のポスチャ プロファイル（NAC or AnyConnect Posture Profile）] ページのフィールドを示します。このページへのナビゲーションパスは、[ポリシー（Policy）]> [ポリシー要素（Policy Elements）]> [結果（Results）]> [クライアント プロビジョニング（Client Provisioning）]> [リソース（Resources）]> [追加（Add）]> [NAC または AnyConnect のポスチャ プロファイル（NAC or AnyConnect Posture Profile）] です。

フィールド	デフォルト値（Default Value）	モード（Cisco ISE NAC Agent にのみ該当）	使用上のガイドライン
エージェントの終了の無効化。（Disable Agent Exit.）（Mac OS X クライアントには適用できません）	なし	マージ	値を [はい（Yes）] に設定すると、ユーザはエージェントをシステムトレイ経由で終了できません。

フィールド	デフォルト値 (Default Value)	モード (Cisco ISE NAC Agent にのみ該当)	使用上のガイドライン
アクセシビリティモードの有効化 (Enable Accessibility Mode) (Mac OS X クライアントには適用できません)	[いいえ (No)] : エージェントは Job Access with Speech (JAWS) と相互作用しません	マージ	<p>値を [はい (Yes)] に設定すると、JAWS 画面リーダーと互換性を持ちます。</p> <p>この機能を有効にすると、パフォーマンスがわずかながら影響を受ける可能性があります。JAWS 画面リーダーがインストールされていないクライアントマシンでこの機能を有効にしても、エージェントは正常に機能します。</p>
署名チェックの有効化 (Enable signature check) (Mac OS X クライアントには適用できません)	なし	上書き	値を [はい (Yes)] に設定すると、修復プログラムを起動する前に Windows は実行ファイルのデジタル署名をチェックできます。
概要画面のバイパス (Bypass Summary Screen) (Mac OS X クライアントには適用できません)	○	マージ	

フィールド	デフォルト値 (Default Value)	モード (Cisco ISE NAC Agent にのみ該当)	使用上のガイドライン
ロケール (Locale) (Mac OS X クライアントには適用できません)	デフォルト	マージ	<p>デフォルト設定では、エージェントはクライアントオペレーティングシステムからロケール設定を使用できます。</p> <p>この設定が、サポートされている言語のID、略称、または正式名称の場合、エージェントは自動的に、クライアントマシンのエージェントダイアログをローカライズされたテキストで表示します。</p>
ポスチャ レポート フィルタ (Posture report filter) (Mac OS X クライアントには適用できません)	表示が失敗しました (Display Failed)	マージ	<p>値を [表示が失敗しました (Display Failed)] に設定した場合、ユーザがエージェントダイアログの [詳細の表示 (Show Details)] をクリックすると、クライアントポスチャ評価レポートに修復エラーのみが表示されます。</p> <p>値を [すべて表示 (Display All)] に設定した場合、ユーザがエージェントダイアログの [詳細の表示 (Show Details)] をクリックすると、クライアントポスチャ評価レポートにすべての結果が表示されます。</p>

フィールド	デフォルト値 (Default Value)	モード (Cisco ISE NAC Agent にのみ該当)	使用上のガイドライン
修復タイマー (Remediation timer)	4	上書き	この設定では、クライアントマシンで失敗したポスチャ評価チェックを修復する時間を指定します。この分数を経過すると、ログインプロセスを再び実行する必要があります。有効な範囲は 1 ～ 300 分です。
ネットワーク遷移遅延 (Network Transition Delay)	3	上書き	この設定では、ネットワーク遷移 (IP アドレスの変更) を待機する時間を指定します。これが経過すると、修復タイマーのカウントダウンが開始されます。有効な範囲は 2 ～ 30 秒です。
ログ ファイル サイズ (Log file size)	5	マージ	<p>この設定では、クライアントマシン上のエージェント ログ ファイルのファイル サイズ (メガバイト単位) を指定します。</p> <p>ログ ファイル サイズがゼロに設定されている場合、エージェントは、クライアントマシン上のユーザセッションに関するログインまたは操作情報を記録しません。</p> <p>ログ ファイル サイズがゼロ以外の場合、エージェントレコードは指定されたメガバイト数までログインおよびセッション情報を記録します。</p>

フィールド	デフォルト値 (Default Value)	モード (Cisco ISE NAC Agent にのみ該当)	使用上のガイドライン
自動クローズの有効化。 (Enable Auto Close.) (AnyConnect には適用されません)	なし	上書き	この設定が [はい (Yes)] の場合、エージェント ログイン ダイアログをユーザ認証後に自動的に閉じることができます。
自動クローズタイマー (Auto close timer) (AnyConnect には該当しません)	[0]	上書き	この設定では、エージェント ログイン画面は指定された時間待機して、ユーザ認証後に自動的に閉じることができます。有効な値の範囲は 0 ～ 30 秒です。



(注) パラメータ値を既存のエージェント プロファイルの設定でマージするか、Windows および Mac OS X クライアントのエージェント動作を適切に設定するために上書きします。



(注) エージェント ログ ファイルは、クライアント マシンのディレクトリに保存されます。1 回目のログインセッションの後、2 つのファイルがディレクトリ内に置かれます。1 つは前回のログインセッションからのバックアップ ファイルで、もう 1 つは現在のセッションのログインおよび操作の情報を含む新しいファイルです。現在のセッションのログ ファイルが大きくなり、指定されたファイルサイズを超えると、エージェントのログインおよび操作情報の最初の部分が自動的にディレクトリ内のバックアップファイルになり、エージェントは引き続き最新のエントリを現在のセッション ファイルに記録していきます。

次の表に、Cisco ISE 2.2 でポスチャ エージェント (AnyConnect) のパラメータを設定できる [NAC または AnyConnect のポスチャ プロファイル (NAC or AnyConnect Posture Profile)] ページのフィールドを示します。Anyconnect のエージェント動作設定のその他のフィールドについては、『[Anyconnect Administrator Guide](#)』を参照してください。

フィールド	デフォルト値 (Default Value)	使用上のガイドライン
ステルス モード (Stealth Mode)	標準 (Standard)	AnyConnect はクライアントレス モードまたは標準モードで動作できます。標準モードでは、AnyConnect エージェントを展開し、クライアントとのやりとりを必要とする Cisco ISE ポスチャ ポリシーをモニタおよび適用します。クライアントレス モードでは、ユーザとのやりとりを行わずに、ポスチャをサービスとして実行できます。

サポートされる言語

表 55: サポートされる言語

[言語 (Language)]	ID	略称	正式名称
英語 (米国)	1033	en	英語
カタロニア語	1027	ca	カタロニア語 (スペイン)
簡体字中国語	2052	zh_cn	中国語 (簡体字)
繁体字中国語	1028	zh_tw	中国語 (繁体字)
チェコ語	1029	cs	チェコ語
デンマーク語	1030	da	デンマーク語
Dutch	1043	nl	オランダ語 (標準)
フィンランド語	1035	fi	フィンランド語
フランス語	1036	fr	フランス語
フランス語 (カナダ)	3084	fr-ca	French-Canadian
ドイツ語	1031	de	ドイツ語
ハンガリー語	1038	hu	ハンガリー語
イタリア語	1040	it	イタリア語
日本語	1041	ja	日本語

[言語 (Language)]	ID	略称	正式名称
Korean	1042	ko	韓国語
Norwegian	1044	No	Norwegian
ポーランド語	1045	pl	ポーランド語
ポルトガル語	2070	pt	ポルトガル語
ロシア語	1049	ru	ロシア語
セルビア語 (ラテン)	2074	sr	セルビア語 (ラテン)
セルビア語 (キリル)	3098	src	セルビア語 (キリル)
スペイン語	1034	es	スペイン語 (従来型)
スウェーデン語	1053	sv	スウェーデン語
Turkish	1055	tr	Turkish

クライアント IP アドレスのリフレッシュ設定

次の表に、VLAN の変更後に IP アドレスをリフレッシュするようにクライアントのパラメータを設定できる [NAC AnyConnect ポスチャ プロファイル (NAC AnyConnect Posture Profile)] ページのフィールドを示します。このページへのナビゲーションパスは、[ポリシー (Policy)]> [ポリシー要素 (Policy Elements)]> [結果 (Results)]> [クライアントプロビジョニング (Client Provisioning)]> [リソース (Resources)]> [追加 (Add)]> [NAC または AnyConnect ポスチャ プロファイル (NAC or AnyConnect Posture Profile)] です。

フィールド	デフォルト値 (Default Value)	モード (Cisco NAC Agent にのみ該当)	使用上のガイドライン
VLAN 検出間隔 (VLAN detection interval)	0、5	マージ	<p>この設定は、エージェントが VLAN 変更をチェックする間隔です。</p> <p>Windows NAC エージェントの場合、デフォルト値は 0 です。デフォルトでは、認証 VLAN 変更機能へのアクセスは Windows に対して無効にされます。有効な値の範囲は 0 ～ 5 秒です。</p> <p>Mac OS X エージェントの場合、デフォルト値は 5 です。Mac OS X のデフォルトでは、認証 VLAN 変更機能へのアクセスは、VlanDetectInterval を 5 秒として有効になっています。有効な範囲は 5 ～ 900 秒です。</p> <p>0 : 認証 VLAN 変更機能へのアクセスは無効化されます。</p> <p>1 ～ 5 : エージェントはインターネット制御メッセージプロトコル (ICMP) またはアドレス解決プロトコル (ARP) クエリーを 5 秒ごとに送信します。</p> <p>6 ～ 900 : ICMP/ARP クエリーが x 秒ごとに送信されます。</p>

フィールド	デフォルト値 (Default Value)	モード (Cisco NAC Agent にのみ該当)	使用上のガイドライン
UI なしの VLAN 検出の有効化 (Enable VLAN detection without UI) (Mac OS X クライアントには適用できません)	なし	マージ	この設定は、ユーザがログインしていないときでも VLAN 検出を有効または無効にします。 No : VLAN 検出機能は無効です。 Yes : VLAN 検出機能が有効です。
再試行検出数 (Retry detection count)	3	マージ	インターネット制御メッセージプロトコル (ICMP) またはアドレス解決プロトコル (ARP) ポーリングが失敗する場合、この設定で、クライアント IP アドレスをリフレッシュする前に x 回再試行するようにエージェントを設定します。
Ping または ARP (Ping or ARP)	[0] 有効な範囲は 0 ~ 2 です。	マージ	この設定は、クライアント IP アドレスの変更を検出するために使用する方式を指定します。 0 : ICMP を使用してポーリング 1 : ARP を使用してポーリング 2 : 最初に ICMP を使用し、(ICMP が失敗した場合は) ARP を使用してポーリング
ping の最大タイムアウト (Maximum timeout for ping)	1 有効な値の範囲は 1 ~ 10 秒です。	マージ	ICMP を使用してポーリングし、指定した時間内に応答がない場合は、ICMP ポーリングの失敗を宣言します。

フィールド	デフォルト値 (Default Value)	モード (Cisco NAC Agent にのみ該当)	使用上のガイドライン
エージェント IP のリフレッシュの有効化 (Enable agent IP refresh)	Yes (デフォルト)	上書き	この設定は、スイッチ（または WLC）が各スイッチポートでクライアントのログインセッション用 VLAN を変更した後にクライアントマシンが IP アドレスをリフレッシュするかどうかを指定します。
DHCP 更新遅延 (DHCP renew delay)	[0] 有効な値の範囲は 0 ～ 60 秒です。	上書き	この設定は、ネットワーク DHCP サーバからの新しい IP アドレスの要求を試行する前に、クライアントマシンが待機するように指定します。
DHCP リリース遅延 (DHCP release delay)	[0] 有効な値の範囲は 0 ～ 60 秒です。	上書き	この設定は、現在の IP アドレスをリリースする前にクライアントマシンが待機するように指定します。



(注) パラメータ値は、既存のエージェントプロファイル設定とマージするか、または上書きして、Windows および Mac OS X クライアントで適切に IP アドレスがリフレッシュされるように設定します。

ポスチャ プロトコル設定

次の表では、ポスチャ プロトコル設定を設定できる [NAC または AnyConnect プロファイル (NAC or AnyConnect Profile)] ページのフィールドについて説明します。このページへのナビゲーションパスは、[ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] > [クライアントプロビジョニング (Client Provisioning)] > [リソース (Resources)] > [追加 (Add)] > [NAC エージェントまたは AnyConnect ポスチャ プロファイル (NAC Agent or AnyConnect Posture Profile)] です。

フィールド	値	[モード (Mode)]	使用上のガイドライン
CRL チェックの許可 (Allow CRL Checks) (Mac OS X クライアントからは不可)	○	上書き	値が No に設定されている場合、検出およびネゴシエーション時の証明書失効リスト (CRL) のチェックがオフになります。
MAC アドレス例外リスト (MAC Address Exemption List) (Mac OS X クライアントからは不可)	カンマで区切った MAC アドレスを入力します。たとえば、AA:BB:CC:DD:EE:FF、11:22:33:44:55:66	マージ	この設定で1つまたは複数の MAC アドレスを指定すると、エージェントは、ログインと認証の間、ネットワーク経路で不要な MAC アドレスが送信されることを防ぐために、これらの MAC アドレスを Cisco ISE にアドバタイズしません。
Discovery Host (Mac OS X クライアントからは不可)	IP アドレスまたは完全修飾ドメイン名 (FQDN) を入力します。	上書き	この設定では、レイヤ 3 配置で Cisco ISE に接続するためにエージェントが使用する Discovery Host のアドレスまたは解決可能なドメイン名を指定します。
Discovery Host の有効化 (Enable Discovery Host) (Mac OS X クライアントからは不可)	○	上書き	Yes : ユーザが [エージェントのプロパティ (agent Properties)] ダイアログボックスの [ホストの検索 (Discovery Host)] フィールドにカスタム値を指定できます。 No : ユーザがクライアント マシンの [ホストの検索 (Discovery Host)] フィールドの値を変更できません。

フィールド	値	[モード (Mode)]	使用上のガイドライン
サーバ名ルール (Server Name Rules)	Cisco ISE サーバの完全修飾ドメイン名 (FQDN) をカンマで区切って入力します。	マージ	このフィールドは、関連する Cisco ISE サーバのカンマ区切り名から構成されます。エージェントは、このリストの名前を使用して、Cisco ISE アクセス ポイントを許可します。このリストが空の場合、許可は実行されません。いずれの名前も見つからない場合、エラーが報告されます。
自動生成 MAC アドレス (Auto-generated MAC Address) (Mac OS X クライアントからは不可)	—	マージ	この設定は、クライアント マシンでの Evolution-Data 最適化接続をサポートしています。クライアントマシンにアクティブなネットワークインターフェイスカードがない場合、エージェントはシステムにダミーの MAC アドレスを作成します。
SWISS タイムアウト (SWISS Timeout) (Mac OS X クライアントからは不可)	1 : エージェントは、設計どおりに SWISS 検出を実行し、追加の UDP 応答パケット遅延タイムアウト値は使用されません。	マージ	値を 1 よりも大きく設定すると、エージェントは Cisco ISE からの SWISS UDP 検出応答パケットを追加の秒数だけ待機してから、別の検出パケットを送信します。エージェントは、このアクションを実行して、ネットワーク遅延による応答パケットの遅延が発生していないことを確認します。(SWISS タイムアウトは UDP SWISS タイムアウトの場合のみ)

フィールド	値	[モード (Mode)]	使用上のガイドライン
L3 SWISS 遅延の無効化 (Disable L3 SWISS delay) (Mac OS X クライアントからは不可)	なし	マージ	この設定が Yes の場合、エージェントはレイヤ 3 検出パケットの送信間隔を長くする機能を無効にします。したがって、レイヤ 3 検出パケットはレイヤ 2 パケットと同様に、5 秒ごとに送信され続けます。
HTTP 検出タイムアウト (HTTP Discovery Timeout) (Mac OS X クライアントからは不可)	30 (Windows クライアントのデフォルト) 有効な範囲は 3 秒以上です。	マージ	<p>この設定は、エージェントからの HTTPS 検出が Cisco ISE からの検出応答を待機する HTTP 検出タイムアウトを指定します。指定時間内に応答がない場合は、検出プロセスはタイムアウトになります。</p> <p>値が 0 に設定されている場合、デフォルトのクライアントマシンのオペレーティングシステムのタイムアウト設定が使用されます。</p> <p>値が 1 または 2 に設定されている場合、値は自動的に 3 に設定されます。</p>

フィールド	値	[モード (Mode)]	使用上のガイドライン
HTTP タイムアウト (HTTP Timeout) (Mac OS X クライアントからは不可)	120 (Windows クライアントのデフォルト) 有効な範囲は3秒以上です。	マージ	<p>この設定は、エージェントからの HTTP 要求が応答を待機する HTTP タイムアウトを指定します。指定時間内に応答がないと、要求はタイムアウトになり、検出プロセスはタイムアウトになります。</p> <p>値が 0 に設定されている場合、デフォルトのクライアントマシンのオペレーティングシステムのタイムアウト設定が使用されます。</p> <p>値が 1 または 2 に設定されている場合、値は自動的に 3 に設定されます。</p>

次の表に、Cisco ISE 2.2 で AnyConnect のポスチャ プロトコル設定を設定できる [NAC または AnyConnect のポスチャ プロファイル (NAC or AnyConnect Posture Profile)] ページのフィールドを示します。Anyconnect のポスチャ プロトコル設定のその他のフィールドについては、『[Anyconnect Administrator Guide](#)』を参照してください。

フィールド	デフォルト値 (Default Value)	使用上のガイドライン
[Call Home リスト (Call Home List)]	—	IP アドレスとポートをコロンで結んだカンマ区切りリストを入力します。
[バックオフ タイマー (Back-off Timer)]	30 秒	この設定により、Anyconnect エージェントは最大時間制限に達するまでディスカバリ パケットを送信することで、ディスカバリ ターゲット (リダイレクション ターゲットおよび以前に接続していた PSN) に継続的に到達できます。有効な値の範囲は 10 ～ 600 秒です。

クライアント ログインセッションの基準

Cisco ISE では、内部ネットワークにユーザがアクセスするときに使用するログインセッションのタイプを分類する場合に、次のようなさまざまな要素を調べます。

- クライアント マシンのオペレーティング システムおよびバージョン
- クライアント マシンのブラウザ タイプおよびバージョン
- ユーザが属するグループ
- (適用したディクショナリ属性に基づく) 条件評価結果

Cisco ISE は、クライアント マシンを分類した後、クライアント プロビジョニング リソース ポリシーを使用して、適切なエージェントバージョン、アンチウイルスとアンチスパイウェアのベンダー サポートに対する最新のコンプライアンス モジュール、および (必要に応じて) 正しいエージェント カスタマイズ パッケージとプロファイルで、クライアント マシンが設定されていることを確認します。

クライアント マシン上のエージェントのダウンロードの問題

問題

ユーザの認証と許可の後、クライアント マシン ブラウザに「ポリシーが一致しません (no policy matched)」のエラー メッセージが表示されます。この問題は、認証のクライアント プロビジョニング フェーズ中のユーザセッションに該当します。

考えられる原因

クライアント プロビジョニング ポリシーに必要な設定が欠落している可能性があります。

ポスチャ エージェントのダウンロードの問題

ポスチャエージェントのインストーラをダウンロードするには、次のものが必要があることに注意してください。

- エージェントを初めてクライアント マシンにインストールする場合、ユーザはブラウザ セッションで ActiveX インストーラを許可する必要があります (クライアント プロビジョニング ダウンロード ページでは、この情報の指定を求められます)。
- クライアント マシンには、インターネット アクセスが必要です。

解像度

- クライアント プロビジョニング ポリシーが Cisco ISE に存在することを確認します。存在する場合は、ポリシー内に定義されているポリシー ID グループ、条件およびエージェントのタイプを確認します (また、すべてのデフォルト値のプロファイルも含め、**[ポリシー**

(Policy)]> [ポリシー要素 (Policy Elements)]> [結果 (Results)]> [クライアント プロビジョニング (Client Provisioning)]> [リソース (Resources)]> [追加 (Add)]> [NAC または AnyConnect ポスチャ プロファイル (NAC or AnyConnect Posture Profile)] で設定されたエージェント プロファイルが存在するかどうかについても確認します)。

- アクセス スイッチのポートをバウンスすることにより、クライアント マシンの再認証を試行します。

Cisco NAC Agent MSI インストーラを使用したクライアントマシンのプロビジョニング

ネットワークとの一致に必要な適切なエージェントプロファイル情報を含むエージェント設定 XML ファイル (NACAgentCFG.xml という名前) とともに、MSI インストーラをディレクトリに、または MSI インストーラの zip バージョンをクライアントマシン上に置くことができます。

ステップ 1 **nacagentsetup-win.msi** または **nacagentsetup-win.zip** インストーラ ファイルをシスコのソフトウェア ダウンロード サイト (<http://software.cisco.com/download/navigator.html>) からダウンロードし、[セキュリティ (Security)]> [アクセス制御とポリシー (Access Control and Policy)]> [Cisco Identity Services Engine] > [Cisco Identity Services Engine ソフトウェア (Cisco Identity Services Engine Software)]> [リリース 1.x (Release 1.x)] に移動します。

ステップ 2 **nacagentsetup-win.msi** ファイルをクライアント マシン上の特定のディレクトリに置きます (たとえば、C:\temp\nacagentsetup-win.msi)。

- MSI インストーラを直接クライアントにコピーする場合は、クライアントマシンから Cisco NAC Agent をインストールする際のインストール元となるディレクトリに、**nacagentsetup-win.msi** ファイルを置きます。
- **nacagentsetup-win.zip** インストーラを使用する場合は、クライアントマシンから Cisco NAC Agent をインストールする際のインストール元となるディレクトリに、zip ファイルの内容を抽出します。

ステップ 3 Agent 設定 XML ファイルを、Cisco NAC Agent MSI パッケージと同じディレクトリに置きます。

Cisco ISE に接続しない場合は、すでに正常にプロビジョニングされたクライアントから **NACAgentCFG.xml** ファイルをコピーできます。ファイルは、C:\Program Files\Cisco\Cisco NAC Agent\NACAgentCFG.xml にあります。

Agent 設定 XML ファイルが MSI インストーラ パッケージと同じディレクトリに存在していれば、インストールプロセスによって Agent 設定 XML ファイルは自動的に適切な Cisco NAC Agent アプリケーションディレクトリに置かれるため、エージェントは最初に起動されたとき、正しいレイヤ 3 ネットワーク上の場所をポイントすることができます。

ステップ 4 クライアント マシンでコマンドプロンプトを開き、次のように入力してインストールを実行します。

```
msiexec.exe /i NACAgentSetup-win.msi /qn /l*v c:\temp\agent-install.log
```

(/qn 修飾子は、Cisco NAC Agent を完全にサイレントでインストールします。/!*v は、インストール セッションを冗長モードで記録します)

NAC Agent をアンインストールするには、次のコマンドを実行します。

```
msiexec /x NACAgentSetup-win-<version>.msi /qn
```

MSI を使用してエージェントの新しいバージョンをインストールする場合、古いバージョンがアンインストールされ、上記のコマンドを使用して新しいバージョンがインストールされます。

ステップ 5 Altiris/SMS を使用して MSI インストーラを分散する場合は、エージェントのカスタマイゼーションファイルを「%TEMP%/CCAA」ディレクトリの「brand」という名前のサブディレクトリに置きます。Cisco NAC Agent がクライアントにインストールされるとき、このカスタマイズは Agent に適用されます。カスタマイズを削除するには、カスタマイズ ファイルなしの MSI を送信します。

Cisco ISE ポスチャ エージェント

エージェントとは、Cisco ISE ネットワークにログインしているクライアント マシンに存在するアプリケーションです。クライアントがネットワークにログインしていない場合でも、エージェントは永続的にすることができ (AnyConnect、Cisco NAC Agent for Windows および Cisco NAC Agent for Mac OS X と同様)、インストール後もクライアント マシンに残ります。エージェントは一時的にすることもでき (Cisco NAC Web Agent と同様)、ログインセッション終了後にクライアントマシンから削除されます。いずれの場合も、エージェントはネットワークにログインし、適切なアクセス プロファイルを受け取り、クライアント マシンでポスチャ評価を実行してネットワークのコアにアクセスする前にネットワーク セキュリティ ガイドラインに従うようにします。



(注) 現在 Cisco NAC Agent および Cisco NAC Web Agent は、クライアント プロビジョニング ポータルおよびネイティブ サプリカント プロビジョニングをサポートします。Cisco NAC Web Agent は、中央 Web 認証フロー (CWA) をサポートしていますが、Cisco NAC Agent は CWA をサポートしません。

ポスチャ エージェントの検出要求と Cisco ISE 応答

Cisco ISE は、Windows および Mac OS x クライアントでの AnyConnect とレガシー Cisco ISE NAC エージェントの共存をサポートします。エージェントは、クライアント上のネットワークに変更があった場合にのみ、ポスチャ検出プローブを開始します。Cisco ISE はクライアント プロビジョニング ポリシーに基づいて、クライアントのポスチャ検出プローブに応答し、対応するエージェントが検出応答を取得します。このエージェントが唯一のアクティブ エージェントになります。

Cisco ISE では、クライアント プロビジョニング ポリシーに基づいて、次のようにエージェント ポスチャ検出プローブへの応答が異なります。

- エンドポイントがレガシー エージェント（Windows および Mac OS x 用の Cisco ISE NAC エージェント）を使用するように設定されている場合、エージェントは検出応答と既存の形式の文字列「X-perfigo-CAS=FQDN」を受信します。レガシー エージェント用の検出応答が受信された場合、AnyConnect は検出を停止します。
- エンドポイントが AnyConnect を使用するように設定されている場合、Cisco ISE は別の形式で応答します。これは、Cisco ISE ポリシー サービス ノードの FQDN および AnyConnect 設定 URL になり、AnyConnect パッケージの場所およびバージョンはクライアント プロビジョニング ポリシーに基づきます。AnyConnect 用の応答が受信された場合、レガシー エージェントは検出を停止します。



(注) MacOSX デバイスは要求をデフォルト ゲートウェイに送信しません。これらのデバイスは次の 2 つのプロープだけを使用します。

- ディスカバリ ホスト
- enroll.cisco.com

enroll.cisco.com を解決するため、MAC OSX デバイスで正しい DNS を設定していることを確認してください。

Web Agent ポスチャの検出要求と Cisco ISE 応答

Web Agent は検出プローブを行いません。Web Agent を使用するようにエンドポイントが設定されている場合、Cisco ISE は X-ISE-PDP-WEBAGENT=FQDN の形式を使用して応答します。Web Agent を使用するようにクライアント プロビジョニング ポリシーが設定されている場合、Web Agent 検出応答はクライアントの Cisco NAC Agent を呼び出すために使用されます。

エージェントが「一時的なアクセス」を表示する

問題

管理者とユーザはフル ネットワーク アクセスを想定していますが、ログインと認証の後にクライアント マシンにネットワークへの「一時的なアクセス」が付与されます。

考えられる原因

この問題は、エージェントを使用して接続するクライアント マシンのログイン セッションで発生します。

クライアントで Cisco NAC Agent が動作しているときに、次の状態で問題が発生する可能性があります。

- クライアント マシンのインターフェイスがダウンした場合
- セッションが終了した場合

解像度

ユーザは、ネットワーク接続を確認して再度ログインを試行し（またポスチャ評価を通過し）、接続の再構築を試みる必要があります。

エージェントがポスチャ評価の開始に失敗する

問題

ユーザに対して「Clean Access Server が使用できません (Clean access server not available)」というメッセージが表示されます。この問題は、Cisco ISE からのすべてのエージェント認証セッションに適用されます。

考えられる原因

このエラーは、セッションが終了していること、またはネットワーク上で Cisco ISE が到達不可能となったことのいずれかを意味する場合があります。

解像度

- ユーザは、ネットワークに再度ログインを試みることができます。
- ユーザは、デフォルト ゲートウェイや RADIUS サーバ IP アドレス、またはネットワーク管理者によって提供された FQDN の ping を試みることができます。
- 管理者は、ユーザのネットワーク アクセス属性（割り当てられた VLAN、ACL、ルーティング、クライアントでの **nslookup** コマンドの実行、クライアントマシン DNS 接続など）を確認できます。

AnyConnect

Cisco ISE は、Cisco ISE ポスチャ要件の AnyConnect で統合モジュールを使用します。AnyConnect は、同じエンドポイントの Cisco ISE NAC Agent と共存するポスチャ エージェントです。Cisco ISE のクライアントプロビジョニングポリシー設定に基づいて、一度に 1 つのエージェントのみをアクティブにします。



- (注) Cisco AnyConnect は CWA フローでサポートされていません。これは、[ワーク センター (Work Centers)] の [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] [設定 (Configure)] > [ゲスト ポータル (Guest Portals)] > [作成、編集または複製 (Create, Edit or Duplicate)] > [ポータルの動作およびフローの設定 (Portal Behavior and Flow Settings)] > [ゲスト デバイスのコンプライアンス設定 (Guest Device Compliance Settings)] ページの [ゲスト デバイス コンプライアンスが必要 (Require guest device compliance)] フィールドを使用してゲスト ポータルからプロビジョニングすることはできません。代わりに、AnyConnect は認証権限に設定されるリダイレクションの結果として、クライアントプロビジョニングポータルからプロビジョニングする必要があります。



- (注) ネットワークのメディアを切り替えるときに、AnyConnect ISE ポスチャ モジュールは、ネットワークの変更を検出し、クライアントを再評価するように、デフォルトゲートウェイの変更を要求します。

AnyConnect エージェントとの統合に Cisco ISE を利用するために、Cisco ISE は次のように動作します。

- AnyConnect のバージョン 4.0 および以降のリリースを展開するためのステージング サーバとして機能します
- Cisco ISE ポスチャ要件の AnyConnect ポスチャ コンポーネントと相互作用します
- AnyConnect プロファイル、カスタマイズ/言語パッケージ、および Windows と Mac OS X の各オペレーティング システムの OPSWAT のライブラリ更新の展開をサポートします
- AnyConnect およびレガシー エージェントを同時にサポートします

Cisco NAC Agent XML ファイルのインストール ディレクトリ

Cisco NAC Agent がデフォルトの場所にインストールされているシステムでは、.xml ファイルは次のディレクトリにあります。

- nac_login.xml ファイルは「C:\Program Files\Cisco\Cisco NAC Agent\UI\nac_divs\login」ディレクトリにあります。
- nacStrings_xx.xml ファイルで、「xx」はロケールを示します。ファイルの全リストは「C:\Program Files\Cisco\Cisco NAC Agent\UI\cues_utility」ディレクトリにあります。

エージェントが別の場所にインストールされている場合には、ファイルは「<Agent Installed path>\Cisco\Cisco NAC Agent\UI\nac_divs\login」および「<Agent Installed path>\Cisco\Cisco NAC Agent\cues_utility」にあります。

Windows クライアント用 Cisco NAC Agent

Cisco NAC Agent には、クライアント マシンに対して、ポスチャ評価および修復を行う機能があります。

ユーザは Cisco NAC Agent（読み取り専用クライアントソフトウェア）をダウンロードしてインストールし、ホストのレジストリ、プロセス、アプリケーション、およびサービスをチェックすることができます。Cisco NAC Agent を使用すると、Windows の更新またはアンチウイルスやアンチスパイウェアの定義の更新を実行したり、正規の修復プログラムを起動したり、Cisco ISE サーバにアップロードされたファイルを配布したり、ユーザがファイルをダウンロードしてシステムを修復できるように Web サイト リンクを Web サイトに配布したり、情報や手順を配布したりすることができます。

シスコは、最新の Windows ホット フィックスとパッチが Windows XP クライアントにインストールされ、Cisco NAC Agent がセキュアで暗号化された Cisco ISE との通信を確立できることを確認することを推奨します（SSL over TCP など）。

Windows 7 以前のクライアントからの Cisco NAC Agent のアンインストール

Cisco NAC Agent は Windows クライアントの **C:\Program Files\Cisco\Cisco NAC Agent** にインストールされます。

Agent は、次の方法でアンインストールできます。

- [Cisco NAC Agent のアンインストール（Uninstall Cisco NAC Agent）] **Uninstall Cisco NAC Agent** デスクトップ アイコンをダブルクリックします。
- [スタート（Start）] メニュー > [プログラム（Programs）] > [Cisco Systems] > [Cisco Clean Access] > [Cisco NAC Agent のアンインストール（Uninstall Cisco NAC Agent）] に移動します。
- [スタート（Start）] メニュー > [コントロール パネル（Control Panel）] > [プログラムの追加と削除（Add or Remove Programs）] > [Cisco NAC Agent] に移動し、Cisco NAC Agent をアンインストールします。

関連トピック

[Windows クライアント用 Cisco NAC Agent](#)（908 ページ）

Windows 8 クライアントの Cisco NAC Agent のアンインストール

メトロ モードで Windows 8 クライアントの Cisco NAC Agent をアンインストールできます。

ステップ 1 メトロ モードに切り替えます。

ステップ 2 [Cisco NAC Agent] タイルを右クリックします。

ステップ 3 画面下部にあるオプションから [アンインストール (Un-Install)] を選択します。

ステップ 4 システムが自動的にデスクトップ モードに切替わり、[追加/削除 (Add/Remove)] コントロール パネルが開きます。

ステップ 5 [追加/削除 (Add/Remove)] コントロール パネルで、次のいずれかの操作を行います。

- a) [Cisco NAC Agent] をダブルクリックし、[アンインストール (Uninstall)] をクリックします。
- b) [Cisco NAC Agent] を選択し、[アンインストール (Uninstall)] をクリックします。
- c) [Cisco NAC Agent] を右クリックし、[アンインストール (Uninstall)] を選択します。

関連トピック

[Windows クライアント用 Cisco NAC Agent](#) (908 ページ)

Windows 8 メトロおよびメトロ アプリケーションのサポート : Toast 通知

[Toast 通知の有効化 (Enable Toast Notification)] オプションは、[Cisco NAC Agent] トレイ アイコンで使用でき、Windows 8 クライアントに関連する通知をユーザに送信できます。

Cisco NAC Agent では、「修復で障害発生」や「ネットワーク アクセスの期限切れ」などのためにユーザがネットワークアクセスを取得できなかった場合は、エージェントによって「Network not available, Click "OK" to continue」という Toast 通知が表示されます。

詳細を取得するには、toast を選択すると、デスクトップ モードにリダイレクトされ、Cisco NAC Agent ダイアログが表示されます。

Toast 通知は、ネットワーク アクセスを取得するために実行する必要があるすべてのプラス推奨処置に対して表示されます。次に例を示します。

- ネットワーク受信ポリシーの場合は、「Click Accept to gain network access」という toast が表示されます。
- エージェント/コンプライアンス モジュールのアップグレードの場合は、「Click OK to Upgrade/Update」という toast が表示されます。
- 「user logged out」イベントでは、Clean Access Manager (CAM) でログオフの「Auto Close」オプションが有効でない場合に、Toast 通知が表示されます。この toast により、ユーザがログアウトされており、ネットワークにアクセスするには再度ログインする必要があることがわかります。

関連トピック

[Windows クライアント用 Cisco NAC Agent](#) (908 ページ)

Macintosh クライアント用 Cisco NAC Agent

Cisco NAC OS X Agent により、Macintosh クライアント マシンはポスチャ評価および修復を実行できます。

ユーザは Cisco NAC OS X Agent（読み取り専用クライアント ソフトウェア）をダウンロードしてインストールし、アンチウイルスおよびアンチスパイウェアの定義の更新をチェックすることができます。

Cisco NAC OS X Agent は、ユーザがログインすると、ユーザ ロールまたはオペレーティング システムに設定された要件を Cisco ISE サーバから取得し、必要なパッケージをチェックし、レポートを Cisco ISE サーバに返送します。クライアントに関する要件が満たされている場合、ユーザはネットワークにアクセスできます。要件が満たされていない場合、エージェントは満たされていない要件ごとに、ユーザにダイアログを表示します。ダイアログにより、クライアント マシンの要件を満たすための手順および対処法が提供されます。あるいは、指定された要件が満たされない場合は、クライアント システムの修復試行中は制限付きのネットワーク アクセスを受け入れるという選択もできます。

Macintosh クライアントからの Cisco NAC Agent のアンインストール

次のアンインストール スクリプトを実行して、Mac OS X クライアントの Cisco NAC Agent をアンインストールできます。

ステップ 1 ナビゲータ ペインを開き、<local drive ID> > [Applications] に移動します。

ステップ 2 [CCAAgent] アイコンを強調表示して右クリックし、選択メニューを表示します。

ステップ 3 [パッケージ コンテンツの表示（Show Package Contents）] を選択し、[NacUninstall] をダブルクリックして、Mac OS X で Cisco NAC Agent をアンインストールします。

関連トピック

[Macintosh クライアント用 Cisco NAC Agent](#)（910 ページ）

Cisco Web Agent

Cisco Web Agent では、クライアント マシンのための一時的なポスチャ評価を提供します。

ユーザは Cisco Web Agent 実行ファイルを起動することができ、ActiveX コントロールまたは Java アプレットによって、クライアント マシンの一時ディレクトリに Web Agent ファイルがインストールされます。

Cisco Web Agent は、ユーザがログインすると、ユーザ ロールまたはオペレーティング システムに設定された要件を Cisco ISE サーバから取得し、必要なパッケージのホスト レジストリ、プロセス、アプリケーション、およびサービスをチェックし、レポートを Cisco ISE サーバに送信します。クライアント マシンに関する要件が満たされている場合、ユーザはネットワーク

にアクセスできます。要件が満たされていない場合、Web Agent は満たされていない要件ごとに、ユーザにダイアログを表示します。ダイアログにより、クライアントマシンの要件を満たすための手順および対処法が提供されます。あるいは、指定された要件が満たされない場合は、ユーザ ログイン ロールの要件を満たすようにクライアントシステムの修復試行中は制限付きのネットワーク アクセスを受け入れるという選択もできます。



(注) ActiveX は 32 ビット版の Internet Explorer でのみサポートされます。Firefox Web ブラウザまたは 64 ビット版の Internet Explorer のバージョンでは、ActiveX をインストールできません。

Cisco NAC Agent ログ

Cisco NAC Agent for Windows で、[エージェント トレイ (Agent Tray)] アイコンを右クリックし、[ログ パッケージ (Log Package)] をクリックして、サポートパッケージを実行し、ログを収集します。

Cisco NAC Agent for Cisco NAC OS X で、[ツール (Tools)] メニューの [エージェント (Agent)] アイコンを右クリックして、[サポートログの収集 (Collect Support Logs)] オプションをクリックして、エージェントのログとサポート情報を収集します。収集された情報は、ZIP ファイルとして提供されます。ユーザは、ファイルの場所とファイル名を選択して、ファイルを保存できます。デフォルトでは、ファイルは *CiscoSupportReport.zip* というファイル名でデスクトップに保存されます。

エージェントがクラッシュまたはハングした場合は、**CCAAgentLogPackager.app** を実行してログを収集することができます。このファイルは /Applications/CCAAgent.app で入手できます。[CCAAgent.app] を右クリックして、[パッケージコンテンツの表示 (Show Package Contents)] を選択し、[CCAAgentLogPackager] をダブルクリックして、サポート情報を収集します。

Cisco NAC Agent のエージェント カスタマイズ ファイルの作成

エージェント カスタマイズ ファイルにより、Cisco NAC Agent 画面ダイアログのロゴ、フィールド、メッセージ テキストをカスタマイズして、特定の Windows クライアントのネットワーク アクセス要件に合致させることができます。

XML ディスクリプタ ファイルを含む .zip ファイルとしてカスタマイゼーション パッケージを作成し、カスタマイズされたオプションから成るコンテンツを含む別の .zip ファイルを作成することができます。

ステップ 1 [エージェント (Agent)] 画面のカスタマイズ パッケージを構成するために必要なファイルを組み合わせます。

- カスタマイズされた nac_login.xml ファイル
- .gif ファイルとしてカスタマイズされた企業/会社のロゴ
- 1 つ以上のカスタマイズされた nacStrings_xx.xml ファイル
- カスタマイズされた updateFeed.xml ディスクリプタ ファイル

ステップ 2 完成したファイルを含む「brand-win.zip」と呼ばれる zip ファイルを作成します。たとえば Linux または UNIX 環境では、次のコマンドを実行します。 **zip -r brand-win.zip nac_login.xml nac_logo.gif nacStrings_en.xml nacStrings_cy.xml nacStrings_el.xml**

ステップ 3 適切な updateFeed.xml ディスクリプタ ファイルと上記で作成された .zip ファイルを含む「custom.zip」ファイルを作成します。たとえば Linux または UNIX 環境では、次のコマンドを実行します。 **zip -r custom.zip updateFeed.xml brand-win.zip**

ステップ 4 完成した「custom.zip」ファイルを、Cisco ISE にアップロードする場合にアクセスできるローカルマシン上の場所に保存します。

関連トピック

[Cisco NAC Agent のデフォルト ログイン画面とカスタマイズされたログイン画面](#)

[カスタム nac_login.xml ファイルのテンプレート \(912 ページ\)](#)

[カスタム nacStrings_xx.xml ファイルのテンプレート \(913 ページ\)](#)

[拡張 nacStrings_xx.xml ファイルのサンプル \(922 ページ\)](#)

[UpdateFeed.xml ディスクリプタ ファイルのテンプレート \(923 ページ\)](#)

[プロファイル作成機能を使用して生成された XML ファイルの例 \(924 ページ\)](#)

カスタム nac_login.xml ファイルのテンプレート

nac_login.xml ファイルは、[エージェント (Agent)] 画面のカスタマイズ パッケージに必要なファイルの 1 つであり、これにより、[プロパティ (Properties)] ウィンドウなどの [Cisco NAC Agent] ダイアログに含まれているロゴ、フィールド、およびメッセージテキストをカスタマイズして、特定の Windows クライアントのネットワーク アクセス要件に合致させることができます。

適切な「nac_login.xml」ファイルを作成して [Cisco NAC Agent] 画面に含まれるロゴ、フィールド、およびメッセージテキストをカスタマイズするには、次のテンプレートを使用します。

次に、カスタマイズされたファイルの例を示します。

```
<tr class="nacLoginMiddleSectionContainerInput">
<td colspan="2">
<fieldset width="100%" id="nacLoginCustomAlert"
style="display:block" class="nacLoginAlertBox">
<table width="100%">
<tr>
<td id="nacLoginCustomAlert.img" valign="top" width="32px">
</img>
</td>
<td id="nacLoginCustomAlert.content" class="nacLoginAlertText">
```

```

<cues:localize key="login.customalert"/>
</td>
</tr>
</table>
</fieldset>
</td>
</tr>
<tr id="nacLoginRememberMe" style="visibility:hidden">
<td>
<cues:localize key="cd.nbsp"/>
</td>
<td class="cuesLoginField">
<nobr>
<input type="checkbox" alt="" title="" name="rememberme"
id="rememberme" checked="true"/>
<cues:localize key="login.remember_me"/>
</nobr>
</td>
</tr>

```

カスタム nacStrings_xx.xml ファイルのテンプレート

これは、[エージェント (Agent)] 画面のカスタマイズパッケージに必要なファイルの 1 つであり、これにより、[プロパティ (Properties)] 画面などの [Cisco NAC Agent] ダイアログに含まれているロゴ、フィールド、およびメッセージテキストをカスタマイズして、特定の Windows クライアントのネットワーク アクセス要件に合致させることができます。

次のテンプレートを使用して、1 つ以上の nacStrings_xx.xml ファイルを作成します。ここで、xx は特定言語の 2 文字の ID です。

次に、カスタマイズされた nacStrings_xx.xml ファイルの例を示します。

```

<cueslookup:appstrings xmlns:cueslookup="http://www.cisco.com/cues/lookup">
<cueslookup:name key="nac.brand.legal_name">Cisco Systems, Inc.</cueslookup:name>
<cueslookup:name key="nac.brand.full_name">Cisco Systems</cueslookup:name>
<cueslookup:name key="nac.brand.short_name">Cisco</cueslookup:name>
<cueslookup:name key="nac.brand.abbreviation">Cisco</cueslookup:name>
<cueslookup:name key="nac.copyright">Copyright </cueslookup:name>
<cueslookup:name key="nac.copyright.period">2009-2013</cueslookup:name>
<cueslookup:name key="nac.copyright.arr">All Rights Reserved</cueslookup:name>
<cueslookup:name key="updateagent.rqst">NAC Agent %1 is available.%br% Do you want to
install this update now?</cueslookup:name>
<cueslookup:name key="updateagent.rqst.retry">Unable to update NAC Agent. Please try
again.</cueslookup:name>
<cueslookup:name key="downloadagent.report">Downloading the update of NAC
Agent.</cueslookup:name>
<cueslookup:name key="downloadagent.packagename.label">Package Name</cueslookup:name>
<cueslookup:name key="downloadagent.completed.label">Completed</cueslookup:name>
<cueslookup:name key="downloadagent.completed.value">%1 of %2 bytes</cueslookup:name>
<cueslookup:name key="downloadagent.speed.label">Speed</cueslookup:name>
<cueslookup:name key="downloadagent.speed.value">%1 bytes/sec</cueslookup:name>
<cueslookup:name key="updateopswat.rqst">NAC Agent Posture component version %1 is
available.%br% Do you want to install this update now?</cueslookup:name>
<cueslookup:name key="updateopswat.rqst.retry">Unable to update NAC Agent Posture
component. Please try again.</cueslookup:name>
<cueslookup:name key="downloadopswat.report">Downloading the update of NAC Agnet Posture
component.</cueslookup:name>
<cueslookup:name key="login.productname">Education First Compliance Check</cueslookup:name>

<cueslookup:name key="login.version">Version</cueslookup:name>
<cueslookup:name key="login.opswatversion">Posture Component Version</cueslookup:name>

```

```

<cueslookup:name key="login.username">Enter your username</cueslookup:name>
<cueslookup:name key="login.password">Enter your PIN</cueslookup:name>
<cueslookup:name key="login.remember_me">Remember Me</cueslookup:name>
<cueslookup:name key="login.server">Server</cueslookup:name>
<cueslookup:name key="login.customalert">Custom EF package version 2.1.1.1 with EF
Logo</cueslookup:name>
<cueslookup:name key="login.Too many users using this account">This account is already
active on another device</cueslookup:name>
<cueslookup:name key="login.differentuser">Login as Different User</cueslookup:name>
<cueslookup:name key="login.removeoldest">Remove Oldest Login Session</cueslookup:name>

<cueslookup:name key="menu_devtools">Dev Tools</cueslookup:name>
<cueslookup:name key="c.sso.ad">Performing Windows Domain automatic login for
NAC</cueslookup:name>
<cueslookup:name key="c.sso.generic">Unknown authentication type</cueslookup:name>
<cueslookup:name key="c.sso.macauth">Performing device filter automatic login for
NAC</cueslookup:name>
<cueslookup:name key="c.sso.vpn">Performing automatic login into NAC environment for
remote user</cueslookup:name>
<cueslookup:name key="c.title.status.authenticating">Authenticating User</cueslookup:name>

<cueslookup:name key="c.title.status.answerchallenge">Sending Response</cueslookup:name>

<cueslookup:name key="c.title.status.checking">Checking Requirements</cueslookup:name>
<cueslookup:name key="c.title.status.checkcomplete">System Check Complete</cueslookup:name>

<cueslookup:name key="c.title.status.loggedin">NAC Process Completed</cueslookup:name>
<cueslookup:name key="c.title.status.netaccess.none">NAC Process
Completed</cueslookup:name>
<cueslookup:name key="c.title.status.netpolicy">Network Usage Policy</cueslookup:name>
<cueslookup:name key="c.title.status.properties">Agent Properties &#x0026;
Information</cueslookup:name>
<cueslookup:name key="c.title.status.remediating">Remediating System</cueslookup:name>
<cueslookup:name key="c.title.status.session.expired">Session has Expired</cueslookup:name>

<cueslookup:name key="c.title.status.update.available">Update Agent</cueslookup:name>
<cueslookup:name key="c.title.status.update.downloading">Downloading
Agent</cueslookup:name>
<cueslookup:name key="c.title.status.update.opswat.available">Update Posture
Component</cueslookup:name>
<cueslookup:name key="c.title.status.update.opswat.downloading">Downloading Posture
Component</cueslookup:name>
<cueslookup:name key="scanning">Checking</cueslookup:name>
<!-- <cueslookup:name key="scanningitemcomplete">Finished Checking</cueslookup:name> -->

<cueslookup:name key="ph.about">About</cueslookup:name>
<cueslookup:name key="ph.cancel">Cancel</cueslookup:name>
<!-- <cueslookup:name key="ph.details">Details</cueslookup:name> -->
<cueslookup:name key="ph.logout">Logout</cueslookup:name>
<cueslookup:name key="title_remediating">Remediating System</cueslookup:name>
<cueslookup:name key="title_check_complete">System Check Complete</cueslookup:name>
<cueslookup:name key="title_full_access_granted">Logged In</cueslookup:name>
<cueslookup:name key="title_access_denied">Network Access Denied</cueslookup:name>
<cueslookup:name key="tempNetAccess">Temporary Network Access</cueslookup:name>
<cueslookup:name key="announcePleaseBePatient">Please be patient while your system is
checked against the network security policy
</cueslookup:name>
<cueslookup:name key="bbtn.accept">Accept</cueslookup:name>
<cueslookup:name key="bbtn.apply">Apply</cueslookup:name>
<cueslookup:name key="bbtn.cancel">Cancel</cueslookup:name>
<cueslookup:name key="bbtn.continue">Update Later</cueslookup:name>
<cueslookup:name key="bbtn.close">Close</cueslookup:name>
<cueslookup:name key="bbtn.detailshide">Hide Compliance</cueslookup:name>
<cueslookup:name key="bbtn.detailsshow">Show Compliance</cueslookup:name>

```



```

<cueslookup:name key="btn.download">Download</cueslookup:name>
<cueslookup:name key="btn.guestAccess">Guest Access</cueslookup:name>
<cueslookup:name key="btn.go2link">Go To Link</cueslookup:name>
<cueslookup:name key="btn.launch">Launch</cueslookup:name>
<cueslookup:name key="btn.login">Log In</cueslookup:name>
<cueslookup:name key="btn.next">Re-Scan</cueslookup:name>
<cueslookup:name key="btn.ok">OK</cueslookup:name>
<cueslookup:name key="btn.propertieshide">Hide Properties</cueslookup:name>
<cueslookup:name key="btn.reject">Reject</cueslookup:name>
<cueslookup:name key="btn.remediate">Repair</cueslookup:name>
<cueslookup:name key="btn.rescan">Rescan</cueslookup:name>
<cueslookup:name key="btn.reset">Reset</cueslookup:name>
<cueslookup:name key="btn.restrictedNet">Get Restricted NET access This one comes down
    from the network</cueslookup:name>
<cueslookup:name key="btn.savereport">Save Report</cueslookup:name>
<cueslookup:name key="btn.skip">Skip</cueslookup:name>
<cueslookup:name key="btn.skipao">Skip All Optional</cueslookup:name>
<cueslookup:name key="btn.submit">Submit</cueslookup:name>
<cueslookup:name key="btn.update">Update</cueslookup:name>
<cueslookup:name key="cd.days">
days
</cueslookup:name>
<cueslookup:name key="cd.nbsp">
&#xA0;
</cueslookup:name>
<cueslookup:name key="cd.tempNetAccess.counting">
There is approximately %1 left until your temporary network access expires
</cueslookup:name>
<cueslookup:name key="cd.tempNetAccess.expired">
Your Temporary Network Access has Expired!
</cueslookup:name>
<cueslookup:name key="cd.tempNetAccessShort.counting">
%1 left
</cueslookup:name>
<cueslookup:name key="cd.tempNetAccessShort.expired">
Expired!
</cueslookup:name>
<cueslookup:name key="cd.window.counting">
This window will close in %1 secs
</cueslookup:name>
<cueslookup:name key="dp.status.fullNetAccess">
Full Network Access
</cueslookup:name>
<cueslookup:name key="dp.status.fullNetAccess.verbose">
Your device conforms with all the security policies for this protected
network
</cueslookup:name>
<cueslookup:name key="dp.status.fullNetAccessWarn.verbose">
Only optional requirements are failing.
It is recommended that you update your system at
your earliest convenience.
</cueslookup:name>
<cueslookup:name key="dp.status.iprefresh.progress.verbose">
Refreshing IP address. Please Wait...
</cueslookup:name>
<cueslookup:name key="dp.status.iprefresh.complete.verbose">
Refreshing IP address succeeded.
</cueslookup:name>
<cueslookup:name key="dp.status.vlanchange.progress.verbose">
Connecting to protected Network. Please Wait...
</cueslookup:name>
<cueslookup:name key="dp.status.guestNetAccess">
Guest Network Access
</cueslookup:name>

```

```

<cueslookup:name key="dp.status.noNetAccess">
Network Access Denied
</cueslookup:name>
<cueslookup:name key="dp.status.noNetAccess.verbose">
There is at least one mandatory requirement failing.
You are required to update your system before
you can access the network.
</cueslookup:name>
<cueslookup:name key="dp.status.rejectNetPolicy.verbose">
Network Usage Terms and Conditions are rejected. You will not be
allowed to access the network.
</cueslookup:name>
<cueslookup:name key="dp.status.RestrictedNetAccess">
Restricted Network Access granted.
</cueslookup:name>
<cueslookup:name key="dp.status.RestrictedNetAccess.verbose">
You have been granted restricted network access because your device
did not conform with all the security policies for this protected
network and you have opted to defer updating your system. It is recommended
that you update your system at your earliest convenience.
</cueslookup:name>
<cueslookup:name key="dp.status.temporaryNetAccess">
Temporary Network Access
</cueslookup:name>
<cueslookup:name key="dp.status.temporaryNetAccess.bepatient.verbose">
Please be patient while your system is checked against the network security policy.
</cueslookup:name>
<cueslookup:name key="dp.status.pra.mandatoryfailure">
Performing Re-assessment
</cueslookup:name>
<cueslookup:name key="dp.status.pra.mandatoryfailure.verbose">
There is at least one mandatory requirement failing.
You are required to update your system otherwise
your network access will be restricted.
</cueslookup:name>
<cueslookup:name key="dp.status.pra.optionalfailure">
Performing Re-assessment
</cueslookup:name>
<cueslookup:name key="dp.status.pra.optionalfailure.verbose">
Only optional requirements are failing.
It is recommended that you update your system at
your earliest convenience.
</cueslookup:name>
<cueslookup:name key="dp.status.SessionTimeout">
Logged out
</cueslookup:name>
<cueslookup:name key="dp.status.SessionTimeout.verbose">
Temporary Access to the network has expired.
</cueslookup:name>
<cueslookup:name key="dp.status.Unauthenticated">
Logged out
</cueslookup:name>
<cueslookup:name key="dp.status.Unauthenticated.verbose">
&#xA0;
</cueslookup:name>
<cueslookup:name key="ia.status.checkcomplete">
Finished Checking Requirements
</cueslookup:name>
<cueslookup:name key="ia.status.check.inprogress">
Please be patient while we determine if your system is compliant with the security policy

</cueslookup:name>
<cueslookup:name key="ia.status.check.inprogress.01">
Checking %1 out of %2

```

```

</cueslookup:name>
<cueslookup:name key="ia.status.netpolicy">
Access to the network requires that you view and accept the following
Network Usage Policy
</cueslookup:name>
<cueslookup:name key="ia.status.netpolicylinktxt">
Network Usage Policy Terms and Conditions
</cueslookup:name>
<cueslookup:name key="ia.status.remediate.inprogress">
Remediating
</cueslookup:name>
<cueslookup:name key="ia.status.remediate.start">
Please Remediate
</cueslookup:name>
<cueslookup:name key="ia.status.remediate.checkinprogress">
Checking for compliance with Requirement
</cueslookup:name>
<cueslookup:name key="ia.table.name">
Name
</cueslookup:name>
<cueslookup:name key="ia.table.location">
Location
</cueslookup:name>
<cueslookup:name key="ia.table.software">
Software
</cueslookup:name>
<cueslookup:name key="ia.table.software.programs">
program(s)
</cueslookup:name>
<cueslookup:name key="ia.table.update">
Update
</cueslookup:name>
<cueslookup:name key="ia.table.locationcode.nochange">
Do not change current setting
</cueslookup:name>
<cueslookup:name key="ia.table.locationcode.notifybeforedownload">
Notify before download
</cueslookup:name>
<cueslookup:name key="ia.table.locationcode.notifybeforeinstall">
Notify before install
</cueslookup:name>
<cueslookup:name key="ia.table.locationcode.scheduledinstallation">
Download and installation
</cueslookup:name>
<cueslookup:name key="ia.table.locationcode.forcenotifybeforedownload">
Change to notify before download
</cueslookup:name>
<cueslookup:name key="ia.table.locationcode.forcenotifybeforeinstall">
Change to notify before installation
</cueslookup:name>
<cueslookup:name key="ia.table.locationcode.forcescheduledinstall">
Change to download and installation
</cueslookup:name>
<cueslookup:name key="ia.table.description">
Description
</cueslookup:name>
<cueslookup:name key="scs.table.title">
Security Compliance Summary
</cueslookup:name>
<cueslookup:name key="scs.table.header1.scan_rslt">
Scan Result
</cueslookup:name>
<cueslookup:name key="scs.table.header1.pack_name">
Requirement Name

```

```

</cueslookup:name>
<cueslookup:name key="scs.table.header1.pack_details">
Requirement Description - Remediation Suggestion
</cueslookup:name>
<cueslookup:name key="scs.table.data.mandatory">
Mandatory
</cueslookup:name>
<cueslookup:name key="scs.table.data.optional">
Optional
</cueslookup:name>
<cueslookup:name key="scs.table.data.pass">
Passed
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_optional_download">
Please download and install the optional software before accessing the network
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_mandatory_download">
Please download and install the required software before accessing the network
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_optional_launch">
Please launch the optional remediation program(s) before accessing the network
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_mandatory_launch">
Please launch the required remediation program(s) before accessing the network
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_optional_opswat_av">
Please update the virus definition file of the specified antivirus software before
accessing the network (optional)
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_mandatory_opswat_av">
Please update the virus definition file of the specified antivirus software before
accessing the network (required)
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_optional_opswat_as">
Please update the spyware definition file of the specified anti-spyware software before
accessing the network (optional)
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_mandatory_opswat_as">
Please update the spyware definition file of the specified anti-spyware software before
accessing the network (required)
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_optional_win_update">
Please download and install the optional windows updates before accessing the network
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_mandatory_win_update">
Please download and install the required windows updates before accessing the network
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_auto_launch_prog">
Launching Remediation Program(s)...
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_auto_launch_url">
Launching Remediation URL...
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_auto_opswat_av">
Updating Virus Definition...
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_auto_opswat_as">
Updating Spyware Definition...
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_auto_win_update">
Launching Windows auto Update(s)...
</cueslookup:name>
<cueslookup:name key="ia.rem_launch_downloaded_file">
Downloaded at %1. %br% Please open this folder &#x0026; double-click executable file to

```

```

install the required software.
</cueslookup:name>
<cueslookup:name key="discoveryhost.label">
Discovery Host
</cueslookup:name>
<cueslookup:name key="properties.table.title">
List of Antivirus &#x0026; Anti-Spyware Products Detected by the Agent
</cueslookup:name>
<cueslookup:name key="properties.table.header1.index">
No.
</cueslookup:name>
<cueslookup:name key="properties.table.header1.description">
Description
</cueslookup:name>
<cueslookup:name key="properties.table.header1.value">
Value
</cueslookup:name>
<cueslookup:name key="properties.table.data.product_type">
Product Type
</cueslookup:name>
<cueslookup:name key="properties.table.data.product_name">
Product Name
</cueslookup:name>
<cueslookup:name key="properties.table.data.product_version">
Product Version
</cueslookup:name>
<cueslookup:name key="properties.table.data.def_version">
Definition Version
</cueslookup:name>
<cueslookup:name key="properties.table.data.def_date">
Definition Date
</cueslookup:name>
<cueslookup:name key="reboot.mandatory.001">
Mandatory System Reboot Required
</cueslookup:name>
<cueslookup:name key="reboot.optional.001">
You need to reboot your system in order for the changes to take effect.
</cueslookup:name>
<cueslookup:name key="rem.error.001">
Unable to remediate particular requirement
</cueslookup:name>
<cueslookup:name key="rem.error.av_access_denied">
The remediation you are attempting is reporting an access denied error. This is usually
due to a privilege issue. Please contact your system administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.av_buffer_too_small">
The remediation you are attempting has failed with an internal error. Please contact
your system administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.av_elevation_required">
The remediation you are attempting requires elevation. Please contact your system
administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.av_failed">
The remediation you are attempting had a failure. If the problem persists contact your
system administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.av_internal_error">
The remediation you are attempting has reported an internal error. If this problem
persists please contact your system administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.av_not_implemented">
The remediation you are attempting is not implemented for this product. Please contact
your system administrator.

```

```

</cueslookup:name>
<cueslookup:name key="rem.error.av_not_supported">
The remediation you are attempting is not supported for this product. Please contact
your system administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.av_update_faile">
The AV/AS update has failed. Please try again and if this message continues to display
contact your system administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.av_update_failed_due_to_network">
The AV/AS update failed due to a networking issue. Please try again and if this message
continues to display contact your system administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.av_timeout">
The remediation you are attempting has timed out waiting for the operation to finish.
If this continues please contact your system administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.file_dist_size_error">
The size of the downloaded file does not match the package! Please discard downloaded
file and check with your administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.file_is_not_signed">
The file that has been requested was not digitally signed. Please try again and if this
message continues to display contact your system administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.file_save_location_error">
The location for the file to be saved to can not be written. Please choose a different
location.
</cueslookup:name>
<cueslookup:name key="rem.error.http_file_not_found">
The requested file is not found. Please try again and if this problem persists, contact
your system administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.launch_file_not_found">
The file that has been requested could not be launched either because it could not be
found or there was a problem launching it. Please contact your system administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.malformed_URL">
The file that is trying to be downloaded has an incorrect URL. Please contact your system
administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.network_error">
There has been a network error, please try the remediation again. If this message continues
to be seen contact your system administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.update_fail_for_non_admin">
The remediation you are trying to do can not be accomplished at your user level. Please
contact your system administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.wsus_search_failure">
The WSUS search failed. This is probably due to a network issue. Please try again and
if this message continues to display contact your system administrator.
</cueslookup:name>
<cueslookup:name key="server.error.generic">
Agent encountered problems logging user
</cueslookup:name>
<cueslookup:name key="server.error.255">
Network Error: NAC Server could not establish a secure connection to NAC Manager.
This could be due to one or more of the following reasons:
1) NAC Manager certificate has expired or
2) NAC Manager certificate cannot be trusted or
3) NAC Manager cannot be reached or
4) NAC Manager is not responding
Please report this to your network administrator.

```

```
</cueslookup:name>
<cueslookup:name key="server.error.5000">
Invalid provider name
</cueslookup:name>
<cueslookup:name key="server.error.5001">
Failed to add user to online list
</cueslookup:name>
<cueslookup:name key="server.error.5002">
Server communication error
</cueslookup:name>
<cueslookup:name key="server.error.5003">
Invalid username or password
</cueslookup:name>
<cueslookup:name key="server.error.5004">
Unknown user
</cueslookup:name>
<cueslookup:name key="server.error.5005">
Account expired
</cueslookup:name>
<cueslookup:name key="server.error.5006">
Account currently disabled
</cueslookup:name>
<cueslookup:name key="server.error.5007">
Exceed quota limit
</cueslookup:name>
<cueslookup:name key="server.error.5008">
Insufficient Clean Access packages installed
</cueslookup:name>
<cueslookup:name key="server.error.5009">
Access to network is blocked by the administrator
</cueslookup:name>
<cueslookup:name key="server.error.5010">
Vulnerabilities not fixed
</cueslookup:name>
<cueslookup:name key="server.error.5011">
This client version is old and not compatible. Please login from web browser to see the
download link for the new version.
</cueslookup:name>
<cueslookup:name key="server.error.5012">
Network policy is not accepted
</cueslookup:name>
<cueslookup:name key="server.error.5013">
Invalid switch configuration
</cueslookup:name>
<cueslookup:name key="server.error.5014">
Too many users using this account
</cueslookup:name>
<cueslookup:name key="server.error.5015">
Invalid session
</cueslookup:name>
<cueslookup:name key="server.error.5016">
Null session
</cueslookup:name>
<cueslookup:name key="server.error.5017">
Invalid user role
</cueslookup:name>
<cueslookup:name key="server.error.5018">
Invalid login page
</cueslookup:name>
<cueslookup:name key="server.error.5019">
Encoding failure
</cueslookup:name>
<cueslookup:name key="server.error.5020">
A security enhancement is required for your Agent. Please upgrade your Agent or contact
```

```

    your network administrator.
  </cueslookup:name>
  <cueslookup:name key="server.error.5021">
    Can not find server reference
  </cueslookup:name>
  <cueslookup:name key="server.error.5022">
    User role currently disabled
  </cueslookup:name>
  <cueslookup:name key="server.error.5023">
    Authentication server is not reachable
  </cueslookup:name>
  <cueslookup:name key="server.error.5024">
    Agent user operating system is not supported
  </cueslookup:name>
  <cueslookup:name key="server.error.generic_emergency">
    The Agent has encountered an unexpected error and is restarting.
  </cueslookup:name>
  <cueslookup:name key="server.error.http_error">
    Clean Access Server is not available on the network.
  </cueslookup:name>
  <cueslookup:name key="server.error.nw_interface_chg">
    Authentication interrupted due to network status change. Press OK to retry.
  </cueslookup:name>
  <cueslookup:name key="server.error.svr_misconfigured">
    Clean Access Server is not properly configured.
  </cueslookup:name>
  <cueslookup:name key="server.clarification.generic_emergency">
    Please contact your administrator if the problem persists.
  </cueslookup:name>
  <cueslookup:name key="announce.savingreport">
    Saving Report
  </cueslookup:name>
  <cueslookup:name key="announce.savingreport.failed">
    Unable to save report
  </cueslookup:name>
  <cueslookup:name key="announce.cancelremediationack">
    Clicking Cancel may change your network connectivity and interrupt download or required
    updates.<p> Do you want to continue?</p>
  </cueslookup:name>
  <cueslookup:name key="announce.dismiss.default">
    Dismiss to continue
  </cueslookup:name>
  <cueslookup:name key="announce.logoutconfirm">
    Successfully logged out from the network!
  </cueslookup:name>
</cueslookup:appstrings>

```



- (注) カスタマイズしたテキストに使用できる文字数に制限はありません。ただし、カスタマイズされたログイン画面がクライアント上に表示された場合に、あまり大きな領域を必要としないように長さを制限することをシスコは推奨します。

拡張 nacStrings_xx.xml ファイルのサンプル

```

<cueslookup:name key="dp.status.fullNetAccess">Full Network Access</cueslookup:name>
<cueslookup:name key="dp.status.fullNetAccess.verbose">Your device conforms with all the
  security policies for this protected network</cueslookup:name>
<cueslookup:name key="dp.status.fullNetAccessWarn.verbose">Only optional requirements

```



```

are failing. It is recommended that you update your system at your earliest
convenience.</cueslookup:name>
<cueslookup:name key="dp.status.iprefresh.progress.verbose">Refreshing IP address. Please
Wait ...</cueslookup:name>
<cueslookup:name key="dp.status.iprefresh.complete.verbose">Refreshing IP address
succeeded.</cueslookup:name>
<cueslookup:name key="dp.status.vlanchange.progress.verbose">Connecting to protected
Network. Please Wait ...</cueslookup:name>
<cueslookup:name key="dp.status.guestNetAccess">Guest Network Access</cueslookup:name>
<cueslookup:name key="dp.status.noNetAccess">Network Access Denied</cueslookup:name>
<cueslookup:name key="dp.status.noNetAccess.verbose">There is at least one mandatory
requirement failing. You are required to update your system before you can access the
network.
</cueslookup:name><cueslookup:name key="dp.status.rejectNetPolicy.verbose">Network Usage
Terms and Conditions are rejected. You will not be allowed to access the
network.</cueslookup:name>
<cueslookup:name key="dp.status.RestrictedNetAccess">Restricted Network Access
granted.</cueslookup:name>
<cueslookup:name key="dp.status.RestrictedNetAccess.verbose">You have been granted
restricted network access because your device did not conform with all the security
policies for this protected network and you have opted to defer updating your system.
It is recommended that you update your system at your earliest
convenience.</cueslookup:name>
<cueslookup:name key="dp.status.temporaryNetAccess">Temporary Network
Access</cueslookup:name>
<cueslookup:name key="dp.status.temporaryNetAccess.bepatient.verbose">Please be patient
while your system is checked against the network security policy.</cueslookup:name>
<cueslookup:name key="dp.status.pra.mandatoryfailure">Performing
Re-assessment</cueslookup:name>
<cueslookup:name key="dp.status.pra.mandatoryfailure.verbose">There is at least one
mandatory requirement failing. You are required to update your system otherwise your
network access will be restricted.</cueslookup:name>
<cueslookup:name key="dp.status.pra.optionalfailure">Performing
Re-assessment</cueslookup:name>
<cueslookup:name key="dp.status.pra.optionalfailure.verbose">Only optional requirements
are failing. It is recommended that you update your system at your earliest
convenience.</cueslookup:name>
<cueslookup:name key="dp.status.SessionTimeout">Logged out</cueslookup:name>
<cueslookup:name key="dp.status.SessionTimeout.verbose">Temporary Access to the network
has expired.</cueslookup:name>
<cueslookup:name key="dp.status.Unauthenticated">Logged out</cueslookup:name>
<cueslookup:name key="dp.status.Unauthenticated.verbose"> </cueslookup:name>

```

UpdateFeed.xml ディスクリプタ ファイルのテンプレート

これは、[エージェント (Agent)] 画面のカスタマイズ パッケージに必要なファイルの 1 つであり、これにより、[プロパティ (Properties)] 画面などの [Cisco NAC Agent] ダイアログに含まれているロゴ、フィールド、およびメッセージテキストをカスタマイズして、特定の Windows クライアントのネットワーク アクセス要件に合致させることができます。

[エージェント (Agent)] 画面のカスタマイズ パッケージを完了する前、適切な updateFeed.xml XML ディスクリプタ ファイルを構築する必要があります。カスタマイゼーション パッケージに必要な updateFeed.xml ディスクリプタ ファイルのセットアップには、次の例をテンプレートとして使用します。

```

<?xml version="1.0" encoding="utf-8"?>
<feed xmlns="http://www.w3.org/2005/Atom"
xmlns:update="http://www.cisco.com/cpm/update/1.0">
<title>Provisioning Update</title>
<updated>2011-12-21T12:00:00Z</updated>

```

プロファイル作成機能を使用して生成された XML ファイルの例

```
<id>https://www.cisco.com/web/secure/pmbu/provisioning-update.xml</id>
<author>
<name>Cisco Support</name>
<email>support@cisco.com</email>
</author>
<!-- Custom Branding -->
<entry>
<id>http://foo.foo.com/foo/AgentCustomizationPackage/1/1/1/7</id>
<title>Agent Customization Package</title>
<updated>2010-06-07T12:00:00Z</updated>
<summary>This is EF Agent Customization Package 1.1.1.7</summary>
<link rel="enclosure" type="application/zip" href="brand-win.zip" length="18884" />
<update:type>AgentCustomizationPackage</update:type>
<update:version>1.1.1.7</update:version>
<update:os>WINDOWS_ALL</update:os>
</entry>
</feed>
```

updateFeed.xml ディスクリプタ ファイルを作成する際は、次の点に注意してください。

- **<update:os>** : Cisco NAC Agent でサポートされているすべての Windows OS バージョンを含めるには、常にこの属性を「WINDOWS_ALL」に設定する必要があります。Cisco NAC Agent でサポートされている Windows OS バージョンのリストについては、『[Support Information for Cisco NAC Appliance Agents](#)』を参照してください。
- **<update:version>** : これは、アップグレード対象のエージェント カスタマイズ パッケージを参照します。この値は、4 桁の **<n.n.n.n>** にする必要があります、現在インストールされているパッケージバージョンよりも大きな値にする必要があります。
- **<id>** : この ID は任意の文字にすることができますが、エージェント カスタマイズ パッケージごとに一意である必要があります。

プロファイル作成機能を使用して生成された XML ファイルの例

```
<?xml version="1.0" ?>
<cfg>
  <VlanDetectInterval>0</VlanDetectInterval>
  <RetryDetection>3</RetryDetection>
  <PingArp>0</PingArp>
  <PingMaxTimeout>1</PingMaxTimeout>
  <EnableVlanDetectWithoutUI>0</EnableVlanDetectWithoutUI>
  <SignatureCheck>0</SignatureCheck>
  <DisableExit>0</DisableExit>
  <PostureReportFilter>displayFailed</PostureReportFilter>
  <BypassSummaryScreen>1</BypassSummaryScreen>
  <LogFileSize>5</LogFileSize>
  <DiscoveryHost></DiscoveryHost>
  <DiscoveryHostEditable>1</DiscoveryHostEditable>
  <Locale>default</Locale>
  <AccessibilityMode>0</AccessibilityMode>
  <SwissTimeout>1</SwissTimeout>
  <HttpDiscoveryTimeout>30</HttpDiscoveryTimeout>
  <HttpTimeout>120</HttpTimeout>
  <ExceptionMACList></ExceptionMACList>
  <GeneratedMAC></GeneratedMAC>
  <AllowCRLChecks>1</AllowCRLChecks>
  <DisableL3SwissDelay>0</DisableL3SwissDelay>
```

```
<ServerNameRules></ServerNameRules>  
</cfg>
```



- (注) このファイルには、2つの静的（つまり、ユーザまたは Cisco ISE 管理者が編集できない）「AgentCfgVersion」パラメータおよび「AgentBrandVersion」パラメータも含まれています。これらのパラメータは、クライアントでエージェントプロファイルおよびエージェントカスタマイズファイルの現在のバージョンをそれぞれ識別するために使用されます。

クライアントプロビジョニングリソースポリシーの設定

クライアントの場合、どのユーザがリソース（エージェント、エージェントコンプライアンスモジュール、エージェントカスタマイズパッケージ/プロファイル）のどのバージョン（または複数のバージョン）をログイン時およびユーザセッション開始時に Cisco ISE から受信するかは、クライアントプロビジョニングリソースポリシーによって決定されます。

AnyConnect の場合、クライアントプロビジョニングリソースページからリソースを選択し、クライアントプロビジョニングポリシーページで使用する AnyConnect 設定を作成することができます。AnyConnect 設定は、AnyConnect ソフトウェアとそのさまざまなコンフィギュレーションファイルとの関連付けであり、これらのファイルには、Windows および Mac OS X クライアントの AnyConnect バイナリパッケージ、コンプライアンスモジュール、モジュールプロファイル、AnyConnect のカスタマイズおよび言語パッケージなどがあります。

Cisco ISE NAC エージェントの場合、クライアントプロビジョニングポリシーページからリソースを選択できます。

始める前に

- 有効なクライアントプロビジョニングリソースポリシーを作成する前に、Cisco ISE にリソースを追加したことを確認します。エージェントコンプライアンスモジュールをダウンロードすると、システムで使用している既存のモジュールがあれば常にそれが上書きされます。
- クライアントプロビジョニングポリシーで使用されているネイティブのサブリカントプロファイルをチェックして、ワイヤレス SSID が正しいことを確認します。iOS デバイスの場合、接続対象ネットワークが非表示の場合は、[iOS の設定 (iOS Settings)] エリアで [ターゲットネットワークが非表示になっている場合に有効にする (Enable if target network is hidden)] チェックボックスをオンにします。

ステップ 1 [ポリシー (Policy)] > [クライアントプロビジョニング (Client Provisioning)] を選択します。

ステップ 2 動作のドロップダウン **Enable** リストから **Disable** [有効 (Enable)]、[無効 (Disable)]、または **Monitor** [モニタ (Monitor)] を選択します。

- **Enable** : ユーザがネットワークにログインし、クライアントプロビジョニングポリシーのガイドラインに従っている場合に、Cisco ISEがこのポリシーを使用して、クライアントプロビジョニング機能を果たすようにします。
- **Disable** : Cisco ISE は、指定されたリソース ポリシーを使用せずにクライアントプロビジョニング機能を果たします。
- **Monitor** : ポリシーを無効にし、クライアントプロビジョニングセッション要求を監視し、Cisco ISE が [モニタ対象 (Monitored)] のポリシーに基づいて起動しようとした回数を確認します。

ステップ 3 [ルール名 (Rule Name)] テキスト ボックスに、新しいリソース ポリシーの名前を入力します。

ステップ 4 Cisco ISE にログインするユーザが属する ID グループを 1 つ以上指定します。

設定した既存の ID グループのリストから、あらゆる ID タイプを指定することも、1 つ以上のグループを選択することもできます。

ステップ 5 [オペレーティング システム (Operating Systems)] フィールドを使用して、ユーザが Cisco ISE にログインする際に使用するクライアントマシンまたはデバイスで動作している 1 つ以上のオペレーティング システムを指定します。

[Android]、[Mac iOS]、[Mac OS X] などの単一のオペレーティング システムや、[Windows XP (すべて) (Windows XP (All))] や [Windows 7 (すべて) (Windows 7 (All))] など、複数のクライアントマシン オペレーティング システムに対応する包括的なオペレーティング システムの指定を選択できます。

(注) Cisco ISE GUI のクライアントプロビジョニング ポリシー ページに、MAC OS 10.6/10.7/10.8 を選択できるオプションがありますが、これらのバージョンは AnyConnect ではサポートされていません。

ステップ 6 [その他の条件 (Other Conditions)] フィールドで、この特定のリソース ポリシー用に作成する新しい式を指定します。

ステップ 7 クライアント マシンの場合は、[エージェント設定 (Agent Configuration)] を使用して、クライアント マシンで利用可能にし、プロビジョニングするエージェント タイプ、コンプライアンス モジュール、エージェント カスタマイズ パッケージ/プロファイルを指定します。

クライアントマシンで NAC エージェントがポップアップできるようにするには、クライアントプロビジョニングの URL を許可ポリシーに含める必要があります。これにより、ランダムなクライアントからの要求が回避され、適切なリダイレクト URL を持つクライアントのみがポストチャ評価を要求できるようになります。

ステップ 8 [保存 (Save)] **Save** をクリックします。

次のタスク

1 つ以上のクライアントプロビジョニングリソース ポリシーを正常に設定したら、ログイン中にクライアントマシンのポストチャ評価を実行するように Cisco ISE の設定を開始できます。

クライアント プロビジョニング ポリシーの Cisco ISE ポスチャ エージェントの設定

クライアントマシンについて、どのエージェントタイプ、コンプライアンスモジュール、エージェント カスタマイズ パッケージ/プロファイルを、ユーザがクライアント マシンにダウンロードおよびインストールできるように準備するかを設定します。

始める前に

Cisco ISE の AnyConnect および Cisco ISE NAC のクライアントプロビジョニング リソースを追加している必要があります。

ステップ 1 [エージェント (Agent)] **Agent** ドロップダウン リストから使用可能なエージェントを選択し、ここで定義したエージェントのアップグレード (ダウンロード) がクライアント マシンに対して必須かどうかを、[アップグレードは必須か (Is Upgrade Mandatory)] **Is Upgrade Mandatory** オプションを必要に応じて有効または無効にすることによって指定します。

Is Upgrade Mandatory 設定は、エージェントのダウンロードにのみ適用されます。Agent プロファイル、コンプライアンス モジュール、および Agent カスタマイズ パッケージの更新は常に必須です。

ステップ 2 [プロファイル (Profile)] **Profile** ドロップダウン リストから既存のエージェント プロファイルを選択します。

ステップ 3 [コンプライアンスモジュール (Compliance Module)] **Compliance Module** ドロップダウン リストを使用して使用可能なコンプライアンス モジュールを選択し、クライアント マシンにダウンロードします。

ステップ 4 [エージェントカスタマイズパッケージ (Agent Customization Package)] **Agent Customization Package** ドロップダウン リストから、クライアント マシンに使用可能なエージェント カスタマイズ パッケージを選択します。

パーソナル デバイスのネイティブ サプリカントの設定

従業員は、Windows、Mac OS、iOS、および Android デバイスで使用可能なネイティブ サプリカントを使用して、ネットワークに自分のパーソナルデバイスを直接接続できます。パーソナル デバイスに関して、登録されているパーソナル デバイスで使用可能にし、プロビジョニングするネイティブ サプリカントの設定を指定します。

始める前に

ユーザがログインするとき、そのユーザの許可要件と関連付けるプロファイルに基づいて、Cisco ISE が、ユーザのパーソナル デバイスを設定するために必要なサプリカント プロビジョニング ウィザードを提供して、ネットワークにアクセスするように、ネイティブ サプリカント プロファイルを作成します。

ステップ 1 [ポリシー (Policy)] > [クライアント プロビジョニング (Client Provisioning)] を選択します。

ステップ 2 動作のドロップダウン **Enable** リストから **Disable** [有効 (Enable)]、[無効 (Disable)]、または **Monitor** [モニタ (Monitor)] を選択します。

ステップ 3 [ルール名 (Rule Name)] テキスト ボックスに、新しいリソース ポリシーの名前を入力します。

ステップ 4 次を指定します。

- [ID グループ (Identity Groups)] フィールドを使用して、Cisco ISE にログインするユーザが属する ID グループを 1 つ以上指定します。
- [オペレーティング システム (Operating System)] フィールドを使用して、ユーザが Cisco ISE にログインする際に使用するパーソナルデバイスで動作している 1 つ以上のオペレーティング システムを指定します。
- [その他の条件 (Other Conditions)] フィールドを使用して、この特定のリソース ポリシー用に作成する新しい式を指定します。

ステップ 5 パーソナルデバイスの場合、[ネイティブ サプリカントの設定 (Native Supplicant Configuration)] を使用し、特定の **Configuration Wizard** を選択して、パーソナル デバイスに配信します。

ステップ 6 指定されたパーソナル デバイス タイプに適用可能な [ウィザード プロファイル (Wizard Profile)] **Wizard Profile** を指定します。

ステップ 7 [保存 (Save)] をクリックします。

クライアント プロビジョニング レポート

Cisco ISE のモニタリングおよびトラブルシューティング機能にアクセスし、ユーザ ログイン セッションの成功または失敗の全体のトレンドをチェックし、特定の期間にネットワークにログインしたクライアント マシンの数およびタイプに関する統計情報を収集し、また、クライアント プロビジョニング リソースでの最近の設定変更をチェックすることができます。

クライアント プロビジョニングの要求

[操作 (Operations)] > [レポート (Reports)] > [ISE レポート (ISE Reports)] > [エンドポイントおよびユーザ (Endpoints and Users)] > [クライアント プロビジョニング (Client Provisioning)] レポートには、クライアント プロビジョニング 要求の成功および失敗に関する統計情報が表示されます。[実行 (Run)] **Run** を選択していずれかのプリセット 期間を指定すると、Cisco ISE によってデータベースが調べられ、生成されたクライアント プロビジョニング データが表示されます。

サプリカント プロビジョニングの要求

[操作 (Operations)] > [レポート (Reports)] > [ISE レポート (ISE Reports)] > [エンドポイントおよびユーザ (Endpoints and Users)] > [サプリカント プロビジョニング (Supplicant Provisioning)] ウィンドウには、最近の成功および失敗したユーザ デバイス 登録およびサプリカント プロビジョニング 要求に関する情報が表示されます。[実行 (Run)] **Run** を選択して

いずれかのプリセット期間を指定すると、Cisco ISE によってデータベースが調べられ、生成されたサブリカント プロビジョニング データが表示されます。

サブリカント プロビジョニング レポートは、特定の期間にデバイス登録ポータルから登録されたエンドポイントのリストに関する情報が提供されます。これには、ログイン日時、ID（ユーザ ID）、IP アドレス、MAC アドレス（エンドポイント ID）、サーバプロファイル、エンドポイント オペレーティング システム、SPW バージョン、障害理由（ある場合）、登録のステータスなどのデータが含まれます。

クライアント プロビジョニング イベント ログ

クライアントの動作の問題の診断に役立つイベント ログ エントリを検索できます。たとえば、ネットワーク上のクライアント マシンがログイン時にクライアント プロビジョニング リソースの更新を取得できないという問題の原因を特定する必要がある場合があります。ポスチャおよびクライアント プロビジョニング の監査、ポスチャおよびクライアント プロビジョニング の診断のログギング エントリを使用できます。



第 26 章

クライアント ポスチャ ポリシーの設定

ポスチャは、Cisco Identity Services Engine (ISE) のサービスです。ポスチャを使用すると、ネットワークに接続されているすべてのエンドポイントの企業セキュリティポリシーとのコンプライアンスに関するステート（ポスチャとも呼ばれる）をチェックできます。これにより、ネットワークの防護領域にアクセスするクライアントを制御できます。

- [ポスチャ サービス \(932 ページ\)](#)
- [ポスチャ管理の設定 \(936 ページ\)](#)
- [Cisco ISE へのポスチャ更新のダウンロード \(940 ページ\)](#)
- [ポスチャ評価の利用規定の設定 \(941 ページ\)](#)
- [ポスチャ条件 \(942 ページ\)](#)
- [単純ポスチャ条件 \(942 ページ\)](#)
- [単純ポスチャ条件の作成 \(943 ページ\)](#)
- [複合ポスチャ条件 \(943 ページ\)](#)
- [Windows クライアントでの自動アップデートを有効にするためのシスコ事前定義の条件 \(944 ページ\)](#)
- [シスコ事前設定済みアンチウイルスおよびアンチスパイウェア条件 \(944 ページ\)](#)
- [アンチウイルスとアンチスパイウェア サポート表 \(944 ページ\)](#)
- [コンプライアンス モジュール \(945 ページ\)](#)
- [複合ポスチャ条件の作成 \(946 ページ\)](#)
- [パッチ管理条件の作成 \(947 ページ\)](#)
- [ディスク暗号化条件の作成 \(948 ページ\)](#)
- [ポスチャ ポリシーの設定 \(948 ページ\)](#)
- [ポスチャ評価オプション \(949 ページ\)](#)
- [ポスチャ修復オプション \(950 ページ\)](#)
- [ポスチャのカスタム条件 \(951 ページ\)](#)
- [カスタム ポスチャ修復アクション \(952 ページ\)](#)
- [ポスチャ評価要件 \(957 ページ\)](#)
- [ポスチャのカスタム権限 \(959 ページ\)](#)
- [標準許可ポリシーの設定 \(960 ページ\)](#)
- [ステルス モードの展開 \(961 ページ\)](#)

- [ポスチャ ポリシーと要件タイプへのステルス モードの影響 \(962 ページ\)](#)
- [ポスチャとネットワーク ドライブ マッピングのベスト プラクティス \(965 ページ\)](#)
- [AnyConnect クライアントレス モード ワークフロー \(965 ページ\)](#)

ポスチャ サービス

ポスチャは、Cisco Identity Services Engine (ISE) のサービスです。ポスチャを使用すると、ネットワークに接続されているすべてのエンドポイントの企業セキュリティポリシーとのコンプライアンスに関するステート（ポスチャとも呼ばれる）をチェックできます。これにより、ネットワークの防護領域にアクセスするクライアントを制御できます。

クライアントは、エンドポイントの AnyConnect ISE ポスチャ エージェントまたはネットワーク アドミッション コントロール (NAC) を介してポスチャ サービスと相互作用して、セキュリティポリシーを適用し、コンプライアンスを満たし、エンドポイントから保護されたネットワークへのアクセスを可能にします。クライアントプロビジョニングは、エンドポイントが適切なポスチャ エージェントを受信できるようにします。

Cisco ISE の ISE ポスチャ エージェントでは、ネイティブ サブリカントを使用する場合は Windows のユーザの簡易切り替え機能がサポートされません。これは、古いユーザの切断が明確にならないためです。新しいユーザが送信されると、古いユーザのプロセスとセッション ID がエージェントによってハングされるため、新しいポスチャセッションを実行できません。Microsoft のセキュリティ ポリシーに従い、ユーザの簡易切り替え機能を無効にすることを推奨します。

ISE コミュニティ リソース

[Configure ISE 2.1 and AnyConnect 4.3 Posture USB Check](#)

[How To Configure Posture with AnyConnect Compliance Module and ISE 2.0](#)

関連トピック

[ポスチャ サービスのコンポーネント \(932 ページ\)](#)

[ポスチャおよびクライアントプロビジョニング ポリシー ワークフロー \(934 ページ\)](#)

[ポスチャ サービス ライセンス \(934 ページ\)](#)

ポスチャ サービスのコンポーネント

Cisco ISE ポスチャ サービスには、主にポスチャ管理サービスとポスチャ ランタイム サービスが含まれます。

ポスチャ管理サービス

Cisco ISE に APeX ライセンスをインストールしていない場合、ポスチャ管理サービス オプションは管理者ポータルから使用できません。

管理サービスは、ポスチャ サービス用に設定された要件および許可ポリシーに関連付けられた、ポスチャ固有のカスタム条件および修復アクションに対するバックエンドサポートを提供します。

ポスチャ ランタイム サービス

ポスチャ ランタイム サービスでは、ポスチャ評価およびクライアントの修復のためにクライアント エージェントと Cisco ISE サーバの間で実行されるすべての相互作用をカプセル化します。

ポスチャ ランタイム サービスは検出フェーズから開始します。エンドポイントセッションは、エンドポイントが 802.1x 認証に成功した後に作成されます。クライアント エージェントは、次の順序で各種の方式によって検出パケットを送信して Cisco ISE ノードへの接続を試行します。

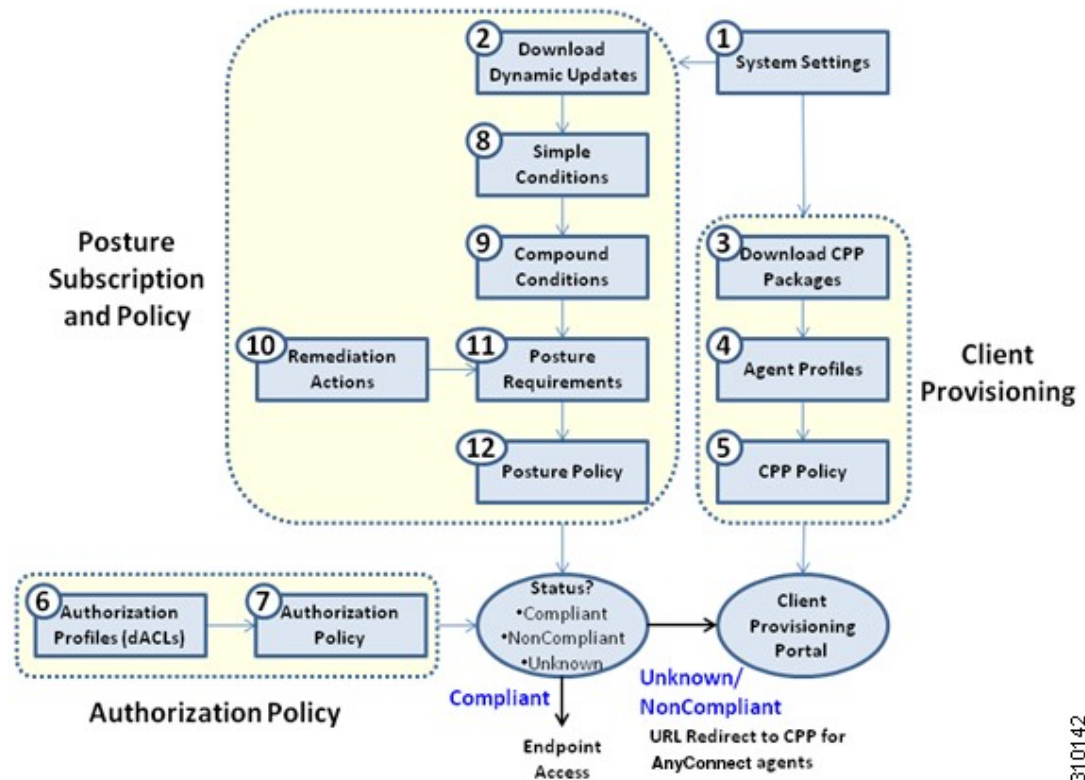
1. HTTP 経由で Cisco ISE サーバのポート 80 へ（設定されている場合）
2. HTTPS 経由で Cisco ISE サーバのポート 8905 へ（設定されている場合）
3. HTTP 経由でデフォルト ゲートウェイのポート 80 へ
4. HTTPS 経由でポート 8905 からそれぞれ前にアクセスしたサーバへ
5. HTTP 経由で enroll.cisco.com のポート 80 へ

ポスチャ フェーズは、利用規定（存在する場合）が受け入れられると開始されます。Cisco ISE ノードはクライアント エージェントにポスチャ ドメインのポスチャ トークンを発行します。ポスチャ トークンにより、エンドポイントではポスチャ プロセスを再度実行せずにネットワークに再接続できます。これには、エージェント GUID、利用規定のステータス、エンドポイントのオペレーティング システム情報などの情報が含まれています。

ポスチャ フェーズで使用するメッセージは、NEA PB/PA 形式 (RFC5792) です。

ポスチャおよびクライアントプロビジョニングポリシーワークフロー

図 51: Cisco ISE のポスチャおよびクライアントプロビジョニングポリシーワークフロー



310142

ポスチャ サービス ライセンス

Cisco ISE は、Base ライセンス、Plus ライセンス、APeX ライセンスの 3 種類のライセンスを提供します。プライマリ PAN で APeX ライセンスをインストールしないと、ポスチャ要求は Cisco ISE で実行されません。Cisco ISE のポスチャサービスは、1 つのノードまたは複数のノードで実行できます。

ポスチャ サービス 展開

Cisco ISE は、スタンドアロン環境（単一ノード）または分散環境（複数ノード）に展開できます。

スタンドアロン Cisco ISE 展開では、単一のノードをすべての管理サービス、モニタリングとトラブルシューティングサービス、およびポリシー実行時サービスに設定できます。

分散 Cisco ISE 展開では、各ノードを、管理サービス、モニタリングとトラブルシューティングサービス、およびポリシー実行時サービスの Cisco ISE ノードとして設定できます。管理サービスを実行しているノードは、Cisco ISE 展開内のプライマリ ノードです。他のサービス

を実行している他のノードは、互いのバックアップ サービス用に設定できるセカンダリ ノードです。

Cisco ISE でのポスチャ セッション サービスの有効化

始める前に

- クライアントから受信したすべてのポスチャ要求に対応するには、Cisco ISE でセッション サービスを有効にし、拡張ライセンス パッケージをインストールする必要があります。
- 分散展開に複数のノードを登録している場合は、登録したすべてのノードがプライマリ ノードとは別に [展開ノード (Deployment Nodes)] ページに表示されます。各ノードを Cisco ISE ノード (管理ペルソナ、ポリシー サービス ペルソナ、およびモニタリング ペルソナ) として設定できます。
- ポスチャ サービスは、ポリシー サービス ペルソナを担当する Cisco ISE ノードでのみ実行 され、分散展開で管理ペルソナとモニタリング ペルソナを担当する Cisco ISE ノードでは 実行されません。

ステップ 1 [管理 (Administration)] > [システム (System)] > [展開 (Deployment)] > [展開 (Deployment)] を選択 します。

ステップ 2 [展開ノード (Deployment Nodes)] ウィンドウから Cisco ISE ノードを選択します。

ステップ 3 [編集 (Edit)] をクリックします。

ステップ 4 [全般設定 (General Settings)] タブで [ポリシーサービス (Policy Service)] チェックボックスをオンにしま す。

[ポリシー サービス (Policy Service)] チェックボックスがオフになっている場合は、セッション サービス とプロファイリング サービスの両方のチェックボックスが無効になります。

ステップ 5 ポリシーサービスペルソナでネットワークアクセス、ポスチャ、ゲスト、およびクライアントプロビジョ ニングのセッション サービスを実行するには、[セッション サービスの有効化 (Enable Session Services)] チェックボックスをオンにします。セッションサービスを停止するには、このチェックボックスをオフに します。

ステップ 6 [保存 (Save)] をクリックします。

ポスチャ評価レポートの実行

ポスチャの詳細な評価を実行して、ポスチャ評価中に使用されるポスチャ ポリシーに対するク ライアントのコンプライアンスの詳細なステータスを生成できます。

ステップ 1 [操作 (Operations)] > [レポート (Reports)] > [ISE レポート (ISE Reports)] > [エンドポイントとユー ザ (Endpoints and Users)] > [ポスチャの詳細な評価 (Posture Detail Assessment)] を選択します。

ステップ 2 [時間範囲 (Time Range)] ドロップダウン リストから特定の期間を選択します。

ステップ 3 [実行 (Run)] をクリックして、選択した期間中にアクティブだったすべてのエンドポイントの概要を表示します。

ポスチャ管理の設定

ポスチャ サービス用の管理者ポータルをグローバルに設定できます。シスコから Web 経由で自動的に Cisco ISE サーバに更新をダウンロードできます。また、オフラインで、後で、Cisco ISE を手動で更新することもできます。さらに、クライアントに AnyConnect、NAC Agent、Web Agent などのエージェントがインストールされていると、クライアントにポスチャ評価および修復サービスが提供されます。クライアント エージェントは、Cisco ISE に対してクライアントのコンプライアンスステータスを定期的に更新します。ログインおよびポスチャの要件評価が正常に完了した後、ネットワーク使用の利用規約への準拠をエンドユーザに求めるリンクが示されたダイアログがクライアント エージェントに表示されます。このリンクを使用して、エンドユーザがネットワークへのアクセス権を取得する前に同意する、企業ネットワークのネットワーク使用情報を定義できます。

関連トピック

[クライアントのタイマー設定](#) (936 ページ)

[非エージェント デバイスへのポスチャ ステータスの設定](#) (938 ページ)

[ポスチャのリース](#) (938 ページ)

[ポスチャ評価の利用規定の設定](#) (941 ページ)

クライアントのタイマー設定

ユーザが修復するためのタイマー、あるステータスから別のステータスに移行するためのタイマー、およびログイン成功画面を制御するためのタイマーをセットアップできます。

エージェントプロファイルを設定して、修復タイマー、ネットワーク遷移遅延タイマー、およびクライアントマシン上でログイン成功画面を制御するために使用するタイマー制御し、これらの設定がポリシーベースになるようにすることを推奨します。[NACまたはAnyConnectポスチャプロファイル (NAC or AnyConnect Posture Profile)] ウィンドウ ([**ポリシー (Policy)**] > [**ポリシー要素 (Policy Elements)**] > [**結果 (Results)**] > [**クライアントプロビジョニング (Client Provisioning)**] > [**リソース (Resources)**] > [**追加 (Add)**] > [NACまたはAnyConnectポスチャプロファイル (NAC or AnyConnect Posture Profile)]) で、クライアントプロビジョニングリソースのエージェントに対して、これらすべてのタイマーを設定できます。

しかし、クライアントプロビジョニングポリシーに一致するように設定されたエージェントプロファイルがない場合、[全般設定 (General Settings)] の設定ウィンドウ ([**管理 (Administration)**] > [**システム (System)**] > [**設定 (Settings)**] > [**ポスチャ (Posture)**] > [**全般設定 (General Settings)**]) の設定を使用できます。

関連トピック

[指定した時間内で修復するためのクライアントの修復タイマーの設定](#) (937 ページ)

[クライアントの遷移のためのネットワーク遷移遅延タイマーの設定](#) (937 ページ)

[ログイン成功ウィンドウを自動的に閉じる設定](#) (937 ページ)

指定した時間内で修復するためのクライアントの修復タイマーの設定

指定した時間内にクライアントを修復するためのタイマーを設定できます。最初の評価時にクライアントが設定されたポスチャポリシーを満たすことに失敗した場合、エージェントは修復タイマーに設定された時間内にクライアントが修復するのを待ちます。クライアントがこの指定時間内の修復に失敗すると、クライアント エージェントはポスチャ ランタイム サービスにレポートを送信します。その後、クライアントは非準拠状態に移行されます。

ステップ 1 [管理 (Administration)] > [システム (System)] > [設定 (Settings)] > [ポスチャ (Posture)] > [全般設定 (General Settings)] を選択します。

ステップ 2 [修復タイマー (Remediation Timer)] フィールドに、分単位で時間の値を入力します。

デフォルト値は 4 分です。有効な範囲は 1 ～ 300 分です。

ステップ 3 [保存 (Save)] をクリックします。

クライアントの遷移のためのネットワーク遷移遅延タイマーの設定

ネットワーク遷移遅延タイマーを使用して、指定した時間内に、クライアントがある状態から別の状態に遷移するためのタイマーを設定できます。これは、許可変更 (CoA) が完了するために必要となります。ポスチャの成功時と失敗時にクライアントが新しい VLAN の IP アドレスを取得するための時間がかかる場合は、より長い遅延時間が必要になることがあります。クライアントが正常にポスチャされると、Cisco ISE は、ネットワーク遷移遅延タイマーで指定された時間内に未知から準拠モードへ移行することを許可します。ポスチャに失敗すると、Cisco ISE は、タイマーで指定された時間内にクライアントが未知から非準拠モードへ移行することを許可します。

ステップ 1 [管理 (Administration)] > [システム (System)] > [設定 (Settings)] > [ポスチャ (Posture)] > [全般設定 (General Settings)] を選択します。

ステップ 2 [ネットワーク遷移遅延 (Network Transition Delay)] フィールドに時間値を秒単位で入力します。

デフォルト値は 3 秒です。有効な値の範囲は 2 ～ 30 秒です。

ステップ 3 [保存 (Save)] をクリックします。

ログイン成功ウィンドウを自動的に閉じる設定

ポスチャ評価が正常に完了した後、クライアント エージェントは一時的なネットワーク アクセス画面を表示します。ユーザはログイン ウィンドウで [OK] ボタンをクリックして、この画面を閉じる必要があります。指定した時間の経過後にこのログイン画面を自動的に閉じるタイマーを設定できます。

ステップ 1 [管理 (Administration)] > [システム (System)] > [設定 (Settings)] > [ポスチャ (Posture)] > [全般設定 (General Settings)] を選択します。

ステップ 2 [経過後にログイン成功画面を自動的に閉じる (Automatically Close Login Success Screen After)] チェックボックスをオンにします。

ステップ 3 [経過後にログイン成功画面を自動的に閉じる (Automatically Close Login Success Screen After)] チェックボックスの横のフィールドに時間値を秒単位で入力します。

有効な値の範囲は 0 ～ 300 秒です。時間をゼロに設定すると、AnyConnect はログイン成功画面を表示しません。

ステップ 4 [保存 (Save)] をクリックします。

非エージェント デバイスへのポスチャ ステータスの設定

Linux または iDevice などの非エージェント デバイスで実行されるエンドポイントのポスチャ ステータスを設定できます。Android デバイスおよび iPod、iPhone、iPad などの Apple の iDevice が Cisco ISE 対応ネットワークに接続する場合、これらのデバイスはデフォルト ポスチャ ステータスの設定を引き継ぎます。

これらの設定は、ポスチャのランタイム中に一致するポリシーが見つからない場合、Windows および Macintosh オペレーティングシステムで実行されるエンドポイントにも適用されます。

始める前に

エンドポイントにポリシーを適用するには、対応するクライアントプロビジョニングポリシー（エージェントのインストールパッケージ）を設定する必要があります。そうしないと、エンドポイントのポスチャ ステータスは自動的にデフォルト設定が反映されます。

ステップ 1 [管理 (Administration)] > [システム (System)] > [設定 (Settings)] > [ポスチャ (Posture)] > [全般設定 (General Settings)] を選択します。

ステップ 2 [デフォルトポスチャステータス (Default Posture Status)] ドロップダウン リストから、オプションに [準拠 (Compliant)] または [非準拠 (Noncompliant)] を選択します。

ステップ 3 [保存 (Save)] をクリックします。

ポスチャのリース

ユーザがネットワークにログインするたびにポスチャ評価を実行したり、指定した間隔でポスチャ評価を実行したりするよう Cisco ISE を設定できます。有効な範囲は 1 ～ 365 日です。

この設定は、ポスチャ評価に AnyConnect エージェントを使用するユーザだけに適用されます。

定期的再評価

定期的再評価（PRA）は、コンプライアンスについてすでに適切にポスチャされているクライアントにのみ実行できます。PRAは、クライアントがネットワーク上で準拠していない場合には実行されません。

PRAは、エンドポイントが準拠ステートになっている場合にのみ有効であり、適用可能です。ポリシーサービスノードは関連するポリシーを調べ、設定で定義されているクライアントロールに応じて要件をコンパイルし、PRAを適用します。PRA設定の一致が見つかった場合、ポリシーサービスノードは、クライアントのPRA設定で定義されているPRA属性を使用して、クライアントエージェントに応答してから、CoA要求を発行します。クライアントエージェントは、設定に指定された間隔に基づいて定期的にPRA要求を送信します。PRAが成功した場合、または、PRA設定に指定されているアクションが続行になっている場合、クライアントは準拠ステートのままになります。クライアントがPRAを満たしていない場合、準拠ステートから非準拠ステートに移行します。

PostureStatus属性は、ポスチャ再評価要求の場合でも、PRA要求で現在のポスチャステータスを不明ではなく準拠と示します。PostureStatusはモニタリングレポートでも更新されます。

ポスチャのリースが有効期限内の場合、アクセスコントロールリスト（ACL）に基づいてエンドポイントが準拠し、PRAが開始されます。PRAが失敗すると、エンドポイントが非準拠になり、ポスチャのリースがリセットされます。

定期的再評価の設定

コンプライアンスに対してすでに正常にポスチャされているクライアントだけの定期的な再評価を設定できます。システムで定義されているユーザIDグループに各PRAを設定できます。

始める前に

- 各PRA設定に、一意のグループ、または設定に割り当てられているユーザIDグループの一意の組み合わせがあることを確認します。
- 2つの一意のロールであるrole_test_1およびrole_test_2をPRA設定に割り当てることができます。論理演算子とこれら2つのロールを組み合わせ、2つのロールの一意の組み合わせとしてPRA設定に割り当てることができます。たとえば、role_test_1 OR role_test_2とします。
- 2つのPRA設定に共通のユーザIDグループがないことを確認します。
- PRA設定がユーザIDグループ「Any」にすでに存在する場合、次のことを実行しないと、他のPRA設定を作成できません。
 - Any以外のユーザIDグループを反映するように、任意のユーザIDグループで既存のPRA設定を更新します。
 - ユーザIDグループ「Any」の既存のPRA設定を削除します。

-
- ステップ 1** [管理 (Administration)] > [システム (System)] > [設定 (Settings)] > [ポスチャ (Posture)] > [再評価 (Reassessments)] を選択します。
- ステップ 2** [追加 (Add)] をクリックします。
- ステップ 3** 新しい PRA を作成するには、[新規再評価の設定 (New Reassessment Configuration)] ページで値を変更します。
- ステップ 4** [送信 (Submit)] をクリックして、PRA 設定を作成します。
-

関連トピック

[定期的再評価](#) (939 ページ)

Cisco ISE へのポスチャ更新のダウンロード

ポスチャ更新には、Windows および Macintosh オペレーティング システムの両方のアンチウイルスとアンチスパイウェアの一連の事前定義済みのチェック、ルール、サポート表、およびシスコでサポートされるオペレーティング システム情報が含まれます。また、ローカル ファイル システムの更新の最新のアーカイブを含むファイルから Cisco ISE をオフラインで更新することもできます。

ネットワークに Cisco ISE を初めて展開する場合は、Web からポスチャ更新をダウンロードできます。通常、このプロセスには約 20 分かかります。初回ダウンロード後に、差分更新が自動的にダウンロードされるように Cisco ISE を設定できます。

Cisco ISE では、初回ポスチャ更新時に 1 回のみ、デフォルトのポスチャ ポリシー、要件、および修復を作成します。それらを削除した場合、Cisco ISE は後続の手動またはスケジュールされた更新中にこれらを再作成しません。

始める前に

ポスチャ リソースを Cisco ISE にダウンロードできる適切なリモートロケーションにアクセスできるようにするには、5-2 ページの「Cisco ISE でのプロキシ設定の指定」の説明に従ってネットワークにプロキシが正しく設定されていることを確認する必要があります。

[ポスチャ更新 (Posture Update)] ページを使用して、Web から更新を動的にダウンロードできます。

-
- ステップ 1** [管理 (Administration)] > [システム (System)] > [設定 (Settings)] > [ポスチャ (Posture)] > [更新 (Updates)] を選択します。
- ステップ 2** [Web] オプションを選択して、更新を動的にダウンロードします。
- ステップ 3** [デフォルトに設定 (Set to Default)] をクリックして、[フィード URL の更新 (Update Feed URL)] フィールドのシスコのデフォルト値を設定します。

ネットワークで URL リダイレクション機能（プロキシ サーバ経由など）を制限しているために、上記の URL へのアクセスに問題がある場合は、Cisco ISE で関連トピックの代替 URL を指定してください。

ステップ 4 [ポスチャ更新 (Posture Updates)] ページの値を変更します。

ステップ 5 シスコからの更新をダウンロードするには、[今すぐ更新 (Update Now)] をクリックします。

ステップ 6 Cisco ISE で他のタスクを続行するには [OK] をクリックします。

更新されると、[ポスチャ更新 (Posture Updates)] ページに、[ポスチャ更新 (Posture Updates)] ページの [更新情報 (Update Information)] セクションの更新の確認として現在のシスコ更新のバージョン情報が表示されます。

関連トピック

[ポスチャ更新の自動ダウンロード](#) (941 ページ)

ポスチャ更新の自動ダウンロード

最初の更新後に、更新を確認し、自動的にダウンロードするように Cisco ISE を設定できます。

始める前に

- 最初にポスチャ更新をダウンロードして、更新を確認し、自動的にダウンロードするように Cisco ISE を設定しておく必要があります。

ステップ 1 [管理 (Administration)] > [システム (System)] > [設定 (Settings)] > [ポスチャ (Posture)] > [更新 (Updates)] を選択します。

ステップ 2 [ポスチャ更新 (Posture Updates)] ページで [初期遅延から開始される更新の自動確認 (Automatically check for updates starting from initial delay)] チェックボックスをオンにします。

ステップ 3 初期遅延時間を hh:mm:ss の形式で入力します。

Cisco ISE は、初期遅延時間の終了後に確認を開始します。

ステップ 4 時間間隔を時間単位で入力します。

Cisco ISE は初期遅延時間から指定した間隔で、展開に更新をダウンロードします。

ステップ 5 [はい (Yes)] をクリックして続行します。

ステップ 6 [保存 (Save)] をクリックします。

ポスチャ評価の利用規定の設定

ログインし、クライアントのポスチャ評価が成功すると、クライアントエージェントにより一時的なネットワークアクセス画面が表示されます。この画面には、利用規定 (AUP) へのリンクが含まれています。ユーザがリンクをクリックすると、ネットワーク利用条件を表示するページにリダイレクトされます。その条件を読み、同意する必要があります。

各利用規定設定には、一意のユーザ ID グループ、またはユーザ ID グループの一意の組み合わせが必要です。Cisco ISE は最初に一致したユーザ ID グループの AUP を見つけ、AUP を表示するクライアント エージェントと通信します。

ステップ 1 [管理 (Administration)] > [システム (System)] > [設定 (Settings)] > [ポスチャ (Posture)] > [利用規定 (Acceptable Use Policy)] を選択します。

ステップ 2 [追加 (Add)] をクリックします。

ステップ 3 [新規利用規定設定 (New Acceptable Use Policy Configuration)] ページで値を変更します。

ステップ 4 [送信 (Submit)] をクリックします。

ポスチャ条件

ポスチャ条件は次の単純条件のいずれかになります。ファイル、レジストリ、アプリケーション、サービス、またはディクショナリ条件。これらの単純条件のうちの1つ以上の条件によって複合条件が形成され、複合条件はポスチャ要件と関連付けることができます。

ネットワークに Cisco ISE を初めて展開する場合は、Web からポスチャ更新をダウンロードできます。このプロセスは、初期ポスチャ更新と呼ばれます。

初期ポスチャ更新の後、Cisco ISE はシスコ定義の単純および複合条件も作成します。シスコ定義の単純条件はプレフィクスとして `pc_` が付けられ、複合条件はプレフィクスとして `pr_` が付けられています。

ダイナミック ポスチャ更新の結果としてシスコ定義の条件を Web を介してダウンロードするように Cisco ISE を設定することもできます。シスコ定義のポスチャ条件を削除または編集することはできません。

ユーザ定義の条件やシスコ定義の条件には、単純条件と複合条件の両方が含まれます。

単純ポスチャ条件

ポスチャ ナビゲーション ペインを使用して、次の単純条件を管理できます。

- **ファイル条件**：ファイルの存在、ファイルの日付、およびクライアントのファイルバージョンを確認する条件。
- **レジストリ条件**：レジストリ キーの存在またはクライアントのレジストリ キーの値を確認する条件。
- **アプリケーション条件**：アプリケーション（プロセス）がクライアント上で実行されているかまたは実行されていないかを確認する条件。
- **サービス条件**：サービスがクライアント上で実行されているかまたは実行されていないかを確認する条件。

- ディクショナリ条件：ディクショナリ属性と値を確認する条件。
- USB 条件：USB マス ストレージ デバイスの有無をチェックする条件。

関連トピック

- [ファイル条件の設定](#) (1369 ページ)
- [レジストリ条件の設定](#) (1377 ページ)
- [アプリケーション条件の設定](#)
- [サービス条件の設定](#) (1381 ページ)
- [ディクショナリ単純条件の設定](#) (1393 ページ)
- [USB 条件の設定](#) (1399 ページ)

単純ポスチャ条件の作成

ポスチャ ポリシーまたは他の複合条件で使用できる、ファイル、レジストリ、アプリケーション、サービス、およびディクショナリ単純条件を作成できます。

始める前に

次のタスクを実行するには、スーパー管理者またはポリシー管理者である必要があります。

-
- ステップ 1** [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [条件 (Conditions)] > [ポスチャ (Posture)] を選択します。
 - ステップ 2** [ファイル (File)]、[レジストリ (Registry)]、[アプリケーション (Application)]、[サービス (Service)]、または [ディクショナリ単純条件 (Dictionary Simple Condition)] のいずれかを選択します。
 - ステップ 3** [追加 (Add)] をクリックします。
 - ステップ 4** フィールドに適切な値を入力します。
 - ステップ 5** [送信 (Submit)] をクリックします。
-

複合ポスチャ条件

複合条件は、1 つ以上の単純条件、または複合条件で構成されます。ポスチャ ポリシーを定義する場合、次の複合条件を使用できます。

- 複合条件：1 つ以上の単純条件、またはタイプがファイル、レジストリ、アプリケーション、またはサービス条件の複合条件が含まれます
- アンチウイルス複合条件：1 つ以上の AV 条件、または AV 複合条件が含まれます
- アンチスパイウェア複合条件：1 つ以上の AS 条件、または AS 複合条件が含まれます

- ディクショナリ複合条件：1 つ以上のディクショナリ単純条件またはディクショナリ複合条件が含まれます
- マルウェア対策条件：1 つ以上の AM 条件が含まれます

Windows クライアントでの自動アップデートを有効にするためのシスコ事前定義の条件

pr_AutoUpdateCheck_Rule はシスコによって事前定義された条件であり、[複合条件 (Compound Conditions)] ページにダウンロードされます。この条件を使用すると、Windows クライアント上で自動アップデート機能が有効になっているかどうかを確認することができます。Windows クライアントがこの要件を満たさない場合、ネットワークアクセスコントロール (NAC) エージェントによって、Windows クライアントの自動アップデート機能が強制的に有効になります (修復)。この修復後、Windows クライアントはポスチャ準拠になります。自動アップデート機能が Windows クライアント上で有効になっていない場合は、ポスチャ ポリシーで関連付けた Windows Update 修復で Windows 管理者設定を上書きします。

シスコ事前設定済みアンチウイルスおよびアンチスパイウェア条件

Cisco ISE の [AV 複合条件 (AV Compound Condition)] および [AS 複合条件 (AS Compound Condition)] ページには、アンチウイルスとアンチスパイウェアの事前設定済みの複合条件がロードされます。これらの条件は、Windows および Macintosh オペレーティングシステムのアンチウイルスおよびアンチスパイウェアサポート表で定義されます。これらの複合条件では、指定されたアンチウイルスとアンチスパイウェア製品がすべてのクライアント上に存在するかどうかを確認できます。Cisco ISE で新しいアンチウイルスとアンチスパイウェアの複合条件を作成することもできます。

アンチウイルスとアンチスパイウェア サポート表

Cisco ISE は、各ベンダー製品の最新バージョンおよび定義ファイルの日付を提供するアンチウイルスとアンチスパイウェアサポート表を使用します。ユーザは頻繁にアンチウイルスとアンチスパイウェアサポート表をポーリングする必要があります。アンチウイルスとアンチスパイウェアのベンダーはアンチウイルスとアンチスパイウェア定義ファイルを頻繁に更新するため、各ベンダー製品の最新バージョンおよび定義ファイルの日付を検索します。

新しいアンチウイルスとアンチスパイウェアのベンダー、製品、リリースのサポートを反映するようにアンチウイルスとアンチスパイウェア サポート表が更新されるたびに、NAC Agent は新しいアンチウイルスとアンチスパイウェア ライブラリを受け取ります。これは、NAC Agent がより新しい追加機能をサポートするのに役立ちます。NAC Agent がこのサポート情報

を取得すると、定期的に更新される `se-checks.xml` ファイル (`se-templates.tar.gz` アーカイブで `se-rules.xml` ファイルとともに公開される) で最新の定義情報をチェックし、クライアントがポスチャポリシーに準拠しているかどうかを決定します。特定のアンチウイルスまたはアンチスパイウェア製品のアンチウイルスとアンチスパイウェアライブラリによってサポートされている機能に応じて、適切な要件が NAC Agent に送信され、ポスチャ検証中にクライアント上でそれらの存在、および特定のアンチウイルスおよびアンチスパイウェア製品のステータスが検証されます。

アンチウイルスとアンチスパイウェア サポート表は、[Cisco.com](https://www.cisco.com) で参照できます。

コンプライアンス モジュール

コンプライアンス モジュールには、ベンダー名、製品バージョン、製品名、および Cisco ISE のポスチャ条件をサポートする OPSWAT が提供する属性などのフィールドのリストが含まれています。

ベンダーは頻繁に製品バージョンや定義ファイルの日付を更新するので、頻繁にアップデートのコンプライアンスモジュールをポーリングすることで、各ベンダーの製品の最新バージョンおよび定義ファイルの日付を調べる必要があります。新しいベンダー、製品、およびリリースのサポートを反映してコンプライアンス モジュールが更新されるたびに、AnyConnect のエージェントは新しいライブラリを受信します。これは、AnyConnect のエージェントがより新しい追加機能をサポートするのに役立ちます。AnyConnect のエージェントがこのサポート情報を取得すると、定期的に更新される `se-checks.xml` ファイル (`se-templates.tar.gz` アーカイブで `se-rules.xml` ファイルとともに公開される) で最新の定義情報をチェックし、クライアントがポスチャポリシーに準拠しているかどうかを決定します。特定のアンチウイルス、アンチスパイウェア、マルウェア対策、ディスク暗号化またはパッチ管理製品のライブラリによってサポートされている機能に応じて、適切な要件が AnyConnect エージェントに送信され、ポスチャ検証中にクライアント上でそれらの存在、およびクライアントでの特定の製品のステータスが検証されます。

コンプライアンス モジュールは、[Cisco.com](https://www.cisco.com) で入手可能です。

ISE ポスチャ ポリシーをサポートするまたはしない OPSWAT API バージョンを次に示します。バージョン 3 および 4 をサポートするエージェントごとに異なるポリシールールがあります。

ポスチャ条件	コンプライアンス モジュールのバージョン
OPSWAT	
アンチウイルス	3.x 以前
スパイウェア対策	3.x 以前
マルウェア対策	4.x 以降
ディスク暗号化	3.x 以前および 4.x 以降
パッチ管理	3.x 以前および 4.x 以降

ポスチャ条件	コンプライアンス モジュールのバージョン
USB	4.x 以降
非 OPSWAT	
ファイル (File)	すべてのバージョン
Application	すべてのバージョン
複合	すべてのバージョン
レジストリ	すべてのバージョン
サービス	すべてのバージョン



(注) 上記のバージョンのいずれかがインストールされた可能性のあるクライアントを予測して、バージョン 3.x 以前およびバージョン 4.x 以降用に別個のポスチャ ポリシーを作成する必要があります。



(注) OESIS バージョン 4 のサポートはコンプライアンス モジュール 4.x および Cisco AnyConnect 4.3 以降に提供されます。しかし、AnyConnect 4.3 は OESIS バージョン 3 とバージョン 4 のポリシーの両方をサポートします。



(注) バージョン 4 コンプライアンス モジュールは、ISE 2.1 以降でサポートされています。

複合ポスチャ条件の作成

ポスチャ評価と検証のポスチャ ポリシーで使用できる複合条件を作成できます。

始める前に

次のタスクを実行するには、スーパー管理者またはポリシー管理者である必要があります。

ステップ 1 [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [条件 (Conditions)] > [ポスチャ (Posture)] > [複合条件 (Compound Conditions)] > [追加 (Add)] を選択します。

ステップ 2 フィールドに適切な値を入力します。

ステップ 3 条件を検証するために [式の確認 (Validate Expression)] をクリックします。

ステップ 4 [送信 (Submit)] をクリックします。

関連トピック

[ポスチャ条件](#) (663 ページ)

[単純ポスチャ条件](#) (664 ページ)

[複合ポスチャ条件](#) (665 ページ)

[Windows クライアントでの自動アップデートを有効にするためのシスコ事前定義の条件](#)
(665 ページ)

[シスコ事前設定済みアンチウイルスおよびアンチスパイウェア条件](#) (665 ページ)

パッチ管理条件の作成

選択したベンダーのパッチ管理製品のステータスを確認するポリシーを作成できます。

たとえば、Microsoft System Center Configuration Manager (SCCM)、クライアントバージョン 4.x ソフトウェア製品がエンドポイントにインストールされているかどうかを確認する条件を作成できます。



(注) Cisco ISE および AnyConnect のサポート対象バージョンは次のとおりです。

- Cisco ISE バージョン 1.4 以降
 - AnyConnect バージョン 4.1 以降
-

始める前に

次のタスクを実行するには、スーパー管理者またはポリシー管理者である必要があります。

ステップ 1 [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [条件 (Conditions)] > [ポスチャ (Posture)] > [パッチ管理条件 (Patch Management Condition)] を選択します。

ステップ 2 [追加 (Add)] をクリックします。

ステップ 3 [パッチ管理条件 (Patch Management Condition)] ページで、フィールドに適切な値を入力します。

ステップ 4 [送信 (Submit)] をクリックします。

関連トピック

[パッチ管理条件の設定](#) (1395 ページ)

[パッチ管理修復の追加](#) (953 ページ)

ディスク暗号化条件の作成

エンドポイントが指定されたデータ暗号化ソフトウェアに準拠しているかどうかを確認するポリシーを作成できます。

たとえば、C: ドライブがエンドポイントで暗号化されているかどうかを確認する条件を作成できます。C: ドライブが暗号化されていない場合、エンドポイントはコンプライアンス違反通知を受信し、ISE はメッセージをログに記録します。

始める前に

次のタスクを実行するには、スーパー管理者またはポリシー管理者である必要があります。AnyConnect ISE ポスチャ エージェントを使用している場合にのみ、ポスチャ要件とディスク暗号化条件を関連付けることができます。

-
- ステップ 1** [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [条件 (Conditions)] > [ポスチャ (Posture)] > [ディスク暗号化条件 (Disk Encryption Condition)] を選択します。
- ステップ 2** [追加 (Add)] をクリックします。
- ステップ 3** [ディスク暗号化条件 (Disk Encryption Condition)] ページで、フィールドに適切な値を入力します。
- ステップ 4** [送信 (Submit)] をクリックします。
-

ポスチャ ポリシーの設定

ポスチャ ポリシーは 1 つ以上の ID グループおよびオペレーティングシステムに関連付けられたポスチャ要件の集合です。ディクショナリ属性は、クライアントの異なるポリシーを定義できる、ID グループおよびオペレーティングシステムと組み合わせられたオプションの条件です。

詳細については、[Cisco ISE 構成ガイドの「ポスチャ サービス」](#)を参照してください。

ポスチャ ポリシーを設定するには、次の手順を実行します。

始める前に

- AUP について理解している必要があります。
- 定期的再評価 (PRA) について理解している必要があります。

-
- ステップ 1** [ポリシー (Policy)] > [ポスチャ (Posture)] または を選択します。
- ステップ 2** [ルールステータス (Rule Status)] ドロップダウンリストで [有効 (Enabled)] または [無効 (Disabled)] を選択します。
- ステップ 3** [ルール名 (Rule Name)] フィールドに、ポリシーの名前を入力します。

(注) 予期しない結果を回避するためのベストプラクティスは、各要件でポスチャ ポリシーを個別のルールとして設定することです。

ステップ 4 [IDグループ (Identity Groups)] 列から必要な ID グループを選択します。

エンドポイント ID グループに基づいてポスチャ ポリシーを作成するには、[IDグループ (Identity Groups)] 列から [エンドポイント ID グループ (Endpoint Identity Groups)] を選択します。

ステップ 5 [オペレーティングシステム (Operating Systems)] 列からオペレーティング システムを選択します。

ステップ 6 [準拠モジュール (Compliance Module)] 列から必要な準拠モジュールを選択します。

- 4.x 以降 (4.x or Later) : マルウェア対策、ディスク暗号化、Patch Management、および USB の各種条件をサポートします。
- 3.x 以前 (3.x or Earlier) : ウイルス対策、スパイウェア対策、ディスク暗号化、および Patch Management の各種条件をサポートします
- すべてのバージョン (Any Version) : ファイル、サービス、レジストリ、アプリケーション、および複合の各種条件をサポートします。

ステップ 7 [ポスチャタイプ (Posture Type)] 列から、[ステルスモード (Stealth Mode)] を選択します。

- [標準 (Standard)] : AnyConnect エージェントを展開し、クライアントとのやりとりが必要な Cisco ISE ポリシーを監視し、適用します。
- [クライアントレス (Clientless)] : AnyConnect エージェントを展開し、クライアントとやりとりしない Cisco ISE ポスチャ ポリシーを監視し、適用します。

ステップ 8 [その他の条件 (Other Conditions)] では、1 つ以上のディクショナリ属性を追加し、単純条件または複合条件としてディクショナリに保存できます。

(注) [ポスチャ ポリシー (Posture Policy)] ページで作成したディクショナリ単純条件とディクショナリ複合条件は、許可ポリシーを設定するときには表示されません。

ステップ 9 [要件 (Requirements)] フィールドに要件を指定します。

ステップ 10 [保存 (Save)] をクリックします。

関連トピック

[クライアントのポスチャ要件の作成](#) (959 ページ)

[定期的再評価の設定](#) (939 ページ)

ポスチャ評価オプション

次の表に、Windows および Macintosh の ISE Posture Agent、および Windows の Web Agent でサポートされるポスチャ評価 (ポスチャ条件) オプションのリストを示します。

表 56: ポスチャ評価オプション

Windows 用 ISE ポスチャ エージェント	Windows 用 Web エージェント	Macintosh OS X 用 ISE ポスチャ エージェント
オペレーティング システム/ サービスパック/ホットフィックス	オペレーティング システム/ サービスパック/ホットフィックス	—
サービス チェック	サービス チェック	サービス チェック (AC 4.1 および ISE 1.4)
レジストリ チェック	レジストリ チェック	—
ファイル チェック	ファイル チェック	ファイル チェック (AC 4.1 および ISE 1.4)
アプリケーション チェック	アプリケーション チェック	アプリケーション チェック (AC 4.1 および ISE 1.4)
アンチウイルスのインストール	アンチウイルスのインストール	アンチウイルスのインストール
アンチウイルスバージョン/アンチウイルス定義日	アンチウイルスバージョン/アンチウイルス定義日	アンチウイルスバージョン/アンチウイルス定義日
アンチスパイウェアのインストール	アンチスパイウェアのインストール	アンチスパイウェアのインストール
アンチスパイウェア バージョン/アンチスパイウェア定義日	アンチスパイウェア バージョン/アンチスパイウェア定義日	アンチスパイウェア バージョン/アンチスパイウェア定義日
パッチ管理チェック (AC 4.1 および ISE 1.4)	—	パッチ管理チェック (AC 4.1 および ISE 1.4)
実行中の Windows Update	実行中の Windows Update	—
Windows Update の設定	Windows Update の設定	—
WSUS のコンプライアンス設定	WSUS のコンプライアンス設定	—

ポスチャ修復オプション

次の表に、Windows および Macintosh の ISE Posture Agent、および Windows の Web Agent でサポートされる修復オプション（ポスチャ条件）のリストを示します。

表 57: ポスチャ修復オプション

ISE ポスチャ エージェント Windows	Web Agent Windows	ISE ポスチャ エージェント Macintosh OS X
メッセージテキスト（ローカル チェック）	メッセージテキスト（ローカル チェック）	メッセージテキスト（ローカル チェック）
URL リンク（リンク分散）	URL リンク（リンク分散）	URL リンク（リンク分散）
ファイル配布	ファイル配布	—
プログラム起動	—	—
アンチウイルス定義更新	—	アンチウイルス ライブ更新
アンチスパイウェア定義更新	—	アンチスパイウェア ライブ更新
パッチ管理修復（AC 4.1 および ISE 1.4）	—	—
Windows Update	—	—
WSUS	—	—

[ISE Community Resource](#)
[Cisco ISE and SCCM integration Reference Guide](#)

ポスチャのカスタム条件

ポスチャ条件は次の単純条件のいずれかになります。ファイル、レジストリ、アプリケーション、サービス、またはディクショナリ条件。これらの単純条件のうちの1つ以上の条件によって複合条件が形成され、複合条件はポスチャ要件と関連付けることができます。

最初のポスチャ更新の後に、Cisco ISE もシスコ定義の単純条件と複合条件を作成します。シスコ定義の単純条件では **pc_as** が使用され、複合条件では **pr_as** が使用されます。

ユーザ定義の条件またはシスコ定義の条件には、単純条件と複合条件の両方が含まれます。

ポスチャサービスは、アンチウイルスおよびアンチスパイウェア（AV/AS）複合条件に基づいた内部チェックを使用します。このため、ポスチャ レポートは、作成した正確な AV/AS 複合条件名を反映しません。レポートには、AV/AS 複合条件の内部チェックの名前だけが表示されます。

たとえば、任意のベンダーおよび製品をチェックする「MyCondition_AV_Check」という名前の AV 複合条件を作成した場合、ポスチャ レポートには、条件名として、「MyCondition_AV_Check」ではなく、内部チェック「av_def_ANY」が表示されます。

カスタム ポスチャ修復アクション

カスタム ポスチャ修復アクションは、ファイル、リンク、アンチウイルスまたはアンチスパイウェア定義の更新、プログラムの起動、Windows Update、Windows Server Update Services (WSUS) の修復タイプです。

関連トピック

- [ファイル修復の追加](#) (952 ページ)
- [リンク修復の追加](#) (952 ページ)
- [アンチウイルス修復の追加](#) (953 ページ)
- [アンチスパイウェア修復の追加](#) (954 ページ)
- [プログラム修復起動の追加](#) (954 ページ)
- [Windows Update 修復の追加](#) (956 ページ)
- [Windows Server Update Services 修復の追加](#) (956 ページ)
- [パッチ管理修復の追加](#) (953 ページ)

ファイル修復の追加

ファイル修復により、クライアントはコンプライアンスに必要なファイルのバージョンをダウンロードできます。クライアントエージェントは、コンプライアンスのためにクライアントが必要とするファイルを使用してエンドポイントを修復します。

[ファイル修復 (File Remediations)] ページでファイル修復をフィルタリング、表示、追加、または削除することはできますが、ファイル修復を編集することはできません。[ファイル修復 (File Remediations)] ページには、すべてのファイル修復がそれらの名前と説明、および修復に必要なファイルとともに表示されます。

ステップ 1 [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] > [ポスチャ (Posture)] を選択します。

ステップ 2 [修復アクション (Remediation Actions)] をクリックします。

ステップ 3 [ファイル修復 (File Remediation)] をクリックします。

ステップ 4 [追加 (Add)] をクリックします。

ステップ 5 [新規ファイル修復 (New File Remediation)] ページで値を入力します。

ステップ 6 [送信 (Submit)] をクリックします。

リンク修復の追加

リンク修復により、クライアントは修復ページまたはリソースにアクセスするための URL をクリックできます。クライアントエージェントはリンクを使用してブラウザを開き、クライアントはコンプライアンスのために自身を修復できます。

[リンク修復 (Link Remediation)] ページには、すべてのリンク修復がそれらの名前と説明、および修復のモードとともに表示されます。

-
- ステップ 1 [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] > [ポスチャ (Posture)] を選択します。
 - ステップ 2 [修復アクション (Remediation Actions)] をクリックします。
 - ステップ 3 [リンク修復 (Link Remediation)] をクリックします。
 - ステップ 4 [追加 (Add)] をクリックします。
 - ステップ 5 [新規リンク修復 (New Link Remediation)] ページで値を変更します。
 - ステップ 6 [送信 (Submit)] をクリックします。
-

パッチ管理修復の追加

パッチ管理修復を作成して、修復後にコンプライアンスのために最新のファイル定義でクライアントを更新できます。

[パッチ管理修復 (Patch Management Remediation)] ページには、修復タイプ、パッチ管理ベンダーの名前、およびさまざまな修復オプションが表示されます。

-
- ステップ 1 [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] > [ポスチャ (Posture)] を選択します。
 - ステップ 2 [修復アクション (Remediation Actions)] をクリックします。
 - ステップ 3 [パッチ管理修復 (Patch Management Remediation)] をクリックします。
 - ステップ 4 [追加 (Add)] をクリックします。
 - ステップ 5 [パッチ管理修復 (Patch Management Remediation)] ページで値を変更します。
 - ステップ 6 [送信 (Submit)] をクリックして、[パッチ管理修復 (Patch Management Remediation)] ページに修復アクションを追加します。
-

関連トピック

[パッチ管理修復](#) (1445 ページ)

アンチウイルス修復の追加

アンチウイルス修復を作成して、修復後にコンプライアンスのために最新のファイル定義でクライアントを更新できます。

[AV 修復 (AV Remediations)] ページには、すべてのアンチウイルス修復がそれらの名前と説明、および修復のモードとともに表示されます。

-
- ステップ 1 [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] > [ポスチャ (Posture)] を選択します。
 - ステップ 2 [修復アクション (Remediation Actions)] をクリックします。
 - ステップ 3 [AV 修復 (AV Remediation)] をクリックします。
 - ステップ 4 [追加 (Add)] をクリックします。
 - ステップ 5 [新規 AV 修復 (New AV Remediation)] ページで値を変更します。
 - ステップ 6 [送信 (Submit)] をクリックします。
-

アンチスパイウェア修復の追加

アンチスパイウェア修復を作成して、修復後にコンプライアンスのために最新のファイル定義でクライアントを更新できます。

[AS 修復 (AS Remediations)] ページには、すべてのアンチウイルス修復がそれらの名前と説明、および修復のモードとともに表示されます。

-
- ステップ 1 [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] > [ポスチャ (Posture)] を選択します。
 - ステップ 2 [修復アクション (Remediation Actions)] をクリックします。
 - ステップ 3 [AS 修復 (AS Remediations)] をクリックします。
 - ステップ 4 [追加 (Add)] をクリックします。
 - ステップ 5 [新規 AS 修復 (New AS Remediations)] ページで値を変更します。
 - ステップ 6 [送信 (Submit)] をクリックします。
-

関連トピック

[アンチスパイウェア修復](#) (1437 ページ)

プログラム修復起動の追加

コンプライアンスのために、クライアントエージェントが1つ以上のアプリケーションを起動してクライアントを修復するプログラム修復起動を作成できます。

[プログラム修復起動 (Launch Program Remediations)] ページには、すべてのプログラム修復起動がそれらの名前と説明、および修復のモードとともに表示されます。

-
- ステップ 1 [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] > [ポスチャ (Posture)] を選択します。
 - ステップ 2 [修復アクション (Remediation Actions)] をクリックします。

- ステップ 3 [プログラム起動修復 (Launch Program Remediation)] をクリックします。
- ステップ 4 [追加 (Add)] をクリックします。
- ステップ 5 [新規プログラム修復起動 (New Launch Program Remediation)] ページで値を変更します。
- ステップ 6 [送信 (Submit)] をクリックします。

プログラム修復起動のトラブルシューティング

問題

プログラム修復起動を使用して、アプリケーションを修復として起動すると、アプリケーションは正常に開始されます (Windows Task Manager で観察されます) が、アプリケーション UI は表示されません。

ソリューション

プログラム起動 UI アプリケーションはシステム権限で実行され、[インタラクティブサービス検出 (ISD) (Interactive Service Detection (ISD))] ウィンドウに表示されます。プログラム起動 UI アプリケーションを表示するには、次の OS で ISD をイネーブルにする必要があります。

- Windows Vista : ISD はデフォルトで停止状態になっています。services.msc で ISD サービスを起動して、ISD をイネーブルにします。
- Windows 7 : ISD サービスはデフォルトでイネーブルになっています。
- Windows 8/8.1 : レジストリ \HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Windows で「NoInteractiveServices」を 1 から 0 に変更することで ISD をイネーブルにします。

Windows Update 修復

Windows Update 修復により、セキュリティ ポリシーに従って Windows クライアントで自動更新設定がオンになるようにします。Windows 管理者は、Windows クライアントで自動更新をオンまたはオフにできます。Microsoft Windows では、この機能を使用して、更新の有無を定期的に確認します。自動更新機能がオンになっていると、Windows は他の更新を行う前に、Windows 推奨の更新プログラムを自動的に更新します。

Windows 自動更新設定は、Windows オペレーティング システムによって異なります。

たとえば、Windows XP は自動更新を設定するために次の設定を提供しています。

- [自動 (Automatic)] (推奨) : Windows は、クライアントが推奨の Windows Update を自動的にダウンロードしてインストールすることを許可します。
- [更新を自動的にダウンロードするが、インストールは手動で実行する (Download updates for me, but let me choose when to install them)] : Windows がクライアントの更新プログラムをダウンロードしますが、更新プログラムをいつインストールするかはクライアントが選択できます。

- [更新を通知するのみで、自動的なダウンロードまたはインストールを実行しない (Notify me but don't automatically download or install them)] : Windows はクライアントに通知するのみで、更新プログラムを自動的にダウンロードまたはインストールしません。
- [自動更新を無効にする (Turn off Automatic Updates)] : Windows は、クライアントが Windows 自動更新機能をオフにすることを許可します。ここで、クライアントは Windows Update Web サイト リンクから更新プログラムを定期的にインストールしないと脆弱になります。

Windows Update サービス (wuaserv) が任意の Windows クライアントで開始または停止されているかどうかを、**pr_AutoUpdateCheck_Rule** を使用して確認できます。これは、ポスチャ要件を作成するために使用できる事前定義されたシスコのルールです。ポスチャ要件が失敗した場合、要件に関連付けた Windows Update 修復は、Windows クライアントに自動更新のオプションの 1 つを使用して修復するように強制します。

Windows Update 修復の追加

[Windows Update 修復 (Windows update remediations)] ページには、すべての Windows Update 修復がそれらの名前と説明、および修復のモードとともに表示されます。

-
- ステップ 1 [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] > > [ポスチャ (Posture)] を選択します。
- ステップ 2 [修復アクション (Remediation Actions)] をクリックします。
- ステップ 3 [Windows Update 修復 (Windows Update Remediation)] をクリックします。
- ステップ 4 [追加 (Add)] をクリックします。
- ステップ 5 [新規 Windows Update 修復 (New Windows Update Remediation)] ページで値を変更します。
- ステップ 6 [送信 (Submit)] をクリックします。
-

Windows Server Update Services 修復の追加

コンプライアンスのためにローカルに管理されているか、または Microsoft で管理されている WSUS サーバから最新の WSUS 更新を受信するように Windows クライアントを設定できます。Windows Server Update Services (WSUS) 修復は、ローカルに管理されている WSUS サーバまたは Microsoft で管理されている WSUS サーバから最新の Windows サービス パック、ホットフィックス、およびパッチをインストールします。

クライアント エージェントをローカルの WSUS Agent と統合して、エンドポイントの WSUS 更新が最新かどうかをチェックする WSUS 修復を作成できます。

-
- ステップ 1 [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] > [ポスチャ (Posture)] を選択します。

ステップ2 [修復アクション (Remediation Actions)] をクリックします。

ステップ3 [Windows Server Update Service 修復 (Windows Server Update Services Remediation)] をクリックします。

ステップ4 [追加 (Add)] をクリックします。

ステップ5 [新規 Windows Server Update Service 修復 (New Windows Server Update Services Remediation)] ページで値を変更します。

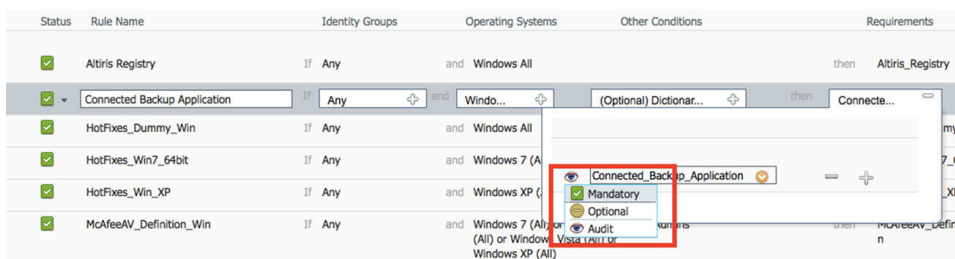
ステップ6 [送信 (Submit)] をクリックします。

ポスチャ評価要件

ポスチャ要件は、ロールおよびオペレーティングシステムとリンクできる修復アクションを伴う一連の複合条件です。ネットワークに接続しているすべてのクライアントは、ネットワークで適合ホストになるためにはポスチャ評価中に必須要件を満たす必要があります。

ポスチャ ポリシー要件は、ポスチャ ポリシーの必須、オプション、または監査タイプに設定できます。要件がオプションで、クライアントがこれらの要件を満たさない場合、クライアントにはエンドポイントのポスチャ評価中に続行するオプションがあります。

図 52: ポスチャ ポリシーの要件タイプ



必須要件

ポリシーの評価時に、エージェントはポスチャポリシーに定義されている必須要件を満たすことができないクライアントに修復オプションを提供します。エンドユーザは、修復タイマー設定で指定された時間内に要件を満たすように修復する必要があります。

たとえば、絶対パス内に C:\temp\text.file があるかをチェックするために、ユーザ定義の条件を含む必須要件を指定したとします。ファイルがない場合、必須要件は失敗し、ユーザは [非準拠 (Non-Compliant)] 状態になります。

オプション要件

ポリシーの評価時に、クライアントがポスチャポリシーに指定されたオプション要件を満たすことができない場合に、エージェントは続行するためのオプションをクライアントに提供します。エンドユーザは、指定されたオプション要件をスキップすることができます。

たとえば、Calc.exe などのクライアントマシンで実行するアプリケーションをチェックするために、ユーザ定義の条件を含むオプション要件を指定したとします。クライアントが条件を満

たすことができない場合、オプション要件がスキップされ、エンドユーザが[準拠 (Compliant)] 状態になるように、さらに続行するためのオプションがエージェントによって促されます。

監査要件

監査要件は内部用に指定され、エージェントはポリシー評価時の合格または失敗のステータスに関係なく、メッセージやエンドユーザからの入力を促しません。

たとえば、エンドユーザにアンチウイルスプログラムの最新バージョンがあるかどうかを確認するために、必須のポリシー条件を作成中だとします。ポリシー条件として実際に適用する前に非準拠のエンドユーザを見つける場合は、その条件を監査要件として指定できます。

可視性要件

ポリシー評価の間に、エージェントが可視性要件のコンプライアンス データを 5 ～ 10 分ごとにレポートします。

関連トピック

[ステルス モードの展開](#) (961 ページ)

[ポスチャ ポリシーと要件タイプへのステルス モードの影響](#) (962 ページ)

[AnyConnect クライアントレス モード ワークフロー](#) (965 ページ)

非準拠状態でスタックしたクライアント システム

クライアント マシンが必須要件を修復できない場合、ポスチャ ステータスは「非準拠」に変更され、エージェント セッションは隔離されます。クライアント マシンを「非準拠」状態から移行するには、エージェントがクライアントマシン上でポスチャ評価を再び開始するようにポスチャ セッションを再起動する必要があります。次のようにポスチャ セッションを再起動できます。

- 802.1X 環境での有線およびワイヤレス許可変更 (CoA) :
 - [新しい許可プロファイル (New Authorization Profiles)] ページで新しい許可プロファイルを作成するときに、特定の許可ポリシーの再認証タイマーを設定できます。詳細については、20-11 ページの「ダウンロード可能 ACL の権限の設定」の項を参照してください。
 - 有線ユーザは、ネットワークの接続を切断して再接続すると、隔離状態から移行できます。ワイヤレス環境では、ユーザは、ワイヤレス LAN コントローラ (WLC) から切断し、ユーザのアイドルタイムアウト時間が過ぎるまで待機してから、ネットワークへの再接続を試行する必要があります。
- VPN 環境 : VPN トンネルを切断し、再接続します。

クライアントのポスチャ要件の作成

[要件 (Requirements)] ページでは、ユーザ定義の条件とシスコ定義の条件、および修復アクションを関連付けて要件を作成できます。[要件 (Requirements)] ページで作成および保存されたユーザ定義の条件および修復アクションは、それぞれのリスト ページに表示されます。

始める前に

- ポスチャの利用規定 (AUP) について理解している必要があります。

ステップ 1 [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] > [ポスチャ (Posture)] > [要件 (Requirements)] を選択します。

ステップ 2 [要件 (Requirements)] ページに値を入力します。

ステップ 3 読み取り専用モードでポスチャ要件を保存するには、[完了 (Done)] をクリックします。

ステップ 4 [保存 (Save)] をクリックします。

関連トピック

[非準拠状態でスタックしたクライアント システム \(958 ページ\)](#)

[ポスチャ評価要件 \(957 ページ\)](#)

ポスチャのカスタム権限

カスタム権限は、Cisco ISE で定義する標準許可プロファイルです。標準許可プロファイルは、エンドポイントの一致するコンプライアンス ステータスに基づいてアクセス権を設定します。ポスチャ サービスでは、ポスチャは大きく不明プロファイル、準拠プロファイル、および非準拠プロファイルに分類されます。ポスチャ ポリシーおよびポスチャ要件によって、エンドポイントのコンプライアンス ステータスが決まります。

VLAN、DACL および他の属性値ペアの異なるセットを持つことができるエンドポイントの不明、準拠、および非準拠のポスチャ ステータスに対して 3 つの異なる許可プロファイルを作成する必要があります。これらのプロファイルは、3 つの異なる許可ポリシーに関連付けることができます。これらの許可ポリシーを区別するために、Session:PostureStatus 属性を他の条件とともに使用できます。

不明プロファイル

エンドポイントに一致するポスチャ ポリシーが定義されていない場合、そのエンドポイントのポスチャ コンプライアンス ステータスは不明に設定されることがあります。不明のポスチャ コンプライアンス ステータスは、一致するポスチャ ポリシーが有効であるが、エンドポイントに対してポスチャ評価がまだ行われておらず、従ってクライアント エージェントによってコンプライアンス レポートが提供されていないエンドポイントにも適用できます。

準拠プロファイル

エンドポイントに一致するポストチャポリシーが定義されている場合、そのエンドポイントのポストチャコンプライアンスステータスは準拠に設定されます。ポストチャ評価が行われると、エンドポイントは、一致するポストチャポリシー内に定義されているすべての必須要件を満たします。準拠とポストチャされているエンドポイントには、ネットワークに対する特権ネットワークアクセスを付与できます。

非準拠プロファイル

エンドポイントのポストチャコンプライアンスステータスが非準拠に設定されるのは、そのエンドポイントに対して一致するポストチャポリシーが定義されているが、ポストチャ評価の実行中にすべての必須要件を満たすことができない場合です。非準拠としてポストチャされたエンドポイントは、修復アクションを含むポストチャ要件に一致し、自らを修復するために修復リソースへ制限付きのネットワークアクセスが付与される必要があります。

関連トピック

[標準許可ポリシーの設定](#) (960 ページ)

標準許可ポリシーの設定

[許可ポリシー (Authorization Policy)] ページでは、標準許可ポリシーと例外許可ポリシーの2種類の許可ポリシーを定義できます。ポストチャに固有の標準許可ポリシーは、エンドポイントのコンプライアンスステータスに基づいて、ポリシー決定を行うために使用されます。

ステップ 1 [ポリシー (Policy)] > [許可 (Authorization)] を選択します。

ステップ 2 [許可ポリシー (Authorization Policy)] ページの上部に表示されるドロップダウンリストから適用する照合ルールタイプを1つ選択します。

- [最初に一致したルールの適用 (First Matched Rules Apply)] : このオプションでは、評価中に標準許可ポリシーのリストで最初に一致した単一の許可ポリシーを使用して、アクセス権限が設定されます。最初の一致許可ポリシーが見つかり、残りの標準許可ポリシーは評価されません。
- [複数の一致するルールの適用 (Multiple Matched Rule Applies)] : このオプションでは、評価中にすべての標準許可ポリシーのリストで一致した服すの許可ポリシーを使用して、アクセス権限が設定されます。

ステップ 3 デフォルトの標準許可ポリシー行の [編集 (Edit)] の横の下矢印をクリックします。

ステップ 4 [新規ルールを上挿入 (Insert New Rule Above)] をクリックします。

ステップ 5 ルール名を入力し、ID グループおよびその他の条件を選択し、デフォルトの標準許可ポリシー行の上に表示される新しい許可ポリシー行に許可プロファイルを関連付けます。

ステップ 6 読み取り専用モードで新しい標準許可ポリシーを作成するには、[完了 (Done)] をクリックします。

ステップ 7 [保存 (Save)] をクリックします。

ステルス モードの展開

Cisco ISE ポスチャ ポリシーをモニタおよび適用するため、AnyConnect エージェントをステルス モードで展開できます。このモードでは、ユーザとのやりとりを行わずにポスチャをサービスとして実行できるため、ステルス モードと呼ばれます。ステルス モードには標準とクライアントレスの 2 種類があります。

標準モードでは、AnyConnect エージェントを展開し、クライアントとのやりとりを必要とする Cisco ISE ポスチャ ポリシーをモニタおよび適用します。

クライアントレスモードでは、ユーザとのやりとりを行わずに、ポスチャをサービスとして実行できます。[クライアントプロビジョニング (Client Provisioning)] ページ ([ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] > [クライアントプロビジョニング (Client Provisioning)] > [リソース (Resources)]) と [ポスチャ要件 (Posture Requirements)] ページ ([ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] > [ポスチャ (Posture)] > [要件 (Requirements)]) に、標準モードとクライアントレスモードが含まれます。推奨されるベストプラクティスは、[クライアントプロビジョニング (Client Provisioning)] ページでポスチャプロファイルをプロビジョニングすることです。

ポスチャ要件でクライアントレスモードを選択すると、一部の条件、修復、または条件内の属性が無効になります (灰色表示)。たとえば、手動修復ではクライアント側のやりとりが必要となるため、クライアントレス モード要件を有効にすると、[手動修復タイプ (Manual Remediation Type)] が無効になります (灰色表示)。

クライアントレス モードの展開で、ポスチャプロファイルを AnyConnect 設定にマッピングし、Anyconnect 設定を [クライアントプロビジョニング (Client Provisioning)] ページにマッピングする場合、次の処理がサポートされます。

- AnyConnect によるポスチャプロファイルの読み取りと必要なモードの設定
- 初回ポスチャ要求における AnyConnect による選択したモードに関する情報の Cisco ISE への送信
- Cisco ISE によるモードおよびその他の要因 (ID グループ、OS、コンプライアンスモジュールなど) に基づく正しいポリシーの照合。



(注) AnyConnect バージョン 4.4 以降では、クライアントレス モードでの Cisco ISE ポスチャがサポートされています。

関連トピック

[ポスチャ評価要件 \(957 ページ\)](#)

[ポスチャ ポリシーと要件タイプへのステルス モードの影響 \(962 ページ\)](#)

[ポスチャとネットワーク ドライブ マッピングのベスト プラクティス \(965 ページ\)](#)

ポスチャポリシーと要件タイプへのステルスモードの影響

[ワーク センター (Work Centers)] > [ポスチャ (Posture)] > [ポスチャ ポリシー (Posture Policy)] ページでのステルス モードの影響は次のとおりです。

- ポスチャ ポリシーで [クライアントレス (Clientless)] を選択し、インラインの新規要件を作成すると、[オペレーティングシステム (Operating Systems)]、[コンプライアンス モジュール (Compliance Module)]、および [標準/クライアントレス モード (Standard/Clientless Mode)] が読み取り専用フィールドとして表示されます。

図 53: インライン要件

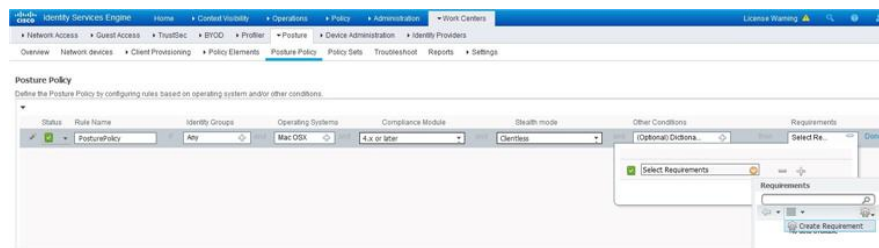
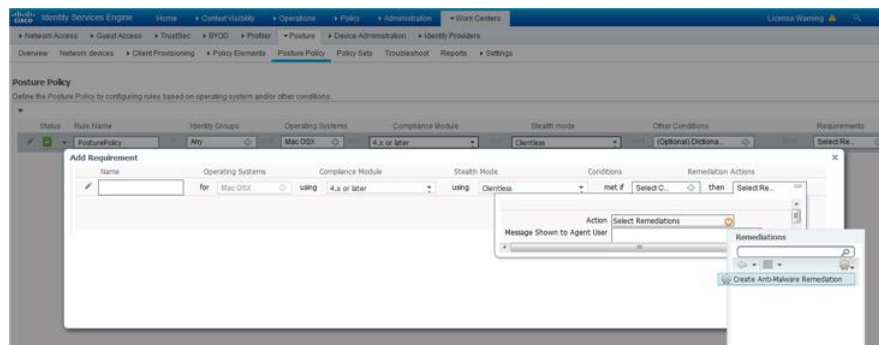
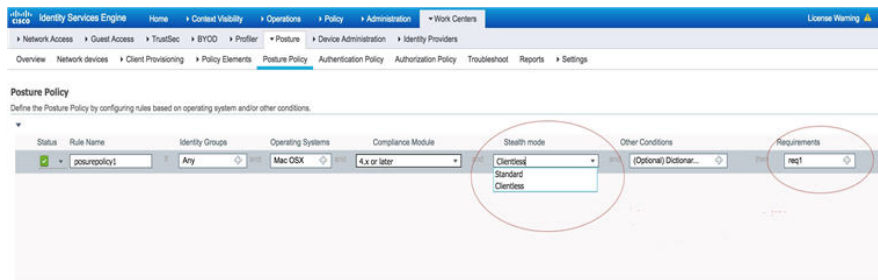


図 54: 読み取り専用フィールド : [オペレーティングシステム (Operating Systems)]、[コンプライアンス モジュール (Compliance Module)]、および [ステルス モード (Stealth Mode)]



- ポスチャ ポリシーでステルス モードの選択を変更すると、選択されている要件がクリアされます。

図 55: 要件に対するステルス モードの影響



[ワーク センター (Work Centers)] > [ポスチャ (Posture)] > [ポリシー要素 (Policy Elements)] > [要件 (Requirements)] ページでのステルス モードの影響は次のとおりです。

- ステルス モードが [クライアントレス (Clientless)] の場合、修復リストで、[修復タイプ (Remediation Type)] が [手動 (Manual)] の修復が除外されます。
- サポートされている修復アクションは、[オペレーティングシステム (Operating Systems)] および [ステルス モード (Stealth Mode)] の選択に基づいてフィルタリングされます。
- 修復アクションは、[カテゴリ別プロビジョニング (Provision By Category)] または [すべてによるプロビジョニング (Provision By Everything)] オプションを使用して設定されたアプリケーション条件には適用されません。

[ワーク センター (Work Centers)] > [ポスチャ (Posture)] > [ポリシー要素 (Policy Elements)] > [修復 (Remediations)] ページでのステルス モードの影響は次のとおりです。

- 修復タイプをポリシー要件に関連付けた場合は、[修復タイプ (Remediation Type)] を [自動 (Automatic)] から [手動 (Manual)] に変更することはできません。
- [インストール ウィザードインターフェイス設定 (Installation Wizard Interface Setting)] を [UI なし (No UI)] から [UI を表示 (Show UI)] に切り替えることはできません。

図 56: 修復タイプとインストール ウィザード インターフェイス 設定

Windows Server Update Services Remediations List > New Windows Server Update Services Remediation

Windows Server Update Services Remediation

* Name: Win_Ser_Update_Services_Rem ⓘ

Description:

Compliance Module: Any version

Remediation Type: **Automatic** (dropdown menu with options: Automatic, Manual)

Interval: (in secs) (Valid Range 0 to 9999)

Retry Count: (Valid Range 0 to 99)

Validate Windows updates using: ☒ Cisco Rules ☐ Severity Level

Windows Updates Severity Level: **Critical** (dropdown menu)

☐ Update to latest OS Service Pack

Windows Updates Installation Source: ☒ Microsoft Server ☐ Managed Server

Installation Wizard Interface Setting: ☐ Show UI ☒ No UI

ステルス モードでは次の修復を設定できます。

- マルウェア対策修復の作成
- プログラム修復起動の作成
- パッチ管理修復の作成
- USB 修復の作成
- Windows Server Update Services 修復の作成
- Windows Update 修復の作成

ステルス モードでは次の修復は設定できません。

- 手動修復
- リンク修復
- ファイル修復
- Windows Server Update Services (WSUS) 修復（「修復タイプとインストール ウィザード インターフェイス 設定」の図を参照）
- パッチ管理修復：パッチ管理ソフトウェア GUI をアクティブにします（修復オプション）。
- AUP ポリシー

ポスチャとネットワーク ドライブ マッピングのベスト プラクティス

Windows エンドポイントのポスチャ アセスメント実行中に、エンドポイント ユーザがデスクトップへのアクセスするときに遅延が生じることがあります。これは、Windows でユーザがデスクトップにアクセスできるようにする前に、ファイルサーバのドライブ文字のマッピングを復元しようとするのが原因で発生する場合があります。ポスチャ実行中の遅延を防ぐためのベスト プラクティスを次に示します。

- ファイル サーバ ドライブ文字をマッピングするときには AD にアクセスする必要があるため、エンドポイントは Active Directory サーバにアクセスする必要があります。
(AnyConnect ISE ポスチャ エージェントを使用した) ポスチャがトリガーされると、AD へのアクセスがブロックされ、これが原因でログインが遅延します。ポスチャが完了する前に、ポスチャ修復 ACL を使用して AD サーバへのアクセスを提供します。
- ポスチャ完了までのログインスクリプトの遅延を設定し、その後 Persistence 属性を NO に設定する必要があります。Windows はログイン中にすべてのネットワーク ドライブへの再接続を試行しますが、AnyConnect ISE ポスチャ エージェントが完全なネットワーク アクセスを得るまでは、この操作を完了できません。

AnyConnect クライアントレス モード ワークフロー

クライアントレスモードでの AnyConnect の設定プロセスには、一連の手順があります。Cisco ISE で次の手順を実行する必要があります。

-
- ステップ 1 [AnyConnect エージェント プロファイルの作成](#)。
 - ステップ 2 [AnyConnect パッケージの AnyConnect 設定の作成](#)。
 - ステップ 3 [Cisco ISE へのオープン DNS プロファイルのアップロード](#)。
 - ステップ 4 [クライアント プロビジョニング ポリシーの作成](#)。
 - ステップ 5 [ポスチャ条件の作成](#)。
 - ステップ 6 [ポスチャ修復の作成](#)。
 - ステップ 7 [クライアントレス モードでのポスチャ要件の作成](#)。
 - ステップ 8 [ポスチャ ポリシーの作成](#)。
-

次のタスク

Anyconnect エージェント プロファイルを作成する必要があります。

AnyConnect エージェント プロファイルの作成

始める前に

Mac および Windows OS 用の AnyConnect Cisco パッケージおよび AnyConnect 準拠モジュールをアップロードする必要があります。

-
- ステップ 1 [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] > [クライアントプロビジョニング (Client Provisioning)] > [リソース (Resources)] ページを選択します。
 - ステップ 2 [追加 (Add)] ドロップダウンリストから、[NAC エージェントまたは AnyConnect ポスチャ プロファイル (NAC Agent or AnyConnect Posture Profile)] を選択します。
 - ステップ 3 [ポスチャ エージェント プロファイルの設定 (Posture Agent Profile Settings)] ドロップダウンリストから [AnyConnect] を選択します。
 - ステップ 4 [名前 (Name)] フィールドに、目的の名前 (たとえば、AC_Agent_Profile) を入力します。
 - ステップ 5 [エージェントの動作 (Agent Behavior)] セクションでは、[ステルス モード (Stealth Mode)] パラメータで [クライアントレス (Clientless)] を選択します。
 - ステップ 6 [保存 (Save)] をクリックします。
-

次のタスク

AnyConnect パッケージの AnyConnect 設定を作成する必要があります。

AnyConnect パッケージの AnyConnect 設定の作成

-
- ステップ 1 [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] > [クライアント プロビジョニング (Client Provisioning)] > [リソース (Resources)] ページに移動します。
 - ステップ 2 [追加 (Add)] ドロップダウンリストから、[AnyConnect 設定 (AnyConnect Configuration)] を選択します。
 - ステップ 3 [AnyConnect パッケージの選択 (Select AnyConnect Package)] ドロップダウンリストから、必要な AnyConnect パッケージを選択します (AnyConnectDesktopWindows 4.4.117.0 など)。
 - ステップ 4 [設定名 (Configuration Name)] テキスト ボックスに、必要な名前を入力します (AC_Win_44117 など)。
 - ステップ 5 [コンプライアンス モジュール (Compliance Module)] ドロップダウンリストで、必要なコンプライアンス モジュールを選択します (AnyConnectComplianceModuleWindows 4.2.437.0 など)。
 - ステップ 6 [AnyConnect モジュール選択 (AnyConnect Module Selection)] セクションで、[ISE ポスチャ (ISE Posture)] と [ネットワーク アクセス マネージャ (Network Access Manager)] のチェック ボックスにマークを付けます。
 - ステップ 7 [プロファイル選択 (Profile Selection)] セクションの [ISE ポスチャ (ISE Posture)] ドロップダウンリストで、AnyConnect エージェント プロファイルを選択します (AC_Agent_Profile など)。

ステップ 8 [ネットワーク アクセス マネージャ (Network Access Manager)] ドロップダウン リストから、必要な AnyConnect エージェント プロファイルを選択します (AC_Agent_Profile など)。

次のタスク

クライアントにプッシュされるオープン DNS プロファイルをアップロードする必要があります。

Cisco ISE へのオープン DNS プロファイルのアップロード

オープン DNS プロファイルがクライアントにプッシュされます。

-
- ステップ 1** [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] > [クライアント プロビジョニング (Client Provisioning)] > [リソース (Resources)] ページに移動します。
 - ステップ 2** [追加 (Add)] ドロップダウン リストから、[ローカルディスクのエージェント リソース (Agent Resources From Local Disk)] を選択します。
 - ステップ 3** [カテゴリ (Category)] ドロップダウン リストから [顧客作成のパッケージ (Customer Created Packages)] を選択します。
 - ステップ 4** [タイプ (Type)] ドロップダウン リストから、[AnyConnect プロファイル (AnyConnect Profile)] を選択します。
 - ステップ 5** [名前 (Name)] テキスト ボックスに、目的の名前 (たとえば、OpenDNS) を入力します。
 - ステップ 6** [参照 (Browse)] をクリックして、ローカル ディスクから JSON ファイルを見つけます。
 - ステップ 7** [送信 (Submit)] をクリックします。
-

次のタスク

クライアント プロビジョニング ポリシーを作成する必要があります。

クライアント プロビジョニング ポリシーの作成

-
- ステップ 1** [ポリシー (Policy)] > [クライアント プロビジョニング (Client Provisioning)] ページに移動します。
 - ステップ 2** 必要なルールを作成します (たとえば、Rule Name=WindowsAll, if Identity Groups=Any and Operating Systems=Windows All and Other Conditions=Conditions, then Results=AC_Win_44117)。
-

次のタスク

ポスチャ条件を作成する必要があります。

ポスチャ条件の作成

-
- ステップ 1** [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [条件 (Conditions)] > [ポスチャ (Posture)] > [ファイル条件 (File Condition)] の順に移動します。
- ステップ 2** 必要な名前を入力します (filechk など)。
- ステップ 3** [オペレーティング システム (Operating Systems)] ドロップダウン リストから、[Windows 7 (すべて) (Windows 7 (All))] を選択します。
- ステップ 4** [ファイル タイプ (File Type)] ドロップダウン リストから、[FileExistence] を選択します。
- ステップ 5** [ファイル パス (File Path)] ドロップダウン リストから、[ABSOLUTE_PATH C:\test.txt] を選択します。
- ステップ 6** [ファイル演算子 (File Operator)] ドロップダウン リストから、[DoesNotExist] を選択します。
-

次のタスク

ポスチャ修復を作成する必要があります。

ポスチャ修復の作成

ファイル条件により、test.txt ファイルがエンドポイントに存在するかどうかを確認されます。存在しない場合の修復は、USB ポートをブロックし、USB デバイスを使用したファイルのインストールを防止することです。

-
- ステップ 1** [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] > [修復アクション (Remediation Actions)] > [USB 修復 (USB Remediations)] ページに移動します。
- ステップ 2** 必要な名前を入力します (clientless_mode_block など)。
- ステップ 3** [送信 (Submit)] をクリックします。
-

次のタスク

ポスチャ要件を作成する必要があります。

クライアントレス モードでのポスチャ要件の作成

[要件 (Requirements)] ページから修復アクションを作成する際は、クライアントレス モードに適した次の修復だけが表示されます: [マルウェア対策 (Anti-Malware)]、[プログラム起動 (Launch Program)]、[パッチ管理 (Patch Management)]、[USB]、[Windows Server Update Services]、および [Windows Update]。

-
- ステップ 1** [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] > [クライアント プロビジョニング (Client Provisioning)] > [リソース (Resources)] ページに移動します。
- ステップ 2** ポスチャの必須要件を作成します (たとえば、Name=win7Req for Operating Systems=Windows7(All) using Compliance Module=4.x or later using Stealth Mode=Clientless met if Condition=filechk then Remediation Actions=clientless_mode_block)。
-

次のタスク

ポスチャ ポリシーを作成する必要があります。

ポスチャ ポリシーの作成

始める前に

ポスチャ ポリシーの要件およびポリシーがクライアントレス モードで作成されていることを確認してください。

-
- ステップ 1** [ポリシー (Policy)] > [ポスチャ (Posture)] を選択します。
- ステップ 2** 必要なルールを作成します。たとえば、Identity Groups=Any and Operating Systems=Windows 7(All) および Compliance Module=4.x or late および Stealth Mode=Clientless の場合、Requirements=win7Req となります。
- (注) URL リダイレクションのないクライアント プロビジョニングの場合、ネットワーク アクセスまたは RADIUS に固有の属性を使用して条件を設定しても条件は機能せず、Cisco ISE サーバで特定ユーザのセッション情報が使用可能ではないことが原因で、クライアント プロビジョニング ポリシーの照合が失敗することがあります。ただし、Cisco ISE では外部で追加された ID グループに対して条件を設定できます。
-



第 27 章

Cisco TrustSec ポリシーの設定

- [TrustSec アーキテクチャ \(971 ページ\)](#)
- [TrustSec ダッシュボード \(975 ページ\)](#)
- [TrustSec のグローバル設定 \(978 ページ\)](#)
- [TrustSec マトリックスの設定 \(979 ページ\)](#)
- [TrustSec デバイスの設定 \(980 ページ\)](#)
- [TrustSec AAA サーバの設定 \(982 ページ\)](#)
- [セキュリティ グループの設定 \(983 ページ\)](#)
- [出力ポリシー \(Egress Policy\) \(989 ページ\)](#)
- [SGT の割り当て \(1009 ページ\)](#)
- [TrustSec の設定およびポリシー プッシュ \(1012 ページ\)](#)
- [セキュリティ グループ タグの交換プロトコル \(1022 ページ\)](#)
- [SXP ドメイン フィルタの追加 \(1024 ページ\)](#)
- [SXP の設定 \(1025 ページ\)](#)
- [TrustSec-ACI 統合 \(1026 ページ\)](#)
- [ACI の設定 \(1027 ページ\)](#)
- [ユーザ レポート別上位 N 個の RBACL ドロップの実行 \(1028 ページ\)](#)

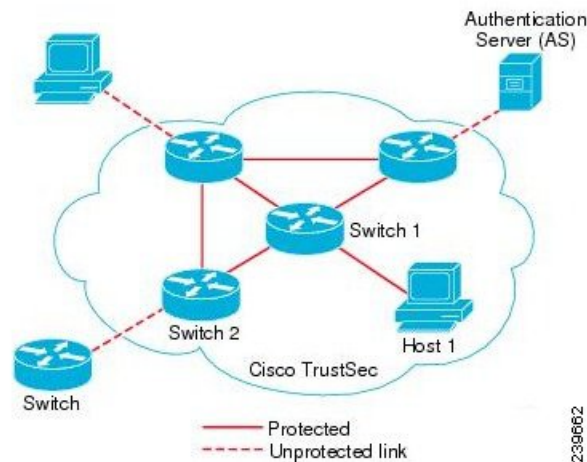
TrustSec アーキテクチャ

Cisco TrustSec ソリューションでは、信頼ネットワーク デバイスのクラウドを確立して、セキュアなネットワークを構築します。Cisco TrustSec クラウド内の個々のデバイスは、そのネイバー（ピア）によって認証されます。TrustSec クラウド内のデバイス間の通信は、暗号化、メッセージ整合性検査、データパスリプレイ防止メカニズムを組み合わせたセキュリティで保護されます。TrustSec ソリューションでは、認証中に取得したデバイスおよびユーザ ID 情報を使用して、ネットワークに入ってきたパケットを分類（色付け）します。このパケット分類は、パケットが TrustSec ネットワークに入ってきたときに、そのパケットにタグ付けすることによって維持されます。これにより、パケットはデータパス全体で正しく識別され、セキュリティおよびその他のポリシー基準が適用されるようになります。このタグは、セキュリティグループタグ（SGT）と呼ばれることもあります。エンドポイント デバイスで SGT に応じてト

ラフィックをフィルタリングできるようにすることにより、Cisco ISE でアクセス コントロール ポリシーを適用できるようになります。

次の図に、TrustSec ネットワーク クラウドの例を示します。

図 57: TrustSec アーキテクチャ



ISE コミュニティ リソース

Cisco TrustSecを使用してネットワークセグメンテーションを簡素化、セキュリティを強化する方法については、「[Simplify Network Segmentation with Cisco TrustSec](#)」と「[Policy-Based Software Defined Segmentation and Cisco TrustSec Improve Security White Paper](#)」を参照してください。

Cisco TrustSec プラットフォーム サポート マトリックスのリストについては、「[Cisco TrustSec Platform Support Matrix](#)」を参照してください。

利用可能な TrustSec のサポート ドキュメントのリストについては、「[Cisco TrustSec](#)」を参照してください。

TrustSec コミュニティ リソースのリストについては、[TrustSec Community](#)を参照してください。

関連トピック

[TrustSec のコンポーネント](#) (972 ページ)

[TrustSec の用語](#) (974 ページ)

[TrustSec のサポートされるスイッチと必要なコンポーネント](#) (975 ページ)

[TrustSec に必要なコンポーネント](#)

TrustSec のコンポーネント

主な TrustSec のコンポーネント：

- ネットワーク デバイス アドミッション コントロール (NDAC)：信頼ネットワークでは、認証中に、TrustSec クラウド内にある各ネットワーク デバイス（イーサネット スイッチ

など) のクレデンシャルおよび信頼性が、そのピアデバイスによって検証されます。NDAC は IEEE 802.1X ポートベース認証を使用し、その拡張認証プロトコル (EAP) 方式として Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) を使用します。NDAC プロセスの認証および許可が成功すると、IEEE 802.1AE 暗号化のセキュリティ アソシエーション プロトコル ネゴシエーションが実行されます。

- エンドポイント アドミSSION コントロール (EAC) : TrustSec クラウドに接続しているエンドポイント ユーザまたはデバイスの認証プロセス。EAC は一般的にアクセス レベル スイッチで実行されます。EAC プロセスの認証および許可が成功すると、ユーザまたはデバイスに対する SGT 割り当てが実行されます。認証および許可の EAC アクセス方法には次のものがあります。
 - 802.1X ポートベースの認証
 - MAC 認証バイパス (MAB)
 - Web 認証 (WebAuth)
- セキュリティ グループ (SG) : アクセスコントロールポリシーを共有するユーザ、エンドポイント デバイス、およびリソースのグループ。SG は、管理者が Cisco ISE で定義します。新規ユーザおよびデバイスが TrustSec ドメインに追加されると、Cisco ISE では、これらの新規エントリを適切なセキュリティ グループに割り当てます。
- セキュリティ グループ タグ (SGT) : TrustSec サービスは各セキュリティ グループに、その範囲が TrustSec ドメイン内でグローバルな一意のセキュリティ グループ番号 (16 ビット) を割り当てます。スイッチ内のセキュリティ グループの数は、認証されたネットワーク エンティティの数に制限されます。セキュリティ グループ番号を手動で設定する必要はありません。これらは自動的に生成されますが、IP と SGT とのマッピング用に SGT の範囲を予約しておくことができます。
- セキュリティ グループ アクセス コントロール リスト (SGACL) : SGACL では、割り当てられている SGT に基づいてアクセスおよび権限を制御できます。権限をロールにまとめることにより、セキュリティポリシーの管理が容易になります。デバイスを追加するときに、1つ以上のセキュリティ グループを割り当てただけで、即座に適切な権限が付与されます。セキュリティ グループを変更することにより、新しい権限を追加したり、現在の権限を制限することもできます。
- セキュリティ 交換 プロトコル (SXP) : SGT 交換プロトコル (SXP) は、TrustSec サービス用に開発されたプロトコルで、SGT 対応ハードウェアをサポートしていないネットワーク デバイス間で、SGT/SGACL をサポートしているハードウェアに IP-SGT バインディングを伝播します。
- 環境データのダウンロード : TrustSec デバイスは、初めて信頼ネットワークに参加するときに、その環境データを Cisco ISE から取得します。デバイス上の一部のデータは、手動で設定することもできます。デバイスでは、期限切れになる前に環境データを更新する必要があります。TrustSec デバイスは、次の環境データを Cisco ISE から取得します。
 - サーバリスト : クライアントがその後の RADIUS 要求に使用できるサーバのリスト (認証および許可の両方)

- デバイス SG : そのデバイス自体が属しているセキュリティ グループ
- 有効期間 : TrustSec デバイスが環境データをダウンロードまたはリフレッシュする頻度を制御する期間
- ID とポートとのマッピング : エンドポイントの接続先のポートでスイッチが ID を定義するための方法で、この ID を使用して Cisco ISE サーバ内の特定の SGT 値が検索されます。

TrustSec の用語

次の表は、TrustSec ソリューションで使用される一般的な用語の一部と、TrustSec 環境でのその意味を示しています。

表 58 : TrustSec の用語

用語	意味
サブリカント	信頼ネットワークへの参加を試行するデバイス。
認証	信頼ネットワークへの参加を許可する前に、各デバイスの ID を検証するプロセス。
許可	信頼ネットワーク上のリソースへのアクセスを要求しているデバイスに対し、デバイスの認証 ID に基づいてアクセスのレベルを決定するプロセス。
アクセス コントロール	各パケットに割り当てられている SGT に基づいて、パケットごとにアクセス コントロールを適用するプロセス。
セキュアな通信	信頼ネットワーク内の各リンクを経由して流れるパケットをセキュリティで保護するための、暗号化、整合性、データパス リプレイ保護のプロセス。
TrustSec デバイス	TrustSec ソリューションをサポートする Cisco Catalyst 6000 シリーズまたは Cisco Nexus 7000 シリーズのスイッチ。
TrustSec 対応デバイス	TrustSec 対応デバイスは、TrustSec 対応のハードウェアとソフトウェアを備えています。たとえば、Nexus オペレーティングシステムを搭載した Nexus 7000 シリーズスイッチなどです。

用語	意味
TrustSec シード デバイス	Cisco ISE サーバに対して直接認証を行う TrustSec デバイス。オーセンティケーターとサブリカントの両方として機能します。
受信側	Cisco TrustSec ソリューションが有効になっているネットワーク内の TrustSec 対応デバイスにパケットが初めて到達すると、SGT を使用してパケットにタグが付けられます。この信頼ネットワークへの入り口点を入力と呼びます。
送信側	Cisco TrustSec ソリューションが有効になっているネットワーク内の最後の TrustSec 対応デバイスをパケットが通過すると、タグが解除されます。この信頼ネットワークからの出口点を出力と呼びます。

TrustSec のサポートされるスイッチと必要なコンポーネント

Cisco TrustSec ソリューションが有効になった Cisco ISE ネットワークを設定するには、TrustSec ソリューションおよび他のコンポーネントをサポートするスイッチが必要です。スイッチ以外に、IEEE 802.1X プロトコルを使用した ID ベースのユーザ アクセス コントロールには、その他のコンポーネントも必要です。TrustSec をサポートするシスコスイッチのプラットフォームおよび必要なコンポーネントの完全な最新のリストについては、「[Cisco TrustSec-Enabled Infrastructure](#)」を参照してください。

TrustSec ダッシュボード

TrustSec ダッシュボードは、TrustSec ネットワークの一元化されたモニタリング ツールです。TrustSec ダッシュボードには次のダッシュレットが含まれています。

- メトリック
- アクティブなSGTセッション (Active SGT Sessions)
- アラーム
- NAD/SGTクイックビュー (NAD / SGT Quick View)
- TrustSecセッション/NADアクティビティライブログ (TrustSec Sessions / NAD Activity Live Log)

メトリック

このセクションには、TrustSec ネットワークの動作に関する統計情報が表示されます。タイムフレーム（たとえば、過去 2 時間、過去 2 日 など）とチャート タイプ（たとえば、棒、折れ線、スプラインなど）を選択できます。

最新のバー値がグラフに表示されます。また、前のバーからのパーセンテージの変化も表示されます。バー値に増加がある場合、プラス記号付きの緑色で表示されます。値に減少がある場合、マイナス記号付きの赤色で表示されます。

値が計算された時刻とその正確な値を <Value:xxxx Date/Time: xxx> 形式で表示するには、グラフのバーにカーソルを置きます。

次のメトリックを表示できます。

SGTセッション（SGT sessions）	選択された時間内に作成された SGT セッションの総数が表示されます。 （注） SGT セッションは、認証フローの一部として SGT を受信したユーザセッションです。
使用中のSGT（SGTs in use）	選択された時間内に使用された固有の SGT の総数が表示されます。たとえば、1 時間で 200 の TrustSec セッションがあったが、ISE が認証応答で 6 つのタイプの SGT でしか応答しなかった場合、グラフにはこの時間に値 6 が表示されます。
アラーム	選択された時間内に発生したアラームおよびエラーの総数が表示されます。エラーは赤色で表示され、アラームは黄色で表示されます。
使用中のNAD（NADs in use）	選択された時間内に TrustSec 認証に参加した固有の NAD の数が表示されます。

現在のネットワーク ステータス

このダッシュボードの中間部分には、TrustSec ネットワークの現在のステータスに関する情報が表示されます。グラフに表示される値は、ページがロードされると更新され、[ダッシュボードの更新（Refresh Dashboard）] オプションを使用して更新できます。

アクティブな SGT セッション

このダッシュレットには、ネットワークで現在アクティブな SGT セッションが表示されます。上位 10 個の最もよく使用されている SGT または最も使用頻度の低い SGT を表示できます。X 軸には SGT 使用率が表示され、Y 軸には SGT の名前が表示されます。

SGT の TrustSec セッションの詳細を表示するには、その SGT に対応するバーをクリックします。その SGT に関連する TrustSec セッションの詳細が [ライブログ（Live Log）] ダッシュレットに表示されます。

アラーム

このダッシュレットには、TrustSec セッション関連のアラームが表示されます。次の詳細情報を表示できます。

- [アラームの重大度 (Alarm Severity)] : アラームの重大度レベルを示すアイコンが表示されます。
 - [高 (High)] : TrustSec ネットワーク内の障害を示すアラームが含まれます (たとえば、PAC の更新が失敗したデバイスなど)。赤色のアイコンが付いています。
 - [中 (Medium)] : ネットワーク デバイスの誤った設定を示す警告が含まれます (たとえば、CoA メッセージの受け入れを失敗したデバイスなど)。黄色でマークされます。
 - [低 (Low)] : ネットワーク動作の一般情報および更新が含まれます (たとえば、TrustSec の設定変更など)。青色でマークされます。
- アラームの説明
- このアラーム カウンタが最後にリセットされてからアラームが発生した回数。
- アラームが最後に発生した時刻

クイック ビュー

[クイックビュー (Quick View)] ダッシュレットには、NAD の TrustSec 関連情報が表示されます。SGT の TrustSec 関連情報を表示することもできます。

NAD クイック ビュー

[検索 (Search)] ボックスに詳細を表示する TrustSec ネットワーク デバイスの名前を入力し、**Enter** を押します。検索ボックスには自動入力機能があり、ユーザがテキストボックスに入力すると、ドロップ ダウンに一致するデバイス名がフィルタされ表示されます。

次の詳細情報が表示されます。

- [NDG (NDGs)] : このネットワーク デバイスが属するネットワーク デバイス グループ (NDG) がリストされます。
- [IPアドレス (IP Address)] : ネットワーク デバイスの IP アドレス。[ライブログ (Live Logs)] ダッシュレットに NAD アクティビティの詳細を表示するには、このリンクをクリックします。
- [アクティブセッション (Active sessions)] : このデバイスに接続されているアクティブな TrustSec セッションの数。
- [PACの有効期限 (PAC expiry)] : PAC の失効日。
- [最後のポリシー更新 (Last Policy Refresh)] : ポリシーを最後にダウンロードした日付。

- [最後の認証 (Last Authentication)] : このデバイスの最後の認証レポートのタイムスタンプ。
- [アクティブSGT (ActiveSGTs)] : このネットワークデバイスに関連するアクティブセッションで使用されている SGT がリストされます。カッコ内に表示される数字は、現在この SGT を使用しているセッションの数を示します。[ライブ ログ (Live Log)] ダッシュレットに TrustSec セッションの詳細を表示するには、SGT のリンクをクリックします。

[最新ログの表示 (Show Latest Logs)] オプションを使用して、デバイスの NAD アクティビティのライブ ログを表示できます。

SGT クイック ビュー

[検索 (Search)] ボックスに詳細を表示する SGT の名前を入力し、**Enter** を押します。

次の情報がこのダッシュレットに表示されます。

- [値 (Value)] : SGT 値 (10 進数と 16 進数の両方)。
- [アイコン (Icon)] : この SGT に割り当てられているアイコンが表示されます。
- [アクティブセッション (Active sessions)] : 現在この SGT を使用しているアクティブなセッションの数。
- [固有ユーザ (Unique users)] : この SGT をアクティブ セッションに保持する固有ユーザ名の数。
- [更新されたNAD (Updated NADs)] : この SGT のポリシーをダウンロードした NAD の数。

ライブ ログ

アクティブな TrustSec セッション (応答の一部として SGT があるセッション) を表示するには [TrustSecセッション (TrustSec Sessions)] リンクをクリックします。

NAD から Cisco ISE への TrustSec プロトコルデータ要求と応答に関する情報を表示するには、[NADアクティビティ (NAD Activity)] リンクをクリックします。

TrustSec のグローバル設定

Cisco ISE が TrustSec サーバとして機能して TrustSec サービスを提供するには、いくつかのグローバル TrustSec 設定を定義する必要があります。

始める前に

- TrustSec グローバル設定を設定する前に、グローバル EAP-FAST 設定が定義されていることを確認します ([管理 (Administration)] > [システム (System)] > [設定 (Settings)] >

[**プロトコル (Protocols)**] > [**EAP-FAST**] > [**EAP-FAST 設定 (EAP-FAST Settings)**] を選択)。

[**機関識別情報の説明 (Authority Identity Info Description)**] を Cisco ISE サーバ名に変更することができます。この説明は、クレデンシャルをエンドポイントクライアントに送信する Cisco ISE サーバを説明したわかりやすい文字列にします。Cisco TrustSec アーキテクチャのクライアントには、IEEE 802.1X 認証の EAP 方式として EAP-FAST を実行するエンドポイント、または Network Device Access Control (NDAC) を実行するサブリカントネットワーク デバイスのいずれも使用できます。クライアントは、この文字列を Protected Access Credentials (PAC) Type-Length-Value (TLV) 情報で認識できます。デフォルト値は、Identity Services Engine です。NDAC 認証時に、ネットワーク デバイスで Cisco ISE PAC 情報が一意に識別されるように、この値を変更する必要があります。

- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 [ワークセンター (Work Centers)] > [TrustSec] > [設定 (Settings)] > [一般TrustSecの設定 (General TrustSec Settings)] の順に選択します。

ステップ 2 フィールドに値を入力します。

ステップ 3 [保存 (Save)] をクリックします。

次のタスク

- [TrustSec デバイスの設定 \(980 ページ\)](#)

TrustSec マトリックスの設定

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 [ワークセンター (Work Centers)] > [TrustSec] > [設定 (Settings)] > [TrustSec マトリックスの設定 (TrustSec Matrix Settings)] の順に選択します。

ステップ 2 [TrustSec マトリックスの設定 (TrustSec Matrix Settings)] ページに必要な詳細を入力します。

ステップ 3 [保存 (Save)] をクリックします。

TrustSec デバイスの設定

Cisco ISE で TrustSec 対応デバイスからの要求を処理するには、これらの TrustSec 対応デバイスを Cisco ISE で定義しておく必要があります。

-
- ステップ 1** [ワークセンター (Work Centers)] > [TrustSec] > [コンポーネント (Components)] > [ネットワークデバイス (Network Devices)] の順に選択します。
- ステップ 2** [追加 (Add)] をクリックします。
- ステップ 3** [ネットワーク デバイス (Network Devices)] セクションで、必要な情報を入力します。
- ステップ 4** TrustSec 対応デバイスを設定するために [高度な TrustSec 設定 (Advanced Trustsec Settings)] チェックボックスをオンにします。
- ステップ 5** [送信 (Submit)] をクリックします。
-

OOB TrustSec PAC

すべての TrustSec ネットワーク デバイスで、EAP-FAST プロトコルの一部として TrustSec PAC が保持されています。これはセキュアな RADIUS プロトコルでも使用され、ここでは RADIUS 共有秘密が PAC で伝送されるパラメータから作成されます。これらのパラメータの 1 つである発信側 ID には、TrustSec ネットワーク デバイス ID、つまりデバイス ID が保持されます。

デバイスが TrustSec PAC を使用して識別される場合、Cisco ISE でそのデバイス用に設定されているデバイス ID と、PAC の発信側 ID が一致していない場合、認証に失敗します。

一部の TrustSec デバイス (Cisco ASA ファイアウォールなど) では EAP-FAST プロトコルをサポートしていません。したがって、Cisco ISE ではこれらのデバイスを EAP-FAST を介した TrustSec PAC でプロビジョニングできません。代わりに、TrustSec PAC は Cisco ISE 上で生成され、手動でデバイスにコピーされます。そのため、これをアウトオブバンド (OOB) TrustSec PAC 生成と呼びます。

Cisco ISE で PAC を生成すると、暗号キーで暗号化された PAC ファイルが生成されます。

ここでは、次の内容について説明します。

関連トピック

[\[設定 \(Settings\)\] 画面からの TrustSec PAC の生成 \(980 ページ\)](#)

[\[ネットワーク デバイス \(Network Devices\)\] 画面からの TrustSec PAC の生成 \(981 ページ\)](#)

[\[ネットワーク デバイス リスト \(Network Devices List\)\] 画面からの TrustSec PAC の生成 \(982 ページ\)](#)

[設定 (Settings)] 画面からの TrustSec PAC の生成

[設定 (Settings)] 画面から TrustSec PAC を生成できます。

-
- ステップ 1 [管理 (Administration)] > [システム (System)] > [設定 (Settings)] を選択します。
- ステップ 2 左側の [設定 (Settings)] ナビゲーション ペインの [プロトコル (Protocols)] をクリックします。
- ステップ 3 [EAP-FAST] > [PAC の生成 (Generate PAC)] を選択します。
- ステップ 4 TrustSec PAC を生成します。
-

[ネットワーク デバイス (Network Devices)] 画面からの TrustSec PAC の生成

[ネットワーク デバイス (Network Devices)] 画面から TrustSec PAC を生成できます。

-
- ステップ 1 [ワークセンター (Work Centers)] > [TrustSec] > [コンポーネント (Components)] > [ネットワーク デバイス (Network Devices)] の順に選択します。
- ステップ 2 [追加 (Add)] をクリックします。[ネットワーク デバイス (Network Devices)] ナビゲーション ペインのアクション アイコンから [新規デバイスの追加 (Add new device)] をクリックすることもできます。
- ステップ 3 新規デバイスを追加する場合は、デバイス名を入力します。
- ステップ 4 TrustSec デバイスを設定するために [高度な TrustSec 設定 (Advanced Trustsec Settings)] チェックボックスをオンにします。
- ステップ 5 [アウトオブバンド (OOB) TrustSec PAC (Out of Band (OOB) TrustSec PAC)] サブ セクションで、[PAC の生成 (Generate PAC)] をクリックします。
- ステップ 6 次の詳細事項を入力します。

- [PAC 存続可能時間 (PAC Time to Live)] : 日、週、月、および年の単位で値を入力します。デフォルト値は 1 年です。最小値は 1 日、最大値は 10 年です。
- [暗号化キー (Encryption Key)] : 暗号キーを入力します。キーの長さは 8 ~ 256 文字にする必要があります。キーはアルファベットの大文字または小文字、数字、または英数字の組み合わせを含むことができます。

暗号キーを使用して、生成されるファイルの PAC が暗号化されます。このキーは、デバイスで PAC ファイルを復号化する場合にも使用されます。したがって、後で使用できるように管理者が暗号キーを保存しておくことを推奨します。

[ID (Identity)] フィールドは TrustSec ネットワーク デバイスのデバイス ID を示し、このフィールドには EAP-FAST プロトコルによって発信側 ID が提供されます。ここに入力した ID 文字列がネットワーク デバイスの作成ページの [TrustSec] セクションで定義されたデバイス ID と一致しない場合、認証は失敗します。

有効期限は、PAC 存続可能時間に基づいて計算されます。

- ステップ 7 [PAC の生成 (Generate PAC)] をクリックします。
-

[ネットワーク デバイス リスト (Network Devices List)] 画面からの TrustSec PAC の生成

[ネットワーク デバイス リスト (Network Devices list)] 画面から TrustSec PAC を生成できます。

-
- ステップ 1** [ワークセンター (Work Centers)] > [TrustSec] > [コンポーネント (Components)] > [ネットワーク デバイス (Network Devices)] の順に選択します。
- ステップ 2** [ネットワーク デバイス (Network Devices)] をクリックします。
- ステップ 3** TrustSec PAC を生成するデバイスの隣にあるチェックボックスをオンにし、[PAC の生成 (Generate PAC)] をクリックします。
- ステップ 4** フィールドで詳細を提供します。
- ステップ 5** [PAC の生成 (Generate PAC)] をクリックします。
-

[プッシュ (Push)] ボタン

出力ポリシーの [プッシュ (Push)] オプションは CoA 通知を開始します。この通知は、Cisco ISE からの出力ポリシー設定変更に関する更新を、ただちに要求するよう TrustSec デバイスに伝えます。

関連トピック

[SGT マトリクスの更新 CoA のフロー](#) (1019 ページ)

TrustSec AAA サーバの設定

展開内の Cisco ISE サーバのリストを AAA サーバリストに設定して、これらの任意のサーバに対して TrustSec デバイスの認証が行われるようにできます。このリストに Cisco ISE サーバを追加すると、これらすべてのサーバの詳細が TrustSec デバイスにダウンロードされます。TrustSec デバイスは、認証を試行するときに、このリストから Cisco ISE サーバを選択します。最初のサーバがダウン状態またはビジー状態の場合、TrustSec デバイスはこのリストにある別の任意のサーバに対して自分自身の認証を行うことができます。デフォルトでは、プライマリ Cisco ISE サーバは、TrustSec AAA サーバです。1 台のサーバがビジー状態の場合、AAA サーバリストの別のサーバが TrustSec 要求を処理できるように、AAA サーバリストで追加の Cisco ISE サーバを設定することを推奨します。

このページには、TrustSec AAA サーバとして設定した展開内の Cisco ISE サーバがリストされます。

[プッシュ (Push)] ボタンをクリックすると、複数の TrustSec AAA サーバを設定した後に、環境 CoA 通知を開始できます。この環境 CoA 通知は、すべての TrustSec ネットワーク デバイスに送信され、変更されたすべての TrustSec AAA サーバの更新を提供します。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 [ワークセンター (Work Centers)] > [TrustSec] > [コンポーネント (Components)] > [TrustSec AAAサーバ (TrustSec AAA Servers)] を選択します。

ステップ 2 [追加 (Add)] をクリックします。

ステップ 3 説明に従って値を入力します。

- [名前 (Name)] : この AAA サーバリスト内で Cisco ISE サーバに割り当てる名前。この名前は、Cisco ISE サーバのホスト名と異なってもかまいません。
- [説明 (Description)] : 説明 (任意)。
- [IP] : AAA サーバリストに追加する Cisco ISE サーバの IP アドレス。
- [ポート (Port)] : TrustSec デバイスとサーバ間の通信が行われるポート。デフォルトは 1812 です。

ステップ 4 [送信 (Submit)] をクリックします。

次のタスク

セキュリティ グループを設定します。

セキュリティ グループの設定

セキュリティグループ (SG) またはセキュリティグループタグ (SGT) は、TrustSec ポリシー設定で使用される要素です。SGT は、パケットが信頼ネットワーク内を移動する場合に付加されます。これらのパケットは、信頼ネットワークに入ったとき (入力) にタグ付けされ、信頼ネットワークから離れるとき (出力) にタグ解除されます。

SGT は順次的な方法で生成されますが、IP と SGT とのマッピング用に SGT の範囲を予約しておくことができます。Cisco ISE は、SGT の生成時に予約済みの番号をスキップします。

TrustSec サービスはこれらの SGT を使用して、出力時に TrustSec ポリシーを適用します。

管理者ポータルで次のページからセキュリティ グループを設定できます。

- [ワークセンター (Work Centers)] > [TrustSec] > [コンポーネント (Components)] > [セキュリティグループ (Security Groups)]。
- [設定 (Configure)] > [新規セキュリティグループの作成 (Create New Security Group)] の出力ポリシーページから直接。

[プッシュ (Push)] ボタンをクリックすると、複数の SGT を更新した後に、環境 CoA 通知を開始できます。この環境 CoA 通知はすべての TrustSec ネットワーク デバイスに送信され、ポリシー/データ リフレッシュ要求を開始することを強制します。

関連トピック

[セキュリティ グループの追加](#) (984 ページ)[出力ポリシーの SGT の設定](#) (1007 ページ)[NDAC 許可の設定](#) (1010 ページ)[TrustSec AAA サーバの設定](#) (982 ページ)

セキュリティ グループの追加

TrustSec ソリューション内の個々のセキュリティ グループに一意の SGT を割り当てる必要があります。Cisco ISE では 65,535 SGT までサポートされていますが、SGT の数を少なくすると、TrustSec ソリューションをより簡単に展開および管理できるようになります。最大で 4,000 SGT までにすることを推奨します。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

-
- ステップ 1** [ワークセンター (Work Centers)] > [TrustSec] > [コンポーネント (Components)] > [セキュリティグループ (Security Groups)] を選択します。
- ステップ 2** [追加 (Add)] をクリックして新規セキュリティ グループを追加します。
- ステップ 3** 新規セキュリティ グループの名前と説明 (オプション) を入力します。
- ステップ 4** この SGT を ACI に反映するには、[ACI に伝播 (Propagate to ACI)] チェック ボックスをオンにします。この SGT に関連する SXP マッピングは、ACI が [ACI の設定 (ACI Settings)] ページで選択した VPN に属するときのみ ACI に反映されます。
- このオプションはデフォルトでは無効になっています。
- ステップ 5** タグ値を入力します。タグ値は、手動で入力したり、自動生成されるようにしたり設定できます。また SGT の範囲を予約できます。これは、から設定できます。[一般 TrustSec の設定 (General TrustSec Settings)] ページ ([ワークセンター (Work Centers)] > [TrustSec] > [設定 (Settings)] > [一般 TrustSec の設定 (General TrustSec Settings)])。
- ステップ 6** [保存 (Save)] をクリックします。
-

次のタスク

[セキュリティ グループ アクセス コントロール リストの設定](#)

Cisco ISE へのセキュリティ グループのインポート

カンマ区切り形式 (CSV) ファイルを使用して Cisco ISE ノードにセキュリティ グループをインポートできます。Cisco ISE にセキュリティ グループをインポートする前に、テンプレートを更新する必要があります。同じリソースタイプのインポートを同時に実行できません。たと

例えば、2つの異なるインポートファイルから同時にセキュリティ グループをインポートできません。

管理者ポータルから CSV テンプレートをダウンロードし、テンプレートにセキュリティ グループの詳細を入力し、Cisco ISE にインポート可能な CSV ファイルとしてテンプレートを保存できます。

セキュリティ グループのインポート中、Cisco ISE で最初のエラーが発生した場合、インポート プロセスを停止できます。

-
- ステップ 1** [ワークセンター (Work Centers)] > [TrustSec] > [コンポーネント (Components)] > [セキュリティグループ (Security Groups)] を選択します。
- ステップ 2** [インポート (Import)] をクリックします。
- ステップ 3** [参照 (Browse)] をクリックして、クライアント ブラウザを実行しているシステムから CSV ファイルを選択します。
- ステップ 4** [最初のエラーでインポートを停止 (Stop Import on First Error)] チェックボックスをオンにします。
- ステップ 5** [インポート (Import)] をクリックします。
-

Cisco ISE からのセキュリティ グループのエクスポート

Cisco ISE で設定されたセキュリティ グループを CSV ファイル形式でエクスポートし、これを使用して別の Cisco ISE ノードにそれらのセキュリティ グループをインポートできます。

-
- ステップ 1** [ワークセンター (Work Centers)] > [TrustSec] > [コンポーネント (Components)] > [セキュリティグループ (Security Groups)] を選択します。
- ステップ 2** [エクスポート (Export)] をクリックします。
- ステップ 3** セキュリティ グループをエクスポートするには、次のいずれかを実行できます。
- エクスポートするグループの隣にあるチェックボックスをオンにし、[エクスポート (Export)] > [選択済みをエクスポート (Export Selected)] を選択します。
 - [エクスポート (Export)] > [すべてエクスポート (Export All)] を選択して、定義されたすべてのセキュリティ グループをエクスポートします。
- ステップ 4** ローカル ハード ディスクに export.csv ファイルを保存します。
-

IP SGT スタティック マッピングの追加

IP-SGT スタティック マッピングを使用して、TrustSec デバイスと SXP ドメインに統一された方法でマッピングを展開することができます。新しい IP-SGT スタティック マッピングを作成

するときに、このマッピングを展開する SXP ドメインとデバイスを指定できます。また、IP-SGT マッピングをマッピング グループに関連付けることもできます。

ステップ 1 [ワークセンター (Work Centers)] > [TrustSec] > [コンポーネント (Components)] > [IP SGT スタティック マッピング (IP SGT Static Mapping)] の順に選択します。

ステップ 2 [追加 (Add)] をクリックします。

ステップ 3 ホスト名または IP アドレスを入力します。

ステップ 4 既存のマッピンググループを使用する場合は、[マッピンググループに追加 (Add to a Mapping Group)] をクリックして、[マッピンググループ (Mapping Group)] ドロップダウン リストから必要なグループを選択します。

この IP アドレス/ホスト名を SGT に個別にマッピングする場合は、[SGT に個別にマッピング (Map to SGT Individually)] をクリックして以下を実行します。

- [SGT] ドロップダウン リストから SGT を選択します。
- マッピングを展開する必要がある SXP VPN グループを選択します。
- このマッピングを展開するデバイスを指定します。すべての TrustSec デバイス、選択されたネットワーク デバイス グループ、または選択されたネットワーク デバイスにマッピングを展開できます。

(注) マッピングを追加した後、[展開 (Deploy)] オプションを使用して、対象のネットワーク デバイスでこのマッピングを展開する必要があります。マッピングをすでに保存している場合でも、これを明示的に行う必要があります。デバイスの展開ステータスを確認するには、[ステータスを確認 (Check Status)] をクリックします。

ステップ 5 [保存 (Save)] をクリックします。

Cisco ISE への IP SGT スタティック マッピングのインポート

CSV ファイルを使用して IP SGT マッピングをインポートできます。

また、管理者ポータルから CSV テンプレートをダウンロードし、マッピングの詳細を入力し、CSV ファイルとしてテンプレートを保存して、Cisco ISE にインポートすることができます。

ステップ 1 [ワークセンター (Work Centers)] > [TrustSec] > [コンポーネント (Components)] > [IP SGT スタティック マッピング (IP SGT Static Mapping)] の順に選択します。

ステップ 2 [インポート (Import)] をクリックします。

ステップ 3 [参照 (Browse)] をクリックして、クライアント ブラウザを実行しているシステムから CSV ファイルを選択します。

ステップ 4 [アップロード (Upload)] をクリックします。

Cisco ISE からの IP SGT スタティック マッピングのエクスポート

IP SGT マッピングを CSV ファイルの形式でエクスポートできます。このファイルを使用して、これらのマッピングを別の Cisco ISE ノードにインポートできます。

-
- ステップ 1** [ワークセンター (Work Centers)] > [TrustSec] > [コンポーネント (Components)] > [IP SGT スタティック マッピング (IP SGT Static Mapping)] の順に選択します。
- ステップ 2** 次のいずれかを実行します。
- エクスポートするマッピングの隣にあるチェックボックスをオンにし、[エクスポート (Export)] > [選択済み (Selected)] を選択します。
 - [エクスポート (Export)] > [すべて (All)] を選択して、すべてのマッピングをエクスポートします。
- ステップ 3** ローカル ハード ディスクに mappings.csv ファイルを保存します。
-

SGT マッピング グループの追加

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

-
- ステップ 1** [ワークセンター (Work Centers)] > [TrustSec] > [コンポーネント (Components)] > [IP SGT スタティック マッピング (IP SGT Static Mapping)] > [グループの管理 (Manage Groups)] の順に選択します。
- ステップ 2** [追加 (Add)] をクリックします。
- ステップ 3** マッピング グループの名前と説明を入力します。
- ステップ 4** 次の手順を実行します。
- [SGT] ドロップダウン リストから SGT を選択します。
 - マッピングを展開する必要がある SXP VPN グループを選択します。
 - マッピングを展開するデバイスを指定します。すべての TrustSec デバイス、選択されたネットワーク デバイス グループ、または選択されたネットワーク デバイスにマッピングを展開できます。
- ステップ 5** [保存 (Save)] をクリックします。
-

あるマッピング グループから別のマッピング グループに IP SGT マッピングを移動できます。

また、マッピングおよびマッピング グループを更新または削除できます。マッピングまたはマッピング グループを更新するには、更新するマッピングまたはマッピング グループの横にあるチェック ボックスにマークを付けてから、[編集 (Edit)] をクリックします。マッピングまたはマッピング グループを削除するには、削除するマッピングまたはマッピング グループ

の横にあるチェック ボックスにマークを付けてから、[ごみ箱 (Trash)] > [選択済み (Selected)] の順にクリックします。マッピング グループが削除されると、そのグループ内の IP SGT マッピングも削除されます。

セキュリティ グループ アクセス コントロール リストの追加

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 [ワークセンター (Work Centers)] > [TrustSec] > [コンポーネント (Components)] > [セキュリティグループ ACL (Security Group ACLs)] を選択します。

ステップ 2 [追加 (Add)] をクリックして新規セキュリティ グループ ACL を作成します。

ステップ 3 次の情報を入力します。

- [名前 (Name)] : SGACL の名前
- [説明 (Description)] : SGACL の説明 (任意)
- [IP バージョン (IP Version)] : この SGACL でサポートされる IP バージョン :
 - [IPv4] : IP バージョン 4 (IPv4) がサポートされます
 - [IPv6] : IP バージョン 6 (IPv6) がサポートされます
 - [非認識 (Agnostic)] : IPv4 と IPv6 の両方がサポートされます
- セキュリティ グループ ACL の内容 : アクセス コントロール リスト (ACL) コマンド。次に例を示します。

permit icmp

deny ip

ISE 内では SGACL 入力の構文が検査されません。スイッチ、ルータ、アクセス ポイントをエラーなく適用できるように、正しい構文を確実に使用してください。デフォルトポリシーを **permit IP**、**permit ip log**、**deny ip**、または **deny ip log** として設定できます。TrustSec ネットワーク デバイスでは、デフォルト ポリシーを特定セルのポリシーの最後に付加します。

参考用に SGACL の 2 つの例を示します。どちらにも最終的な **catch-all** ルールが含まれています。最初の例では、最終的な **catch-all** ルールとして拒否し、2 番目の例では許可します。

Permit_Web_SGACL

```
permit tcp dst eq 80
permit tcp dst eq 443
deny ip
```

Deny_JumpHost_Protocols

```
deny tcp dst eq 23
deny tcp dst eq 23
```

```
deny tcp dst eq 3389
permit ip
```

次の表に、IOS、IOS XE、NS OS オペレーティング システム用の SGACL の構文を示します。

SGACL CLI と ACE	IOS、IOS XE、NX OS で共通の構文
config acl	deny、exit、no、permit
拒否 許可	ahp、eigrp、gre、icmp、igmp、ip、nos、ospf、pcp、pim、tcp、udp
deny tcp deny tcp src deny tcp dst	dst、log、src
deny tcp dst eq deny tcp src eq	<0-65535> port number
deny udp deny udp src deny udp dest	Dst、log、src
deny tcp dst eq www deny tcp src eq www	<0-65535> port number

ステップ 4 [送信 (Submit)] をクリックします。

出力ポリシー (Egress Policy)

出力テーブルには、送信元 SGT および宛先 SGT が、予約済みのものもそうでないものもあわせてリストされます。また、このページでは、出力テーブルをフィルタリングして特定のポリシーを表示することや、これらのプリセットフィルタを保存することもできます。送信元 SGT から宛先 SGT に到達しようとする、TrustSec 対応デバイスは、出力ポリシーで定義されている TrustSec ポリシーに基づいて SGACL を適用します。Cisco ISE はポリシーを作成してプロビジョニングします。

TrustSec ポリシーの作成に必要な基本的構築ブロックである SGT および SGACL を作成した後に、SGACL を送信元 SGT および宛先 SGT に割り当てることによって、それらの関係を確立できます。

送信元 SGT と宛先 SGT のそれぞれの組み合わせが、出力ポリシーのセルになります。

出力ポリシーは、[ワークセンター (Work Centers)] > [TrustSec] > [TrustSec ポリシー (TrustSec Policy)] > [出力ポリシー (Egress Policy)] ページで表示できます。

それぞれ異なる 3 つの方法で出力ポリシーを表示できます。

- 送信元ツリー ビュー
- 宛先ツリー ビュー
- マトリクス ビュー

関連トピック

- [マトリクス操作](#) (993 ページ)
- [出力ポリシー テーブルセルの設定](#) (1005 ページ)
- [出力ポリシーの SGT の設定](#) (1007 ページ)
- [不明セキュリティ グループ](#) (1008 ページ)
- [セキュリティ グループの設定](#) (983 ページ)
- [セキュリティ グループ アクセス コントロール リストの設定](#)

送信元ツリー ビュー

送信元ツリー ビューには、簡潔で組織化された送信元 SGT のビューが折りたたまれた状態で表示されます。送信元 SGT を展開すると、選択した送信元 SGT に関連するすべての情報が含まれた内部テーブルを表示できます。このビューには、宛先 SGT にマッピングされている送信元 SGT のみが表示されます。特定の送信元 SGT を展開すると、この送信元 SGT にマッピングされているすべての宛先 SGT とその対応するポリシー (SGACL) がテーブルに表示されます。

一部のフィールドの隣に 3 個のドット (...) が表示されます。これは、セルにより多くの情報が含まれていることを示しています。カーソルを 3 個のドットの上に置くと、クイックビューポップアップに残りの情報が表示されます。カーソルを SGT 名または SGACL 名の上に置くと、クイック ビュー ポップアップが開き、その特定の SGT または SGACL の内容が表示されます。

宛先ツリー ビュー

宛先ツリー ビューには、簡潔で組織化された宛先 SGT のビューが折りたたまれた状態で表示されます。宛先 SGT を展開すると、選択した宛先 SGT に関連するすべての情報が含まれた内部テーブルを表示できます。このビューには、送信元 SGT にマッピングされている宛先 SGT のみが表示されます。特定の宛先 SGT を展開すると、この宛先 SGT にマッピングされているすべての送信元 SGT と対応するポリシー (SGACL) が表に示されます。

一部のフィールドの隣に 3 個のドット (...) が表示されます。これは、セルにより多くの情報が含まれていることを示しています。カーソルを 3 個のドットの上に置くと、クイックビューポップアップに残りの情報が表示されます。カーソルを SGT 名または SGACL 名の上に置くと、クイック ビュー ポップアップが開き、その特定の SGT または SGACL の内容が表示されます。

マトリクス ビュー

出力ポリシーのマトリクスビューは、スプレッドシートに似ています。ここには2つの軸があります。

- 送信元軸：垂直軸にはすべての送信元 SGT がリストされます。
- 宛先軸：水平軸にはすべての宛先 SGT がリストされます。

送信元 SGT と宛先 SGT のマッピングが、セルとして示されます。セルにデータが含まれている場合、対応する送信元 SGT と宛先 SGT 間にマッピングがあるということになります。マトリクス ビューには2つのタイプのセルがあります。

- マッピングされたセル：送信元 SGT と宛先 SGT のペアが、順序付けされた SGACL のセットに関連付けられ、特定のステータスになっている場合。
- マッピングされていないセル：送信元 SGT と宛先 SGT のペアが、SGACL に関連付けられてなく、特定のステータスになっていない場合。

出力ポリシー セルには、送信元 SGT、宛先 SGT、最終的な catch-all ルールが1つのリストとして SGACL の下にカンマで区切られて表示されます。最終的な catch-all ルールは、[なし (None)] に設定されている場合には表示されません。マトリクス内の空のセルは、マッピングされていないセルを示します。

出力ポリシーのマトリクスビューでは、マトリクスをスクロールして目的のセルのセットを表示できます。ブラウザがマトリクスデータ全体を一度にロードすることはありません。ブラウザは、ユーザがスクロールした領域に移入されるデータをサーバに要求します。これにより、メモリのオーバーフローとパフォーマンスの問題が回避されます。

[表示 (View)] ドロップダウン リストで次のオプションを使用して、マトリクス ビューを変更できます。

- [SGACL名ありで簡易設定 (Condensed with SGACL names)]：このオプションを選択すると、空のセルは非表示になり、SGACL 名がセルに表示されます。
- [SGACL名なしで簡易設定 (Condensed without SGACL names)]：空のセルは非表示になり、SGACL 名はセルに表示されません。このビューは、より多くのマトリクス セルを表示し、色、パターンおよびアイコン (セルのステータス) を使用して、セルの内容を区別する場合に便利です。
- [SGACL名ありでフル (Full with SGACL names)]：このオプションを選択すると、左側と上側のメニューは非表示になり、SGACL 名がセルに表示されます。
- [SGACL名なしでフル (Full without SGACL names)]：このオプションを選択すると、マトリクスは全画面モードで表示され、SGACL 名はセルに表示されません。

ISE では、カスタムビューを作成し、名前を付け、保存できます。カスタムビューを作成するには、[表示 (Show)] > [カスタムビューの作成 (Create Custom View)] の順に選択します。また、ビューの条件を更新したり、未使用のビューを削除することもできます。

[マトリックス (Matrix)] ビューは、[ソース (Source)] ビューおよび [送信先 (Destination)] ビューと同じ GUI 要素を持っています。ただし、次の追加要素を含みます。

関連トピック

[マトリクス操作](#) (993 ページ)

マトリクスの次元

次元ビューの [次元 (Dimension)] ドロップダウン リストでは、マトリクスの次元を設定することができます。

マトリクスのインポート/エクスポート

[インポート (Import)] および [エクスポート (Export)] ボタンを使用すると、マトリクスをインポートまたはエクスポートできます。

カスタム ビューの作成

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 [マトリックスビュー (Matrix View)] ページで、[表示 (Show)] ドロップダウン リストから [カスタム ビューの作成 (Create Custom View)] オプションを選択します。

ステップ 2 [ビューの編集 (Edit View)] ダイアログボックスで、次の詳細情報を入力します。

- [ビュー名 (View Name)] : カスタム ビューの名前を入力します。
- [送信元セキュリティグループ (Source Security Groups)] : カスタム ビューに含める SGT を [表示 (Show)] 転送ボックスに移動します。
- [着信先関連の表示 (Show Relevant for Destination)] : [送信元セキュリティグループの表示 (Source Security Group Show)] 転送ボックスの選択内容を上書きして、[着信先セキュリティグループの非表示 (Destination Security Group Hide)] 転送ボックスのすべてのエントリをコピーするには、このチェックボックスをオンにします。200を超えるエントリがある場合、データはコピーされず、警告メッセージが表示されます。
- [着信先セキュリティグループ (Destination Security Groups)] : カスタム ビューに含める SGT を [表示 (Show)] 転送ボックスに移動します。
- [送信元関連の表示 (Show Relevant for Source)] : [着信先セキュリティグループの表示 (Destination Security Group Show)] 転送ボックスの選択内容を上書きして、[送信元セキュリティグループの非表示 (Source Security Group Hide)] 転送ボックスのすべてのエントリをコピーするには、このチェックボックスをオンにします。
- [次によってマトリクスをソートする (Sort Matrix By)] : 次のいずれかのオプションを選択します。
 - 手動順序 (Manual Order)
 - タグ番号 (Tag Number)

- SGT名 (SGT Name)

ステップ3 [保存 (Save)] をクリックします。

マトリクス操作

マトリクスでの移動

カーソルでマトリクス コンテンツ領域をドラッグするか、または水平および垂直スクロールバーを使用して、マトリクス内を移動できます。セルをクリックしたままにし、マトリクスコンテンツ全体を任意の方向にドラッグできます。送信元および宛先のバーがセルと一緒に移動します。セルを選択すると、マトリクスビューによってそのセルと対応する行 (送信元 SGT) およびカラム (宛先 SGT) が強調表示されます。選択したセルの座標 (送信元 SGT および宛先 SGT) がマトリクス コンテンツ領域の下に表示されます。

マトリクスでのセルの選択

マトリクスビューでセルを選択するには、該当のセルをクリックします。選択したセルが別の色で表示され、送信元 SGT および宛先 SGT が強調表示されます。セルをもう一度クリックするか、または別のセルを選択することで、セルの選択を解除できます。複数セルの選択は、マトリクスビューでは許可されていません。セルをダブルクリックして、セルの設定を編集します。

出力ポリシーの SGACL の設定

[出力ポリシー (Egress Policy)] ページでセキュリティ グループ ACL を直接作成できます。

ステップ1 [ワークセンター (Work Centers)] > [TrustSec] > [TrustSecポリシー (TrustSec Policy)] > [出力ポリシー (Egress Policy)] の順に選択します。

ステップ2 [送信元ツリービュー (Source Tree View)] または [宛先ツリービュー (Destination Tree View)] ページから、[設定 (Configure)] > [新しいセキュリティグループACLの作成 (Create New Security Group ACL)] を選択します。

ステップ3 必要な詳細を入力し、[送信 (Submit)] をクリックします。

ワーク プロセスの設定

始める前に

次のタスクを実行するには、スーパー管理者である必要があります。

ステップ 1 [ワーク センター (Work Centers)] > [TrustSec] > [設定 (Settings)] > [ワーク プロセスの設定 (Work Process Settings)] の順に選択します。

ステップ 2 次のオプションのいずれかを選択します。

- 単一マトリックス (Single Matrix) : TrustSec ネットワーク上のすべてのデバイスに対してポリシーマトリックスを 1 つのみ作成するには、このオプションを選択します。
- 複数マトリックス (Multiple Matrices) : さまざまなシナリオで複数のポリシーマトリックスを作成できるようにします。これらのマトリックスを使用して、さまざまなネットワークデバイスに異なるポリシーを展開できます。

(注) マトリックスは独立していて、各ネットワーク デバイスを 1 つのマトリックスのみに割り当てることができます。

- 承認プロセス付き実稼働およびステージングマトリックス (Production and Staging Matrices with Approval Process) : ワークフローモードを有効にするには、このオプションを選択します。エディタロールおよび承認者ロールに割り当てられるユーザを選択します。ユーザは、ポリシー管理者グループおよびスーパー管理者グループからのみ選択できます。ユーザはエディタロールおよび承認者ロールの両方に割り当ててはできません。

エディタまたは承認者ロールが割り当てられたユーザの電子メールアドレスが設定されていることを確認します。設定されていないと、ワークフロープロセスに関する電子メール通知がこれらのユーザに送信されません。

ワークフローモードを有効にすると、エディタのロールが割り当てられたユーザは、ステージングマトリックスを作成し、ステージングポリシーを展開するデバイスを選択して、承認者に承認を求めるステージングポリシーを送信できます。承認者ロールが割り当てられたユーザは、ステージングポリシーを確認し、要求を承認または拒否することができます。ステージングポリシーが承認者によって確認され、承認された後でのみ、ステージングポリシーを選択したネットワークデバイスに展開できます。

ステップ 3 DEFCON マトリックスを作成する場合は、[DEFCON を使用する (Use DEFCONS)] チェックボックスをオンにします。

DEFCONS マトリックスは、ネットワーク セキュリティ侵害の発生時に簡単に展開できるスタンバイ ポリシー マトリックスです。

重大度レベル[重大 (Critical)]、[深刻 (Severe)]、[実質的 (Substantial)]、および[適度 (Moderate)]の DEFCON マトリックスを作成できます。

DEFCON マトリックスがアクティブになると、対応する DEFCON ポリシーがすべての TrustSec ネットワーク デバイスにすぐに展開されます。ネットワーク デバイスから DEFCON ポリシーを削除するには、非アクティブ化オプションを使用できます。

ステップ 4 [保存 (Save)] をクリックします。

[マトリックス登録 (Matrices Listing)] ページ

TrustSec ポリシー マトリックスと DEFCON マトリックスは、[マトリックス登録 (Matrices Listing)] ページに表示されます ([ワークセンター (Work Centers)] > [TrustSec] > [TrustSec ポリシー (TrustSec Policy)] > [出力ポリシー (Egress Policy)] > [マトリックス登録 (Matrices List)])。各マトリックスに割り当てられているデバイスの数を確認することもできます。



(注) [マトリックス登録 (Matrices Listing)] ページは、単一マトリックス モードが有効であり、DEFCON マトリックス オプションが無効な場合は表示されません。

[マトリックス登録 (Matrices Listing)] ページからは、次のことが行えます。

- 新しいマトリックスの追加
- 既存のマトリックスの編集
- マトリックスの削除
- 既存のマトリックスの複製
- マトリックスへの NAD の割り当て

[NAD の割り当て (Assign NADs)] オプションを使用して、マトリックスに NAD を割り当てることができます。手順は次のとおりです。

1. [ネットワーク デバイスの割り当て (Assign Network Devices)] ウィンドウで、マトリックスに割り当てるネットワーク デバイスを選択します。フィルタ オプションを使用してネットワーク デバイスを選択することもできます。
2. [マトリックス (Matrix)] ドロップダウン リストから、マトリックスを選択します。既存のすべてのマトリックスとデフォルトのマトリックスがこのドロップダウン リストに表示されます。

デバイスをマトリックスに割り当てたら、[プッシュ (Push)] をクリックし、TrustSec の設定変更を該当するネットワーク デバイスに通知します。

[マトリックス登録 (Matrices Listing)] ページで作業を行うときは、次の点に注意してください。

- デフォルトのマトリックスを編集、削除、名前変更することはできません。
- 新しいマトリックスを作成する際は、空のマトリックスから開始することや、既存のマトリックスからポリシーをコピーすることができます。
- マトリックスを削除すると、そのマトリックスに割り当てられている NAD が自動的にデフォルトのマトリックスに移動します。
- 既存のマトリックスをコピーするとマトリックスのコピーが作成されますが、デバイスはコピーされたマトリックスに自動的に割り当てられません。

- 複数マトリックスモードでは、すべてのデバイスが初期段階でデフォルトのマトリックスに割り当てられます。
- 複数マトリックスモードでは、一部の SGACL がマトリックス間で共有されることがあります。この場合、SGACL コンテンツを変更すると、セルにその SGACL が含まれているすべてのマトリックスに影響します。
- 複数マトリックスは、ステージングが進行中のときに有効にすることはできません。
- 複数マトリックスモードから単一マトリックスモードに変更すると、すべての NAD が自動的にデフォルトのマトリックスに割り当てられます。
- 現在有効になっている場合は、DEFCON マトリックスを削除することはできません。

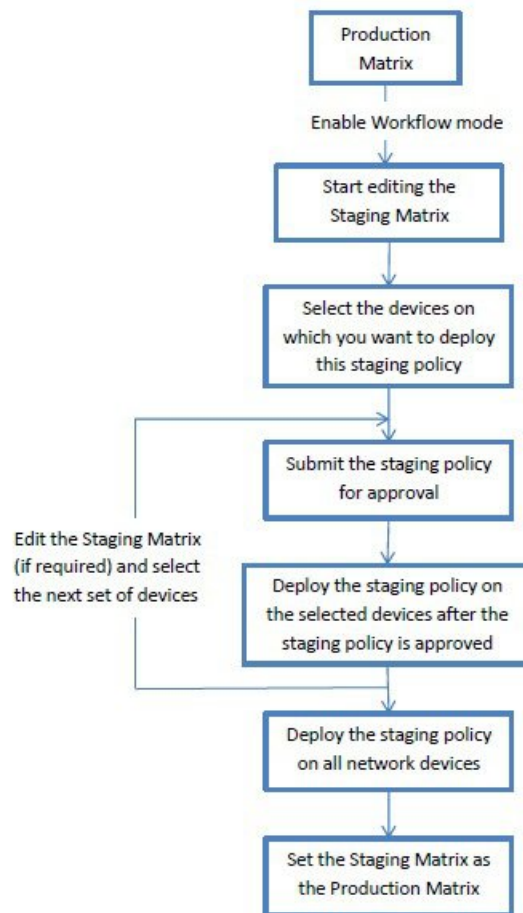
TrustSec マトリックス ワークフロー プロセス

マトリックスのワークフロー機能は、すべてのネットワーク デバイスにポリシーを導入する前に、このマトリックスのドラフト版（ステージング マトリックスとも呼ばれます）を使用して、デバイスの制限されたセットで新しいポリシーをテストできます。承認のためのステージング ポリシーを送信し、承認されると、選択したネットワーク デバイスにステージング ポリシーを導入できます。この機能により、必要に応じて、デバイスの制限されたセットへの新しいポリシーの導入、適切に機能しているかの確認、変更を行うことができます。次の一連のデバイスまたはすべてのデバイスにポリシーを適用し続けることもできます。ステージング ポリシーがすべてのネットワーク デバイスに導入されると、ステージング マトリックスは新たな実稼働マトリックスとして設定できます。

ワークフロー モードを有効にすると、エディタ ロールに割り当てられたユーザは、ステージング マトリックスを作成し、マトリックス セルを編集できます。ステージング マトリックスは、TrustSec ネットワークに現在展開されている実稼働マトリックスのコピーです。エディタは、ステージング ポリシーを展開し、承認のために承認者にステージング ポリシーを送信するデバイスを選択できます。承認者ロールが割り当てられたユーザは、ステージング ポリシーを確認し、要求を承認または拒否することができます。ステージング ポリシーが承認者によって確認され、承認された後でのみ、ステージング ポリシーを選択したネットワーク デバイスに展開できます。

次の図で、ワークフロー プロセスについて説明します。

図 58: マトリックス ワークフロー プロセス



上級管理ユーザは、ワークフロープロセスの設定ページ（[ワーク センター（Work Centers）] > [TrustSec] > [設定（Settings）] > [ワークフロー プロセス（Workflow Process）]）で、エディタおよび承認者ロールに割り当てられたユーザを選択できます。

ステージングポリシーが選択されたデバイスに導入された後では、SGTおよびSGACLを編集できませんが、マトリクスセルは編集できます。設定の差分レポートを使用して、実稼働マトリックスとステージングマトリックスの違いを追跡できます。また、ステージング処理中にそのセルへの変更を表示するには、セルで[デルタ（Delta）]アイコンをクリックします。

次の表では、ワークフローのさまざまな段階を説明します。

ステージ	説明
ステージングを編集中 (Staging in Edit)	エディタがステージングマトリックスの編集を開始すると、マトリックスは [ステージングを編集中 (Staging in Edit)] 状態に移行します。ステージング マトリックスを編集したら、エディタは、新しいステージング ポリシーを導入するデバイスを選択できます。
ステージングの承認待ち (Staging Awaiting Approval)	<p>マトリックスの編集後、エディタは確認および承認を受けるために承認者にステージング マトリックスを送信します。</p> <p>承認のためにステージング マトリックスを送信する時に、エディタは承認者に送信される電子メールにコメントを追加できます。</p> <p>承認者は、ステージング ポリシーを確認し、要求を承認または拒否することができます。承認者は、選択したネットワーク デバイスと設定の差分レポートを表示できます。要求の承認または拒否時に、承認者はエディタに送信される電子メールにコメントを追加できます。</p> <p>エディタはステージング ポリシーがどのネットワーク デバイスにも導入されていない場合は承認リクエストをキャンセルできます。</p>
展開の承認取得済み (Deploy Approved)	<p>承認者が要求を承認すると、ステージング マトリックスは [展開の承認取得済み (Deploy Approved)] 状態に移行します。要求が拒否された場合、マトリックスは [ステージングを編集中 (Staging in Edit)] 状態に戻されます。</p> <p>エディタはステージング ポリシーが承認者によって承認された後でのみ、ステージングポリシーを選択したネットワーク デバイスに導入できます。</p>

ステージ	説明
一部展開済み (Partially deployed)	<p>ステージング マトリックスが選択したデバイスに展開された後、マトリックスは [一部展開済み (Partially deployed)] 状態に移行します。マトリックスは、ステージングポリシーがすべてのネットワーク デバイスに導入されるまで、[一部展開済み (Partially deployed)] ステージのままです。</p> <p>このステージでは、SGT および SGACL を編集できませんが、マトリックス セルは編集できます。</p> <p>最新のポリシーが導入されていないデバイス (同期していないデバイス) は、[ネットワーク デバイスの導入 (Network Device Deployment)] ウィンドウにオレンジ色 (イタリック体) で表示されます。このステータスは、導入の進捗状況のステータス バーにも表示されます。エディタはこれらのデバイスを選択し、さまざまな導入サイクルで更新されたデバイスを同期するように承認を要求できます。</p>
完全に展開済み (Fully deployed)	<p>上記の手順は、ステージングポリシーがすべてのネットワーク デバイスに展開されるまで繰り返されます。ステージング マトリックスをすべてのネットワーク デバイスに展開する場合、承認者はステージング マトリックスを実稼働マトリックスとして設定できます。</p> <p>実稼働マトリックスをステージング マトリックスに置き換えた後では、実稼働マトリックスの以前のバージョンへのロールバックはできないため、新たな実稼働マトリックスとしてステージング マトリックスを設定する前に実稼働マトリックスのコピーを取得しておくことをお勧めします。</p>

[ワークフロー (Workflow)] ドロップダウンリストに表示されるオプションは、ワークフローの状態とユーザロール (エディタまたは承認者) によって異なります。次の表に、エディタおよび承認者に表示されるメニュー オプションを示します。

ワークフローの状態	エディタに表示されるメニュー	承認者に表示されるメニュー
ステージングを編集 (Staging in Edit)	<ul style="list-style-type: none"> ネットワークデバイスの選択 (Select network devices) 次のオプションが[ネットワーク デバイスの導入 (Network Device Deployment)]ウィンドウで使用できます。 <ul style="list-style-type: none"> 選択したデバイスの承認要求 (Request approval for selected devices) すべての/フィルタリングされたステージングリストの承認要求 (Request approval for all/filtered Staging list) すべての/フィルタリングされた実稼働リストの承認要求 (Request approval for all/filtered Production list) すべての/フィルタリングされたデバイスの承認要求 (Request approval for all/filtered devices) 選択したデバイスの承認要求 (Request approval for selected devices) ステージングの破棄 (Discard staging) デルタの表示 (View deltas) 	<ul style="list-style-type: none"> ネットワークデバイスの表示 (View network devices) デルタの表示 (View deltas)

ワークフローの状態	エディタに表示されるメニュー	承認者に表示されるメニュー
ステージングの承認待ち (Staging Awaiting Approval)	<ul style="list-style-type: none">承認要求のキャンセル (Cancel approval request)ネットワークデバイスの表示 (View network devices) 次のオプションが[ネットワーク デバイスの導入 (Network Device Deployment)]ウィンドウで使用できます。 <ul style="list-style-type: none">承認要求のキャンセル (Cancel approval request)デルタの表示 (View deltas)	<ul style="list-style-type: none">展開の承認 (Approve deploy)展開の拒否 (Reject deploy)ネットワークデバイスの表示 (View network devices) 次のオプションが[ネットワーク デバイスの導入 (Network Device Deployment)]ウィンドウで使用できます。 <ul style="list-style-type: none">展開の承認 (Approve deploy)展開の拒否 (Reject deploy) <ul style="list-style-type: none">デルタの表示 (View deltas)

ワークフローの状態	エディタに表示されるメニュー	承認者に表示されるメニュー
承認済み：展開の準備完了 (Approved - ready to deploy)	<ul style="list-style-type: none"> • [展開 (Deploy)] • 承認要求のキャンセル (Cancel approval request) • ネットワークデバイスの表示 (View network devices) <p>次のオプションが[ネットワーク デバイスの導入 (Network Device Deployment)]ウィンドウで使用できます。</p> <ul style="list-style-type: none"> • [展開 (Deploy)] • 承認要求のキャンセル (Cancel approval request) <ul style="list-style-type: none"> • デルタの表示 (View deltas) 	<ul style="list-style-type: none"> • 展開の拒否 (Reject deploy) • ネットワークデバイスの表示 (View network devices) <p>次のオプションが[ネットワーク デバイスの導入 (Network Device Deployment)]ウィンドウで使用できます。</p> <ul style="list-style-type: none"> • 展開の拒否 (Reject deploy) <ul style="list-style-type: none"> • デルタの表示 (View deltas)

ワークフローの状態	エディタに表示されるメニュー	承認者に表示されるメニュー
一部展開済み (Partially deployed)	<ul style="list-style-type: none"> ネットワークデバイスの選択 (Select network devices) 次のオプションが[ネットワーク デバイスの導入 (Network Device Deployment)]ウィンドウで使用できます。 <ul style="list-style-type: none"> 選択したデバイスの承認要求 (Request approval for selected devices) すべての/フィルタリングされたステージング リストの承認要求 (Request approval for all/filtered Staging list) すべての/フィルタリングされた実稼働 リストの承認要求 (Request approval for all/filtered Production list) すべての/フィルタリングされたデバイスの承認要求 (Request approval for all/filtered devices) 選択したデバイスの承認要求 (Request approval for selected devices) デルタの表示 (View deltas) 	<ul style="list-style-type: none"> ネットワークデバイスの表示 (View network devices) デルタの表示 (View deltas)

ワークフローの状態	エディタに表示されるメニュー	承認者に表示されるメニュー
完全に展開済み (Fully deployed)	<ul style="list-style-type: none"> ネットワークデバイスの選択 (Select network devices) 次のオプションが[ネットワーク デバイスの導入 (Network Device Deployment)]ウィンドウで使用できます。 <ul style="list-style-type: none"> 選択したデバイスの承認要求 (Request approval for selected devices) すべての/フィルタリングされたステージングリストの承認要求 (Request approval for all/filtered Staging list) すべての/フィルタリングされた実稼働リストの承認要求 (Request approval for all/filtered Production list) すべての/フィルタリングされたデバイスの承認要求 (Request approval for all/filtered devices) 選択したデバイスの承認要求 (Request approval for selected devices) デルタの表示 (View deltas) 	<ul style="list-style-type: none"> 実稼働として設定 (Set as production) ネットワークデバイスの表示 (View network devices) デルタの表示 (View deltas)

ワークフロー オプションは、[送信元ツリービュー (Source Tree View)]と[宛先ツリービュー (Destination Tree View)]でも使用できます。

TrustSec ポリシーのダウンロード レポート ([ワーク センター (Work Centers)] > [TrustSec] > [レポート (Reports)]) を使用して、ステージング/実稼働ポリシーをダウンロードしたデバイスのリストを表示できます。TrustSec ポリシーのダウンロードは、ポリシー (SGT/SGACL) のダウンロードのために、ネットワークデバイスによって送信された要求と ISE によって送信された詳細を示します。ワークフローモードを有効にしている場合、要求を実稼働マトリックスまたはステージング マトリックスに対してフィルタ処理することができます。

出力ポリシー テーブル セルの設定

Cisco ISE では、ツールバーで使用可能なさまざまなオプションを使用して、セルを設定できます。Cisco ISE では、選択した送信元 SGT および宛先 SGT がマッピングされたセルと同一である場合には、セルを設定できません。

関連トピック

[出力ポリシー セルのマッピングの追加](#) (1005 ページ)

[出力ポリシーの SGT の設定](#) (1007 ページ)

出力ポリシー セルのマッピングの追加

[ポリシー (Policy)] ページから出力ポリシーのマッピング セルを追加できます。

ステップ 1 [ワークセンター (Work Centers)] > [TrustSec] > [TrustSec ポリシー (TrustSec Policy)] > [出力ポリシー (Egress Policy)] の順に選択します。

ステップ 2 マトリックス セルを選択するには、次の手順を実行します。

- マトリックス ビューで、セルをクリックして選択します。
- 送信元ツリー ビューおよび宛先ツリー ビューで、内部テーブル内の行のチェックボックスをオンにして選択します。

ステップ 3 新しいマッピング セルを追加するには [追加 (Add)] をクリックします。

ステップ 4 次の項目について適切な値を選択します。

- 送信元セキュリティ グループ (Source Security Group)
- 宛先セキュリティ グループ (Destination Security Group)
- ステータス (Status) 、セキュリティ グループ ACL (Security Group ACLs)
- 最終的な catch-all ルール (Final Catch All Rule)

ステップ 5 [保存 (Save)] をクリックします。

出力ポリシーのエクスポート

ステップ 1 [ワーク センター (Work Centers)] > [TrustSec] > [TrustSec ポリシー (TrustSec Policy)] > [出力ポリシー (Egress Policy)] > [マトリックス (Matrix)] > [エクスポート (Export)] の順に選択します。

ステップ 2 エクスポートしたファイルに空のセル (SGACL が設定されていないセル) を含める場合は、[空のセルを含める (Include Empty Cells)] チェック ボックスにマークを付けます。

このオプションが有効になっている場合、マトリックス全体がエクスポートされ、空のセルは[SGACL]列に「空 (Empty)」キーワードでマークされます。

(注) エクスポートされたファイルに 500000 を超える行が含まれていないことを確認してください。そうでない場合、エクスポートが失敗する場合があります。

ステップ 3 次のオプションのいずれかを選択します。

- [ローカルディスク (Local Disk)] : ローカル ドライブにファイルをエクスポートする場合は、このオプションを選択します。
- [リポジトリ (Repository)] : リモート リポジトリにファイルをエクスポートする場合は、このオプションを選択します。

ファイルをエクスポートする前にリポジトリを設定する必要があります。リポジトリを設定するには、[管理 (Administration)] > [メンテナンス (Maintenance)] > [リポジトリ (Repository)] の順に選択します。読み取りおよび書き込みアクセス権が選択したリポジトリに提供されていることを確認します。

暗号キーを使用してエクスポートされたファイルを暗号化できます。

ファイル名は変更することができます。ファイル名は、50 文字以内でなければなりません。デフォルトでは、ファイル名には現在の時刻が含まれていますが、同じファイル名がリモート リポジトリに存在する場合は、ファイルが上書きされます。

ステップ 4 [エクスポート (Export)] をクリックします。

出力ポリシーのインポート

出力ポリシーをオフラインで作成し、Cisco ISE にインポートすることができます。セキュリティ グループ タグの数が多い場合、セキュリティ グループ ACL マッピングを 1 つずつ作成すると、時間がかかることがあります。代わりに、出力ポリシーをオフラインで作成し、Cisco ISE にインポートすることにより、時間を節約できます。インポート中、Cisco ISE は CSV ファイルのエントリを出力ポリシー マトリックスに追加し、データは上書きしません。

次の場合、出力ポリシーのインポートは失敗します。

- 送信元または宛先 SGT が存在しない
- SGACL が存在しない
- モニタ ステータスが、そのセルについて Cisco ISE で現在設定されているものと異なる

-
- ステップ 1** [ワークセンター (Work Centers)] > [TrustSec] > [TrustSecポリシー (TrustSec Policy)] > [出力ポリシー (Egress Policy)] > [マトリックス (Matrix)] > [インポート (Import)] の順に選択します。
- ステップ 2** [テンプレートの生成 (Generate a Template)] をクリックします。
- ステップ 3** [出力ポリシー (Egress Policy)] ページからテンプレート (CSV ファイル) をダウンロードし、CSV ファイルに次の情報を入力します。
- 送信元 SGT (Source SGT)
 - 宛先 SGT (Destination SGT)
 - SGACL
 - モニタ ステータス (有効、無効、またはモニタ対象)
- ステップ 4** インポートするポリシーで既存のポリシーが上書きされるようにする場合は、[新しいデータで既存のデータを上書き (Overwrite Existing Data with New Data)] チェックボックスをオンにします。空セル (「Empty」キーワードでマークされた、[SGACL] 列のセル) がインポートされたファイルに含まれていると、対応するマトリックスのセルの既存のポリシーが削除されます。
- イーグレス ポリシーをエクスポートする際に空セルを含めるには、[空のセルを含める (Include Empty Cells)] チェックボックスをオンにします。詳細については、[出力ポリシーのエクスポート \(1006 ページ\)](#) を参照してください。
- ステップ 5** [ファイルの検証 (Validate File)] をクリックして、インポートされたファイルを検証します。Cisco ISE は、ファイルをインポートする前に CSV 構造、SGT 名、SGACL、およびファイル サイズを検証します。
- ステップ 6** エラーが発生した場合にインポートを中止するには、[最初のエラーでインポートを停止 (Stop Import on First Error)] チェックボックスをオンにします。
- ステップ 7** [インポート (Import)] をクリックします。
-

出力ポリシーの SGT の設定

[出力ポリシー (Egress Policy)] ページでセキュリティ グループを直接作成できます。

-
- ステップ 1** [ワークセンター (Work Centers)] > [TrustSec] > [TrustSecポリシー (TrustSec Policy)] > [出力ポリシー (Egress Policy)] の順に選択します。
- ステップ 2** [送信元ツリービュー (Source Tree View)] または [宛先ツリービュー (Destination Tree View)] ページから、[設定 (Configure)] > [新しいセキュリティグループの作成 (Create New Security Group)] を選択します。
- ステップ 3** 必要な詳細を入力し、[送信 (Submit)] をクリックします。
-

モニタ モード

出力ポリシーの[すべてをモニタ (Monitor All)] オプションを使用すると、出力ポリシー設定ステータス全体を 1 回のクリックでモニタ モードに変更できます。[出力ポリシー (egress policy)] ページの[すべてをモニタ (Monitor All)] チェックボックスをオンにして、すべてのセルの出力ポリシー設定ステータスをモニタ モードに変更します。[すべてをモニタ (Monitor All)] チェックボックスをオンにすると、設定ステータスが次のように変更されます。

- ステータスが [有効 (Enabled)] であるセルはモニタ対象として動作しますが、有効であるかのように表示されます。
- ステータスが [無効 (Disabled)] であるセルは何も影響を受けません。
- ステータスが [モニタ (Monitor)] であるセルは、[モニタ対象 (Monitored)] のままになります。

[すべてをモニタ (Monitor All)] チェックボックスをオフにすると、元の設定ステータスに戻ります。データベース内の実際のセルのステータスは変更されません。[すべてをモニタ (Monitor All)] をオフにすると、出力ポリシーのそれぞれのセルが元の設定ステータスに戻ります。

モニタ モードの機能

モニタ モードのモニタリング機能は次の操作に役立ちます。

- フィルタリングされているけれども、モニタモードではモニタされているトラフィックの量の確認
- SGT-DGT ペアがモニタ モードであるか強制モードであるかの確認と、ネットワーク内で異常なパケット ドロップが発生していないかどうかの観察
- SGACL ドロップが実際に強制モードによって強制されているのか、またはモニタ モードによって許可されているのかの確認
- モードのタイプ (モニタ、強制、または両方) に基づいたカスタム レポートの作成
- NAD に適用されている SGACL、および表示の不一致 (ある場合) の識別

関連トピック

[ユーザ レポート別上位 N 個の RBACL ドロップの実行 \(1028 ページ\)](#)

不明セキュリティ グループ

不明セキュリティ グループは事前に設定されているセキュリティ グループで、変更不可能であり、タグ値 0 の TrustSec を表します。

Cisco セキュリティ グループのネットワーク デバイスは、送信元または宛先のいずれかの SGT がない場合に不明 SGT を参照するセルを要求します。送信元のみが不明の場合、要求は <不明, 宛先 SGT> セルに適用されます。宛先のみが不明の場合、要求は <送信元 SGT, 不明> セルに適用されます。送信元および宛先の両方が不明の場合、要求は <不明, 不明> セルに適用されます。

デフォルト ポリシー

デフォルト ポリシーは、<ANY,ANY> セルを参照します。任意の送信元 SGT が任意の宛先 SGT にマッピングされています。ここでは、ANY SGT は変更不可能であり、送信元 SGT にも宛先 SGT にも表示されません。ANY SGT は ANY SGT とのみペアにできます。他の SGT とはペアにできません。TrustSec ネットワーク デバイスでは、デフォルト ポリシーを特定セルのポリシーの最後に付加します。

- つまり、セルが空白の場合は、デフォルト ポリシーのみが含まれることになります。
- セルにポリシーが含まれる場合、結果のポリシーは、セル固有のポリシーとその後に続くデフォルト ポリシーの組み合わせになります。

Cisco ISE では、セル ポリシーおよびデフォルト ポリシーは 2 つの別々の SGACL セットになり、デバイスは 2 つの別々のポリシー クエリーの応答としてこれらのセットを取得します。

デフォルト ポリシーの設定は、他のセルと次の点で異なります。

- ステータスは [有効 (Enabled)] または [モニタ対象 (Monitored)] の 2 つの値しかとることができません。
- セキュリティ グループ ACL は、デフォルト ポリシーでは任意のフィールドであるため、空白のままにできます。
- 最終的な catch-all ルールは次のいずれかになります。許可 IP、拒否 IP、許可 IP ログ、または拒否 IP ログ。デフォルト ポリシーを上回る安全策はないため、ここで [なし (None)] オプションを使用できないことは明らかです。

[プッシュ (Push)] ボタン

出力ポリシーの [プッシュ (Push)] オプションは CoA 通知を開始します。この通知は、Cisco ISE からの出力ポリシー設定変更に関する更新を、ただちに要求するよう TrustSec デバイスに伝えます。

関連トピック

[SGT マトリクスの更新 CoA のフロー](#) (1019 ページ)

SGT の割り当て

Cisco ISE では、デバイスのホスト名または IP アドレスがわかっている場合に、TrustSec デバイスに SGT を割り当てることができます。特定のホスト名または IP アドレスを持つデバイスがネットワークに参加すると、Cisco ISE によって認証前に SGT が割り当てられます。

次の SGT がデフォルトで作成されています。

- SGT_TrustSecDevices
- SGT_NetworkServices
- SGT_Employee

- SGT_Contractor
- SGT_Guest
- SGT_ProductionUser
- SGT_Developer
- SGT_Auditor
- SGT_PointofSale
- SGT_ProductionServers
- SGT_DevelopmentServers
- SGT_TestServers
- SGT_PCIServers
- SGT_BYOD
- SGT_Quarantine

セキュリティ グループ タグをエンドポイントにマップするようにデバイスを手動で設定する必要がある場合もあります。このマッピングは[セキュリティ グループ マッピング (Security Group Mappings)] ページから作成できます。この操作を実行する前に、SGT の範囲が予約済みであることを確認します。

ISE では、最大 10,000 の IP-to-SGT マッピングを作成できます。IP-to-SGT マッピング グループを作成して、このような大規模なマッピングを論理的にグループ化することができます。各 IP-to-SGT マッピング グループには、IP アドレスのリスト、マップ先の単一のセキュリティ グループ、およびこれらのマッピングの展開対象であるネットワーク デバイスまたはネットワーク デバイス グループが含まれています。

NDAC 許可

デバイスに SGT を割り当てることで TrustSec ポリシーを設定できます。TrustSec デバイスの ID 属性に基づいて、デバイスにセキュリティ グループを割り当てることができます。

関連トピック

[TrustSec のグローバル設定](#) (978 ページ)


[TrustSec AAA サーバの設定](#) (982 ページ)

NDAC 許可の設定

始める前に

- ポリシーで使用するためのセキュリティ グループを作成します。
- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

- ステップ 1** [ワークセンター (Work Centers)] > [TrustSec] > [TrustSecポリシー (TrustSec Policy)] > [ネットワークデバイス許可 (Network Device Authorization)] の順に選択します。
- ステップ 2** [デフォルトルール (Default Rule)] 行の右側にある [操作 (Action)] アイコンをクリックし、[新規行を上] に挿入 (Insert New Row Above)] をクリックします。
- ステップ 3** このルールの名前を入力します。
- ステップ 4** [条件 (Conditions)] の隣にあるプラス記号 (+) をクリックして、ポリシー条件を追加します。
- ステップ 5** [新しい条件の作成 (高度なオプション) (Create New Condition (Advance Option))] をクリックすると、新しい条件を作成できます。
- ステップ 6** [セキュリティグループ (Security Group)] ドロップダウンリストから、この条件の評価が true になった場合に割り当てる SGT を選択します。
- ステップ 7** この行の [操作 (Action)] アイコンをクリックして、現在のルールの上または下に、デバイス属性に基づいた別のルールを追加します。このプロセスを繰り返して、TrustSec ポリシーに必要なすべてのルールを

作成できます。ルールをドラッグアンドドロップし、 アイコンをクリックすることでこれらの順序を変更できます。既存の条件を複製することもできますが、ポリシー名は必ず変更してください。

評価が true になる最初のルールによって、評価の結果が決まります。いずれのルールも一致しなかった場合、デフォルトルールが適用されます。デフォルトルールを編集して、いずれのルールも一致しなかった場合にデバイスに適用される SGT を指定できます。

- ステップ 8** [保存 (Save)] をクリックして TrustSec ポリシーを保存します。

ネットワーク デバイス ポリシーを設定した後に、TrustSec デバイスで認証を行おうとすると、デバイスはその SGT およびそのピアの SGT を取得し、関連するすべての詳細をダウンロードできるようになります。

エンドユーザの許可の設定

Cisco ISE では、許可ポリシー評価の結果としてセキュリティグループを割り当てることができます。このオプションを使用すると、ユーザおよびエンドポイントにセキュリティグループを割り当てることができます。

始める前に

- 許可ポリシーについての情報を参照してください。
- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

- ステップ 1** [ワークセンター (Work Centers)] > [TrustSec] > [承認ポリシー (Authorization Policy)] の順に選択します。
- ステップ 2** 新しい許可ポリシーを作成します。
- ステップ 3** 権限のセキュリティグループを選択します。

あるユーザまたはエンドポイントについて、この許可ポリシーで指定した条件が **true** の場合、このセキュリティグループがそのユーザまたはエンドポイントに割り当てられ、このユーザまたはエンドポイントによって送信されたすべてのデータ パケットにこの特定の SGT でタグが付けられます。

TrustSec の設定およびポリシー プッシュ

Cisco ISE では、許可変更 (CoA) がサポートされています。これを使用すると、Cisco ISE で TrustSec の設定およびポリシーの変更を TrustSec デバイスに通知でき、デバイスでは関連データの取得要求でこれに応答できるようになります。

CoA 通知では、TrustSec ネットワーク デバイスをトリガーし、環境 CoA またはポリシー CoA のいずれかを送信できます。

また、基本的に TrustSec CoA 機能をサポートしないデバイスに設定変更をプッシュできます。

関連トピック

[CoA でサポートされるネットワーク デバイス](#) (1012 ページ)

[環境 CoA 通知のフロー](#) (1014 ページ)

[SGACL コンテンツ更新のフロー](#) (1017 ページ)

[ポリシーの更新 CoA 通知のフロー](#) (1019 ページ)

[SGT マトリクスの更新 CoA のフロー](#) (1019 ページ)

[TrustSec CoA の概要](#) (1021 ページ)

CoA でサポートされるネットワーク デバイス

Cisco ISE は次のネットワーク デバイスに CoA 通知を送信します。

- 単一の IP アドレスを持つネットワーク デバイス (サブネットはサポートされません)
- TrustSec デバイスとして設定されているネットワーク デバイス
- CoA サポート対象として設定されているネットワーク デバイス

複数のセカンダリが存在する分散環境に Cisco ISE が展開されており、これらのセカンダリがそれぞれ異なるデバイス セットと相互運用している場合、CoA 要求は Cisco ISE プライマリ ノードからすべてのネットワーク デバイスに送信されます。そのため、TrustSec ネットワーク デバイスは、Cisco ISE プライマリ ノードで CoA クライアントとして設定されている必要があります。

デバイスは、Cisco ISE プライマリ ノードに CoA NAK または ACK を返します。ただし、ネットワーク デバイスからの次の TrustSec セッションは、ネットワーク デバイスが他の AAA 要求をすべて送信する Cisco ISE ノードに送信され、必ずしもプライマリ ノードに送信されるわけではありません。

非 CoA サポート デバイスへの設定変更のプッシュ

一部のプラットフォームでは、許可変更 (CoA) について Cisco ISE の「プッシュ」機能はサポートされていません。例: Nexus ネットワーク デバイスの一部のバージョン。この場合、ISE はネットワーク デバイスに接続し、ISE に対して更新された設定要求をデバイスがトリガーするようにします。これを行うために、ISE はネットワーク デバイスへの SSHv2 トンネルを開き、TrustSec ポリシーマトリックスのリフレッシュをトリガーするコマンドを送信します。この方法は、CoA プッシュをサポートするネットワーク プラットフォームでも実行できます。

-
- ステップ 1** [ワークセンター (Work Centers)] > [デバイス管理 (Device Administration)] > [ネットワークリソース (Network Resources)] > [ネットワークデバイス (Network Devices)] の順に選択します。
- ステップ 2** 必要なネットワーク デバイスの横にあるチェックボックスをオンにし、[編集 (Edit)] をクリックします。
- ネットワーク デバイスの名前、IP アドレス、RADIUS および TrustSec 設定が正しく設定されていることを確認します。
- ステップ 3** [高度な TrustSec 設定 (Advanced TrustSec Settings)] まで下にスクロールし、[TrustSec 通知および更新 (TrustSec Notifications and Updates)] セクションで、[デバイスに設定変更を送信 (Send configuration changes to device)] チェックボックスをオンにして [CLI (SSH) (CLI (SSH))] オプション ボタンをクリックします。
- ステップ 4** (任意) SSH キーを指定します。
- ステップ 5** デバイス インターフェイスのクレデンシャルを使用して IP-SGT マッピングを取得するには、この SGA デバイスに対して [セキュリティ グループ タグ マッピングの展開時にこのデバイスを含める (Include This Device When Deploying Security Group Tag Mapping Updates)] チェックボックスをオンにします。
- ステップ 6** EXEC モードでデバイス設定を編集する権限を持つユーザのユーザ名とパスワードを入力します。
- ステップ 7** (任意) 設定を編集できるデバイスの EXEC モードパスワードを有効にするためのパスワードを入力します。[表示 (Show)] をクリックして、このデバイスにすでに設定されている EXEC モードパスワードを表示できます。
- ステップ 8** ページの下部にある [送信 (Submit)] をクリックします。
-

ネットワーク デバイスは、TrustSec の変更をプッシュするように設定されました。Cisco ISE ポリシーを変更した後で、ネットワーク デバイスに新規設定を反映させるには、[プッシュ (Push)] をクリックします。

SSH キーの検証

SSH キーを使用してセキュリティを強化することもできます。Cisco ISE では、SSH キー検証機能によってこれをサポートします。

この機能を使用するには、Cisco ISE からネットワーク デバイスに SSHv2 トンネルを開いて、ネットワーク デバイスの独自の CLI を使用して SSH キーを取得します。このキーをコピーし、検証のために Cisco ISE に貼り付けます。SSH キーが誤っている場合、Cisco ISE は接続を終了します。

制限：現在、Cisco ISE が検証できるのは 1 つの IP のみです（IP の範囲、または IP 内のサブネットは検証できません）

始める前に

次のものがが必要です。

- ログイン クレデンシャル
- SSH キーを取得する CLI コマンド

（Cisco ISE とセキュアに通信できるようにするネットワーク デバイスのもの）

ステップ 1 ネットワーク デバイス上：

- Cisco ISE が SSH キー検証を使用して通信するネットワーク デバイスにログインします。
- デバイスの CLI を使用して SSH キーを表示します。

例：

Catalyst デバイスの場合、コマンドは次のとおりです。 `sho ip ssh`。

- 表示された SSH キーをコピーします。

ステップ 2 Cisco ISE ユーザ インターフェイスから、次の手順を実行します。

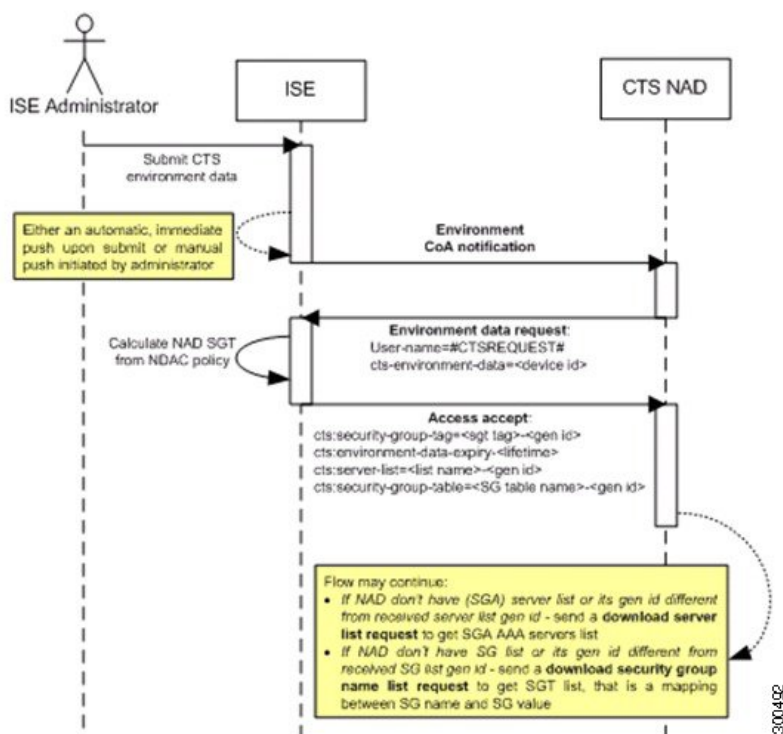
- [ワークセンター (Work Centers)] > [デバイス管理 (Device Administration)] > [ネットワークリソース (Network Resources)] > [ネットワークデバイス (Network Devices)] を選択し、必要なネットワーク デバイス名、IP アドレス、RADIUS および TrustSec 設定が正しく設定されていることを確認します。
- [高度な TrustSec 設定 (Advanced TrustSec Settings)] まで下にスクロールし、[TrustSec 通知および更新 (TrustSec Notifications and Updates)] セクションで、[デバイスに設定変更を送信 (Send configuration changes to device)] チェックボックスをオンにして [CLI (SSH) (CLI (SSH))] オプション ボタンをクリックします。
- [SSH キー (SSHKey)] フィールドに、ネットワーク デバイスから取得した SSH キーを貼り付けます。
- ページの下部にある [送信 (Submit)] をクリックします。

ネットワーク デバイスは、SSH キー検証を使用して Cisco ISE と通信するようになりました。

環境 CoA 通知のフロー

次の図は、環境 CoA 通知のフローを示しています。

図 59: 環境 CoA 通知のフロー



1. Cisco ISE は、TrustSec ネットワーク デバイスに環境 CoA 通知を送信します。
2. デバイスは、環境データ要求を返します。
3. 環境データ要求への応答で、Cisco ISE は次の情報を返します。

要求を送信したデバイスの環境データ：これには、（NDAC ポリシーから推測される）TrustSec デバイスの SGT およびダウンロード環境 TTL が含まれます。

TrustSec AAA サーバ リストの名前および生成 ID。

（複数の可能性がある）SGT テーブルの名前および生成 ID：これらのテーブルには SGT 名と SGT 値がリストされ、一緒に SGT の完全リストも保持されます。

4. デバイスが TrustSec AAA サーバ リストを保持していない場合、または生成 ID が受信した生成 ID と異なる場合、デバイスは別の要求を送信して、AAA サーバ リストの内容を取得します。
5. デバイスが応答にリストされている SGT テーブルを保持していない場合、または生成 ID が受信した生成 ID と異なる場合、デバイスは別の要求を送信して、その SGT テーブルの内容を取得します。

環境 CoA トリガー

環境 CoA は次のものに関して開始できます。

- ネットワーク デバイス
- セキュリティ グループ
- AAA サーバ

関連トピック

- [ネットワーク デバイスの環境 CoA のトリガー](#) (1016 ページ)
- [セキュリティ グループの環境 CoA のトリガー](#) (1016 ページ)
- [TrustSec AAA サーバの環境 CoA のトリガー](#) (1016 ページ)

ネットワーク デバイスの環境 CoA のトリガー

ネットワーク デバイスに関する環境 CoA をトリガーするには、次の手順を実行します。

ステップ 1 [管理 (Administration)] > [ネットワーク リソース (Network Resources)] > [ネットワーク デバイス (Network Devices)] | [ワーク センター (Work Centers)] > [デバイス管理 (Device Administration)] > [ネットワーク リソース (Network Resources)] > [ネットワーク デバイス (Network Devices)] を選択します。

ステップ 2 ネットワーク デバイスを追加または編集します。

ステップ 3 [高度な TrustSec 設定 (Advanced TrustSec Settings)] セクションで、[TrustSec 通知および更新 (TrustSec Notifications and Updates)] パラメータを更新します。

環境属性の変更は、変更が発生した特定の TrustSec ネットワーク デバイスにのみ通知されます。

単一のデバイスのみが影響を受けるため、環境 CoA 通知は送信直後に送信されます。結果として、そのデバイスの環境属性が更新されます。

セキュリティ グループの環境 CoA のトリガー

セキュリティ グループに関する環境 CoA をトリガーするには、次の手順を実行します。

ステップ 1 [ワークセンター (Work Centers)] > [TrustSec] > [コンポーネント (Components)] > [セキュリティグループ (Security Groups)] を選択します。

ステップ 2 [セキュリティ グループ (Security Group)] ページで、SGT の名前を変更します。これにより、その SGT のマッピング値の名前が変更されます。これで環境変更がトリガーされます。

ステップ 3 複数の SGT の名前を変更した後、[プッシュ (Push)] ボタンをクリックして、環境 CoA 通知を開始します。この環境 CoA 通知は、すべての TrustSec ネットワーク デバイスに送信され、変更されたすべての SGT の更新が提供されます。

TrustSec AAA サーバの環境 CoA のトリガー

TrustSec AAA サーバに関する環境 CoA をトリガーするには、次の手順を実行します。

-
- ステップ 1** [ワークセンター (Work Centers)] > [TrustSec] > [コンポーネント (Components)] > [TrustSec AAA サーバ (TrustSec AAA Servers)] を選択します。
- ステップ 2** [TrustSec AAA サーバ (TrustSec AAA Servers)] ページで、TrustSec AAA サーバの設定を作成、削除、または更新します。これで環境変更がトリガーされます。
- ステップ 3** 複数の TrustSec AAA サーバを設定した後、[プッシュ (Push)] ボタンをクリックして、環境 CoA 通知を開始します。この環境 CoA 通知は、すべての TrustSec ネットワーク デバイスに送信され、変更されたすべての TrustSec AAA サーバの更新を提供します。
-

NDAC ポリシーの環境 CoA のトリガー

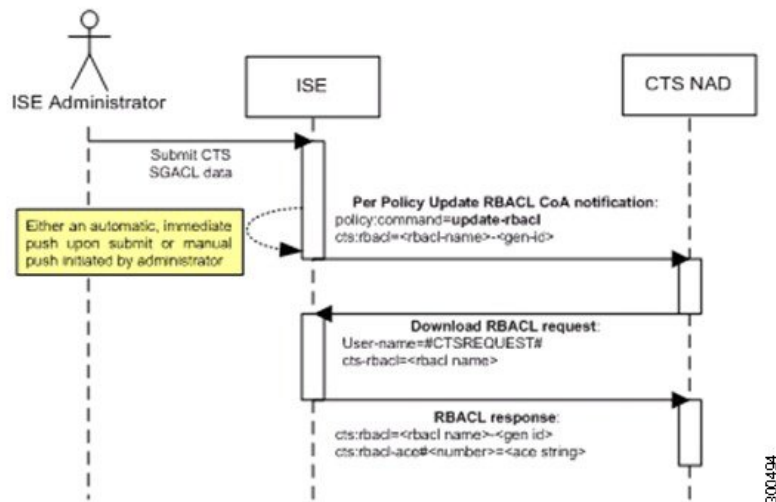
NDAC ポリシーに関する環境 CoA をトリガーするには、次の手順を実行します。

-
- ステップ 1** [ワークセンター (Work Centers)] > [TrustSec] > [ポリシー (Policy)] > [ネットワークデバイス許可 (Network Device Authorization)] の順に選択します。
- [NDAC ポリシー (NDAC policy)] ページで、NDAC ポリシーのルールを作成、削除、または更新できます。これらの環境変更は、すべてのネットワーク デバイスに通知されます。
- ステップ 2** [ワークセンター (Work Centers)] > [TrustSec] > [TrustSec ポリシー (TrustSec Policy)] > [ネットワークデバイス許可 (Network Device Authorization)] の順に選択します。
- [NDAC ポリシー (NDAC policy)] ページで、NDAC ポリシーのルールを作成、削除、または更新できます。これらの環境変更は、すべてのネットワーク デバイスに通知されます。
- ステップ 3** [NDAC ポリシー (NDAC policy)] ページで [プッシュ (Push)] ボタンをクリックすることで、環境 CoA 通知を開始できます。この環境 CoA 通知は、すべての TrustSec ネットワーク デバイスに送信され、ネットワーク デバイス自体の SGT の更新を提供します。
-

SGACL コンテンツ更新のフロー

次の図に、SGACL コンテンツ更新のフローを示します。

図 60: SGACL コンテンツ更新のフロー



1. Cisco ISE は、TrustSec ネットワーク デバイスに SGACL 名前付きリストの更新 CoA 通知を送信します。通知には、SGACL 名と生成 ID が含まれます。
2. デバイスは、次の両方の条件が満たされた場合に、SGACL データ要求で応答できます。

SGACL が、デバイスが保持する出力セルに含まれている場合。デバイスには出力ポリシーデータのサブセットが保持されます。これらは、そのネイバーデバイスおよびエンドポイントの SGT に関連するセルです（選択した宛先 SGT の出力ポリシー カラム）。

CoA 通知内の生成 ID が、この SGACL 用にデバイスが保持している生成 ID と異なっている。

3. SGACL データ要求への応答で、Cisco ISE は SGACL のコンテンツ（ACE）を返します。

SGACL 名前付きリストの更新 CoA の開始

SGACL 名前付きリストの更新 CoA をトリガーするには、次の手順を実行します。

- ステップ 1** [ワークセンター（Work Centers）]>[TrustSec]>[コンポーネント（Components）]>[セキュリティグループ ACL（Security Group ACLs）] を選択します。
- ステップ 2** SGACL のコンテンツを変更します。SGACL を送信すると、SGACL の生成 ID が変更されます。
- ステップ 3** 複数の SGACL のコンテンツを変更した後、[プッシュ（Push）] ボタンをクリックして、SGACL 名前付きリストの更新 CoA 通知を開始します。この通知は、すべての TrustSec ネットワーク デバイスに送信され、関連するデバイスのその SGACL コンテンツの更新が提供されます。

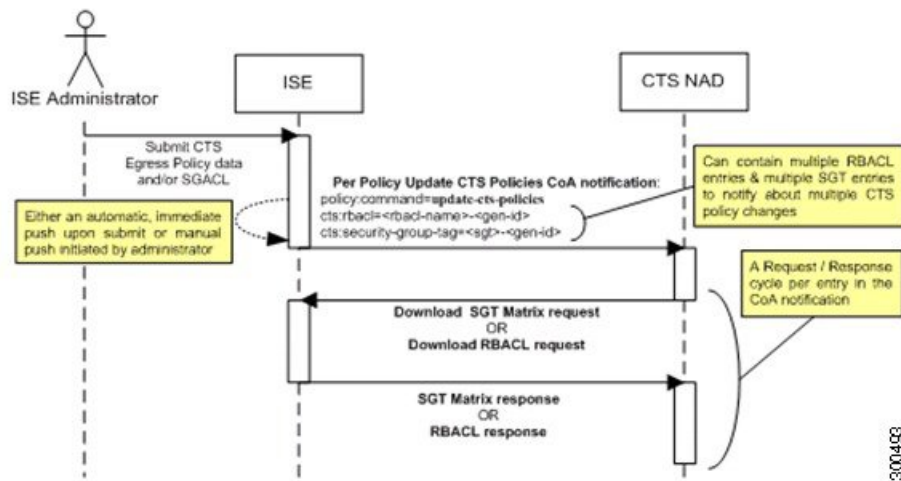
SGACL の名前または IP バージョンを変更しても、その生成 ID は変更されません。そのため、SGACL 名前付きリストの更新 CoA 通知を送信する必要はありません。

ただし、出力ポリシーで使用中の SGACL の名前または IP バージョンを変更することは、その SGACL を含むセルが変更されることを意味するため、この変更でそのセルの宛先 SGT の生成 ID が変更されます。

ポリシーの更新 CoA 通知のフロー

次の図に、ポリシーの CoA 通知のフローを示します。

図 61: ポリシーの CoA 通知のフロー

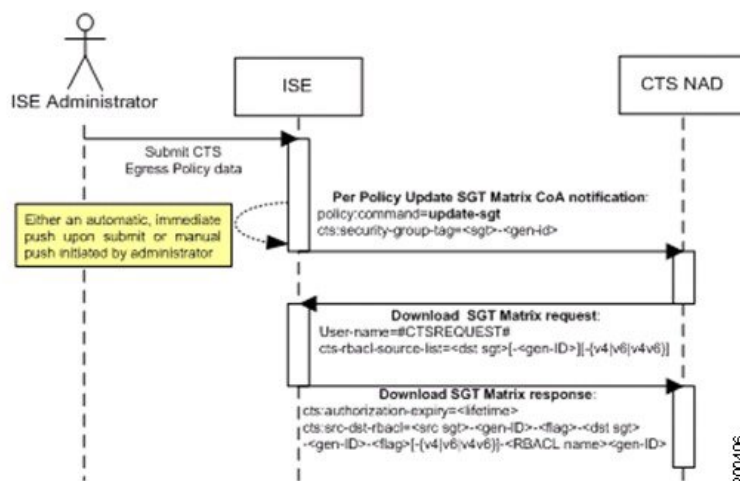


1. Cisco ISE は、TrustSec ネットワーク デバイスにポリシーの更新 CoA 通知を送信します。通知には、複数の SGACL 名とその生成 ID、および複数の SGT 値とその生成 ID が含まれることがあります。
2. デバイスは、複数の SGACL データ要求か複数の SGT データ、またはその両方で応答できます。
3. 各 SGACL データ要求または SGT データ要求に対する応答で、Cisco ISE は関連するデータを返します。

SGT マトリクスの更新 CoA のフロー

次の図に、SGT マトリクスの更新 CoA のフローを示します。

図 62: SGT マトリクスの更新 CoA のフロー



1. Cisco ISE は、TrustSec ネットワーク デバイスに SGT マトリクスの更新 CoA 通知を送信します。通知には、SGT 値と生成 ID が含まれます。
2. デバイスは、次の両方の条件が満たされた場合に、SGT データ要求で応答できます。
SGT がネイバーデバイスまたはエンドポイントの SGT である場合。デバイスは、ネイバーデバイスおよびエンドポイントの SGT に関連するセルをダウンロードして保持します（宛先 SGT）。
CoA 通知内の生成 ID が、この SGT 用にデバイスが保持している生成 ID と異なっている。
3. SGT データ要求に対する応答で、Cisco ISE は、送信元および宛先 SGT、セルのステータス、そのセルに設定されている SGACL 名の順序リストなど、すべての出力セルのデータを返します。

出力ポリシーからの、SGT マトリクスの更新 CoA の開始

-
- ステップ 1** [ワークセンター（Work Centers）] > [TrustSec] > [TrustSec ポリシー（TrustSec Policy）] > [出力ポリシー（Egress Policy）] の順に選択します。
- ステップ 2** [出力ポリシー（Egress Policy）] ページで、セルの内容（ステータス、SGACL）を変更します。
- ステップ 3** 変更を送信すると、そのセルの宛先 SGT の生成 ID が変更されます。
- ステップ 4** 複数の出力セルの内容を変更した後、[プッシュ（Push）] ボタンをクリックして、SGT マトリクスの更新 CoA 通知を開始します。この通知は、すべての TrustSec ネットワーク デバイスに送信され、関連するデバイスのセルの内容の更新が提供されます。
-

TrustSec CoA の概要

次の表に、TrustSec CoA の開始を要求するさまざまなシナリオ、各シナリオで使用される CoA のタイプ、および関連する UI ページの概要を示します。

表 59 : TrustSec CoA の概要

UI ページ	CoA をトリガーする操作	トリガー方法	CoA タイプ	送信先
ネットワーク デバイス (Network Device)	ページの [TrustSec] セクションでの環境 TTL の変更	TrustSec ネットワーク デバイスで正常に送信が行われたとき	環境	特定のネットワーク デバイス
TrustSec AAA サーバ (TrustSec AAA Server)	TrustSec AAA サーバの変更 (作成、更新、削除、順序変更)	[TrustSec AAA サーバ (TrustSec AAA servers)] リスト ページの [プッシュ (Push)] ボタンをクリックすると、累積された変更をプッシュできます。	環境	すべての TrustSec ネットワーク デバイス
セキュリティ グループ (Security Group)	SGT の変更 (作成、名前変更、削除)	[SGT] リスト ページの [プッシュ (Push)] ボタンをクリックすると、累積された変更をプッシュできます。	環境	すべての TrustSec ネットワーク デバイス
NDAC ポリシー (NDAC Policy)	NDAC ポリシーの変更 (作成、更新、削除)	[NDAC ポリシー (NDAC policy)] ページの [プッシュ (Push)] ボタンをクリックすると、累積された変更をプッシュできます。	環境	すべての TrustSec ネットワーク デバイス

UI ページ	CoA をトリガーする操作	トリガー方法	CoA タイプ	送信先
SGACL	SGACL ACE の変更	[SGACL] リストページの [プッシュ (Push)] ボタンをクリックすると、累積された変更をプッシュできます。	RBACL 名前付きリストの更新	すべての TrustSec ネットワーク デバイス
	SGACL 名または IP バージョンの変更	[SGACL] リストページの [プッシュ (Push)] ボタンまたは出力テーブルのポリシー プッシュ ボタンをクリックすると、累積された変更をプッシュできます。	更新 SGT マトリクス	すべての TrustSec ネットワーク デバイス
出力ポリシー (Egress Policy)	SGT の生成 ID を変更するすべての操作	[出力ポリシー (egress policy)] ページの [プッシュ (Push)] ボタンをクリックすると、累積された変更をプッシュできます。	更新 SGT マトリクス	すべての TrustSec ネットワーク デバイス

セキュリティ グループ タグの交換プロトコル

セキュリティ グループ タグ (SGT) の交換プロトコル (SXP) は、TrustSec のハードウェア サポートがないネットワーク デバイスに SGT を伝播するために使用されます。SXP は、ある SGT 対応ネットワーク デバイスから別のデバイスに IP アドレスとともにエンドポイントの SGT を転送するために使用されます。SXP が転送するデータは、IP-SGT マッピングと呼ばれます。エンドポイントが属する SGT は静的または動的に割り当てることができ、SGT はネットワーク ポリシーで分類子として使用できます。

SXP はトランスポート プロトコルとして TCP を使用して、2 つの個別のネットワーク デバイス間に SXP 接続をセットアップします。各 SXP 接続には、SXP スピーカーとして指定されたピアと、SXP リスナーとして指定されたピアがあります。ピアは双方向モードで設定することもでき、そのモードでは、それぞれがスピーカーとリスナーの両方として機能します。接続は

いずれかのピアによって開始できますが、マッピング情報は常にスピーカーからリスナーに伝播されます。



(注) セッションのバインディングは常にデフォルトの SXP ドメインに伝播されます。

次の表には、SXP 環境で使用される一般的な用語のいくつかを示しています。

IP-SGT マッピング	SXP 接続を介して交換される SGT マッピングへの IP アドレス。 SXP デバイスで学習されたすべてのマッピング（スタティック マッピングおよびセッションマッピングを含む）を表示するには、[ワークセンター（WorkCenters）] > [TrustSec] > [SXP] > [すべてのSXPマッピング（All SXP Mappings）] の順に選択します。
SXP スピーカー	SXP 接続を介して IP-SGT マッピングを送信するピア。
SXP リスナー	SXP 接続を介して IP-SGT マッピングを受信するピア。

Cisco ISE に追加された SXP ピア デバイスを表示するには、[ワークセンター（Work centers）] > [TrustSec] > [SXP] > [SXP デバイス（SXP Devices）] の順に選択します。



(注) SXP サービスはスタンドアロン ノードで実行することを推奨します。

SXP サービスを使用する際は、次の点に注意してください。

- Cisco ISE は、同じ IP アドレスを持つ複数の SXP セッションバインディングをサポートしていません。
- RADIUS アカウンティング更新の頻度が高すぎる（数秒に約 6 から 8 のアカウンティング更新）場合、アカウンティング更新パケットがドロップされる可能性があり、SXP が IP-SGT バインディングを受信できないことがあります。
- 以前のバージョンの ISE からアップグレードした後は、SXP は自動的に起動しません。アップグレード後に、SXP パスワードを変更し、SXP プロセスを再起動する必要があります。

SXP デバイスの追加

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 [ワークセンター (Work Centers)] > [TrustSec] > [SXP] > [SXPデバイス (SXP Devices)] の順に選択します。

ステップ 2 [追加 (Add)] をクリックします。

ステップ 3 デバイスの詳細を入力します。

- CSVファイルを使用して SXP デバイスを追加するには、[CSVファイルからアップロード (Upload from a CSV file)] をクリックします。CSV ファイルを参照して選択し、[アップロード (Upload)] をクリックします。

また、CSV テンプレートファイルをダウンロードして、追加するデバイスの詳細を入力し、CSV ファイルをアップロードすることもできます。

- 各 SXP デバイスのデバイスの詳細を手動で追加するには、[単一デバイスの追加 (Add Single Device)] をクリックします。

ピアデバイスの名前、IP アドレス、SXP ロール (リスナー、スピーカー、または両方)、パスワードタイプ、SXP バージョン、および接続されている PSN を入力します。また、ピアデバイスが接続されている SXP ドメインも指定する必要があります。

ステップ 4 (任意) [詳細設定 (Advanced Settings)] をクリックし、次の詳細を入力します。

- [最小許容ホールドタイマー (Minimum Acceptable Hold Timer)] : スピーカーが接続状態を保持するためにキープアライブ メッセージを送信する時間を秒単位で指定します。値の範囲は 1 ~ 65534 です。
- [キープアライブタイマー (Keep Alive Timer)] : アップデート メッセージによって他の情報がエクスポートされないインターバル期間にキープアライブ メッセージのディスパッチをトリガーするためにスピーカーによって使用されます。値の範囲は 0 ~ 64000 です。

ステップ 5 [保存 (Save)] をクリックします。

SXP ドメイン フィルタの追加

SXP デバイスで学習されたすべてのマッピング (スタティック マッピングおよびセッション マッピングを含む) は、[ワークセンター (Work Centers)] > [TrustSec] > [SXP] > [すべての SXP マッピング (All SXP Mappings)] ページで表示できます。

デフォルトでは、ネットワーク デバイスから学習されたセッション マッピングは、デフォルトの VPN グループにのみ送信されます。SXP ドメイン フィルタを作成して、異なる SXP ドメイン (VPN) にマッピングを送信できます。

SXP ドメイン フィルタを追加するには、次の手順を実行します。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 [ワーク センター (Work Centers)] > [TrustSec] > [SXP] > [すべての SXP マッピング (All SXP Mappings)] の順に選択します。

ステップ 2 [SXP ドメイン フィルタの追加 (Add SXP Domain Filter)] をクリックします。

ステップ 3 次の手順を実行します。

- サブネットの詳細を入力します。このサブネットからの IP アドレスを持つネットワーク デバイスのセッション マッピングは、[SXP ドメイン (SXP Domain)] フィールドで選択された SXP ドメイン (VPN) に送信されます。
- [SGT] ドロップダウンリストから SGT を選択します。この SGT に関連するセッションマッピングは、[SXP ドメイン (SXP Domain)] フィールドで選択された SXP ドメインに送信されます。
サブネットと SGT の両方を指定した場合、このフィルタに一致するセッション マッピングは、[SXP ドメイン (SXP Domain)] フィールドで選択した SXP ドメインに送信されます。
- マッピングを送信する必要がある SXP ドメインを選択します。

ステップ 4 [保存 (Save)] をクリックします。

SXP ドメインフィルタを更新または削除することもできます。フィルタを更新するには、[SXP ドメインフィルタの管理 (Manage SXP Domain Filter)] をクリックし、更新するフィルタの横にあるチェックボックスをオンにして、[編集 (Edit)] をクリックします。フィルタを削除するには、削除するフィルタの横にあるチェックボックスをオンにして、[ごみ箱 (Trash)] > [選択済み (Selected)] をクリックします。

SXP の設定

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 [ワークセンター (Work Centers)] > [TrustSec] > [設定 (Settings)] > [SXP設定 (SXP Settings)] の順に選択します。

ステップ 2 [SXP設定 (SXP Settings)] ページに必要な詳細を入力します。

[SXP バインディングを PxGrid で公開 (Publish SXP Bindings on PxGrid)] チェックボックスをオフにすると、IP-SGT マッピングはネットワーク デバイス全体に伝達されません。

ステップ 3 [保存 (Save)] をクリックします。

(注) SXP 設定が変更されると、SXP サービスが再起動されます。

TrustSec-ACI 統合

Cisco ISE では、SGT および SXP マッピングを内部エンドポイントグループ (IEPG)、外部エンドポイントグループ (EEPG)、シスコ アプリケーション セントリック インフラストラクチャ (ACI) のエンドポイント (EP) 設定と同期することができます。

Cisco ISE は、ISE で IEPG を同期して関連する読み取り専用 SGT を作成することで、ACI ドメインから TrustSec ドメインに着信するパケットをサポートします。これらの SGT は、ACI に設定されたエンドポイントをマッピングし、ISE で関連 SXP マッピングを作成するために使用されます。これらの SGT は [セキュリティグループ (Security Groups)] ページに表示されます ([学習元 (Learned From)] フィールドに値 [ACI] が入った状態で)。[すべての SXP マッピング (All SXP Mappings)] ページで SXP マッピングを表示できます。これらのマッピングは、[ACI の設定 (ACI Settings)] ページで [ポリシー プレーン (Policy Plane)] オプションが選択され、SXP デバイスが [ACI の設定 (ACI Settings)] ページで選択された SXP ドメインに属している場合にのみ、ACI に伝播されます。



(注) 読み取り専用 SGT は、IP-SGT マッピング、マッピング グループ、および SXP ローカル マッピングでは使用できません。

ACI に伝播される SGT を選択できます。セキュリティ グループを追加する際には、[ACI に伝播 (Propagate to ACI)] オプションを使用して、SGT を ACI に伝播する必要があるかどうかを指定できます。このオプションを有効にすると、この SGT に関連する SXP マッピングは、[ACI の設定 (ACI Settings)] ページで [ポリシー プレーン (Policy Plane)] オプションが選択され、SXP デバイスが [ACI の設定 (ACI Settings)] ページで選択した VPN に属する場合に ACI に伝播されます。

ACI は SGT を同期して関連する EEPG を作成することで、ACI ドメインから TrustSec ドメインに着信するパケットをサポートします。ACI は Cisco ISE から伝播された SXP マッピングに基づいて EEPG でサブネットを作成します。これらのサブネットは、対応する SXP マッピングが Cisco ISE で削除されるときに、ACI から削除されません。

IEPG が ACI で更新されると、対応する SGT 設定が Cisco ISE で更新されます。SGT が Cisco ISE に追加されると、新しい EEPG が ACI に作成されます。SGT が削除されると、対応する EEPG が ACI で削除されます。エンドポイントが ACI で更新されると、対応する SXP マッピングは Cisco ISE で更新されます。

ACI サーバとの接続が失われると、接続が再確立されるときに、Cisco ISE は再びデータを再同期します。



(注) ACI の統合機能を使用するには、SXP サービスを有効にする必要があります。

ACI の設定

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

- ステップ 1** 信頼できる証明書ストアに ACI 証明書をインポートします。[管理 (Administration)] > [システム (System)] > [証明書 (Certificates)] > [信頼できる証明書 (Trusted Certificates)] > [インポート (Import)] の順に選択し、証明書をインポートします。
- ステップ 2** [ワークセンター (Work Centers)] > [TrustSec] > [設定 (Settings)] > [ACI の設定 (ACI Settings)] の順に選択します。
- ステップ 3** [TrustSec-ACI ポリシー要素の交換 (TrustSec-ACI Policy Element Exchange)] チェックボックスをオンにして、SGT および SXP マッピングと ACI の IEPG、EEPG、エンドポイントの設定とを同期します。
- ステップ 4** 次のオプションのいずれかを選択します。
- [ポリシープレーン (Policy Plane)] : Cisco ISE が SGT、EPG、および SXP 情報を交換するために APIC データセンターだけとやりとりするようにするには、このオプションを選択します。
 - [データプレーン (Data Plane)] : このオプションを選択すると、TrustSec ネットワークと APIC 制御ネットワーク間で接続する ASR デバイスに対し、SGT と EPG 以外に追加情報が提供されます。これらの ASR デバイスには、SGT から EPG および EPG から SGT への変換のための変換テーブルが含まれている必要があります。
- (注) [データプレーン (Data Plane)] オプションを選択した場合、SXP マッピングは ACI に伝播されません。
- ステップ 5** [ポリシープレーン (Policy Plane)] オプションを選択した場合は、次の詳細を入力してください。
- IP アドレス/ホスト名 (IP address/Hostname) : ACI サーバの IP アドレスまたはホスト名を入力します。カンマで区切った 3 つの IP アドレスまたはホスト名を入力できます。
 - 管理者名/パスワード (Admin Name/Password) : ACI 管理ユーザのユーザ名とパスワードを入力します。
 - テナント (Tenant) : ACI で設定されているテナントの名前を入力します。
 - L3 ルートネットワーク名 (L3 Route Network Name) : ポリシー要素を同期させるために ACI で設定されているレイヤ 3 ルートネットワークの名前を入力します。
- [テスト設定 (Test Settings)] をクリックして、ACI サーバとの接続性を確認します。
- 新規 SGT サフィックス (New SGT Suffix) : このサフィックスは、ACI から学習された EPG に基づいて新規に作成された SGT に追加されます。
- (注) EPG 名が 32 文字を超える場合は切り捨てられます。ただし、[セキュリティグループ (Security Groups)] リストページの [説明 (Description)] フィールドで EPG のフルネーム、アプリケーションプロファイル名、SGT サフィックスの詳細を確認できます。

- 新規 EPG サフィックス (New EPG Suffix) : このサフィックスは、Cisco ISE から学習された SGT に基づいて ACI で新規に作成された EPG に追加されます。
- [SXP 伝達 (SXP Propagation)] 領域で、すべての SXP ドメインを選択するか、または ACI とマッピングを共有する SXP ドメインを指定することができます。

ステップ 6 [データ プレーン (Data Plane)] オプションを選択した場合は、次の詳細を入力してください。

- [SXP を使用して伝播 (Propagate using SXP)] : Cisco ISE に ACI からエンドポイント (EP) データを学習させ、SXP を使用して EP データを伝播させる場合は、このチェックボックスをオンにします。
(注) このオプションを選択する場合は、展開ノード ([管理 (Administration)] > [システム (System)] > [展開 (Deployment)]) で SXP サービスが有効になっていることを確認します。
- IP アドレス/ホスト名 (IP address/Hostname) : ACI サーバの IP アドレスまたはホスト名を入力します。カンマで区切った 3 つの IP アドレスまたはホスト名を入力できます。
- 管理者名/パスワード (Admin Name/Password) : ACI 管理ユーザのユーザ名とパスワードを入力します。
- テナント (Tenant) : ACI で設定されているテナントの名前を入力します。
[テスト設定 (Test Settings)] をクリックして、ACI サーバとの接続性を確認します。
- IEPG の最大数 (Max number of IEPGs) : SGT に変換される IEPG の最大数を指定します。IEPG はアルファベット順に変換されます。デフォルト値は 1000 です。
- SGT の最大数 (Max number of SGTs) : IEPG に変換される SGT の最大数を指定します。SGT はアルファベット順に変換されます。デフォルト値は 500 です。
- 新規 SGT サフィックス (New SGT Suffix) : このサフィックスは、ACI から学習された EPG に基づいて新規に作成された SGT に追加されます。
- 新規 EPG サフィックス (New EPG Suffix) : このサフィックスは、Cisco ISE から学習された SGT に基づいて ACI で新規に作成された EPG に追加されます。
- [タグなしパケットの EEPG 名 (EEPG name for untagged packets)] : EEPG に変換されない TrustSec パケットは、ACI でこの名前を使用してタグ付けされます。

ステップ 7 [保存 (Save)] をクリックします。

ユーザ レポート別上位 N 個の RBACL ドロップの実行

ユーザ レポート別上位 N 個の RBACL ドロップを実行して、特定のユーザによるポリシー違反 (パケット ドロップに基づく) を表示できます。

ステップ 1 [操作 (Operations)] > [レポート (Reports)] > [TrustSec] を選択します。

ステップ 2 [ユーザ別上位 N 個の RBACL ドロップ (Top N RBACL Drops by User)] をクリックします。

ステップ 3 [フィルタ (Filters)] ドロップダウン メニューから、必要なモニタ モードを追加します。

ステップ 4 選択したパラメータの値をこれに応じて入力します。[強制モード (Enforcement mode)] ドロップダウン リストから、[強制 (Enforce)]、[モニタ (Monitor)]、または[両方 (Both)] としてモードを指定できます。

ステップ 5 [時間範囲 (Time Range)] ドロップダウン メニューから、レポートデータを収集する期間を選択します。

ステップ 6 [実行 (Run)] をクリックして、選択したパラメータとともに特定の期間のレポートを実行します。

ユーザ レポート別上位 **N** 個の **RBACL** ドロップの実行



第 **VI** 部

Cisco ISE のモニタリングおよびトラブルシューティング

- [モニタリングおよびトラブルシューティング \(1033 ページ\)](#)
- [レポート \(1095 ページ\)](#)



第 28 章

モニタリングおよびトラブルシューティング

- [Cisco ISE のモニタリングとトラブルシューティング サービス \(1033 ページ\)](#)
- [モニタリングのためのデバイス設定 \(1039 ページ\)](#)
- [プロファイラ フィードのトラブルシューティング \(1039 ページ\)](#)
- [ポスチャ コンプライアンス \(1039 ページ\)](#)
- [Cisco ISE プロセスをモニタする SNMP トラップ \(1040 ページ\)](#)
- [Cisco ISE アラーム \(1042 ページ\)](#)
- [ログ収集 \(Log Collection\) \(1067 ページ\)](#)
- [ライブ認証 \(1068 ページ\)](#)
- [エンドポイントのグローバル検索 \(1070 ページ\)](#)
- [エンドポイントのセッションのトレース \(1071 ページ\)](#)
- [認証概要レポート \(1073 ページ\)](#)
- [診断トラブルシューティング ツール \(1074 ページ\)](#)
- [セッション トレース テスト ケース \(1077 ページ\)](#)
- [高度なトラブルシューティングのテクニカル サポートのトンネル \(1078 ページ\)](#)
- [着信トラフィックを検証する TCP ダンプ ユーティリティ \(1080 ページ\)](#)
- [モニタリング ノードからのエンドポイント統計データのダウンロード \(1084 ページ\)](#)
- [その他のトラブルシューティング情報の入手 \(1085 ページ\)](#)
- [モニタリング データベース \(1091 ページ\)](#)

Cisco ISE のモニタリングとトラブルシューティングサービス

モニタリングおよびトラブルシューティング サービスは、すべての Cisco ISE 実行時サービスを対象とした包括的なアイデンティティ ソリューションです。[操作 (Operations)] メニューには次のコンポーネントが表示されます。このメニューはプライマリ PAN からのみ表示できます。[操作 (Operations)] メニューはプライマリ モニタリング ノードには表示されません。

- **モニタリング**：ネットワーク上のアクセスアクティビティの状態を表す意味のあるデータのリアルタイム表示を提供します。これを把握することにより、操作の状態を簡単に解釈し、作用することができます。
- **トラブルシューティング**：ネットワーク上のアクセスの問題を解決するための状況に応じたガイダンスを提供します。また、ユーザの懸念に対応してタイムリーに解決策を提供できます。
- **レポート**：トレンドを分析し、システムパフォーマンスおよびネットワークアクティビティをモニタするために使用できる、標準レポートのカatalogを提供します。レポートをさまざまな方法でカスタマイズし、今後使用するために保存できます。次のフィールドのすべてのレポートで、ワイルドカードおよび複数値を使用してレコードを検索できます：[ID (Identity)]、[エンドポイントID (Endpoint ID)]、および [ISEノード (ISE Node)] (健全性の概要レポートは除く)。

ISE コミュニティ リソース

トラブルシューティングに関するテクニカルノートのリストについては、「[ISE Troubleshooting TechNotes](#)」を参照してください。

Cisco ISE ダッシュボード

Cisco ISE ダッシュボードまたはホームページ ([ホーム (Home)] > [概要 (Summary)]) は、Cisco ISE 管理コンソールにログインすると表示されるランディングページです。ダッシュボードは、ウィンドウの上部に沿って表示されるメトリックメーターと下にあるダッシュレットで構成された、集中化された管理コンソールです。デフォルトのダッシュボードは、[概要 (Summary)]、[エンドポイント (Endpoints)]、[ゲスト (Guests)]、[脆弱性 (Vulnerability)]、[脅威 (Threat)] です。



(注) ダッシュボードデータはプライマリ PAN にのみ表示されます。

ダッシュボードのリアルタイムデータによって、ネットワークにアクセスしているデバイスおよびユーザの一目で確認できるステータスと、システム健全性の概要が示されます。



(注) ダッシュレットと対応するすべてのドリルダウン ページを適切に表示するには、ブラウザに Adobe Flash Player がインストールされている必要があります。

[ダッシュボード設定 (Dashboard Settings)] では次のオプションを使用できます。

オプション	説明
新しいダッシュボードの追加 (Add New Dashboard)	<p>プラス記号をクリックするか、ページの右上にある [ダッシュボード設定 (Dashboard Settings)] をクリックすることで新しいダッシュボードを追加できます。</p> <p>(注) 5つのデフォルトのダッシュボードを含めて、最大で 20 個のダッシュボードを追加できます。</p>
ダッシュボードの名前の変更	<p>ダッシュボードの名前を変更するには、次の手順を実行します (カスタム ダッシュボードに対してのみ使用可能)。</p> <ol style="list-style-type: none">1. [ダッシュボード設定 (Dashboard Settings)] > [ダッシュボードの名前の変更 (Rename Dashboard)] の順に選択します。2. 新しい名前を指定します。3. [適用 (Apply)] をクリックします。
ダッシュレットの追加 (Add Dashlet)	<p>ダッシュレットを追加するには、次の手順を実行します。</p> <ol style="list-style-type: none">1. [ダッシュボード設定 (Dashboard Settings)] > [ダッシュレットの追加 (Add Dashlet(s))] の順に選択します。2. [ダッシュレットの追加 (Add Dashlets)] ウィンドウで、追加するダッシュレットに対して [追加 (Add)] をクリックします。3. [保存 (Save)] をクリックします。 <p>(注) ダッシュボードごとに最大で 9 個のダッシュレットを追加できます。</p>

オプション	説明
エクスポート (Export)	<p>ダッシュレットデータを PDF または CSV ファイルとしてエクスポートできます。</p> <p>手順は次のとおりです。</p> <ol style="list-style-type: none"> 1. Cisco ISE ホーム ページから必要なダッシュボード ([概要 (Summary)] など) を選択します。 2. [ダッシュボード設定 (Dashboard Settings)] > [エクスポート (Export)] の順に選択します。 3. [エクスポート (Export)] ダイアログボックスで、次のいずれかのファイル形式を選択します。 <ul style="list-style-type: none"> • 選択したダッシュレットのスナップショットを表示するには、PDF 形式を選択します。 • 選択したダッシュボードデータを ZIP ファイルとしてダウンロードするには、CSV 形式を選択します。 4. [ダッシュレット (Dashlets)] セクションで必要なダッシュレットを選択します。 5. [エクスポート (Export)] をクリックします。 <p>ZIP ファイルの名前は、選択したダッシュボードに基づいて指定されます (例: Summary.zip)。ZIP ファイルには、選択したダッシュボードの個々のダッシュレット CSV ファイルが含まれています。ダッシュレットの各タブに関連するデータは、対応するダッシュレット CSV ファイルで個別のセクションとして示されます。</p> <p>カスタム ダッシュボードをエクスポートする場合、ファイルは同じ名前でエクスポートされます。たとえば、MyDashboard という名前のカスタム ダッシュボードをエクスポートすると、エクスポートされたファイルの名前は MyDashboard となります。</p>

オプション	説明
レイアウト テンプレート (Layout Template)	<p>ダッシュレットが表示されるテンプレートのレイアウトを変更できます。</p> <p>レイアウトを変更するには、次の手順を実行します。</p> <ol style="list-style-type: none"> 1. [ダッシュボード設定 (Dashboard Settings)] > [レイアウト テンプレート (Layout Template)] の順に選択します。 2. 使用可能なオプションから目的のレイアウトを選択します。
ダッシュボードの管理	<p>[ダッシュボードの管理 (Manage Dashboards)] では次のオプションを使用できます。</p> <ul style="list-style-type: none"> • デフォルトのダッシュボードにする (Mark as Default Dashboard) : ダッシュボードをデフォルトダッシュボード (ホームページ) として設定するには、このオプションを使用します • すべてのダッシュボードのリセット (Reset all Dashboards) : すべてのダッシュボードを元の設定にリセットするには、このオプションを使用します

カスタム ダッシュボードの横にある閉じる (x) アイコンをクリックすることで作成したダッシュボードを削除できます。



(注) デフォルト ダッシュボードの名前を変更したり、削除することはできません。

すべてのダッシュレットには右上にツールバーがあり、次のオプションが含まれています。

1. 分離 (Detach) : 別のウィンドウにダッシュレットを表示します。
2. 更新 (Refresh) : ダッシュレットを更新します。
3. 削除 (Remove) : ダッシュボードからダッシュレットを削除します。

ダッシュレットの左上隅にあるグリッパアイコンを使用して、ダッシュレットをドラッグアンドドロップできます。

[アラーム (Alarms)] ダッシュレットのクイック フィルタ : [重大 (Critical)]、[警告 (Warning)]、[情報 (Info)] などの重大度に基づいてアラームをフィルタリングできます。
[アラーム (Alarms)] ダッシュレットはホームページに表示されます。このダッシュレットの

[フィルタ (Filter)] ドロップダウンには、重大度に基づいてアラームを検索するためのクイック フィルタが含まれています。

NPF イベント フロー プロセス

NPF 認証および許可イベントフローでは、次の表に記載されているプロセスが使用されます。

プロセス ステージ	説明
1	NADによって許可またはフレックス許可が実行されます。
2	未知のエージェントレス ID が Web 許可を使用してプロファイリングされます。
3	RADIUS サーバによってアイデンティティが認証および許可されます。
4	許可がポートでアイデンティティに対してプロビジョニングされます。
5	許可されないエンドポイント トラフィックはドロップされます。

モニタリングおよびトラブルシューティング機能のユーザロールと権限

モニタリングおよびトラブルシューティング機能は、デフォルトのユーザロールに関連付けられます。実行を許可されるタスクは、割り当てられているユーザ ロールに直接関係します。

モニタリング データベースに格納されているデータ

Cisco ISE モニタリング サービスでは、データが収集され、特化したモニタリング データベースに格納されます。ネットワーク機能のモニタリングに使用されるデータのレートおよび量によっては、モニタリング専用のノードが必要な場合があります。Cisco ISE ネットワークによって、ポリシー サービス ノードまたはネットワーク デバイスからロギングデータが高いレートで収集される場合は、モニタリング専用の Cisco ISE ノードを推奨します。

モニタリングデータベースに格納される情報を管理するには、データベースのフルバックアップおよび差分バックアップを実行する必要があります。これには、不要なデータの消去とデータベースの復元が含まれます。

関連トピック

[モニタリング データベース](#) (1091 ページ)

モニタリングのためのデバイス設定

モニタリング ノードにより、ネットワーク上のデバイスからのデータが受信および使用されて、ダッシュボードに表示されます。モニタリング ノードとネットワーク デバイスの間の通信を有効にするには、スイッチおよびネットワーク アクセス デバイス (NAD) を正しく設定する必要があります。

プロファイラ フィードのトラブルシューティング

テストが Cisco フィード サーバに接続できた場合は、テスト接続が成功したことを示すポップアップが表示されます。

接続に失敗した場合は、テスト ボタンの領域に、次の例のようなサーバからの応答が表示されます。メッセージの太字部分はメッセージの重要な部分を示します。

```
Test result: Failure: FeedService test connection failed : Feed Service unavailable : SocketTimeoutException
invoking https://ise.cisco.com:8443/feedserver/feed/serverinfo:
sun.security.validator.ValidatorException:PKIX path building failed:
Sun.security.provider.certpath.SunCertPathBuilderException Unable to find valid certification path to
requested target
```

考えられるエラー メッセージと実行すべきアクションを次に示します。

- 要求されたターゲットへの有効な認証パスを見つけることができません (Unable to find valid certification path to requested target) : フィードサーバが使用した証明書が無効です。Verisign 証明書がイネーブルになっていることを確認します。
- ホストへのルートがありません (No route to host) : ISE サーバから外部ネットワークへのアクティブな接続があるかを確認します。
- UnknownHostException (エラー メッセージの先頭) : ISE サーバから外部ネットワークへのアクティブな接続があるかを確認します。

ポスチャ コンプライアンス

ポスチャ コンプライアンス ダッシュレットは、ネットワークにアクセスしているユーザとそのユーザがポスチャ コンプライアンスに適合するかどうかに関する情報を示します。データは、現在ネットワークに接続されているデバイスに関して表示されます。積み上げ棒には、オペレーティングシステムやその他の基準に従って配置された非コンプライアンス統計情報が表示されます。スパークラインは、ポスチャ試行の準拠と非準拠のパーセンテージを表します。

ポスチャ コンプライアンスのチェック

ステップ 1 Cisco ISE ダッシュボードに進みます。

ステップ 2 [ポスチャ コンプライアンス (Posture Compliance)] ダッシュレットで、カーソルを積み上げ棒またはスパークラインに合わせます。

ツールチップに詳細情報が示されます。

ステップ 3 データ カテゴリを展開すると、詳細を参照できます。

ステップ 4 [ポスチャ コンプライアンス (Posture Compliance)] ダッシュレットを大きくします。

詳細なリアルタイム レポートが表示されます。

(注) [コンテキストの可視性 (Context Visibility)] ページにポスチャ コンプライアンス レポートを表示できます。[コンテキストの可視性 (Context Visibility)] ページ ([コンテキストの可視性 (Context Visibility)] > [エンドポイント (Endpoints)] > [コンプライアンス (Compliance)]) には、コンプライアンス ステータス、場所、エンドポイントのタイプ、およびステータストレンドに基づいてさまざまなチャートが表示されます。

Cisco ISE プロセスをモニタする SNMP トラップ

SNMP トラップは、Cisco ISE プロセスの状態を監視できます。Cisco ISE サーバにアクセスせずに、Cisco ISE プロセスをモニタする場合、Cisco ISE の SNMP ホストとして MIB ブラウザを設定できます。その後、MIB ブラウザから Cisco ISE プロセスのステータスを監視することもできます。

Cisco ISE は cron ジョブを使用してこれらのトラップをトリガーします。CLI から SNMP ホスト コマンドを設定した後、5 分ごとに cron ジョブを実行して Cisco ISE プロセスを監視します。最初の SNMP ホストの設定時に、Cisco ISE で実行されている各プロセスに対し、そのステータスとは関係なく、SNMP サーバでトラップを個別に受信していることがわかります。

設定済みの SNMP サーバが Cisco ISE から送信されたトラップを受信できることを確認できます。その後、トラップは Cisco ISE プロセス ステータスが増加した場合にのみ、Cisco ISE から送信されます。MIB ブラウザのトラップ レシーバを使用して SNMP トラップを表示できます。

Cisco ISE は、HOST-RESOURCES MIB に属している hrSWRunName の OID を使用してトラップを送信し、<PROCESS NAME> - <PROCESS STATUS> として OID 値を設定します。

たとえば、runtime - running。

Cisco ISE は、SNMPv1、SNMPv2c、および SNMPv3 をサポートします。

CLI から SNMP ホストを設定した場合は、Cisco ISE は次の汎用システム トラップを送信します。

- Cold start : デバイスをリブートするとき

- Linkup：イーサネット インターフェイスを起動するとき
- Linkdown：イーサネット インターフェイスをダウンするとき
- Authentication failure：コミュニティ スtring が一致しないとき

Cisco ISE は、次のステータスのトラップを設定済みの SNMP サーバに送信します。

- Process Start（監視状態）
- Process Stop（監視されていない状態）
- Execution Failed：プロセスの状態が「monitored」から「execution failed」に変更されるとトラップが送信されます。
- Does not exists：プロセスの状態が「monitored」から「does not exists」に変更されるとトラップが送信されます。
- Disk utilization：Cisco ISE のパーティションのディスク使用率がしきい値に到達したとき（設定された空きディスク領域の量に達するとトラップが送信されます）。

SNMP サーバで、すべてのオブジェクトについて一意のオブジェクト ID が生成され、値が OID に割り当てられます。SNMP サーバの OID 値でオブジェクトを検索できます。実行中のトラップの OID 値は「running」で、監視されないトラップ、存在しないトラップ、実行に失敗したトラップの OID 値は「stopped」です。

Cisco ISE が SNMP トラップを SNMP サーバに送信するのを停止させるには、Cisco ISE CLI から SNMP 設定を削除します。この操作によって、SNMP トラップの送信と、SNMP マネージャからのポーリングが停止されます。

snmp-server host および **snmp-server trap** コマンドの詳細については、『Cisco Identity Services Engine CLI Reference Guide』を参照してください。



- (注) ISE には、プロセス ステータスまたはディスク使用状況の MIB はありません。Cisco ISE は SNMP トラップの送信に OID HOST-RESOURCES-MIB::hrSWRunName を使用します。プロセス ステータスまたはディスク使用状況の照会には **snmp walk** または **snmp get** コマンドは使用できません。

OID	SNMP トラップ (SNMP Trap)
ディスク使用率の SNMP トラップ イベント	
1.3.6.1.4.1.2021.9.1.9	UCD_SNMP_OID:dskPercent
1.3.6.1.4.1.2021.9.1.2	UCD_SNMP_OID:dskPath
プロセス ステータスの SNMP トラップ通知	
1.3.6.1.2.1.25.4.2.1.2	HOST-RESOURCES-MIB:hrSWRunName

OID	SNMP トラップ (SNMP Trap)
通知イベントがデフォルトで通信されるその他の SNMP トラップ。詳細については、 http://oidref.com/1.3.6.1.6.3.1.1.5 を参照してください。	
1.3.6.1.6.3.1.1.5.1	ColdStart
1.3.6.1.6.3.1.1.5.5	AuthenticationFailure
ネットワークから Cisco ISE に送信される SNMP トラップ イベント	
1.3.6.1.6.3.1.1.5.3	linkUp イベント
1.3.6.1.6.3.1.1.5.4	linkDown イベント
1.3.6.1.2.1.11.0.3	Cisco Link Up イベント
1.3.6.1.2.1.11.0.2	Cisco Link Down イベント
1.3.6.1.4.1.9.9.215.2.0.1	Cisco Mac 変更通知
1.3.6.1.4.1.9.9.215.2.0.2	Cisco Mac 移動通知

Cisco Mac 変更通知 SNMP トラップ OID を使用して、MAC-Address、Timestamp、MacStatus、Vlan、および dot1dBasePort の各属性は、エンドポイントの作成に使用されます。

SNMP トラップ イベント CommandResponderEvent を使用して、ネットワーク デバイスのアドレスである peerAddress を読み取ることができます。CommandResponderEvent PDU コマンド変数から IfIndex、Vlan、および MAC-Address 属性を読み取り、これらを使用してネットワーク上で SNMP クエリを実行して CDP 属性を取得し、エンドポイントに追加することができます。

Cisco ISE アラーム

アラームは、ネットワークの重大な状態を通知し、[アラーム (Alarms)] ダッシュレットに表示されます。データ消去イベントなど、システムアクティビティの情報も提供されます。システムアクティビティについてどのように通知するかを設定したり、それらを完全に無効にしたりできます。また、特定のアラームのしきい値を設定できます。

大半のアラームには関連付けられているスケジュールがなく、イベント発生後即時に送信されます。その時点で最新の 15,000 件のアラームのみが保持されます。

イベントが繰り返し発生した場合、同じアラームは約 1 時間抑制されます。イベントが繰り返し発生する間は、トリガーに応じて、アラームが再び表示されるのに約 1 時間かかる場合があります。

次の表に、すべての Cisco ISE アラームおよびその説明と解決方法を示します。

表 60: Cisco ISE アラーム

アラーム名	アラームの説明	アラームの解決方法
管理および操作の監査の管理		
展開のアップグレードの失敗 (Deployment Upgrade Failure)	ISE ノードでアップグレードに失敗しました。	アップグレードが失敗した原因と修正措置について、失敗したノードの ADE ログを確認します。
アップグレードバンドルのダウンロードの失敗 (Upgrade Bundle Download failure)	アップグレードバンドルのダウンロードが ISE ノードで失敗しました。	アップグレードが失敗した原因と修正措置について、失敗したノードの ADE ログを確認します。
SXP 接続障害 (SXP Connection Failure)	SXP 接続に失敗しました。	SXP サービスが実行していることを確認します。ピアに互換性があることを確認します。
シスコプロファイルの全デバイスへの適用 (Cisco profile applied to all devices)	ネットワークデバイスプロファイルによって、MAB、Dot1X、CoA、Web Redirect などのネットワークアクセスデバイスの機能が定義されます。ISE 2.0 へのアップグレードにより、デフォルトのシスコネットワークデバイスプロファイルがすべてのネットワークデバイスに適用されました。	シスコ以外のネットワークデバイスの設定を必要に応じて編集し、適切なプロファイルを割り当てます。
CRL で失効した証明書が見つかったことによるセキュア LDAP 接続の再接続 (Secure LDAP connection reconnect due to CRL found revoked certificate)	CRL チェックの結果、LDAP 接続で使用された証明書が失効していることが検出されました。	CRL 設定が有効であることを確認します。LDAP サーバ証明書とその発行元の証明書が失効していないことを確認します。失効している場合は、新しい証明書を発行して LDAP サーバにインストールします。

アラーム名	アラームの説明	アラームの解決方法
OCSPで失効した証明書が見つかったことによるセキュア LDAP 接続の再接続 (Secure LDAP connection reconnect due to OCSP found revoked certificate)	OCSP チェックの結果、LDAP 接続で使用された証明書が失効していることが検出されました。	OCSP 設定が有効であることを確認します。LDAP サーバ証明書とその発行元の証明書が失効していないことを確認します。失効している場合は、新しい証明書を発行して LDAP サーバにインストールします。
CRL で失効した証明書が見つかったことによるセキュア syslog 接続の再接続 (Secure syslog connection reconnect due to CRL found revoked certificate)	CRL チェックの結果、syslog 接続で使用された証明書が失効していることが検出されました。	CRL 設定が有効であることを確認します。syslog サーバ証明書とその発行元の証明書が失効していないことを確認します。失効している場合は、新しい証明書を発行して syslog サーバにインストールします。
OCSPで失効した証明書が見つかったことによるセキュア syslog 接続の再接続 (Secure syslog connection reconnect due to OCSP found revoked certificate)	OCSP チェックの結果、syslog 接続で使用された証明書が失効していることが検出されました。	OCSP 設定が有効であることを確認します。syslog サーバ証明書とその発行元の証明書が失効していないことを確認します。失効している場合は、新しい証明書を発行して syslog サーバにインストールします。
管理者アカウントがロック/無効 (Administrator account Locked/Disabled)	パスワードの失効または不正なログイン試行のために、管理者アカウントがロックされているか、または無効になっています。詳細については、管理者パスワード ポリシーを参照してください。	管理者パスワードは、GUI または CLI を使用して、他の管理者によってリセットできます。
ERS が非推奨の URL を検出 (ERS identified deprecated URL)	ERS が非推奨の URL を検出しました。	要求された URL が非推奨であるため、使用しないでください。
ERS が古い URL を検出 (ERS identified out-dated URL)	ERS が古い URL を検出しました。	要求された URL が古いため、新しいものを使用してください。この URL は今後のリリースで削除されません。

アラーム名	アラームの説明	アラームの解決方法
ERS 要求 Content-Type ヘッダーが古い (ERS request content-type header is outdated)	ERS 要求 Content-Type ヘッダーが最新ではありません。	要求 Content-Type ヘッダーで指定された要求のリソースバージョンが最新ではありません。これはリソース スキーマが変更されたことを意味します。いくつかの属性が追加または削除された可能性があります。古いスキーマをこのまま処理するために、ERS エンジンでデフォルト値が使用されます。
ERS XML 入力が XSS またはインジェクション攻撃の原因です (ERS XML input is a suspect for XSS or Injection attack)	ERS XML 入力が XSS またはインジェクション攻撃の原因になっています。	XML 入力を確認してください。
バックアップに失敗 (Backup Failed)	ISE バックアップ操作に失敗しました。	Cisco ISE とリポジトリ間のネットワーク接続を確認します。次の点を確認します。 <ul style="list-style-type: none"> リポジトリに使用するクレデンシャルが正しいこと。 リポジトリに十分なディスク領域があること。 リポジトリ ユーザが書き込み特権を持っていること。
CA サーバがダウン (CA Server is down)	CA サーバがダウンしています。	CA サービスが CA サーバで稼働中であることを確認します。
CA サーバが稼働中 (CA Server is Up)	CA サーバは稼働中です。	CA サーバが稼働中であることを管理者に通知します。

アラーム名	アラームの説明	アラームの解決方法
証明書の有効期限 (Certificate Expiration)	この証明書はももなく有効期限が切れます。これが失効すると、Cisco ISE がクライアントとのセキュアな通信を確立しないようにします。	証明書を交換します。信頼できる証明書の場合、発行元の認証局 (CA) にお問い合わせください。CA 署名付きローカル証明書の場合、CSR を生成し、CA に新しい証明書を作成してもらいます。自己署名したローカル証明書の場合、Cisco ISE を使用して、有効期限を延長します。使用されなくなった場合、証明書を削除できます。
証明書が失効 (Certificate Revoked)	管理者は、内部 CA がエンドポイントに発行した証明書を取り消しました。	BYOD フローに従って最初から新しい証明書を使用してプロビジョニングします。
証明書プロビジョニング初期化エラー (Certificate Provisioning Initialization Error)	証明書プロビジョニングの初期化に失敗しました。	複数の証明書でサブジェクトの CN (CommonName) 属性が同じ値になっており、証明書チェーンを構築できません。SCEP サーバからそれらを含むシステムのすべての証明書を確認します。
証明書の複製に失敗 (Certificate Replication Failed)	セカンダリ ノードへの証明書の複製に失敗しました。	証明書がセカンダリ ノードで無効であるか、他の永続的なエラー状態があります。セカンダリ ノードに矛盾する証明書が存在しないかどうかを確認します。見つかった場合、セカンダリ ノードに存在するその証明書を削除し、プライマリの新しい証明書をエクスポートしてから削除し、その後インポートすることによって複製を再試行します。
証明書の複製に一時的に失敗 (Certificate Replication Temporarily Failed)	セカンダリ ノードへの証明書の複製に一時的に失敗しました。	証明書は、ネットワークの停止などの一時的な条件によりセカンダリ ノードに複製されませんでした。複製は、成功するまで再試行されます。

アラーム名	アラームの説明	アラームの解決方法
証明書が失効 (Certificate Expired)	この証明書の期限が切れています。Cisco ISE がクライアントとのセキュアな通信を確立しないようにします。ノードツーノード通信も影響を受ける場合があります。	証明書を交換します。信頼できる証明書の場合、発行元の認証局 (CA) にお問い合わせください。CA 署名付きローカル証明書の場合、CSR を生成し、CA に新しい証明書を作成してもらいます。自己署名したローカル証明書の場合、Cisco ISE を使用して、有効期限を延長します。使用されなくなった場合、証明書を削除できます。
証明書要求転送に失敗 (Certificate Request Forwarding Failed)	証明書要求転送に失敗しました。	受信する証明書要求が送信者からの属性に一致することを確認します。
設定が変更 (Configuration Changed)	Cisco ISE 設定が更新されています。このアラームは、ユーザとエンドポイントに設定変更があってもトリガーされません。	設定変更が想定どおりであるかどうかを確認します。
CRL の取得に失敗 (CRL Retrieval Failed)	サーバから CRL を取得できません。これは、指定した CRL が使用できない場合に発生することがあります。	ダウンロード URL が正しく、サービスに使用可能であることを確認します。
DNS 解決に失敗 (DNS Resolution Failure)	ノードで DNS 解決に失敗しました。	<p>コマンド ip name-server で設定した DNS サーバが到達可能であることを確認してください。</p> <p>「CNAME <hostname of the node> に対する DNS 解決が失敗しました (DNS Resolution failed for CNAME <hostname of the node>)」というアラームが表示された場合は、各 Cisco ISE ノードの A レコードとともに CNAME RR を作成できることを確認します。</p>

アラーム名	アラームの説明	アラームの解決方法
ファームウェアの更新が必要 (Firmware Update Required)	このホスト上でファームウェアの更新が必要です。	Cisco Technical Assistance Center に問い合わせてファームウェア アップデートを入手してください。
仮想マシン リソースが不十分 (Insufficient Virtual Machine Resources)	このホストでは、CPU、RAM、ディスク容量、IOPS などの仮想マシン (VM) リソースが不十分です。	Cisco ISE Hardware Installation Guide に指定されている VM ホストの最小要件を確認します。
NTP サービスの障害 (NTP Service Failure)	NTP サービスがこのノードでダウンしています。	これは、NTP サーバと Cisco ISE ノードとの間に大きな時間差 (1000 秒を超える) があるために発生することがあります。NTP サーバが正しく動作していることを確認し、 ntp server <servername> CLI コマンドを使用して NTP サービスを再起動して、時間を同期します。
NTP 同期に失敗 (NTP Sync Failure)	このノードに構成されているすべての NTP サーバが到達不能です。	CLI で show ntp コマンドを実行してトラブルシューティングを行います。Cisco ISE から NTP サーバに到達可能であることを確認します。NTP 認証が設定されている場合、キー ID と値がサーバの対応する値に一致することを確認します。
スケジュールされた設定バックアップなし (No Configuration Backup Scheduled)	Cisco ISE 設定バックアップがスケジュールされていません。	設定バックアップのスケジュールを作成します。
操作 DB 消去に失敗 (Operations DB Purge Failed)	操作データベースから古いデータを消去できません。このことは、M&T ノードがビジー状態である場合に発生する可能性があります。	[データ消去の監査 (Data Purging Audit)] レポートをチェックし、 used_space が threshold_space を下回ることを確認します。CLI を使用して M&T ノードにログインし、消去操作を手動で実行します。

アラーム名	アラームの説明	アラームの解決方法
プロファイラ SNMP 要求に失敗 (Profiler SNMP Request Failure)	SNMP 要求がタイムアウトしたか、または SNMP コミュニティまたはユーザ認証データが不正です。	SNMP が NAD で動作していることを確認し、Cisco ISE の SNMP 設定が NAD に一致していることを確認します。
複製に失敗 (Replication Failed)	セカンダリ ノードは複製されたメッセージを消費できませんでした。	Cisco ISE GUI にログインし、展開ページから手動同期を実行します。影響を受ける Cisco ISE ノードを登録解除してから登録します。
復元に失敗 (Restore Failed)	Cisco ISE 復元操作に失敗しました。	Cisco ISE とリポジトリ間のネットワーク接続を確認します。リポジトリに使用するクレデンシャルが正しいことを確認します。バックアップファイルが破損していないことを確認します。CLI で reset-config コマンドを実行して、正常な既知の最終バックアップを復元します。
パッチに失敗 (Patch Failure)	パッチ プロセスがサーバで失敗しました。	サーバにパッチ プロセスを再インストールします。
パッチに成功 (Patch Success)	パッチ プロセスがサーバで成功しました。	-
外部 MDM サーバ API バージョンが不一致 (External MDM Server API Version Mismatch)	外部 MDM サーバ API バージョンが Cisco ISE に設定されたものと一致しません。	MDM サーバ API バージョンが Cisco ISE に設定されたものと同じであることを確認します。Cisco ISE MDM サーバ設定を更新します (必要な場合)。
外部 MDM サーバ接続に失敗 (External MDM Server Connection Failure)	外部 MDM サーバへの接続に失敗しました。	MDM サーバが稼働し、Cisco ISE-MDM API サービスが MDM サーバで稼働していることを確認します。
外部 MDM サーバ応答エラー (External MDM Server Response Error)	外部 MDM サーバ応答エラーです。	Cisco ISE-MDM API サービスが MDM サーバで適切に動作していることを確認します。

アラーム名	アラームの説明	アラームの解決方法
複製が停止 (Replication Stopped)	ISE ノードが PAN から設定データを複製できませんでした。	Cisco ISE GUI にログインして展開ページから手動同期を実行するか、または影響を受けた ISE ノードを登録解除してから必須フィールドで再登録します。
エンドポイント証明書が期限切れ (Endpoint certificates expired)	エンドポイント証明書が日次スケジュールジョブで期限切れとマークされました。	エンドポイント デバイスを再登録して新しいエンドポイント証明書を取得してください。
エンドポイント証明書が消去 (Endpoint certificates purged)	期限切れのエンドポイント証明書が日次スケジュールジョブによって消去されました。	アクションは必要ありません。これは、管理者が開始したクリーンアップ操作です。
エンドポイントのアクティビティ消去 (Endpoints Purge Activities)	過去 24 時間のエンドポイントのアクティビティを消去します。このアラームは、真夜中にトリガーされます。	[操作 (Operations)] > [レポート (Reports)] > [エンドポイントとユーザ (Endpoints and Users)] > [エンドポイントのアクティビティ消去 (Endpoints Purge Activities)] で消去アクティビティを確認します。
複製低速エラー (Slow Replication Error)	低速またはスタックした複製が検出されました。	ノードが到達可能であり、展開の一部であることを確認してください。
複製低速情報 (Slow Replication Info)	低速またはスタックした複製が検出されました。	ノードが到達可能であり、展開の一部であることを確認してください。
複製低速警告 (Slow Replication Warning)	低速またはスタックした複製が検出されました。	ノードが到達可能であり、展開の一部であることを確認してください。
PAN 自動フェールオーバー：フェールオーバーが失敗しました (PAN Auto Failover - Failover Failed)	セカンダリ管理ノードへのプロモーション要求が失敗しました。	解決方法については、アラームの詳細を参照してください。
PAN 自動フェールオーバー：フェールオーバーがトリガーされました (PAN Auto Failover - Failover Triggered)	プライマリ ロールにセカンダリ管理ノードのフェールオーバーが正常にトリガーされました。	セカンダリ PAN のプロモーションが完了するまで待機し、古いプライマリ PAN を起動してください。

アラーム名	アラームの説明	アラームの解決方法
PAN 自動フェールオーバー：ヘルスチェックの非アクティビティ (PAN Auto Failover - Health Check Inactivity)	PAN がモニタリング ノードからヘルス チェックのモニタリング要求を受け取りませんでした。	報告されたモニタリング ノードがダウンまたは同期していないかどうかを確認し、必要な場合は手動で同期してください。
PAN 自動フェールオーバー：無効なヘルスチェック (PAN Auto Failover - Invalid Health Check)	自動フェールオーバーで無効なヘルス チェック モニタリング要求が受信されました。	ヘルス チェック モニタリング ノードが同期していることを確認し、必要な場合は手動で同期してください。
PAN 自動フェールオーバー：プライマリ管理ノードのダウン (PAN Auto Failover - Primary Administration Node Down)	プライマリ管理ノードがダウンしているか、またはモニタリング ノードから到達不能です。	PAN を起動して、フェールオーバーが発生するまで待機します。
PAN 自動フェールオーバー：フェールオーバーの試行が拒否されました (PAN Auto Failover - Rejected Failover Attempt)	ヘルス チェック モニタ ノードによって行われたプロモーション要求をセカンダリ管理ノードが拒否しました。	解決方法については、アラームの詳細を参照してください。
EST サービスの停止	EST サービスが停止しています。	CA および EST サービスが稼働しており、証明書サービスのエンドポイント サブ CA 証明書チェーンが完了したことを確認します。
EST サービスの稼働	EST サービスが稼働しています。	EST サービスが稼働中であることを管理者に通知します。
Smart Call Home の通信障害	Smart Call Home メッセージが正常に送信されませんでした。	Cisco ISE と Cisco システムの間でネットワーク接続があることを確認します。
テレメトリ メッセージの障害	テレメトリ メッセージが正常に送信されませんでした。	Cisco ISE と Cisco システムの間でネットワーク接続があることを確認します。
アダプタに接続できない	Cisco ISE は、アダプタに接続できません。	エラーの詳細はアダプタ ログを確認してください。
アダプタのエラー	アダプタにエラーが生じています。	アラームの説明を確認してください。

アラーム名	アラームの説明	アラームの解決方法
アダプタ接続の失敗	アダプタは、送信元のサーバに接続できません。	送信元のサーバがアクセス可能であることを確認してください
エラーによるアダプタの停止	アダプタにエラーが発生し、望ましい状態ではありません。	アダプタの設定が正しく、送信元サーバがアクセス可能であることを確認してください。エラーの詳細はアダプタログを確認してください。
サービス コンポーネントのエラー	サービス コンポーネントにエラーが生じています。	アラームの説明を確認してください。
サービス コンポーネントの情報	サービス コンポーネントが情報を送信しました。	なし。
ISE サービス		
過剰な TACACS 認証試行 (Excessive TACACS Authentication Attempts)	ISE ポリシー サービス ノードで TACACS 認証の割合が想定よりも多くなっています。	ネットワーク デバイスの再認証タイマーをチェックします。ISE インフラストラクチャのネットワーク接続を確認します。
過剰な TACACS 認証の失敗した試行 (Excessive TACACS Authentication Failed Attempts)	ISE ポリシー サービス ノードで失敗した TACACS 認証の割合が想定よりも多くなっています。	根本原因を特定するために認証手順を確認します。ID と秘密の不一致がないか、ISE/NAD 設定を確認します。
MSE ロケーションサーバへのアクセス回復 (MSE Location Server accessible again)	MSE ロケーションサーバへのアクセスが回復しました。	なし。
MSE ロケーションサーバにアクセス不能 (MSE Location Server not accessible.)	MSE ロケーションサーバはアクセス不能でダウンしています。	MSE ロケーションサーバが稼働中で、ISE ノードからアクセスできるかどうかを確認します。
AD コネクタを再起動する必要があります (AD Connector had to be restarted)	AD コネクタが突然シャットダウンし、再起動が必要となりました。	この問題が連続して発生する場合は、Cisco TAC にお問い合わせください。

アラーム名	アラームの説明	アラームの解決方法
Active Directory フォレストが使用不可 (Active Directory forest is unavailable)	Active Directory フォレスト GC (グローバル カタログ) が使用できず、認証、許可、およびグループと属性の取得に使用できません。	DNS 設定、Kerberos 設定、エラー状態、およびネットワーク接続を確認します。
認証ドメインが使用不可 (Authentication domain is unavailable)	認証ドメインが使用できず、認証、許可、およびグループと属性の取得に使用できません。	DNS 設定、Kerberos 設定、エラー状態、およびネットワーク接続を確認します。
ISE の認証非アクティビティ (ISE Authentication Inactivity)	Cisco ISE ポリシー サービス ノードは、ネットワーク デバイスから認証要求を受け取っていません。	ISE/NAD 設定を確認します。ISE/NAD インフラストラクチャのネットワーク接続を確認します。
ID マッピングの認証非アクティビティ (ID Map. Authentication Inactivity)	ユーザ認証イベントが過去 15 分に ID マッピング サービス によって収集されませんでした。	これがユーザ認証が想定される時間 (たとえば、勤務時間) である場合は、Active Directory ドメイン コントローラへの接続を確認します。
CoA 失敗 (COA Failed)	ネットワーク デバイスが、Cisco ISE ポリシー サービス ノードによって発行された許可変更 (CoA) 要求を拒否しました。	Cisco ISE から許可変更 (CoA) を受け入れるようにネットワーク デバイスが設定されていることを確認します。CoA が有効なセッションに対して発行されているかどうかを確認します。
設定されたネーム サーバがダウン (Configured nameserver is down)	設定されたネーム サーバがダウンしているか、使用できません。	DNS 設定とネットワーク接続を確認します。

アラーム名	アラームの説明	アラームの解決方法
サブリカントが応答停止 (Supplicant Stopped Responding)	Cisco ISE がクライアントに最後のメッセージを 120 秒前に送信しましたが、クライアントから応答がありません。	サブリカントが Cisco ISE との完全な EAP キャンバセーションを行えるように適切に設定されていることを確認します。サブリカントとの間で EAP メッセージを転送するように NAS が正しく設定されていることを確認します。サブリカントまたは NAS で、EAP キャンバセーションのタイムアウトが短くないことを確認します。
過剰な認証試行 (Excessive Authentication Attempts)	Cisco ISE ポリシー サービス ノードで認証の割合が想定よりも多くなっています。	ネットワーク デバイスの再認証タイマーをチェックします。Cisco ISE インフラストラクチャのネットワーク接続を確認します。 しきい値が満たされた場合、[過剰な認証試行 (Excessive Authentication Attempts)] および [過剰な失敗試行 (Excessive Failed Attempts)] アラームがトリガーされます。[説明 (Description)] カラムの横に表示される数値は、過去 15 分間で Cisco ISE に対して認証されたか失敗した認証の合計数です。

アラーム名	アラームの説明	アラームの解決方法
過剰な失敗試行 (Excessive Failed Attempts)	Cisco ISE ポリシー サービス ノードで認証失敗の割合が想定よりも多くなっています。	根本原因を特定するために認証手順を確認します。ID と秘密の不一致がないか、Cisco ISE/NAD 設定を確認します。 しきい値が満たされた場合、[過剰な認証試行 (Excessive Authentication Attempts)]および[過剰な失敗試行 (Excessive Failed Attempts)]アラームがトリガーされます。[説明 (Description)]カラムの横に表示される数値は、過去 15 分間で Cisco ISE に対して認証されたか失敗した認証の合計数です。
AD : マシン TGT のリフレッシュに失敗 (AD: Machine TGT refresh failed)	ISE サーバ TGT (チケット認可チケット) のリフレッシュに失敗しました。これは AD 接続とサービスに使用されます。	ISE マシン アカウントが存在し、有効であることを確認します。また、クロック スキュー、複製、Kerberos 設定やネットワーク エラーも確認します。
AD : ISE アカウントパスワードの更新に失敗 (AD: ISE account password update failed)	ISE サーバは、AD マシン アカウント パスワードを更新できませんでした。	ISE マシン アカウント パスワードが変更されていないことと、マシン アカウントが無効でなく制限もされていないことを確認します。KDC への接続を確認します。
参加しているドメインが使用不可 (Joined domain is unavailable)	参加しているドメインが使用できず、認証、許可、およびグループと属性の取得に使用できません。	DNS 設定、Kerberos 設定、エラー状態、およびネットワーク接続を確認します。
ID ストアが使用不可 (Identity Store Unavailable)	Cisco ISE ポリシー サービス ノードは設定された ID ストアに到達できません。	Cisco ISE と ID ストア間のネットワーク接続を確認します。
正しく設定されていないネットワーク デバイスを検出 (Misconfigured Network Device Detected)	Cisco ISE は、NAS から多すぎる RADIUS アカウンティング情報を検出しました。	非常に多くの重複する RADIUS アカウンティング情報が、NAS から ISE に送信されました。正確なアカウンティング頻度で NAS を設定します。

アラーム名	アラームの説明	アラームの解決方法
正しく設定されていないサブ リカントを検出 (Misconfigured Supplicant Detected)	Cisco ISE は、ネットワーク上 で正しく設定されていないサ ブリカントを検出しました。	サブリカントの設定が正しい ことを確認します。
アカウンティングの開始なし (No Accounting Start)	Cisco ISE ポリシー サービス ノードではセッションを許可 していますが、ネットワーク デバイスからアカウンティン グ開始を受信しませんでした。	RADIUS アカウンティングが ネットワーク デバイス上に設 定されていることを確認しま す。ローカル許可に対する ネットワーク デバイス設定を 確認します。
NAD が不明な (Unknown NAD)	Cisco ISE ポリシー サービス ノードは、Cisco ISE に設定さ れていないネットワーク デバ イスから認証要求を受信して います。	ネットワーク デバイスが正規 の要求であるかどうかを確認 してから、それを設定に追加 します。シークレットが一致 することを確認します。
SGACL がドロップ (SGACL Drops)	セキュリティグループアクセ ス (SGACL) ドロップが発生 しました。これは、SGACL ポ リシーの違反により、TrustSec 対応デバイスがパケットをド ロップすると発生します。	RBACL ドロップ概要レポート を実行し、SGACL ドロップを 引き起こしているソースを確認 します。攻撃ソースに CoA を発行してセッションを再許 可または切断します。
RADIUS 要求がドロップ (RADIUS Request Dropped)	NAD からの認証とアカウン ティング要求がサイレントに 廃棄されています。これは、 NAD が不明であるか、共有秘 密鍵が不一致であるか、RFC ごとのパケット内容が無効で あるために発生することがあ ります。	NAD/AAA クライアントにつ いて Cisco ISE に有効な設定が あることを確認します。 NAD/AAA クライアントと Cisco ISE の共有秘密鍵が一致 しているかどうかを確認しま す。AAA クライアントとネッ トワーク デバイスにハード ウェアの問題または RADIUS 互換性の問題がないことを確 認します。また、Cisco ISE に デバイスを接続するネット ワークにハードウェア上の問 題がないことを確認します。
EAP セッションの割り当てに 失敗 (EAP Session Allocation Failed)	RADIUS 要求は EAP セッシ ョンの制限に達したためにド ロップされました。この状態 の原因として、並列 EAP 認証 要求が多すぎることが考えら れます。	新しい EAP セッションで別の RADIUS 要求を呼び出す前に 数秒間待ちます。システムの オーバーロードが発生する場 合は、ISE サーバの再起動を試 してください。

アラーム名	アラームの説明	アラームの解決方法
RADIUS コンテキストの割り当てに失敗 (RADIUS Context Allocation Failed)	RADIUS 要求はシステムのオーバーロードのためにドロップされました。この状態の原因として、並列認証要求が多すぎるが考えられます。	新しい RADIUS 要求を呼び出す前に数秒間待ちます。システムのオーバーロードが発生する場合は、ISE サーバの再起動を試してください。
AD : ISE のマシンアカウントにグループを取得するために必要な権限がない	Cisco ISE のマシンアカウントにグループを取得するために必要な権限がありません。	Cisco ISE のマシンアカウントに Active Directory のユーザグループを取得する権限があるかどうかを確認します。
システムの状態 (System Health)		
ディスク I/O 使用率が高い (High Disk I/O Utilization)	Cisco ISE システムは、ディスク I/O 使用率が高くなっています。	システムに十分なリソースがあるかどうかを確認します。システムの実際の作業量、たとえば、認証数、プロファイラ アクティビティなどを確認します。負荷を分散するためにさらにサーバを追加します。
ディスク領域の使用率が高い (High Disk Space Utilization)	Cisco ISE システムは、ディスク領域の使用率が高くなっています。	システムに十分なリソースがあるかどうかを確認します。システムの実際の作業量、たとえば、認証数、プロファイラ アクティビティなどを確認します。負荷を分散するためにさらにサーバを追加します。
負荷平均が高い (High Load Average)	Cisco ISE システムは、不可平均が高くなっています。	システムに十分なリソースがあるかどうかを確認します。システムの実際の作業量、たとえば、認証数、プロファイラ アクティビティなどを確認します。負荷を分散するためにさらにサーバを追加します。

アラーム名	アラームの説明	アラームの解決方法
メモリ使用率が高い (High Memory Utilization)	Cisco ISE システムは、メモリ使用率が高くなっています。	システムに十分なリソースがあるかどうかを確認します。システムの実際の作業量、たとえば、認証数、プロファイラ アクティビティなどを確認します。負荷を分散するためにさらにサーバを追加します。
操作DBの使用率が高い (High Operations DB Usage)	ノードをモニタする Cisco ISE は、syslog データの量が想定よりも多くなっています。	操作データの消去設定ウィンドウを確認して削減します。
認証待ち時間が長い (High Authentication Latency)	Cisco ISE システムは、認証待ち時間が長くなっています。	システムに十分なリソースがあるかどうかを確認します。システムの実際の作業量、たとえば、認証数、プロファイラ アクティビティなどを確認します。負荷を分散するためにさらにサーバを追加します。
ヘルス ステータスが使用不可 (Health Status Unavailable)	モニタリング ノードは Cisco ISE ノードからヘルス ステータスを受信しませんでした。	Cisco ISE ノードが稼働中であることを確認します。Cisco ISE ノードがモニタリング ノードと通信できることを確認します。
プロセスがダウン (Process Down)	Cisco ISE プロセスの 1 つが動作していません。	Cisco ISE アプリケーションを再起動します。
プロファイラ キューサイズの制限に到達 (Profiler Queue Size Limit Reached)	ISE プロファイラ キュー サイズの制限に到達しました。キュー サイズの制限に達した後に受信されたイベントはドロップされます。	システムに十分なリソースがあることを確認し、エンドポイント属性フィルタが有効になっていることを確認します。
OCSP トランザクションしきい値に到達	OCSP トランザクションしきい値に到達しました。このアラームは、内部 OCSP サービスが大量のトラフィックに到達するとトリガーされます。	システムに十分なリソースがあるかどうかを確認してください。
ライセンシング		

アラーム名	アラームの説明	アラームの解決方法
ライセンスがまもなく期限切れ (License About to Expire)	Cisco ISE ノードにインストールされたライセンスがまもなく期限切れになります。	Cisco ISE の [ライセンスング (Licensing)] ページを参照してライセンスの使用状況を確認します。
ライセンスが期限切れ (License Expired)	Cisco ISE ノードにインストールされたライセンスの期限が切れました。	シスコアカウントチームに問い合わせて、新しいライセンスを購入してください。
ライセンス違反 (License Violation)	Cisco ISE ノードは、許可されたライセンス数を超過しているか、まもなく超過することを検出しました。	シスコアカウントチームに問い合わせて、追加のライセンスを購入してください。
スマート ライセンスの認証の期限切れ	スマート ライセンスの認証の有効期限が切れました。	[Cisco ISE ライセンス管理 (Cisco ISE License Administration)] ページを参照して、手動でスマート ライセンスの登録を更新するか、Cisco Smart Software Manager とのネットワーク接続を確認してください。問題が続くようであれば、シスコ パートナーまでお問い合わせください。
スマート ライセンスの認証の更新の失敗	Cisco Smart Software Manager を使用した認証の更新に失敗しました。	[Cisco ISE ライセンス管理 (Cisco ISE License Administration)] ページを参照し、[ライセンス (Licenses)] テーブルの [更新 (Refresh)] ボタンを使用して、Cisco Smart Software Manager で、手動で認証を更新します。問題が続くようであれば、シスコ パートナーまでお問い合わせください。
スマート ライセンスの認証の更新の成功	Cisco Smart Software Manager を使用した認証の更新に成功しました。	Cisco Smart Software Manager を使用した Cisco ISE の認証の更新が完了したことを通知します。

アラーム名	アラームの説明	アラームの解決方法
スマート ライセンスの通信障害	Cisco Smart Software Manager と Cisco ISE の通信が失敗しました。	Cisco Smart Software Manager とのネットワーク接続を確認します。問題が続くようであれば、Cisco Smart Software Manager にログインするか、またはシスコ パートナーまでお問い合わせください。
復元されたスマート ライセンスの通信	Cisco Smart Software Manager と Cisco ISE の通信が復元されました。	Cisco Smart Software Manager とのネットワーク接続が復元されたことを通知します。
スマート ライセンスの登録解除の障害	Cisco Smart Software Manager を使用した Cisco ISE の登録解除に失敗しました。	詳細については、[Cisco ISE ライセンス管理 (Cisco ISE License Administration)] ページを参照してください。問題が続くようであれば、Cisco Smart Software Manager にログインするか、またはシスコ パートナーまでお問い合わせください。
スマート ライセンスの登録解除の成功	Cisco Smart Software Manager を使用した Cisco ISE の登録解除に成功しました。	Cisco Smart Software Manager を使用した Cisco ISE の登録解除に成功したことを通知します。
スマート ライセンスの無効化	スマート ライセンスは Cisco ISE で無効になり、従来のライセンスが使用されています。	スマート ライセンスを再度有効にするには、[ライセンスの管理 (License Administration)] ページを参照してください。Cisco ISE のスマート ライセンスの使用の詳細については、管理ガイドを参照するか、シスコ パートナーにお問い合わせください。
スマート ライセンスの評価期間の期限切れ	スマート ライセンスの評価期間が終了しました。	Cisco Smart Software Manager を使用して Cisco ISE を登録するには、[Cisco ISE ライセンス管理 (Cisco ISE License Administration)] ページを参照してください。

アラーム名	アラームの説明	アラームの解決方法
スマート ライセンスの HA 役割の変更	スマート ライセンスの使用中に、ハイ アベイラビリティの役割の変更が発生しました。	Cisco ISE でのハイ アベイラビリティの役割が変化したことを通知します。
スマート ライセンス ID 証明書の期限切れ	スマート ライセンス証明書の期限が切れました。	手動でスマート ライセンスの登録を更新するには、[Cisco ISE ライセンス管理 (Cisco ISE License Administration)] ページを参照してください。問題が続くようであれば、シスコパートナーまでお問い合わせください。
スマート ライセンス ID 証明書の更新の失敗	Cisco Smart Software Manager を使用したスマート ライセンスの登録の更新が失敗しました。	手動でスマート ライセンスの登録を更新するには、[Cisco ISE ライセンス管理 (Cisco ISE License Administration)] ページを参照してください。問題が続くようであれば、シスコパートナーまでお問い合わせください。
スマート ライセンス ID 証明書の更新の成功	Cisco Smart Software Manager を使用したスマート ライセンスの登録の更新が成功しました。	Cisco Smart Software Manager を使用した登録の更新が成功したことを通知します。
スマート ライセンスの無効な要求	無効な要求が Cisco Smart Software Manager に送信されました。	詳細については、[Cisco ISE ライセンス管理 (Cisco ISE License Administration)] ページを参照してください。問題が続くようであれば、Cisco Smart Software Manager にログインするか、またはシスコパートナーまでお問い合わせください。
コンプライアンスに準拠していないスマート ライセンス	Cisco ISE ライセンスがコンプライアンスに準拠していません。	詳細については、[ISE ライセンス管理 (ISE License Administration)] ページを参照してください。新しいライセンスを購入するには、パートナーまたはシスコ アカウントチームにお問い合わせください。

アラーム名	アラームの説明	アラームの解決方法
スマート ライセンスの登録の障害	Cisco Smart Software Manager を使用した Cisco ISE の登録が失敗しました。	詳細については、[ISE ライセンス管理 (ISE License Administration)] ページを参照してください。問題が続くようであれば、Cisco Smart Software Manager にログインするか、またはシスコ パートナーまでお問い合わせください。
スマート ライセンスの登録の成功	Cisco Smart Software Manager を使用した Cisco ISE の登録に成功しました。	Cisco Smart Software Manager を使用した Cisco ISE の登録が成功したことを通知します。
システム エラー		
ログ収集エラー (Log Collection Error)	コレクタ プロセスをモニタする Cisco ISE が、ポリシー サービス ノードから生成された監査ログを保持できません。	これは、ポリシー サービス ノードの実際の機能に影響を与えません。その他の解決のために TAC に連絡してください。
スケジュールされているレポートのエクスポートに失敗 (Scheduled Report Export Failure)	設定されたりポジトリにエクスポートされたレポート (CSV ファイル) をコピーできません。	設定されたりポジトリを確認します。それが削除されていた場合は、再度追加します。それが使用できないか、またはそれに到達できない場合は、リポジトリを再設定して有効にします。
TrustSec		
不明な SGT のプロビジョニング (Unknown SGT was provisioned)	不明な SGT がプロビジョニングされました。	ISE は承認フローの一部として不明な SGT をプロビジョニングしました。不明な SGT は既知のフローの一部として割り当てることはできません。
一部の TrustSec ネットワーク デバイスに最新の ISE IP-SGT マッピング設定がありません (Some TrustSec network devices do not have the latest ISE IP-SGT mapping configuration)	一部の TrustSec ネットワーク デバイスに最新の ISE IP-SGT マッピング設定がありません。	ISE が異なる IP-SGT マッピング セットを持ついくつかのネットワーク デバイスを検出しました。[IP-SGT マッピング 展開 (IP-SGT mapping Deploy)] オプションを使用してデバイスを更新します。

アラーム名	アラームの説明	アラームの解決方法
TrustSec SSH 接続の失敗 (TrustSec SSH connection failed)	TrustSec SSH 接続に失敗しました。	ISE がネットワーク デバイスへの SSH 接続を確立できませんでした。[ネットワーク デバイス (Network Device)] ページでネットワーク デバイスの SSH クレデンシャルがネットワーク デバイス上のクレデンシャルと類似していることを確認します。ネットワーク デバイスで ISE (IP アドレス) からの SSH 接続が有効になっていることを確認します。
TrustSec で識別された ISE は 1.0 以外の TLS バージョンで動作するよう設定されました (TrustSec identified ISE was set to work with TLS versions other than 1.0)	TrustSec で識別された ISE は 1.0 以外の TLS バージョンで動作するよう設定されています。	TrustSec は TLS バージョン 1.0 のみをサポートします。
TrustSec PAC の検証の失敗 (Trustsec PAC validation failed)	TrustSec PAC の検証に失敗しました。	ISE がネットワーク デバイスから送信された PAC を検証できませんでした。[ネットワーク デバイス (Network Device)] ページとデバイスの CLI で、Trustsec デバイス クレデンシャルを確認します。デバイスが ISE サーバによってプロビジョニングされた有効な pac を使用していることを確認します。
TrustSec 環境データのダウンロードの失敗	TrustSec 環境データのダウンロードに失敗しました	Cisco ISE は不正な環境データ要求を受信しました。 次のことを確認してください。 <ul style="list-style-type: none">• 要求に PAC が存在し有効である。• すべての属性が要求に存在している。

アラーム名	アラームの説明	アラームの解決方法
TrustSec CoA メッセージの無視	TrustSec CoA メッセージは無視されました	Cisco ISE は、TrustSec CoA メッセージを送信し、応答を受信しませんでした。ネットワーク デバイスが CoA 対応であることを確認してください。ネットワーク デバイス設定を確認してください。
TrustSec のデフォルトの出力ポリシーの変更	TrustSec のデフォルトの出力ポリシーが変更されました。	TrustSec のデフォルトの出力ポリシーのセルが変更されました。セキュリティ ポリシーに合致していることを確認します。

アラームは、Cisco ISE にユーザまたはエンドポイントを追加する場合にはトリガーされません。

アラーム設定

次の表に、[アラーム設定 (Alarm Settings)] ページのフィールドの説明を示します。 ([管理 (Administration)] > [システム (System)] > [設定 (Settings)] > [アラーム設定 (Alarm Settings)])

フィールド	説明
アラーム タイプ (Alarm Type)	ドロップダウンリストからアラーム タイプを選択します。
アラーム名	アラームの名前を入力します。
説明	アラームの説明を入力します。
推奨されるアクション (Suggested Actions)	アラームがトリガーされるときに実行する推奨アクションを入力します。
ステータス	ステータスとして、アラーム ルールの [有効化 (Enable)] または [無効化 (Disable)] を選択します。

フィールド	説明
重大度 (Severity)	<p>ドロップダウンリストボックスを使用して、アラームの重大度レベルを選択します。有効なオプションは次のとおりです。</p> <ul style="list-style-type: none"> • [重大 (Critical)] : 重大なエラーの条件を示します。 • [警告 (Warning)] : 正常ではあるものの重要な状態を示します。これがデフォルトの条件です。 • [情報 (Info)] : 情報メッセージを示します。
syslog メッセージを送信 (Send Syslog Message)	Cisco ISE で生成される各システム アラームの syslog メッセージを送信する場合に、このチェックボックスをオンにします。
複数の電子メール アドレスをカンマで区切って入力 (Enter Multiple Emails Separated with Comma)	電子メール アドレスまたは ISE 管理者名あるいはその両方のカンマ区切りリストを入力します。
電子メールのカスタムテキスト (Custom Text in Email)	システムアラームに関連付けるカスタムテキスト メッセージを入力します。

カスタム アラームの追加

Cisco ISE には [メモリ使用率が高い (High Memory Utilization)]、[設定変更 (Configuration Change)] など 12 種類のデフォルト アラームがあります。Cisco によって定義されるシステムアラームは [アラーム設定 (Alarms Settings)] ページに表示されます ([管理 ((Administration)] > [システム (System)] > [設定 (Settings)] > [アラーム設定 (Alarms Settings)])。システムアラームだけを編集できます。

既存のシステムアラームの他に、既存のアラームタイプでカスタムアラームを追加、編集、削除できます。

各アラームタイプで最大 5 つのアラームを作成でき、アラームの合計数は 200 に制限されます。

アラームを追加するには、次の手順を実行します。

- ステップ 1** [管理 (Administration)] > [システム (System)] > [設定 (Settings)] > [アラーム設定 (Alarm Settings)] を選択します。
- ステップ 2** [アラームの設定 (Alarm Configuration)] タブで、[追加 (Add)] をクリックします。
- ステップ 3** 次の必須詳細情報を入力します。詳細については、「[アラーム設定](#)」の項を参照してください。

アラーム タイプに基づいて ([メモリ使用率が高い (High Memory Utilization)]、[過剰な RADIUS 認証試行 (Excessive RADIUS Authentication Attempts)]、[過剰な TACACS 認証試行 (Excessive TACACS Authentication Attempts)] など)、追加の属性が [アラーム設定 (Alarm Configuration)] ページに表示されます。たとえば、設定変更アラームには、[オブジェクト名 (ObjectName)]、[オブジェクトタイプ (Object Types)] および [管理者名 (Admin Name)] フィールドが表示されます。さまざまな基準で同じアラームの複数のインスタンスを追加できます。

ステップ 4 [送信 (Submit)] をクリックします。

Cisco ISE アラーム通知およびしきい値

Cisco ISE アラームを有効または無効にし、重大な状態を通知するようにアラーム通知動作を設定できます。特定のアラームに対して、過剰な失敗試行アラームの最大失敗試行数、または高ディスク使用量アラームの最大ディスク使用量などのしきい値を設定できます。

アラームごとに通知設定を設定できます。各アラームに対し通知する必要があるユーザの電子メール ID を入力できます (システム定義およびユーザ定義アラームの両方)。



(注) アラーム ルール レベルで指定された受信者の電子メール アドレスは、グローバルの受信者の電子メール アドレスより優先されます。

アラームの有効化および設定

ステップ 1 [管理 (Administration)] > [システム (System)] > [設定 (Settings)] > [アラーム設定 (Alarm Settings)] を選択します。

ステップ 2 デフォルト アラームのリストからアラームを選択して [編集 (Edit)] をクリックします。

ステップ 3 [有効 (Enable)] または [無効 (Disable)] を選択します。

ステップ 4 アラームしきい値を必要に応じて設定します。

ステップ 5 [送信 (Submit)] をクリックします。

モニタリング用の Cisco ISE アラーム

Cisco ISE は、重大なシステム状態が発生するたびに通知するシステムアラームを提供します。Cisco ISE によって生成されたアラームは [アラーム (Alarm)] ダッシュレットに表示されます。これらの通知は、自動的にアラーム ダッシュレットに表示されます。

アラーム ダッシュレットには最近のアラームのリストが表示され、ここから選択してアラームの詳細を表示できます。電子メールおよび syslog メッセージを介してアラームの通知を受信することもできます。

モニタリング アラームの表示

ステップ 1 Cisco ISE ダッシュボードに進みます。

ステップ 2 [アラーム (Alarm)] ダッシュレットでアラームをクリックします。アラームの詳細および推奨アクションが表示された新しいウィンドウが開きます。

ステップ 3 アラームをリフレッシュするには、[リフレッシュ (Refresh)] をクリックします。

ステップ 4 選択したアラームを確認するには、[確認 (Acknowledge)] をクリックします。タイムスタンプの前で使用可能なチェックボックスをクリックしてアラームを選択できます。これにより、読み取りとマークされているときに、アラーム カウンタ (アラームが発生した回数) が減少します。

ステップ 5 選択したアラームに対応する [詳細 (Details)] リンクをクリックします。選択したアラームに対応する詳細が表示された新しいウィンドウが開きます。

(注) ペルソナの変更前に生成された以前のアラームに対応する [詳細 (Details)] リンクに、データは表示されません。

ログ収集 (Log Collection)

モニタリングサービスはログと設定データを収集し、そのデータを保存してから、レポートおよびアラームを生成するために処理します。展開内の任意のサーバから収集されたログの詳細を表示できます。

アラーム syslog 収集場所

システム アラーム通知を syslog メッセージとして送信するようにモニタリング機能を設定した場合は、通知を受信する syslog ターゲットが必要です。アラーム syslog ターゲットは、アラーム syslog メッセージが送信される宛先です。

syslog メッセージを受信するには、syslog サーバとして設定されたシステムも必要です。アラーム syslog ターゲットを作成、編集、および削除できます。



(注) Cisco ISE モニタリングでは、logging-source interface の設定にネットワーク アクセス サーバ (NAS) の IP アドレスを使う必要があります。Cisco ISE モニタリング用のスイッチを設定する必要があります。

ライブ認証

[ライブ認証 (Live Authentications)] ページから、発生した最近の RADIUS 認証をモニタできます。このページには、直近の 24 時間での上位 10 件の RADIUS 認証が表示されます。この項では、[ライブ認証 (Live Authentications)] ページの機能について説明します。

[ライブ認証 (Live Authentications)] ページには、認証イベントの発生時に、その認証イベントに対応するライブ認証エントリが表示されます。認証エントリに加えて、このページには、そのイベントに対応するライブセッションエントリも表示されます。また、目的のセッションをドリルダウンして、そのセッションに対応する詳細レポートを表示することもできます。

[ライブ認証 (Live Authentications)] ページには、最近の RADIUS 認証が発生順に表形式で表示されます。[ライブ認証 (Live Authentications)] ページの下部に表示される最終更新には、サーバ日付、時刻、およびタイムゾーンが示されます。

1 つのエンドポイントが正常に認証されると、2 つのエントリが [ライブ認証 (Live Authentications)] ページに表示されます。1 つは認証レコードに対応し、もう 1 つは (セッション ライブ ビューからプルされた) セッション レコードに対応しています。その後、デバイスで別の認証が正常に実行されると、セッションレコードに対応する繰り返しカウンタの数が増えます。[ライブ認証 (Live Authentications)] ページに表示される繰り返しカウンタには、抑制されている重複した RADIUS 認証成功メッセージの数が示されます。

「最近の RADIUS 認証」の項で説明されているデフォルトで表示されるライブ認証データ カテゴリを参照してください。

すべてのカラムを表示するか、選択したデータカラムのみを表示するように選択できます。表示するカラムを選択した後で、選択を保存できます。

ライブ認証のモニタ

- ステップ 1** [操作 (Operations)] > [RADIUS ライブログ (RADIUS Livelog)] の順に選択します。
- ステップ 2** データ リフレッシュ レートを変更するには、[更新 (Refresh)] ドロップダウン リストから時間間隔を選択します。
- ステップ 3** データを手動で更新するには、[更新 (Refresh)] アイコンをクリックします。
- ステップ 4** 表示されるレコードの数を変更するには、[表示 (Show)] ドロップダウン リストからオプションを選択します。
- ステップ 5** 時間間隔を指定するには、[次の範囲内 (Within)] ドロップダウン リストからオプションを選択します。
- ステップ 6** 表示されるカラムを変更するには、[カラムの追加または削除 (Add or Remove Columns)] をクリックし、ドロップダウン リストからオプションを選択します。
- ステップ 7** ドロップダウン リストの下部にある [保存 (Save)] をクリックして、変更を保存します。
- ステップ 8** ライブ RADIUS セッションを表示するには、[ライブセッションの表示 (Show Live Sessions)] をクリックします。

アクティブな RADIUS セッションを動的に制御できるライブセッションの動的な許可変更 (CoA) 機能を使用できます。ネットワーク アクセス デバイス (NAD) に再認証または接続解除要求を送信できます。

[ライブ認証 (Live Authentications)] ページでのデータのフィルタリング

[ライブ認証 (Live Authentications)] ページのフィルタを使用して、必要な情報をフィルタリングし、ネットワーク認証の問題を迅速にトラブルシューティングできます。[認証 (ライブログ) (Authentication (live logs))] ページのレコードをフィルタして、目的のレコードのみを表示できます。認証ログには多数の詳細が含まれており、特定のユーザまたはロケーションから認証をフィルタリングすると、データをすばやくスキャンするために役立ちます。[ライブ認証 (Live Authentications)] ページの各種フィールドで使用する複数の演算子を使用して、検索基準に基づいてレコードをフィルタリングできます。

- 「abc」 : 「abc」を含む
- 「!abc」 : 「abc」を含まない
- 「{ }」 : 空
- 「!{ }」 : 空でない
- 「abc*」 : 「abc」で開始する
- 「*abc」 : 「abc」で終了する
- 「\!」、 「*」、 「\{ }」、 「\\」 : エスケープ

エスケープオプションを使用すると、特殊文字を含むテキストをフィルタリングできます (フィルタとして使用される特殊文字を含む)。特殊文字の前にバック スラッシュ (\) を付ける必要があります。たとえば、「Employee!」という ID を持つユーザの認証レコードを確認する場合は、ID フィルタ テキスト ボックスに "Employee\\" と入力します。この例では、Cisco ISE は感嘆符 (!) を特殊文字ではなくリテラル文字と見なします。

また、[ステータス (Status)] フィールドでは、成功した認証レコード、失敗した認証、ライブセッションなどのみをフィルタリングできます。緑色のチェック マークは以前発生したすべての成功した認証をフィルタリングします。赤い十字マークはすべての失敗した認証をフィルタリングします。青い [i] アイコンはすべてのライブセッションをフィルタリングします。これらのオプションの組み合わせを表示することも選択できます。

ステップ 1 [操作 (Operations)] > [RADIUS ライブログ (RADIUS LiveLog)] の順に選択します。

ステップ 2 [ライブ認証の表示 (Show Live Authentications)] ページのいずれかのフィールドに基づいてデータをフィルタリングします。

成功または失敗した認証、あるいはライブセッションに基づいて結果をフィルタリングできます。

エンドポイントのグローバル検索

Cisco ISE ホーム ページの上部にあるグローバル検索ボックスを使用して、エンドポイントを検索できます。次の条件を使用してエンドポイントを検索できます。

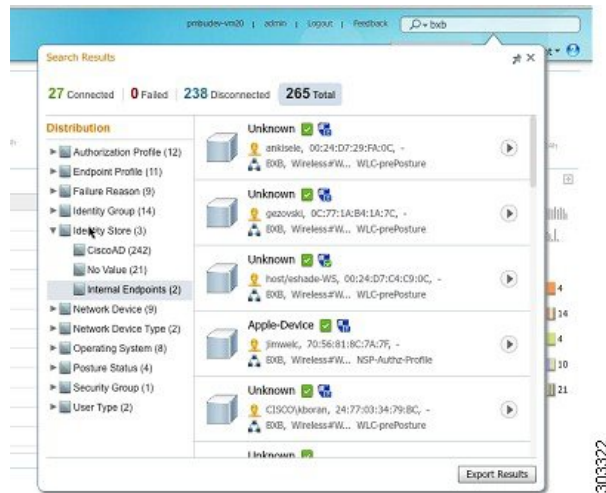
- ユーザ名 (User name)
- MAC アドレス
- [IP アドレス (IP Address)]
- 許可プロファイル
- エンドポイント プロファイル
- 失敗の理由
- ID グループ
- ID ストア
- ネットワーク デバイス名
- ネットワーク デバイス タイプ
- オペレーティング システム (Operating System)
- ポスチャ ステータス
- 参照先
- セキュリティ グループ (Security Group)
- ユーザ タイプ (User Type)

データを表示するには、[検索 (Search)] フィールドに任意の検索条件の少なくとも 3 文字以上を入力する必要があります。

検索結果には、エンドポイントの現在のステータスに関する詳細および概要の情報が表示され、これをトラブルシューティングに使用することができます。検索結果には、上位 25 のエントリのみが表示されます。結果を絞り込むためにフィルタを使用することを推奨します。

次の図は、検索結果の例を示しています。

図 63: エンドポイントの検索結果



左パネルの任意のプロパティを使用して、結果をフィルタリングします。エンドポイントをクリックして、エンドポイントに関する次のような詳細情報を表示することもできます。

- セッションのトレース
- 認証の詳細
- アカウンティングの詳細
- ポスチャの詳細
- プロファイラの詳細
- クライアントプロビジョニングの詳細
- ゲスト アカウンティングおよびアクティビティ

関連トピック

[エンドポイントのセッションのトレース](#) (1071 ページ)

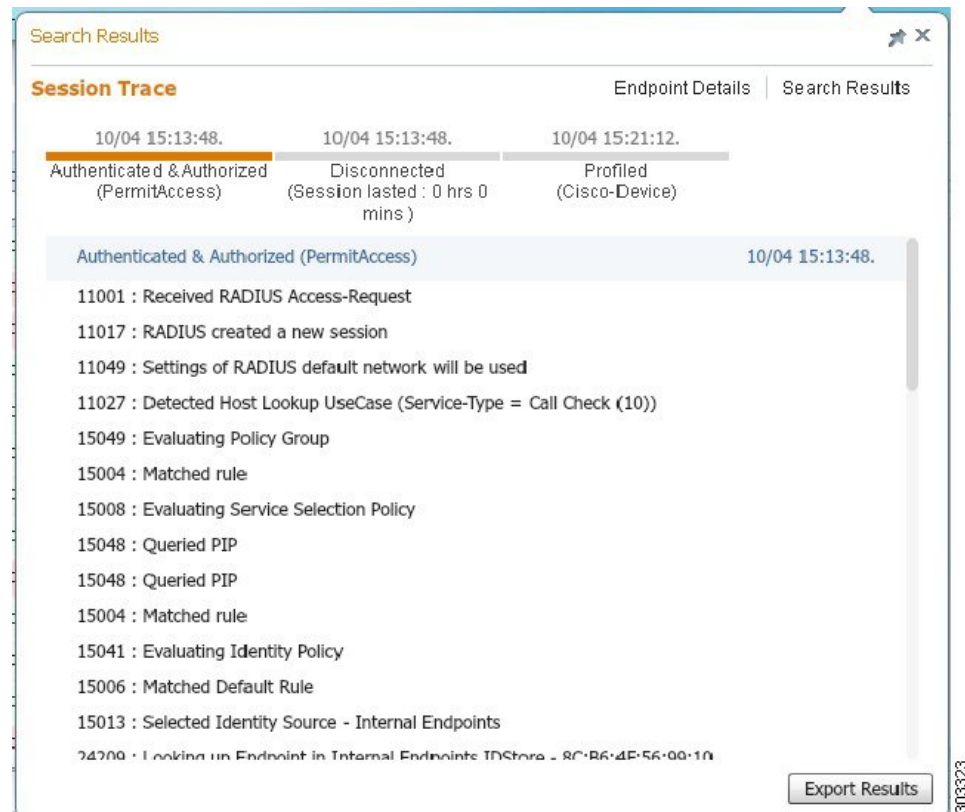
エンドポイントのセッションのトレース

Cisco ISE ホーム ページの上部にあるグローバル検索ボックスを使用して、特定のエンドポイントのセッション情報を取得できます。基準に基づいて検索する場合は、エンドポイントのリストを取得します。エンドポイントのセッショントレース情報を表示するには、そのエンドポイントをクリックします。次の図に、エンドポイントに表示されるセッショントレース情報の例を示します。



(注) 検索に使用されるデータセットは、インデックスとしてのエンドポイント ID に基づいています。したがって、認証が行われる場合、検索結果セットにそれらを含めるには、認証にエンドポイントのエンドポイント ID が必要です。

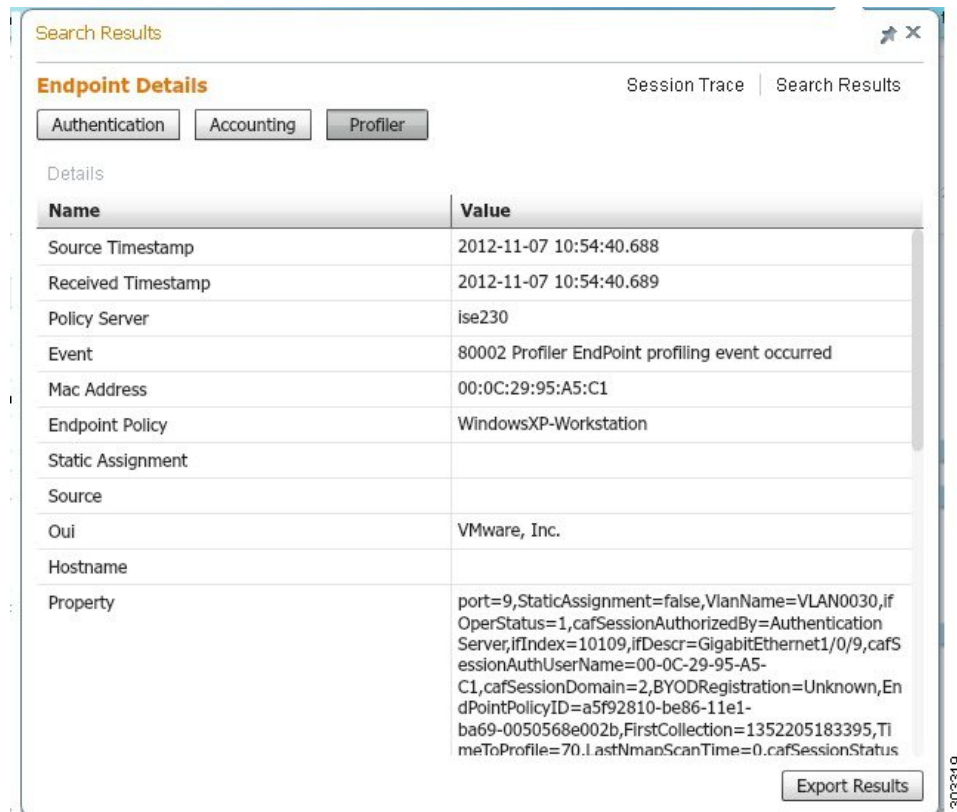
図 64: エンドポイントのセッションのトレース



上部にあるクリック可能なタイムラインを使用すると、主な許可の遷移を確認できます。[結果のエクスポート (Export Results)] ボタンをクリックして、.csv 形式で結果をエクスポートすることもできます。レポートはブラウザにダウンロードされます。

特定のエンドポイントの認証、アカウンティング、およびプロファイラの詳細情報を表示するには、[エンドポイントの詳細 (Endpoint Details)] リンクをクリックします。次の図に、エンドポイントに対して表示されたエンドポイントの詳細情報の例を示します。

図 65: エンドポイントの詳細



Name	Value
Source Timestamp	2012-11-07 10:54:40.688
Received Timestamp	2012-11-07 10:54:40.689
Policy Server	ise230
Event	80002 Profiler EndPoint profiling event occurred
Mac Address	00:0C:29:95:A5:C1
Endpoint Policy	WindowsXP-Workstation
Static Assignment	
Source	
Oui	VMware, Inc.
Hostname	
Property	port=9,StaticAssignment=false,VlanName=VLAN0030,ifOperStatus=1,cafSessionAuthorizedBy=AuthenticationServer,ifIndex=10109,ifDescr=GigabitEthernet1/0/9,cafSessionAuthUserName=00-0C-29-95-A5-C1,cafSessionDomain=2,BYODRegistration=Unknown,EndPointPolicyID=a5f92810-be86-11e1-ba69-0050568e002b,FirstCollection=1352205183395,TimeToProfile=70.LastNmanScanTime=0.cafSessionStatus

ディレクトリからのセッションの削除

次のように、セッションが、モニタリングおよびトラブルシューティング ノード上のセッション ディレクトリから削除されます。

- 終了したセッションは、終了後 15 分で削除されます。
- 認証はあるがアカウントがない場合、このようなセッションは 1 時間後に削除されます。
- すべての非アクティブ セッションは、7 日後に削除されます。

関連トピック

[エンドポイントのグローバル検索](#) (1070 ページ)

認証概要レポート

認証要求に関連する属性に基づいて、特定のユーザ、デバイス、または検索条件についてネットワークアクセスをトラブルシューティングできます。このことは、認証概要レポートを実行して行います。

ネットワーク アクセスの問題のトラブルシューティング

ステップ 1 [操作 (Operations)] > [レポート (Reports)] > [認証概要レポート (Authentication Summary Report)] を選択します。

ステップ 2 失敗の理由でレポートをフィルタリングします。

ステップ 3 レポートの [失敗の理由別の認証 (Authentication by Failure Reasons)] セクションのデータを確認し、ネットワーク アクセスの問題をトラブルシューティングします。

(注) 認証概要レポートが失敗または成功した認証に対応する最新のデータを収集して表示するため、レポートの内容は数分の遅延の後に表示されます。

関連トピック

[予期せぬ RADIUS 認証結果のトラブルシューティング](#) (1075 ページ)

診断トラブルシューティング ツール

診断ツールは、Cisco ISE ネットワークの問題の診断およびトラブルシューティングに役立ち、問題解決方法の詳細な手順を提供します。これらのツールを使用して、認証をトラブルシューティングし、TrustSec デバイスなどのネットワーク上のネットワーク デバイスの設定を評価できます。

RADIUS 認証のトラブルシューティング ツール

このツールを使用すると、予期せぬ認証結果がある場合に、RADIUS 認証または RADIUS 認証に関連する Active Directory を検索および選択して、トラブルシューティングを実行することができます。認証が成功すると予想していたのに失敗した場合、またはユーザやマシンが特定の特権レベルを持っていると予想したのにユーザやマシンがこれらの特権を持っていなかった場合は、このツールを使用できます。

- トラブルシューティングのために、ユーザ名、エンドポイント ID、ネットワーク アクセス サービス (NAS) の IP アドレス、および認証失敗理由に基づいて RADIUS 認証を検索すると、Cisco ISE はシステム (現在) の日付の認証だけを表示します。
- トラブルシューティングのために NAS ポートに基づいて RADIUS 認証を検索すると、Cisco ISE は前月の初めから現在までのすべての NAS ポート値を表示します。



(注) NAS IP アドレスおよび [エンドポイント ID (Endpoint ID)] フィールドに基づいて RADIUS 認証を検索する場合、検索はまず運用データベースで実行され、その後設定データベースで実行されます。

予期せぬ RADIUS 認証結果のトラブルシューティング

- ステップ 1** [操作 (Operations)] > [トラブルシューティング (Troubleshoot)] > [診断ツール (Diagnostic Tools)] > [一般ツール (General Tools)] > [RADIUS 認証トラブルシューティング (RADIUS Authentication Troubleshooting)] を選択します。
- ステップ 2** 必要に応じてフィールドに検索基準を指定します。
- ステップ 3** [検索 (Search)] をクリックして、検索条件に一致する RADIUS 認証を表示します。
AD 関連の認証を検索する際に、展開に Active Directory サーバが設定されていない場合は、「AD が設定されていない」ことを示すメッセージが表示されます。
- ステップ 4** テーブルから RADIUS 認証レコードを選択し、[トラブルシューティング (Troubleshoot)] をクリックします。
AD 関連の認証をトラブルシューティングする必要がある場合は、[管理 (Administration)] > [ID の管理 (Identity Management)] > [外部 ID ソース (External Identity Sources)] > [Active Directory] > [AD ノード (AD node)] で、診断ツールに移動します。
- ステップ 5** [ユーザ入力必須 (User Input Required)] をクリックし、必要に応じてフィールドを変更して、[送信 (Submit)] をクリックします。
- ステップ 6** [完了 (Done)] をクリックします。
- ステップ 7** トラブルシューティングが完了したら、[結果概要の表示 (Show Results Summary)] をクリックします。
- ステップ 8** 診断、問題を解決するための手順、およびトラブルシューティング概要を表示するには、[完了 (Done)] をクリックします。

ネットワーク デバイス ツールの実行

Execute Network Device Command 診断ツールを使用すると、ネットワーク デバイスに対して **show** コマンドを実行することができます。結果は、コンソールに表示される場合とまったく同じ形式であり、デバイスの設定における問題を特定するために使用できます。設定が間違っていると思われる場合や、設定を検証したい場合、または単にどのように設定されているか関心がある場合に、使用することができます。

設定を確認する IOS show コマンドの実行

- ステップ 1** [操作 (Operations)] > [トラブルシューティング (Troubleshoot)] > [診断ツール (Diagnostic Tools)] > [一般ツール (General Tools)] > [ネットワーク デバイス コマンドの実行 (Execute Network Device Command)] を選択します。
- ステップ 2** 該当するフィールドに情報を入力します。
- ステップ 3** [実行 (Run)] をクリックして、指定したネットワーク デバイスでコマンドを実行します。
- ステップ 4** [ユーザ入力必須 (User Input Required)] をクリックし、必要に応じてフィールドを変更します。

ステップ 5 [送信 (Submit)] をクリックして、ネットワーク デバイス上でコマンドを実行し、出力を表示します。

設定バリデータ ツールの評価

この診断ツールを使用して、ネットワーク デバイスの設定を評価し、設定の問題を特定できます。Expert Troubleshooter によって、デバイスの設定が標準設定と比較されます。

ネットワーク デバイス設定の問題のトラブルシューティング

- ステップ 1 [操作 (Operations)] > [トラブルシューティング (Troubleshoot)] > [診断ツール (Diagnostic Tools)] > [一般的なツール (General Tools)] > [設定バリデータの評価 (Evaluate Configuration Validator)] を選択します。
- ステップ 2 設定を評価するデバイスのネットワーク デバイス IP アドレスを入力し、必要に応じて他のフィールドを指定します。
- ステップ 3 推奨テンプレートと比較する設定オプションを選択します。
- ステップ 4 [実行 (Run)] をクリックします。
- ステップ 5 [ユーザ入力必須 (User Input Required)] をクリックし、必要に応じてフィールドを変更します。
- ステップ 6 分析するインターフェイスの隣のチェックボックスをオンにして、[送信 (Submit)] をクリックします。
- ステップ 7 [結果概要の表示 (Show Results Summary)] をクリックします。

ポスチャのトラブルシューティング ツール

[ポスチャのトラブルシューティング (Posture Troubleshooting)] ツールは、ポスチャ チェック エラーの原因を見つけ、次のことを識別するのに役立ちます。

- どのエンドポイントがポスチャに成功し、どのエンドポイントが成功しなかったか。
- エンドポイントがポスチャに失敗した場合、ポスチャプロセスのどの手順が失敗したか。
- どの必須および任意のチェックが成功および失敗したか。

ユーザ名、MAC アドレス、ポスチャ ステータスなどのパラメータに基づいて要求をフィルタリングすることによって、この情報を特定します。

エンドポイント ポスチャの障害のトラブルシューティング

- ステップ 1 [操作 (Operations)] > [トラブルシューティング (Troubleshoot)] > [診断ツール (Diagnostic Tools)] > [一般ツール (General Tools)] > [ポスチャのトラブルシューティング (Posture Troubleshooting)] を選択します。

ステップ2 該当するフィールドに情報を入力します。

ステップ3 [検索 (Search)] をクリックします。

ステップ4 説明を見つけ、イベントの解決策を決定するには、リストでイベントを選択し、[トラブルシューティング (Troubleshoot)] をクリックします。

セッショントレーステストケース

このツールでは、予測できる方法でポリシーフローをテストし、実際のトラフィックを実際のデバイスから発信することなく、ポリシーの設定方法を確認、検証できます。

テストケースで使用する属性と値のリストを設定できます。この詳細情報を使用して、ポリシーシステムとのやりとりが行われ、実行時のポリシー呼び出しがシミュレートされます。

属性はディクショナリを使用して設定できます。[属性 (Attributes)] フィールドに、単純な RADIUS 認証で使用可能なディクショナリがすべて示されます。



(注) 単純な RADIUS 認証のテストケースのみを設定できます。

セッショントレーステストケースの設定

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ1 [操作 (Operations)] > [トラブルシューティング (Troubleshoot)] > [診断ツール (Diagnostic Tools)] > [一般ツール (General Tools)] > [セッショントレーステストケース (Session Trace Test Cases)] を選択します。

ステップ2 [追加 (Add)] をクリックします。

ステップ3 [テストの詳細 (Test Details)] タブで、テストケースの名前と説明を入力します。

ステップ4 事前定義テストケースを1つ選択するか、または必須属性とその値を設定します。使用可能な事前定義テストケースを次に示します。

- [基本認証済みアクセス (Basic Authenticated Access)]
- [プロファイリングされている Cisco Phone (Profiled Cisco Phones)]
- [準拠デバイスアクセス (Compliant Devices Access)]
- [Wi-Fi ゲスト (リダイレクト) (Wi-Fi Guest (Redirect))]
- [Wi-Fi ゲスト (アクセス) (Wi-Fi Guest (Access))]

事前定義テスト ケースを選択すると、Cisco ISE によりそのテスト ケースの関連する属性に自動的に値が取り込まれます。これらの属性のデフォルト値を使用するか、または表示されるオプションから目的の値を選択することができます。また、テスト ケースにカスタム属性を追加することもできます。

テスト ケースに追加する属性と値は、([カスタム属性 (Custom Attributes)] フィールドの下の) [テキスト (Text)] フィールドに示されます。[テキスト (Text)] フィールドの内容を編集すると、Cisco ISE により更新後の内容の有効性と構文がチェックされます。

[テストの詳細 (Test Details)] ページの下部に、すべての属性の概要が表示されます。

ステップ 5 [送信 (Submit)] をクリックして、テスト ケースを作成します。

Cisco ISE はテストの詳細を保存する前に、属性とその値を検証してエラーがある場合はエラーを表示します。

ステップ 6 [テスト ビジュアライザ (Test Visualizer)] タブで、このテスト ケースを実行するノードを選択します。

[ISE ノード (ISE Node)] ドロップダウン リストには、ポリシー サービス ペルソナを担当するノードだけが表示されます。

[ユーザ グループ/属性 (User Groups/Attributes)] をクリックして、外部 ID ストアからユーザのグループと属性を取得します。

ステップ 7 [実行 (Execute)] をクリックします。

Cisco ISE はテスト ケースを実行し、テスト ケースのステップごとの結果を表形式で表示します。ポリシー ステージ、一致ルール、結果オブジェクトが表示されます。緑色のアイコンをクリックして各ステップの詳細を表示します。

ステップ 8 [以前のテスト実行 (Previous Test Executions)] タブをクリックし、以前のテスト実行結果を表示します。また、2 つのテスト ケースを選択して比較することもできます。Cisco ISE では、各テスト ケースの属性の比較ビューが表形式で表示されます。

[RADIUS ライブ ログ (RADIUS Live Logs)] ページから [セッション トレース テスト ケース (Session Trace Test Case)] ツールを起動できます。[セッション トレース テスト ケース (Session Trace Test Case)] ツールを起動するには、[ライブ ログ (Live Logs)] ページでエントリを選択し、([詳細 (Details)] 列の) [アクション (Actions)] アイコンをクリックします。Cisco ISE により、対応するログ エントリから関連する属性と値が抽出されます。必要に応じてこれらの属性と値を変更してから、テスト ケースを実行できます。

高度なトラブルシューティングのテクニカルサポートのトンネル

Cisco ISE は、Cisco IronPort トンネル インフラストラクチャを使用して、ISE サーバに接続してシステムの問題をトラブルシューティングするための、シスコ テクニカル サポート エンジン用のセキュア トンネルを作成します。Cisco ISE は SSH を使用して、トンネル経由のセキュアな接続を作成します。

管理者として、トンネル アクセスを制御できます。サポート エンジニアにアクセス権を付与する時期と期間を選択できます。シスコ カスタマー サポートは、ユーザの介入なしにトンネルを確立できません。サービスログインに関する通知を受信します。任意の時点でトンネル接続をディセーブルにできます。デフォルトでは、テクニカルサポート トンネルは 72 時間開いたままになりますが、すべてのトラブルシューティング作業が完了したら、ご自身またはサポート エンジニアがトンネルを閉じることを推奨します。必要に応じて、72 時間を超えてトンネルを延長することもできます。

tech support-tunnel enable コマンドを使用して、トンネル接続を開始できます。

tech support-tunnel status コマンドでは、接続のステータスが表示されます。このコマンドでは、接続が確立されたかどうか、または認証エラーがあるかどうか、あるいはサーバが到達不能であるかどうかに関する情報が提示されます。トンネルサーバは到達可能であるが ISE が認証できない場合、ISE は 30 分にわたり 5 分ごとに再認証を試行し、その後トンネルは無効になります。

tech support-tunnel disable コマンドを使用してトンネル接続を無効にできます。このコマンドでは、サポート エンジニアが現在ログインしている場合も既存のトンネルが切断されます。

ISE サーバからのトンネル接続をすでに確立している場合は、生成される SSH キーを ISE サーバで使用できます。後でサポート トンネルをイネーブルにしようとすると、システムによって、以前に生成された SSH キーを再使用するよう指示されます。同じキーを使用するか、または新しいキーを生成するかを選択できます。また、**tech support-tunnel resetkey** コマンドを使用してキーを手動でリセットすることもできます。トンネル接続が有効な場合にこのコマンドを実行すると、先に接続をディセーブルにするよう求めるプロンプトが表示されます。既存の接続を続け、無効にしないことを選択した場合、キーは既存の接続が無効になった後でリセットされます。接続を無効にすることを選択した場合、トンネル接続はドロップされ、キーは即座にリセットされます。

トンネル接続の確立後に、**tech support-tunnel extend** コマンドを使用して拡張することができます。

tech support-tunnel コマンドの使用上のガイドラインについては、『Cisco Identity Services Engine CLI Reference Guide』を参照してください。

テクニカル サポート トンネルの確立

Cisco ISE コマンドライン インターフェイス (CLI) からセキュア トンネルを確立できます。

ステップ 1 Cisco ISE CLI から、次のコマンドを入力します。

tech support-tunnel enable

トンネルのパスワードとニックネームの入力が求められます。

ステップ 2 パスワードを入力します。

ステップ 3 (任意) トンネルのニックネームを入力します。

システムによって SSH キーが生成され、パスワード、デバイスのシリアル番号および SSH キーが表示されます。サポート エンジニアがシステムに接続できるように、この情報をシスコ カスタマー サポートに渡す必要があります。

ステップ 4 パスワード、デバイスのシリアル番号および SSH キーをコピーし、シスコ カスタマー サポートに送信します。

これで、サポート エンジニアが ISE サーバに安全に接続できるようになります。サービス ログに関する定期的な通知を受信します。

着信トラフィックを検証する TCP ダンプユーティリティ

これは、予想されたパケットが実際にノードに到達したことを調査する場合に、パケットをスニффリングするツールです。たとえば、レポートに示されている着信認証またはログがない場合、着信トラフィックがないのではないかと疑われる場合があります。このような場合、検証するためにこのツールを実行できます。

TCP ダンプ オプションを設定し、ネットワーク トラフィックからデータを収集して、ネットワークの問題をトラブルシューティングすることができます。



注意 TCP ダンプを起動すると、以前のダンプファイルは自動的に削除されます。以前のダンプファイルを保存するには、新しい TCP ダンプ セッションを開始する前に、「TCP ダンプ ファイルの保存」の項の説明に従ってタスクを実行します。

関連トピック

[TCP ダンプ ファイルの保存](#) (1081 ページ)

ネットワーク トラフィックのモニタリングでの TCP ダンプの使用

始める前に

- [TCP ダンプ (TCP Dump)] ページの [ネットワーク インターフェイス (Network Interface)] ドロップダウン リストには、IPv4 または IPv6 アドレスが設定されているネットワーク インターフェイス カード (NIC) のみが表示されます。デフォルトでは、すべての NIC は VMware に接続されるため、NIC は、IPv6 アドレスを使用して設定され、[ネットワーク インターフェイス (Network Interface)] ドロップダウン リストに表示されます。
- tcpdump ファイルを表示するには、Cisco ISE 管理 ノードに Adobe Flash Player がインストールされている必要があります。

- ステップ 1** [操作 (Operations)] > [トラブルシューティング (Troubleshoot)] > [診断ツール (Diagnostic Tools)] > [一般ツール (General Tools)] > [TCP ダンプ (TCP Dump)] を選択します。
- ステップ 2** TCP ダンプ ユーティリティのソースとして [ホスト名 (Host Name)] を選択します。
- ステップ 3** モニタする [ネットワーク インターフェイス (Network Interface)] をドロップダウン リストから選択します。
- ステップ 4** オプション ボタンをクリックして、オンかオフにして、無差別モードを設定します。デフォルトは [オン (On)] です。
- 無差別モードは、ネットワーク インターフェイスがシステムの CPU にすべてのトラフィックを渡すデフォルト パケット スニффイング モードです。[オン (On)] のままにしておくことを推奨します。
- ステップ 5** [フィルタ (Filter)] テキスト ボックスに、フィルタリングのもとになるブール演算式を入力します。
- サポートされている標準 tcpdump フィルタ式：
- ```
ip host 10.77.122.123
ip host 10.77.122.123 and not 10.77.122.119
ip host ISE123
```
- ステップ 6** [開始 (Start)] をクリックして、ネットワークのモニタリングを開始します。
- ステップ 7** 十分な量のデータが収集された時点で [停止 (Stop)] をクリックするか、最大パケット数 (500,000) が累積されてプロセスが自動的に終了するまで待機します。



(注) Cisco ISE は、1500 より大きいフレーム (ジャンボ フレーム) の MTU をサポートしません。

#### 関連トピック

[TCP ダンプ ファイルの保存](#) (1081 ページ)

## TCP ダンプ ファイルの保存

### 始める前に

「ネットワーク トラフィックのモニタリングでの TCP ダンプの使用」の項の説明に従って、タスクを完了しておく必要があります。



(注) Cisco ISE CLI を使用して TCPdump にアクセスすることもできます。詳細については、『*Cisco Identity Services Engine CLI Reference Guide*』を参照してください。

- ステップ 1 [操作 (Operations)] > [トラブルシューティング (Troubleshoot)] > [診断ツール (Diagnostic Tools)] > [一般ツール (General Tools)] > [TCP ダンプ (TCP Dump)] を選択します。
- ステップ 2 [形式 (Format)] をドロップダウンリストから選択します。[可読 (Human Readable)] がデフォルトです。
- ステップ 3 [ダウンロード (Download)] をクリックし、必要な場所に移動して、[保存 (Save)] をクリックします。
- ステップ 4 最初に以前のダンプ ファイルを保存しないで除去するには、[削除 (Delete)] をクリックします。

## エンドポイントまたはユーザの予期しない SGACL の比較

- ステップ 1 [操作 (Operations)] > [トラブルシューティング (Troubleshoot)] > [診断ツール (Diagnostic Tools)] > [TrustSec ツール (Trustsec Tools)] > [出力 (SGACL) ポリシー (Egress (SGACL) Policy)] を選択します。
- ステップ 2 SGACL ポリシーを比較する TrustSec デバイスのネットワーク デバイス IP アドレスを入力します。
- ステップ 3 [実行 (Run)] をクリックします。
- ステップ 4 [ユーザ入力必須 (User Input Required)] をクリックし、必要に応じてフィールドを変更します。
- ステップ 5 [送信 (Submit)] をクリックします。
- ステップ 6 [結果概要の表示 (Show Results Summary)] をクリックして、診断および推奨される解決手順を表示します。

## 出力ポリシー診断フロー

出力ポリシー診断ツールでは、次の表に示すプロセスを使用して比較が行われます。

| プロセス ステージ | 説明                                                                            |
|-----------|-------------------------------------------------------------------------------|
| 1         | 指定した IP アドレスを使用してデバイスに接続し、送信元 SGT と宛先 SGT の各ペアに対するアクセスコントロールリスト (ACL) を取得します。 |
| 2         | Cisco ISE に設定された出力ポリシーをチェックし、送信元 SGT と宛先 SGT の各ペアに対する ACL を取得します。             |
| 3         | ネットワーク デバイスから取得された SGACL ポリシーと、Cisco ISE から取得された SGACL ポリシーを比較します。            |



| プロセス ステージ | 説明                                                             |
|-----------|----------------------------------------------------------------|
| 4         | ポリシーが一致しない送信元 SGT と宛先 SGT のペアを表示します。また、追加情報として、一致するエントリも表示します。 |

## SXP-IP マッピングを持つ TrustSec 対応ネットワークの接続問題のトラブルシューティング

**ステップ 1** [操作 (Operations)] > [トラブルシューティング (Troubleshoot)] > [診断ツール (Diagnostic Tools)] > [TrustSec ツール (Trustsec Tools)] > [SXP-IP マッピング (SXP-IP Mappings)] を選択します。

**ステップ 2** ネットワーク デバイスのネットワーク デバイス IP アドレスを入力し、[選択 (Select)] をクリックします。

**ステップ 3** [実行 (Run)] をクリックし、[ユーザ入力必須 (User Input Required)] をクリックして、必要なフィールドを変更します。

Expert Troubleshooter によって、ネットワーク デバイスから TrustSec SXP 接続が取得されて、ピア SXP デバイスを選択するように再度要求するプロンプトが表示されます。

**ステップ 4** [ユーザ入力必須 (User Input Required)] をクリックし、必要な情報を入力します。

**ステップ 5** SXP マッピングを比較するピア SXP デバイスのチェックボックスをオンにして、共通接続パラメータを入力します。

**ステップ 6** [送信 (Submit)] をクリックします。

**ステップ 7** [結果概要の表示 (Show Results Summary)] をクリックして、診断および解決手順を表示します。

## IP-SGT マッピングを持つ TrustSec 対応ネットワークの接続問題のトラブルシューティング

**ステップ 1** [操作 (Operations)] > [トラブルシューティング (Troubleshoot)] > [診断ツール (Diagnostic Tools)] > [TrustSec ツール (Trustsec Tools)] > [IP ユーザ SGT (IP User SGT)] を選択します。

**ステップ 2** 必要に応じてフィールドに情報を入力します。

**ステップ 3** [実行 (Run)] をクリックします。

追加入力が要求されます。

**ステップ 4** [ユーザ入力必須 (User Input Required)] をクリックし、必要に応じてフィールドを変更して、[送信 (Submit)] をクリックします。

**ステップ 5** [結果概要の表示 (Show Results Summary)] をクリックして、診断および解決手順を表示します。

## デバイス SGT ツール

TrustSec ソリューションが有効なデバイスの場合、RADIUS 認証によって各ネットワーク デバイスに SGT 値が割り当てられます。デバイス SGT 診断ツールは、（提供された IP アドレスを使用して）ネットワーク デバイスに接続し、ネットワーク デバイス SGT 値を取得します。次に RADIUS 認証レコードをチェックして、割り当てられた最新の SGT 値を特定します。最後に、デバイス SGT ペアを表形式で表示して、SGT 値が同じであるかどうかを特定します。

## デバイス SGT マッピングの比較による TrustSec 対応ネットワークの接続問題のトラブルシューティング

ステップ 1 [操作 (Operations)] > [トラブルシューティング (Troubleshoot)] > [診断ツール (Diagnostic Tools)] > [TrustSec ツール (Trustsec Tools)] > [デバイス SGT (Device SGT)] を選択します。

ステップ 2 必要に応じてフィールドに情報を入力します。

デフォルトのポート番号は、Telnet は 23、SSH は 22 です。

ステップ 3 [実行 (Run)] をクリックします。

ステップ 4 [結果概要の表示 (Show Results Summary)] をクリックして、デバイス SGT 比較の結果を表示します。

## モニタリングノードからのエンドポイント統計データのダウンロード

モニタリングノードからネットワークに接続するエンドポイントの統計データをダウンロードできます。ロード、CPU 使用率、認証トラフィックデータを含む主要パフォーマンスメトリック (KPM) が使用可能で、ネットワークの問題の監視およびトラブルシューティングに使用できます。日次 KPM 統計情報または過去 8 週間の KPM 統計情報をそれぞれダウンロードするには、Cisco ISE コマンドライン インターフェイス (CLI) から、**application configure ise** コマンドを使用し、オプション 12 または 13 を使用します。

このコマンドの出力では、エンドポイントに関する次のデータが提供されます。

- ネットワーク上のエンドポイントの総数
- 正常な接続を確立したエンドポイントの数
- 認証に失敗したエンドポイントの数。
- 毎日の接続済みの新しいエンドポイントの総数
- 毎日のオンボーディングしたエンドポイントの総数

出力には、タイムスタンプの詳細、展開内の各ポリシー サービス ノード (PSN) を介して接続したエンドポイントの総数、エンドポイントの総数、アクティブエンドポイント、負荷、および認証トラフィックの詳細も含まれています。

このコマンドの詳細については、『*Cisco Identity Services Engine CLI Reference Guide*』を参照してください。

## その他のトラブルシューティング情報の入手

Cisco ISE を使用すると、管理者ポータルから、サポートおよびトラブルシューティング情報をダウンロードできます。サポートバンドルを使用して、Cisco Technical Assistance Center (TAC) が Cisco ISE の問題をトラブルシューティングするための診断情報を準備できます。



(注) サポートバンドルおよびデバッグログにより、高度なトラブルシューティング情報が TAC に提供されます。サポートバンドルおよびデバッグログは解釈が困難です。Cisco ISE で提供されるさまざまなレポートおよびトラブルシューティングツールを使用して、ネットワークで直面している問題を診断およびトラブルシューティングできます。

### 関連トピック

[ネットワーク アクセスの問題のトラブルシューティング](#) (1074 ページ)

## Cisco ISE のサポート バンドル

サポートバンドルに含めるログを設定できます。たとえば、特定のサービスのログをデバッグログに含めるように設定できます。また、日付に基づいてログをフィルタリングできます。

ダウンロードできるログは、次のように分類されます。

- 完全な設定データベース : Cisco ISE 設定データベースは、人間が読み取れる XML 形式でダウンロードされます。問題をトラブルシューティングしようとするときに、このデータベース設定を別の Cisco ISE ノードにインポートして、シナリオを再現できます。
- デバッグログ : ブートストラップ、アプリケーション設定、ランタイム、展開、公開キーインフラストラクチャ (PKI) 情報、およびモニタリングとレポートが取得されます。

デバッグログによって、特定の Cisco ISE コンポーネントのトラブルシューティング情報が提供されます。デバッグログを有効にするには、第11章「ログ」を参照してください。デバッグログを有効にしない場合、情報メッセージ (INFO) はすべてサポートバンドルに含まれます。詳細については、[Cisco ISE デバッグログ \(1088 ページ\)](#) を参照してください。

- ローカル ログ : Cisco ISE で実行されるさまざまなプロセスからの syslog メッセージが含まれています。

- コアファイル：クラッシュの原因の特定に役立つ重要な情報が含まれています。これらのログは、アプリケーションがクラッシュし、アプリケーションにヒープダンプが含まれている場合に作成されます。
- モニタリングおよびレポートログ：アラートおよびレポートに関する情報が含まれています。
- システム ログ：Cisco Application Deployment Engine（ADE）関連の情報が含まれています。
- ポリシー設定：Cisco ISE で設定されたポリシーが人間が読み取れる形式で含まれます。

これらのログは、Cisco ISE CLI から **backup-logs** コマンドを使用してダウンロードできます。詳細については、『*Cisco Identity Services Engine CLI Reference Guide*』を参照してください。



(注) インライン ポスチャ ノードの場合、管理者ポータルからサポートバンドルをダウンロードできません。Cisco ISE CLI から **backup-logs** コマンドを使用して、インライン ポスチャ ノードのログをダウンロードする必要があります。

これらのログを管理者ポータルからダウンロードすることを選択した場合、次の操作を実行できます。

- デバッグ ログやシステム ログなどのログ タイプに基づいて、ログのサブセットのみをダウンロードします。
- 選択したログタイプの最新の「*n*」個のファイルのみをダウンロードします。このオプションによって、サポートバンドルのサイズとダウンロードにかかる時間を制御できます。

モニタリングログによって、モニタリング、レポート、およびトラブルシューティング機能に関する情報が提供されます。ログのダウンロードの詳細については、[Cisco ISE ログ ファイルのダウンロード \(1086 ページ\)](#) を参照してください。

## サポート バンドル

サポート バンドルは、単純な tar.gpg ファイルとしてローカル コンピュータにダウンロードできます。サポート バンドルは、日付とタイム スタンプを使用して、`ise-support-bundle_ise-support-bundle-mm-dd-yyyy--hh-mm.tar.gpg` という形式で名前が付けられます。ブラウザに、適切な場所にサポートバンドルを保存するように要求するプロンプトが表示されます。サポートバンドルの内容を抽出し、README.TXT ファイルを表示できます。このファイルには、サポートバンドルの内容と、ISE データベースがサポートバンドルに含まれている場合はその内容をインポートする方法が示されています。

## Cisco ISE ログ ファイルのダウンロード

ネットワークでの問題のトラブルシューティング時に、Cisco ISE ログ ファイルをダウンロードして、詳細情報を確認できます。

インストールとアップグレードに関する問題のトラブルシューティングを行うには、ADE-OS および他のログ ファイルを含む、システム ログをダウンロードすることもできます。

サポートバンドルをダウンロードする際には、暗号化キーを手動で入力する代わりに、暗号化用の公開キーを使用するように選択できるようになりました。このオプションを選択すると、Cisco PKI はサポートバンドルの暗号化および復号化に使用されます。Cisco TAC は、公開キーと秘密キーを保持します。Cisco ISE はサポートバンドルの暗号化に公開キーを使用します。Cisco TAC は、秘密キーを使用してサポートバンドルを復号化できます。このオプションは、トラブルシューティング用に Cisco TAC にサポートバンドルを提供する場合に使用します。オンプレミスの問題をトラブルシューティングしている場合、共有キー暗号化を使用します。

### 始める前に

- 次のタスクを実行するには、スーパー管理者またはシステム管理者の権限が必要です。
- デバッグ ログとデバッグ ログ レベルを設定します。

**ステップ 1** [操作 (Operations)] > [トラブルシューティング (Troubleshoot)] > [ログのダウンロード (Download Logs)] > > [アプライアンス ノード リスト (Appliance node list)] を選択します。

**ステップ 2** サポートバンドルをダウンロードするノードをクリックします。

**ステップ 3** [サポートバンドル (Support Bundle)] タブでは、サポートバンドルに入力するパラメータを選択します。

すべてのログを含めると、サポートバンドルが大きくなりすぎて、ダウンロードに時間がかかります。ダウンロードプロセスを最適化するには、最新の *n* ファイルのみをダウンロードするように選択します。

**ステップ 4** サポートバンドルを生成する開始日と終了日を入力します。

**ステップ 5** 次のいずれかを実行します。

- 公開キー暗号化 (Public Key Encryption) : このオプションは、トラブルシューティング用に Cisco TAC にサポートバンドルを提供する場合に選択します。
- 共有キー暗号化 (Shared Key Encryption) : このオプションは、オンプレミスでローカルで問題をトラブルシューティングする場合に選択します。このオプションを選択すると、サポートバンドル用の暗号キーを入力する必要があります。

**ステップ 6** サポートバンドルの暗号キーを入力し、再入力します。

**ステップ 7** [サポートバンドルの作成 (Create Support Bundle)] をクリックします。

**ステップ 8** [ダウンロード (Download)] をクリックして、新しく作成されたサポートバンドルをダウンロードします。

サポートバンドルは、アプリケーション ブラウザを実行しているクライアントシステムにダウンロードされる tar.gpg ファイルです。

### 次のタスク

特定のコンポーネントのデバッグ ログをダウンロードします。

## 関連トピック

[デバッグ ログのダウンロード](#) (1090 ページ)

## Cisco ISE デバッグ ログ

デバッグ ログには、さまざまな Cisco ISE コンポーネントのトラブルシューティング情報が含まれています。デバッグ ログには、過去 30 日間に生成された重大な警告アラームと、過去 7 日間に生成された情報アラームが含まれています。問題を報告しているときに、これらのデバッグ ログを有効にして、問題の診断と解決のためにこれらのログを送信するよう求められる場合があります。

### デバッグ ログの入手

**ステップ 1** [デバッグ ログの設定 (Debug Log Configuration)] ページで、デバッグ ログを取得するコンポーネントを設定します。

**ステップ 2** デバッグ ログをダウンロードします。

## 関連トピック

[デバッグ ログのダウンロード](#) (1090 ページ)

## Cisco ISE コンポーネントおよび対応するデバッグ ログ

表 61: コンポーネントおよび対応するデバッグ ログ

| コンポーネント                           | デバッグ ログ         |
|-----------------------------------|-----------------|
| Active Directory                  | ad_agent.log    |
| Cache Tracker                     | tracking.log    |
| Entity Definition Framework (EDF) | edf.log         |
| JMS                               | ise-psc.log     |
| ライセンス                             | ise-psc.log     |
| Notification Tracker              | tracking.log    |
| Replication-Deployment            | replication.log |
| Replication-JGroup                | replication.log |
| Replication Tracker               | tracking.log    |
| RuleEngine-Attributes             | ise-psc.log     |
| RuleEngine-Policy-IDGroups        | ise-psc.log     |
| accessfilter                      | ise-psc.log     |
| admin-infra                       | ise-psc.log     |

| コンポーネント             | デバッグ ログ     |
|---------------------|-------------|
| boot-strap wizard   | ise-psc.log |
| cisco-mnt           | ise-psc.log |
| クライアント              | ise-psc.log |
| cpm-clustering      | ise-psc.log |
| cpm-mnt             | ise-psc.log |
| epm-pdp             | ise-psc.log |
| epm-pip             | ise-psc.log |
| anc                 | ise-psc.log |
| anc                 | ise-psc.log |
| ers                 | ise-psc.log |
| guest               | ise-psc.log |
| ゲスト アクセス管理          | guest.log   |
| ゲスト アクセス            | guest.log   |
| MyDevices           | guest.log   |
| ポータル (Portal)       | guest.log   |
| ポータル セッション マネージャ    | guest.log   |
| ポータル Web アクション      | guest.log   |
| guestauth           | ise-psc.log |
| guestportal         | ise-psc.log |
| identitystore-AD    | ise-psc.log |
| infrastructure      | ise-psc.log |
| mdm                 | ise-psc.log |
| mdm-pip             | ise-psc.log |
| mnt-alarm           | alarms.log  |
| mnt-report          | reports.log |
| mydevices           | ise-psc.log |
| nsf                 | ise-psc.log |
| nsf-session         | ise-psc.log |
| org-apache          | ise-psc.log |
| org-apache-cxf      | ise-psc.log |
| org-apache-digester | ise-psc.log |

| コンポーネント         | デバッグ ログ             |
|-----------------|---------------------|
| ポスチャ            | ise-psc.log         |
| profiler        | profiler.log        |
| provisioning    | ise-psc.log         |
| prrt-JNI        | prrt-management.log |
| runtime-AAA     | prrt-management.log |
| runtime-config  | prrt-management.log |
| runtime-logging | prrt-management.log |
| sponsorportal   | ise-psc.log         |
| swiss           | ise-psc.log         |

## デバッグ ログのダウンロード

### 始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

**ステップ 1** [操作 (Operations)] > [トラブルシューティング (Troubleshoot)] > [ログのダウンロード (Download Logs)] > > [アプライアンス ノード リスト (Appliance node list)] を選択します。

**ステップ 2** [アプライアンス ノード リスト (Appliance node list)] で、デバッグ ログをダウンロードするノードをクリックします。

**ステップ 3** [デバッグ ログ (Debug Logs)] タブをクリックします。

デバッグ ログ タイプとデバッグ ログのリストが表示されます。このリストは、デバッグ ログの設定に基づいています。

**ステップ 4** ダウンロードするログファイルをクリックし、クライアントブラウザを実行しているシステムに保存します。

必要に応じて、このプロセスを繰り返して他のログファイルをダウンロードできます。次に示すのは、[デバッグ ログ (Debug Logs)] ページからダウンロードできるその他のデバッグ ログです。

- isebootstrap.log : ブートストラップ ログ メッセージを提供します
- monit.log : ウォッチドッグ メッセージを提供します
- pki.log : サードパーティの暗号ライブラリ ログを提供します
- iseLocalStore.log : ローカル ストア ファイルに関するログを提供します
- ad\_agent.log : Microsoft Active Directory サードパーティ ライブラリ ログを提供します



- catalina.log : サードパーティ ログを提供します

## モニタリング データベース

モニタリング機能によって利用されるデータ レートおよびデータ量には、これらの目的専用のノード上に別のデータベースが必要です。

ポリシーサービスと同様に、モニタリングには専用のデータベースがあり、この項で説明するトピックのようなメンテナンス タスクを実行する必要があります。

### 関連トピック

[ログ収集 \(Log Collection\)](#) (1067 ページ)

[モニタリング データベースのバックアップと復元](#) (1091 ページ)

[モニタリング データベースの消去](#) (1091 ページ)

## モニタリング データベースのバックアップと復元

モニタリングデータベースは、大量のデータを処理します。時間が経つにつれ、モニタリングノードのパフォーマンスと効率は、そのデータをどう管理するかによって変わってきます。効率を高めるために、データを定期的にバックアップして、それをリモートのリポジトリに転送することを推奨します。このタスクは、自動バックアップをスケジュールすることによって自動化できます。



- (注) 消去操作の実行中には、バックアップを実行しないでください。消去操作の実行中にバックアップが開始されると、消去操作が停止または失敗します。

セカンダリ モニタリング ノードを登録する場合は、最初にプライマリ モニタリング ノードをバックアップしてから、新しいセカンダリ モニタリング ノードにデータを復元することを推奨します。これにより、新しい変更内容が複製されるため、プライマリ モニタリング ノードの履歴が新しいセカンダリ ノードと同期状態となります。

## モニタリング データベースの消去

消去プロセスでは、消去時にデータを保持する月数を指定することで、モニタリング データベースのサイズを管理できます。デフォルトは3ヵ月間です。この値は、消去用のディスク領域使用率しきい値（ディスク領域のパーセンテージ）に達したときに使用されます。このオプションでは、各月は30日で構成されます。デフォルトの3ヵ月は90日間です。

### 関連トピック

[モニタリング データベースの消去に関するガイドライン](#) (1092 ページ)

## モニタリング データベースの消去に関するガイドライン

次に、モニタリングデータベースのディスク使用に関連して従うべきガイドラインをいくつか示します。

- モニタリングデータベースのディスク使用量がしきい値設定の 80% を超えた場合、データベース サイズが割り当てられたディスク サイズを超過したことを示すクリティカルアラームが生成されます。ディスク使用量が 90% より大きい場合は、別のアラームが生成されます。

消去プロセスが実行され、ステータス履歴レポートが作成されます。このレポートは、**[操作 (Operations)] > [レポート (Reports)] > [展開ステータス (Deployment Status)] > [データ消去の監査 (Data Purging Audit)]** を選択して表示できます。消去の完了時に情報 (INFO) アラームが生成されます。

- 消去は、データベースの使用済みディスク領域のパーセンテージにも基づきます。モニタリングデータベースの使用済みディスク領域がしきい値 (デフォルトは 80%) 以上になると、消去プロセスが開始されます。このプロセスは、管理者ポータルの設定に関係なく、過去 7 日間のモニタリング データのみを削除します。ディスク領域が 80% 未満になるまで繰り返しプロセスを続行します。消去では、処理の前にモニタリングデータベースのディスク領域制限が常にチェックされます。

## 運用データの消去

[運用データの消去 (Operational Data Purging)] ページ ([管理 (Administration)] > [システム (System)] > [メンテナンス (Maintenance)] > [運用データの消去 (Operational Data Purging)]) には、[データベースの使用状況 (Database Utilization)] 領域と [データを今すぐ消去 (Purge Data Now)] 領域があります。[データベースの使用状況 (Database Utilization)] 領域には、使用可能なデータベース容量の合計と、保存されている RADIUS および TACACS データが表示されます。ステータスバーをマウスオーバーすると、利用可能なディスク容量と、データベースに既存データが保存されている日数が表示されます。RADIUS データと TACACS データを保持できる期間を [データ保存期間 (Data Retention Period)] 領域に指定できます。データは毎朝午前 4 時に消去されます。また、保存日数を指定して、消去前にデータをリポジトリにエクスポートするように設定できます。[リポジトリのエクスポートを有効にする (Enable Export Repository)] チェックボックスをオンにして、リポジトリを選択して作成し、暗号キーを指定できます。

[データを今すぐ消去 (Purge Data Now)] 領域では、すべての RADIUS および TACACS データを消去するか、またはデータ消去までに保存できる日数を指定できます。



- (注) 消去前にリポジトリにエクスポートできるテーブルは、RADIUS 認証およびアカウントティング、TACACS 認証およびアカウントティング、RADIUS エラー、および設定が誤っているサブリカントの各テーブルです。

## 関連トピック

[古い運用データの消去](#) (1093 ページ)

## 古い運用データの消去

運用データはサーバに一定期間集められています。すぐに削除することも、定期的に削除することもできます。データ消去の監査レポートを表示して、データ消去が成功したかどうかを確認できます。

## 始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

**ステップ 1** [管理 (Administration)] > [システム (System)] > [メンテナンス (Maintenance)] > [運用データの消去 (Operational Data Purging)] を選択します。

**ステップ 2** 次のいずれかを実行します。

- [データ保持期間 (Data Retention Period)] 領域で次の操作を行います。
  1. RADIUS または TACACS データを保持する期間を日単位で指定します。指定した期間より前のデータはすべてリポジトリにエクスポートされます。
  2. [リポジトリ (Repository)] 領域で、[リポジトリのエクスポートを有効にする (Enable Export Repository)] チェックボックスをオンにし、データを保存するリポジトリを選択します。詳細については、「リポジトリの作成」の項を参照してください。
  3. [暗号キー (Encryption Key)] テキスト ボックスに必要なパスワードを入力します。
  4. [保存 (Save)] をクリックします。

(注) 設定した保持期間が診断データに対応する既存の保持しきい値未満の場合、設定値は既存のしきい値を上書きします。たとえば、保持期間を 3 日に設定し、この値が診断テーブルの既存のしきい値 (たとえば、5 日のデフォルト) 未満の場合、データはこのページで設定した値 (3 日) に従って消去されます。
- [データを今すぐ消去 (Purge Data Now)] 領域で、次の操作を行います。
  1. すべてのデータを消去するか、または指定された日数よりも古いデータを消去します。データはリポジトリに保存されません。
  2. [消去 (Purge)] をクリックします。





## 第 29 章

# レポート

- [Cisco ISE レポート](#) (1095 ページ)
- [レポート フィルタ](#) (1096 ページ)
- [クイック フィルタ条件の作成](#) (1096 ページ)
- [拡張フィルタ条件の作成](#) (1097 ページ)
- [レポートの実行および表示](#) (1098 ページ)
- [レポートのナビゲーション](#) (1098 ページ)
- [レポートのエクスポート](#) (1098 ページ)
- [レポートのスケジュールと保存](#) (1100 ページ)
- [Cisco ISE のアクティブな RADIUS セッション](#) (1100 ページ)
- [使用可能なレポート](#) (1103 ページ)

## Cisco ISE レポート

モニタリング機能およびトラブルシューティング機能とともに Cisco Identity Services Engine (ISE) レポートを使用して、集中管理する場所からのトレンドの分析、システム パフォーマンスおよびネットワーク アクティビティのモニタリングを行います。

Cisco ISE はネットワーク全体からログおよび設定データを収集します。その後、表示と分析のために、データがレポートに集約されます。Cisco ISE には、使用可能な事前定義されたレポートが用意されており、必要に応じてカスタマイズできます。

Cisco ISE レポートは事前設定されており、認証、セッション トラフィック、デバイス管理、設定と管理、およびトラブルシューティングに関する情報の論理カテゴリにグループ化されます。

### 関連トピック

- [レポートの実行および表示](#) (1098 ページ)
- [レポートのエクスポート](#) (1098 ページ)
- [使用可能なレポート](#) (1103 ページ)

## レポート フィルタ

レポートには、シングルセクション レポートとマルチセクション レポートの 2 種類があります。シングルセクション レポートには 1 つのグリッドが含まれており（RADIUS 認証レポート）、マルチセクション レポートには複数のグリッドが含まれており（認証概要レポート）、データがグラフと表の形式で示されます。シングルセクション レポートの [フィルタ (Filter)] ドロップダウンメニューには、[クイック フィルタ (Quick Filter)] と [拡張 フィルタ (Advanced Filter)] があります。マルチセクション レポートでは、拡張 フィルタだけを指定できます。

マルチセクション レポートには、入力が必要な必須拡張 フィルタが 1 つ以上含まれていることがあります。たとえば、健全性の概要レポート（[操作 (Operations)] > [レポート (Reports)] > [診断 (Diagnostics)] ページ）をクリックすると、2 つの必須拡張 フィルタ（[サーバ (Server)] と [時間範囲 (Time Range)]）が表示されます。レポートを生成するには、この両方のフィルタで演算子コマンド、サーバ名、必要な値を指定し、[実行 (Go)] をクリックする必要があります。プラス記号 (+) をクリックして新しい拡張 フィルタを追加できます。マルチセクション レポートは PDF 形式でのみエクスポートできます。特定の時刻または時間間隔で Cisco ISE マルチセクション レポートを実行または再実行するようにスケジュールすることはできません。



(注) レポートをクリックすると、デフォルトでは過去 7 日間のデータが生成されます。ただし一部のマルチセクション レポートでは、時間範囲以外にもユーザが入力する必要のある項目があります。

シングルセクション レポートでは、デフォルトでクイック フィルタが 1 番目の行として表示されます。フィールドには、検索基準を選択できるドロップダウンリストまたはテキストボックスが含まれています。

拡張 フィルタには、1 つ以上の内部条件を含む外部条件が含まれています。外部条件では、検索で指定された内部条件すべてに一致する必要があるか、またはいずれかに一致する必要があるかを指定します。内部条件には、カテゴリ（[エンドポイント ID (Endpoint ID)]、[ID グループ (Identity Group)]）、メソッド（Contains、Does Not Contain などの演算子コマンド）、および時間範囲を条件として指定するために使用される 1 つ以上の条件が含まれています。

## クイック フィルタ条件の作成

ここでは、クイック フィルタ条件の作成方法を説明します。クイック フィルタ条件はシングルセクション レポートでのみ作成できます。

**ステップ 1** [操作 (Operations)] > [レポート (Reports)] を選択し、必要なレポートをクリックします。

**ステップ 2** [設定 (Settings)] ドロップダウンリストから必須フィールドを選択します。

**ステップ 3** データをフィルタリングするため、必須フィールドでドロップダウンリストから選択するか、または特定の文字を入力できます。検索では **Contains** 演算子コマンドが使用されます。たとえば、「K」で始まるテキストをフィルタリングするには **K** と入力し、テキスト内の任意の位置に「geo」が含まれているテキストをフィルタリングするには **geo** と入力します。また、アスタリスク (\*) を使用することもできます。たとえば、**\*abc** で始まり **\*def** で終わる正規表現などです。

クイック フィルタで使用される条件には、**contains**、**starts with**、**ends with**、**starts with or ends with**、および **OR** 演算子で結合する複数の値があります。

**ステップ 4** Enter キーを押します。

## 拡張フィルタ条件の作成

ここでは、拡張フィルタ条件の作成方法を説明します。拡張フィルタは、シングルセクションレポートとマルチセクションレポートで作成できます。シングルセクションレポートの [フィルタ (Filter)] ドロップダウンメニューには、[クイック フィルタ (Quick Filter)] と [拡張フィルタ (Advanced Filter)] があります。マルチセクションレポートでは、拡張フィルタだけを指定できます。

**ステップ 1** [操作 (Operations)] > [レポート (Reports)] を選択し、必要なレポートをクリックします。

**ステップ 2** [フィルタ (Filters)] セクションで [一致 (Match)] ドロップダウンリストから次のいずれかのオプションを選択します。

- a) 指定したすべての条件に一致する必要がある場合は、[すべて (All)] を選択します。
- b) 指定したいいずれか 1 つの条件に一致すればよい場合は、[いずれか (Any)] を選択します。

**ステップ 3** [時間範囲 (Time Range)] ドロップダウンリストから必要なカテゴリを選択します。

**ステップ 4** [演算子コマンド (Operator Commands)] ドロップダウンリストから、必要なコマンドを選択します。たとえば、特定の文字で始まるテキストや ([次の文字で始まる (Begin With)] を使用)、テキスト内の任意の位置に特定の文字が含まれているテキスト ([次の文字を含む (Contains)] を使用) をフィルタリングできます。あるいは、[ログに記録された時刻 (Logged Time)] と対応する [カスタム (Custom)] オプションを選択し、カレンダーからデータをフィルタリングする期間の開始日時と終了日時を指定します。

**ステップ 5** [時間範囲 (Time Range)] ドロップダウンリストから必要なオプションを選択します。

**ステップ 6** [移動 (Go)] をクリックします。

今後の参照のために、フィルタリングされたレポートを保存し、[フィルタ (Filter)] ドロップダウンリストから取得することができます。

## レポートの実行および表示

ここでは、Reports View を使用してレポートを実行、表示、およびナビゲートする方法について説明します。デフォルトでは、レポートをクリックすると過去7日間のデータが生成されます。レポートにデータを表示する時間の増分を指定できます。

**ステップ 1** [操作 (Operations)] > [レポート (Reports)] > [ISE レポート (ISE Reports)] を選択します。

また、各ワークセンターの[レポート (Reports)]リンクに移動して、ワークセンター固有の一連のレポートを確認することもできます。

**ステップ 2** 使用可能なレポート カテゴリからレポートをクリックします。

**ステップ 3** レポートを実行する 1 つ以上のフィルタを選択します。各レポートに、異なるフィルタを使用できます。フィルタの一部は必須で一部は任意選択です。

**ステップ 4** フィルタに適切な値を入力します。

**ステップ 5** [移動 (Go)] をクリックします。

### 関連トピック

[レポートのエクスポート](#) (1098 ページ)

[使用可能なレポート](#) (1103 ページ)

[使用可能なレポート](#) (1103 ページ)

## レポートのナビゲーション

レポート出力から詳細情報を取得できます。たとえば、5 カ月の期間に 1 つのレポートを生成した場合、グラフと表には月単位の目盛りでレポートの集約データが表示されます。

表内の特定の値をクリックすると、この特定のフィールドに関連する別のレポートを表示できます。たとえば、認証概要レポートには、ユーザまたはユーザグループの失敗したカウントが表示されます。失敗したカウントをクリックすると、その特定の失敗したカウントについての認証概要レポートが開きます。

## レポートのエクスポート

次のファイル形式でレポート データをエクスポートできます。

- カンマ区切り値 (.csv) ファイルとしての Excel スプレッドシート。データをエクスポートすると、レポートの場所を詳細に示した電子メールを受信します。
- ローカル ディスクに保存できる Microsoft Excel のカンマ区切り値 (.csv) ファイル。
- ローカル ディスクに保存できる Adobe Acrobat Document (.pdf) ファイル。





- (注) Microsoft Excel 形式の場合、エクスポートできるのは 5000 レコードです。PDF ファイル形式の場合、エクスポートできるのは 1000 レコードです。

次のレポートは PDF ファイル形式でのみエクスポートできます。

- 認証概要 (Authentication Summary)
- 健全性の概要
- RBACL ドロップ概要



- (注) RBACL 廃棄パケットのフローは、Cisco Catalyst 6500 シリーズ スイッチでのみ使用できます。

- ゲスト スポンサー概要
- エンドポイント プロファイルの変更
- ネットワーク デバイスのセッション ステータス



- (注) レポートをエクスポートした後で英語以外の文字を正しく表示するには、UTF-8 文字エンコーディングを有効にして Microsoft Excel にファイルをインポートする必要があります。UTF-8 文字エンコーディングを有効にしないで、エクスポートした .csv ファイルを Microsoft Excel で直接開いた場合、レポートの英語以外の文字は文字化けした状態で表示されます。



- (注) レポート データは、プライマリ PAN からのみ .csv 形式にエクスポートできます。

**ステップ 1** 「レポートの実行と表示」の項の説明に従ってレポートを実行します。

**ステップ 2** レポートサマリーページの右上隅にある [エクスポート (Export)] [エクスポート先 (Export To)] をクリックします。

**ステップ 3** エクスポートするデータ カラムを指定します。

**ステップ 4** ドロップダウン リストからリポジトリを選択します。

**ステップ 5** [エクスポート (Export)] をクリックします。

## レポートのスケジュールと保存

レポートをカスタマイズし、変更内容を新しいレポートとして保存するか、またはレポートサマリー ページの右上隅にある [マイ レポート (My Reports)] でデフォルトのレポート設定を復元できます。

Cisco ISE レポートをカスタマイズおよびスケジュールして、特定の時間または時間間隔で実行および再実行することもできます。レポートが生成されたら、電子メール通知を送受信することもできます。

次のレポートはスケジュールできません。

- 認証概要 (Authentication Summary)
- 健全性の概要
- RBACL ドロップ概要
- ゲスト スポンサー概要
- エンドポイント プロファイルの変更
- ネットワーク デバイスのセッション ステータス



(注) Cisco ISE レポートの保存またはスケジュールリング (カスタマイズ) は、PAN からのみ実行できます。

**ステップ 1** 「レポートの実行と表示」の項の説明に従ってレポートを実行します。

**ステップ 2** レポート サマリー ページの右上隅の [マイ レポート (My Reports)] をクリックします。

**ステップ 3** ダイアログボックスに必要な詳細を入力します。

**ステップ 4** [新規として保存 (Save as New)] をクリックします。

レポートを保存した後、保存済みレポートに戻ると、すべてのフィルタ オプションがデフォルトでオンになります。使用しないフィルタをオフにする必要があります。

[マイ レポート (My Reports)] カテゴリから、保存したレポートを削除することもできます。

## Cisco ISE のアクティブな RADIUS セッション

Cisco ISE では、ライブ セッション用の動的な許可変更 (CoA) 機能が提供されます。この機能を使用すると、アクティブな RADIUS セッションを動的に制御できます。次のタスクを実行

するために再認証または接続解除要求をネットワーク アクセス デバイス (NAD) に送信できます。

- 認証に関連する問題のトラブルシューティング：[セッション再認証 (Session reauthentication)] オプションを使用して、再認証を試みることができます。ただし、アクセスを制限するためにこのオプションを使用しないでください。アクセスを制限するには、シャットダウン オプションを使用します。
- 問題のあるホストのブロック：[ポート シャットダウンによるセッション終了 (Session termination with port shutdown)] オプションを使用して、ネットワークに大量のトラフィックを送信する、ウイルスなどに感染したホストをブロックできます。ただし、RADIUS プロトコルでは、シャットダウンされたポートを再度有効にするための方法は現在サポートされていません。
- エンドポイントでの IP アドレス再取得の強制：サブリカントまたはクライアントを持たないエンドポイントに対して [ポート バウンスでのセッション終了 (Session termination with port bounce)] オプションを使用し、VLAN 変更後に DHCP 要求を生成できます。
- エンドポイントへの更新された許可ポリシーのプッシュ：[セッション再認証 (Session reauthentication)] オプションを使用して、管理者の裁量に基づいた既存のセッションの許可ポリシーの変更などの、更新されたポリシー設定を適用できます。たとえば、ポスチャ確認が有効である場合にエンドポイントが最初にアクセスを許可されると、通常、エンドポイントは隔離されます。エンドポイントのアイデンティティおよびポスチャが確認された後、Session reauthentication コマンドをエンドポイントに送信して、エンドポイントがそのポスチャに基づいて実際の許可ポリシーを取得できるようにすることが可能です。

デバイスによって CoA コマンドが認識されるためには、適切にオプションを設定することが重要です。

CoA が適切に動作するには、動的な許可変更を必要とする各デバイスの共有秘密情報を設定する必要があります。Cisco ISE では、デバイスからのアクセス要求、およびデバイスへの CoA コマンドの発行において、共有秘密情報設定が使用されます。



(注) このリリースの Cisco ISE では、表示可能な認証されたエンドポイント セッションの最大数が 100,000 に制限されています。

#### 関連トピック

[RADIUS セッションの許可の変更](#) (1101 ページ)

## RADIUS セッションの許可の変更

ネットワークの一部のネットワーク アクセス デバイスでは、リロード後にアカウンティング 停止パケットまたはアカウンティング オフ パケットが送信されないことがあります。このため、[セッションディレクトリ (Session Directory)] の下のレポートでは、有効なセッションと期限切れのセッションの 2 つのセッションが表示される場合があります。

アクティブな RADIUS セッションの許可を動的に変更する場合や、アクティブな RADIUS セッションの接続を解除する場合には、最新のセッションを選択する必要があります。

**ステップ 1** [操作 (Operations)] > [RADIUS ライブログ (RADIUS Livelog)] の順に選択します。

**ステップ 2** [ライブ セッションの表示 (Show Live Session)] にビューを切り替えてください。

**ステップ 3** CoA を発行する RADIUS セッションの CoA リンクをクリックし、次のいずれかのオプションを選択します。

- [SAnet セッションクエリー (SAnet Session Query)] : SAnet でサポートされるデバイスからのセッションに関する情報をクエリーするために使用します。
- [セッション再認証 (Session reauthentication)] : セッションを再認証します。CoA をサポートする ASA デバイスに確立されるセッションにこのオプションを選択すると、セッションポリシーブッシュ CoA が呼び出されます。
- [最後の方式でのセッション再認証 (Session reauthentication with last)] : そのセッションに対して、最後に成功した認証方式を使用します。
- [再実行によるセッション再認証 (Session reauthentication with rerun)] : 設定されている認証方式を最初から実行します。

(注) [最後の方式でのセッション再認証 (Session reauthentication with last)] オプションおよび [再実行によるセッション再認証 (Session reauthentication with rerun)] オプションは、Cisco IOS ソフトウェアで現在サポートされていません。

- [セッション終了 (Session termination)] : 単にセッションを終了します。スイッチは、異なるセッションでクライアントを再認証します。
- [ポート バウンスでのセッション終了 (Session termination with port bounce)] : セッションを終了し、ポートを再起動します。
- [ポート シャットダウンによるセッション終了 (Session termination with port shut down)] : セッションを終了し、ポートをシャットダウンします。

**ステップ 4** [実行 (Run)] をクリックして、選択した再認証または終了オプションとともに CoA を発行します。

CoA に失敗した場合は、次の理由が考えられます。

- デバイスで CoA がサポートされていない。
- アイデンティティまたは許可ポリシーに変更があった。
- 共有秘密が一致しない。

## 使用可能なレポート

次の表に、事前設定済みレポートをカテゴリ別に分類して示します。また、レポートの機能およびロギング カテゴリについても説明します。

| レポート名          | 説明                                                                                                   | ロギング カテゴリ                                                                                                                                                                              |
|----------------|------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 監査 (Audit)     |                                                                                                      |                                                                                                                                                                                        |
| 適応型ネットワーク制御の監査 | 適応型ネットワーク制御の監査レポートは、RADIUS アカウンティングに基づきます。つまり、エンドポイントごとにすべてのネットワーク セッションの履歴レポートを表示します。               | [管理 (Administration)] > [システム (System)] > [ロギング (Logging)] > [ロギング カテゴリ (Logging Categories)] を選択し、[成功した認証 (Passed Authentications)] および [RADIUS アカウンティング (RADIUS Accounting)] を選択します。 |
| 管理者ログイン        | 管理者ログイン レポートには、GUI ベースの管理者ログイン イベントと成功した CLI ログイン イベントに関する情報が提供されます。                                 | [管理 (Administration)] > [システム (System)] > [ロギング (Logging)] > [ロギング カテゴリ (Logging Categories)] を選択して、[管理および操作の監査 (Administrative and Operational audit)] を選択します。                        |
| 変更設定監査         | 変更設定監査レポートは、指定した期間内の設定変更の詳細を提供します。機能をトラブルシューティングする必要がある場合、このレポートは、最新の設定変更が問題の原因となったかどうかを決定するのに役立ちます。 | [管理 (Administration)] > [システム (System)] > [ロギング (Logging)] > [ロギング カテゴリ (Logging Categories)] を選択して、[管理および操作の監査 (Administrative and Operational audit)] を選択します。                        |

| レポート名    | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | ロギング カテゴリ |
|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| データ消去の監査 | <p>データ消去の監査レポートは、ロギング データが消去されている時間を記録します。</p> <p>このレポートは、データ消去の 2 つのソースを反映します。</p> <p>毎日午前 4 時に、Cisco ISE は、[管理 (Administration)] &gt; [メンテナンス (Maintenance)] &gt; [データ消去 (Data Purging)] ページで設定した基準に一致するロギング ファイルがあるかどうかを確認します。あった場合は、ファイルが削除され、このレポートに記録されます。さらに、Cisco ISE は、常にログ ファイルに使用される記憶域を最大 80% に維持します。1 時間ごとに、Cisco ISE はこの割合を確認し、80% のしきい値に再び到達するまで、最も古いデータが削除されます。この情報もこのレポートに記録されます。</p> <p>高いディスク容量使用率がある場合、しきい値の 80% で「ISE モニタ ノードはもうすぐ割り当てられている最大量を超えます (ISE Monitor node(s) is about to exceed the maximum amount allocated)」という警告メッセージが表示されます。その後、しきい値の 90% で「ISE モニタ ノードは割り当てられている最大量を超えました (ISE Monitor node(s) has exceeded the maximum amount allocated)」という警告メッセージが表示されます。</p> | —         |

| レポート名             | 説明                                                                                                               | ロギング カテゴリ                                                                                                                                                       |
|-------------------|------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| エンドポイントのアクティビティ消去 | エンドポイントのアクティビティ消去レポートを使用すると、エンドポイントのアクティビティ消去の履歴を確認できます。このレポートは、プロファイラ ロギング カテゴリが有効である必要があります。デフォルトでは有効になっています。  | [管理 (Administration)] > [システム (System)] > [ロギング (Logging)] > [ロギング カテゴリ (Logging Categories)] を選択し、[プロファイラ (Profiler)] を選択します。                                  |
| 内部管理者の概要          | 内部管理者の概要レポートを使用すると、管理者ユーザのエンタイトルメントを確認できます。このレポートから、管理者ログイン レポートおよび変更設定監査レポートにもアクセスでき、それにより、管理者ごとにこれらの詳細を表示できます。 | —                                                                                                                                                               |
| 操作監査              | 操作監査レポートは、次のような操作の変更にに関する詳細を提供します。バックアップの実行、Cisco ISE ノードの登録、またはアプリケーションの再起動。                                    | [管理 (Administration)] > [システム (System)] > [ロギング (Logging)] > [ロギング カテゴリ (Logging Categories)] を選択して、[管理および操作の監査 (Administrative and Operational audit)] を選択します。 |

| レポート名                      | 説明                                                                                                                                                                                                                                                     | ロギング カテゴリ                                            |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------|
| pxGrid 管理者の監査              | <p>pxGrid 管理者の監査レポートは、プライマリ PAN でのクライアントの登録、クライアントの登録解除、クライアントの承認、トピックの作成、トピックの削除、パブリッシャとサブスクライバの追加、およびパブリッシャとサブスクライバの削除など、pxGrid の管理処理の詳細を提供します。</p> <p>すべてのレコードに、ノードで処理を実行した管理者の名前が示されます。</p> <p>管理者およびメッセージの基準に基づいて、pxGrid 管理者の監査レポートをフィルタできます。</p> | —                                                    |
| セキュアな通信の監査                 | <p>セキュアな通信の監査レポートには、認証の失敗、ブレイクインの可能性がある試み、SSH ログイン、失敗したパスワード、SSH ログアウト、無効なユーザ アカウントなどが含まれる、Cisco ISE 管理 CLI のセキュリティ関連イベントに関する監査の詳細が提供されます。</p>                                                                                                         | —                                                    |
| User Change Password Audit | User Change Password Audit レポートは、従業員のパスワード変更に関する検証を表示します。                                                                                                                                                                                              | 管理および操作の監査<br>(Administrative and Operational audit) |
| デバイス管理                     |                                                                                                                                                                                                                                                        |                                                      |



| レポート名                | 説明                                                                                                                                                              | ロギング カテゴリ                                                                                                                                                    |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| TACACS アカウンティング      | TACACS アカウンティング レポートは、デバイス セッションのアカウンティングの詳細を提供します。ユーザおよびデバイスの生成された時刻およびログに記録された時刻に関する情報が表示されます。                                                                | [管理 (Administration)] > [システム (System)] > [ロギング (Logging)] > [ロギングカテゴリ (Logging Categories)] を選択し、[TACACS アカウンティング (TACACS Accounting)] を選択します。              |
| TACACS 認証            | TACACS 認証レポートは、Cisco ISE と認証されたユーザまたはデバイスの間のネットワーク セッションおよびセッションを認証した ISE ノードの詳細、さらに認証が失敗した原因に関する詳細を提供します。使用されるセッション キーおよび認証ポリシーも表示されます。                        | [管理 (Administration)] > [システム (System)] > [ロギング (Logging)] > [ロギングカテゴリ (Logging Categories)] を選択し、[TACACS 認証 (TACACS Authentication)] を選択します。                |
| TACACS 許可            | TACACS 許可レポートは、Cisco ISE とユーザまたはデバイスの間のネットワーク セッションの詳細を提供します。ISE ノードによって許可されたネットワーク デバイス名に関する情報が表示されます。デバイスとそのポートの位置に関する情報が表示されます。管理権限とデバイス管理者が実行したコマンドも表示されます。 | [管理 (Administration)] > [システム (System)] > [ロギング (Logging)] > [ロギングカテゴリ (Logging Categories)] を選択し、[TACACS 許可 (TACACS Authorization)] を選択します。                 |
| TACACS コマンド アカウンティング | TACACS コマンド アカウンティング レポートは、デバイス管理者によって実行されたコマンドおよびコマンド引数の詳細と、対応するネットワーク デバイスの詳細を提供します。                                                                          | [管理 (Administration)] > [システム (System)] > [ロギング (Logging)] > [ロギングカテゴリ (Logging Categories)] を選択し、[TACACS コマンド アカウンティング (TACACS Command Accounting)] を選択します。 |
| 診断                   |                                                                                                                                                                 |                                                                                                                                                              |

| レポート名             | 説明                                                                                                                                                                             | ロギング カテゴリ                                                                                                                                                                                                                                                                       |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AAA の診断           | AAA の診断レポートは、Cisco ISE とユーザ間のすべてのネットワークセッションの詳細を提供します。ユーザがネットワークにアクセスできない場合、トレンドを識別し、問題が特定のユーザに隔離されているか、またはより広範囲の問題を示しているかを識別するために、このレポートを確認できます。                              | [管理 (Administration) ]>[システム (System) ]>[ロギング (Logging) ]>[ロギング カテゴリ (Logging Categories) ] を選択し、次のロギング カテゴリを選択します。[ポリシー診断 (Policy Diagnostics) ]、[ID ストア診断 (Identity Stores Diagnostics) ]、[認証フロー診断 (Authentication Flow Diagnostics) ]、および [RADIUS 診断 (RADIUS Diagnostics) ]。 |
| AD コネクタ操作         | AD コネクタ操作レポートは、Cisco ISE サーバのパスワードのリフレッシュ、Kerberos チケットの管理、DNS クエリ、DC 検出、LDAP、および RPC 接続管理など、AD コネクタが実行する操作のログを提供します。<br><br>AD の障害がいくつか発生している場合、このレポートで詳細を確認して考えられる原因を特定できます。 | [管理 (Administration) ]>[システム (System) ]>[ロギング (Logging) ]>[ロギング カテゴリ (Logging Categories) ] を選択し、[AD コネクタ (AD Connector) ] を選択します。                                                                                                                                              |
| エンドポイント プロファイルの変更 | エンドポイント (MAC アドレス) 別上位認証レポートは、ネットワークにアクセスするために各エンドポイントの MAC アドレスが Cisco ISE によって許可された回数を表示します。                                                                                 | 成功した認証、失敗した試行 (Passed Authentications, Failed Attempts)                                                                                                                                                                                                                         |

| レポート名  | 説明                                                                                                                                                                                                                                                                                                                                                                                                         | ロギング カテゴリ |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| 健全性の概要 | <p>健全性の概要レポートは、ダッシュボードのような詳細を提供します。ただし、ダッシュボードは過去 24 時間のデータしか表示しませんが、このレポートを使用するとより多くの履歴データを確認できます。</p> <p>データの一貫したパターンを調べるためにこのデータを評価できます。たとえば、大多数の従業員が就業時間を開始するときに、非常に高い CPU 使用率が予想されます。これらのトレンドの不整合がわかれば、潜在的な問題を識別できます。</p> <p>[CPU 使用率 (CPU Usage) ]</p> <p>テーブルには、各種 Cisco ISE 機能の CPU 使用率 (%) が表示されます。 <b>show cpu usage</b> CLI コマンドの出力がこのテーブルに表示されるため、これらの値を、展開内で発生している問題と関連付け、原因を特定することができます。</p> | —         |

| レポート名         | 説明                                                                                                                                                                                                                                                                                                                                                                 | ロギング カテゴリ |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| ISE カウンタ      | <p>ISE カウンタ レポートには、さまざまな属性のしきい値が示されます。各種属性の値の収集間隔は異なり、またデータは表形式で表示されます。5 分間隔で収集される属性と 5 分よりも長い間隔で収集される属性があります。</p> <p>このデータを評価してトレンドを確認し、しきい値よりも高い値を検出した場合には、展開内で発生している問題にこの情報を関連付け、考えられる原因を特定できます。</p> <p>Cisco ISE はデフォルトでこれらの属性の値を収集します。このデータ収集を無効にするには、Cisco ISE CLI で <b>application configure ise</b> コマンドを使用します。カウンタ属性の収集を有効または無効にするには、オプション 14 を選択します。</p> | —         |
| 主要パフォーマンス測定指標 | <p>主要パフォーマンス測定指標 レポートには、展開に接続しているエンドポイントの数と、1 時間あたりに各 PAN が処理する RADIUS 要求の数に関する統計情報が表示されます。このレポートには、サーバの平均負荷、要求あたりの平均遅延、および平均トランザクション数/秒が示されます。</p>                                                                                                                                                                                                                | —         |

| レポート名          | 説明                                                                                                                                                                                         | ロギング カテゴリ |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| 設定が誤っている NAS   | <p>設定が誤っている NAS レポートは、通常、アカウントティング情報を頻繁に送信するときに、アカウントティング頻度が不正確な NAD に関する一般情報を提供します。修正処置を行い、設定が誤っている NAD を修正すると、レポートはレポートに修正済み確認を表示します。</p> <p>(注) レポートを実行するには、RADIUS 抑制を有効にする必要があります。</p> | —         |
| 設定が誤っているサブリカント | <p>設定が誤っているサブリカントのレポートは、特定のサブリカントが実行した失敗試行のため、設定が誤っているサブリカントの一覧および統計情報を提供します。修正処置を行い、設定が誤っているサブリカントを修正すると、レポートはレポートに修正済み確認を表示します。</p> <p>(注) レポートを実行するには、RADIUS 抑制を有効にする必要があります。</p>       | —         |

| レポート名                   | 説明                                                                                                                                                                                                                                                                                                                                    | ロギング カテゴリ                                                                                                                                                |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| ネットワーク デバイスのセッション ステータス | <p>ネットワーク デバイスのセッション ステータス概要レポートを使用すると、直接スイッチにログインせずにスイッチ設定を表示することができます。</p> <p>Cisco ISE は SNMP クエリを使用してこれらの詳細にアクセスするので、ネットワーク デバイスは SNMP v1/v2c を使用して設定されている必要があります。</p> <p>ユーザにネットワークの問題が発生している場合に、このレポートは、問題が Cisco ISE ではなくスイッチの設定に関連しているかどうかを識別するのに役立ちます。</p>                                                                   | —                                                                                                                                                        |
| OCSP モニタリング             | <p>OCSP モニタリング レポートは、Online Certificate Status Protocol (OCSP) サービスのステータスを指定します。</p> <p>Cisco ISE が正常に証明書サーバに連絡し、証明書ステータス監査を提供できるかどうかを識別します。Cisco ISE によって実行されたすべての OCSP 証明書検証操作の概要が提供されます。適切な/失効したプライマリ/セカンダリ証明書に関連する情報を OCSP サーバから取得します。Cisco ISE は、応答をキャッシュし、後続の OCSP モニタリング レポートの生成に使用します。キャッシュがクリアされる場合は、OCSP サーバから情報を取得します。</p> | <p>[管理 (Administration)] &gt; [システム (System)] &gt; [ロギング (Logging)] &gt; [ロギング カテゴリ (Logging Categories)] を選択し、[システム診断 (System Diagnostics)] を選択します。</p> |

| レポート名       | 説明                                                                                                                                                                                                                                                                                            | ロギング カテゴリ                                                                                                                                                                                                                                                                         |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RADIUS エラー  | <p>RADIUS エラー レポートを使用すると、ドロップされた RADIUS 要求（未知のネットワーク アクセス デバイスからの廃棄された認証/アカウント要求）、EAP 接続タイムアウトおよび未知の NAD をチェックできます。</p> <p>(注) ISE は、ユーザ認証が進行中のときにエンドポイントのアカウント停止要求をサイレントにドロップする場合があります。ただし、ISE はユーザ認証が完了すると、すべてのアカウント要求の認識を開始します。</p>                                                        | <p>[管理 (Administration)] &gt; [システム (System)] &gt; [ロギング (Logging)] &gt; [ロギング カテゴリ (Logging Categories)] を選択し、[失敗した試行 (Failed Attempts)] を選択します。</p>                                                                                                                             |
| システム診断      | <p>システム診断レポートは Cisco ISE ノードのステータスの詳細を提供します。Cisco ISE ノードが登録できない場合、このレポートを確認して問題をトラブルシューティングすることができます。</p> <p>このレポートでは、最初に複数の診断ロギング カテゴリを有効にする必要があります。これらのログを収集すると、Cisco ISE パフォーマンスに悪影響を及ぼすことがあります。したがって、これらのカテゴリはデフォルトで有効ではなく、データを収集するのに十分な時間だけ有効にする必要があります。そうでない場合は、30 分後に自動的に無効になります。</p> | <p>[管理 (Administration)] &gt; [システム (System)] &gt; [ロギング (Logging)] &gt; [ロギング カテゴリ (Logging Categories)] を選択し、次のロギング カテゴリを選択します。[内部操作診断 (Internal Operations Diagnostics)]、[分散管理 (Distributed Management)]、および [管理者の認証と許可 (Administrator Authentication and Authorization)]。</p> |
| エンドポイントとユーザ |                                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                   |

| レポート名 | 説明                                                                                                                                                                                                                                                                 | ロギング カテゴリ |
|-------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| 認証概要  | <p>認証概要レポートは、RADIUS 認証に基づいています。それにより、最も一般的な認証および認証失敗の原因を特定することができます。たとえば、ある Cisco ISE サーバが他のサーバよりもはるかに多くの認証を処理している場合、負荷を適切に分散するためにユーザを別の Cisco ISE サーバに再割り当てする場合があります。</p> <p>(注) 認証概要レポートまたはダッシュボードが失敗または成功した認証に対応する最新のデータを収集して表示するため、レポートの内容は数分の遅延の後に表示されます。</p> | —         |



| レポート名          | 説明                                                                                                                                                                                                                                                                                                   | ロギング カテゴリ                                                                                                                                                                                                                                                                            |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| クライアントプロビジョニング | <p>クライアントプロビジョニングレポートは、特定のエンドポイントに適用されるクライアントプロビジョニングエージェントについて示します。このレポートを使用すると、各エンドポイントに適用されるポリシーを確認してエンドポイントが正しくプロビジョニングされたことを確認することができます。</p> <p>(注) エンドポイントが ISE に接続されない (セッションが確立されない) 場合、またはネットワークアドレス変換 (NAT) アドレスがセッションで使用される場合、エンドポイントの MAC アドレスは [エンドポイントID (Endpoint ID)] 列に表示されません。</p> | <p>[管理 (Administration)] &gt; [システム (System)] &gt; [ロギング (Logging)] &gt; [ロギング カテゴリ (Logging Categories)] を選択し、[ポスチャおよびクライアントプロビジョニングの監査 (Posture and Client Provisioning Audit)] および [ポスチャおよびクライアントプロビジョニングの診断 (Audit and Posture and Client Provisioning Diagnostics)] を選択します。</p> |
| 現在のアクティブなセッション | <p>現在アクティブなセッションレポートを使用すると、指定の期間内のその時点でネットワーク上に存在していた者に関する詳細を含むレポートをエクスポートできます。</p> <p>ユーザがネットワークにアクセスできない場合、セッションが認証または終了されているかどうか、またはセッションに別の問題があるかどうかを確認できます。</p>                                                                                                                                 | —                                                                                                                                                                                                                                                                                    |

| レポート名            | 説明                                                                                                                                                                                                  | ロギング カテゴリ                                                                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| 外部モバイル デバイス管理    | <p>外部モバイル デバイス管理レポートは、Cisco ISE と外部モバイルデバイス管理 (MDM) サーバ間の統合に関する詳細を提供します。</p> <p>このレポートを使用すると、MDMサーバに直接ログインせずに、MDMサーバによってプロビジョニングされたエンドポイントを確認することができます。また、登録および MDM コンプライアンス ステータスなどの情報が表示されます。</p> | [管理 (Administration)] > [システム (System)] > [ロギング (Logging)] > [ロギング カテゴリ (Logging Categories)] を選択し、[MDM] を選択します。                         |
| パッシブ ID          | パッシブ ID レポートでは、ドメインコントローラへの WMI 接続の状態をモニタし、関連する統計情報 (受信した通知の数、1 秒あたりのユーザ ログイン/ログアウト回数など) を収集することができます。                                                                                              | [管理 (Administration)] > [システム (System)] > [ロギング (Logging)] > [ロギング カテゴリ (Logging Categories)] を選択し、[ID マッピング (Identity Mapping)] を選択します。 |
| 手動証明書プロビジョニング    | 手動証明書プロビジョニング レポートには、証明書プロビジョニング ポータル経由で手動でプロビジョニングされたすべての証明書がリストされます。                                                                                                                              | —                                                                                                                                        |
| 条件によるポスチャ アセスメント | 条件によるポスチャ アセスメント レポートでは、ISE に設定されたポスチャ ポリシー条件に基づいてレコードを表示し、最新のセキュリティ設定またはアプリケーションがクライアント マシンで利用可能かどうかを確認できます。                                                                                       | —                                                                                                                                        |

| レポート名                 | 説明                                                                                                                                                                                                        | ロギング カテゴリ                                                                                                                           |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| エンドポイントによるポスチャ アセスメント | [エンドポイントによるポスチャ アセスメント (Posture Assessment by Endpoint) ] レポートには、エンドポイントの時間、ステータス、PRA アクションなどの詳細な情報が提供されます。[詳細 (Details) ] をクリックして、エンドポイントの詳細情報を表示することができます。                                              | —                                                                                                                                   |
| プロファイリングされたエンドポイントの概要 | <p>プロファイリングされたエンドポイントの概要レポートは、ネットワークにアクセスしているエンドポイントに関するプロファイリングの詳細を提供します。</p> <p>(注) Cisco IP Phone など、セッション時間を登録しないエンドポイントの場合、[エンドポイント (Endpoint) ] セッション時間フィールドに、[該当なし (Not Applicable) ] と表示されます。</p> | [管理 (Administration) ] > [システム (System) ] > [ロギング (Logging) ] > [ロギング カテゴリ (Logging Categories) ] を選択し、[プロファイラ (Profiler) ] を選択します。 |

| レポート名           | 説明                                                                                                                                                                                                                                                                                   | ロギング カテゴリ                                                                                                                                                                              |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RADIUS アカウンティング | <p>RADIUS アカウンティング レポートは、ユーザがネットワーク上に存在した時間を識別します。ユーザがネットワークにアクセスできない場合、Cisco ISE がネットワーク接続問題の原因であるかどうか、このレポートを使用して識別できます。</p> <p>(注) 暫定アップデートに、指定されたセッションの IPv4 または IPv6 アドレスの変更にに関する情報が含まれている場合、Radius アカウンティング暫定アップデートは [RADIUS アカウンティング (RADIUS Accounting) ] レポートに含まれていません。</p> | [管理 (Administration) ]>[システム (System) ]>[ロギング (Logging) ]>[ロギング カテゴリ (Logging Categories) ] を選択し、[RADIUS アカウンティング (RADIUS Accounting) ] を選択します。                                        |
| RADIUS 認証       | RADIUS 認証レポートを使用すると、認証失敗および成功の履歴を確認できます。ユーザがネットワークにアクセスできない場合、このレポートの詳細を確認して考えられる原因を識別できます。                                                                                                                                                                                          | [管理 (Administration) ]>[システム (System) ]>[ロギング (Logging) ]>[ロギング カテゴリ (Logging Categories) ] を選択し、次のロギング カテゴリを選択します。[成功した認証 (Passed Authentications) ] および [失敗した試行 (Failed Attempts) ]。 |
| 登録済みエンドポイント     | 登録済みエンドポイント レポートは、従業員によって登録されているすべてのパーソナル デバイスを表示します。                                                                                                                                                                                                                                | —                                                                                                                                                                                      |

| レポート名           | 説明                                                                                                                     | ロギング カテゴリ                                                                                                                |
|-----------------|------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| 拒否エンドポイント       | 拒否エンドポイント レポートには、従業員が登録したパーソナル デバイスのうち、拒否されたデバイスまたはリリースされたデバイスがすべて表示されます。このレポートのデータは、Plus ライセンスをインストールしている場合にのみ使用可能です。 | —                                                                                                                        |
| サブリカント プロビジョニング | サブリカント プロビジョニング レポートは、従業員のパーソナル デバイスにプロビジョニングされたサブリカントに関する詳細を提供します。                                                    | ポスチャおよびクライアント<br>プロビジョニングの監査<br>(Posture and Client Provisioning Audit)                                                  |
| エンドポイントによる上位承認  | エンドポイント (MAC アドレス) 別上位承認レポートは、ネットワークにアクセスするために各エンドポイントの MAC アドレスが Cisco ISE によって許可された回数を表示します。                         | 成功した認証、失敗した試行<br>(Passed Authentications, Failed Attempts)                                                               |
| ユーザ別上位承認        | ユーザ別上位承認レポートは、ネットワークにアクセスするために各ユーザが Cisco ISE によって許可された回数を表示します。                                                       | 成功した認証、失敗した試行<br>(Passed Authentications, Failed Attempts)                                                               |
| ゲスト             |                                                                                                                        |                                                                                                                          |
| AUP 受け入れステータス   | AUP 受け入れステータス レポートには、すべてのゲストポータルからの AUP 承認の詳細が示されます。                                                                   | [管理 (Administration)] > [システム (System)] > [ロギング (Logging)] > [ロギング カテゴリ (Logging Categories)] を選択し、[ゲスト (Guest)] を選択します。 |

| レポート名        | 説明                                                                                                    | ロギング カテゴリ |
|--------------|-------------------------------------------------------------------------------------------------------|-----------|
| ゲスト アカウンティング | ゲスト アカウンティング レポートは、RADIUS アカウンティング レポートのサブセットです。アクティブなゲストまたはゲスト ID グループに割り当てられたすべてのユーザがこのレポートに表示されます。 | —         |

| レポート名         | 説明 | ロギング カテゴリ                                                                                                                                          |
|---------------|----|----------------------------------------------------------------------------------------------------------------------------------------------------|
| マスター ゲスト レポート |    | [管理 (Administration) ]>[システム (System) ]>[ロギング (Logging) ]>[ロギング カテゴリ (Logging Categories) ]<br>を選択して、[成功した認証 (Passed Authentications) ]<br>を選択します。 |

| レポート名 | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | ロギング カテゴリ |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
|       | <p>マスター ゲスト レポートは、さまざまなゲストアクセスレポートからデータを結合し、異なるレポート ソースからデータをエクスポートできるようにします。マスター ゲスト レポートは、ゲスト ユーザがアクセスしている Web サイトに関する詳細も提供します。このレポートは、セキュリティ 監査の目的で使用し、ゲスト ユーザがネットワークにアクセスした時間、およびそこで行った操作を示すことができます。</p> <p>また、ゲスト トラフィックに使用するネットワーク アクセス デバイス (NAD) の HTTP インスペクションを有効にする必要もあります。この情報は、NAD によって Cisco ISE に返送されます。</p> <p>クライアントが最大同時セッションの制限数に到達した時期を確認するには、管理者ポータルから、[管理 (Administration)] &gt; [システム (System)] &gt; [ロギング (Logging)] &gt; [ロギングカテゴリ (Logging Categories)] の順に選択し、次を実行します。</p> <ol style="list-style-type: none"> <li>1. 「認証フロー診断」のロギング カテゴリのログ レベルを [警告 (WARN)] から [情報 (INFO)] に上げます。</li> <li>2. AAA 診断の [ロギングカテゴリ (Logging Category)] の下で [LogCollectorターゲット</li> </ol> |           |



| レポート名           | 説明                                                                                                                                                                                                                                              | ロギング カテゴリ                                                                                                                           |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
|                 | (LogCollector Target) ] を [使用可能 (Available) ] から [選択済み (Selected) ] に変更します。                                                                                                                                                                     |                                                                                                                                     |
| デバイスのログインおよび監査  | デバイスのログインおよび監査レポートは、デバイス ポータルでユーザが実行するログイン アクティビティと操作についての詳細を提供します。                                                                                                                                                                             | [管理 (Administration) ] > [システム (System) ] > [ロギング (Logging) ] > [ロギング カテゴリ (Logging Categories) ] を選択し、[デバイス (My Devices) ] を選択します。 |
| スポンサーのログインおよび監査 | <p>スポンサーのログインおよび監査レポートは、スポンサー ポータルでのゲスト ユーザのログイン、追加、削除、有効化、一時停止、および更新操作の詳細、ならびにスポンサーのログイン アクティビティの詳細を提供します。</p> <p>ゲスト ユーザを一括で追加すると、[ゲストユーザ (Guest Users) ] カラムの下に表示されます。このカラムは、デフォルトではオフになっています。エクスポート時に、これらの一括処理されたユーザもエクスポート ファイルに存在します。</p> | [管理 (Administration) ] > [システム (System) ] > [ロギング (Logging) ] > [ロギング カテゴリ (Logging Categories) ] を選択し、[ゲスト (Guest) ] を選択します。       |
| SXP             |                                                                                                                                                                                                                                                 |                                                                                                                                     |
| SXP バインディング     | SXP バインディング レポートは、SXP 接続を介して交換される IP-SGT バインディングに関する情報を提供します。                                                                                                                                                                                   | —                                                                                                                                   |
| SXP 接続          | このレポートを使用して、SXP 接続のステータスをモニタしたり、ピア IP、SXP ノード IP、VPN 名、SXP モードなど、その接続に関連する情報を収集できます。                                                                                                                                                            | —                                                                                                                                   |

| レポート名        | 説明                                                                                                                                                                                                                                                                                            | ロギング カテゴリ |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| TrustSec     |                                                                                                                                                                                                                                                                                               |           |
| RBACL ドロップ概要 | <p>RBACL ドロップ概要レポートは、拡張 Cisco ISE ライセンスのみで利用できる TrustSec 機能に固有です。</p> <p>また、このレポートでは、ドロップされたイベントの NetFlow イベントを Cisco ISE に送信するようにネットワーク デバイスを設定する必要があります。</p> <p>ユーザが特定のポリシーまたはアクセスに違反した場合、パケットがドロップされ、このレポートに示されます。</p> <p>(注) RBACL 廃棄パケットのフローは、Cisco Catalyst 6500 シリーズスイッチでのみ使用できます。</p> | —         |

| レポート名                  | 説明                                                                                                                                                                                                                                                                                                | ロギング カテゴリ |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| ユーザ別上位 N 個の RBACL ドロップ | <p>ユーザ別上位 N 個の RBACL ドロップ レポートは、拡張 Cisco ISE ライセンスのみで利用できる TrustSec 機能に固有です。</p> <p>また、このレポートでは、ドロップされたイベントの NetFlow イベントを Cisco ISE に送信するようにネットワーク デバイスを設定する必要があります。</p> <p>このレポートは、特定のユーザ別にポリシー違反（パケット ドロップに基づく）を表示します。</p> <p>(注) RBACL 廃棄パケットのフローは、Cisco Catalyst 6500 シリーズスイッチでのみ使用できます。</p> | —         |
| TrustSec ACI           | <p>このレポートには、IEPG、EEPG、エンドポイント、APIC のサブネット設定と同期された SGT および SXP のマッピングが一覧表示されます。これらの詳細は、TrustSec APIC 統合機能が有効になっている場合にのみ表示されます。</p>                                                                                                                                                                 | —         |

| レポート名                | 説明                                                                                                                                                      | ロギング カテゴリ                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| TrustSec ポリシーのダウンロード | このレポートには、ポリシー（SGT/SGACL）のダウンロードのためにネットワーク デバイスによって送信された要求と、ISEによって送信された詳細が一覧表示されます。ワークフロー モードを有効にしている場合、要求を実稼働マトリックスまたはステージングマトリックスに対してフィルタ処理することができます。 | このレポートを表示するには、次の手順を実行する必要があります。<br><ol style="list-style-type: none"> <li>1. <b>[管理（Administration）] &gt; [システム（System）] &gt; [ロギング（Logging）] &gt; [ロギングカテゴリ（Logging Categories）]</b> を選択します。</li> <li>2. <b>[AAA 診断（AAA Diagnostics）] &gt; [RADIUS 診断（RADIUS Diagnostics）]</b> を選択します。</li> <li>3. RADIUS 診断の <b>[ログ重大度レベル（Log Severity Level）]</b> を <b>DEBUG</b> に設定します。</li> </ol> |
| 脅威中心型 NAC サービス       |                                                                                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                        |
| アダプタのステータス           | アダプタのステータス レポートには、脅威および脆弱性のアダプタのステータスが表示されます。                                                                                                           | —                                                                                                                                                                                                                                                                                                                                                                                      |
| COA イベント             | 脆弱性イベントがエンドポイントに受信されると、Cisco ISE はそのエンドポイントの CoA をトリガーします。CoA イベント レポートには、これらの CoA イベントのステータスが表示されます。また、これらのエンドポイントの新旧の認証ルールとプロファイルの詳細が表示されます。          | —                                                                                                                                                                                                                                                                                                                                                                                      |
| 脅威イベント               | 脅威イベント レポートには、設定したさまざまなアダプタから Cisco ISE が受信した脅威イベントがすべて表示されます。                                                                                          | —                                                                                                                                                                                                                                                                                                                                                                                      |

| レポート名     | 説明                                                                                                          | ロギング カテゴリ |
|-----------|-------------------------------------------------------------------------------------------------------------|-----------|
| 脆弱性アセスメント | 脆弱性アセスメント レポートには、エンドポイントで行われているアセスメントに関する情報が提供されます。このレポートを表示して、設定されたポリシーに基づいてアセスメントが行われているかどうかを確認することができます。 | —         |





## 第 VII 部

### 参照

- [管理のユーザ インターフェイスのリファレンス \(1131 ページ\)](#)
- [ゲスト アクセスのユーザ インターフェイスのリファレンス \(1291 ページ\)](#)
- [Web ポータルのカスタマイズのリファレンス \(1331 ページ\)](#)
- [ポリシーのユーザ インターフェイスのリファレンス \(1349 ページ\)](#)
- [操作のユーザ インターフェイスのリファレンス \(1451 ページ\)](#)
- [ネットワーク アクセス フロー \(1475 ページ\)](#)
- [Cisco ISE の機能をサポートするために必要なスイッチとワイヤレス LAN コントローラの設定 \(1485 ページ\)](#)
- [Cisco ISE でサポートされる管理情報ベース \(1499 ページ\)](#)







## 第 30 章

# 管理のユーザ インターフェイスのリファレンス

- [システム管理](#) (1131 ページ)
- [ID の管理](#) (1205 ページ)
- [ネットワーク リソース](#) (1227 ページ)
- [デバイス ポータルの管理](#) (1261 ページ)

## システム管理

### 展開設定

[展開ノード (Deployment Nodes)] ページを使用すると、Cisco ISE (管理、ポリシー サービス、およびモニタリング) ノードを設定し、展開を設定することができます。

### 展開のノード リスト ページ

次の表に、展開内の Cisco ISE ノードを設定するために使用できる [展開のノードリスト (Deployment Nodes List)] ページのフィールドを示します。このページへのナビゲーションパスは、[管理 (Administration)] > [システム (System)] > [展開 (Deployment)] です。

| フィールド               | 使用上のガイドライン                                                                                                            |
|---------------------|-----------------------------------------------------------------------------------------------------------------------|
| ホストネーム              | ノードのホスト名を表示します。                                                                                                       |
| ノード タイプ (Node Type) | ノード タイプを表示します。次のいずれかを設定できます。 <ul style="list-style-type: none"><li>• Cisco ISE (管理、ポリシー サービス、およびモニタリング) ノード</li></ul> |

| フィールド           | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                           |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ペルソナ (Personas) | (ノードタイプが Cisco ISE の場合にのみ表示) Cisco ISE ノードが担当してきたペルソナがリストされます。[管理 (Administration)]、[ポリシー サービス (Policy Service)] などがあります。                                                                                                                                                                                                            |
| [役割 (Role)]     | <p>このノードで管理ペルソナまたはモニタリングペルソナが有効になっている場合、これらのペルソナが担当しているロール (プライマリ、セカンダリ、またはスタンドアロン) が示されます。ロールは、次のうちの 1 つまたは複数にできます。</p> <ul style="list-style-type: none"><li>• [PRI(A)] : プライマリ PAN を意味します</li><li>• [SEC(A)] : セカンダリ PAN を意味します</li><li>• [PRI(M)] : プライマリ モニタリング ノードを意味します</li><li>• [SEC(M)] : セカンダリ モニタリング ノードを意味します</li></ul> |
| サービス            | <p>(ポリシーサービスペルソナが有効な場合にのみ表示) この Cisco ISE ノードで実行されているサービスがリストされます。サービスは次のいずれか 1 つとなります。</p> <ul style="list-style-type: none"><li>• セッション (Session)</li><li>• プロファイリング</li><li>• すべて (All)</li></ul>                                                                                                                                 |

| フィールド                   | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ノード ステータス (Node Status) | <p>データ レプリケーション用の展開内の各 ISE ノードのステータスを示します。</p> <ul style="list-style-type: none"> <li>• [緑 (接続) (Green (Connected))] : すでに展開に登録されている ISE ノードがプライマリ PAN と同期していることを示します。</li> <li>• [赤 (切断)] : ISE ノードに到達できないか、ISE ノードがダウンしているか、またはデータ レプリケーションが行われていないことを示します。</li> <li>• [オレンジ (進行中) (Orange (In Progress))] : ISE ノードがプライマリ PAN に新規に登録されているか、手動同期操作を実行したか、または ISE ノードがプライマリ PAN と同期していないことを示します。</li> </ul> <p>詳細については、[ノード ステータス (Node Status)] カラムで各 ISE ノードのクイック ビュー アイコンをクリックします。</p> |

#### 関連トピック

[Cisco ISE 分散展開 \(56 ページ\)](#)

[Cisco ISE 展開の用語 \(55 ページ\)](#)

[Cisco ISE ノードの設定 \(60 ページ\)](#)

[セカンダリ Cisco ISE ノードの登録 \(61 ページ\)](#)

## ノードの一般設定

次の表では、[ノードの一般設定 (General Node Settings)] ページのフィールドについて説明します。これらのフィールドを使用して、展開を設定し、各ノード上で実行するサービスを設定できます。このタブのナビゲーションパスは、**[管理 (Administration)] > [システム (System)] > [展開 (Deployment)] > [ISE ノード (ISE Node)] > [編集 (Edit)] > [一般設定 (General Settings)]** です。

表 62: ノードの一般設定

| フィールド  | 使用上のガイドライン                                              |
|--------|---------------------------------------------------------|
| ホストネーム | Cisco ISE ノードのホスト名を表示します。                               |
| [FQDN] | Cisco ISE ノードの完全修飾ドメイン名を表示します。たとえば、ise1.cisco.com などです。 |

| フィールド                  | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [IPアドレス (IP Address) ] | Cisco ISE ノードの IP アドレスを表示します。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| ノード タイプ (Node Type)    | ノード タイプを表示します。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| ペルソナ (Personas)        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 管理 (Administration)    | <p>Cisco ISE ノードに管理ペルソナを担当させる場合は、このチェックボックスをオンにします。管理ペルソナは、管理サービスを提供するようライセンスされているノードでのみ有効にできます。</p> <p>ロール (Role) : 管理ペルソナが展開で担当しているロールを表示します。[スタンドアロン (Standalone) ]、[プライマリ (Primary) ]、[セカンダリ (Secondary) ] のいずれかの値になります。</p> <p>プライマリにする (Make Primary) : ノードをプライマリ Cisco ISE ノードにする場合にこのボタンをクリックします。展開では 1 つのプライマリ Cisco ISE ノードのみを使用できます。このページのその他のオプションは、ノードをプライマリにした後にのみアクティブになります。展開では 2 つの管理ノードのみを使用できます。ノードにスタンドアロン ロールが割り当てられている場合、[プライマリにする (Make Primary) ] ボタンがノードの横に表示されます。ノードにセカンダリ ロールが割り当てられている場合、[プライマリに昇格 (Promote to Primary) ] ボタンがノードの横に表示されます。ノードにプライマリ ロールがあり、そのノードを使用して登録されている他のノードがない場合は、ノードの横に[スタンドアロンにする (Make Standalone) ] ボタンが表示されます。このボタンをクリックすると、プライマリ ノードをスタンドアロン ノードにすることができます。</p> |

| フィールド               | 使用上のガイドライン |
|---------------------|------------|
| モニタリング (Monitoring) |            |

| フィールド | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       | <p>Cisco ISE ノードにモニタリング ペルソナを担当させ、ログ コレクタとして機能させる場合は、このチェックボックスをオンにします。分散展開内にモニタリング ノードが少なくとも 1 つ存在する必要があります。プライマリ PAN の設定時に、モニタリング ペルソナを有効にする必要があります。展開内のセカンダリ モニタリング ノードを登録した後、必要に応じてプライマリ PAN を編集したり、モニタリング ペルソナを無効にしたりできます。</p> <p>VMware プラットフォームで Cisco ISE ノードをログ コレクタとして設定するには、次のガイドラインに従って最低限必要なディスク領域を決定します。1 日あたりネットワーク内のエンドポイント 1 つにつき 180 KB、1 日あたりネットワーク内の Cisco ISE ノード 1 つにつき 2.5 MB となります。</p> <p>モニタリング ノードに何ヵ月分のデータを格納するかに応じて、必要な最大ディスク領域を計算します。展開にモニタリング ノードが 1 つしかない場合は、スタンドアロン ロールを担当します。展開に 2 つのモニタリング ノードがある場合は、Cisco ISE に、プライマリ-セカンダリ ロールを設定する他のモニタリング ノードの名前が表示されます。これらのロールを設定するには、次のいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• プライマリ (Primary) : 現在のノードをプライマリ モニタリング ノードにする場合。</li> <li>• セカンダリ (Secondary) : 現在のノードをセカンダリ モニタリング ノードにする場合。</li> <li>• なし (None) : モニタリング ノードにプライマリ/セカンダリ ロールを担当させない場合。</li> </ul> <p>モニタリング ノードの 1 つをプライマリまたはセカンダリとして設定すると、もう一方のモニタリング ノードが自動的にそれぞれセカンダリ ノードまたはプライマリ ノードになります。プライマリ モニタリング ノードおよび</p> |

| フィールド | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                              |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       | <p>セカンダリ モニタリング ノードは、管理ログおよびポリシー サービス ログを受信します。1 つのモニタリング ノードのロールを [なし (None) ] に変更した場合、他方のモニタリング ノードのロールも同様に [なし (None) ] になり、それによって高可用性ペアがキャンセルされます。モニタリング ノードとしてノードを指定すると、そのノードが [管理 (Administration) ] &gt; [システム (System) ] &gt; [ロギング (Logging) ] &gt; [リモートロギング ターゲット (Remote Logging Targets) ] ページで syslog ターゲットとして表示されます。</p> |

| フィールド                      | 使用上のガイドライン |
|----------------------------|------------|
| ポリシー サービス (Policy Service) |            |



| フィールド | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       | <p>次のサービスの 1 つまたはすべてを有効にするには、このチェックボックスをオンにします。</p> <ul style="list-style-type: none"> <li>• セッションサービスの有効化 (Enable Session Services) : ネットワーク アクセス サービス、ポスチャ サービス、ゲスト サービス、およびクライアント プロビジョニング サービスを有効にするには、このチェックボックスをオンにします。このポリシー サービス ノードが属するグループを、[ノードをノードグループに含める (Include Node in Node Group)] ドロップダウン リストから選択します。</li> </ul> <p>そのポリシー サービス ノードをグループに含めない場合は、[&lt;なし&gt; (&lt;none&gt;)] を選択します。</p> <p>同じノード グループ内のすべてのノードが、ネットワーク アクセス デバイス (NAD) で RADIUS クライアントとして設定され、CoA の許可を得る必要があります。これは、それらすべてのノードで、ノード グループ内の任意のノードを介して確立されたセッションに関する CoA 要求を発行できるためです。ロード バランサを使用していない場合、ノード グループ内のノードは、NAD で設定されている RADIUS サーバおよびクライアントと同じであるか、またはこれらのサブセットである必要があります。これらのノードは RADIUS サーバとしても設定できます。</p> <p>多数の ISE ノード (RADIUS サーバおよび動的許可クライアントとして) を持つ単一の NAD を設定できますが、すべてのノードが同じノード グループに属している必要はありません。</p> <p>ノード グループのメンバーは、ギガビット イーサネットなどの高速 LAN 接続を使用して相互に接続する必要があります。ノード グループのメンバーは L2 隣接関係である必要はありませんが、十分な帯</p> |

| フィールド | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       | <p>域幅と到達可能性を確保するにはL2隣接関係が強く推奨されます。詳細については、<a href="#">ポリシーサービスノードグループの作成（83ページ）</a>を参照してください。</p> <ul style="list-style-type: none"> <li>• プロファイリングサービスの有効化<br/>       (Enable Profiling Service) : プロファイラ サービスを有効にするには、このチェックボックスをオンにします。プロファイリング サービスを有効にする場合は、[Profiling Configuration (プロファイリング設定)] タブをクリックし、必要に応じて詳細を入力する必要があります。ポリシーサービスノードで実行されるサービスを有効または無効にしたり、このノードを変更したりする場合は、そのサービスが実行されるアプリケーション サーバプロセスを再起動します。これらのサービスが再起動されるまで遅延が発生します。ノードでアプリケーション サーバがいつ再起動したかを確認するには、CLI で <code>show application status ise</code> コマンドを使用します。</li> <li>• 脅威中心型 NAC サービスの有効化<br/>       (Enable Threat Centric NAC Service) : 脅威中心型ネットワーク アクセス コントロール (TC-NAC) 機能を有効にするには、このチェック ボックスにマークを付けます。この機能では、脅威と脆弱性のアダプタから受信した脅威と脆弱性の属性に基づいて認証ポリシーを作成することができます。脅威の重大度レベルと脆弱性評価の結果は、エンドポイントまたはユーザのアクセス レベルを動的に制御するために使用できます。</li> </ul> |

| フィールド | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       | <ul style="list-style-type: none"><li>• <b>SXPサービスの有効化 (Enable SXP Service)</b> : ノードで <b>SXP</b> サービスをイネーブルにするには、このチェックボックスをオンにします。また、<b>SXP</b> サービスに使用するインターフェイスを指定する必要があります。</li></ul> <p>NIC ボンディングまたはチーミングを設定している場合は、ボンディングされたインターフェイスも物理インターフェイスとともに [使用インターフェイス (Use Interface) ] ドロップダウンリストに表示されます。</p> <ul style="list-style-type: none"><li>• <b>デバイス管理サービスの有効化 (Enable Device Admin Service)</b> : TACACS ポリシーセット、ポリシー結果などを作成し、ネットワーク デバイスの設定を制御および監査するには、このチェックボックスをオンにします。</li><li>• <b>パッシブ ID サービスの有効化 (Enable Passive Identity Service)</b> : ID マッピング機能を有効にするには、このチェックボックスにマークを付けます。この機能を使用すると、Cisco ISE ではなくドメインコントローラ (DC) で認証されるユーザをモニタすることができます。Cisco ISE がユーザのネットワーク アクセスをアクティブには認証しないネットワークでは、ID マッピング機能を使用して、Active Directory (AD) ドメインコントローラからユーザ認証情報を収集することができます。</li></ul> |

| フィールド  | 使用上のガイドライン                                                                                                                                                                                                                                                                                           |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| pxGrid | pxGrid ペルソナを有効にするには、このチェックボックスをオンにします。Cisco pxGrid は、Cisco ISE セッションディレクトリから Cisco Adaptive Security Appliance (ASA) などの他のポリシー ネットワーク システムへコンテキスト依存情報を共有するために使用されます。pxGrid フレームワークは、ポリシー データや設定データをノード間で交換するためにも使用できます (たとえば、ISE とサードパーティベンダー間でのタグやポリシー オブジェクトの共有)。また、脅威情報など、非 ISE 関連情報の交換用にも使用できます。 |

#### 関連トピック

- [分散 Cisco ISE 展開のペルソナ \(56 ページ\)](#)
- [管理ノード \(63 ページ\)](#)
- [ポリシー サービス ノード \(72 ページ\)](#)
- [モニタリング ノード \(73 ページ\)](#)
- [pxGrid ノード \(76 ページ\)](#)
- [プライマリおよびセカンダリの Cisco ISE ノードの同期 \(81 ページ\)](#)
- [ポリシー サービス ノード グループの作成 \(83 ページ\)](#)
- [ISE pxGrid ノードの展開 \(84 ページ\)](#)
- [ノード ペルソナとサービスの変更 \(82 ページ\)](#)
- [自動フェールオーバー用のモニタリング ノードの設定 \(85 ページ\)](#)

## プロファイリングノードの設定

次の表では、プロファイラ サービスのプロープの設定に使用できる [プロファイリング設定 (Profiling Configuration)] ページのフィールドについて説明します。このページへのナビゲーションパスは、[管理 (Administration)] > [システム (System)] > [展開 (Deployment)] > [ISE ノード (ISE Node)] > [編集 (Edit)] > [プロファイリング設定 (Profiling Configuration)] です。

表 63: プロファイリングノードの設定

| フィールド     | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                 |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NetFlow   | <p>ルータから送信された NetFlow パケットを受信および解析するために、ポリシー サービス ペルソナを担当した Cisco ISE ノードごとに NetFlow を有効にする場合は、このチェックボックスをオンにします。次のオプションを選択します。</p> <ul style="list-style-type: none"><li>• [インターフェイス (Interface)] : ISE ノード上のインターフェイスを選択します。</li><li>• [ポート (Port)] : NetFlow エクスポートがルータから受信した NetFlow リスナーポート番号を入力します。デフォルトポートは 9996 です。</li></ul>                       |
| DHCP      | <p>IP ヘルパーから DHCP パケットをリッスンするために、ポリシー サービス ペルソナを担当した Cisco ISE ノードごとに DHCP を有効にする場合は、このチェックボックスをオンにします。次のオプションを選択します。[ポート (Port)] : DHCP サーバの UDP ポート番号を入力します。デフォルトポートは 67 です。</p> <ul style="list-style-type: none"><li>• [インターフェイス (Interface)] : ISE ノード上のインターフェイスを選択します。</li><li>• [ポート (Port)] : DHCP サーバの UDP ポート番号を入力します。デフォルトポートは 67 です。</li></ul> |
| DHCP SPAN | <p>DHCP パケットを収集するために、ポリシー サービス ペルソナを担当した Cisco ISE ノードごとに DHCP SPAN を有効にする場合は、このチェックボックスをオンにします。</p> <ul style="list-style-type: none"><li>• [インターフェイス (Interface)] : ISE ノード上のインターフェイスを選択します。</li></ul>                                                                                                                                                   |
| HTTP      | <p>HTTP パケットを受信および解析するために、ポリシー サービス ペルソナを担当した Cisco ISE ノードごとに HTTP を有効にする場合は、このチェックボックスをオンにします。</p> <ul style="list-style-type: none"><li>• [インターフェイス (Interface)] : ISE ノード上のインターフェイスを選択します。</li></ul>                                                                                                                                                   |

| フィールド                                    | 使用上のガイドライン                                                                                                                                                                                                                                                                           |
|------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RADIUS                                   | IOS センサー対応デバイスから RADIUS セッション属性、さらに CDP 属性と LLDP 属性を収集するために、ポリシー サービス ペルソナを担当した ISE ノードごとに RADIUS を有効にする場合は、このチェックボックスをオンにします。                                                                                                                                                       |
| ネットワーク スキャン (NMAP) (Network Scan (NMAP)) | NMAP プローブをイネーブルにするには、このボックスをオンにします。                                                                                                                                                                                                                                                  |
| DNS                                      | <p>FQDN の DNS ルックアップを実行するために、ポリシー サービス ペルソナを担当した ISE ノードごとに DNS を有効にする場合は、このチェックボックスをオンにします。秒単位でタイムアウト時間を入力します。</p> <p>(注) DNS プローブを分散展開内の特定の Cisco ISE ノードで動作させるには、DHCP、DHCP SPAN、HTTP、RADIUS、SNMP のいずれかのプローブを有効にする必要があります。DNS ルックアップの場合、上記のいずれかのプローブを DNS プローブとともに起動する必要があります。</p> |

| フィールド                 | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SNMP クエリ (SNMP Query) | <p>指定した間隔でネットワーク デバイスをポーリングするために、ポリシー サービス ペルソナを担当した ISE ノードごとに SNMP クエリを有効にする場合は、このチェックボックスをオンにします。[再試行 (Retries) ]、[タイムアウト (Timeout) ]、[イベント タイムアウト (Event Timeout) ]、任意の [説明 (Description) ] の各フィールドに値を入力します。</p> <p>(注) SNMP クエリープローブの設定に加えて、[管理 (Administration) ] &gt; [ネットワーク リソース (Network Resources) ] &gt; [ネットワーク デバイス (Network Devices) ] の場所にある他の SNMP 設定も行う必要があります。ネットワーク デバイスで SNMP 設定を行う場合は、ネットワーク デバイスでシスコ デバイス プロトコル (CDP) および Link Layer Discovery Protocol (LLDP) をグローバルに有効にしていることを確認します。</p> |

| フィールド                 | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SNMP トラップ (SNMP Trap) | <p>ネットワーク デバイスから linkUp、linkDown、MAC 通知トラップを受信するために、ポリシー サービス ペルソナを担当した ISE ノードごとに SNMP トラッププロブを有効にする場合は、このチェックボックスをオンにします。次のいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• [リンク トラップ クエリー (Link Trap Query)] : SNMP トラップを介して受信する linkup 通知と linkdown 通知を受信して解釈するには、このチェックボックスをオンにします。</li> <li>• [MAC トラップ クエリー (MAC Trap Query)] : SNMP トラップを介して受信する MAC 通知を受信して解釈するには、このチェックボックスをオンにします。</li> <li>• [インターフェイス (Interface)] : ISE ノードのインターフェイスを選択します。</li> <li>• [ポート (Port)] : 使用するホストの UDP ポートを入力します。デフォルト ポートは 162 です。</li> </ul> |
| Active Directory      | 定義された Active Directory サーバをスキャンして、Windows ユーザに関する情報を探します。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| pxGrid                | ISE で pxGrid を介してエンドポイント属性を収集 (プロファイリング) できるようになります。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

#### 関連トピック

[Cisco ISE プロファイリング サービス \(770 ページ\)](#)

[プロファイリング サービスによって使用されるネットワーク プロブ \(773 ページ\)](#)

[Cisco ISE ノードでのプロファイリング サービスの設定 \(772 ページ\)](#)

## 証明書ストアの設定

[証明書ストア (Certificate Store)] ページでは、認証に使用できる証明書を Cisco ISE で設定することができます。



## 自己署名証明書の設定

次の表では、[自己署名証明書の生成（Generate Self Signed Certificate）] ページのフィールドについて説明します。このページでは、ノード間通信、EAP-TLS 認証、Cisco ISE Web ポータル、および pxGrid コントローラとの通信用のシステム証明書を作成できます。このページのナビゲーションパスは、[管理（Administration）]>[システム（System）]>[証明書（Certificates）]>[システム証明書（System Certificates）]>[自己署名証明書の生成（Generate Self Signed Certificate）] です。

| フィールド                                      | 使用上のガイドライン                                                                       |
|--------------------------------------------|----------------------------------------------------------------------------------|
| ノードの選択<br>(Select Node)                    | (必須) システム証明書を生成するノード。                                                            |
| 一般名 (Common Name) (CN)                     | (SAN を指定しない場合に必須) デフォルトでは、一般名は自己署名証明書を生成する ISE ノードの完全修飾ドメイン名です。                  |
| 組織                                         | 組織ユニット名。Engineering など。                                                          |
| 組織<br>(Organization)<br>(O)                | 組織名。Cisco など。                                                                    |
| 都市 (City) (L)                              | (省略不可) 都市名。San Jose など。                                                          |
| 州 (State) (ST)                             | (省略不可) 州名。California など。                                                         |
| 国 (Country) (C)                            | 国名。2 文字の ISO 国番号を入力する必要があります。US など。                                              |
| サブジェクト代替名 (Subject Alternative Name) (SAN) | 証明書に関連付けられた IP アドレス、DNS 名、または Uniform Resource Identifier (URI)。                 |
| Key Length                                 | パブリック CA 署名付き証明書を取得する場合、または FIPS 準拠ポリシー管理システムとして Cisco ISE を展開する場合は、2048 を選択します。 |
| 署名するダイジェスト (Digest to Sign With)           | ハッシュ アルゴリズム SHA-1 または SHA-256 を選択します。                                            |
| 証明書ポリシー (Certificate Policies)             | 証明書が従うべき証明書ポリシーの OID または OID のリストを入力します。OID を区切るには、カンマまたはスペースを使用します。             |
| TTL 有効期限 (Expiration TTL)                  | 証明書が失効するまでの日数を指定します。                                                             |

| フィールド                                       | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| フレンドリ名<br>(Friendly Name)                   | 証明書のフレンドリ名を入力します。名前を指定しない場合は、<common name> # <issuer> # <nnnnn> の形式で自動的に名前が作成されます。ここで、<nnnnn> は固有の 5 桁の数値です。                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| ワイルドカード証明書の許可 (Allow Wildcard Certificates) | 自己署名したワイルドカード証明書 (サブジェクトの任意の一般名またはサブジェクト代替名の DNS 名、またはその両方にアスタリスク (*) が含まれている証明書) を生成する場合は、このチェックボックスをオンにします。たとえば、SAN に割り当てられている DNS 名が *.amer.cisco.com の場合です。                                                                                                                                                                                                                                                                                                                                                                                                             |
| 使用方法                                        | <p>このシステム証明書を使用する必要があるサービスを選択します。</p> <ul style="list-style-type: none"> <li>• [管理者 (Admin)] : 管理者ポータルとの通信および展開内の ISE ノード間の通信の保護に使用されるサーバ証明書</li> <li>• [EAP 認証 (EAP Authentication)] : SSL/TLS トンネリングの EAP プロトコルを使用する認証に使用されるサーバ証明書</li> <li>• [RADIUS DTLS] : RADIUS DTLS 認証に使用するサーバ証明書</li> <li>• [pxGrid] : pxGrid クライアントとサーバの間の通信を保護するクライアントおよびサーバ証明書</li> <li>• [SAML] : SAML ID プロバイダ (IdP) とのセキュア通信に使用するサーバ証明書。SAML 用の使用を目的とした証明書は、管理者認証や EAP 認証などのその他のサービスのために使用することはできません。</li> <li>• [ポータル (Portal)] : すべての Cisco ISE Web ポータルとの通信を保護するために使用されるサーバ証明書</li> </ul> |

#### 関連トピック

[システム証明書 \(169 ページ\)](#)

[システム証明書の表示 \(170 ページ\)](#)

[自己署名証明書の生成 \(172 ページ\)](#)

## 証明書署名要求の設定

Cisco ISE では、1 つの要求で、管理者ポータルから展開内のすべてのノードの CSR を生成することができます。また、展開内の単一ノードまたは複数両方のノードのどちらの CSR を生成するのか選択することもできます。単一ノードの CSR を生成する場合、ISE は証明書サブジェクトの [CN=] フィールドの特定ノードの完全修飾ドメイン名 (FQDN) を自動的に置き換えます。証明書の [サブジェクト代替名 (Subject Alternative Name (SAN))] フィールドにエントリを含めることを選択した場合、他の SAN 属性に加えて ISE ノードの FQDN を入力する必要があります。展開内のすべてのノードの CSR を生成することを選択した場合は、[ワイルドカード証明書の許可 (Allow Wildcard Certificates)] チェックボックスをオンにして、[SAN]

フィールド（DNS 名）にワイルドカード表記で FQDN を入力します（\*.amer.example.com など）。EAP 認証に証明書を使用する場合は、[CN=] フィールドにワイルドカード値を入力しないでください。

ワイルドカード証明書を使用することにより、各 Cisco ISE ノードに固有の証明書を生成する必要がなくなります。また、証明書の警告を防ぐために、SAN フィールドに複数の FQDN 値を入力する必要もありません。SAN フィールドでアスタリスク（\*）を使用すると、展開内の複数の両方のノードで単一の証明書を共有できるようになり、証明書名の不一致による警告を防止することができます。ただし、ワイルドカード証明書は、各 Cisco ISE ノードに固有のサーバ証明書を割り当てる場合よりも安全性が低いと見なされます。

次の表に、認証局（CA）が署名可能な証明書署名要求（CSR）の生成に使用できる [証明書署名要求（Certificate Signing Request）] ページのフィールドを示します。このページのナビゲーションパスは [管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [証明書管理（Certificate Management）] > [証明書署名要求（Certificate Signing Request）] です。

| フィールド                                          | 使用上のガイドライン |
|------------------------------------------------|------------|
| 証明書の用途<br>(Certificate(s) will<br>be used for) |            |

| フィールド | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       | <p>証明書を使用するサービスを選択します。</p> <p><b>Cisco ISE ID 証明書</b></p> <ul style="list-style-type: none"> <li>• 複数使用：複数のサービス（管理者、EAP-TLS 認証、pxGrid、およびポータル）に使用されます。複数使用の証明書は、クライアントとサーバ両方のキーの用途を使用します。署名 CA の証明書テンプレートは、コンピュータまたはマシン証明書テンプレートと呼ばれます。このテンプレートには、次のプロパティがあります。 <ul style="list-style-type: none"> <li>• キーの用途：デジタル署名（署名）</li> <li>• キーの拡張用途：TLS Web サーバ認証（1.3.6.1.5.5.7.3.1）および TLS Web クライアント認証（1.3.6.1.5.5.7.3.2）</li> </ul> </li> <li>• 管理者：サーバ認証に使用されます（管理者ポータルとの通信および展開内の ISE ノード間の通信を保護するため）。署名 CA の証明書テンプレートは、Web サーバ証明書テンプレートと呼ばれます。このテンプレートには、次のプロパティがあります。 <ul style="list-style-type: none"> <li>• キーの用途：デジタル署名（署名）</li> <li>• キーの拡張用途：TLS Web サーバ認証（1.3.6.1.5.5.7.3.1）</li> </ul> </li> <li>• EAP 認証：サーバ認証に使用されます。署名 CA の証明書テンプレートは、コンピュータまたはマシン証明書テンプレートと呼ばれます。このテンプレートには、次のプロパティがあります。 <ul style="list-style-type: none"> <li>• キーの用途：デジタル署名（署名）</li> <li>• キーの拡張用途：TLS Web サーバ認証（1.3.6.1.5.5.7.3.1）</li> </ul> </li> <li>• DTLS RADIUS：RADIUS DTLS サーバの認証に使用されます。このテンプレートには、次のプロパティがあります。 <ul style="list-style-type: none"> <li>• キーの用途：デジタル署名（署名）</li> <li>• キーの拡張用途：TLS Web サーバ認証（1.3.6.1.5.5.7.3.1）</li> </ul> </li> <li>• ポータル：サーバ認証に使用されます（すべての ISE Web ポータルとの通信を保護するため）。署名 CA の証明書テンプレートは、コンピュータまたはマシン証明書テンプレートと呼ばれます。このテンプレートには、次のプロパティがあります。 <ul style="list-style-type: none"> <li>• キーの用途：デジタル署名（署名）</li> <li>• キーの拡張用途：TLS Web サーバ認証（1.3.6.1.5.5.7.3.1）</li> </ul> </li> <li>• pxGrid：クライアント認証とサーバ認証の両方に使用されます（pxGrid クライアントとサーバ間の通信を保護するため）。署名 CA の証明</li> </ul> |

| フィールド | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       | <p>書テンプレートは、コンピュータまたはマシン証明書テンプレートと呼ばれます。このテンプレートには、次のプロパティがあります。</p> <ul style="list-style-type: none"> <li>• キーの用途：デジタル署名（署名）</li> <li>• キーの拡張用途：TLS Web サーバ認証（1.3.6.1.5.5.7.3.1）および TLS Web クライアント認証（1.3.6.1.5.5.7.3.2）</li> </ul> <p>• SAML：SAML ID プロバイダー（IdP）とのセキュア通信に使用するサーバ証明書。SAML 用の使用を目的とした証明書は、管理者認証や EAP 認証などのその他のサービスのために使用することはできません。</p> <ul style="list-style-type: none"> <li>• キーの用途：デジタル署名（署名）</li> <li>• キーの拡張用途：TLS Web サーバ認証（1.3.6.1.5.5.7.3.1）</li> </ul> <p>（注） 拡張キーの使用状況属性に任意の目的のオブジェクト識別子のための 2.5.29.37.0 の値が含まれている証明書を使用しないことをお勧めします。拡張キーの使用状況属性に任意の目的のオブジェクト識別子のための 2.5.29.37.0 の値が含まれている証明書を使用する場合、証明書は無効と見なされ、次のエラーメッセージが表示されます。</p> <pre>source=local ; type=fatal ; message="unsupported certificate"</pre> <p><b>Cisco ISE 認証局証明書</b></p> <ul style="list-style-type: none"> <li>• ISE ルート CA（内部 CA サービスにのみ適用可能）：プライマリ PAN のルート CA および PSN の下位 CA を含む内部 CA 証明書チェーン全体を再生成するために使用されます。</li> <li>• ISE 中間 CA（内部 CA サービス、および ISE が外部 PKI の中間 CA として機能する場合にのみ適用可能）：プライマリ PAN の中間 CA 証明書および PSN の下位 CA 証明書の生成に使用されます。署名 CA の証明書テンプレートは、下位認証局と呼ばれます。このテンプレートには、次のプロパティがあります。 <ul style="list-style-type: none"> <li>• 基本制約：重要、認証局</li> <li>• キーの用途：証明書の署名、デジタル署名</li> <li>• キーの拡張用途：OCSP 署名（1.3.6.1.5.5.7.3.9）</li> </ul> </li> <li>• ISE OCSP 応答側証明書の更新（内部 CA サービスにのみ適用可能）：展開全体の ISE OCSP 応答側証明書の更新に使用されます（証明書署名要求ではありません）。セキュリティ上の理由から、ISE OCSP 応答側証明書を 6 ヶ月ごとに更新することを推奨します。</li> </ul> |

| フィールド                                            | 使用上のガイドライン                                                                                                                                                                                                                                                                                                     |
|--------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ワイルドカード証明書の許可 (Allow Wildcard Certificates)      | 証明書の [SAN] フィールドの CN/DNS 名にワイルドカード文字 (*) を使用するには、このチェックボックスをオンにします。このチェックボックスをオンにすると、展開内のすべてのノードが自動的に選択されます。左端のラベルの位置にアスタリスク (*) ワイルドカード文字を使用する必要があります。ワイルドカード証明書を使用する場合は、セキュリティを強化するためにドメイン領域を分割することを推奨します。たとえば、*.example.com の代わりに *.amer.example.com を使用して領域を分割することができます。ドメインを分割しないと、セキュリティ問題が発生する可能性があります。 |
| これらのノードの CSR の生成 (Generate CSRs for these Nodes) | 証明書を生成するノードの隣のチェックボックスをオンにします。展開内の選択されたノードの CSR を生成するには、[ワイルドカード証明書の許可 (Allow Wildcard Certificates)] オプションをオフにします。                                                                                                                                                                                            |
| 一般名 (Common Name) (CN)                           | デフォルトでは、一般名は CSR を生成する ISE ノードの FQDN です。\$FQDN\$ は ISE ノードの FQDN を意味します。展開内の複数ノードの CSR を生成すると、CSR の [一般名 (Common Name)] フィールドは各 ISE ノードの FQDN に置き換えられます。                                                                                                                                                       |
| 組織                                               | 組織ユニット名。Engineering など。                                                                                                                                                                                                                                                                                        |
| 組織 (Organization) (O)                            | 組織名。Cisco など。                                                                                                                                                                                                                                                                                                  |
| 都市 (City) (L)                                    | (省略不可) 都市名。San Jose など。                                                                                                                                                                                                                                                                                        |
| 州 (State) (ST)                                   | (省略不可) 州名。California など。                                                                                                                                                                                                                                                                                       |
| 国 (Country) (C)                                  | 国名。2 文字の ISO 国番号を入力する必要があります。US など。                                                                                                                                                                                                                                                                            |

| フィールド                                      | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| サブジェクト代替名 (Subject Alternative Name) (SAN) | <p>証明書に関連付けられている IP アドレス、DNS 名、Uniform Resource Identifier (URI)、またはディレクトリ名。</p> <ul style="list-style-type: none"> <li>• DNS 名 : DNS 名を選択した場合は、ISE ノードの完全修飾ドメイン名を入力します。[ワイルドカード証明書の許可 (Allow Wildcard Certificates)] オプションをオンにした場合は、ワイルドカード表記 (ドメイン名の前にアスタリスクとピリオドを入力) を指定します。<br/>*.amer.example.com など。</li> <li>• IP アドレス : 証明書に関連付けられる ISE ノードの IP アドレス。</li> <li>• Uniform Resource Identifier : 証明書に関連付ける URI。</li> <li>• ディレクトリ名 : RFC 2253 に従って定義される識別名 (DN) の文字列表現。DN 間はカンマ (,) で区切ります。「dnQualifier」RDN の場合は、カンマをエスケープし、区切り文字としてバックスラッシュ カンマ 「\,」を使用します。たとえば、<br/>CN=AAA,dnQualifier=O=Example\,DC=COM,C=IL などです。</li> </ul> |
| キーの長さ (Key Length)                         | パブリック CA の署名付き証明書を取得するか、FIPS 準拠ポリシー管理システムとして Cisco ISE を展開する場合は 2048 以上を選択します。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| 署名するダイジェスト (Digest to Sign With)           | ハッシュ アルゴリズム SHA-1 または SHA-256 を選択します。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 証明書ポリシー (Certificate Policies)             | 証明書が従うべき証明書ポリシーの OID または OID のリストを入力します。OID を区切るには、カンマまたはスペースを使用します。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

#### 関連トピック

[証明書署名要求 \(181 ページ\)](#)

[証明書署名要求の作成と認証局への CSR の送信 \(181 ページ\)](#)

[CSR への CA 署名付き証明書のバインド \(182 ページ\)](#)

## 発行および失効した証明書

次の表で、[発行および失効した証明書の概要 (Overview of Issued and Revoked Certificates)] ページのフィールドについて説明します。展開内の PSN ノードがエンドポイントに証明書を発行します。このページでは、展開内の各 PSN ノードが発行するエンドポイント証明書に関する情報を示します。このページへのナビゲーションパスは、[管理 (Administration)] > [システム (System)] > [証明書 (Certificates)] > [概要 (Overview)] です。

| フィールド | 使用上のガイドライン                       |
|-------|----------------------------------|
| ノード名  | 証明書を発行したポリシー サービス ノード (PSN) の名前。 |



| フィールド                               | 使用上のガイドライン                           |
|-------------------------------------|--------------------------------------|
| [発行された証明書 (Certificates Issued) ]   | PSN ノードが発行したエンドポイント証明書の数。            |
| [取り消された証明書 (Certificates Revoked) ] | 失効したエンドポイント証明書 (PSN ノードが発行した証明書) の数。 |
| [証明書要求 (Certificates Requests) ]    | PSN ノードが処理した証明書ベースの認証要求の数。           |
| [失敗した証明書 (Certificates Failed) ]    | PSN ノードが処理する失敗した認証要求の数。              |

#### 関連トピック

[発行された証明書](#) (200 ページ)

[ユーザおよびエンドポイントの証明書の更新](#) (187 ページ)

[証明書を使用してパーソナル デバイスを許可するための Cisco ISE の設定](#) (204 ページ)

[ユーザによる証明書の更新を許可する Cisco ISE の設定](#) (188 ページ)

[エンドポイント証明書の失効](#) (223 ページ)

## 証明書定期チェックの設定

Cisco ISE は、証明書失効リスト (CRL) を定期的にチェックします。このページを使用して、自動的にダウンロードされた CRL に対して進行中のセッションをチェックするように Cisco ISE を設定できます。OCSP または CRL のチェックを毎日開始する時刻と、OCSP サーバまたは CRL を再度チェックする前に Cisco ISE が待機する時間間隔を時間単位で指定できます。

次の表では、[証明書定期チェックの設定 (Certificate Periodic Check Settings) ] ページのフィールドについて説明します。このページを使用して、証明書 (OCSP または CRL) のステータスをチェックする時間間隔を指定できます。このページへのナビゲーションパスは、[管理 (Administration) ] > [システム (System) ] > [証明書 (Certificates) ] > [証明書管理 (Certificate Management) ] > [証明書定期チェックの設定 (Certificate Periodic Check Settings) ] です。

| フィールド      | 使用上のガイドライン |
|------------|------------|
| 証明書チェックの設定 |            |

| フィールド                                                                                       | 使用上のガイドライン                                                             |
|---------------------------------------------------------------------------------------------|------------------------------------------------------------------------|
| 自動的に取得されたCRLに対する進行中のセッションのチェック (Check ongoing sessions against automatically retrieved CRL) | Cisco ISE が自動的にダウンロードされた CRL に対する進行中のセッションをチェックするには、このチェックボックスをオンにします。 |
| <b>CRL/OCSP の定期的な証明書チェック</b>                                                                |                                                                        |
| 最初のチェック時刻 (First check at)                                                                  | CRL または OCSP のチェックを毎日開始する時刻を指定します。00:00 ～ 23:59 の時間範囲の値を入力します。         |
| チェック間隔 (Check every)                                                                        | CRL または OCSP サーバを再度チェックする前に Cisco ISE が待機する時間間隔を時間単位で指定します。            |

#### 関連トピック

[OCSP サービス](#) (224 ページ)

[OCSP クライアントプロファイルの追加](#) (226 ページ)

## システム証明書のインポート設定

次の表では、サーバ証明書をインポートするために使用できる [システム証明書のインポート (Import System Certificate) ] ページのフィールドについて説明します。このページへのナビゲーションパスは、[管理 (Administration) ]>[システム (System) ]>[証明書 (Certificates) ]>[システム証明書 (System Certificates) ]>[インポート (Import) ] です。

| フィールド                        | 説明                                                                                                           |
|------------------------------|--------------------------------------------------------------------------------------------------------------|
| ノードの選択 (Select Node)         | (必須) システム証明書をインポートする Cisco ISE ノードを選択します。                                                                    |
| 証明書ファイル (Certificate file)   | (必須) [参照 (Browse) ] をクリックして、ローカルシステムから証明書ファイルを選択します。                                                         |
| 秘密キー ファイル (Private key file) | (必須) [参照 (Browse) ] をクリックして、秘密キーファイルを選択します。                                                                  |
| [パスワード (Password) ]          | (必須) 秘密キーファイルを復号化するためのパスワードを入力します。                                                                           |
| フレンドリ名 (Friendly Name)       | 証明書のフレンドリ名を入力します。名前を指定しない場合は、<common name> # <issuer> # <nnnnn> の形式で自動的に名前が作成されます。ここで、<nnnnn> は固有の 5 桁の数値です。 |

| フィールド                                          | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ワイルドカード証明書の許可<br>(Allow Wildcard Certificates) | ワイルドカード証明書 (サブジェクトの任意の一般名またはサブジェクト代替名の DNS 名、またはその両方にアスタリスク (*) が含まれている証明書) をインポートする場合は、このチェックボックスをオンにします。たとえば、SAN に割り当てられている DNS 名が *.amer.cisco.com の場合です。このチェックボックスをオンにすると、Cisco ISE は展開内の他のすべてのノードにこの証明書をインポートします。                                                                                                                                                                                                                                                                                                                                                         |
| 証明書の拡張の検証 (Validate Certificate Extensions)    | Cisco ISE に証明書の拡張の検証を許可する場合は、このチェックボックスをオンにします。このチェックボックスをオンにし、かつインポートする証明書に CA フラグが true に設定された基本制約拡張が含まれている場合は、キー使用拡張が存在すること、および keyEncipherment ビットと keyAgreement ビットのいずれかまたは両方が設定されていることを確認します。                                                                                                                                                                                                                                                                                                                                                                            |
| 使用方法                                           | <p>このシステム証明書を使用する必要があるサービスを選択します。</p> <ul style="list-style-type: none"> <li>• [管理者 (Admin) ] : 管理者ポータルとの通信および展開内の ISE ノード間の通信の保護に使用されるサーバ証明書</li> <li>• [EAP 認証 (EAP Authentication) ] : SSL/TLS トンネリングの EAP プロトコルを使用する認証に使用されるサーバ証明書</li> <li>• [RADIUS DTLS] : RADIUS DTLS 認証に使用するサーバ証明書</li> <li>• [pxGrid] : pxGrid クライアントとサーバの間の通信を保護するクライアントおよびサーバ証明書</li> <li>• [SAML] : SAML ID プロバイダ (IdP) とのセキュア通信に使用するサーバ証明書。SAML 用の使用を目的とした証明書は、管理者認証や EAP 認証などのその他のサービスのために使用することはできません。</li> <li>• [ポータル (Portal) ] : すべての Cisco ISE Web ポータルとの通信を保護するために使用されるサーバ証明書</li> </ul> |

#### 関連トピック

[システム証明書 \(169 ページ\)](#)

[システム証明書の表示 \(170 ページ\)](#)

[システム証明書のインポート \(171 ページ\)](#)

## [信頼できる証明書ストア (Trusted Certificate Store) ] ページ

次の表では、管理ノードに追加された証明書を表示するために使用できる [信頼できる証明書ストア (Trusted Certificates Store) ] ページのフィールドについて説明します。このページへのナビゲーションパスは、[管理 (Administration) ] > [システム (System) ] > [証明書 (Certificates) ] > [信頼できる証明書 (Trusted Certificates) ] です。

表 64:信頼できる証明書ページ

| フィールド                         | 使用上のガイドライン                                                                                                                                                                                                                                  |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| フレンドリ名 (Friendly Name)        | 証明書の名前を表示します。                                                                                                                                                                                                                               |
| ステータス (Status)                | 有効または無効にします。[無効 (Disabled)] の場合、ISEは信頼を確立するために証明書を使用しません。                                                                                                                                                                                   |
| 信頼対象 (Trusted for)            | 証明書を使用するサービスを表示します。                                                                                                                                                                                                                         |
| 発行先 (Issued To)               | 証明書のサブジェクトの一般名 (CN)。                                                                                                                                                                                                                        |
| 発行元 (Issued By)               | 証明書の発行元の一般名 (CN)。                                                                                                                                                                                                                           |
| 有効期限の開始 (Valid From)          | 「Not Before」証明書属性。                                                                                                                                                                                                                          |
| 期限日 (Expiration Date)         | 「Not After」証明書属性。                                                                                                                                                                                                                           |
| 有効期限ステータス (Expiration Status) | <p>証明書の有効期限のステータスに関する情報です。このコラムに表示される情報メッセージには5つのアイコンとカテゴリがあります。</p> <ul style="list-style-type: none"> <li>・ 緑：期限切れまで 90 日を超える</li> <li>・ 青色：90 日以内に期限切れ</li> <li>・ 黄：60 日以内に期限切れ</li> <li>・ オレンジ：30 日以内に期限切れ</li> <li>・ 赤：期限切れ</li> </ul> |

## 関連トピック

[信頼できる証明書ストア](#) (175 ページ)

[信頼できるストア証明書の表示](#) (177 ページ)

[信頼できる証明書ストアの証明書のステータス変更](#) (178 ページ)

[信頼できる証明書ストアへの証明書の追加](#) (178 ページ)

## 証明書設定の編集

次の表では、認証局 (CA) 証明書属性を編集するために使用できる [証明書ストアの証明書編集 (Certificate Store Edit Certificate)] ページのフィールドについて説明します。このページへのナビゲーションパスは、[管理 (Administration)] > [システム (System)] > [証明書 (Certificates)] > [信頼できる証明書 (Trusted Certificates)] > [証明書 (Certificate)] > [編集 (Edit)] です。

表 65: 証明書ストア編集設定

| フィールド                                                                  | 使用上のガイドライン                                                                                                                                                                                                                                                                                                     |
|------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 証明書発行元 (Certificate Issuer)                                            |                                                                                                                                                                                                                                                                                                                |
| フレンドリ名 (Friendly Name)                                                 | 証明書のフレンドリ名を入力します。                                                                                                                                                                                                                                                                                              |
| ステータス (Status)                                                         | [有効 (Enabled) ] または [無効 (Disabled) ] を選択します。[無効 (Disabled) ] の場合、ISE は信頼を確立するために証明書を使用しません。                                                                                                                                                                                                                    |
| 説明                                                                     | 任意で説明を入力します。                                                                                                                                                                                                                                                                                                   |
| 使用方法                                                                   |                                                                                                                                                                                                                                                                                                                |
| ISE 内の認証用に信頼する (Trust for authentication within ISE)                   | この証明書で (他の ISE ノードまたは LDAP サーバから) サーバ証明書を検証する場合は、このチェックボックスをオンにします。                                                                                                                                                                                                                                            |
| クライアント認証および syslog 用に信頼する (Trust for client authentication and Syslog) | <p>([ISE 内の認証用に信頼する (Trust for authentication within ISE) ] チェックボックスをオンにした場合に限り適用可能) この証明書を使用して次を行う場合は、このチェックボックスをオンにします。</p> <ul style="list-style-type: none"> <li>• EAP プロトコルを使用した ISE に接続するエンドポイントの認証</li> <li>• syslog サーバの信頼</li> </ul>                                                                  |
| シスコサービスの認証用に信頼する (Trust for authentication of Cisco Services)          | フィードサービスなどの外部シスコサービスを信頼するためにこの証明書を使用する場合は、このチェックボックスをオンにします。                                                                                                                                                                                                                                                   |
| 証明書ステータスの検証 (Certificate Status Validation)                            | <p>ISE は、特定の CA が発行するクライアントまたはサーバ証明書の失効ステータスをチェックする 2 つの方法をサポートしています。</p> <p>1 つは、Online Certificate Status Protocol (OCSP) を使用して証明書を検証することです (OCSP は、CA によって保持される OCSP サービスに要求を行います)。もう 1 つは、ISE に CA からダウンロードした証明書失効リスト (CRL) に対して証明書を検証することです。両方の方法は、OCSP を最初に使用し、ステータスを判断できないときに限り CRL を使用する場合に使用できます。</p> |

| フィールド                                                                            | 使用上のガイドライン                                                                                                                                         |
|----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| OCSP サービスに対して検証する (Validate Against OCSP Service)                                | OCSP サービスに対して証明書を検証するには、このチェックボックスをオンにします。このボックスをオンにするには、まず OCSP サービスを作成する必要があります。                                                                 |
| OCSP が不明なステータスを返した場合は要求を拒否する (Reject the request if OCSP returns UNKNOWN status) | 認証ステータスが OCSP によって判別されなかった場合に要求を拒否するには、このチェックボックスをオンにします。このチェックボックスをオンにした場合、OCSP サービスによって不明のステータス値が返されると、ISE は現在評価されているクライアントまたはサーバ証明書を拒否します。      |
| OCSP 応答側が到達不能な場合は要求を拒否する (Reject the request if OCSP Responder is unreachable)   | OCSP 応答側が到達不能な場合に ISE が要求を拒否するには、このチェックボックスをオンにします。                                                                                                |
| CRL のダウンロード (Download CRL)                                                       | Cisco ISE で CRL をダウンロードするには、このチェックボックスをオンにします。                                                                                                     |
| CRL 配信 URL (CRL Distribution URL)                                                | CA から CRL をダウンロードするための URL を入力します。認証局証明書で指定されている場合、このフィールドは自動的に読み込まれます。URL は「http」、「https」、または「ldap」で始まる必要があります。                                   |
| CRL の取得 (Retrieve CRL)                                                           | CRL は、自動的または定期的にダウンロードできます。ダウンロードの時間間隔を設定します。                                                                                                      |
| ダウンロードが失敗した場合は待機する (If download failed, wait)                                    | Cisco ISE が CRL を再度ダウンロードするまでに待機する時間間隔を設定します。                                                                                                      |
| CRL を受信しない場合 CRL 検証をバイパスする (Bypass CRL Verification if CRL is not Received)      | このチェックボックスをオンにした場合、クライアント要求は CRL が受信される前に受け入れられます。このチェックボックスをオフにした場合、選択した CA によって署名された証明書を使用するすべてのクライアント要求は、Cisco ISE によって CRL ファイルが受信されるまで拒否されます。 |

| フィールド                                                                       | 使用上のガイドライン                                                                                                                                                                                                                                                                                                          |
|-----------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CRL がまだ有効でないか、または期限切れの場合は無視する (Ignore that CRL is not yet valid or expired) | <p>Cisco ISE で開始日と期限日を無視し、まだアクティブでないかまたは期限切れの CRL を引き続き使用し、CRL の内容に基づいて EAP-TLS 認証を許可または拒否する場合は、このチェックボックスをオンにします。</p> <p>Cisco ISE で [有効日 (Effective Date)] フィールドの開始日と [次の更新 (Next Update)] フィールドの期限日を CRL ファイルでチェックする場合は、このチェックボックスをオフにします。CRL がまだアクティブではないか、または期限切れの場合、その CA によって署名された証明書を使用するすべての認証は拒否されます。</p> |

#### 関連トピック

[信頼できる証明書ストア](#) (175 ページ)

[信頼できる証明書の編集](#) (179 ページ)

## 信頼できる証明書のインポート設定

次の表では、認証局 (CA) 証明書を Cisco ISE に追加するために使用できる [信頼できる証明書のインポート (Trusted Certificate Import)] ページのフィールドについて説明します。このページへのナビゲーションパスは [管理 (Administration)] > [システム (System)] > [証明書 (Certificates)] > [信頼できる証明書 (Trusted Certificates)] > [インポート (Import)] です。

表 66: 信頼できる証明書のインポート設定

| フィールド                                                | 説明                                                                                                                     |
|------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|
| 証明書ファイル (Certificate file)                           | [参照 (Browse)] をクリックして、ブラウザを実行しているコンピュータから証明書ファイルを選択します。                                                                |
| フレンドリ名 (Friendly Name)                               | 証明書のフレンドリ名を入力します。名前を指定しない場合は、Cisco ISE により <common name>#<issuer>#<nnnnn> の形式で自動的に名前が作成されます。ここで、<nnnnn> は固有の 5 桁の数値です。 |
| ISE 内の認証用に信頼する (Trust for authentication within ISE) | この証明書を (他の ISE ノードまたは LDAP サーバから) サーバ証明書の検証に使用する場合は、このチェックボックスをオンにします。                                                 |

| フィールド                                                                  | 説明                                                                                                                                                                                                                                           |
|------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| クライアント認証および syslog 用に信頼する (Trust for client authentication and Syslog) | <p>([ISE 内の認証用に信頼する (Trust for authentication within ISE)] チェックボックスをオンにした場合に限り適用可能) この証明書を使用して次を行う場合は、このチェックボックスをオンにします。</p> <ul style="list-style-type: none"> <li>• EAP プロトコルを使用した ISE に接続するエンドポイントの認証</li> <li>• syslog サーバの信頼</li> </ul> |
| シスコサービスの認証用に信頼する (Trust for authentication of Cisco Services)          | フィードサービスなどの外部シスコサービスを信頼するためにこの証明書を使用する場合は、このチェックボックスをオンにします。                                                                                                                                                                                 |
| 証明書の拡張の検証 (Validate Certificate Extensions)                            | <p>([クライアント認証用に信頼する (Trust for client authentication)] オプションと [証明書拡張の検証を有効にする (Enable Validation of Certificate Extensions)] オプションの両方をオンにした場合のみ) 「keyUsage」拡張が存在し、「keyCertSign」ビットが設定されていることと、CA フラグが true に設定された基本制約拡張が存在することを確認します。</p>    |
| 説明                                                                     | 任意で説明を入力します。                                                                                                                                                                                                                                 |

#### 関連トピック

[信頼できる証明書ストア \(175 ページ\)](#)

[証明書チェーンのインポート \(181 ページ\)](#)

[信頼できる証明書ストアへのルート証明書のインポート \(180 ページ\)](#)

## OCSP クライアント プロファイル設定

次の表では、OCSP クライアント プロファイル設定を行うために使用できる [OCSP クライアント プロファイル (OCSP Client Profile)] ページのフィールドについて説明します。このページへのナビゲーションパスは、**[管理 (Administration)] > [証明書 (Certificates)] > [証明書管理 (Certificate Management)] > [OCSP クライアント プロファイル (OCSP Client Profile)]** です。

| フィールド                                         | 使用上のガイドライン           |
|-----------------------------------------------|----------------------|
| [名前 (Name)]                                   | OCSP クライアント プロファイル名。 |
| 説明                                            | 任意で説明を入力します。         |
| <b>OCSP 応答側の設定 (Configure OCSP Responder)</b> |                      |



| フィールド                                                                              | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| セカンダリ サーバの有効化<br>(Enable Secondary Server)                                         | ハイ アベイラビリティのセカンダリ OCSP サーバを有効にするには、このチェックボックスをオンにします。                                                                                                                                                                                                                                                                                                                                        |
| 常にプライマリ サーバに最初にアクセスする (Always Access Primary Server First)                         | このオプションは、セカンダリ サーバへの移動を試行する前にプライマリ サーバをチェックする場合に使用します。プライマリが以前にチェックされ、応答しないことがわかっている場合にも、Cisco ISE はセカンダリ サーバに移動する前にプライマリ サーバへの要求の送信を試行します。                                                                                                                                                                                                                                                  |
| $n$ 分経過後にプライマリ サーバにフォールバック (Fallback to Primary Server After Interval $n$ Minutes) | このオプションは、Cisco ISE がセカンダリ サーバに移動してから、再度プライマリ サーバにフォールバックする場合に使用します。この場合、その他の要求はすべてスキップされ、テキスト ボックスで設定した時間セカンダリ サーバが使用されます。許可される時間の範囲は 1 ～ 999 分です。                                                                                                                                                                                                                                           |
| <b>プライマリ サーバとセカンダリ サーバ (Primary and Secondary Servers)</b>                         |                                                                                                                                                                                                                                                                                                                                                                                              |
| URL                                                                                | プライマリおよびセカンダリ OCSP サーバの URL を入力します。                                                                                                                                                                                                                                                                                                                                                          |
| ナンス拡張サポートの有効化<br>(Enable Nonce Extension Support)                                  | ナンスが OCSP 要求の一部として送信されるように設定できます。ナンスには、OCSP 要求の疑似乱数が含まれます。応答で受信される数値は要求に含まれる数値と同じであることが検証されています。このオプションにより、リプレイ アタックで古い通信を再利用できないことが保証されます。                                                                                                                                                                                                                                                  |
| 応答の署名の検証 (Validate Response Signature)                                             | <p>OCSP レスポンダは、次のいずれかの証明書を使用して応答に署名します。</p> <ul style="list-style-type: none"> <li>• CA 証明書</li> <li>• CA 証明書とは別の証明書</li> </ul> <p>Cisco ISE が応答の署名を検証するためには、OCSP 応答側が応答を証明書とともに送信する必要があります。そうでない場合、応答の検証は失敗し、証明書のステータスは利用できません。RFC に従い、OCSP は異なる証明書を使用して応答に署名できます。このことは、OCSP が Cisco ISE による検証用に応答に署名した証明書を送信する限り当てはまります。OCSP が Cisco ISE で設定されているものとは異なる証明書を使用して応答に署名した場合、応答の検証は失敗します。</p> |

| フィールド                                                                                                                  | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Authority Information Access (AIA) に指定されたOCSP URLを使用する (Use OCSP URLs specified in Authority Information Access (AIA)) | Authority Information Access の拡張で指定されている OCSP URL を使用するには、オプション ボタンをクリックします。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>応答キャッシュ (Response Cache)</b>                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| キャッシュエントリの存続可能時間 $n$ 分(Cache Entry Time To Live $n$ Minutes)                                                           | <p>キャッシュ エントリが期限切れになる時間を分単位で入力します。</p> <p>OCSP サーバからの各応答には <b>nextUpdate</b> 値が含まれています。この値は、証明書のステータスがサーバで次にいつ更新されるかを示します。OCSP 応答がキャッシュされるとき、2 つの値 (1 つは設定から、もう 1 つは応答から) が比較され、この 2 つの最小値の時間だけ応答がキャッシュされます。<b>nextUpdate</b> 値が 0 の場合、応答はまったくキャッシュされません。</p> <p>Cisco ISE は設定された時間 OCSP 応答をキャッシュします。キャッシュは複製されず、永続的でもないため、Cisco ISE が再起動するとキャッシュはクリアされます。</p> <p>次の理由により、OCSP キャッシュはOCSP 応答を保持するために使用されます。</p> <ul style="list-style-type: none"> <li>• 既知の証明書に関する OCSP サーバからのネットワークトラフィックと負荷を低減するため</li> <li>• 既知の証明書のステータスをキャッシュすることによって Cisco ISE のパフォーマンスを向上させるため</li> </ul> <p>デフォルトでは、キャッシュは内部CA OCSP クライアントプロファイルに対し 2 分に設定されています。エンドポイントが最初の認証から 2 分以内にもう一度認証すると、OCSP のキャッシュが使用され、OCSP レスポンダには問い合わせされません。エンドポイントの証明書がキャッシュ期間内に失効した場合、以前の OCSP のステータス [良好 (Good)] が使用され、認証は成功します。キャッシュを 0 分に設定すると、応答はキャッシュされません。このオプションでは、セキュリティは向上しますが、認証のパフォーマンスは低下します。</p> |

| フィールド                   | 使用上のガイドライン                                                                                                                                                                    |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| キャッシュのクリア (Clear Cache) | <p>OCSP サービスに接続されているすべての認証局のエントリをクリアするには、[キャッシュのクリア (Clear Cache)] をクリックします。</p> <p>展開内で、[キャッシュのクリア (Clear Cache)] はすべてのノードと相互作用して、処理を実行します。このメカニズムでは、展開内のすべてのノードが更新されます。</p> |

#### 関連トピック

[OCSP サービス](#) (224 ページ)

[Cisco ISE CA サービスの Online Certificate Status Protocol レスポンド](#) (224 ページ)

[OCSP 証明書のステータスの値](#) (225 ページ)

[OCSP ハイ アベイラビリティ](#) (225 ページ)

[OCSP の障害](#) (225 ページ)

[OCSP 統計情報カウンタ](#) (227 ページ)

[OCSP クライアント プロファイルの追加](#) (226 ページ)

## 内部 CA の設定

次の表では、内部 CA の設定ページのフィールドについて説明します。内部 CA の設定を表示し、このページから内部 CA サービスを無効にできます。このページへのナビゲーションパスは、[管理 (Administration)] > [システム (System)] > [証明書 (Certificates)] > [内部 CA の設定 (Internal CA Settings)] です。

| フィールド                                                       | 使用上のガイドライン                                                         |
|-------------------------------------------------------------|--------------------------------------------------------------------|
| 認証局の無効化 (Disable Certificate Authority)                     | 内部 CA サービスを無効にするには、このボタンをクリックします。                                  |
| ホスト名 (Host Name)                                            | CA サービスを実行している Cisco ISE ノードのホスト名。                                 |
| ペルソナ (Personas)                                             | CA サービスを実行しているノードで有効な Cisco ISE ノードのペルソナ。たとえば、管理、ポリシー サービスなどです。    |
| ロール (Role(s))                                               | CA サービスを実行する Cisco ISE ノードが担当するロール。たとえば、スタンドアロンまたはプライマリまたはセカンダリです。 |
| CA、EST、および OCSP 応答側のステータス (CA, EST & OCSP Responder Status) | 有効または無効                                                            |

| フィールド                                | 使用上のガイドライン                             |
|--------------------------------------|----------------------------------------|
| OCSP 応答側 URL<br>(OCSP Responder URL) | OCSP サーバにアクセスするための Cisco ISE ノードの URL。 |
| SCEP URL                             | SCEP サーバにアクセスするための Cisco ISE ノードの URL。 |

#### 関連トピック

[Cisco ISE CA サービス](#) (191 ページ)

[証明書を使用してパーソナル デバイスを許可するための Cisco ISE の設定](#) (204 ページ)

## 証明書テンプレートの設定

次の表に、クライアントプロビジョニングポリシーで使用される SCEP RA プロファイルの定義に使用できる [CA 証明書テンプレート (CA Certificate Template)] ページのフィールドを示します。このページへのナビゲーションパスは、[管理 (Administration)] > [システム (System)] > [証明書 (Certificates)] > [証明書テンプレート (Certificate Templates)] > [追加 (Add)] です。



- (注) 証明書テンプレートフィールド ([組織ユニット (Organizational Unit)], [組織 (Organization)], [都市 (City)], [州 (State)], および [国 (Country)]) の UTF-8 文字はサポートしていません。UTF-8 文字を証明書テンプレートで使用すると、証明書プロビジョニングが失敗します。

| フィールド                  | 使用上のガイドライン                                              |
|------------------------|---------------------------------------------------------|
| [名前 (Name)]            | (必須) 証明書テンプレートの名前を入力します。たとえば、Internal_CA_Template とします。 |
| 説明                     | (任意) 説明を入力します。                                          |
| 一般名 (Common Name) (CN) | (表示のみ) 一般名にはユーザ名が自動入力されます。                              |
| 組織                     | 組織ユニット名。Engineering など。                                 |
| 組織 (Organization) (O)  | 組織名。Cisco など。                                           |
| 都市 (City) (L)          | (省略不可) 都市名。San Jose など。                                 |
| 州 (State) (ST)         | (省略不可) 州名。California など。                                |

| フィールド                                      | 使用上のガイドライン                                           |
|--------------------------------------------|------------------------------------------------------|
| 国 (Country) (C)                            | 国名。2 文字の ISO 国番号を入力する必要があります。US など。                  |
| サブジェクト代替名 (Subject Alternative Name) (SAN) | (表示のみ) エンドポイントの MAC アドレス。                            |
| キー タイプ                                     | RSA または ECC                                          |
| キー サイズ                                     | (RSA を選択した場合にのみ適用可能) 1024 以上のキー サイズを指定します。           |
| 曲線タイプ (Curve Type)                         | (ECC を選択した場合にのみ適用可能) 曲線のタイプを指定します (デフォルトは P-384 です)。 |
| SCEP RA プロファイル (SCEP RA Profile)           | ISE 内部 CA または作成した外部 SCEP RA プロファイルを選択します。            |
| 有効期限 (Valid Period)                        | 証明書の期限が切れるまでの日数を入力します。                               |
| 拡張キーの使用状況                                  |                                                      |
| クライアント認証                                   | クライアント認証にこの証明書を使用する場合は、このチェック ボックスをオンにします。           |
| サーバ認証 (Server Authentication)              | サーバ認証にこの証明書を使用する場合は、このチェック ボックスをオンにします。              |

#### 関連トピック

[証明書テンプレート](#) (197 ページ)

[証明書テンプレート名の拡張子](#) (198 ページ)

[証明書をを使用してパーソナル デバイスを許可するための Cisco ISE の設定](#) (204 ページ)

[pxGrid コントローラ用の Cisco ISE CA 証明書の展開](#) (198 ページ)

[許可ポリシー条件での証明書テンプレート名の使用](#) (198 ページ)

## ロギングの設定

次の各ページでは、デバッグ ログの重大度の設定、外部ログ ターゲットの作成が可能です。また、Cisco ISE がこれらの外部ログ ターゲットにログ メッセージを送信できるようにできます。

## リモート ロギング ターゲットの設定

次の表では、外部の場所（syslogサーバ）を作成してロギングメッセージを保存するために使用できる [リモート ロギング ターゲット（Remote Logging Targets）] ページのフィールドについて説明します。このページへのナビゲーションパスは、**[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [リモート ロギング ターゲット（Remote Logging Targets）]** です。

表 67: リモート ロギング ターゲットの設定

| フィールド                                               | 使用上のガイドライン                                                                                                                                                                                                                          |
|-----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [名前（Name）]                                          | 新しいターゲットの名前を入力します。                                                                                                                                                                                                                  |
| ターゲット タイプ（Target Type）                              | ターゲット タイプを選択します。デフォルトでは、[UDP Syslog] に設定されます。                                                                                                                                                                                       |
| 説明                                                  | 新しいターゲットの簡単な説明を入力します。                                                                                                                                                                                                               |
| [IP アドレス（IP Address）]                               | ログを格納する宛先マシンの IP アドレスを入力します。                                                                                                                                                                                                        |
| [ポート（Port）]                                         | 宛先マシンのポート番号を入力します。                                                                                                                                                                                                                  |
| ファシリティ コード（Facility Code）                           | ロギングに使用する syslog ファシリティ コードを選択します。有効なオプションは、Local0 ～ Local7 です。                                                                                                                                                                     |
| 最大長（Maximum Length）                                 | リモート ログ ターゲット メッセージの最大長を入力します。有効なオプションは 200 ～ 1024 バイトです。                                                                                                                                                                           |
| サーバダウン時のバッファ メッセージ（Buffer Message When Server Down） | TCP syslog ターゲットおよびセキュア syslog ターゲットが使用できないときに Cisco ISE に syslog メッセージをバッファするには、このチェックボックスをオンにします。ISE は、接続が再開されるとターゲットへのメッセージの送信を再試行します。接続が再開された後、メッセージは古いものから順に送信され、バッファ内のメッセージは常に新しいメッセージの前に送信されます。バッファがいっぱいになると、古いメッセージが廃棄されます。 |
| バッファ サイズ（MB）（Buffer Size (MB)）                      | 各ターゲットのバッファサイズを設定します。デフォルトでは、100 MB に設定されます。バッファ サイズを変更するとバッファがクリアされ、特定のターゲットのバッファリングされた既存のすべてのメッセージが失われます。                                                                                                                         |

| フィールド                                              | 使用上のガイドライン                                                                                                                     |
|----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| 再接続タイムアウト（秒）（Reconnect Timeout (Sec)）              | サーバがダウンしている場合に TCP およびセキュア syslog を廃棄する前に保持する期間を秒単位で指定します。                                                                     |
| CA 証明書の選択（Select CA Certificate）                   | クライアント証明書を選択します。                                                                                                               |
| サーバ証明書有効性を無視（Ignore Server Certificate validation） | ISE でサーバ証明書認証が無視されるようにして、syslog サーバを許可するには、このチェックボックスをオンにします。デフォルトでは、このオプションが無効になっているときにシステムが FIPS モードでない限り、このオプションはオフに設定されます。 |

#### 関連トピック

- [Cisco ISE ロギング メカニズム](#)（313 ページ）
- [Cisco ISE システム ログ](#)（314 ページ）
- [リモート syslog メッセージの形式](#)（316 ページ）
- [Cisco ISE メッセージ カタログ](#)（321 ページ）
- [収集フィルタ](#)（323 ページ）
- [イベント抑制バイパス フィルタ](#)（324 ページ）
- [リモート syslog 収集場所の設定](#)（319 ページ）
- [収集フィルタの設定](#)（324 ページ）

## ロギング カテゴリの設定

次の表では、[ロギング カテゴリ（Logging Categories）] ページのフィールドについて説明します。これらのフィールドを使用して、ログの重大度レベルを設定し、選択したカテゴリのログが保存されるロギング ターゲットを選択できます。このページへのナビゲーションパスは、[管理（Administration）]>[システム（System）]>[ロギング（Logging）]>[ロギング カテゴリ（Logging Categories）] です。

表 68: ロギング カテゴリの設定

| フィールド      | 使用上のガイドライン          |
|------------|---------------------|
| [名前（Name）] | ロギング カテゴリの名前を表示します。 |

| フィールド                          | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ログの重大度レベル (Log Severity Level) | <p>次のオプションから、診断ロギング カテゴリの重大度レベルを選択できます。</p> <ul style="list-style-type: none"> <li>• [重大 (FATAL)] : 緊急事態。このオプションは、Cisco ISE が使用できないため、緊急措置が必要であることを意味します</li> <li>• [エラー (ERROR)] : このオプションは深刻な状態またはエラー状態を示します。</li> <li>• [警告 (WARN)] : このオプションは、通常の状態ではあるが重大な状態を示します。これがデフォルトの条件です。</li> <li>• [情報 (INFO)] : このオプションは、情報メッセージを示します。</li> <li>• [デバッグ (DEBUG)] : このオプションは、診断バグ メッセージを示します。</li> </ul> |
| ローカル ロギング (Local Logging)      | ローカル ノードで上のこのカテゴリのロギング イベントを有効にするには、このチェックボックスをオンにします。                                                                                                                                                                                                                                                                                                                                                 |
| ターゲット (Target)                 | 左アイコンと右アイコンを使用して[使用可能 (Available)]と[選択済み (Selected)]のボックス間でターゲットを移動することによって、カテゴリのターゲットを変更できます。[使用可能 (Available)]ボックスには、論理（事前定義済み）と外部（ユーザ定義）という両方の既存のロギング ターゲットが含まれています。最初は空の[選択済み (Selected)]ボックスには、特定のカテゴリの選択済みターゲットが含まれます。                                                                                                                                                                           |

#### 関連トピック

[リモート syslog メッセージの形式](#) (316 ページ)

[Cisco ISE メッセージ コード](#) (320 ページ)

[リモート syslog 収集場所の設定](#) (319 ページ)

[メッセージ コードの重大度レベルの設定](#) (320 ページ)



## メンテナンスの設定

これらのページでは、バックアップ、復元、およびデータ消去機能を使用してデータを管理できます。

### リポジトリの設定

次の表では、リポジトリを作成してバックアップファイルを保存するために使用できる [リポジトリ リスト (Repository List)] ページのフィールドについて説明します。このページへのナビゲーションパスは、[管理 (Administration)] > [システム (System)] > [メンテナンス (Maintenance)] > [リポジトリ (Repository)] です。

表 69: リポジトリの設定

| フィールド              | 使用上のガイドライン                                                                                                                                                                                  |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| リポジトリ (Repository) | リポジトリの名前を入力します。最大 80 文字の英数字を使用できます。                                                                                                                                                         |
| プロトコル              | 使用する使用可能なプロトコルの 1 つを選択します。                                                                                                                                                                  |
| サーバ名 (Server Name) | (TFTP、HTTP、HTTPS、FTP、SFTP、および NFS で必須) リポジトリの作成先サーバのホスト名または IPv4 アドレスを入力します。                                                                                                                |
| パス                 | リポジトリへのパスを入力します。このパスは、リポジトリの作成時に有効であり、存在する必要があります。<br><br>この値は、サーバのルートディレクトリを示す 2 つのスラッシュ (/) または単一のスラッシュ (/) で開始できます。ただし、FTP プロトコルの場合は、単一のスラッシュ (/) はルートディレクトリではなく FTP ユーザのホームディレクトリを示します。 |
| PKI 認証を有効にします。     | (オプション: SFTP リポジトリにのみ適用)<br>SFTP リポジトリで RSA 公開キー認証を有効にするには、このチェック ボックスをオンにします。                                                                                                              |
| ユーザ名 (User Name)   | (FTP、SFTP、および NFS で必須) 指定されたサーバに対する書き込み権限を持つユーザ名を入力します。使用できる文字は英数字のみです。                                                                                                                     |

| フィールド               | 使用上のガイドライン                                                                                                        |
|---------------------|-------------------------------------------------------------------------------------------------------------------|
| [パスワード (Password) ] | (FTP、SFTP、およびNFS で必須) 指定されたサーバへのアクセスに使用するパスワードを入力します。パスワードに使用できる文字は、0～9、a～z、A～Z、-、.、 、@、#、\$、%、^、&、*、,、+、および= です。 |

表 70: リポジトリの設定

| フィールド              | 使用上のガイドライン                                                                                                                                                                                           |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| リポジトリ (Repository) | リポジトリの名前を入力します。最大 80 文字の英数字を使用できます。                                                                                                                                                                  |
| プロトコル              | 使用する使用可能なプロトコルの 1 つを選択します。                                                                                                                                                                           |
| ホスト                | (TFTP、HTTP、HTTPS、FTP、SFTP、およびNFS で必須) リポジトリの作成先サーバのホスト名または IPv4 アドレスを入力します。                                                                                                                          |
| パス                 | <p>リポジトリへのパスを入力します。このパスは、リポジトリの作成時に有効であり、存在している必要があります。</p> <p>この値は、サーバのルートディレクトリを示す 2 つのスラッシュ (/) または単一のスラッシュ (/) で開始できます。ただし、FTP プロトコルの場合は、単一のスラッシュ (/) はルートディレクトリではなく FTP ユーザのホームディレクトリを示します。</p> |

## 関連トピック

[バックアップ/復元リポジトリ](#) (328 ページ)

[リポジトリの作成](#) (329 ページ)

## オンデマンドバックアップの設定

次の表では、バックアップを任意の時点で取得するために使用できる [オンデマンドバックアップ (On-Demand Backup) ] ページのフィールドについて説明します。このページへのナビゲーションパスは、[管理 (Administration) ] > [システム (System) ] > [バックアップ/復元 (Backup & Restore) ] です。

表 71: オンデマンド バックアップの設定

| フィールド                    | 使用上のガイドライン                                                                                                                                                                                                                              |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| バックアップ名 (Backup Name)    | バックアップ ファイルの名前を入力します。                                                                                                                                                                                                                   |
| タイプ (Type)               | 次のいずれかを選択します。 <ul style="list-style-type: none"> <li>• [設定バックアップ (Configuration backup)] : アプリケーション固有および Cisco ADE オペレーティング システム両方の設定データが含まれます。</li> <li>• [操作バックアップ (Operational backup)] : モニタリングおよびトラブルシューティングのデータが含まれます。</li> </ul> |
| リポジトリ名 (Repository Name) | バックアップファイルを保存するリポジトリ。ここにリポジトリ名を入力することはできません。ドロップダウン リストから利用可能なリポジトリのみを選択できます。バックアップの実行前にリポジトリを作成していることを確認してください。                                                                                                                        |
| 暗号化キー (Encryption Key)   | このキーは、バックアップ ファイルの暗号化および解読に使用されます。                                                                                                                                                                                                      |

#### 関連トピック

- [バックアップ データのタイプ](#) (327 ページ)
- [オンデマンドおよびスケジュール バックアップ](#) (331 ページ)
- [バックアップ履歴](#) (336 ページ)
- [バックアップの失敗](#) (336 ページ)
- [Cisco ISE 復元操作](#) (337 ページ)
- [認証および許可ポリシー設定のエクスポート](#) (344 ページ)
- [分散環境でのプライマリ ノードとセカンダリ ノードの同期](#) (345 ページ)
- [オンデマンド バックアップの実行](#) (332 ページ)

## スケジュール バックアップの設定

次の表では、フル バックアップまたは差分バックアップの復元に使用できる [スケジュール バックアップ (Scheduled Backup)] ページのフィールドについて説明します。このページへのナビゲーションパスは、[管理 (Administration)] > [システム (System)] > [バックアップ/復元 (Backup and Restore)] です。

表 72: スケジュール バックアップの設定

| フィールド                              | 使用上のガイドライン                                                                                                                                                                                                                                                              |
|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [名前 (Name) ]                       | バックアップ ファイルの名前を入力します。任意の説明的な名前を入力できます。Cisco ISE は、バックアップ ファイル名にタイムスタンプを追加して、ファイルをリポジトリに格納します。一連のバックアップを設定しても、バックアップ ファイル名は一意になります。[スケジュール バックアップ (Scheduled Backup) ] リストページでは、ファイルが <b>kron occurrence</b> ジョブであることを示すために、バックアップ ファイル名に「 <b>backup_occur</b> 」が付加されます。 |
| 説明                                 | バックアップの説明を入力します。                                                                                                                                                                                                                                                        |
| リポジトリ名 (Repository Name)           | バックアップ ファイルを保存するリポジトリを選択します。ここにリポジトリ名を入力することはできません。ドロップダウン リストから利用可能なリポジトリのみを選択できます。バックアップの実行前にリポジトリを作成していることを確認してください。                                                                                                                                                 |
| 暗号化キー (Encryption Key)             | バックアップ ファイルを暗号化および復号化するためのキーを入力します。                                                                                                                                                                                                                                     |
| スケジュールリング オプション (Schedule Options) | スケジュール バックアップの頻度を選択し、適宜他のオプションに入力します。                                                                                                                                                                                                                                   |

## 関連トピック

- [バックアップ データのタイプ](#) (327 ページ)
- [オンデマンドおよびスケジュール バックアップ](#) (331 ページ)
- [バックアップ履歴](#) (336 ページ)
- [バックアップの失敗](#) (336 ページ)
- [Cisco ISE 復元操作](#) (337 ページ)
- [認証および許可ポリシー設定のエクスポート](#) (344 ページ)
- [分散環境でのプライマリ ノードとセカンダリ ノードの同期](#) (345 ページ)
- [CLI を使用したバックアップ](#) (336 ページ)
- [バックアップのスケジュール](#) (334 ページ)

## 管理者アクセスの設定

これらのページにより、管理者のアクセス設定を行うことができます。

## 管理者パスワードポリシーの設定

次の表に、管理者パスワードが満たす必要のある基準を定義するために使用できる [管理者パスワードポリシー (Administrator Password Policy)] ページのフィールドを示します。このページのナビゲーションパスは、[管理 (Administration)] > [システム (System)] > [管理アクセス (Admin Access)] > [認証 (Authentication)] > [パスワードポリシー (Password Policy)] です。

表 73: 管理者パスワードポリシーの設定

| フィールド                | 使用上のガイドライン                            |
|----------------------|---------------------------------------|
| 最小長 (Minimum Length) | パスワードの最小長 (文字数) を設定します。デフォルトは 6 文字です。 |

| フィールド                                     | 使用上のガイドライン                                                                                                                    |
|-------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| パスワードに使用できない文字 (Password may not contain) | [管理者名またはその文字の逆順は使用できません (Admin name or its characters in reverse order)] : このチェックボックスをオンにして、管理者ユーザ名またはその文字の逆順での使用を制限します。      |
|                                           | [「cisco」またはその文字の逆順は使用できません ("cisco" or its characters in reverse order)] : このチェックボックスをオンにして、単語「cisco」またはその文字の逆順での使用を制限します。    |
|                                           | [この単語またはその文字の逆順は使用できません (This word or its characters in reverse order)] : このチェックボックスをオンにして、定義したすべての単語またはその文字の逆順での使用を制限します。    |
|                                           | [4 回以上連続する繰り返し文字は使用できません (Repeated characters four or more times consecutively)] : このチェックボックスをオンにして、4 回以上連続する繰り返し文字の使用を制限します。 |

| フィールド                       | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                             | <p>[辞書の単語、その文字の逆順、または文字の置き換えは使用できません (Dictionary words, their characters in reverse order or their letters replaced with other characters)]: 辞書の単語、単語の文字の逆順での使用、単語の文字の置き換えでの使用を制限します。</p> <p>「s」を「\$」、「a」を「@」、「o」を「0」、「l」を「1」、「i」を「!」、「e」を「3」に置き換えることはできません。たとえば Pa\$\$w0rd などです。</p> <ul style="list-style-type: none"><li>• [デフォルトの辞書 (Default Dictionary)]: Cisco ISE でデフォルトの Linux 辞書を使用するには、このオプションを選択します。デフォルトの辞書には約 480,000 件の英単語が含まれています。</li></ul> <p>デフォルトでは、このオプションが選択されています。</p> <ul style="list-style-type: none"><li>• [カスタム辞書 (Custom Dictionary)]: カスタマイズした辞書を使用するには、このオプションを選択します。[ファイルの選択 (Choose File)] をクリックし、カスタム辞書ファイルを選択します。このテキストファイルでは、単語が改行文字で区切られており、拡張子は .dic、サイズは 20 MB 以下である必要があります。</li></ul> |
| 必須の文字 (Required Characters) | <p>管理者パスワードに、次の選択肢から選択したタイプの文字が少なくとも 1 つ含まれている必要があることを指定します。</p> <ul style="list-style-type: none"><li>• 小文字の英文字 (Lowercase alphabetic characters)</li><li>• 大文字の英文字 (Uppercase alphabetic characters)</li><li>• 数字 (Numeric characters)</li><li>• 英数字以外の文字 (Non-alphanumeric characters)</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                          |

| フィールド                                                                                | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| パスワード履歴 (Password History)                                                           | <p>同じパスワードが繰り返し使用されるのを防ぐために、新しいパスワードと異なっている必要がある以前のパスワードの数を指定します。</p> <p>また、以前のパスワードと異なる必要がある文字数を指定します。</p> <p>ユーザがパスワードを再使用できない日数を入力します。</p>                                                                                                                                                                                                                                          |
| パスワードライフタイム (Password Lifetime)                                                      | <p>次のオプションを指定して、指定した期間後にパスワードを変更するようユーザに強制します。</p> <ul style="list-style-type: none"> <li>パスワードが変更されなかった場合に管理者アカウントを無効にするまでの時間 (日数) (Time (in days) before the administrator account is disabled if the password is not changed.) (使用可能な範囲は 0 ~ 2,147,483,647 日です)。</li> <li>管理者アカウントが無効になるまでのリマインダ (日数)。(Reminder (in days) before the administrator account is disabled.)</li> </ul> |
| ログイン試行の不正なアカウントをロックまたは一時停止する (Lock or Suspend Account with Incorrect Login Attempts) | <p>Cisco ISE が、管理者を Cisco ISE からロックアウトし、アカウントクレデンシャルを一時停止または無効にするまでに、誤った管理者パスワードを記録する回数を指定します。</p> <p>アカウントがロックされる管理者に電子メールが送信されます。カスタム電子メール修復メッセージを入力することができます。</p>                                                                                                                                                                                                                   |
| ネットワーク デバイスの機密データの表示                                                                 |                                                                                                                                                                                                                                                                                                                                                                                        |
| 管理者パスワードが必要 (Require Admin Password)                                                 | <p>共有秘密やパスワードなどのネットワーク デバイスの機密データを表示するために管理者ユーザがログイン パスワードを入力するようにする場合には、このチェックボックスにマークを付けます。</p>                                                                                                                                                                                                                                                                                      |



| フィールド                               | 使用上のガイドライン                                                                                                        |
|-------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| パスワードのキャッシュ期間 (Password cached for) | 管理者ユーザによって入力されたパスワードは、この期間キャッシュされます。管理者ユーザはこの間、ネットワークデバイスの機密データを表示するためにパスワードの再入力を求められることはありません。有効な範囲は 1 ～ 60 分です。 |

#### 関連トピック

[Cisco ISE 管理者](#) (117 ページ)

[新しい Cisco ISE 管理者の作成](#) (118 ページ)

## セッション タイムアウトおよびセッション情報の設定

次の表では、セッションタイムアウトを定義し、アクティブな管理セッションを終了するために使用できる[セッション (Session)] ページのフィールドについて説明します。このページへのナビゲーションパスは、**[管理 (Administration)] > [システム (System)] > [管理者アクセス (Admin Access)] > [設定 (Settings)] > [セッション (Session)]** です。

表 74: セッション タイムアウトおよびセッション情報の設定

| フィールド                                   | 使用上のガイドライン                                                                                  |
|-----------------------------------------|---------------------------------------------------------------------------------------------|
| セッションのタイムアウト (Session Timeout)          |                                                                                             |
| セッションアイドル タイムアウト (Session Idle Timeout) | アクティビティがない場合に管理者をログアウトするまでに Cisco ISE が待機する時間 (分) を入力します。デフォルト値は 60 分です。有効な範囲は 6 ～ 100 分です。 |
| セッション情報 (Session Info)                  |                                                                                             |
| 無効化 (Invalidate)                        | 終了するセッション ID の隣にあるチェックボックスをオンにし、[無効化 (Invalidate)] をクリックします。                                |

#### 関連トピック

[管理者アクセスの設定](#) (136 ページ)

[管理者のセッション タイムアウトの設定](#) (139 ページ)

[アクティブな管理セッションの終了](#) (140 ページ)

## 設定

これらのページでは、さまざまなサービスの全般設定を行うことができます。

## ポスチャの全般設定

次の表では、修復時間およびポスチャステータスなどの一般的なポスチャ設定を行うために使用できる [ポスチャの全般設定 (Posture General Settings)] ページのフィールドについて説明します。このページへのナビゲーションパスは、[管理 (Administration)] > [システム (System)] > [設定 (Settings)] > [ポスチャ (Posture)] > [全般設定 (General Settings)] です。

表 75: ポスチャの全般設定

| フィールド                                                                          | 使用上のガイドライン                                                                                                                                                                                     |
|--------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 修復タイマー (Remediation Timer)                                                     | 分単位で時間値を入力します。デフォルト値は 4 分です。有効な範囲は 1 ～ 300 分です。                                                                                                                                                |
| ネットワーク遷移遅延 (Network Transition Delay)                                          | 秒単位で時間値を入力します。デフォルト値は 3 秒です。有効な値の範囲は 2 ～ 30 秒です。                                                                                                                                               |
| デフォルトのポスチャステータス (Default Posture Status)                                       | 準拠または非準拠を選択します。Linux のような非エージェント デバイスは、ネットワークに接続している間、このステータスを想定します。                                                                                                                           |
| 一定時間 (秒) 経過後にログイン成功画面を自動的に閉じる (Automatically Close Login Success Screen After) | このチェックボックスをオンにすると、指定された時間後に、ログイン成功画面が自動的に閉じます。<br><br>チェックボックスの隣のフィールドに、時間値を秒単位で入力します。<br><br>0 ～ 300 秒にログイン画面が自動的に閉じるようにタイマーを設定できます。時間をゼロに設定すると、NAC Agent および Web Agent にログイン成功画面が表示されなくなります。 |
| 連続モニタリング間隔 (Continuous Monitoring Interval)                                    | AnyConnect がモニタリングデータの送信を開始するまでの時間間隔を指定します。アプリケーション条件の場合、デフォルト値は 5 分です。                                                                                                                        |
| ステルスモードでの利用規約 (Acceptable Use Policy in Stealth Mode)                          | 会社のネットワーク使用条件が満たされていない場合、ステルスモードで [ブロック (Block)] を選択して、クライアントを非準拠ポスチャステータスに移行します。                                                                                                              |
| ポスチャのリース                                                                       |                                                                                                                                                                                                |

| フィールド                                                                                              | 使用上のガイドライン                                                         |
|----------------------------------------------------------------------------------------------------|--------------------------------------------------------------------|
| ユーザがネットワークに接続するたびにポスチャ評価を行う (Perform posture assessment every time a user connects to the network) | ユーザがネットワークに接続するたびにポスチャ評価を開始するには、このオプションを選択します。                     |
| $n$ 日おきにポスチャ評価を行う (Perform posture assessment every $n$ days)                                      | クライアントがすでにポスチャ準拠であるものの、指定された日数が経過したら、ポスチャ評価を開始する場合は、このオプションを選択します。 |

### 関連トピック

[ポスチャ サービス \(932 ページ\)](#)

[ポスチャ管理の設定 \(936 ページ\)](#)

[ポスチャのリース \(938 ページ\)](#)

[Cisco ISE でのポスチャセッションサービスの有効化 \(935 ページ\)](#)

[指定した時間内で修復するためのクライアントの修復タイマーの設定 \(937 ページ\)](#)

[クライアントの遷移のためのネットワーク遷移遅延タイマーの設定 \(937 ページ\)](#)

[ログイン成功ウィンドウを自動的に閉じる設定 \(937 ページ\)](#)

[非エージェント デバイスへのポスチャ ステータスの設定 \(938 ページ\)](#)

## ポスチャ再評価の構成設定

次の表では、ポスチャ再評価の設定に使用できる [ポスチャ再評価設定 (Posture Reassessment Configurations)] ページのフィールドについて説明します。このページへのナビゲーションパスは、[管理 (Administration)] > [システム (System)] > [設定 (Settings)] > [ポスチャ (Posture)] > [再評価 (Reassessments)] です。

表 76: ポスチャ再評価の構成設定

| フィールド                                     | 使用上のガイドライン                                  |
|-------------------------------------------|---------------------------------------------|
| 構成名                                       | PRA 設定の名前を入力します。                            |
| 設定の説明 (Configuration Description)         | PRA 設定の説明を入力します。                            |
| 再評価適用を使用? (Use Reassessment Enforcement?) | ユーザ ID グループの PRA 設定を適用するには、チェックボックスをオンにします。 |

| フィールド                    | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 適用タイプ (Enforcement Type) | <p>適用する次のアクションを選択します。</p> <ul style="list-style-type: none"> <li>• [続行 (Continue)] : ユーザはポスチャ要件に関係なくクライアントを修復できるようにユーザ介入なしの特権アクセスが引き続き提供されます。</li> <li>• [ログオフ (Logoff)] : クライアントが非準拠の場合、ユーザを強制的にネットワークからログオフします。 クライアントが再度ログインしたときのコンプライアンスステータスは不明です。</li> <li>• [修復 (Remediate)] : クライアントが非準拠の場合、エージェントは修復のために指定の期間待機します。 クライアントが修復された後、エージェントはポリシーサービスノードに PRA レポートを送信します。 修復がクライアントで無視された場合、エージェントはクライアントにネットワークからログオフすることを強制するために、ポリシーサービスノードにログオフ要求を送信します。</li> </ul> <p>ポスチャ要件が [必須 (mandatory)] に設定されている場合、RADIUS セッションは PRA 障害アクションの結果としてクリアされ、クライアントを再びポスチャするには新しい RADIUS セッションを開始する必要があります。</p> <p>ポスチャ要件が [オプション (optional)] に設定されている場合、NAC Agent ではユーザがエージェントから [続行 (continue)] オプションをクリックできます。ユーザは、制限なしで現在のネットワークにとどまることができます。</p> |
| インターバル (Interval)        | <p>最初のログイン成功後にクライアントで PRA を開始する間隔を分単位で入力します。</p> <p>デフォルト値は 240 分です。最小値は 60 分、最大値は 1440 分です。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

| フィールド                                        | 使用上のガイドライン                                                                                                                                                                                                                            |
|----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 猶予時間 (Grace time)                            | <p>クライアントが修復を完了することのできる時間間隔を分単位で入力します。猶予時間をゼロにすることはできません。また、PRA 間隔より大きくする必要があります。デフォルトの最小間隔 (5 分) から最小 PRA 間隔までの範囲にすることができます。</p> <p>最小値は 5 分、最大値は 60 分です。</p> <p>(注) 猶予時間は、クライアントがポスチャの再評価に失敗した後、適用タイプが修復アクションに設定されている場合にだけ有効です。</p> |
| ユーザ ID グループの選択 (Select User Identity Groups) | PRA 設定に対して一意のグループまたはグループの一意の組み合わせを選択します。                                                                                                                                                                                              |
| PRA の設定 (PRA configurations)                 | 既存の PRA 設定と PRA 設定に関連付けられたユーザ ID グループを表示します。                                                                                                                                                                                          |

#### 関連トピック

- [ポスチャのリース \(938 ページ\)](#)
- [定期的再評価 \(939 ページ\)](#)
- [ポスチャ評価オプション](#)
- [ポスチャ修復オプション \(950 ページ\)](#)
- [ポスチャのカスタム条件 \(951 ページ\)](#)
- [カスタム ポスチャ修復アクション \(952 ページ\)](#)
- [定期的再評価の設定 \(939 ページ\)](#)

## ポスチャの利用規定の構成設定

次の表では、ポスチャのアクセプタブルユースポリシーを設定するために使用できるポスチャの [利用規定設定 (Acceptable Use Policy Configurations)] ページのフィールドについて説明します。このページへのナビゲーションパスは、**[管理 (Administration)] > [システム (System)] > [設定 (Settings)] > [ポスチャ (Posture)] > [利用規定 (Acceptable Use Policy)]** です。

表 77: ポスチャ AUP の設定

| フィールド | 使用上のガイドライン                |
|-------|---------------------------|
| 構成名   | ユーザが作成する AUP 設定の名前を入力します。 |

| フィールド                                                                                 | 使用上のガイドライン                                                                                                                                                                   |
|---------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 設定の説明 (Configuration Description)                                                     | ユーザが作成する AUP 設定の説明を入力します。                                                                                                                                                    |
| エージェント ユーザへの AUP の表示 (Show AUP to Agent users) (Windows の NAC Agent および Web Agent のみ) | オンにした場合、[エージェント ユーザへの AUP の表示 (Show AUP to Agent users)] チェックボックスはユーザ (Windows の NAC Agent と Web Agent のみ) にネットワークの利用規約へのリンクを表示し、それをクリックすると、認証およびポスチャ評価が成功したときに AUP が表示されます。 |
| AUP メッセージの URL を使用 (Use URL for AUP message) オプション ボタン                                | 選択した場合、認証およびポスチャ評価が成功したときにクライアントがアクセスする必要がある AUP メッセージへの URL を AUP URL に入力する必要があります。                                                                                         |
| AUP メッセージのファイルを使用 (Use file for AUP message) オプション ボタン                                | 選択した場合、場所を参照し、トップ レベルに index.html を含む AUP ファイルにジップ形式のファイルをアップロードします。<br><br>.zip ファイルには、index.html ファイルに加えて、他のファイルおよびサブディレクトリを含めることができます。これらのファイルは、HTML タグを使用して相互に参照できます。    |
| AUP URL                                                                               | クライアントは認証およびポスチャ評価が成功したときにアクセスする必要がある AUP への URL を入力します。                                                                                                                     |
| AUP ファイル (AUP File)                                                                   | [AUP ファイル (AUP File)] で、ファイルを参照し、Cisco ISE サーバにアップロードします。これは zip 形式のファイルで、zip 形式のファイルではトップ レベルに index.html ファイルを含める必要があります。                                                  |

| フィールド                                                                     | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ユーザ ID グループの選択 (Select User Identity Groups)                              | <p>[ユーザ ID グループの選択 (Select User Identity Groups) ] ドロップダウン リストで、AUP 設定の一意のユーザ ID グループまたはユーザ ID グループの一意の組み合わせを選択します。</p> <p>AUP 設定を作成する場合は、次の点に注意してください。</p> <ul style="list-style-type: none"> <li>• ポスチャ AUP は、ゲストフローには適用できません。</li> <li>• 各設定には、一意のユーザ ID グループ、またはユーザ ID グループの一意の組み合わせが必要です。</li> <li>• 2 つの設定が共通のユーザ ID グループを持つことはできません。</li> <li>• ユーザ ID グループ「Any」で AUP 設定を作成する場合は、まず他のすべての AUP 設定を削除します。</li> <li>• ユーザ ID グループ「Any」を使用して AUP 設定を作成した場合、一意のユーザ ID グループ、または複数のユーザ ID グループを使用して他の AUP 設定を作成することはできません。Any 以外のユーザ ID グループを使用して AUP 設定を作成するには、最初にユーザ ID グループ「Any」を使用した既存の AUP 設定を削除するか、ユーザ ID グループ「Any」を使用した既存の AUP 設定を一意のユーザ ID グループまたは複数のユーザの ID グループを使用して更新します。</li> </ul> |
| 利用規定設定 - 設定リスト (Acceptable use policy configurations—Configurations list) | <p>既存の AUP 設定と AUP 設定に関連付けられたエンドユーザ ID グループを一覧表示します。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

#### 関連トピック

[ポスチャ サービス \(932 ページ\)](#)

[ポスチャ評価の利用規定の設定 \(941 ページ\)](#)

## EAP-FAST 設定

次の表に、EAP-FAST、EAP-TLS、およびPEAPプロトコルを設定するために使用できる[プロトコル設定 (Protocol Settings)] ページのフィールドを示します。このページへのナビゲーションパスは、[管理 (Administration)] > [システム (System)] > [設定 (Settings)] > [プロトコル (Protocols)] > [EAP-FAST] > [EAP-FAST 設定 (EAP-FAST Settings)] です。

表 78: EAP-FAST の設定

| フィールド                                                    | 使用上のガイドライン                                                                                                                                                                |
|----------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 機関識別情報の説明 (Authority Identity Info Description)          | クレデンシャルをクライアントに送信する Cisco ISE ノードを説明したわかりやすい文字列を入力します。クライアントは、この文字列をタイプ、長さ、および値 (TLV) の Protected Access Credentials (PAC) 情報で認識できます。デフォルト値は、Identity Services Engine です。 |
| マスター キー生成期間 (Master Key Generation Period)               | マスターキー生成期間を、秒、分、時間、日、または週単位で指定します。値は、1 ～ 2147040000 秒の正の整数である必要があります。デフォルトは 604800 秒で、これは 1 週間と同等です。                                                                      |
| すべてのマスター キーおよび PAC の失効 (Revoke all master keys and PACs) | すべてのマスターキーと PAC を失効させるには、[失効 (Revoke)] をクリックします。                                                                                                                          |
| PAC なしセッション再開の有効化 (Enable PAC-less Session Resume)       | PAC ファイルなしで EAP-FAST を使用する場合は、このチェックボックスをオンにします。                                                                                                                          |
| PAC なしセッションのタイムアウト (PAC-less Session Timeout)            | PAC なしセッションの再開がタイムアウトするまでの時間を秒単位で指定します。デフォルトは 7200 秒です。                                                                                                                   |

### 関連トピック

[認証用のプロトコルの設定 \(686 ページ\)](#)

[認証プロトコルとして EAP-FAST を使用するためのガイドライン \(686 ページ\)](#)

[EAP-FAST の利点 \(1483 ページ\)](#)

[EAP-FAST の設定 \(687 ページ\)](#)

## EAP-FAST の PAC の生成の設定

次の表では、[PAC の生成 (Generate PAC)] ページ上のフィールドについて説明します。これらのフィールドを使用して、EAP-FAST 認証用の Protected Access Credentials を設定します。このページのナビゲーションパスは、[管理 (Administration)] > [システム (System)] > [設定



(Settings) ] > [ プロトコル (Protocols) ] > [ EAP-FAST ] > [ PAC の生成 (Generate PAC) ] です。

表 79: EAP-FAST の PAC の生成の設定

| フィールド                         | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                             |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| トンネル PAC (Tunnel PAC)         | トンネル PAC を生成するには、このオプション ボタンをクリックします。                                                                                                                                                                                                                                                                                                                                                                  |
| マシン PAC (Machine PAC)         | マシン PAC を生成するには、このオプション ボタンをクリックします。                                                                                                                                                                                                                                                                                                                                                                   |
| TrustSec PAC                  | TrustSec PAC を生成するには、このオプション ボタンをクリックします。                                                                                                                                                                                                                                                                                                                                                              |
| ID (Identity)                 | (トンネル PAC およびマシン PAC の ID フィールド用) EAP-FAST プロトコルによって「内部ユーザ名」として示されるユーザ名またはマシン名を指定します。ID 文字列がそのユーザ名と一致しない場合、認証は失敗します。これは、適応型セキュリティ アプライアンス (ASA) で定義されているホスト名です。ID 文字列は、ASA ホスト名に一致する必要があります。一致しない場合、ASA は生成された PAC ファイルをインポートできません。TrustSec PAC を生成する場合、[ID (Identity) ] フィールドにより TrustSec ネットワーク デバイスのデバイス ID が指定され、EAP-FAST プロトコルによりイニシエータ ID とともに提供されます。ここに入力した ID 文字列がそのデバイス ID に一致しない場合、認証は失敗します。 |
| PAC 存続可能時間 (PAC Time To Live) | (トンネル PAC およびマシン PAC 用) PAC の有効期限を指定する値を秒単位で入力します。デフォルトは 604800 秒で、これは 1 週間と同等です。この値は、1 ~ 157680000 秒の正の整数である必要があります。TrustSec PAC に対しては、日、週、月、または年単位で値を入力します。デフォルト値は 1 年です。最小値は 1 日、最大値は 10 年です。                                                                                                                                                                                                       |
| 暗号化キー (Encryption Key)        | 暗号化キーを入力します。キーの長さは 8 ~ 256 文字にする必要があります。キーはアルファベットの大文字または小文字、数字、または英数字の組み合わせを含むことができます。                                                                                                                                                                                                                                                                                                                |

| フィールド                 | 使用上のガイドライン                                     |
|-----------------------|------------------------------------------------|
| 期限日 (Expiration Date) | (TrustSec PAC のみ) 有効期限は、PAC 存続可能時間に基づいて計算されます。 |

#### 関連トピック

[認証用のプロトコルの設定](#) (686 ページ)

[認証プロトコルとして EAP-FAST を使用するためのガイドライン](#) (686 ページ)

[EAP-FAST の PAC の生成](#) (687 ページ)

## EAP-TTLS 設定

次の表では、[EAP-TTLS設定 (EAP-TTLS Settings)] ページのフィールドについて説明します。このページへのナビゲーションパスは、[管理 (Administration)] > [システム (System)] > [設定 (Settings)] > [プロトコル (Protocols)] > [EAP-TTLS] です。

表 80: EAP-TTLS 設定

| フィールド                                                   | 使用上のガイドライン                                                                                                                                                                                                                                                                                         |
|---------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| EAP-TTLSセッションの再開を有効にする (Enable EAP-TTLS Session Resume) | このチェックボックスをオンにすると、Cisco ISE はユーザが EAP-TTLS 認証のフェーズ 2 で正常に認証された場合に限り、EAP-TTLS 認証のフェーズ 1 で作成された TLS セッションをキャッシュします。ユーザが再接続しようとする場合、元の EAP-TTLS セッションがタイムアウトしていなければ、Cisco ISE はキャッシュされた TLS セッションを使用します。このため、EAP-TTLS のパフォーマンスが向上し、AAA サーバの負荷が軽減されます。<br><br>(注) EAP-TTLS セッションが再開されると、内部方式はスキップされます。 |
| EAP-TTLSセッションタイムアウト (EAP-TTLS Session Timeout)          | EAP-TTLS セッションがタイムアウトするまでの時間を秒単位で指定します。デフォルト値は 7200 秒です。                                                                                                                                                                                                                                           |

#### 関連トピック

[認証用のプロトコルの設定](#) (686 ページ)

[認証プロトコルとしての EAP-TTLS の使用](#) (688 ページ)

[EAP-TLS の設定](#) (688 ページ)

## EAP-TLS 設定

次の表に、EAP-TLS プロトコル設定を行うために使用できる [EAP-TLS 設定 (EAP-TLS Settings)] ページのフィールドを示します。このページへのナビゲーションパスは、[管理 (Administration)] > [システム (System)] > [設定 (Settings)] > [プロトコル (Protocols)] > [EAP-TLS] です。

表 81: EAP-TLS 設定

| フィールド                                                  | 使用上のガイドライン                                                                                                                                                       |
|--------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| EAP-TLS セッションの再開を有効にする (Enable EAP-TLS Session Resume) | 完全な EAP-TLS 認証に成功したユーザの簡略化された再認証をサポートする場合にオンにします。この機能により、Secure Sockets Layer (SSL) ハンドシェイクのみでユーザの再認証が可能となり、証明書の適用が不要になります。EAP-TLS セッションは、タイムアウトしていない限り動作を再開します。 |
| EAP-TLS セッションタイムアウト (EAP-TLS Session Timeout)          | EAP-TLS セッションがタイムアウトするまでの時間を秒単位で指定します。デフォルト値は 7200 秒です。                                                                                                          |
| [ステートレス セッション再開 (Stateless Session Resume)]            |                                                                                                                                                                  |
| マスター キー生成期間 (Master Key Generation Period)             | マスターキー再生成までの時間を入力します。この値により、マスター キーがアクティブである期間が決定します。この値は秒、分、時、日数、または週数で入力できます。                                                                                  |
| [取り消し (Revoke)]                                        | これまでに生成されたすべてのマスター キーとチケットをキャンセルするには、[取り消し (Revoke)] をクリックします。このオプションは、セカンダリ ノードでは無効です。                                                                          |

### 関連トピック

[認証用の プロトコルの設定](#) (686 ページ)

[EAP-TLS の設定](#) (689 ページ)

## PEAP 設定

次の表では、PEAP プロトコル設定を行うために使用できる [PEAP 設定 (PEAP Settings)] ページのフィールドについて説明します。このページへのナビゲーションパスは、[管理 (Administration)] > [システム (System)] > [設定 (Settings)] > [プロトコル (Protocols)] > [PEAP] です。

表 82: PEAP 設定

| フィールド                                            | 使用上のガイドライン                                                                                                                                                                                                                                                                               |
|--------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PEAP セッションの再開を有効にする (Enable PEAP Session Resume) | このチェックボックスをオンにすると、Cisco ISE はユーザが PEAP 認証のフェーズ 2 で正常に認証された場合に限り、PEAP 認証のフェーズ 1 で作成された TLS セッションをキャッシュします。ユーザが再接続しようとする場合、元の PEAP セッションがタイムアウトしていなければ、Cisco ISE はキャッシュされた TLS セッションを使用します。このため、PEAP のパフォーマンスが向上し、AAA サーバの負荷が軽減されます。PEAP セッション再開機能を動作させるには、PEAP セッション タイムアウト値を指定する必要があります。 |
| PEAP セッションタイムアウト (PEAP Session Timeout)          | PEAP セッションがタイムアウトするまでの時間を秒単位で指定します。デフォルト値は 7200 秒です。                                                                                                                                                                                                                                     |
| 高速再接続を有効にする (Enable Fast Reconnect)              | このチェックボックスをオンにすると、セッション再開機能が有効な場合に、ユーザ クレデンシャルを確認しないで PEAP セッションが Cisco ISE で再開することが許可されます。                                                                                                                                                                                              |

## 関連トピック

[認証用の プロトコルの設定](#) (686 ページ)

[PEAP の設定](#) (689 ページ)

[PEAP の使用の利点](#) (1481 ページ)

[PEAP プロトコルでサポートされているサブリカント](#) (1481 ページ)

[PEAP プロトコルのフロー](#) (1481 ページ)

## RADIUS 設定

次の表に、[RADIUS 設定 (RADIUS Settings)] ページにある各フィールドの説明を示します。このページへのナビゲーションパスは、[管理 (Administration)] > [システム (System)] > [設定 (Settings)] > [プロトコル (Protocols)] > [RADIUS] です。

[繰り返し失敗するクライアントの抑制 (Suppress Repeated Failed Clients)] オプションを有効にすると、認証が繰り返し失敗するクライアントは監査ログに出力されず、指定された期間にわたってこれらのクライアントからの要求が自動的に拒否されます。また、認証失敗回数を指定できます。失敗回数がこの回数を超えると、これらのクライアントからの要求は拒否されます。たとえばこの値を 5 に設定すると、クライアント認証が 5 回失敗した場合、指定された期間にわたってそのクライアントから受信する要求はすべて拒否されます。

表 83: RADIUS 設定

| フィールド                                                                                            | 使用上のガイドライン                                                                                                                                                                                                                 |
|--------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [繰り返し失敗するクライアントの抑制 (Suppress Repeated Failed Clients) ]                                          |                                                                                                                                                                                                                            |
| [繰り返し失敗するクライアントの抑制 (Suppress Repeated Failed Clients) ]                                          | 同じ理由で繰り返し認証に失敗するクライアントを抑止するには、このチェックボックスをオンにします。これらのクライアントは監査ログに出力されず、また[繰り返し失敗したクライアントからの RADIUS 要求を拒否する (Reject RADIUS Requests from Clients with Repeated Failures) ] オプションが有効な場合には、指定された期間にわたってこれらのクライアントからの要求が拒否されます。 |
| [2回の失敗を検出する期間 (Detect Two Failures Within) ]                                                     | 分単位で時間間隔を入力します。クライアントがこの期間内に同じ理由で 2 回認証に失敗すると、監査ログに出力されず、また[繰り返し失敗したクライアントからの RADIUS 要求を拒否する (Reject RADIUS Requests from Clients with Repeated Failures) ] オプションが有効な場合には、指定された期間にわたってこのクライアントからの要求が拒否されます。                |
| [失敗を報告する間隔 (Report Failures Once Every) ]                                                        | 報告対象の認証失敗の時間間隔を分単位で入力します。たとえば、この値を 15 分に設定すると、繰り返し認証に失敗するクライアントが 15 分に 1 回だけ監査ログに報告されるため、報告の重複が防止されます。                                                                                                                     |
| [繰り返し失敗したクライアントからの RADIUS 要求を拒否する (Reject RADIUS Requests from Clients with Repeated Failures) ] | 認証が繰り返し失敗するクライアントからの RADIUS 要求を自動的に拒否するには、このチェック ボックスをオンにします。Cisco ISE による不要な処理を防ぎ、Denial of Service (DoS) 攻撃から防御するには、このオプションを有効にします。                                                                                      |
| [自動拒否前の失敗回数 (Failures Prior to Automatic Rejection) ]                                            | 認証失敗回数を入力します。認証失敗回数がこの値を超えると、繰り返し失敗するクライアントからの要求は自動的に拒否されます。設定されている期間 ([要求を拒否する期間 (Continue Rejecting Requests for) ] で指定) にわたり、これらのクライアントから受信する要求はすべて自動的に拒否されます。この期間が経過した後では、これらのクライアントからの認証要求が処理されます。                    |

| フィールド                                                                    | 使用上のガイドライン                                                                                                                                                                |
|--------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [要求を拒否する期間 (Continue Rejecting Requests for) ]                           | 繰り返し失敗するクライアントからの要求を拒否する時間間隔を分単位で入力します。                                                                                                                                   |
| [繰り返し発生するアカウンティング更新を無視する期間 (Ignore Repeated Accounting Updates Within) ] | この期間内に繰り返し発生するアカウンティング更新は無視されます。                                                                                                                                          |
| [成功レポートの抑制 (Suppress Successful Reports) ]                               |                                                                                                                                                                           |
| 繰り返される認証成功の抑制 (Suppress Repeated Successful Authentications)             | 直近の 24 時間で、ID、ネットワーク デバイス、および許可のコンテキストに変更がない認証要求成功が繰り返し報告されないようにするには、このチェックボックスをオンにします。                                                                                   |
| [認証の詳細 (Authentications Details) ]                                       |                                                                                                                                                                           |
| [次よりも長いステップを強調表示 (Highlight Steps Longer Than) ]                         | ミリ秒単位で時間間隔を入力します。1つのステップの実行が指定のしきい値を超えると、認証詳細ページでそのステップがクロック アイコンでマークされます。                                                                                                |
| RADIUS UDP ポート                                                           |                                                                                                                                                                           |
| 認証ポート (Authentication Port)                                              | RADIUS UDP の認証フローに使用するポートを指定します。最大 4 つのポート番号（カンマ区切り）を指定できます。デフォルトでは、ポート 1812 とポート 1645 が使用されます。値の範囲は 1024 ～ 65535 です。                                                     |
| アカウンティング ポート (Accounting Port)                                           | RADIUS UDP のアカウンティングフローに使用するポートを指定します。最大 4 つのポート番号（カンマ区切り）を指定できます。デフォルトでは、ポート 1813 とポート 1646 が使用されます。値の範囲は 1024 ～ 65535 です。<br><br>(注) これらのポートが他のサービスにより使用されていないことを確認します。 |
| RADIUS DTLS                                                              |                                                                                                                                                                           |

| フィールド                                                     | 使用上のガイドライン                                                                                                                               |
|-----------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| 認証およびアカウントリング ポート<br>(Authentication and Accounting Port) | RADIUS DTLS の認証およびアカウントリング フローに使用するポートを指定します。デフォルトでは、ポート 2083 が使用されます。値の範囲は 1024 ～ 65535 です。<br><br>(注) このポートが他のサービスにより使用されていないことを確認します。 |
| アイドル タイムアウト                                               | パケットがネットワーク デバイスから届かなかったら、TLS セッションを終了する前に、Cisco ISE を待機する時間を秒単位で入力します。デフォルト値は 120 秒です。有効な範囲は 60 ～ 600 秒です。                              |

#### 関連トピック

[認証用の プロトコルの設定](#) (686 ページ)

[Cisco ISE の RADIUS プロトコルのサポート](#) (1476 ページ)

[RADIUS の設定](#) (689 ページ)

## 一般 TrustSec の設定

Cisco ISE が TrustSec サーバとして機能したり、TrustSec サービスを提供したりするには、グローバル TrustSec 設定を定義する必要があります。以下の表に、[TrustSec 設定 (TrustSec Settings)] ウィンドウのフィールドの説明を示します ([ワークセンター (Work Centers)] > [TrustSec] > [設定 (Settings)] > [一般 TrustSec の設定 (General TrustSec Settings)] )。

表 84 : TrustSec 設定の設定

| フィールド                                      | 使用上のガイドライン                                                                                                                                                                                                                                                                   |
|--------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| トンネル PAC の存続可能時間 (Tunnel PAC Time to Live) | PAC の有効期限を指定します。トンネル PAC は EAP-FAST プロトコル用のトンネルを生成します。時間を秒、分、時、日数、または週数で指定できます。デフォルト値は 90 日です。有効な範囲は次のとおりです。 <ul style="list-style-type: none"> <li>• 1 ～ 157680000 秒</li> <li>• 1 ～ 2628000 分</li> <li>• 1 ～ 43800 時間</li> <li>• 1 ～ 1825 日</li> <li>• 1 ～ 260 週</li> </ul> |

| フィールド                                                                                    | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| プロアクティブ PAC 更新は後で実行する<br>(Proactive PAC Update Will Occur After)                         | Cisco ISE は、認証に成功した後、設定したパーセンテージのトンネル PAC TTL が残っているときに、新しい PAC をクライアントに予防的に提供します。PAC の有効期限が切れる前に最初の正常な認証が行われると、サーバはトンネル PAC の更新を開始します。このメカニズムにより、有効な PAC でクライアントが更新されます。デフォルト値は 10% です。                                                                                                                                                                                                                                    |
| システムは SGT 番号を割り当てます (System will Assign SGT Numbers)                                     | Cisco ISE ですべての SGT 番号を自動的に生成する場合は、このオプションを選択します。                                                                                                                                                                                                                                                                                                                                                                           |
| この範囲の数値を除く (Except Numbers in Range)                                                     | デバイスに手動で設定するためにある範囲の SGT 番号を予約する場合は、このオプションを選択します。Cisco ISE は、SGT の生成時にこの範囲の数値を使用しません。                                                                                                                                                                                                                                                                                                                                      |
| ユーザは SGT 番号を手動で入力する必要があります (User Must Enter SGT Numbers Manually)                        | SGT 番号を手動で定義するには、このオプションを選択します。                                                                                                                                                                                                                                                                                                                                                                                             |
| APIC EPG のセキュリティグループタグのナンバリング (Security Group Tag Numbering for APIC EPGs)               | このチェックボックスをオンにして、APIC から学習された EPG に基づいて作成される SGT に使用される番号の範囲を指定します。                                                                                                                                                                                                                                                                                                                                                         |
| 許可ルール作成時のセキュリティグループの自動作成 (Auto Create Security Groups When Creating Authorization Rules) | <p>許可ポリシールールの作成時に SGT を自動的に作成するには、このチェックボックスをオンにします。</p> <p>このオプションを選択すると、[許可ポリシー (Authorization Policy)] ウィンドウの上部に、「自動セキュリティ グループの作成がオンです (Auto Security Group Creation is On)」というメッセージが表示されます。</p> <p>自動作成された SGT は、ルール属性に基づいて命名されます。SGT 名と値を編集するには、[権限 (Permissions)] フィールドに表示されているプラス (+) 記号をクリックします。</p> <p>(注) 自動作成された SGT は、それに対応する許可ポリシールールが削除されても削除されません。</p> <p>デフォルトでは、新規インストールまたはアップグレードの後でこのオプションが無効になります。</p> |



| フィールド                                             | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 自動作成のSGT番号範囲 (SGT Number Range For Auto-Creation) | <p>このチェックボックスをオンにして、自動作成される SGT に使用する番号の範囲を指定します。</p> <p>自動作成される SGT に割り当てられた番号の範囲を使い切ると、Cisco ISE は 50 ずつ範囲を拡張し、この変更をユーザに通知します。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| 自動命名オプション (Automatic Naming Options)              | <p>自動作成される SGT の命名規則を定義するには、このオプションを使用します。</p> <p>(必須) [名前に次が含まれます (Name Will Include) ] : 次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"><li>• ルール名</li><li>• SGT 番号 (SGT number)</li><li>• ルール名およびSGT番号 (Rule name and SGT number)</li></ul> <p>デフォルトでは、[ルール名 (Rule name) ] オプションが選択されます。</p> <p>オプションで、SGT 名に以下の情報を追加できます。</p> <ul style="list-style-type: none"><li>• [ポリシー セット名 (Policy Set Name) ]<br/>(このオプションは [ポリシーセット (Policy Sets) ] が有効な場合にのみ使用可能です)</li><li>• [プレフィックス (Prefix) ] (8 文字まで)</li><li>• [サフィックス (Suffix) ] (8 文字まで)</li></ul> <p>Cisco ISE は、選択内容に応じて [サンプル名 (Example Name) ] フィールドにサンプル SGT 名を表示します。</p> <p>同じ名前の SGT がすでに存在する場合、ISE は SGT 名に「_x」を付け加えます。x は 1 から始まる (現在の名前に使用されていない) 最初の値です。新しい名前が 32 文字より長い場合、Cisco ISE によって最初の 32 文字に切り捨てられます。</p> |

## 関連トピック

[TrustSec アーキテクチャ](#) (971 ページ)

[TrustSec のコンポーネント](#) (972 ページ)

[TrustSec のグローバル設定](#) (978 ページ)

## TrustSec マトリックスの設定

次の表に、[TrustSecマトリックスの設定 (TrustSec Matrix Settings)] ページにある各フィールドの説明を示します。このページへのナビゲーションパスは、[ワークセンター (WorkCenters)] > [TrustSec] > [設定 (Settings)] > [TrustSecマトリックスの設定 (TrustSec Matrix Settings)] です。

表 85: TrustSec マトリックスの設定

| フィールド                               | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 複数のSGACLを許可 (Allow Multiple SGACLs) | <p>セル内で複数のSGACLを許可するには、このチェックボックスをオンにします。このオプションが選択されていない場合、Cisco ISE はセル 1 つあたり 1 つの SGACL のみを許可します。</p> <p>デフォルトでは、新たにインストールすると、このオプションはディセーブルになります。</p> <p>アップグレード後、Cisco ISE は出力セルをスキャンし、複数の SGACL が割り当てられたセルを少なくとも 1 つ特定した場合、管理者に複数の SGACL をセルに追加することを許可します。それ以外の場合は、セル 1 つあたり 1 つの SGACL のみを許可します。</p> <p>(注) 複数の SGACL を無効にする前に、複数の SGACL を含むセルを 1 つの SGACL のみを含めるように編集する必要があります。</p> |

| フィールド                          | 使用上のガイドライン                                                                                                                                                                                                                                                                                                  |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| モニタリングの許可 (Allow Monitoring)   | <p>マトリクス内のすべてのセルのモニタリングをイネーブルにする場合は、このチェックボックスをオンにします。モニタリングがディセーブルの場合、[セルの編集 (Edit Cell)] ダイアログで、[すべてをモニタ (Monitor All)] アイコンはグレー表示され、[モニタ (Monitor)] オプションはディセーブルになります。</p> <p>デフォルトでは、新たにインストールすると、モニタリングはディセーブルになります。</p> <p>(注) マトリクス レベルでモニタリングをディセーブルにする前に、現在モニタされているセルのモニタリングをディセーブルにする必要があります。</p> |
| SGT番号の表示 (Show SGT Numbers)    | <p>マトリクス セルの SGT 値 (10 進数および 16 進数の両方) を表示または非表示にするには、このオプションを使用します。</p> <p>デフォルトでは、SGT 値はセルに表示されます。</p>                                                                                                                                                                                                    |
| アピアランス設定 (Appearance Settings) | <p>次のオプションを使用できます。</p> <ul style="list-style-type: none"><li>• [カスタム設定 (Custom settings)] : デフォルトのテーマ (パターンなしの色) が最初に表示されます。独自の色とパターンを設定できます。</li><li>• [デフォルト設定 (Default settings)] : パターンなしの色の定義済みリスト (編集不可)。</li><li>• [アクセシビリティ設定 (Accessibility settings)] : パターンありの色の定義済みリスト (編集不可)。</li></ul>        |

| フィールド                  | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 色/パターン (Color/Pattern) | <p>マトリックスを読み取りやすくするために、セルの内容に基づいて、マトリックスセルに色とパターンを適用できます。</p> <p>使用可能な表示タイプは、次のとおりです。</p> <ul style="list-style-type: none"> <li>• [IPを許可/IPログを許可 (Permit IP/Permit IP Log)] : セル内に設定されます</li> <li>• [IPを拒否/IPログを拒否 (Deny IP/Deny IP Log)] : セル内に設定されます</li> <li>• [SGACL (SGACLs)] : セル内に設定されている SGACL 用</li> <li>• [IPを許可/IPログを許可 (継承) (Permit IP/Permit IP Log (Inherited))] : デフォルト ポリシーから取得されます (設定されていないセル用)</li> <li>• [IPを拒否/IPログを拒否 (継承) (Deny IP/Deny IP Log (Inherited))] : デフォルト ポリシーから取得されます (設定されていないセル用)</li> <li>• [SGACL (継承) (SGACLs (Inherited))] : デフォルト ポリシーから取得されます (設定されていないセル用)</li> </ul> |

#### 関連トピック

[出力ポリシー \(Egress Policy\)](#) (989 ページ)

[マトリックス ビュー](#) (991 ページ)

[TrustSec マトリックスの設定](#) (979 ページ)

## SMS ゲートウェイ設定 (SMS Gateway Settings)

電子メール サーバ経由でゲストとスポンサーに SMS メッセージを送信するように設定するには、次の設定を使用します。

表 86: SMS 電子メール ゲートウェイの SMS ゲートウェイ設定

| フィールド                                                | 使用上のガイドライン                                                                                                                                                                                                                                                                              |
|------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SMS ゲートウェイ プロバイダー ドメイン (SMS Gateway Provider Domain) | プロバイダー ドメインと、ゲストアカウントの携帯電話の番号を入力します。プロバイダーの SMS/MMS ゲートウェイにメッセージを送信するとき、前者が電子メール アドレスのホスト部として使用され、後者はユーザ部分として使用されます。                                                                                                                                                                    |
| プロバイダー アカウント アドレス (Provider account address)         | (オプション)<br>アカウント アドレスを入力します。これは、電子メールの送信元アドレス (通常、アカウント アドレス) として使用され、[ゲスト アクセス (Guest Access)] > [設定 (Settings)] の [デフォルトの電子メールアドレス (Default Email Address)] グローバル設定を上書きします。                                                                                                           |
| SMTP API 宛先アドレス (SMTP API destination address)       | (オプション)<br>Clickatell SMTP API などの、特定のアカウント受信者アドレスを必要とする SMTP SMS API を使用する場合は、SMTP API 宛先アドレスを入力します。<br><br>これは、電子メールの送信先アドレスとして使用され、メッセージ本文のテンプレートはゲストアカウントの携帯電話の番号に置き換えられます。                                                                                                         |
| SMTP API 本文テンプレート (SMTP API body template)           | (オプション)<br>Clickatell SMTP API など、SMS の送信に特定の電子メール本文テンプレートを必要とする SMTP SMS API を使用する場合は、SMTP API 本文テンプレートを入力します。<br><br>サポートされる動的置換は \$mobilenumber\$、(形式 \$YYYYMMDDHHHMISSmimi\$ の) \$timestamp\$、および \$message\$ です。URL に固有識別子が必要な SMS ゲートウェイには \$timestamp\$\$mobilenumber\$ を使用できます。 |

これらの設定へのナビゲーションパスは、[ゲスト アクセス (Guest Access)] > [設定 (Settings)] > [SMS ゲートウェイ (SMS Gateway)] です。

HTTP API (GET 方式または POST 方式) でゲストとスポンサーに SMS メッセージを送信するように設定するには、次の設定を使用します。

表 87: SMS HTTP API 用の SMS ゲートウェイ設定 (SMS Gateway Settings for SMS HTTP API)

| フィールド                                                                                                                          | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                 |
|--------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| URL                                                                                                                            | <p>API の URL を入力します。</p> <p>このフィールドは、符号化された URL ではありません。ゲスト アカウントの携帯電話の番号は、URL に置き換えられます。サポートされる動的置換は \$mobilenumber\$ および \$message\$ です。</p> <p>HTTP API で HTTPS を使用した場合、HTTPS を URL 文字列に含め、Cisco ISE にプロバイダーの信頼できる証明書をアップロードします。[管理 (Administration)] &gt; [システム (System)] &gt; [証明書 (Certificates)] &gt; [信頼できる証明書 (Trusted Certificates)] を選択します。</p> |
| データ (URL エンコード部分) (Data (Url encoded portion))                                                                                 | <p>GET 要求または POST 要求のデータ (URL エンコード部分) を入力します。</p> <p>このフィールドは、符号化された URL です。デフォルトの GET 方式を使用している場合、データが上で指定した URL に付加されます。</p>                                                                                                                                                                                                                            |
| データ部分に HTTP POST 方式を使用 (Use HTTP POST method for data portion)                                                                 | <p>POST 方式を使用する場合は、このオプションをオンにします。</p> <p>上で指定したデータは、POST 要求の内容として使用されます。</p>                                                                                                                                                                                                                                                                              |
| HTTP POST データ コンテンツ タイプ (HTTP POST data content type)                                                                          | <p>POST 方式を使用する場合は、「plain/text」や「application/xml」などのコンテンツタイプを指定します。</p>                                                                                                                                                                                                                                                                                    |
| HTTPS ユーザ名 (HTTPS Username)<br>HTTPS パスワード (HTTPS Password)<br>HTTPS ホスト名 (HTTPS Host name)<br>HTTPS ポート番号 (HTTPS Port number) | <p>この情報を入力します。</p>                                                                                                                                                                                                                                                                                                                                         |

#### 関連トピック

[SMS プロバイダーおよびサービス \(536 ページ\)](#)

[ゲストに SMS 通知を送信するための SMS ゲートウェイの設定 \(537 ページ\)](#)

## DHCP および DNS サービス

これらの設定のためのナビゲーションパスは、**[管理 (Administration)] > [システム (System)] > [設定 (Settings)] > [DHCP および DNS サービス (DHCP & DNS Services)]** です。

認証 VLAN URL リダイレクトのシミュレーションを有効にするために、これらの設定を使用して、DHCP、およびオプションのDNSを設定します。さまざまなISEノードに適用するために、複数のスコープを作成できます。1つのISEノードに複数のスコープを適用する場合、同じネットワーク インターフェイスで設定する必要があります。



- (注) プロファイリングのために、DHCP プローブを必要とすることがあります。ISE DHCP プローブは認証 VLAN DHCP サービスと同じUDPポート67を使用します。そのため、DHCP プローブは、異なるインターフェイスで設定される必要があるか、またはこのISEノードで無効にすることができます。DHCP プローブの詳細については、[DHCP プローブ \(774 ページ\)](#) を参照してください。

表 88: 認証 VLAN URL リダイレクトのシミュレーション用の DHCP と DNS サービスの設定

| フィールド              | 使用上のガイドライン                                                                                                                                                           |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| スコープ名              | このスコープの目的を容易に記憶できる名前を入力します。                                                                                                                                          |
| ステータス              | [有効 (Enabled)] または [無効 (Disabled)] を選択します。有効の場合、スコープは ISE ノードにのみ使用できます。                                                                                              |
| ISE ノード (ISE Node) | DHCP/DNS サーバとして機能するように ISE ノードを適用します。ドロップダウン リストから、このスコープを使用する ISE ノードを選択します。認証 VLAN は ISE ノード/ネットワーク インターフェイスごとに設定され、2 つのインターフェイスまたは 2 つのノードが同じ VLAN を共有することはできません。 |

| フィールド                               | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                       |
|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ネットワーク インターフェイス (Network Interface) | 選択した ISE ノードで利用可能なネットワーク インターフェイスは、選択した ISE ノードに基づいて動的にこのドロップダウン リストに表示されます。認証 VLAN は ISE ノード/ネットワーク インターフェイスごとに設定され、2つのインターフェイスまたは2つのノードが同じVLANを共有することはできません。DHCP/DNS サーバがリスニングするインターフェイスを選択します。NAD の VLAN IP ヘルパーを設定することによって、複数のVLANが1つのネットワーク インターフェイス カードに接続される可能性があります。IPヘルパーの設定の詳細については、デバイス用のアドミニストレーション ガイドの指示を参照してください。 |
| ドメイン名 (Domain Name)                 | このスコープで使用する DHCP サーバのドメイン名を入力します。                                                                                                                                                                                                                                                                                                |
| DHCP アドレス範囲                         | ネットワーク定義に基づいて、このスコープに使用可能な DHCP アドレスの範囲を選択します。                                                                                                                                                                                                                                                                                   |
| サブネット マスク (Subnet mask)             | ネットワーク定義に基づいて、このスコープに使用するネットワークマスクを選択します。                                                                                                                                                                                                                                                                                        |
| ネットワーク ID (Network ID)              | 入力した DHCP の属性に基づいて、Cisco ISE により自動的に決定されます。                                                                                                                                                                                                                                                                                      |
| 除外アドレス範囲                            | ネットワーク定義に基づいて、このスコープに使用すべきでない DHCP アドレスの範囲を選択します。                                                                                                                                                                                                                                                                                |
| デフォルト ゲートウェイ                        | デフォルト ゲートウェイの IP アドレスを入力します。                                                                                                                                                                                                                                                                                                     |
| DHCP リース期間                          | DHCP リース期間を定義します。                                                                                                                                                                                                                                                                                                                |



| フィールド                        | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [DHCP オプション (DHCP options) ] | <p>これはオプションのフィールドです。</p> <p>DHCP オプションは、DHCP サーバが DHCP クライアントに渡すことができる追加の設定パラメータです。DHCP オプションにより、ネットワークにアクセスするため、または最終認証前にデバイスをブートストラップする手段として、オプション値に指定されている情報を必要とするデバイス（カメラ、アクセス ポイント、電話）がサポートされます。DHCP サーバは、DHCP 要求メッセージをクライアントから受信すると、(通常) DHCP ACK パケットをクライアントに送信することで応答します。この時点で、サーバは DHCP ACK パケットで設定されているすべてのオプションを転送します。</p> <p>詳細については、次の表の後に続く「DHCP オプション」の項を参照してください。</p> |
| 外部 DNS サーバ                   | すべての企業ネットワークにアクセスするための認証を受ける前に、ユーザが認証 VLAN 外の外部ドメインにアクセスできるようにする場合、外部 DNS 名を解決するために DNS サーバの IP アドレスを入力します。                                                                                                                                                                                                                                                                           |
| 外部ドメイン                       | すべての企業ネットワークにアクセスするための認証を受ける前に、ユーザが特定のサイトにアクセスできるようにする場合、これらのフィールドにそれらのサイトのドメイン名を入力します。                                                                                                                                                                                                                                                                                               |

## DHCP オプション

ISE で DHCP サービスを設定すると、Auth VLAN に接続するクライアントに特定の DHCP オプションを割り当てることができます。定義する各範囲に複数の DHCP オプションを追加できます。

ドロップダウン リストで選択できるオプションは、RFC 2132 のものです。また、(RFC 2132 から) カスタマイズしたオプションを追加するには、ドロップダウン リストから [カスタム (Custom) ] を選択し、オプション コードを入力します。

一般に、最もよく使用される DHCP オプションがいくつかあります。

一般的なオプションとしては、次のようなものがあります。

- オプション 12（ホスト名）：ノードの完全修飾ドメイン名の「ホスト名」部分を渡すために使用されます。たとえば mail.ise.com の「mail」です。
- オプション 42（NTP サーバ）：ネットワークで使用される NTP サーバを渡します。
- オプション 66（TFTP サーバ）：IP アドレスまたはホスト名を渡すために使用されます。このオプションは、ドロップダウンリストから選択できます。
- オプション 82（DHCP リレー エージェント）：サーバ側 DHCP リレー サーバ情報のその他のサブオプションを渡すために使用されます。

オプション値を定義するには、ドロップダウンリストからオプションを選択します。事前定義のオプションを選択すると、コードとタイプが自動的に取り込まれます。

[カスタム (Custom)] を選択してコードを入力すると、[タイプ (Type)] が自動的に更新されます。オプションの値を入力します。

図 66: DHCP オプション

The screenshot shows the DHCP configuration page. A red box highlights the 'Domain name' field set to 'Guest' and the 'DHCP options' table. The table has columns: Option, Actions, Code, Type, and Value.

| Option       | Actions          | Code | Type   | Value    |
|--------------|------------------|------|--------|----------|
| DHCP options | Custom           | 12   | Text   | mail     |
|              | Class Identifier | 60   | String | pxelinux |

次に例を示します。

- ホスト名の設定：[オプション (Option)] から [カスタム (Custom)] を選択します。[コード (Code)] に 12 と入力します。[タイプ (Type)] が自動的に [テキスト (Text)] に更新されます。[値 (Value)] にホスト名 (mail.ise.com の「mail」など) を入力します。
- TFTP サーバ名の設定：[オプション (Option)] から [TFTP サーバ名 (TFTP Server Name)] を選択します。[コード (Code)] と [タイプ (Type)] がそれぞれ自動的に更新されます。[値 (Value)] に TFTP サーバのホスト名を入力します。



(注) 一部の DHCP オプションは、ISE に対して自動的に定義されているため、手動で入力できません。たとえばオプション 15 (ドメイン名) はカスタム オプションとして定義できません。これは、DHCP ドメイン名は、この画面で必須フィールドとして定義されており、上書きできないためです。

複数のオプションを入力するには、[アクション (Actions)] の下のプラス記号をクリックします。

#### 関連トピック

[Cisco ISE でのサードパーティ ネットワーク デバイスのサポート](#) (251 ページ)

[Cisco ISE でのサードパーティ製ネットワーク デバイスの設定](#) (256 ページ)

[DHCP プローブ](#) (774 ページ)

## ID の管理

これらのページは、Cisco ISE の ID を設定し、管理することができます。

## エンドポイント

これらのページでは、ネットワークに接続するエンドポイントを設定および管理することができます。

### エンドポイント設定

次の表に、エンドポイントを作成し、エンドポイントにポリシーを割り当てるために使用できる [エンドポイント (Endpoints)] ページのフィールドを示します。このページへのナビゲーションパスは、[ワーク センター (Work Centers)] > [ネットワーク アクセス (Network Access)] > [ID (Identities)] > [エンドポイント (Endpoints)] です。

表 89: エンドポイント設定

| フィールド                  | 使用上のガイドライン                                                                                                      |
|------------------------|-----------------------------------------------------------------------------------------------------------------|
| MAC アドレス (MAC Address) | <p>エンドポイントを静的に作成するには、MAC アドレスを 16 進数形式で入力します。</p> <p>MAC アドレスは、Cisco ISE 対応のネットワークに接続するインターフェイスのデバイス ID です。</p> |

| フィールド                          | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| スタティック割り当て (Static Assignment) | <p>[エンドポイント (Endpoints) ] ページでエンドポイントを静的に作成する場合このチェックボックスをオンにすると、静的割り当てのステータスが <b>static</b> に設定されます。</p> <p>エンドポイントのスタティック割り当てのステータスを静的から動的に、または動的から静的に切り替えできます。</p>                                                                                                                                                                                                                                                                               |
| ポリシー割り当て                       | <p>(スタティック割り当てが選択されていない限り、デフォルトで無効) [ポリシー割り当て (Policy Assignment) ] ドロップダウンリストから一致するエンドポイント ポリシーを選択します。</p> <p>次のいずれかを実行できます。</p> <ul style="list-style-type: none"><li>• 一致するエンドポイント ポリシーを選択しないで、デフォルトのエンドポイントポリシーである不明を使用する場合、スタティック割り当てステータスはエンドポイントに対して動的に設定され、それにより、エンドポイントの動的プロファイリングが可能になります。</li><li>• 不明ではなく、一致するエンドポイントポリシーを選択する場合、スタティック割り当てステータスはそのエンドポイントに対して静的に設定され、[スタティック割り当て (Static Assignment) ] チェックボックスが自動的にオンにされます。</li></ul> |

| フィールド                                     | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| スタティック グループ割り当て (Static Group Assignment) | <p>([スタティック グループ割り当て (Static Group Assignment) ]が選択されていない限り、デフォルトで無効) エンドポイントを ID グループに静的に割り当てる場合、このチェックボックスをオンにします。</p> <p>このチェックボックスをオンにした場合、プロファイリングサービスは、前に他のエンドポイント ID グループに動的に割り当てられたエンドポイントの次のエンドポイントポリシーの評価時に、そのエンドポイント ID グループを変更しません。</p> <p>このチェックボックスをオフにした場合、エンドポイント ID グループは、ポリシー設定に基づいて ISE プロファイラにより割り当てられたダイナミック グループです。[スタティック グループ割り当て (Static Group Assignment) ] オプションを選択しない場合、エンドポイントは、エンドポイント ポリシーの次回評価時に一致する ID グループに自動的に割り当てられます。</p> |

| フィールド       | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ID グループ割り当て | <p>エンドポイントを割り当てるエンドポイント ID グループを選択します。</p> <p>エンドポイントを静的に作成する場合、またはエンドポイントのエンドポイント ポリシーの評価時に [一致する ID グループの作成 (Create Matching Identity Group) ] オプションを使用しない場合は、エンドポイント ID グループに割り当てることができます。</p> <p>Cisco ISE には、次のシステムによって作成された次のエンドポイント ID グループがあります。</p> <ul style="list-style-type: none"> <li>• ブラックリスト</li> <li>• GuestEndpoints</li> <li>• プロファイル済み <ul style="list-style-type: none"> <li>• Cisco IP-Phone</li> <li>• ワークステーション</li> </ul> </li> <li>• RegisteredDevices</li> <li>• 不明</li> </ul> |

#### 関連トピック

[識別されたエンドポイント](#) (813 ページ)

[ポリシーおよび ID グループのスタティック割り当てによるエンドポイントの作成](#) (807 ページ)

## エンドポイントの、LDAP からのインポートの設定

次の表では、LDAP サーバからのエンドポイントのインポートに使用できる [LDAP からのインポート (Import from LDAP) ] ページのフィールドについて説明します。このページへのナビゲーションパスは、[ワークセンター (Work Centers) ] > [ネットワーク アクセス (Network Access) ] > [ID (Identities) ] > [エンドポイント (Endpoints) ] です。

表 90: エンドポイントの、LDAP からのインポートの設定

| フィールド | 使用上のガイドライン                      |
|-------|---------------------------------|
| 接続の設定 |                                 |
| ホスト   | LDAP サーバのホスト名または IP アドレスを入力します。 |

| フィールド                                   | 使用上のガイドライン                                                                                                                                                                                        |
|-----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [ポート (Port) ]                           | <p>LDAP サーバのポート番号を入力します。デフォルトポート 389 を使用して LDAP サーバからインポートするか、デフォルトポート 636 を使用して SSL を介して LDAP サーバからインポートできます。</p> <p>(注) Cisco ISE では、任意の設定済みポート番号をサポートします。設定済みの値は、LDAP サーバ接続詳細に一致する必要があります。</p> |
| セキュア接続を有効にする (Enable Secure Connection) | SSL を介して LDAP サーバからインポートするには、[セキュア接続を有効にする (Enable Secure Connection) ] チェックボックスをオンにします。                                                                                                          |
| ルート CA 証明書名                             | <p>ドロップダウン矢印をクリックして、信頼できる CA 証明書を表示します。</p> <p>ルート CA 証明書名は、LDAP サーバに接続する場合に必要な信頼できる CA 証明書を指します。Cisco ISE 内の CA 証明書は、追加 (インポート)、編集、削除、およびエクスポートが可能です。</p>                                        |
| 匿名バインド (Anonymous Bind)                 | <p>匿名バインドを有効にするには、[匿名バインド (Anonymous Bind) ] チェックボックスをオンにします。</p> <p>[匿名バインド (Anonymous Bind) ] チェックボックスをオンにするか、または slapd.conf コンフィギュレーションファイルの LDAP 管理者クレデンシャルを入力する必要があります。</p>                  |
| 管理者 DN (Admin DN)                       | <p>slapd.conf コンフィギュレーションファイルで LDAP 管理者に設定されている識別名 (DN) を入力します。</p> <p>管理者 DN フォーマット例 : cn=Admin, dc=cisco.com, dc=com</p>                                                                        |
| [パスワード (Password) ]                     | LDAP 管理者に設定されたパスワードを slapd.conf コンフィギュレーションファイルに入力します。                                                                                                                                            |

| フィールド                                          | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ベース DN (Base DN)                               | 親エントリの認定者名を入力します。<br><br>ベース DN フォーマット例: dc=cisco.com, dc=com                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| クエリ設定 (Query Settings)                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| MAC アドレス objectClass (MAC Address objectClass) | MAC アドレスのインポートに使用するクエリフィルタを入力します。たとえば、ieee802Device です。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| MAC アドレス属性名 (MAC Address Attribute Name)       | インポートに対して返される属性名を入力します。たとえば、macAddress です。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| プロファイル属性名 (Profile Attribute Name)             | LDAP 属性の名前を入力します。この属性は、LDAP サーバで定義されている各エンドポイント エントリのポリシー名を保持します。<br><br>[プロファイル属性名 (Profile Attribute Name)] フィールドを設定する場合は、次の点を考慮してください。<br><br><ul style="list-style-type: none"> <li>• [プロファイル属性名 (Profile Attribute Name)] フィールドでこの LDAP 属性を指定しない場合、またはこの属性を誤って設定した場合、インポート操作時にエンドポイントは「不明」としてマークされ、これらのエンドポイントは一致するエンドポイントプロファイリング ポリシーに個別にプロファイリングされます。</li> <li>• [プロファイル属性名 (Profile Attribute Name)] フィールドで LDAP 属性を設定した場合、その属性値は、エンドポイント ポリシーが Cisco ISE 内の既存のポリシーに一致することを確認するために検証され、エンドポイントがインポートされます。エンドポイント ポリシーが既存のポリシーと一致しない場合、それらのエンドポイントはインポートされません。</li> </ul> |
| タイムアウト (秒) (Time Out [seconds])                | 時間を秒単位 (1 ~ 60 秒) で入力します。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

#### 関連トピック

[識別されたエンドポイント \(813 ページ\)](#)

[LDAP サーバからのエンドポイントのインポート \(812 ページ\)](#)



## グループ (Groups)

これらのページでは、エンドポイント ID グループを設定および管理することができます。

### エンドポイント ID グループの設定

次の表に、エンドポイント グループを作成するために使用できる [エンドポイント ID グループ (Endpoint Identity Groups)] ページのフィールドを示します。このページへのナビゲーションパスは、[管理 (Administration)] > [ID の管理 (Identity Management)] > [グループ (Groups)] > [エンドポイント ID グループ (Endpoint Identity Groups)] です。

表 91: エンドポイント ID グループの設定

| フィールド                | 使用上のガイドライン                                                                             |
|----------------------|----------------------------------------------------------------------------------------|
| [名前 (Name)]          | 作成するエンドポイント ID グループの名前を入力します。                                                          |
| 説明                   | 作成するエンドポイント ID グループの説明を入力します。                                                          |
| 親グループ (Parent Group) | 新しく作成したエンドポイント ID グループを関連付けるエンドポイント ID グループを、[親グループ (Parent Group)] ドロップダウンリストから選択します。 |

#### 関連トピック

[識別されたエンドポイントの、エンドポイント ID グループでのグループ化](#) (816 ページ)  
[エンドポイント ID グループの作成](#) (815 ページ)

## 外部 ID ソース

これらのページでは、Cisco ISE が認証および認可に使用するユーザ データが含まれる外部 ID ソースを設定および管理することができます。

### LDAP ID ソースの設定

次の表では、[LDAP ID ソース (LDAP Identity Sources)] ページのフィールドについて説明します。これらのフィールドを使用して LDAP インスタンスを作成し、これに接続します。このページへのナビゲーションパスは、[管理 (Administration)] > [ID の管理 (Identity Management)] > [外部 ID ソース (External Identity Sources)] > [LDAP] です。

#### LDAP 一般設定

以下の表では、[一般 (General)] タブのフィールドについて説明します。

表 92: LDAP 一般設定

| フィールド                                   | 使用上のガイドライン                                                                                                                                                                                                                                                                                             |
|-----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [名前 (Name) ]                            | LDAP インスタンスの名前を入力します。この値は、サブジェクト DN および属性を取得するために検索で使用されます。この値は string 型で、最大長は 64 文字です。                                                                                                                                                                                                                |
| 説明                                      | LDAP インスタンスの説明を入力します。この値は string 型で、最大長は 1024 文字です。                                                                                                                                                                                                                                                    |
| スキーマ (Schema)                           | <p>次の組み込みのスキーマ タイプのいずれかを選択するか、カスタム スキーマを作成できます。</p> <ul style="list-style-type: none"> <li>• Active Directory</li> <li>• Sun Directory Server</li> <li>• Novell eDirectory</li> </ul> <p>[スキーマ (Schema) ]の隣の矢印をクリックすると、スキーマの詳細を表示できます。</p> <p>事前定義されたスキーマの属性を編集すると、Cisco ISE が自動的にカスタム スキーマを作成します。</p> |
| (注) 次のフィールドは、カスタム スキーマを選択した場合にのみ編集できます。 |                                                                                                                                                                                                                                                                                                        |
| サブジェクト オブジェクト クラス (Subject Objectclass) | サブジェクト DN および属性を取得するために検索で使用する値を入力します。この値は string 型で、最大長は 256 文字です。                                                                                                                                                                                                                                    |
| サブジェクト名属性 (Subject Name Attribute)      | 要求内のユーザ名を含む属性の名前を入力します。この値は string 型で、最大長は 256 文字です。                                                                                                                                                                                                                                                   |
| グループ名属性 (Group Name Attribute)          | <p>[グループ名属性 (Group Name Attribute) ] フィールドに CN または DN またはサポートされる属性を入力します。</p> <ul style="list-style-type: none"> <li>• CN : 共通名に基づいて LDAP ID ストア グループを取得します。</li> <li>• DN : 識別名に基づいて LDAP ID ストア グループを取得します。</li> </ul>                                                                               |

| フィールド                                                                         | 使用上のガイドライン                                                                                                                                      |
|-------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| 証明書属性 (Certificate Attribute)                                                 | 証明書定義を含む属性を入力します。証明書ベースの認証の場合、クライアントによって提示された証明書を検証するために、これらの定義が使用されます。                                                                         |
| グループ オブジェクト クラス (Group Objectclass)                                           | グループとして認識されるオブジェクトを指定するために、検索に使用する値を入力します。この値は string 型で、最大長は 256 文字です。                                                                         |
| グループ マップ属性 (Group Map Attribute)                                              | マッピング情報を含む属性を指定します。この属性は、選択した参照方向に基づいて、ユーザまたはグループ属性を指定できます。                                                                                     |
| サブジェクト オブジェクトにグループへの参照が含まれる (Subject Objects Contain Reference To Groups)     | 所属するグループを指定する属性がサブジェクト オブジェクトに含まれている場合は、このオプション ボタンをクリックします。                                                                                    |
| グループ オブジェクトにサブジェクトへの参照が含まれる (Group Objects Contain Reference To Subjects)     | サブジェクトを指定する属性がグループ オブジェクトに含まれている場合は、このオプション ボタンをクリックします。この値はデフォルト値です。                                                                           |
| グループ内のサブジェクトをメンバー属性に保存 (Subjects In Groups Are Stored In Member Attribute As) | ([グループ オブジェクトにサブジェクトへの参照が含まれる (Group Objects Contain Reference To Subjects) ] オプション ボタンの選択時に限り使用可能) グループ メンバー属性にメンバーが供給される方法を指定します (デフォルトは DN)。 |

| フィールド                          | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ユーザ情報属性 (User Info Attributes) | <p>デフォルトでは、事前設定された属性が次の組み込みのスキーマタイプのユーザ情報（名、姓、電子メール、電話、地域など）を収集するために使用されます。</p> <ul style="list-style-type: none"> <li>• Active Directory</li> <li>• Sun Directory Server</li> <li>• Novell eDirectory</li> </ul> <p>事前定義されたスキーマの属性を編集すると、Cisco ISE が自動的にカスタム スキーマを作成します。</p> <p>[スキーマ (Schema)] ドロップダウン リストから [カスタム (Custom)] オプションを選択し、要件に基づいてユーザ情報の属性を編集することもできます。</p> |

## LDAP の接続設定

以下の表では、[接続設定 (Connection Settings)] タブのフィールドについて説明します。

表 93: LDAP の接続設定

| フィールド                                               | 使用上のガイドライン                                                                                                                                               |
|-----------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| セカンダリ サーバの有効化 (Enable Secondary Server)             | プライマリ LDAP サーバに障害が発生した場合にバックアップとして使用するセカンダリ LDAP サーバを有効にする場合は、このオプションをオンにします。このチェックボックスをオンにする場合は、セカンダリ LDAP サーバの設定パラメータを入力する必要があります。                     |
| プライマリ サーバとセカンダリ サーバ (Primary and Secondary Servers) |                                                                                                                                                          |
| ホスト名/IP (Hostname/IP)                               | LDAP ソフトウェアを実行しているマシンの IP アドレスまたは DNS 名を入力します。ホスト名は 1 ～ 256 文字か、または文字列として表される有効な IP アドレスです。ホスト名の有効な文字は、英数字 (a ～ z、A ～ Z、0 ～ 9)、ドット (.)、およびハイフン (-) だけです。 |

| フィールド                                               | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [ポート (Port) ]                                       | LDAP サーバがリスンしている TCP/IP ポート番号を入力します。有効な値は 1 ～ 65,535 です。デフォルトは、LDAP 仕様の記述に従って 389 です。ポート番号が不明な場合は、LDAP サーバの管理者からポート番号を取得できます。                                                                                                                                                                                                                                               |
| 各 ISE ノードのサーバの指定 (Specify server for each ISE node) | プライマリおよびセカンダリ LDAP サーバの hostnames/IP および各 PSN のポートを設定するには、このチェック ボックスをオンにします。<br><br>このオプションを有効にすると、導入のすべてのノードを表示するテーブルが表示されます。ノードを選択し、プライマリおよびセカンダリ LDAP サーバの hostname/IP および選択したノードのポートを設定する必要があります。                                                                                                                                                                      |
| アクセス (Access)                                       | [匿名アクセス (Anonymous Access) ] : LDAP ディレクトリの検索が匿名で行われるようにする場合にクリックします。サーバではクライアントが区別されず、認証されていないクライアントに対してアクセス可能に設定されているデータへの、クライアント読み取りアクセスが許可されます。認証情報をサーバに送信することを許可する特定のポリシーがない場合、クライアントは匿名接続を使用する必要があります。<br><br>[認証されたアクセス (Authenticated Access) ] : LDAP ディレクトリの検索が管理クレデンシャルによって行われるようにする場合にクリックします。その場合、[管理者 DN (Admin DN) ] および [パスワード (Password) ] フィールドの情報を入力します。 |

| フィールド                                       | 使用上のガイドライン                                                                                                                                                                                      |
|---------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 管理者 DN (Admin DN)                           | 管理者の DN を入力します。管理者 DN は、[ユーザ ディレクトリ サブツリー (User Directory Subtree)] 下のすべての必要なユーザの検索およびグループの検索を行う権限を持つ LDAP アカウントです。指定した管理者に対して、検索でのグループ名属性の表示が許可されていない場合、該当 LDAP サーバで認証されたユーザのグループ マッピングは失敗します。 |
| [パスワード (Password)]                          | LDAP 管理者アカウントのパスワードを入力します。                                                                                                                                                                      |
| セキュアな認証 (Secure Authentication)             | SSL を使用して Cisco ISE とプライマリ LDAP サーバ間の通信を暗号化する場合にクリックします。[ポート (Port)] フィールドに LDAP サーバでの SSL に使用されるポート番号が入力されていることを確認します。このオプションを有効にした場合は、ルート CA を選択する必要があります。                                    |
| LDAP サーバのルート CA (LDAP Server Root CA)       | ドロップダウンリストボックスから信頼できるルート認証局を選択して、証明書による安全な認証を有効にします。                                                                                                                                            |
| サーバ タイムアウト (Server timeout)                 | プライマリ LDAP サーバでの接続または認証が失敗したと判断する前に Cisco ISE がプライマリ LDAP サーバからの応答を待つ秒数を入力します。有効な値は 1 ～ 99 です。デフォルトは 10 です。                                                                                     |
| 最大管理接続 (Max. Admin Connections)             | 特定の LDAP 設定に対して実行できる LDAP 管理者アカウント権限での同時接続の最大数 (0 より大きい数) を入力します。これらの接続は、ユーザディレクトリ サブツリーおよびグループディレクトリ サブツリーの下にあるユーザおよびグループのディレクトリの検索に使用されます。有効な値は 1 ～ 99 です。デフォルトは 20 です。                       |
| N 秒ごとに再接続 (Force reconnect every N seconds) | このチェック ボックスをオンにし、2 つ目のテキスト ボックスに、サーバを指定された間隔で LDAP 接続を更新するための適切な値を入力します。有効な範囲は 1 ～ 60 分です。                                                                                                      |

| フィールド                                                      | 使用上のガイドライン                                                                                                                                                |
|------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| サーバへのバインドをテスト (Test Bind To Server)                        | LDAP サーバの詳細およびクレデンシャルが正常にバインドできることをテストおよび確認する場合にクリックします。テストが失敗した場合は、LDAP サーバの詳細を編集して再テストします。                                                              |
| フェールオーバー                                                   |                                                                                                                                                           |
| 常にプライマリ サーバに最初にアクセスする (Always Access Primary Server First) | Cisco ISE の認証と認可のために常にプライマリ LDAP サーバに最初にアクセスするように設定するには、このオプションをクリックします。                                                                                  |
| 経過後にプライマリ サーバにフェールバック (Failback to Primary Server After)   | Cisco ISE で接続しようとしたプライマリ LDAP サーバが到達不可能な場合、Cisco ISE はセカンダリ LDAP サーバへの接続を試行します。Cisco ISE に再びプライマリ LDAP サーバを使用するように設定するには、このオプションをクリックし、テキスト ボックスに値を入力します。 |

### [LDAP] の [ディレクトリ構成 (Directory Organization)] タブ

次の表では、[ディレクトリ構成 (Directory Organization)] タブのフィールドについて説明します。

表 94: [LDAP] の [ディレクトリ構成 (Directory Organization)] タブ

| フィールド                             | 使用上のガイドライン                                                                                                                                                                                                                                   |
|-----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| サブジェクト検索ベース (Subject Search Base) | <p>すべてのサブジェクトを含むサブツリーの DN を入力します。次に例を示します。</p> <p>o=corporation.com</p> <p>サブジェクトを含むツリーがベース DN である場合は、LDAP 設定に応じて</p> <p>o=corporation.com</p> <p>または</p> <p>dc=corporation,dc=com</p> <p>と入力します。詳細については、LDAP データベースに関するドキュメントを参照してください。</p> |

| フィールド                                               | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| グループ検索ベース (Group Search Base)                       | <p>すべてのグループを含むサブツリーの DN を入力します。次に例を示します。</p> <p>ou = 組織ユニット、ou = 次の組織ユニット、o = corporation.com</p> <p>グループを含むツリーがベース DN である場合は、LDAP 設定に応じて</p> <p>o=corporation.com</p> <p>または</p> <p>dc=corporation,dc=com</p> <p>と入力します。詳細については、LDAP データベースに関するドキュメントを参照してください。</p>                                                                                                                                                                                                                                                  |
| 形式での MAC アドレスの検索 (Search for MAC Address in Format) | <p>LDAP データベースでの検索に使用する、Cisco ISE の MAC アドレス形式を入力します。内部 ID ソースの MAC アドレスは、xx-xx-xx-xx-xx-xx の形式で供給されます。LDAP データベースの MAC アドレスは、異なる形式で供給できます。ただし、Cisco ISE でホスト ルックアップ要求が受信されると、MAC アドレスは内部形式からこのフィールドで指定した形式に変換されます。</p> <p>ドロップダウン リストを使用して、特定の形式での MAC アドレスの検索を有効にします。&lt;format&gt; は次のいずれかです。</p> <ul style="list-style-type: none"> <li>• XXXX.XXXX.XXXX</li> <li>• XXXXXXXXXXXXX</li> <li>• XX-XX-XX-XX-XX-XX</li> <li>• XX:XX:XX:XX:XX:XX</li> </ul> <p>選択する形式は、LDAP サーバに供給されている MAC アドレスの形式と一致している必要があります。</p> |



| フィールド                                                                                                 | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| サブジェクト名の先頭から最後に出現する区切り文字まで削除 (Strip start of subject name up to the last occurrence of the separator) | <p>ユーザ名からドメインプレフィックスを削除するための適切なテキストを入力します。</p> <p>ユーザ名の中で、このフィールドに指定した区切り文字が Cisco ISE で検出されると、そのユーザ名の初めから区切り文字までのすべての文字が削除されます。ユーザ名に、<code>&lt;start_string&gt;</code> ボックスに指定した文字が複数含まれている場合は、Cisco ISE によって最後の区切り文字までの文字が削除されます。たとえば、区切り文字がバックスラッシュ (\) で、ユーザ名が DOMAIN\user1 である場合、Cisco ISE によって user1 が LDAP サーバに送信されます。</p> <p>(注) <code>&lt;start_string&gt;</code> ボックスには、特殊文字であるシャープ記号 (#)、疑問符 (?)、引用符 (")、アスタリスク (*)、右山カッコ (&gt;)、および左山カッコ (&lt;) を入力できません。Cisco ISE では、ユーザ名にこれらの文字を使用できません。</p> |
| 最初に出現する区切り文字からサブジェクト名の末尾まで削除 (Strip end of subject name from the first occurrence of the separator)   | <p>ユーザ名からドメインサフィックスを削除するための適切なテキストを入力します。</p> <p>ユーザ名の中で、このフィールドに指定した区切り文字が Cisco ISE で検出されると、その区切り文字からユーザ名の末尾までのすべての文字が削除されます。ユーザ名に、このフィールドに指定した文字が複数含まれている場合は、Cisco ISE によって最初の区切り文字から文字が削除されます。たとえば、区切り文字が @ で、ユーザ名が user1@domain であれば、Cisco ISE は user1 を LDAP サーバに送信します。</p> <p>(注) <code>&lt;end_string&gt;</code> ボックスには、特殊文字であるシャープ記号 (#)、疑問符 (?)、引用符 (")、アスタリスク (*)、右山カッコ (&gt;)、および左山カッコ (&lt;) を入力できません。Cisco ISE では、ユーザ名にこれらの文字を使用できません。</p>                                                   |

## LDAP グループ設定

表 95: LDAP グループ設定

| フィールド    | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                             |
|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 追加 (Add) | <p>[追加 (Add)] &gt; [グループの追加 (Add Group)] を選択して新しいグループを追加するか、[追加 (Add)] &gt; [ディレクトリからグループを選択 (Select Groups From Directory)] を選択して LDAP ディレクトリからグループを選択します。</p> <p>グループの追加を選択した場合は、新しいグループの名前を入力します。ディレクトリから選択する場合は、フィルタ基準を入力し、[グループの取得 (Retrieve Groups)] をクリックします。選択するグループの隣にあるチェックボックスをオンにし、[OK] をクリックします。選択したグループが [グループ (Groups)] ページに表示されます。</p> |

## LDAP 属性設定

表 96: LDAP 属性設定

| フィールド    | 使用上のガイドライン                                                                                                                                                                                                                                                                                                       |
|----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 追加 (Add) | <p>[追加 (Add)] &gt; [属性の追加 (Add Attribute)] を選択して新しい属性を追加するか、[追加 (Add)] &gt; [ディレクトリから属性を選択 (Select Attributes From Directory)] を選択して LDAP サーバから属性を選択します。</p> <p>属性を追加する場合は、新しい属性の名前を入力します。ディレクトリから選択する場合は、ユーザ名を入力し、[属性の取得 (Retrieve Attributes)] をクリックしてユーザの属性を取得します。選択する属性の隣にあるチェックボックスをオンにし、[OK] をクリックします。</p> |

## LDAP 詳細設定

以下の表では、[詳細設定 (Advanced Settings)] タブのフィールドについて説明します。

表 97: LDAP 詳細設定

| フィールド                                      | 使用上のガイドライン                                                                                                                                                                                                                 |
|--------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [パスワードの変更を有効にする (Enable password change) ] | デバイス管理に PAP プロトコルを使用し、ネットワーク アクセスに RADIUS EAP-GTC プロトコルを使用している場合に、パスワードが期限切れになるか、またはパスワードがリセットされるときに、ユーザがパスワードを変更できるようにするには、このチェックボックスをオンにします。サポートされていないプロトコルでは、ユーザ認証が失敗します。このオプションでは、ユーザが次のログイン時にパスワードを変更できるようにすることもできます。 |

## 関連トピック

[LDAP ディレクトリ サービス \(482 ページ\)](#)

[LDAP ユーザ認証 \(483 ページ\)](#)

[LDAP ユーザ ルックアップ \(487 ページ\)](#)

[LDAP ID ソースの追加 \(487 ページ\)](#)

## RADIUS トークン ID ソースの設定

次の表では、RADIUS 外部 ID ソースを設定し、それに接続するために使用できる [RADIUS トークン ID ソース (RADIUS Token Identity Sources) ] ページのフィールドについて説明します。このページへのナビゲーションパスは、[管理 (Administration) ]> [ID の管理 (Identity Management) ]> [外部 ID ソース (External Identity Sources) ]> [RADIUS トークン (RADIUS Token) ] です。

表 98: RADIUS トークン ID ソースの設定

| フィールド                          | 使用上のガイドライン                                          |
|--------------------------------|-----------------------------------------------------|
| [名前 (Name) ]                   | RADIUS トークンサーバの名前を入力します。許容最大文字数は 64 文字です。           |
| 説明                             | RADIUS トークンサーバの説明を入力します。最大文字数は 1024 です。             |
| SafeWord サーバ (SafeWord Server) | RADIUS ID ソースが SafeWord サーバである場合はこのチェックボックスをオンにします。 |

| フィールド                                                      | 使用上のガイドライン                                                                                                                                      |
|------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| セカンダリ サーバの有効化 (Enable Secondary Server)                    | プライマリに障害が発生した場合にバックアップとして使用する Cisco ISE のセカンダリ RADIUS トークン サーバを有効にするには、このチェックボックスをオンにします。このチェックボックスをオンにする場合は、セカンダリ RADIUS トークン サーバを設定する必要があります。 |
| 常にプライマリ サーバに最初にアクセスする (Always Access Primary Server First) | Cisco ISE が常にプライマリ サーバに最初にアクセスするには、このオプション ボタンをクリックします。                                                                                         |
| 経過後にプライマリ サーバにフォールバック (Fallback to Primary Server after)   | プライマリ サーバに到達できない場合に Cisco ISE がセカンダリ RADIUS トークン サーバを使用して認証できる時間 (分単位) を指定するには、このオプション ボタンをクリックします。この時間を過ぎると、Cisco ISE はプライマリ サーバに対する認証を再試行します。 |
| <b>プライマリ サーバ (Primary Server)</b>                          |                                                                                                                                                 |
| ホスト名/アドレス (Host IP)                                        | プライマリ RADIUS トークン サーバの IP アドレスを入力します。このフィールドには、文字列として表される有効な IP アドレスを入力できます。このフィールドで使用する文字は、数字とドット (.) です。                                      |
| 共有秘密鍵 (Shared Secret)                                      | この接続のプライマリ RADIUS トークン サーバで設定されている共有秘密を入力します。                                                                                                   |
| 認証ポート (Authentication Port)                                | プライマリ RADIUS トークン サーバが受信しているポート番号を入力します。有効な値は 1 ～ 65,535 です。デフォルトは 1812 です。                                                                     |
| サーバ タイムアウト (Server timeout)                                | プライマリ サーバがダウンしていると判断する前に Cisco ISE がプライマリ RADIUS トークン サーバからの応答を待つ時間 (秒単位) を指定します。有効な値は 1 ～ 300 です。デフォルトは 5 です。                                  |
| 接続試行回数 (Connection Attempts)                               | セカンダリ サーバ (定義されている場合) に移動する前、またはセカンダリ サーバが定義されていない場合は要求をドロップする前に、Cisco ISE がプライマリ サーバへの再接続を試行する回数を指定します。有効な値は 1 ～ 9 です。デフォルトは 3 です。             |

| フィールド                               | 使用上のガイドライン                                                                                                     |
|-------------------------------------|----------------------------------------------------------------------------------------------------------------|
| <b>セカンダリ サーバ (Secondary Server)</b> |                                                                                                                |
| ホスト名/アドレス (Host IP)                 | セカンダリ RADIUS トークン サーバの IP アドレスを入力します。このフィールドには、文字列として表される有効な IP アドレスを入力できます。このフィールドで使用する文字は、数字とドット (.) です。     |
| 共有秘密鍵 (Shared Secret)               | この接続のセカンダリ RADIUS トークン サーバで設定されている共有秘密を入力します。                                                                  |
| 認証ポート (Authentication Port)         | セカンダリ RADIUS トークン サーバが受信しているポート番号を入力します。有効な値は 1 ～ 65,535 です。デフォルトは 1812 です。                                    |
| サーバ タイムアウト (Server timeout)         | セカンダリ サーバがダウンしていると判断する前に Cisco ISE がセカンダリ RADIUS トークン サーバからの応答を待つ時間 (秒単位) を指定します。有効な値は 1 ～ 300 です。デフォルトは 5 です。 |
| 接続試行回数 (Connection Attempts)        | 要求をドロップする前に Cisco ISE がセカンダリ サーバへの再接続を試行する回数を指定します。有効な値は 1 ～ 9 です。デフォルトは 3 です。                                 |

#### 関連トピック

[RADIUS トークン ID ソース \(499 ページ\)](#)

[RADIUS トークン サーバの追加 \(502 ページ\)](#)

## RSA SecurID ID ソースの設定

次の表では、RSA SecurID ID ソースを作成し、それに接続するために使用できる [RSA SecurID ID ソース (RSA SecurID Identity Sources)] ページのフィールドについて説明します。このページへのナビゲーションパスは、**[管理 (Administration)] > [ID の管理 (Identity Management)] > [外部 ID ソース (External Identity Sources)] > [RSA SecurID]** です。

#### RSA プロンプトの設定

次の表では、[RSA プロンプト (RSA Prompts)] タブ内のフィールドについて説明します。

表 99: RSA プロンプトの設定

| フィールド                                 | 使用上のガイドライン               |
|---------------------------------------|--------------------------|
| パスコードプロンプトの入力 (Enter Passcode Prompt) | パスコードを取得するテキスト文字列を入力します。 |

| フィールド                                | 使用上のガイドライン                       |
|--------------------------------------|----------------------------------|
| 次のトークンコードの入力 (Enter Next Token Code) | 次のトークンを要求するテキスト文字列を入力します。        |
| PIN タイプの選択 (Choose PIN Type)         | PIN タイプを要求するテキスト文字列を入力します。       |
| システム PIN の受け入れ (Accept System PIN)   | システム生成の PIN を受け付けるテキスト文字列を入力します。 |
| 英数字 PIN の入力 (Enter Alphanumeric PIN) | 英数字 PIN を要求するテキスト文字列を入力します。      |
| 数値 PIN の入力 (Enter Numeric PIN)       | 数値 PIN を要求するテキスト文字列を入力します。       |
| PIN の再入力 (Re-enter PIN)              | ユーザに PIN の再入力を要求するテキスト文字列を入力します。 |

### RSA メッセージ設定 (RSA Message Settings)

次の表では、[RSA メッセージ (RSA Messages)] タブ内のフィールドについて説明します。

表 100: RSA メッセージ設定 (RSA Messages Settings)

| フィールド                                          | 使用上のガイドライン                                    |
|------------------------------------------------|-----------------------------------------------|
| システム PIN メッセージの表示 (Display System PIN Message) | システム PIN メッセージのラベルにするテキスト文字列を入力します。           |
| システム PIN 通知の表示 (Display System PIN Reminder)   | ユーザに新しい PIN を覚えるように通知するテキスト文字列を入力します。         |
| 数字を入力する必要があるエラー (Must Enter Numeric Error)     | PIN には数字のみを入力するようにユーザに指示するメッセージを入力します。        |
| 英数字を入力する必要があるエラー (Must Enter Alpha Error)      | PIN には英数字のみを入力するようにユーザに指示するメッセージを入力します。       |
| PIN 受け入れメッセージ (PIN Accepted Message)           | ユーザの PIN がシステムによって受け入れられたときに表示されるメッセージを入力します。 |
| PIN 拒否メッセージ (PIN Rejected Message)             | ユーザの PIN がシステムによって拒否されたときに表示されるメッセージを入力します。   |
| ユーザの PIN が異なるエラー (User Pins Differ Error)      | ユーザが不正な PIN を入力したときに表示されるメッセージを入力します。         |

| フィールド                                            | 使用上のガイドライン                                                   |
|--------------------------------------------------|--------------------------------------------------------------|
| システム PIN 受け入れメッセージ (System PIN Accepted Message) | ユーザの PIN がシステムによって受け入れられたときに表示されるメッセージを入力します。                |
| 不正パスワード長エラー (Bad Password Length Error)          | ユーザが指定した PIN が、PIN 長ポリシーで指定されている範囲に収まらない場合に表示されるメッセージを入力します。 |

#### 関連トピック

[RSA ID ソース \(504 ページ\)](#)

[Cisco ISE と RSA SecurID サーバの統合 \(505 ページ\)](#)

[RSA ID ソースの追加 \(507 ページ\)](#)

## ID の管理の設定

### ユーザ認証ポリシーの設定

次の表に、ユーザ パスワード用の基準の定義と、管理者およびネットワーク アクセス ユーザ アカウントの無効化のために使用できる、[ユーザ認証設定 (User Authentication Settings)] ページのフィールドについて説明します。このページへのナビゲーションパスは、[管理 (Administration)] > [ID の管理 (Identity Management)] > [設定 (Settings)] > [ユーザ認証設定 (User Authentication Settings)] です。

表 101: ユーザ パスワード ポリシーの設定

| オプション                         | 説明                             |
|-------------------------------|--------------------------------|
| 最小長 (Minimum Length)          | パスワードの最小長を設定します (文字単位)。        |
| [ユーザ名 (Username)]             | ユーザ名またはその文字の逆順での使用を制限します。      |
| Cisco                         | 「cisco」またはその文字の逆の順序での使用を制限します。 |
| 特殊文字                          | 定義した特殊文字の逆の順序での使用を制限します。       |
| 文字の繰り返し (Repeated characters) | 同じ文字を 4 回以上連続して繰り返すことを制限します。   |

| オプション                                                                                | 説明                                                                                                                                                                                                                                                                                                                                     |
|--------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 必須の文字 (Required characters)                                                          | <p>パスワードに、次のタイプがそれぞれ少なくとも 1 つは含まれている必要があります。</p> <ul style="list-style-type: none"> <li>• 小文字の英文字 (Lowercase alphabetic characters)</li> <li>• 大文字の英文字 (Uppercase alphabetic characters)</li> <li>• 数字 (Numeric characters)</li> <li>• 英数字以外の文字 (Non-alphanumeric characters)</li> </ul>                                               |
| パスワード履歴 (Password History)                                                           | <p>同じパスワードが繰り返し使用されるのを防ぐために、パスワードと異なっている必要がある前のバージョンの数を入力します。</p> <p>また、以前のパスワードと異なる必要がある文字数を入力できます。</p> <p>ユーザがパスワードを再使用できない日数を入力します。</p>                                                                                                                                                                                             |
| パスワードライフタイム (Password Lifetime)                                                      | <p>次のオプションを指定して、指定した期間後にパスワードを変更するようユーザに強制します。</p> <ul style="list-style-type: none"> <li>• パスワードが変更されなかった場合にユーザ アカウントを無効にするまでの時間 (日数) (Time (in days) before the user account is disabled if the password is not changed)</li> <li>• ユーザ アカウントが無効になるまでのリマインダ (日数) (Reminder (in days) before the user account is disabled)</li> </ul> |
| ログイン試行の不正なアカウントをロックまたは一時停止する (Lock or Suspend Account with Incorrect Login Attempts) | <p>Cisco ISE が、管理者を Cisco ISE からロックアウトし、アカウント クレデンシャルを一時停止または無効にするまでに、誤った管理者パスワードを記録する回数を指定します。</p> <p>アカウントがロックされる管理者に電子メールが送信されます。カスタム電子メール修復メッセージを入力することができます。</p>                                                                                                                                                                  |



## アカウント表示ポリシー

ユーザの認証またはクエリ中に、Cisco ISE はグローバル アカウント無効化ポリシー設定 ([管理 (Administration)] > [ID の管理 (Identity Management)] > [設定 (Settings)] > [ユーザ認証設定 (User Authentication Settings)]) を確認します。

- 指定した日付 (yyyy-mm-dd) を超えているユーザ アカウントを無効にします。ただし、特定のネットワーク アクセス ユーザ用のアカウント無効化ポリシー設定 ([管理 (Administration)] > [ID の管理 (Identity Management)] > [ID (Identities)] > [ユーザ (Users)] > [アカウント無効化ポリシー (Account Disable Policy)]) はグローバル設定よりも優先されます。
- ユーザ アカウントが作成されてから、またはユーザが最後に有効にされた日付から ([管理 (Administration)] > [ID の管理 (Identity Management)] > [ID (Identities)] > [ユーザ (Users)] > [ステータス (Status)])、指定された日数を超えたユーザ アカウントを無効にします。
- 連続する日数の間認証されていない管理者およびユーザ アカウントを無効にします。

Cisco Secure ACS でネットワーク アクセス ユーザに指定されているアカウント無効化ポリシー設定が Cisco ISE に移行されます。

## 関連トピック

[ユーザ アカウントのカスタム属性およびパスワード ポリシー](#) (363 ページ)

[ユーザの追加](#) (367 ページ)

# ネットワーク リソース

## ネットワーク デバイス

これらのページを使用すると、ネットワーク デバイスを追加し、管理することができます。

## ネットワーク デバイス定義の設定

次の表は、Cisco ISE のネットワーク アクセス デバイスを設定するために使用できる [ネットワーク デバイス (Network Devices)] ページのフィールドについて説明しています。このページへのナビゲーションパスは、[管理 (Administration)] > [ネットワーク リソース (Network Resources)] > [ネットワーク デバイス (Network Devices)] です。

## ネットワーク デバイスの設定

次の表に、[ネットワーク デバイス (Network Device)] セクションのフィールドを示します。

表 102: ネットワーク デバイスの設定

| フィールド                         | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [名前 (Name) ]                  | <p>ネットワーク デバイスの名前を入力します。</p> <p>ネットワーク デバイスに、デバイスのホスト名とは異なるわかりやすい名前を指定できます。デバイス名は論理識別子です。</p> <p>(注) 一度設定したデバイスの名前は編集できません。</p>                                                                                                                                                                                                                                                                                                                                                                                           |
| 説明                            | デバイスの説明を入力します。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| IP アドレス/マスク (IP Address/Mask) | <p>1 つの IP アドレスおよびサブネット マスクを入力します。</p> <p>IP アドレスとサブネット マスクを定義するときに従う必要があるガイドラインを次に示します。</p> <ul style="list-style-type: none"><li>• 特定の IP アドレスを定義するか、サブネット マスクを使用して範囲を定義できます。デバイス A の IP アドレス範囲が定義されている場合、デバイス A に定義されている範囲の個別のアドレスを別のデバイス B に設定できます。</li><li>• 最終オクテットの IP アドレス範囲を定義します。IP アドレスの範囲を指定するときに、ハイフン (-) またはアスタリスク (*) をワイルドカードとして使用できます。たとえば 1.1.1.1-10 または 1.1.1.* などです</li><li>• 同じ IP アドレスを持つ 2 台のデバイスを定義することはできません。</li><li>• 同じ IP 範囲を持つ 2 台のデバイスを定義することはできません。IP 範囲は、一部または全部が重複することはできません。</li></ul> |

| フィールド                                   | 説明                                                                                                                                                                                                                                                                                                                                 |
|-----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| デバイスタイプ (Device Type)                   | <p>ドロップダウン リストをクリックして、ネットワーク デバイスのベンダーを選択します。</p> <p>ドロップダウン リストの横にあるツールのヒントを使用して、選択したベンダーのネットワーク デバイスがサポートしているフローおよびサービスと、デバイスで使用されている RADIUS CoA ポートと URL リダイレクトのタイプを表示できます。これらの属性は、デバイスタイプのネットワーク デバイス プロファイルで定義されます。</p>                                                                                                       |
| モデル名 (Model Name)                       | <p>ドロップダウン リストをクリックして、デバイス モデルなどを選択します。</p> <p>モデル名は、ルールベースのポリシーの条件をチェックするときに、パラメータの 1 つとして使用できます。この属性は、デバイス ディクショナリにあります。</p>                                                                                                                                                                                                     |
| ソフトウェア バージョン (Software Version)         | <p>ドロップダウン リストをクリックして、ネットワーク デバイスで実行するソフトウェアのバージョンを選択します。</p> <p>ソフトウェア バージョンは、ルールベースのポリシーの条件をチェックするときに、パラメータの 1 つとして使用できます。この属性は、デバイス ディクショナリにあります。</p>                                                                                                                                                                           |
| ネットワーク デバイス グループ (Network Device Group) | <p>[ロケーション (Location) ] および [デバイス タイプ (Device Type) ] ドロップダウン リストをクリックし、ネットワーク デバイスに関連付けることができるロケーションとデバイス タイプを選択します。</p> <p>グループを設定するときに、明確にデバイスをグループに割り当てないと、そのデバイスはデフォルトのデバイス グループ (ルート NDG) に含まれます。これにより、ロケーションはすべてのロケーション、デバイス タイプはすべてのデバイス タイプとなり、デフォルトのデバイス グループ (ルート NDG) が割り当てられます。たとえば、すべてのロケーションとすべてのデバイス グループなどです。</p> |

**RADIUS 認証設定**

次の表では、[RADIUS 認証設定 (RADIUS Authentication Settings)] セクションのフィールドについて説明します。

表 103: RADIUS 認証設定

| フィールド                 | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>RADIUS UDP の設定</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| プロトコル                 | 選択したプロトコルとして RADIUS を表示します。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| 共有秘密鍵 (Shared Secret) | <p>ネットワーク デバイスの共有秘密鍵を入力します。</p> <p>共有秘密鍵は、<b>pac</b> オプションを指定した <b>radius-host</b> コマンドを使用してネットワーク デバイスに設定したキーです。</p> <p>(注) 共有秘密鍵の長さは、[デバイスのセキュリティ設定 (Device Security Settings)] ページの [RADIUS 共有秘密鍵の最小長 (Minimum RADIUS Shared Secret Length)] フィールドで設定された値と同等以上である必要があります ([管理 (Administration)] &gt; [ネットワーク リソース (Network Resources)] &gt; [ネットワーク デバイス (Network Devices)] &gt; [デバイス セキュリティ設定 (Device Security Settings)] )。</p> <p>RADIUS サーバでのベストプラクティスは、22 文字にすることです。新規インストールとアップグレードした展開の場合、デフォルトではこの値は 4 文字であることに注意してください。この値は [デバイス セキュリティ設定 (Device Security Settings)] ページで変更できます。</p> |

| フィールド                  | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CoA ポート (CoA Port)     | <p>RADIUS CoA に使用するポートを指定します。</p> <p>デバイスのデフォルトの CoA ポートはネットワーク デバイス プロファイルで定義されます。</p> <p>(注) [RADIUS 認証設定 (RADIUS Authentication Settings)] の [ネットワーク デバイス (Network Devices)] ページ ([管理 (Administration)] &gt; [ネットワーク リソース (Network Resources)] &gt; [ネットワーク デバイス (Network Devices)]) で指定した CoA ポートを変更する場合は、[ネットワーク デバイス プロファイル (Network Device Profile)] ページ ([管理 (Administration)] &gt; [ネットワーク リソース (Network Resources)] &gt; [ネットワーク デバイス プロファイル (Network Device Profiles)]) で対応するプロファイルに必ず同じ CoA ポートを指定します。</p> |
| <b>RADIUS DTLS の設定</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| 必要な DTLS               | <p>このオプションを有効にすると、Cisco ISE ではこのデバイスからの DTLS 要求だけが処理されます。このオプションを無効にすると、Cisco ISE ではこのデバイスからの UDP 要求と DTLS 要求の両方が処理されます。</p> <p>RADIUS DTLS は SSL トンネルの確立および RADIUS の通信用に強化されたセキュリティを提供します。</p>                                                                                                                                                                                                                                                                                                                        |
| 共有秘密鍵 (Shared Secret)  | RADIUS DTLS に使用される共有秘密鍵が表示されます。この値は固定されており、MD5 整合性チェックを計算するために使用されます。                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| CoA ポート (CoA Port)     | RADIUS DTLS CoA に使用するポートを指定します。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| CoA の ISE 証明書の発行元 CA   | ドロップダウンリストから RADIUS DTLS CoA に使用する認証局を選択します。                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

| フィールド                                                        | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>全般設定</b>                                                  |                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>KeyWrap の有効化 (Enable KeyWrap)</b>                         | <p>ネットワーク デバイスでサポートされる場合にのみ、このチェックボックスをオンにします。これにより、AES KeyWrap アルゴリズムによって RADIUS のセキュリティが強化されます。</p> <p>(注) FIPS モードで Cisco ISE を実行する場合は、ネットワークデバイス上で KeyWrap を有効にする必要があります。</p>                                                                                                                                                                                                                |
| <b>キー暗号キー (Key Encryption Key)</b>                           | (KeyWrap を有効にしている場合だけ表示されます) セッション暗号化 (秘密) に使用される暗号キーを入力します。                                                                                                                                                                                                                                                                                                                                     |
| <b>メッセージオーセンティケーターコードキー (Message Authenticator Code Key)</b> | (KeyWrap を有効にしている場合だけ表示されます) RADIUS メッセージのキー付き Hashed Message Authentication Code (HMAC) の計算に使用されるキーを入力します。                                                                                                                                                                                                                                                                                      |
| <b>キー入力形式 (Key Input Format)</b>                             | <p>次の形式のいずれか 1 つを選択します。</p> <ul style="list-style-type: none"> <li>• [ASCII] : キー暗号キーの長さは 16 文字 (バイト)、メッセージオーセンティケーターコードキーの長さは 20 文字 (バイト) である必要があります。</li> <li>• [16 進数 (Hexadecimal) ] : キー暗号キーの長さは 32 バイトであり、メッセージオーセンティケーターコードキーの長さは 40 バイトである必要があります。</li> </ul> <p>Cisco ISE FIPS 暗号キーの入力に使用するキー入力形式を指定します。これは、WLC の設定と一致する必要があります (指定する値はキーの正しい (全体の) 長さにする必要があります、それよりも短い値は許可されません)。</p> |

### TACACS+ 認証設定

次の表では、ネットワーク デバイスの TACACS+ 認証を設定するために使用できる [ネットワークデバイス (Network Devices) ] ページのフィールドについて説明します。ナビゲーションパスは次のとおりです。

- (ネットワーク デバイスの場合) [ワークセンター (Work Centers)] > [デバイス管理 (Device Administration)] > [ネットワークリソース (Network Resources)] > [ネットワークデバイス (Network Devices)] > [追加 (Add)] > [TACACS認証設定 (TACACS Authentication Settings)]。
- (デフォルトのデバイスの場合) [ワークセンター (Work Centers)] > [デバイス管理 (Device Administration)] > [ネットワークリソース (Network Resources)] > [デフォルトのデバイス (Default Devices)] > [TACACS認証設定 (TACACS Authentication Settings)]。詳細については、「[Cisco ISE でのデフォルトのネットワーク デバイス定義](#)」の項を参照してください。

| フィールド                                               | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                |
|-----------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 共有秘密鍵 (Shared Secret)                               | TACACS+ プロトコルがイネーブルのときにネットワーク デバイスに割り当てられたテキストの文字列。ユーザは、ネットワーク デバイスによってユーザ名およびパスワードが認証される前にテキストを入力する必要があります。ユーザが共有秘密情報を提示するまで、接続は拒否されます。これは必須フィールドではありません。                                                                                                                                                                                                |
| 廃止された共有秘密がアクティブです (Retired Shared Secret is Active) | リタイアメント期間がアクティブな場合に表示されます。                                                                                                                                                                                                                                                                                                                                |
| 廃止 (Retire)                                         | 既存の共有秘密を終了する代わりに廃止します。[廃止 (Retire)] をクリックすると、メッセージボックスが表示されます。[はい (Yes)] または [いいえ (No)] をクリックできます。                                                                                                                                                                                                                                                        |
| 残りの廃止期間 (Remaining Retired Period)                  | <p>(上のメッセージボックスで [はい (Yes)] を選択した場合にのみ利用可能) 次のナビゲーションパスで指定されたデフォルト値が表示されます。[ワークセンター (Work Centers)] &gt; [デバイス管理 (Device Administration)] &gt; [設定 (Settings)] &gt; [接続設定 (Connection Settings)] &gt; [デフォルトの共有秘密リタイアメント期間 (Default Shared Secret Retirement Period)]。デフォルト値は変更することができます。</p> <p>これにより、新しい共有秘密を入力でき、古い共有秘密は指定された日数にわたってアクティブなままになります。</p> |

| フィールド                                        | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                         |
|----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 終了 (End)                                     | (上のメッセージ ボックスで [はい (Yes) ] を選択した場合にのみ利用可能) リタイアメント期間が終了し、古い共有秘密が終了します。                                                                                                                                                                                                                                                             |
| シングル接続モードを有効にする (Enable Single Connect Mode) | <p>ネットワーク デバイスとのすべての TACACS+ 通信に単一の TCP 接続を使用する場合にオンにします。次のいずれかを実行します。</p> <ul style="list-style-type: none"><li>• [レガシーシスコデバイス (Legacy Cisco Devices) ]</li><li>• または、[TACACS+ドラフトコンプライアンスシングル接続のサポート (TACACS+ Draft Compliance Single Connect Support) ]。シングル接続モードをディセーブルにすると、ISEはすべての TACACS+ 要求に対して新しい TCP 接続を使用します。</li></ul> |

## SNMP 設定

次の表では、[SNMP 設定 (SNMP Settings) ] セクションのフィールドについて説明します。



表 104: SNMP 設定

| フィールド                              | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SNMP バージョン (SNMP Version)          | <p>[バージョン (Version) ] ドロップダウン リストから要求に使用される SNMP のバージョンを選択します。</p> <p>次のバージョンがあります。</p> <ul style="list-style-type: none"><li>• 1 : SNMPv1 は informs をサポートしていません。</li><li>• 2c</li><li>• 3 : SNMPv3 は、[Priv] セキュリティ レベルを選択した場合にパケット暗号化が可能であるため、最もセキュアなモデルです。</li></ul> <p>(注) ネットワーク デバイスに SNMPv3 パラメータを設定した場合、モニタリング サービス ([操作 (Operations) ]&gt;[レポート (Reports) ]&gt;[カタログ (Catalog) ]&gt;[ネットワーク デバイス (Network Device) ]&gt;[セッション ステータス概要 (Session Status Summary) ]) によって提供されるネットワーク デバイス セッション ステータス概要レポートを生成できません。ネットワーク デバイスが SNMPv1 または SNMPv2c パラメータを使用して設定されている場合は、このレポートを正常に生成できます。</p> |
| SNMP RO コミュニティ (SNMP RO Community) | <p>(SNMP バージョン 1 および 2c で選択された場合のみ) Cisco ISE にデバイスへの特定タイプのアクセスを提供する読み取り専用コミュニティ スtring を入力します。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| SNMP ユーザ名 (SNMP Username)          | <p>(SNMP バージョン 3 の場合のみ) SNMP ユーザ名を入力します。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

| フィールド                       | 使用上のガイドライン                                                                                                                                                                                                                                                                   |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| セキュリティ レベル (Security Level) | <p>(SNMP バージョン 3 の場合のみ) 次からセキュリティ レベルを選択します。</p> <ul style="list-style-type: none"><li>• [Auth] : Message Digest 5 またはセキュア ハッシュ アルゴリズム (SHA) パケット 認証をイネーブルにします</li><li>• [No Auth] : 認証なし、プライバシーなしのセキュリティ レベル。</li><li>• [Priv] : データ暗号規格 (DES) パケットの暗号化をイネーブルにします</li></ul> |
| 認証プロトコル (Auth Protocol)     | <p>(SNMP バージョン 3 でセキュリティ レベル Auth および Priv を選択した場合のみ) ネットワーク デバイスで使用する認証プロトコルを選択します。</p> <p>認証プロトコルには、Auth および Priv のセキュリティ レベルに対して次のいずれかが含まれます。</p> <ul style="list-style-type: none"><li>• MD5</li><li>• SHA</li></ul>                                                     |
| 認証パスワード (Auth Password)     | <p>(SNMP バージョン 3 でセキュリティ レベル Auth および Priv を選択した場合のみ) 認証キーを入力します。このキーは 8 文字以上の長さにする必要があります。</p> <p>デバイスにすでに設定されている認証パスワードを表示するには、[表示 (Show)] をクリックします。</p>                                                                                                                   |

| フィールド                                              | 使用上のガイドライン                                                                                                                                                                                                                                      |
|----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| プライバシー プロトコル (Privacy Protocol)                    | <p>(SNMP バージョン 3 でセキュリティ レベル Priv を選択した場合のみ) ネットワーク デバイスで使用するプライバシー プロトコルを選択します。</p> <p>プライバシープロトコルは次のいずれかです。</p> <ul style="list-style-type: none"> <li>• DES</li> <li>• AES128</li> <li>• AES192</li> <li>• AES256</li> <li>• 3DES</li> </ul> |
| プライバシー パスワード (Privacy Password)                    | <p>(SNMP バージョン 3 でセキュリティ レベル Priv を選択した場合のみ) プライバシー キーを入力します。</p> <p>デバイスにすでに設定されているプライバシー パスワードを表示するには、[表示 (Show)] をクリックします。</p>                                                                                                               |
| ポーリング間隔 (Polling Interval)                         | ポーリング間隔を秒単位で入力します。デフォルトは 3600 秒です。                                                                                                                                                                                                              |
| リンク トラップ クエリー (Link Trap Query)                    | SNMP トラップを介して受信する linkup 通知と linkdown 通知を受信して解釈するには、このチェックボックスをオンにします。                                                                                                                                                                          |
| MAC トラップ クエリ (MAC Trap Query)                      | SNMP トラップを介して受信する MAC 通知を受信して解釈するには、このチェックボックスをオンにします。                                                                                                                                                                                          |
| 送信元ポリシー サービス ノード (Originating Policy Service Node) | SNMP データのポーリングに使用される ISE サーバを示します。デフォルトでは自動ですが、別の値を割り当てて設定を上書きできます。                                                                                                                                                                             |

### 高度な TrustSec 設定

次の表は、[高度な TrustSec 設定 (Advanced TrustSec Settings)] セクションのフィールドについて説明しています。

表 105: 高度な TrustSec 設定

| フィールド                                                                                       | 使用上のガイドライン                                                                                                                                   |
|---------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| <b>TrustSec デバイスの通知および更新の設定</b>                                                             |                                                                                                                                              |
| <b>TrustSec ID にデバイス ID を使用 (Use Device ID for TrustSec Identification)</b>                 | [デバイス ID (Device ID) ] フィールドにデバイス ID としてデバイス名をリストするには、このチェックボックスをオンにします。                                                                     |
| <b>デバイス ID (Device ID)</b>                                                                  | [TrustSec ID にデバイス ID を使用 (Use Device ID for TrustSec Identification) ] チェックボックスがオンでない場合にのみ、このフィールドにデバイス ID を入力できます。                         |
| <b>[パスワード (Password) ]</b>                                                                  | TrustSec デバイスを認証するために TrustSec デバイス CLI で設定したパスワードを入力します。<br><br>TrustSec デバイスの認証に使用されるパスワードを表示するには、[表示 (Show) ] をクリックします。                   |
| <b>環境データのダウンロード間隔 &lt;...&gt; (Download Environment Data Every &lt;...&gt;)</b>             | デバイスが Cisco ISE から環境データをダウンロードする必要がある時間間隔を指定します。時間を秒、分、時、日、または週で指定できます。デフォルト値は 1 日です。                                                        |
| <b>ピア許可ポリシーのダウンロード間隔 &lt;...&gt; (Download Peer Authorization Policy Every &lt;...&gt;)</b> | デバイスが Cisco ISE からピア許可ポリシーをダウンロードする必要がある時間間隔を指定します。時間を秒、分、時、日、または週で指定できます。デフォルト値は 1 日です。                                                     |
| <b>再認証間隔 &lt;...&gt; (Reauthentication Every &lt;...&gt;)</b>                               | 最初の認証後、デバイスが Cisco ISE に対して自身を再認証する時間間隔を指定します。時間を秒、分、時、日、または週で設定できます。たとえば 1000 秒と入力すると、デバイスは 1000 秒ごとに Cisco ISE に対して自身を認証します。デフォルト値は 1 日です。 |
| <b>SGACL リストのダウンロード間隔 &lt;...&gt; (Download SGACL Lists Every &lt;...&gt;)</b>              | デバイスが Cisco ISE から SGACL をダウンロードする必要がある時間間隔を指定します。時間を秒、分、時、日、または週で設定できます。デフォルト値は 1 日です。                                                      |

| フィールド                                                                                                                   | 使用上のガイドライン                                                                                                                           |
|-------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| その他の TrustSec デバイスでこのデバイスを信頼する（信頼できる TrustSec）（ <b>Other TrustSec Devices to Trust This Device (TrustSec Trusted)</b> ） | すべてのピア デバイスでこの TrustSec デバイスを信頼する場合は、このチェックボックスをオンにします。このチェックボックスをオフにした場合、ピア デバイスはこのデバイスを信頼せず、このデバイスから到着したすべてのパケットが適宜色付けまたはタグ付けされます。 |
| TrustSec 設定の変更についてこのデバイスに通知する（ <b>Notify this device about TrustSec configuration changes</b> ）                         | Cisco ISE でこの TrustSec デバイスに TrustSec CoA 通知を送信するには、このチェックボックスをオンにします。                                                               |
| デバイス設定の展開設定                                                                                                             |                                                                                                                                      |
| セキュリティグループタグマッピングの展開時にこのデバイスを含める（ <b>Include this device when deploying Security Group Tag Mapping Updates</b> ）        | この TrustSec デバイスで、デバイス インターフェイスクレデンシアルを使用して IP と SGT の間のマッピングを取得するには、このチェックボックスをオンにします。                                              |
| EXEC モード ユーザ名（ <b>EXEC Mode Username</b> ）                                                                              | TrustSec デバイスへのログインに使用するユーザ名を入力します。                                                                                                  |
| EXEC モード パスワード（ <b>EXEC Mode Password</b> ）                                                                             | デバイス パスワードを入力します。                                                                                                                    |
| 有効モード パスワード（ <b>Enable Mode Password</b> ）                                                                              | （省略可能）特権モードで TrustSec デバイスの構成を編集するために使用する有効なパスワードを入力します。                                                                             |
| アウトオブバンド TrustSec PAC ディスプレイ（ <b>Out Of Band TrustSec PAC Display</b> ）                                                 |                                                                                                                                      |
| 発行日（ <b>Issue Date</b> ）                                                                                                | この TrustSec デバイス用に Cisco ISE によって生成された最後の TrustSec PAC の発行日を表示します。                                                                   |
| 期限日（ <b>Expiration Date</b> ）                                                                                           | この TrustSec デバイス用に Cisco ISE によって生成された最後の TrustSec PAC の有効期限を表示します。                                                                  |
| 発行元（ <b>Issued By</b> ）                                                                                                 | このデバイス用に Cisco ISE によって生成された最後の TrustSec PAC の発行者（TrustSec 管理者）の名前を表示します。                                                            |
| PAC の生成（ <b>Generate PAC</b> ）                                                                                          | TrustSec デバイスのアウトオブバンド TrustSec PAC を生成するには、このオプションをクリックします。                                                                         |

## 関連トピック

- [Cisco ISE のネットワーク デバイス定義 \(247 ページ\)](#)
- [Cisco ISE でのサードパーティ ネットワーク デバイスのサポート \(251 ページ\)](#)
- [ネットワーク デバイス グループ \(Network Device Groups\) \(259 ページ\)](#)
- [Cisco ISE でのネットワーク デバイス定義の作成 \(220 ページ\)](#)
- [Cisco ISE でのサードパーティ製ネットワーク デバイスの設定 \(256 ページ\)](#)

## デフォルトのネットワーク デバイス定義の設定

次の表に、Cisco ISE が RADIUS または TACACS+ 認証に使用できる、デフォルトのネットワーク デバイスを設定できるようにする [デフォルトのネットワーク デバイス (Default Network device)] ページのフィールドを示します。次のいずれかのナビゲーションパスを選択します。

- [管理 (Administration)] > [ネットワーク リソース (Network Resources)] > [ネットワーク デバイス (Network Devices)] > [デフォルトのデバイス (Default Devices)]
- [ワーク センター (Work Centers)] > [デバイス管理 (Device Administration)] > [ネットワーク リソース (Network Resources)] > [デフォルトのデバイス (Default Devices)]

表 106: デフォルトのネットワーク デバイス定義の設定

| フィールド                                                   | 使用上のガイドライン                                                                                                                                                                                        |
|---------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| デフォルトのネットワーク デバイスのステータス (Default Network Device Status) | デフォルトのネットワーク デバイス定義を有効にするには、[デフォルトのネットワーク デバイスのステータス (Default Network Device Status)] ドロップダウン リストから [有効化 (Enable)] を選択します。<br><br>(注) デフォルトデバイスが有効になっている場合、RADIUS または TACACS+ で認証設定を有効にする必要があります。 |
| デバイス プロファイル                                             | デフォルトのデバイス ベンダーとしてシスコを表示します。                                                                                                                                                                      |
| RADIUS 認証設定                                             |                                                                                                                                                                                                   |
| RADIUS の有効化                                             | デバイスへの RADIUS 認証を有効にする場合は、このチェック ボックスをオンにします。                                                                                                                                                     |
| RADIUS UDP の設定                                          |                                                                                                                                                                                                   |

| フィールド                 | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 共有秘密鍵 (Shared Secret) | <p>共有秘密を入力します。共有秘密情報の長さは、最大 127 文字です。</p> <p>共有秘密鍵は、<b>pac</b> オプションを指定した <b>radius-host</b> コマンドを使用してネットワーク デバイスに設定したキーです。</p> <p>(注) 共有秘密鍵の長さは、[デバイスのセキュリティ設定 (Device Security Settings)] ページの [RADIUS 共有秘密鍵の最小長 (Minimum RADIUS Shared Secret Length)] フィールドで設定された値と同等以上である必要があります ([管理 (Administration)] &gt; [ネットワーク リソース (Network Resources)] &gt; [ネットワーク デバイス (Network Devices)] &gt; [デバイス セキュリティ設定 (Device Security Settings)] )。デフォルトでは、この値は新規インストールとアップグレードされた展開用は 4 文字です。RADIUS サーバでのベスト プラクティスは、22 文字にすることです。</p> |
| RADIUS DTLS の設定       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 必要な DTLS              | <p>このオプションを有効にすると、Cisco ISE ではこのデバイスからの DTLS 要求だけが処理されます。このオプションを無効にすると、Cisco ISE ではこのデバイスからの UDP 要求と DTLS 要求の両方が処理されます。</p> <p>RADIUS DTLS は SSL トンネルの確立および RADIUS の通信用に強化されたセキュリティを提供します。</p>                                                                                                                                                                                                                                                                                                                                 |
| 共有秘密鍵 (Shared Secret) | RADIUS DTLS に使用される共有秘密鍵が表示されます。この値は固定されており、MD5 整合性チェックを計算するために使用されます。                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| CoA の ISE 証明書の発行元 CA  | ドロップダウンリストから RADIUS DTLS CoA に使用する認証局を選択します。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 全般設定                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

| フィールド                                                    | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| KeyWrap の有効化 (Enable KeyWrap)                            | <p>ネットワーク デバイスでサポートされる場合にのみ、このチェックボックスをオンにします。これにより、AES KeyWrap アルゴリズムによって RADIUS のセキュリティが強化されます。</p> <p>FIPS モードで Cisco ISE を実行する場合は、ネットワーク デバイス上で KeyWrap を有効にする必要があります。</p>                                                                                                                                                                                                                        |
| キー暗号キー (Key Encryption Key)                              | KeyWrap を有効にしているときに、セッションの暗号化 (秘密) に使用される暗号キーを入力します。                                                                                                                                                                                                                                                                                                                                                  |
| メッセージ オーセンティケーター コード キー (Message Authenticator Code Key) | KeyWrap を有効にしているときに、RADIUS メッセージに対するキー付き Hashed Message Authentication Code (HMAC) の計算に使用されるキーを入力します。                                                                                                                                                                                                                                                                                                 |
| キー入力形式 (Key Input Format)                                | <p>次の形式のいずれか 1 つを選択します。</p> <ul style="list-style-type: none"> <li>• [ASCII] : キー暗号キーの長さは 16 文字 (バイト)、メッセージ オーセンティケーター コード キーの長さは 20 文字 (バイト) である必要があります。</li> <li>• [16 進数 (Hexadecimal) ] : キー暗号キーの長さは 32 バイトであり、メッセージ オーセンティケーター コード キーの長さは 40 バイトである必要があります。</li> </ul> <p>Cisco ISE FIPS 暗号キーの入力に使用するキー入力形式を指定します。これは、WLC の設定と一致する必要があります (指定する値はキーの正しい (全体の) 長さにする必要があり、それよりも短い値は許可されません) 。</p> |
| TACACS 認証設定                                              |                                                                                                                                                                                                                                                                                                                                                                                                       |
| 共有秘密鍵 (Shared Secret)                                    | TACACS+ プロトコルがイネーブルのときにネットワーク デバイスに割り当てられたテキストの文字列。ユーザは、ネットワーク デバイスによってユーザ名およびパスワードが認証される前にテキストを入力する必要があります。ユーザが共有秘密情報を提示するまで、接続は拒否されます。                                                                                                                                                                                                                                                              |



| フィールド                                               | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                  |
|-----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 廃止された共有秘密がアクティブです (Retired Shared Secret is Active) | リタイアメント期間がアクティブな場合に表示されます。                                                                                                                                                                                                                                                                                                                                  |
| 廃止 (Retire)                                         | 既存の共有秘密を終了する代わりに廃止します。[廃止 (Retire)] をクリックすると、メッセージ ボックスが表示されます。[はい (Yes)] または [いいえ (No)] をクリックできます。                                                                                                                                                                                                                                                         |
| 残りの廃止期間 (Remaining Retired Period)                  | <p>(上のメッセージ ボックスで [はい (Yes)] を選択した場合にのみ利用可能) 次のナビゲーション パスで指定されたデフォルト値が表示されます。[ワークセンター (Work Centers)] &gt; [デバイス管理 (Device Administration)] &gt; [設定 (Settings)] &gt; [接続設定 (Connection Settings)] &gt; [デフォルトの共有秘密リタイアメント期間 (Default Shared Secret Retirement Period)]。デフォルト値は変更することができます。</p> <p>これにより、新しい共有秘密を入力でき、古い共有秘密は指定された日数にわたってアクティブなままになります。</p> |
| 終了 (End)                                            | (上のメッセージ ボックスで [はい (Yes)] を選択した場合にのみ利用可能) リタイアメント期間が終了し、古い共有秘密が終了します。                                                                                                                                                                                                                                                                                       |
| シングル接続モードを有効にする (Enable Single Connect Mode)        | <p>ネットワーク デバイスとのすべての TACACS+ 通信に単一の TCP 接続を使用する場合にオンにします。次のいずれかを実行します。</p> <ul style="list-style-type: none"> <li>• [レガシーシスコデバイス (Legacy Cisco Devices)]</li> <li>• または、[TACACS+ ドラフトコンプライアンスシングル接続のサポート (TACACS+ Draft Compliance Single Connect Support)]。このオプションをディセーブルにすると、すべての TACACS+ 要求に対して新しい TCP 接続が ISE で使用されます。</li> </ul>                       |

## デバイス セキュリティ設定

RADIUS 共有秘密の最小長を指定します。新規インストールとアップグレードした展開の場合、デフォルトではこの値は4文字になります。RADIUS サーバでのベストプラクティスは、22 文字にすることです。



- (注) [ネットワーク デバイス (Network Devices)] ページに入力した共有秘密の長さは、[デバイス セキュリティ設定 (Device Security Settings)] ページの [RADIUS 共有秘密の最小長 (Minimum RADIUS Shared Secret Length)] フィールドで設定した値以上でなければなりません。

### 関連トピック

[ネットワーク デバイス定義の設定](#) (1227 ページ)

## ネットワーク デバイスのインポート設定

次の表では、ネットワーク デバイスの詳細を Cisco ISE にインポートするために使用する [ネットワーク デバイス インポート (Network Device Import)] ページのフィールドについて説明します。このページへのナビゲーションパスは、[管理 (Administration)] > [ネットワーク リソース (Network Resources)] > [ネットワーク デバイス (Network Devices)] です。

表 107: ネットワーク デバイスのインポート設定

| フィールド                           | 使用上のガイドライン                                                                                                                                                          |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| テンプレートの生成 (Generate a Template) | カンマ区切り形式 (.csv) テンプレート ファイルを作成するには、このリンクをクリックします。<br><br>同じ形式のネットワーク デバイス情報でテンプレートを更新し、それらのネットワーク デバイスを Cisco ISE 展開にインポートするためにローカルで保存します。                          |
| ファイル (File)                     | 作成したか、または Cisco ISE 展開から以前にエクスポートしたカンマ区切り形式ファイルの場所を参照するには、[参照 (Browse)] をクリックします。<br><br>インポートを使用して、新しい、更新されたネットワーク デバイス情報を含むネットワーク デバイスを別の Cisco ISE 展開にインポートできます。 |

| フィールド                                                        | 使用上のガイドライン                                                                                                                                                                                |
|--------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 新しいデータで既存のデータを上書き<br>(Overwrite existing data with new data) | <p>Cisco ISE で既存のネットワーク デバイスをインポート ファイル内のデバイスに置き換える場合は、このチェックボックスをオンにします。</p> <p>このチェックボックスをオンにしない場合、インポート ファイル内の新しいネットワーク デバイス定義がネットワーク デバイス リポジトリに追加されます。重複エントリは無視されます。</p>             |
| 最初のエラーでインポートを停止 (Stop Import on First Error)                 | <p>インポート中にエラーが発生したときに Cisco ISE にインポートを中止させる場合、このチェックボックスをオンにしますが、Cisco ISE はエラーのその時点までネットワーク デバイスをインポートします。</p> <p>このチェックボックスがオフで、エラーが発生した場合は、エラーが報告され、Cisco ISE はデバイスを引き続きインポートします。</p> |

#### 関連トピック

[Cisco ISE のネットワーク デバイス定義](#) (247 ページ)

[Cisco ISE でのサードパーティ ネットワーク デバイスのサポート](#) (251 ページ)

[Cisco ISE へのネットワーク デバイスのインポート](#) (250 ページ)

## ネットワーク デバイス グループ (Network Device Groups)

これらのページを使用すると、ネットワーク デバイス グループを設定し、管理することができます。

### ネットワーク デバイス グループの設定

次の表では、ネットワーク デバイス グループを作成するために使用できる [ネットワーク デバイス グループ (Network Device Groups)] ページのフィールドについて説明します。このページへのナビゲーションパスは、[管理 (Administration)] > [ネットワーク リソース (Network Resources)] > [ネットワーク デバイス グループ (Network Device Groups)] > [グループ (Groups)] です。

[ワークセンター (Work Centers)] > [デバイス管理 (Device Administration)] > [ネットワーク デバイスグループ (Network Device Groups)] > [グループ (Groups)] ページでネットワーク デバイス グループを作成することもできます。

表 108: ネットワーク デバイス グループの設定

| フィールド                | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                             |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [名前 (Name) ]         | <p>ルート ネットワーク デバイス グループ (NDG) の名前を入力します。ルート NDG の下の後続のすべての子ネットワーク デバイス グループに対して、新しいネットワーク デバイス グループの名前を入力します。</p> <p>ネットワーク デバイス グループの完全な名前には最大で100文字使用できます。たとえば、親グループ Global &gt; Asia の下にサブグループ India を作成している場合、作成している NDG の完全な名前は Global#Asia#India になります。この完全な名前は 100 文字を超えないようにしてください。NDG の完全な名前が 100 文字を超えた場合、NDG の作成は失敗します。</p> |
| 説明                   | ルートまたは子のネットワーク デバイス グループの説明を入力します。                                                                                                                                                                                                                                                                                                     |
| 親グループ (Parent Group) | 親グループとして既存のグループを選択するか、ルートグループとして、この新しいグループを追加できます。                                                                                                                                                                                                                                                                                     |

## 関連トピック

[ネットワーク デバイス グループ \(Network Device Groups\)](#) (259 ページ)

[ポリシー評価で Cisco ISE が使用するネットワーク デバイスの属性](#) (260 ページ)

[Cisco ISE でのネットワーク デバイス定義の作成](#) (220 ページ)

## ネットワーク デバイス グループのインポート設定

次の表では、Cisco ISE にネットワーク デバイス グループをインポートするために使用できる [ネットワーク デバイス グループ インポート (Network Device Group Import) ] ページのフィールドについて説明します。このページへのナビゲーションパスは、**[管理 (Administration) ] > [ネットワーク リソース (Network Resources) ] > [ネットワーク デバイス グループ (Network Device Groups) ] > [グループ (Groups) ]** です。

表 109: ネットワーク デバイス グループのインポート設定

| フィールド                                                     | 使用上のガイドライン                                                                                                                                                                                        |
|-----------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| テンプレートの生成 (Generate a Template)                           | <p>カンマ区切り形式 (.csv) テンプレート ファイルを作成するには、このリンクをクリックします。</p> <p>同じ形式のネットワーク デバイス グループ情報でテンプレートを更新し、それらのネットワーク デバイス グループを Cisco ISE 展開にインポートするためにローカルで保存します。</p>                                       |
| ファイル (File)                                               | <p>作成したか、または Cisco ISE 展開から以前にエクスポートしたカンマ区切り形式ファイルの場所を参照するには、[参照 (Browse) ] をクリックします。</p> <p>インポートを使用して、新しい、更新されたネットワーク デバイス グループ情報を含むネットワーク デバイス グループを別の Cisco ISE 展開にインポートできます。</p>             |
| 新しいデータで既存のデータを上書き (Overwrite existing data with new data) | <p>Cisco ISE で既存のネットワーク デバイス グループをインポートファイル内のデバイス グループに置き換える場合は、このチェックボックスをオンにします。</p> <p>このチェックボックスをオンにしない場合、インポート ファイル内の新しいネットワーク デバイス グループがネットワーク デバイス グループ リポジトリに追加されます。重複エントリは無視されます。</p>    |
| 最初のエラーでインポートを停止 (Stop Import on First Error)              | <p>インポート中にエラーが発生すると、Cisco ISE にインポートを中止させる場合、このチェックボックスをオンにしますが、Cisco ISE はエラーのその時点までネットワーク デバイス グループをインポートします。</p> <p>このチェックボックスがオフで、エラーが発生した場合は、エラーが報告され、Cisco ISE はデバイス グループを引き続きインポートします。</p> |

## 関連トピック

[ネットワーク デバイス グループ \(Network Device Groups\)](#) (259 ページ)

[ポリシー評価で Cisco ISE が使用するネットワーク デバイスの属性](#) (260 ページ)

Cisco ISE へのネットワーク デバイス グループのインポート (260 ページ)

## ネットワーク デバイス プロファイル設定

次の表は、[ネットワーク デバイス プロファイル (Network Device Profiles)] ページのフィールドについての説明です。このページを使用して、プロトコル、リダイレクト URL および CoA 設定に対するデバイスのサポートなど、特定のベンダーからのネットワーク デバイスのタイプに対するデフォルト設定を構成することができます。その後、プロファイルを使用して特定のネットワーク デバイスを定義します。

このページへのナビゲーションパスは、[管理 (Administration)] > [ネットワーク リソース (Network Resources)] > [ネットワーク デバイス プロファイル (Network Device Profiles)] です。

### ネットワーク デバイス プロファイルの設定

次の表は、[ネットワーク デバイス プロファイル (Network Device Profile)] セクションのフィールドについての説明です。

表 110: ネットワーク デバイス プロファイルの設定

| フィールド         | 説明                                                                                                                    |
|---------------|-----------------------------------------------------------------------------------------------------------------------|
| [名前 (Name)]   | ネットワーク デバイス プロファイルの名前を入力します。                                                                                          |
| 説明            | ネットワーク デバイス プロファイルの説明を入力します。                                                                                          |
| アイコン (Icon)   | ネットワーク デバイス プロファイルに使用するアイコンを選択します。このアイコンには、選択したベンダーのアイコンがデフォルトで設定されます。<br><br>選択するアイコンは 16 X 16 の PNG ファイルである必要があります。 |
| ベンダー (Vendor) | ネットワーク デバイス プロファイルのベンダーを選択します。<br><br>選択可能なベンダーは、シスコ、Aruba、HP、Motorola、Brocade、Alcatel などです。                          |
| サポートされるプロトコル  |                                                                                                                       |
| RADIUS        | このネットワーク デバイス プロファイルが RADIUS をサポートしている場合は、このチェックボックスをオンにします。                                                          |

| フィールド                                | 説明                                                                                          |
|--------------------------------------|---------------------------------------------------------------------------------------------|
| TACACS+                              | このネットワーク デバイス プロファイルが TACACS+ をサポートしている場合は、このチェックボックスをオンにします。                               |
| TrustSec                             | このネットワーク デバイス プロファイルが TrustSec をサポートしている場合は、このチェックボックスをオンにします。                              |
| RADIUS ディクショナリ (RADIUS Dictionaries) | このプロファイルでサポートされる 1 つ以上の RADIUS ディクショナリを選択します。プロファイルを作成する前に、ベンダー固有の RADIUS ディクショナリをインポートします。 |

### 認証/許可テンプレートの設定

次の表は、[認証/許可 (Authentication/Authorization) ]セクションのフィールドについての説明です。

表 111: 認証/許可の設定

| フィールド                            | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| フロータイプの条件 (Flow Type Conditions) | <p>Cisco ISE では、802.1X、MAC 認証バイパス (MAB) 、およびブラウザベースの Web 認証ログインが、有線ネットワークと無線ネットワークの両方を介した基本的なユーザ認証およびアクセスでサポートされます。</p> <p>このタイプのネットワーク デバイスがサポートする認証ログインのチェックボックスをオンにします。次の 1 つ以上の項目を指定できます。</p> <ul style="list-style-type: none"> <li>• 有線 MAC 認証バイパス (MAB) (Wired MAC authentication bypass (MAB))</li> <li>• 無線 MAB (Wireless MAB)</li> <li>• 有線 802.1x (Wired 802.1X)</li> <li>• 無線 802.1x (Wireless 802.1X)</li> <li>• 有線 Web 認証 (Wired Web Authentication)</li> <li>• 無線 Web 認証 (Wireless Web Authentication)</li> </ul> <p>ネットワーク デバイス プロファイルでサポートされる認証ログインをオンにした後、ログインの条件を指定します。</p> |
| 属性エイリアシング (Attribute Aliasing)   | <p>ポリシー ルールのフレンドリ名としてデバイスのサービスセット識別子 (SSID) を使用する場合は、[SSID] チェックボックスをオンにします。これにより、ポリシー ルールで使用する一貫した名前を作成でき、その名前は複数のデバイスに適用されます。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| ホスト ルックアップ (MAB)                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |



| フィールド                               | 説明                                                                                                                                                                                                                                                                                                         |
|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ホスト ルックアップの処理 (Process Host Lookup) | <p>ネットワーク デバイス プロファイルで使用するホスト ルックアップ用のプロトコルを定義するには、このチェックボックスをオンにします。</p> <p>さまざまなベンダーからのネットワーク デバイスは、MAB 認証を異なる方法で実行します。デバイス タイプに応じて、使用しているプロトコルの [パスワードを確認 (Check Password)] チェックボックス、[Calling-Station-IdがMACアドレスと等しいかを確認 (Checking Calling-Station-Id equals MAC Address)] チェックボックス、またはその両方をオンにします。</p> |
| PAP/ASCII 経由 (Via PAP/ASCII)        | <p>ホスト ルックアップ要求としてネットワーク デバイス プロファイルからの PAP 要求を検出するように Cisco ISE を設定するには、このチェックボックスをオンにします。</p>                                                                                                                                                                                                            |
| CHAP 経由 (Via CHAP)                  | <p>ホスト ルックアップ要求としてネットワーク デバイスからのこのタイプの要求を検出するように Cisco ISE を設定するには、このチェックボックスをオンにします。</p> <p>このオプションによって、CHAP 認証が有効になります。CHAP は、パスワードの暗号化とともにチャレンジ/レスポンス方式を使用します。CHAP は、Microsoft Active Directory では使用できません。</p>                                                                                          |
| EAP-MD5 経由 (EAP-MD5)                | <p>ネットワーク デバイス プロファイルに EAP ベースの MD5 ハッシュ認証を有効にするには、このチェックボックスをオンにします。</p>                                                                                                                                                                                                                                  |

### 権限テンプレートの設定

このネットワーク デバイス プロファイルに使用される VLAN および ACL の権限を定義できます。プロファイルを保存すると、Cisco ISE は設定された各権限に対し許可プロファイルを自動的に生成します。次の表は、[権限 (Permissions)] セクションのフィールドについての説明です。

表 112: 権限の設定

| フィールド               | 説明                                                                                                                                                                                                                                                                                                             |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| VLAN の設定 (Set VLAN) | <p>このネットワーク デバイス プロファイルに VLAN 権限を設定するには、このチェックボックスをオンにします。次のいずれかのオプションを選択します。</p> <ul style="list-style-type: none"> <li>• IETF 802.1X 属性 (IETF 802.1X Attributes) : Internet Engineering Task Force で定義されたデフォルトの RADIUS 属性のセットです。</li> <li>• 一意の属性 (Unique Attributes) : 複数の RADIUS 属性値のペアを指定できます。</li> </ul> |
| ACL の設定 (Set ACL)   | RADIUS 属性をネットワーク デバイス プロファイルの ACL に設定する場合は、このチェックボックスをオンにします。                                                                                                                                                                                                                                                  |

## 許可変更 (CoA) テンプレートの設定

このテンプレートは、CoA がこのタイプのネットワーク デバイスにどのように送信されるかを定義します。次の表は、[許可変更 (CoA) (Change of Authorization (CoA))] セクションのフィールドについての説明です。

表 113: 許可変更 (CoA) の設定

| フィールド                             | 定義 (Definition)                                                                                                                  |
|-----------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| 次による CoA (CoA by)                 | RADIUS により、または SNMP により、ネットワーク デバイス プロファイルに CoA パケットを送信するか、あるいはまったくしないかを選択します。                                                   |
| RADIUS による CoA (CoA by RADIUS)    |                                                                                                                                  |
| デフォルトの CoA ポート (Default CoA Port) | <p>RADIUS CoA を送信するポート。シスコ デバイスのデフォルトポートは 1700 で、他のベンダーのデバイスでは 3799 です。</p> <p>[ネットワークデバイス (Network Device)] ページでこれを上書きできます。</p> |
| タイムアウト間隔 (Timeout Interval)       | CoA の送信後に Cisco ISE が応答を待機する秒数。                                                                                                  |

| フィールド                       | 定義 (Definition)                                                                                                                                                                                                                                                                                                                                                  |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 再試行回数 (Retry Count)         | 最初のタイムアウト後に Cisco ISE が CoA の送信を試行する回数。                                                                                                                                                                                                                                                                                                                          |
| 切断                          | <p>これらのデバイスに接続解除要求を送信する方法を選択します。</p> <ul style="list-style-type: none"> <li>• RFC 5176 (RFC 5176) : 標準のセッション終了の場合はこのチェックボックスをオンにし、RFC 5176 に従って定義されているように、ポートを新しいセッション用に残しておきます。</li> <li>• ポート バウンス (Port Bounce) : セッションを終了して、ポートを再起動するには、このチェックボックスをオンにします。</li> <li>• ポートのシャットダウン (Port Shutdown) : セッションを終了して、ポートをシャットダウンするには、このチェックボックスをオンにします。</li> </ul> |
| 再認証 (Re-authenticate)       | <p>ネットワーク デバイスに再認証要求を送信する方法を選択します。これは現在、シスコデバイスのみでサポートされています。</p> <ul style="list-style-type: none"> <li>• 基本 (Basic) : 標準のセッション再認証の場合はこのチェックボックスをオンにします。</li> <li>• 再実行 (Rerun) : 認証方式によって最初から実行する場合は、このチェックボックスをオンにします。</li> <li>• 最後 (Last) : 最後に成功した認証方式をセッションに使用します。</li> </ul>                                                                             |
| CoA プッシュ (CoA Push)         | ネットワークデバイスがシスコの TrustSec CoA 機能をサポートしない場合は、このオプションを選択して、Cisco ISE が設定の変更をデバイスにプッシュできるようにします。                                                                                                                                                                                                                                                                     |
| SNMP による CoA (CoA by SNMP)  |                                                                                                                                                                                                                                                                                                                                                                  |
| タイムアウト間隔 (Timeout Interval) | CoA の送信後に Cisco ISE が応答を待機する秒数。                                                                                                                                                                                                                                                                                                                                  |

| フィールド               | 定義 (Definition)                                                                                                                                                                                                                                                                                         |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 再試行回数 (Retry Count) | Cisco ISE が CoA の送信を試行する回数。                                                                                                                                                                                                                                                                             |
| NAD ポートの検出          | 関連する RADIUS 属性は、現時点での唯一のオプションです。                                                                                                                                                                                                                                                                        |
| 関連する RADIUS 属性      | NAD ポートを検出する方法を選択します。 <ul style="list-style-type: none"> <li>• Nas-Port</li> <li>• Nas-Port-ID</li> </ul>                                                                                                                                                                                               |
| 切断                  | これらのデバイスに接続解除要求を送信する方法を選択します。 <ul style="list-style-type: none"> <li>• 再認証します。セッションを終了して、ポートを再起動するには、このチェックボックスをオンにします。</li> <li>• ポート バウンス (Port Bounce) : セッションを終了して、ポートを再起動するには、このチェックボックスをオンにします。</li> <li>• ポートのシャットダウン (Port Shutdown) : セッションを終了して、ポートをシャットダウンするには、このチェックボックスをオンにします。</li> </ul> |

### リダイレクトテンプレートの設定

ネットワーク デバイスは、許可プロファイルで設定されている場合、クライアントの HTTP 要求をリダイレクトできます。このテンプレートは、このネットワーク デバイス プロファイルが URL リダイレクトをサポートするかどうかを指定します。デバイス タイプに固有の URL パラメータ名を使用します。

次の表は、[リダイレクト (Redirect) ] セクションのフィールドについての説明です。

表 114: リダイレクトの設定

| フィールド                                | 定義 (Definition)                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| タイプ (Type)                           | <p>ネットワーク デバイス プロファイルが静的または動的 URL リダイレクトをサポートするかを選択します。</p> <p>デバイスがどちらもサポートしていない場合、[未サポート (Not Supported)] を選択し、[設定 (Settings)] &gt; [DHCP および DNS サービス (DHCP &amp; DNS Services)] から VLAN を設定します (詳細については、<a href="#">#unique_347</a>を参照してください)。Cisco ISE が提供する認証 VLAN リダイレクトのシミュレーションの設定に関する詳細については、次を参照してください <a href="#">Cisco ISE でのサードパーティ製ネットワーク デバイスの設定 (256 ページ)</a></p> |
| リダイレクト URL パラメータ名                    |                                                                                                                                                                                                                                                                                                                                                                                    |
| クライアント IP アドレス                       | ネットワーク デバイスがクライアントの IP アドレスに使用するパラメータ名を入力します。                                                                                                                                                                                                                                                                                                                                      |
| クライアント MAC アドレス (Client MAC Address) | ネットワーク デバイスがクライアントの MAC アドレスに使用するパラメータ名を入力します。                                                                                                                                                                                                                                                                                                                                     |
| 元の URL (Originating URL)             | ネットワーク デバイスが元の URL に使用するパラメータ名を入力します。                                                                                                                                                                                                                                                                                                                                              |
| セッション ID                             | ネットワーク デバイスがセッション ID に使用するパラメータ名を入力します。                                                                                                                                                                                                                                                                                                                                            |
| SSID                                 | ネットワーク デバイスがサービスセット識別子 (SSID) に使用するパラメータ名を入力します。                                                                                                                                                                                                                                                                                                                                   |
| ダイナミック URL パラメータ                     |                                                                                                                                                                                                                                                                                                                                                                                    |
| パラメータ                                | 動的 URL リダイレクトを選択する場合は、これらのネットワーク デバイスがリダイレクト URL を作成する方法を指定する必要があります。また、リダイレクト URL がセッション ID またはクライアントの MAC アドレスを使用するかを指定できます。                                                                                                                                                                                                                                                     |

### 詳細設定 (Advanced Settings)

ネットワーク デバイス プロファイルを使用して、ネットワーク デバイスをポリシー ルールで使いやすくするために、多数のポリシー要素を生成できます。これらの要素には、複合条件、許可プロファイル、および許可されているプロトコルが含まれています。

これらの要素を作成するには、[ポリシー要素の作成 (Generate Policy Elements)] ボタンをクリックします。

### 関連トピック

[ネットワーク デバイス プロファイル \(254 ページ\)](#)

[Cisco ISE でのサードパーティ ネットワーク デバイスのサポート \(251 ページ\)](#)

[ネットワーク デバイス プロファイルの作成 \(257 ページ\)](#)

## 外部 RADIUS サーバの設定

次の表では、[外部 RADIUS サーバ (External RADIUS Server)] ページのフィールドについて説明します。これらのフィールドを使用して、RADIUS サーバを設定できます。Cisco ISE が RADIUS サーバとして機能するためには、このページで設定する必要があります。このページのナビゲーションパスは、[管理 (Administration)] > [ネットワーク リソース (Network Resources)] > [外部 RADIUS サーバ (External RADIUS Servers)] です。

表 115: 外部 RADIUS サーバの設定

| フィールド                         | 使用上のガイドライン                                                                                                                                                                                          |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [名前 (Name)]                   | 外部 RADIUS サーバの名前を入力します。                                                                                                                                                                             |
| 説明                            | 外部 RADIUS サーバの説明を入力します。                                                                                                                                                                             |
| ホスト名/アドレス (Host IP)           | 外部 RADIUS サーバの IP アドレスを入力します。                                                                                                                                                                       |
| 共有秘密鍵 (Shared Secret)         | 外部 RADIUS サーバの認証に使用される、Cisco ISE と外部 RADIUS サーバの間の共有秘密を入力します。共有秘密情報は、予期されるテキスト文字列です。ユーザは、ネットワーク デバイスによってユーザ名およびパスワードが認証されるようにこれらの情報を提示する必要があります。ユーザが共有秘密情報を提示するまで、接続は拒否されます。共有秘密情報の長さは、最大 128 文字です。 |
| KeyWrap の有効化 (Enable KeyWrap) | このオプションをオンにすると、Cisco ISE で FIPS 140-2 準拠が有効になり、AES KeyWrap アルゴリズムにより RADIUS プロトコルのセキュリティが強化されます。                                                                                                    |

| フィールド                                                 | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| キー暗号キー (Key Encryption Key)                           | <p>[keyWrap を有効にする (Enable keyWrap) ] チェックボックスをオンにした場合のみ) セッション暗号化 (秘密) に使用される暗号キーを入力します。</p>                                                                                                                                                                                                                                                                                 |
| メッセージオーセンティケーターコードキー (Message Authenticator Code Key) | <p>[keyWrap を有効にする (Enable keyWrap) ] チェックボックスをオンにした場合のみ) RADIUS メッセージ上のキー付き HMAC 計算に使用されるキーを入力します。</p>                                                                                                                                                                                                                                                                       |
| キー入力形式 (Key Input Format)                             | <p>Cisco ISE 暗号キーの入力に使用する形式を指定します。これは、WLAN コントローラ上の設定と一致する必要があります。(指定する値の長さは、次に定義されているキーの最大長と正確に一致している必要があります。これより短い値は許可されません)。</p> <ul style="list-style-type: none"> <li>• [ASCII] : キー暗号キーの長さは 16 文字 (バイト)、メッセージオーセンティケーターコードキーの長さは 20 文字 (バイト) である必要があります。</li> <li>• [16 進数 (Hexadecimal) ] : キー暗号キーの長さは 32 バイトであり、メッセージオーセンティケーターコードキーの長さは 40 バイトである必要があります。</li> </ul> |
| 認証ポート (Authentication Port)                           | RADIUS 認証のポート番号を入力します。値の範囲は 1 ～ 65535 です。デフォルトは 1812 です。                                                                                                                                                                                                                                                                                                                      |
| アカウンティングポート (Accounting Port)                         | RADIUS アカウンティングのポート番号を入力します。値の範囲は 1 ～ 65535 です。デフォルトは 1813 です。                                                                                                                                                                                                                                                                                                                |
| サーバタイムアウト (Server timeout)                            | Cisco ISE が外部 RADIUS サーバからの応答を待機する秒数を入力します。デフォルトは 5 秒です。有効な値は 5 ～ 120 です。                                                                                                                                                                                                                                                                                                     |
| 接続試行回数 (Connection Attempts)                          | Cisco ISE が外部 RADIUS サーバへの接続を試行する回数を入力します。デフォルトは 3 回に設定されています。有効な値は 1 ～ 9 です。                                                                                                                                                                                                                                                                                                 |

#### 関連トピック

[RADIUS プロキシ サーバとして機能する Cisco ISE](#) (696 ページ)

[外部 RADIUS サーバの設定](#) (697 ページ)

## RADIUS サーバ順序

次の表では、RADIUS サーバ順序を作成するために使用する [RADIUS サーバ順序 (RADIUS Server Sequences)] ページのフィールドについて説明します。このページへのナビゲーションパスは、[管理 (Administration)] > [ネットワークリソース (Network Resources)] > [RADIUS サーバ順序 (RADIUS Server Sequences)] > [追加 (Add)] です。

表 116: RADIUS サーバ順序

| フィールド                                                                                                  | 使用上のガイドライン                                                                                                         |
|--------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| [名前 (Name)]                                                                                            | RADIUS サーバ順序の名前を入力します。                                                                                             |
| 説明                                                                                                     | 任意で説明を入力します。                                                                                                       |
| ホスト名/アドレス (Host IP)                                                                                    | 外部 RADIUS サーバの IP アドレスを入力します。                                                                                      |
| ユーザが選択したサービス タイプ (User Selected Service Type)                                                          | [使用可能 (Available)] リスト ボックスで、ポリシー サーバとして使用する外部 RADIUS サーバを選択し、選択した外部 RADIUS サーバを [選択済み (Selected)] リスト ボックスに移動します。 |
| リモート アカウンティング (Remote Accounting)                                                                      | リモート ポリシー サーバでアカウンティングを有効にするには、このチェックボックスをオンにします。                                                                  |
| ローカル アカウンティング (Local Accounting)                                                                       | Cisco ISE でのアカウンティングを有効にするには、このチェックボックスをオンにします。                                                                    |
| 高度な属性設定 (Advanced Attributes Settings)                                                                 |                                                                                                                    |
| サブジェクト名の先頭から最後に出現する区切り文字まで削除 (Strip Start of Subject Name up to the First Occurrence of the Separator) | プレフィクスからユーザ名を取り除くには、このチェックボックスをオンにします。たとえば、サブジェクト名が acme\userA、区切り文字が \ の場合、ユーザ名は userA になります。                     |



| フィールド                                                                                              | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 最初に出現する区切り文字からサブジェクト名の末尾まで削除 (Strip End of Subject Name from the Last Occurrence of the Separator) | <p>サフィックスからユーザ名を取り除くには、このチェックボックスをオンにします。たとえば、サブジェクト名が userA@abc.com、区切り文字が @ の場合、ユーザ名は userA になります。</p> <ul style="list-style-type: none"><li>• NetBIOS または User Principle Name (UPN) フォーマットのユーザ名 (user@domain.com または /domain/user) からユーザ名を抽出するには、これらのストリップ オプションを有効にする必要があります。RADIUS サーバでユーザを認証するために、ユーザ名だけが RADIUS サーバに渡されるためです。</li><li>• \ および @ の両方のストリップ機能をアクティブ化し、Cisco AnyConnect を使用している場合、Cisco ISE は最初に出現する \ を文字列から正確に取り除くことができません。ただし、各ストリップ機能は、Cisco AnyConnect を考慮して設計されているため、個別に使用する場合は動作します。</li></ul> |
| 外部 RADIUS サーバへの要求に含まれる属性を変更する (Modify Attributes in the Request to the External RADIUS Server)     | <p>認証済みの RADIUS サーバとの間で送受信する属性の操作を Cisco ISE に許可するには、このチェックボックスをオンにします。</p> <p>次の属性操作が可能です。</p> <ul style="list-style-type: none"><li>• [追加 (Add)] : RADIUS 要求/応答全体に属性を追加します。</li><li>• [更新 (Update)] : 属性値 (固定または静的) を変更します。または属性を別の属性値 (動的) で置き換えます。</li><li>• [削除 (Remove)] : 属性または属性と値のペアを削除します。</li><li>• [すべて削除 (RemoveAny)] : 存在するすべての属性を削除します。</li></ul>                                                                                                                                                          |

| フィールド                                                                       | 使用上のガイドライン                                                                                                                                                                           |
|-----------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 認証ポリシーに進む (Continue to Authorization Policy)                                | IDストアグループおよび属性の取得に基づいて、プロキシフローを許可ポリシーの実行に誘導して、より詳細な意思決定を行うには、このチェックボックスをオンにします。このオプションを有効にすると、外部RADIUSサーバからの応答に含まれる属性が、認証ポリシーの選択に使用されます。このコンテキストの既存の属性は、AAAサーバの受け入れ応答属性の適切な値で更新されます。 |
| Access-Accept の送信前に属性を変更する (Modify Attributes before send an Access-Accept) | 応答をデバイスに返送する直前に属性を変更するには、このチェックボックスをオンにします。                                                                                                                                          |

#### 関連トピック

[RADIUS プロキシサーバとして機能する Cisco ISE](#) (696 ページ)

[RADIUS サーバ順序の定義](#) (697 ページ)

## NAC マネージャの設定

次の表では、NAC マネージャを追加するために使用できる [新規 NAC Manager (New NAC Manager)] ページのフィールドについて説明します。このページへのナビゲーションパスは、[管理 (Administration)] > [ネットワーク リソース (Network Resources)] > [NAC Managers] です。

表 117: NAC マネージャの設定

| フィールド          | 使用上のガイドライン                                                                               |
|----------------|------------------------------------------------------------------------------------------|
| [名前 (Name)]    | Cisco Access Manager (CAM) の名前を入力します。                                                    |
| ステータス (Status) | CAM への接続を認証する Cisco ISE プロファイルからの REST API 通信を有効にする場合は、[ステータス (Status)] チェックボックスをオンにします。 |
| 説明             | CAM の説明を入力します。                                                                           |

| フィールド                  | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                          |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [IPアドレス (IP Address) ] | <p>CAM の IP アドレスを入力します。Cisco ISE でCAMを作成して保存した後、CAM の IP アドレスを編集することはできません。</p> <p>0.0.0.0 と 255.255.255.255 は、Cisco ISE で CAM の IP アドレスを検証するときに除外され、CAM の [IP アドレス (IP Address) ] フィールドで使用できる有効な IP アドレスではないため、使用できません。</p> <p>(注) ハイ アベイラビリティ構成で CAM のペアが共有する仮想サービス IP アドレスを使用できます。これで、ハイ アベイラビリティ構成で CAM のフェールオーバーをサポートできます。</p> |
| [ユーザ名 (Username) ]     | CAM のユーザインターフェイスにログオンできる CAM 管理者のユーザ名を入力します。                                                                                                                                                                                                                                                                                        |
| [パスワード (Password) ]    | CAM のユーザインターフェイスにログオンできる CAM 管理者のパスワードを入力します。                                                                                                                                                                                                                                                                                       |

#### 関連トピック

[Cisco NAC アプライアンスとの Cisco ISE 統合](#) (794 ページ)

[Cisco Clean Access Manager の追加](#) (795 ページ)

## デバイス ポータルの管理

### デバイス ポータルの設定

#### デバイス ポータルのグローバル設定

[ワーク センター (Work Centers) ] > [BYOD] > [設定 (Settings) ] > [従業員が登録するデバイス (Employee Registered Devices) ] または [管理 (Administration) ] > [デバイス ポータルの管理 (Device Portal Management) ] > [設定 (Settings) ] を選択します。

BYOD ポータルおよびデバイス ポータルの次の一般設定を設定できます。

- [従業員が登録するデバイス (Employee Registered Devices) ] : [従業員を制限 (Restrict employees to) ] に、従業員が登録できるデバイスの最大数を入力します。デフォルトでは、この値は 5 デバイスに設定されています。

- [再試行 URL (Retry URL)] : デバイスを Cisco ISE にリダイレクトするために使用できる URL を [オンボードのための再試行 URL (Retry URL for onboarding)] に入力します。

これらの一般的な設定値を設定したら、これらの設定は会社を設定したすべて BYOD ポータルおよびデバイス ポータルに適用されます。

#### 関連トピック

[従業員が登録するパーソナル デバイス数の制限](#)

[BYOD 登録に再接続する URL の提供](#) (593 ページ)

[分散環境のエンドユーザのデバイス ポータル](#) (584 ページ)

## デバイス ポータルのポータル ID 設定

これらの設定へのナビゲーションパスは、[管理 (Administration)] > [デバイス ポータル管理 (Device Portal Management)] > [ブラックリスト ポータル (Blacklist Portal)]/[クライアント プロビジョニング ポータル (Client Provisioning Portals)]/[BYOD ポータル (BYOD Portals)]/[MDM ポータル (MDM Portals)]/[デバイス ポータル (My Device Portals)] > [作成、編集または複製 (Create, Edit or Duplicate)] > [ポータルの設定およびカスタマイズ (Portals Settings and Customization)] です。

- ポータル名 (Portal Name) : このポータルにアクセスするための一意のポータル名を入力します。このポータル名を、その他のスポンサーやゲスト ポータルおよび非ゲスト ポータル (ブラックリスト、個人所有デバイス持ち込み (BYOD)、クライアント プロビジョニング、モバイル デバイス管理 (MDM)、またはデバイスの各ポータル) に使用しないでください。

この名前は、許可プロファイルのポータルの選択でリダイレクションの選択肢として表示され、ポータルのリストで他のポータルの中から簡単に識別するために使用されます。

- [説明 (Description)] : 任意項目です。
- ポータル テスト URL (Portal test URL) : [保存 (Save)] をクリックした後にリンクとして表示されるシステムにより生成された URL。ポータルをテストするために使用します。

リンクをクリックすると、このポータルの URL を表示する新しいブラウザ タブが開きます。これを有効にするには、ポリシー サービスを含むポリシー サービス ノード (PSN) をオンにする必要があります。ポリシー サービスがオンになっていない場合、PSN は管理者用ポータルのみを表示します。



- (注) テスト ポータルは RADIUS セッションをサポートしていないため、すべてのポータルに対するポータルフローの全体は表示されません。BYOD およびクライアント プロビジョニングは RADIUS セッションに依存するポータルの例です。たとえば、外部 URL へのリダイレクションは機能しません。

- 言語ファイル (Language File) : 各ポータル タイプは、デフォルトで 15 種類の言語をサポートします。これらの言語は、個々のプロパティファイルとして使用できます。これらのファイルは、圧縮された単一の言語ファイル内にまとめてバンドルされています。ポータルで使用する圧縮言語ファイルをエクスポートまたはインポートします。圧縮言語ファイルには、ポータルのテキストを表示するために使用可能な個別の言語ファイルがすべて含まれています。

言語ファイルには、その言語のポータル全体のすべての文字列設定に加え、特定のブラウザのロケール設定 (例: フランス語の場合は fr、fr-fr、fr-ca) へのマッピングが含まれています。1 つの言語ファイルには、翻訳およびローカリゼーションの目的に容易に使用できるように、サポートされるすべての言語が含まれています。

1 つの言語用のブラウザ ロケール設定を変更した場合、変更内容は他のすべてのエンドユーザ Web ポータルに適用されます。たとえば、ホットスポット ゲスト ポータルの French.properties ブラウザ ロケールを fr,fr-fr,fr-ca から fr,fr-fr に変更すると、この変更内容がデバイス ポータルにも適用されます。

[ポータルページのカスタマイズ (Portal Page Customizations) ] タブでいずれかのポータル ページ テキストをカスタマイズすると、警告アイコンが表示されます。警告メッセージは、ポータルのカスタマイズ時に 1 つの言語で行った変更をすべてのサポート対象の言語 プロパティファイルで更新するように注意を促します。ドロップダウンリストのオプションを使用して、手動で警告アイコンが表示されないようにします。また、警告アイコンは、更新された圧縮言語ファイルのインポート後に自動的に表示されなくなります。

•

#### 関連トピック

[許可ポリシー ルールの作成](#) (609 ページ)

[許可プロファイルの作成](#) (609 ページ)

[パーソナル デバイス ポータル](#) (585 ページ)

## ブラックリスト ポータルのポータル設定

この設定のナビゲーションパスは、[管理 (Administration) ] > [デバイス ポータル管理 (Device Portal Management) ] > [ブラックリスト ポータル (Blacklist Portal) ] > [編集 (Edit) ] > [ポータルの動作およびフローの設定 (Portal Behavior and Flow Settings) ] > [ポータル設定 (Portal Settings) ] です

これらの設定を使用して、ユーザ (状況に応じてゲスト、スポンサー、または従業員) に表示される特定のポータルページではなく、ポータル全体に適用される値を指定したり動作を定義したりします。

- [HTTPS ポート (HTTPS port) ] : 8000 ~ 8999 の範囲のポート値を入力します。デフォルト値はすべてのデフォルト ポータルで 8443 です。ただし、ブラックリスト ポータルは 8444 です。この範囲外のポート値を使用してアップグレードした場合は、このページで変更を加えるまで維持されます。このページを変更する場合は、この制限に従うようにポート設定を更新します。

ゲスト ポータルに非ゲスト ポータル (マイ デバイスなど) によって使用されるポートを割り当てると、エラー メッセージが表示されます。

ポスチャ評価と修復についてのみ、クライアントプロビジョニングポータルはポート 8905 および 8909 も使用します。それ以外の場合は、ゲスト ポータルへの割り当てと同じポートを使用します。

同じ HTTPS ポートに割り当てられたポータルは、同じギガビットイーサネットインターフェイスまたは別のインターフェイスを使用できます。これらのポータルが同じポートとインターフェイスの組み合わせを使用している場合、同じ証明書グループタグを使用する必要があります。次に例を示します。

- スポンサー ポータルを例として使用した有効な組み合わせを次に示します。
    - スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書タグ **A**、およびデバイス ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**
    - スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**、およびデバイス ポータル：ポート **8445**、インターフェイス **0**、証明書グループ **B**
    - スポンサー ポータル：ポート **8444**、インターフェイス **1**、証明書グループ **A**、およびブラックリストポータル：ポート **8444**、インターフェイス **0**、証明書グループ **B**
  - 無効な組み合わせには次が含まれます。
    - スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**、およびデバイス ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **B**
    - スポンサー ポータル：ポート **8444**、インターフェイス **0**、証明書タグ **A**、およびブラックリストポータル：ポート **8444**、インターフェイス **0**、証明書グループ **A**
  - [使用可能インターフェイス (Allowed interfaces)] : PAN がポータルの実行に使用できる PSN インターフェイスを選択します。ポータルを開く要求が PAN で行われると、PAN は PSN で使用可能なポートを探します。異なるサブネット上の IP アドレスを使用してイーサネット インターフェイスを設定する必要があります。
- これらのインターフェイスは、ポリシーサービスがオンになっているすべての PSN (VM ベースを含む) で使用可能である必要があります。これは、これらのすべての PSN がゲストセッションの開始時にリダイレクトに使用される可能性があるため、必須要件です。
- イーサネット インターフェイスは、異なるサブネット上の IP アドレスを使用する必要があります。
  - ここで有効にするインターフェイスは、ポリシーサービスがオンになっているときの VM ベースのものを含む、すべての PSN で使用できるものでなければなりません。これは、これらのすべての PSN がゲストセッションの開始時にリダイレクトに使用される可能性があるため必須です。
  - ポータルの証明書のサブジェクト名とサブジェクトの代替名はインターフェイス IP に解決する必要があります。

- ISE CLI で **ip host x.x.x.x yyy.domain.com** を設定して、セカンダリ インターフェイス IP を FQDN にマッピングします。これは、証明書のサブジェクト名とサブジェクトの代替名と一致させるために使用されます。
- ボンディングされた NIC のみが選択されている場合：PSN がポータルを設定しようとする、最初にボンディング インターフェイスを設定しようとする。これが成功しない場合、おそらくは、その PSN でボンディングが設定されていないために、PSN でエラーが記録されて終了します。PSN は物理 インターフェイスでのポータルの開始を試みません。
- **NIC チーミング**またはボンディングは、高可用性（耐障害性）のために2つの個別の NIC を設定できる、O/S 設定オプションです。どちらかの NIC に障害が発生すると、ボンディングされた接続の一部であるもう一方の NIC は、接続を続行します。1 つの NIC がポータル設定に基づきポータルに対して選択されます。
  - 物理 NIC と対応するボンディングされた NIC の両方が設定されている場合：PSN がポータルを設定しようとする、最初にボンディング インターフェイスへ接続しようとする。これが成功しない場合、その PSN にボンドセットアップがなかったことが原因である可能性があるため、PSN は物理 インターフェイスでポータルを開始しようとする。
- [証明書グループ タグ (Certificate group tag)]：ポータルの HTTPS トラフィックに使用する証明書を指定する証明書グループ タグを選択します。
- **表示言語**
  - [ブラウザのロケールを使用する (Use browser locale)]：クライアント ブラウザのロケール設定で指定された言語をポータルの表示言語として使用します。ブラウザ ロケールの言語が ISE でサポートされていない場合は、フォールバック言語が言語ポータルとして使用されます。
  - [フォールバック言語 (Fallback language)]：ブラウザ ロケールから言語を取得できない場合、またはブラウザ ロケール言語が ISE でサポートされていない場合に使用する言語を選択します。
  - [常に使用 (Always use)]：ポータルに使用する表示言語を選択します。この設定は、ユーザのブラウザのロケール オプションを上書きします。

[スポンサーに使用可能な SSID (SSIDs available to sponsors)]：ゲストの訪問にあたり、スポンサーが正しい接続先ネットワークとしてゲストに通知できる、ネットワークの名前または SSID (セッション サービス識別子) を入力します。

## 関連トピック

[ブラックリスト ポータルの編集](#) (598 ページ)

[ブラックリスト ポータル](#) (586 ページ)

[ブラックリスト ポータルの言語ファイルの HTML サポート](#) (1336 ページ)

## BYOD と MDM ポータルのポータル設定

この設定のナビゲーションパスは、[管理 (Administration)] > [デバイス ポータル管理 (Device Portal Management)] > [BYOD ポータルまたは MDM ポータル (BYOD Portals or MDM Portals)] > [作成、編集または複製 (Create, Edit or Duplicate)] > [ポータルの動作およびフローの設定 (Portal Behavior and Flow Settings)] > [ポータル設定 (Portal Settings)] です。

これらを設定して、ポータル ページの動作を定義します。

- [HTTPS ポート (HTTPS port)] : 8000 ~ 8999 の範囲のポート値を入力します。デフォルト値はすべてのデフォルト ポータルで 8443 です。ただし、ブラックリスト ポータルは 8444 です。この範囲外のポート値を使用してアップグレードした場合は、このページで変更を加えるまで維持されます。このページを変更する場合は、この制限に従うようにポート設定を更新します。

ゲスト ポータルに非ゲスト ポータル (マイ デバイスなど) によって使用されるポートを割り当てると、エラー メッセージが表示されます。

ポスチャ評価と修復についてのみ、クライアントプロビジョニングポータルはポート 8905 および 8909 も使用します。それ以外の場合は、ゲスト ポータルへの割り当てと同じポートを使用します。

同じ HTTPS ポートに割り当てられたポータルは、同じギガビットイーサネットインターフェイスまたは別のインターフェイスを使用できます。これらのポータルが同じポートとインターフェイスの組み合わせを使用している場合、同じ証明書グループタグを使用する必要があります。次に例を示します。

- スポンサー ポータルを例として使用した有効な組み合わせを次に示します。
  - スポンサー ポータル : ポート **8443**、インターフェイス **0**、証明書タグ **A**、およびデバイス ポータル : ポート **8443**、インターフェイス **0**、証明書グループ **A**
  - スポンサー ポータル : ポート **8443**、インターフェイス **0**、証明書グループ **A**、およびデバイス ポータル : ポート **8445**、インターフェイス **0**、証明書グループ **B**
  - スポンサー ポータル : ポート **8444**、インターフェイス **1**、証明書グループ **A**、およびブラックリスト ポータル : ポート **8444**、インターフェイス **0**、証明書グループ **B**
- 無効な組み合わせには次が含まれます。
  - スポンサー ポータル : ポート **8443**、インターフェイス **0**、証明書グループ **A**、およびデバイス ポータル : **8443**、インターフェイス **0**、証明書グループ **B**
  - スポンサー ポータル : ポート **8444**、インターフェイス **0**、証明書タグ **A**、およびブラックリスト ポータル : ポート **8444**、インターフェイス **0**、証明書グループ **A**
- [使用可能インターフェイス (Allowed interfaces)] : PAN がポータルの実行に使用できる PSN インターフェイスを選択します。ポータルを開く要求が PAN で行われると、PAN は



PSN で使用可能なポートを探します。異なるサブネット上の IP アドレスを使用してイーサネット インターフェイスを設定する必要があります。

これらのインターフェイスは、ポリシー サービスがオンになっているすべての PSN（VM ベースを含む）で使用可能である必要があります。これは、これらのすべての PSN がゲストセッションの開始時にリダイレクトに使用される可能性があるため、必須要件です。

- イーサネット インターフェイスは、異なるサブネット上の IP アドレスを使用する必要があります。
- ここで有効にするインターフェイスは、ポリシー サービスがオンになっているときの VM ベースのものを含む、すべての PSN で使用できるものでなければなりません。これは、これらのすべての PSN がゲストセッションの開始時にリダイレクトに使用される可能性があるため必須です。
- ポータルの証明書のサブジェクト名とサブジェクトの代替名はインターフェイス IP に解決する必要があります。
- ISE CLI で **ip host x.x.x.x yyy.domain.com** を設定して、セカンダリ インターフェイス IP を FQDN にマッピングします。これは、証明書のサブジェクト名とサブジェクトの代替名と一致させるために使用されます。
- ボンディングされた NIC のみが選択されている場合：PSN がポータルを設定しようとする、最初にボンディングインターフェイスを設定しようとします。これが成功しない場合、おそらく、その PSN でボンディングが設定されていないために、PSN でエラーが記録されて終了します。PSN は物理インターフェイスでのポータルの開始を試みません。
- **NIC チーミング**またはボンディングは、高可用性（耐障害性）のために2つの個別の NIC を設定できる、O/S 設定オプションです。どちらかの NIC に障害が発生すると、ボンディングされた接続の一部であるもう一方の NIC は、接続を続行します。1 つの NIC がポータル設定に基づきポータルに対して選択されます。
  - 物理 NIC と対応するボンディングされた NIC の両方が設定されている場合：PSN がポータルを設定しようとする、最初にボンディングインターフェイスへ接続しようとします。これが成功しない場合、その PSN にボンドセットアップがなかったことが原因である可能性があるため、PSN は物理インターフェイスでポータルを開始しようとします。
- [証明書グループ タグ (Certificate group tag)]：ポータルの HTTPS トラフィックに使用する証明書を指定する証明書グループ タグを選択します。
- エンドポイント ID グループ (Endpoint identity group)：ゲストのデバイスを追跡するためのエンドポイント ID グループを選択します。Cisco ISE はデフォルトとして使用する **GuestEndpoints** のエンドポイント ID グループを提供します。デフォルトを使用しない場合、追加のエンドポイント ID グループを作成することもできます。

従業員のデバイスを追跡するためのエンドポイント ID グループを選択します。Cisco ISE はデフォルトとして使用する **RegisteredDevices** のエンドポイント ID グループを提供しま

す。デフォルトを使用しない場合、追加のエンドポイント ID グループを作成することもできます。

#### • 表示言語

- [ブラウザのロケールを使用する (Use browser locale)] : クライアントブラウザのロケール設定で指定された言語をポータルの表示言語として使用します。ブラウザロケールの言語が ISE でサポートされていない場合は、フォールバック言語が言語ポータルとして使用されます。
- [フォールバック言語 (Fallback language)] : ブラウザロケールから言語を取得できない場合、またはブラウザロケール言語が ISE でサポートされていない場合に使用する言語を選択します。
- [常に使用 (Always use)] : ポータルに使用する表示言語を選択します。この設定は、ユーザのブラウザのロケール オプションを上書きします。

[スポンサーに使用可能な SSID (SSIDs available to sponsors)] : ゲストの訪問にあたり、スポンサーが正しい接続先ネットワークとしてゲストに通知できる、ネットワークの名前または SSID (セッション サービス識別子) を入力します。

#### 関連トピック

[個人所有デバイスの持ち込みポータル](#) (586 ページ)

[BYOD ポータルの作成](#) (600 ページ)

[モバイル デバイス管理ポータル](#) (587 ページ)

[MDM ポータルの作成](#) (605 ページ)

[個人所有デバイスの持ち込みポータルの言語ファイルの HTML サポート](#) (1336 ページ)

[モバイル デバイス管理ポータルの言語ファイルの HTML サポート](#) (1343 ページ)

## BYOD ポータルの BYOD 設定

この設定のナビゲーションパスは、[管理 (Administration)] > [デバイス ポータル管理 (Device Portal Management)] > [BYOD ポータル (BYOD Portals)] > [作成、編集または複製 (Create, Edit or Duplicate)] > [ポータルの動作およびフローの設定 (Portal Behavior and Flow Settings)] > [BYOD 設定 (BYOD Settings)] です。

この設定を使用して、パーソナル デバイスを使用する従業員の個人所有デバイスの持ち込み (BYOD) 機能を有効にし、企業ネットワークにアクセスできるようにします。

| フィールド                                                          | 使用上のガイドライン                                                                             |
|----------------------------------------------------------------|----------------------------------------------------------------------------------------|
| AUP をページに含める/AUP をリンクとして含める (Include an AUP (on page/as link)) | 会社のネットワーク使用の諸条件を、現在ユーザに表示されるページ上のテキストとして、または AUP テキストが含まれる新しいタブまたはウィンドウを開くリンクとして表示します。 |

| フィールド                                                                | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 同意が必要 (Require acceptance)                                           | ユーザのアカウントが完全に有効になる前に、ユーザはAUPに同意する必要があります。[ログイン (Login)] ボタンは、ユーザがAUPを受け入れない場合は有効になりません。ユーザがAUPに同意しない場合、ネットワークにアクセスできません。                                                                                                                                                                                                                                                                              |
| AUP の最後までスクロールが必要 (Require scrolling to end of AUP)                  | このオプションは、[AUP をページに含める (Include an AUP on page)] が有効である場合のみ表示されます。<br><br>ユーザがAUPを最後まで読んだことを確認します。[同意 (Accept)] ボタンは、ユーザがAUPの最後までスクロールするとアクティブになります。                                                                                                                                                                                                                                                  |
| 登録時にデバイス ID フィールドを表示する (Display Device ID field during registration) | 登録プロセス中に、デバイスIDをユーザに表示します。これは、デバイスIDが事前設定されており、BYOD ポータルを使用しているときに変更できない場合も含まれます。                                                                                                                                                                                                                                                                                                                     |
| 元の URL (Originating URL)                                             | ネットワークへの認証に成功すると、可能な場合はユーザのブラウザを、ユーザがアクセスしようとしていた元の Web サイトにリダイレクトします。リダイレクトできない場合は、認証成功ページが表示されます。リダイレクト URL が NAD のアクセス コントロール リストとその NAD の ISE で設定された許可プロファイルにより、PSN のポート 8443 で動作することを確認します。<br><br>Windows、MAC、および Android デバイスの場合、制御はプロビジョニングを実行するセルフプロビジョニングウィザードアプリケーションに渡されます。そのため、これらのデバイスは元の URL にリダイレクトされません。ただし、iOS (dot1X) およびサポート対象外のデバイス (ネットワーク アクセスが許可されている) では、この URL にリダイレクトされます。 |
| 成功ページ (Success page)                                                 | デバイスの登録が成功したことを示すページを表示します。                                                                                                                                                                                                                                                                                                                                                                           |

| フィールド | 使用上のガイドライン                                                    |
|-------|---------------------------------------------------------------|
| URL   | ネットワークへの認証に成功すると、ユーザのブラウザを指定された URL（会社の Web サイトなど）にリダイレクトします。 |



(注) 認証後に外部 URL にゲストをリダイレクトする場合、URL アドレスを解決して、セッションがリダイレクトされるまでに遅延が生じることがあります。

#### 関連トピック

[個人所有デバイスの持ち込みポータル](#)（586 ページ）

[BYOD ポータルの作成](#)（600 ページ）

[個人所有デバイスの持ち込みポータルの言語ファイルの HTML サポート](#)（1336 ページ）

## 証明書プロビジョニング ポータルのポータル設定

これらの設定へのナビゲーションパスは、**[管理 (Administration)] > [デバイス ポータル管理 (Device Portal Management)] > [証明書プロビジョニング ポータル (Certificate Provisioning Portal)] > [作成、編集または複製 (Create, Edit or Duplicate)] > [ポータルの動作およびフローの設定 (Portal Behavior and Flow Settings)] > [ポータル設定 (Portal Settings)]** です。

- **[HTTPS ポート (HTTPS port)]** : 8000 ~ 8999 の範囲のポート値を入力します。デフォルト値はすべてのデフォルト ポータルで 8443 です。ただし、ブラックリスト ポータルは 8444 です。この範囲外のポート値を使用してアップグレードした場合は、このページで変更を加えるまで維持されます。このページを変更する場合は、この制限に従うようにポート設定を更新します。

ゲスト ポータルに非ゲスト ポータル（マイ デバイスなど）によって使用されるポートを割り当てると、エラー メッセージが表示されます。

ポスチャ評価と修復についてのみ、クライアントプロビジョニングポータルはポート 8905 および 8909 も使用します。それ以外の場合は、ゲスト ポータルへの割り当てと同じポートを使用します。

同じ HTTPS ポートに割り当てられたポータルは、同じギガビットイーサネットインターフェイスまたは別のインターフェイスを使用できます。これらのポータルが同じポートとインターフェイスの組み合わせを使用している場合、同じ証明書グループタグを使用する必要があります。次に例を示します。

- スポンサー ポータルを例として使用した有効な組み合わせを次に示します。
  - スポンサー ポータル : ポート **8443**、インターフェイス **0**、証明書タグ **A**、およびデバイス ポータル : ポート **8443**、インターフェイス **0**、証明書グループ **A**
  - スポンサー ポータル : ポート **8443**、インターフェイス **0**、証明書グループ **A**、およびデバイス ポータル : ポート **8445**、インターフェイス **0**、証明書グループ **B**

- スポンサー ポータル：ポート **8444**、インターフェイス **1**、証明書グループ **A**、およびブラックリスト ポータル：ポート **8444**、インターフェイス **0**、証明書グループ **B**
- 無効な組み合わせには次が含まれます。
  - スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**、およびデバイス ポータル： **8443**、インターフェイス **0**、証明書グループ **B**
  - スポンサー ポータル：ポート **8444**、インターフェイス **0**、証明書タグ **A**、およびブラックリスト ポータル：ポート **8444**、インターフェイス **0**、証明書グループ **A**
- [使用可能インターフェイス (Allowed interfaces) ] : PAN がポータルの実行に使用できる PSN インターフェイスを選択します。ポータルを開く要求が PAN で行われると、PAN は PSN で使用可能なポートを探します。異なるサブネット上の IP アドレスを使用してイーサネット インターフェイスを設定する必要があります。

これらのインターフェイスは、ポリシー サービスがオンになっているすべての PSN (VM ベースを含む) で使用可能である必要があります。これは、これらのすべての PSN がゲストセッションの開始時にリダイレクトに使用される可能性があるため、必須要件です。

  - イーサネット インターフェイスは、異なるサブネット上の IP アドレスを使用する必要があります。
  - ここで有効にするインターフェイスは、ポリシー サービスがオンになっているときの VM ベースのものを含む、すべての PSN で使用できるものでなければなりません。これは、これらのすべての PSN がゲストセッションの開始時にリダイレクトに使用される可能性があるため必須です。
  - ポータルの証明書のサブジェクト名とサブジェクトの代替名はインターフェイス IP に解決する必要があります。
  - ISE CLI で **ip host x.x.x.x yyy.domain.com** を設定して、セカンダリ インターフェイス IP を FQDN にマッピングします。これは、証明書のサブジェクト名とサブジェクトの代替名と一致させるために使用されます。
  - ボンディングされた NIC のみが選択されている場合 : PSN がポータルを設定しようとする、最初にボンディング インターフェイスを設定しようとしします。これが成功しない場合、おそらくは、その PSN でボンディングが設定されていないために、PSN でエラーが記録されて終了します。PSN は物理インターフェイスでのポータルの開始を試みません。
  - **NIC チーミング**またはボンディングは、高可用性 (耐障害性) のために2つの個別の NIC を設定できる、O/S 設定オプションです。どちらかの NIC に障害が発生すると、ボンディングされた接続の一部であるもう一方の NIC は、接続を続行します。1 つの NIC がポータル設定に基づきポータルに対して選択されます。
    - 物理 NIC と対応するボンディングされた NIC の両方が設定されている場合 : PSN がポータルを設定しようとする、最初にボンディング インターフェイスへ接続

しようとします。これが成功しない場合、その PSN にボンドセットアップがなかったことが原因である可能性があるため、PSN は物理インターフェイスでポータルを開始しようとします。

- [証明書グループ タグ (Certificate group tag)] : ポータルの HTTPS トラフィックに使用する証明書を指定する証明書グループ タグを選択します。
- [認証方式 (Authentication Method)] : ユーザ認証に使用する ID ソース順序 (ISS) または ID プロバイダー (IdP) を選択します。ISS は、ユーザ クレデンシャルを確認するために順番に検索される ID ストアのリストです。たとえば、内部ゲスト ユーザ、内部ユーザ、Active Directory、LDAP ディレクトリ などがあります。

Cisco ISE には、スポンサー ポータル Sponsor\_Portal\_Sequence 用のデフォルトのスポンサー ID ソース順序が含まれています。

IdP を設定するには、[管理 (Administration)] > [ID の管理 (Identity Management)] > [外部 ID ソース (External Identity Sources)] > [SAML ID プロバイダー (SAML Id Providers)] の順に選択します。

ID ソース順序を設定するには、[管理 (Administration)] > [ID の管理 (Identity Management)] > [ID ソース順序 (Identity Source Sequences)] の順に選択します。

- [承認済みグループの設定 (Configure Authorized Groups)] : 証明書を生成してそれを [選択済み (Chosen)] ボックスに移動するための権限を付与するユーザ ID グループを選択します。
- [完全修飾ドメイン名 (FQDN) (Fully Qualified Domain Name (FQDN))] : スポンサーまたはデバイス ポータルに対応する 1 つの固有の FQDN またはホスト名を入力します。たとえば、**sponsorportal.yourcompany.com, sponsor** と入力することで、ユーザはブラウザにこれらのいずれかを入力すると、スポンサー ポータルが表示されます。カンマを使用して名前を区切りますが、エントリ間にスペースを挿入しないでください。

デフォルトの FQDN を変更する場合は、次を実行します。

- DNS を更新して、新しい URL の FQDN が有効なポリシー サービス ノード (PSN) の IP アドレスに解決するようにします。PSN のプールを提供するロード バランサの仮想 IP アドレスを指定することもできます。
- 名前の不一致による証明書の警告メッセージを回避するために、Cisco ISE PSN のローカル サーバ証明書のサブジェクト代替名 (SAN) 属性に、カスタマイズされた URL の FQDN またはワイルドカードを含めます。
- [アイドル タイムアウト (Idle timeout)] : ポータルでアクティビティがない場合にユーザをログアウトするまでに Cisco ISE が待機する時間 (分) を入力します。有効な範囲は 1 ~ 30 分です。

## ログイン ページの設定 (Login Page Settings)

- [頻度制限までの最大ログイン試行失敗数 (Maximum failed login attempts before rate limiting)] : Cisco ISE がアカウントのスロットルを開始するまでの単一のブラウザセッションからのログイン試行失敗回数を指定します。これにより、アカウントのロックアウトは起きません。スロットル率は、[頻度制限時のログイン試行間隔 (Time between login attempts when rate limiting)] で設定されます。
- [AUP を含める (Include an AUP)] : フローに利用規約ページを追加します。AUP をページに追加したり、別のページへのリンクを設定することができます。これを追加すると、右側のフローの画像が変わります。
  - [同意が必要 (require acceptance)] : フローを続行する前に、ユーザが AUP に同意するように強制します。
- 

## 利用規定 (AUP) ページ設定 (Acceptable Use Policy (AUP) Page Settings)

- [AUP ページを含める (Include an AUP page)] : 会社のネットワーク使用諸条件を、別のページでユーザに表示します。
- [従業員に別の AUP を使用する (Use different AUP for employees)] : 従業員専用 to 別の AUP およびネットワーク使用諸条件を表示します。このオプションを選択すると、[従業員用の AUP をスキップ (Skip AUP for employees)] は選択できません。
- [従業員用の AUP をスキップ (Skip AUP for employees)] : 従業員は、ネットワークにアクセスする前に AUP に同意する必要はありません。このオプションを選択すると、[従業員に別の AUP を使用する (Use different AUP for employees)] は選択できません。
- [同意が必要 (Require acceptance)] : ユーザのアカウントが完全に有効になる前に、ユーザは AUP に同意する必要があります。[ログイン (Login)] ボタンは、ユーザが AUP を受け入れない場合は有効になりません。ユーザが AUP に同意しない場合、ネットワークにアクセスできません。
- [AUP の最後までスクロールが必要 (Require scrolling to end of AUP)] : [AUP をページに含める (Include an AUP on page)] を有効にした場合にのみ、このオプションが表示されます。

ユーザが AUP を最後まで読んだことを確認します。[同意 (Accept)] ボタンは、ユーザが AUP の最後までスクロールするとアクティブになります。AUP がユーザに表示された場合に設定します。

- [初回のログインのみ (On first login only)] : ユーザが初めてネットワークまたはポータルにログインしたときに AUP を表示します。
- [ログインごと (On every login)] : ユーザがネットワークまたはポータルにログインするごとに、AUP を表示します。
- [\_\_ 日ごと (初回のログインから) (Every \_\_ days (starting at first login))] : ネットワークやポータルにユーザが初めてログインした後は、AUP を定期的に表示します。

.

### 関連トピック

[証明書プロビジョニング ポータル](#) (586 ページ)

[クライアント プロビジョニング ポータルの作成](#) (602 ページ)

[証明書プロビジョニング ポータルの言語ファイルの HTML サポート](#) (1337 ページ)

## クライアント プロビジョニング ポータルのポータル設定

これらの設定へのナビゲーションパスは、**[管理 (Administration)] > [デバイス ポータル管理 (Device Portal Management)] > [クライアント プロビジョニング ポータル (Client Provisioning Portals)] > [作成、編集、複製または削除 (Create, Edit, Duplicate, or Delete)] > [ポータルの動作およびフローの設定 (Portal Behavior and Flow Settings)]** です。

### ポータル設定

- **HTTPS ポート (HTTPS Port)** : 8000 ~ 8999 の範囲のポート値を入力します。デフォルト値はすべてのデフォルト ポータルで 8443 です。ただし、ブラックリスト ポータルは 8444 です。この範囲外のポート値を使用してアップグレードした場合は、このページで変更を加えるまで維持されます。このページを変更する場合、この制限に従うようにポート設定を変更する必要があります。
- **使用可能インターフェイス (Allowed interfaces)** : ポータルを実行できる PSN インターフェイスを選択します。PSN で使用可能なインターフェイスを備えた PSN のみがポータルを作成できます。物理およびボンディングされたインターフェイスの任意の組み合わせを設定できます。これは PSN 全体の設定です。すべてのポータルはこれらのインターフェイスでのみ動作し、このインターフェイス設定はすべての PSN に適用されます。
  - 異なるサブネット上の IP アドレスを使用してイーサネット インターフェイスを設定する必要があります。
  - ここで有効にするインターフェイスは、ポリシーサービスがオンになっているときの VM ベースのものを含む、すべての PSN で使用できるものでなければなりません。これは、これらのすべての PSN がゲスト セッションの開始時にリダイレクトに使用される可能性があるため必須です。
  - ポータルの証明書のサブジェクト名とサブジェクトの代替名は、インターフェイス IP に解決される必要があります。
  - ISE CLI の `ip host x.x.x.x yyy.domain.com` をセカンダリ インターフェイス IP と FQDN をマッピングするように設定します。これは証明書のサブジェクト名/サブジェクトの代替名を一致させるために使用されます。
  - ボンディングされた NIC のみが選択されている場合 : PSN がポータルを設定しようとする、最初にボンディングインターフェイスを設定しようとし、これが成功しない場合、その PSN にボンドセットがなかったことが原因である可能性があるため、PSN はエラーを記録して終了します。物理インターフェイスでポータルを開始しようとはしません。



- **NIC チーミング**またはボンディングは、高可用性（耐障害性）のために2つの個別のNICを設定できる、O/S 設定オプションです。どちらかのNICに障害が発生すると、ボンディングされた接続の一部であるもう一方のNICは、接続を続行します。1つのNICがポータル設定に基づきポータルに対して選択されます。

- 物理NICと対応するボンディングされたNICの両方が設定されている場合：PSNがポータルを設定しようとする、最初にボンディングインターフェイスへ接続しようとします。これが成功しない場合、そのPSNにボンドセットアップがなかったことが原因である可能性があるため、PSNは物理インターフェイスでポータルを開始しようとします。

- **証明書グループタグ (Certificate group tag)** : ポータルのHTTPSトラフィックに使用する証明書グループのグループタグを選択します。
- **[認証方式 (Authentication Method)]** : ユーザ認証に使用するIDソース順序 (ISS) またはIDプロバイダー (IdP) を選択します。ISSは、ユーザクレデンシャルを確認するために順番に検索されるIDストアのリストです。たとえば、内部ゲストユーザ、内部ユーザ、Active Directory、LDAP などがあります。

Cisco ISE には、クライアントプロビジョニングポータル用のデフォルトのクライアントプロビジョニングIDソース順序 `Certificate_Portal_Sequence` が含まれています。

- **完全修飾ドメイン名 (FQDN) (Fully Qualified Domain Name (FQDN))** : クライアントプロビジョニングポータル用に少なくとも1つの一意のFQDN、ホスト名、またはその両方を入力します。たとえば、「`provisionportal.yourcompany.com`」と入力した場合、ユーザはこれらのいずれかをブラウザに入力して証明書プロビジョニングポータルに到達できます。
- DNSを更新して、新しいURLのFQDNが有効なポリシーサービスノード (PSN) のIPアドレスに確実に解決するようにします。PSNのプールを提供するロードバランサの仮想IPアドレスを指定することもできます。
- 名前の不一致による証明書の警告メッセージを回避するために、Cisco ISE PSNのローカルサーバ証明書のサブジェクト代替名 (SAN) 属性に、カスタマイズされたURLのFQDNまたはワイルドカードを含めます。



(注) URLリダイレクトなしのクライアントプロビジョニングの場合、[完全修飾ドメイン名 (FQDN) (Fully Qualified Domain Name (FQDN))] フィールドに入力するポータル名は、DNS設定で設定されている必要があります。URLリダイレクトなしのクライアントプロビジョニングを有効にするため、このURLをユーザに通知する必要があります。

- **アイドルタイムアウト (Idle timeout)** : ポータルでアクティビティがない場合にユーザをログアウトするまでに Cisco ISE が待機する時間 (分) を入力します。有効な範囲は1 ~ 30 分です。



- (注) クライアントプロビジョニングポータルではポート番号と証明書を定義できます。これにより、ホストはクライアントプロビジョニングとポスチャに同じ証明書をダウンロードすることを許可します。ポータル証明書が正式な認証局により署名されている場合、セキュリティ警告は表示されません。自己署名証明書の場合、ポータルと Cisco AnyConnect Posture コンポーネントの両方でセキュリティ警告を受け取ります。

### ログイン ページの設定 (Login Page Settings)

- [ログインの有効化 (Enable Login)] : クライアントプロビジョニングポータルのログイン手順を有効にするには、このチェックボックスを選択します
- [頻度制限までの最大ログイン試行失敗数 (Maximum failed login attempts before rate limiting)] : 単一のブラウザセッションからのログイン試行失敗回数を指定します。この回数を超過すると、Cisco ISE はログイン試行を実行できる頻度を意図的に低下させて、追加のログイン試行を防ぎます。ログイン失敗がこの回数に達した後のログイン試行の間隔は、[頻度制限時のログイン試行間隔 (Time between login attempts when rate limiting)] で指定されます。
- [頻度制限時のログイン試行間隔 (Time between login attempts when rate limiting)] : [頻度制限までの最大ログイン試行失敗数 (Maximum failed login attempts before rate limiting)] で定義された回数のログインの失敗後に、ユーザが再度ログインを試行するまでに待機する必要がある時間を分単位で設定します。
- [AUP をページに含める/AUP をリンクとして含める (Include an AUP (on page/as link))] : 会社のネットワーク使用の諸条件を、現在ユーザに表示されるページ上のテキストとして、または AUP テキストが含まれる新しいタブまたはウィンドウを開くリンクとして表示します。
- [同意が必要 (Require acceptance)] : ポータルにアクセスする前にユーザが AUP を受け入れることを要求します。[ログイン (Login)] ボタンは、ユーザが AUP を受け入れない場合は有効になりません。AUP を受け入れないユーザは、ポータルにアクセスできません。
- [AUP の最後までスクロールが必要 (Require scrolling to end of AUP)] : [AUP をページに含める (Include an AUP on page)] を有効にした場合にのみ、このオプションが表示されます。ユーザが AUP を最後まで読んだことを確認します。[同意 (Accept)] ボタンは、ユーザが AUP の最後までスクロールするとアクティブになります。

### 利用規定 (AUP) ページ設定 (Acceptable Use Policy (AUP) Page Settings)

- [AUP を含める (Include an AUP)] : 会社のネットワーク使用諸条件を、別のページでユーザに表示します。
- [AUP の最後までスクロールが必要 (Require scrolling to end of AUP)] : ユーザが AUP を完全に読んだことを確認します。[同意 (Accept)] ボタンは、ユーザが AUP の最後までスクロールするとアクティブになります。

- [初回のログインのみ (On first login only)] : ユーザがネットワークまたはポータルに初めてログインしたときのみ、AUP を表示します。
- [ログインごと (On every login)] : ユーザがネットワークまたはポータルにログインするごとに、AUP を表示します。
- [\_\_ 日ごと (初回のログインから) (Every \_\_\_\_ days (starting at first login))] : ネットワークやポータルにユーザが初めてログインした後は、AUP を定期的に表示します。

### ポストログイン バナー ページ設定 (Post-Login Banner Page Settings)

[ポストログイン バナー ページを含める (Include a Post-Login Banner page)] : ユーザが正常にログインした後、ネットワーク アクセスを付与される前に追加情報を表示します。

### パスワード変更設定 (Change Password Settings)

[内部ユーザに自身のパスワードの変更を許可する (Allow internal users to change their own passwords)] : 従業員がクライアントプロビジョニングポータルにログインして、自分のパスワードを変更できるようにします。これは、アカウントが Cisco ISE データベース保存されている従業員に適用され、Active Directory や LDAP などの外部データベースに保存されている場合には適用されません。

#### 関連トピック

[クライアントプロビジョニングポータル \(587 ページ\)](#)

[クライアントプロビジョニングポータルの作成 \(603 ページ\)](#)

[クライアントプロビジョニングポータルの言語ファイルのHTMLサポート \(1338 ページ\)](#)

## MDM ポータルの従業員のモバイル デバイス管理設定

これらの設定へのナビゲーションパスは、[管理 (Administration)] > [デバイス ポータル管理 (Device Portal Management)] > [MDM ポータル (MDM Portals)] > [作成、編集または複製 (Create, Edit or Duplicate)] > [ポータルの動作およびフローの設定 (Portal Behavior and Flow Settings)] > [従業員のモバイル デバイス管理設定 (Employee Mobile Device Management Settings)] です。

これらの設定を使用して、MDMポータルを使用する従業員のモバイルデバイス管理 (MDM) 機能を有効にし、AUP エクスペリエンスを定義します。

| フィールド                                                          | 使用上のガイドライン                                                                           |
|----------------------------------------------------------------|--------------------------------------------------------------------------------------|
| AUP をページに含める/AUP をリンクとして含める (Include an AUP (on page/as link)) | 会社のネットワーク使用の諸条件を、現在ユーザに表示されるページ上のテキストとして、またはAUPテキストが含まれる新しいタブまたはウィンドウを開くリンクとして表示します。 |

| フィールド                                               | 使用上のガイドライン                                                                                                                                               |
|-----------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| 同意が必要 (Require acceptance)                          | ユーザのアカウントが完全に有効になる前に、ユーザはAUPに同意する必要があります。[ログイン (Login)] ボタンは、ユーザが AUP を受け入れない場合は有効になりません。ユーザが AUP に同意しない場合、ネットワークにアクセスできません。                             |
| AUP の最後までスクロールが必要 (Require scrolling to end of AUP) | このオプションは、[AUP をページに含める (Include an AUP on page)] が有効である場合のみ表示されます。<br><br>ユーザが AUP を最後まで読んだことを確認します。[同意 (Accept)] ボタンは、ユーザが AUP の最後までスクロールするとアクティブになります。 |

#### 関連トピック

[モバイル デバイス管理ポータル](#) (587 ページ)

[MDM ポータルの作成](#) (605 ページ)

[Mobile Device Manager と Cisco ISE との相互運用性](#) (8 ページ)

## デバイス ポータルのポータル設定

これらの設定へのナビゲーションパスは、[管理 (Administration)] > [デバイス ポータル管理 (Device Portal Management)] > [デバイス ポータル (My Devices Portals)] > [作成、編集または複製 (Create, Edit or Duplicate)] > [ポータルの動作およびフローの設定 (Portal Behavior and Flow Settings)] > [ポータル設定 (Portal Settings)] です。

- [HTTPS ポート (HTTPS port)] : 8000 ~ 8999 の範囲のポート値を入力します。デフォルト値はすべてのデフォルトポータルで 8443 です。ただし、ブラックリストポータルは 8444 です。この範囲外のポート値を使用してアップグレードした場合は、このページで変更を加えるまで維持されます。このページを変更する場合は、この制限に従うようにポート設定を更新します。

ゲストポータルに非ゲストポータル (マイ デバイスなど) によって使用されるポートを割り当てると、エラーメッセージが表示されます。

ポスチャ評価と修復についてのみ、クライアントプロビジョニングポータルはポート 8905 および 8909 も使用します。それ以外の場合は、ゲストポータルへの割り当てと同じポートを使用します。

同じ HTTPS ポートに割り当てられたポータルは、同じギガビットイーサネットインターフェイスまたは別のインターフェイスを使用できます。これらのポータルが同じポートとインターフェイスの組み合わせを使用している場合、同じ証明書グループタグを使用する必要があります。次に例を示します。

- スポンサーポータルを例として使用した有効な組み合わせを次に示します。

- スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書タグ **A**、およびデバイス ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**
  - スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**、およびデバイス ポータル：ポート **8445**、インターフェイス **0**、証明書グループ **B**
  - スポンサー ポータル：ポート **8444**、インターフェイス **1**、証明書グループ **A**、およびブラックリスト ポータル：ポート **8444**、インターフェイス **0**、証明書グループ **B**
- 無効な組み合わせには次が含まれます。
- スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**、およびデバイス ポータル： **8443**、インターフェイス **0**、証明書グループ **B**
  - スポンサー ポータル：ポート **8444**、インターフェイス **0**、証明書タグ **A**、およびブラックリスト ポータル：ポート **8444**、インターフェイス **0**、証明書グループ **A**
- [使用可能インターフェイス (Allowed interfaces) ] : PAN がポータルの実行に使用できる PSN インターフェイスを選択します。ポータルを開く要求が PAN で行われると、PAN は PSN で使用可能なポートを探します。異なるサブネット上の IP アドレスを使用してイーサネット インターフェイスを設定する必要があります。
- これらのインターフェイスは、ポリシー サービスがオンになっているすべての PSN (VM ベースを含む) で使用可能である必要があります。これは、これらのすべての PSN がゲストセッションの開始時にリダイレクトに使用される可能性があるため、必須要件です。
- イーサネット インターフェイスは、異なるサブネット上の IP アドレスを使用する必要があります。
  - ここで有効にするインターフェイスは、ポリシー サービスがオンになっているときの VM ベースのものを含む、すべての PSN で使用できるものでなければなりません。これは、これらのすべての PSN がゲストセッションの開始時にリダイレクトに使用される可能性があるため必須です。
  - ポータルの証明書のサブジェクト名とサブジェクトの代替名はインターフェイス IP に解決する必要があります。
  - ISE CLI で **ip host x.x.x.x yyy.domain.com** を設定して、セカンダリ インターフェイス IP を FQDN にマッピングします。これは、証明書のサブジェクト名とサブジェクトの代替名と一致させるために使用されます。
  - ボンディングされた NIC のみが選択されている場合 : PSN がポータルを設定しようとする、最初にボンディングインターフェイスを設定しようとし、これが成功しない場合、おそらく、その PSN でボンディングが設定されていないために、PSN でエラーが記録されて終了します。PSN は物理インターフェイスでのポータルの開始を試みません。

- **NIC チーミング**または**ボンディング**は、高可用性（耐障害性）のために2つの個別のNICを設定できる、O/S 設定オプションです。どちらかのNICに障害が発生すると、ボンディングされた接続の一部であるもう一方のNICは、接続を続行します。1つのNICがポータル設定に基づきポータルに対して選択されます。

- 物理NICと対応するボンディングされたNICの両方が設定されている場合：PSNがポータルを設定しようとする、最初にボンディングインターフェイスへ接続しようとします。これが成功しない場合、そのPSNにボンドセットアップがなかったことが原因である可能性があるため、PSNは物理インターフェイスでポータルを開始しようとします。

- [証明書グループ タグ (Certificate group tag)] : ポータルの HTTPS トラフィックに使用する証明書を指定する証明書グループ タグを選択します。
- [完全修飾ドメイン名 (FQDN) (Fully Qualified Domain Name (FQDN))] : スポンサーまたはデバイス ポータルに対応する1つの固有のFQDNまたはホスト名を入力します。たとえば、**sponsorportal.yourcompany.com**, **sponsor** と入力することで、ユーザはブラウザにこれらのいずれかを入力すると、スポンサーポータルが表示されます。カンマを使用して名前を区切りますが、エントリ間にスペースを挿入しないでください。

デフォルトのFQDNを変更する場合は、次を実行します。

- DNSを更新して、新しいURLのFQDNが有効なポリシー サービス ノード (PSN) のIPアドレスに解決するようにします。PSNのプールを提供するロード バランサの仮想IPアドレスを指定することもできます。
- 名前の不一致による証明書の警告メッセージを回避するために、Cisco ISE PSNのローカルサーバ証明書のサブジェクト代替名 (SAN) 属性に、カスタマイズされたURLのFQDNまたはワイルドカードを含めます。

- [認証方式 (Authentication Method)] : ユーザ認証に使用するIDソース順序 (ISS) またはIDプロバイダー (IdP) を選択します。ISSは、ユーザ クレデンシャルを確認するために順番に検索されるIDストアのリストです。たとえば、内部ゲスト ユーザ、内部ユーザ、Active Directory、LDAP ディレクトリ などがあります。

Cisco ISE には、スポンサーポータル Sponsor\_Portal\_Sequence 用のデフォルトのスポンサーIDソース順序が含まれています。

IdPを設定するには、[管理 (Administration)] > [IDの管理 (Identity Management)] > [外部IDソース (External Identity Sources)] > [SAML ID プロバイダー (SAML Id Providers)] の順に選択します。

IDソース順序を設定するには、[管理 (Administration)] > [IDの管理 (Identity Management)] > [IDソース順序 (Identity Source Sequences)] の順に選択します。

- エンドポイント ID グループ (Endpoint identity group) : ゲストのデバイスを追跡するためのエンドポイント ID グループを選択します。Cisco ISE はデフォルトとして使用する **GuestEndpoints** のエンドポイント ID グループを提供します。デフォルトを使用しない場合、追加のエンドポイント ID グループを作成することもできます。

従業員のデバイスを追跡するためのエンドポイント ID グループを選択します。Cisco ISE はデフォルトとして使用する **RegisteredDevices** のエンドポイント ID グループを提供します。デフォルトを使用しない場合、追加のエンドポイント ID グループを作成することもできます。

- \_\_日に達した場合にこの ID グループ内のエンドポイントを消去する（Purge endpoints in this identity group when they reach \_\_ days）：Cisco ISE データベースから消去されるまでの、ユーザのデバイスの登録からの日数を変更します。消去は毎日実行され、消去アクティビティは全体的な消去タイミングと同期されます。変更は、このエンドポイント ID グループ全体に適用されます。

その他のポリシー条件に基づいてエンドポイント消去ポリシーに変更が加えられた場合、この設定は使用できなくなります。

- [アイドル タイムアウト（Idle timeout）]：ポータルでアクティビティがない場合にユーザをログアウトするまでに Cisco ISE が待機する時間（分）を入力します。有効な範囲は 1 ～ 30 分です。

- **表示言語**

- [ブラウザのロケールを使用する（Use browser locale）]：クライアント ブラウザのロケール設定で指定された言語をポータルの表示言語として使用します。ブラウザ ロケールの言語が ISE でサポートされていない場合は、フォールバック言語が言語ポータルとして使用されます。

- [フォールバック言語（Fallback language）]：ブラウザ ロケールから言語を取得できない場合、またはブラウザ ロケール言語が ISE でサポートされていない場合に使用する言語を選択します。

- [常に使用（Always use）]：ポータルに使用する表示言語を選択します。この設定は、ユーザのブラウザのロケール オプションを上書きします。

[スポンサーに使用可能な SSID（SSIDs available to sponsors）]：ゲストの訪問にあたり、スポンサーが正しい接続先ネットワークとしてゲストに通知できる、ネットワークの名前または SSID（セッション サービス識別子）を入力します。

## 関連トピック

[デバイス ポータル](#)（588 ページ）

[デバイス ポータルの作成](#)（607 ページ）

# デバイス ポータルのログイン ページ設定

## デバイス ポータルのログイン ページ設定

- [頻度制限までの最大ログイン試行失敗数（Maximum failed login attempts before rate limiting）]：Cisco ISE がアカウントのスロットルを開始するまでの単一のブラウザ セッションからのログイン試行失敗回数を指定します。これにより、アカウントのロックアウト

トは起きません。スロットル率は、[頻度制限時のログイン試行間隔（Time between login attempts when rate limiting）] で設定されます。

- [頻度制限までの最大ログイン試行失敗数（Maximum failed login attempts before rate limiting）] : Cisco ISE がアカウントのスロットルを開始するまでの単一のブラウザセッションからのログイン試行失敗回数を指定します。これにより、アカウントのロックアウトは起きません。スロットル率は、[頻度制限時のログイン試行間隔（Time between login attempts when rate limiting）] で設定されます。
- [AUP を含める（Include an AUP）] : フローに利用規約ページを追加します。AUP をページに追加したり、別のページへのリンクを設定することができます。これを追加すると、右側のフローの画像が変わります。
  - [同意が必要（require acceptance）] : フローを続行する前に、ユーザが AUP に同意するように強制します。

•

#### 関連トピック

[デバイス ポータル](#)（588 ページ）

[デバイス ポータルの作成](#)（607 ページ）

[デバイス ポータルおよびエンドポイント アクティビティのモニタ](#)（611 ページ）

## デバイス ポータルの利用規定（AUP） ページ設定

このページのナビゲーションパスは、[ワーク センター（Work Centers）] > [管理（Administration）] > [デバイス ポータル管理（Device Portal Management）] > [デバイス ポータル（My Devices Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [利用規定（AUP） ページ設定（Acceptable Use Policy (AUP) Page Settings）] です。

これらの設定を使用して、ユーザ（状況に応じてゲスト、スポンサーまたは従業員）に対して AUP エクスペリエンスを定義します。

| フィールド                                              | 使用上のガイドライン                                                                    |
|----------------------------------------------------|-------------------------------------------------------------------------------|
| AUP ページを含める（Include an AUP page）                   | 会社のネットワーク使用諸条件を、別のページでユーザに表示します。                                              |
| AUP の最後までスクロールが必要（Require scrolling to end of AUP） | ユーザが AUP を最後まで読んだことを確認します。[同意（Accept）] ボタンは、ユーザが AUP の最後までスクロールするとアクティブになります。 |
| 初回のログインのみ（On first login only）                     | ユーザがネットワークまたはポータルに初めてログインしたときのみ、AUP を表示します。                                   |
| ログインごと（On every login）                             | ユーザがネットワークまたはポータルにログインするごとに、AUP を表示します。                                       |



| フィールド                                                      | 使用上のガイドライン                                   |
|------------------------------------------------------------|----------------------------------------------|
| __ 日ごと（初回のログインから）（Every __ days (starting at first login)） | ユーザがネットワークまたはポータルに初めてログインした後に、定期的にAUPを表示します。 |

#### 関連トピック

[デバイス ポータル](#)（588 ページ）

[デバイス ポータルの作成](#)（607 ページ）

## デバイス ポータルのポストログイン バナー ページ設定

このページのナビゲーションパスは、**[管理（Administration）]** > **[デバイス ポータル管理（Device Portal Management）]** > **[デバイス ポータル（My Devices Portals）]** > **[作成、編集または複製（Create, Edit or Duplicate）]** > **[ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）]** > **[ポストログイン バナー ページ設定（Post-Login Banner Page Settings）]** です。

これらの設定を使用して、正常なログイン後にユーザ（状況に応じてゲスト、スポンサーまたは従業員）に追加情報を通知します。

| フィールド                                                     | 使用上のガイドライン                                    |
|-----------------------------------------------------------|-----------------------------------------------|
| ポストログイン バナー ページを含める<br>（Include a Post-Login Banner page） | ユーザが正常にログインした後、ネットワーク アクセスを付与される前に追加情報を表示します。 |

#### 関連トピック

[デバイス ポータル](#)（588 ページ）

[デバイス ポータルの作成](#)（607 ページ）

## デバイス ポータルの従業員によるパスワード変更の設定

このページへのナビゲーションパスは、**[管理（Administration）]** > **[デバイス ポータル管理（Device Portal Management）]** > **[デバイス ポータル（My Devices Portals）]** > **[作成、編集または複製（Create, Edit or Duplicate）]** > **[ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）]** > **[従業員のパスワード変更設定（Employee Change Password Settings）]** です。これらの設定を使用して、デバイス ポータルを使用している従業員のパスワード要件を定義します。

従業員のパスワードポリシーを設定するには、**[管理 (Administration)] > [ID の管理 (Identity Management)] > [設定 (Settings)] > [ユーザ名パスワード ポリシー (Username Password Policy)]** を選択します。

| フィールド                                                            | 使用上のガイドライン                                                                                                                                               |
|------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| 内部ユーザにパスワードの変更を許可する<br>(Allow internal users to change password) | 従業員が、デバイス ポータルにログインした後で、自分のパスワードを変更することを許可します。<br><br>これは、アカウントが Cisco ISE データベース保存されている従業員に適用され、Active Directory や LDAP などの外部データベースに保存されている場合には適用されません。 |

#### 関連トピック

[デバイス ポータルの作成 \(607 ページ\)](#)

[ポータルでの UTF-8 文字のサポート \(30 ページ\)](#)

## デバイス ポータルのデバイス管理設定

これらの設定へのナビゲーションパスは、**[管理 (Administration)] > [デバイス ポータル管理 (Device Portal Management)] > [デバイス ポータル (My Devices Portals)] > [作成、編集または複製 (Create, Edit or Duplicate)] > [ポータル ページのカスタマイズ (Portal Page Customization)] > [デバイスの管理 (Manage Device)]** です。

[ページのカスタマイズ (Page Customizations)] で、デバイス ポータルの [アカウントの管理 (Manage Accounts)] タブに表示される、メッセージ、タイトル、コンテンツ、手順、およびフィールドやボタンのラベルをカスタマイズできます。

[設定 (Settings)] では、このデバイス ポータルを使用する従業員が各自の登録されたパーソナル デバイスで実行可能なアクションを指定できます。

表 118: デバイス ポータルのデバイス管理設定

| フィールド     | 使用上のガイドライン                                                                                                                             |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------|
| 紛失 (Lost) | すべてのデバイス。<br><br>デバイスを紛失したことを従業員が示すことができるようにします。このアクションは、デバイス ポータルのデバイスのステータスを [紛失 (Lost)] に更新し、ブラックリストのエンドポイントの ID グループにそのデバイスを追加します。 |

| フィールド          | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 復元 (Reinstate) | <p>すべてのデバイス。</p> <p>このアクションでは、ブラックリストに記載されているか、紛失したか、または盗難されたデバイスを復元し、そのステータスを最後の既知の値にリセットします。このアクションでは、ネットワークに接続する前に追加プロビジョニングを実行する必要があるため、盗難デバイスのステータスを [未登録 (Not Registered) ] にリセットします。</p> <p>ブラックリストに記載されているデバイスを従業員が復元できないようにする場合は、デバイスポータルでこのオプションを有効にしないでください。</p>                                                                                                                                                                                                                                                                                                                           |
| 削除 (Delete)    | <p>すべてのデバイス。</p> <p>登録済みデバイスの最大数に到達した場合、従業員が、登録されたデバイスをデバイス ポータルから削除したり、未使用のデバイスを削除して新しいデバイスを追加したりできるようにします。このアクションによって、デバイス ポータルに表示されるデバイス リストからデバイスが削除されますが、デバイスは Cisco ISE データベースに残り、エンドポイントのリストに表示されます。</p> <p>BYOD またはデバイス ポータルを使用して従業員が登録できるパーソナル デバイスの最大数を定義するには、[管理 (Administration) ] &gt; [デバイス ポータル管理 (Device Portal Management) ] &gt; [設定 (Settings) ] &gt; [従業員登録済みデバイス (Employee Registered Devices) ] を選択します。</p> <p>Cisco ISE データベースからデバイスを完全に削除するには、[ワーク センター (Work Centers) ] &gt; [ネットワーク アクセス (Network Access) ] &gt; [ID (Identities) ] &gt; [エンドポイント (Endpoints) ] を選択します。</p> |
| 盗難 (Stolen)    | <p>すべてのデバイス。</p> <p>デバイスが盗まれたことを従業員が示すことができるようにします。このアクションは、デバイスポータルのデバイスのステータスを [盗難 (Stolen) ] に更新し、ブラックリストのエンドポイントの ID グループにそのデバイスを追加し、証明書を削除します。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                               |

| フィールド            | 使用上のガイドライン                                                                                                                                                                           |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| デバイス ロック         | MDM 登録デバイスのみ。<br><br>デバイスの紛失または盗難が発生した場合、従業員がすぐにデバイス ポータルからリモートでデバイスをロックできるようにします。このアクションによって、デバイスの不正使用が防止されます。<br><br>ただし、デバイス ポータルでは PIN を設定できないため、従業員が事前にモバイル デバイスに設定しておく必要があります。 |
| 登録解除 (Unenroll)  | MDM 登録デバイスのみ。<br><br>職場でデバイスを使用する必要がなくなった場合に、従業員がこのオプションを選択できるようにします。このアクションでは、会社がインストールしているアプリケーションと設定のみが削除され、従業員のモバイルデバイス上の他のアプリケーションおよびデータは維持されます。                                |
| 完全消去 (Full wipe) | MDM 登録デバイスのみ。<br><br>デバイスを紛失したり、新しいものに交換したりした場合に、従業員がこのオプションを選択できるようにします。このアクションでは、従業員のモバイル デバイスを工場出荷時のデフォルト設定にリセットし、インストール済みのアプリケーションとデータを削除します。                                    |

#### 関連トピック

[従業員が追加するパーソナル デバイスの管理](#) (610 ページ)

[デバイス ポータル](#) (588 ページ)

## デバイス ポータルのデバイス カスタマイズの追加、編集、および検索

これらの設定へのナビゲーションパスは、**[管理 (Administration)] > [デバイス ポータル管理 (Device Portal Management)] > [デバイス ポータル (My Devices Portals)] > [作成、編集または複製 (Create, Edit or Duplicate)] > [ポータル ページのカスタマイズ (Portal Page Customization)] > [デバイスの追加、デバイスの編集またはデバイスの検索 (Add Devices, Edit Devices or Locate Devices)]** です。

[ページのカスタマイズ (Page Customizations)] で、デバイス ポータルの [追加 (Add)]、[編集 (Edit)]、および [検索 (Locate)] の各タブに表示される、メッセージ、タイトル、コンテンツ、手順、およびフィールドやボタンのラベルをカスタマイズできます。

#### 関連トピック

[デバイス ポータル](#) (588 ページ)

## デバイス ポータルの作成 (607 ページ)

### デバイス ポータルのサポート情報ページの設定

このページのナビゲーションパスは、**[管理 (Administration)] > [デバイス ポータル管理 (Device Portal Management)] > [BYOD ポータル (BYOD Portals)]/[クライアント プロビジョニング ポータル (Client Provisioning Portals)]/[MDM ポータル (MDM Portals)]/[デバイス ポータル (My Device Portals)] > [作成、編集または複製 (Create, Edit or Duplicate)] > [ポータルの動作およびフローの設定 (Portal Behavior and Flow Settings)] > [サポート情報ページの設定 (Support Information Page Settings)]** です。

これらの設定を使用して、ヘルプデスクがユーザ（状況に応じてゲスト、スポンサーまたは従業員）が体験したアクセスの問題をトラブルシューティングするために使用できる情報を表示します。

| フィールド                                              | 使用上のガイドライン                                                                                                                                                                    |
|----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| サポート情報ページを含める (Include a Support Information Page) | 該当ポータルのすべての有効なページ上で、問い合わせ先などの情報へのリンクを表示します。                                                                                                                                   |
| MAC アドレス                                           | [サポート情報 (Support Information)] ページにデバイスの MAC アドレスを含めます。                                                                                                                       |
| IP アドレス                                            | [サポート情報 (Support Information)] ページにデバイスの IP アドレスを含めます。                                                                                                                        |
| ブラウザのユーザエージェント (Browser user agent)                | [サポート情報 (Support Information)] ページに、要求の発信元のユーザ エージェントの製品名とバージョン、レイアウトエンジン、バージョンなど、ブラウザの詳細を含めます。                                                                               |
| ポリシー サーバ (Policy server)                           | [サポート情報 (Support Information)] ページに、このポータルを提供している ISE ポリシー サービス ノード (PSN) の IP アドレスを含めます。                                                                                     |
| 障害コード (Failure code)                               | 可能な場合は、ログメッセージカタログ内の対応する番号を含めます。メッセージカタログにアクセスしてこれを表示するには、 <b>[管理 (Administration)] &gt; [システム (System)] &gt; [ロギング (Logging)] &gt; [メッセージカタログ (Message Catalog)]</b> に移動します。 |

| フィールド                                            | 使用上のガイドライン                                                                                                                                                                                                 |
|--------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| フィールドを隠す (Hide field)                            | 含める情報が存在しない場合、[サポート情報 (Support Information)] ページ上の該当するフィールドラベルを表示しません。たとえば、障害コードが不明であるために空白である場合、[障害コード (Failure code)] は、選択されている場合でも表示されません。                                                              |
| 値のないラベルを表示 (Display label with no value)         | 含める情報が存在しない場合でも、選択されているすべてのフィールドのラベルを[サポート情報 (Support Information)] ページに表示します。たとえば、障害コードが不明な場合、[障害コード (Failure code)] は空白であっても表示されます。                                                                      |
| デフォルト値でラベルを表示 (Display label with default value) | [サポート情報 (Support Information)] ページ上の選択されているフィールドに含まれる情報が存在しない場合、このテキストがこれらのすべてのフィールドに表示されます。たとえば、このフィールドに「Not Available」と入力した場合に障害コード不明が不明な場合は、[障害コード (Failure code)] に [使用できません (Not Available)] と表示されます。 |

#### 関連トピック

[デバイス ポータルおよびエンドポイント アクティビティのモニタ](#) (611 ページ)

[デバイス ポータルへのアクセス](#) (585 ページ)

## 脅威中心型 NAC サービス

SourceFire FireAMP または Qualys アダプタを追加できます。

### 新しいベンダー インスタンスの追加

次の表に、[新しいベンダー インスタンスの追加 (Add New Vendor Instance)] ページにある各フィールドの説明を示します。このページのナビゲーションパスは、[管理 (Administration)] > [脅威中心型 NAC (Threat Centric NAC)] > [サードパーティ ベンダー (Third Party Vendors)] > [追加 (Add)] です。

| フィールド                      | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ベンダー                       | <p>追加するアダプタに基づいて、次のいずれかのオプションを選択します。</p> <ul style="list-style-type: none"><li>• AMP : 脅威 (AMP : Threat) : SourceFire FireAMP アダプタを追加するにはこのオプションを選択します。FireAMP アダプタの設定方法の詳細については、<a href="#">SourceFire FireAMP アダプタの追加 (741 ページ)</a> を参照してください。</li><li>• Qualys : VA : Qualys アダプタを追加するにはこのオプションを選択します。Qualys アダプタの設定方法の詳細については、<a href="#">Qualys アダプタの設定 (747 ページ)</a> を参照してください。</li></ul> |
| [インスタンス名 (Instance Name) ] | アダプタ インスタンスの名前を入力します。                                                                                                                                                                                                                                                                                                                                                                           |







## 第 31 章

# ゲスト アクセスのユーザ インターフェイスのリファレンス

- [ゲスト ポータル設定 \(1291 ページ\)](#)
- [スポンサー ポータル アプリケーションの設定 \(1313 ページ\)](#)
- [グローバル設定 \(Global Settings\) \(1322 ページ\)](#)

## ゲスト ポータル設定

### ポータル ID 設定

これらの設定へのナビゲーションパスは、[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [ゲスト ポータルまたはスポンサー ポータル (Guest Portals or Sponsor Portals)] > [作成、編集または複製 (Create, Edit or Duplicate)] > [ゲスト ポータルおよびスポンサー ポータルの設定とカスタマイズ (Guest Portals or Sponsor Portals Settings and Customization)] です。

- **ポータル名 (Portal Name)** : このポータルにアクセスするための一意のポータル名を入力します。このポータル名を、その他のスポンサーやゲスト ポータルおよび非ゲスト ポータル (ブラックリスト、個人所有デバイス持ち込み (BYOD)、クライアントプロビジョニング、モバイル デバイス管理 (MDM)、またはデバイスの各ポータル) に使用しないでください。

この名前は、許可プロファイルのポータルの選択でリダイレクションの選択肢として表示され、ポータルのリストで他のポータルの中から簡単に識別するために使用されます。

- **[説明 (Description)]** : 任意項目です。
- **ポータル テスト URL (Portal test URL)** : [保存 (Save)] をクリックした後にリンクとして表示されるシステムにより生成された URL。ポータルをテストするために使用します。  
リンクをクリックすると、このポータルの URL を表示する新しいブラウザ タブが開きます。これを有効にするには、ポリシー サービスを含むポリシー サービス ノード (PSN)

をオンにする必要があります。ポリシー サービスがオンになっていない場合、PSN は管理者用ポータルのみを表示します。



(注) テスト ポータルは RADIUS セッションをサポートしていないため、すべてのポータルに対するポータルフローの全体は表示されません。BYOD およびクライアントプロビジョニングは RADIUS セッションに依存するポータルの例です。たとえば、外部 URL へのリダイレクションは機能しません。

- 言語ファイル (Language File) : 各ポータル タイプは、デフォルトで 15 種類の言語をサポートします。これらの言語は、個々のプロパティファイルとして使用できます。これらのファイルは、圧縮された単一の言語ファイル内にまとめてバンドルされています。ポータルで使用する圧縮言語ファイルをエクスポートまたはインポートします。圧縮言語ファイルには、ポータルのテキストを表示するために使用可能な個別の言語ファイルがすべて含まれています。

言語ファイルには、その言語のポータル全体のすべての文字列設定に加え、特定のブラウザのロケール設定 (例: フランス語の場合は `fr`、`fr-fr`、`fr-ca`) へのマッピングが含まれています。1 つの言語ファイルには、翻訳およびローカリゼーションの目的に容易に使用できるように、サポートされるすべての言語が含まれています。

1 つの言語用のブラウザ ロケール設定を変更した場合、変更内容は他のすべてのエンドユーザ Web ポータルに適用されます。たとえば、ホットスポット ゲスト ポータルの `French.properties` ブラウザ ロケールを `fr,fr-fr,fr-ca` から `fr,fr-fr` に変更すると、この変更内容がデバイス ポータルにも適用されます。

[ポータルページのカスタマイズ (Portal Page Customizations)] タブでいずれかのポータルページテキストをカスタマイズすると、警告アイコンが表示されます。警告メッセージは、ポータルのカスタマイズ時に 1 つの言語で行った変更をすべてのサポート対象の言語プロパティファイルで更新するように注意を促します。ドロップダウンリストのオプションを使用して、手動で警告アイコンが表示されないようにします。また、警告アイコンは、更新された圧縮言語ファイルのインポート後に自動的に表示されなくなります。

## ホットスポット ゲスト ポータルのポータル設定

このページへのナビゲーションパスは、[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [ゲスト ポータル (Guest Portals)] > [作成、編集または複製 (Create, Edit or Duplicate)] > [ポータルの動作およびフローの設定 (Portal Behavior and Flow Settings)] > [ポータル設定 (Portal Settings)] です。

- [HTTPS ポート (HTTPS port)] : 8000 ~ 8999 の範囲のポート値を入力します。デフォルト値はすべてのデフォルト ポータルで 8443 です。ただし、ブラックリスト ポータルは 8444 です。この範囲外のポート値を使用してアップグレードした場合は、このページで変

更を加えるまで維持されます。このページを変更する場合は、この制限に従うようにポート設定を更新します。

ゲスト ポータルに非ゲスト ポータル（マイ デバイスなど）によって使用されるポートを割り当てると、エラー メッセージが表示されます。

ポスチャ評価と修復についてのみ、クライアントプロビジョニングポータルはポート 8905 および 8909 も使用します。それ以外の場合は、ゲスト ポータルへの割り当てと同じポートを使用します。

同じ HTTPS ポートに割り当てられたポータルは、同じギガビットイーサネットインターフェイスまたは別のインターフェイスを使用できます。これらのポータルが同じポートとインターフェイスの組み合わせを使用している場合、同じ証明書グループタグを使用する必要があります。次に例を示します。

- スポンサー ポータルを例として使用した有効な組み合わせを次に示します。
    - スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書タグ **A**、およびデバイス ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**
    - スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**、およびデバイス ポータル：ポート **8445**、インターフェイス **0**、証明書グループ **B**
    - スポンサー ポータル：ポート **8444**、インターフェイス **1**、証明書グループ **A**、およびブラックリスト ポータル：ポート **8444**、インターフェイス **0**、証明書グループ **B**
  - 無効な組み合わせには次が含まれます。
    - スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**、およびデバイス ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **B**
    - スポンサー ポータル：ポート **8444**、インターフェイス **0**、証明書タグ **A**、およびブラックリスト ポータル：ポート **8444**、インターフェイス **0**、証明書グループ **A**
  - [使用可能インターフェイス（Allowed interfaces）]：PAN がポータルの実行に使用できる PSN インターフェイスを選択します。ポータルを開く要求が PAN で行われると、PAN は PSN で使用可能なポートを探します。異なるサブネット上の IP アドレスを使用してイーサネット インターフェイスを設定する必要があります。
- これらのインターフェイスは、ポリシー サービスがオンになっているすべての PSN（VM ベースを含む）で使用可能である必要があります。これは、これらのすべての PSN がゲストセッションの開始時にリダイレクトに使用される可能性があるため、必須要件です。
- イーサネット インターフェイスは、異なるサブネット上の IP アドレスを使用する必要があります。
  - ここで有効にするインターフェイスは、ポリシー サービスがオンになっているときの VM ベースのものを含む、すべての PSN で使用できるものでなければなりません。こ

これは、これらのすべての PSN がゲスト セッションの開始時にリダイレクトに使用される可能性があるため必須です。

- ポータルの証明書のサブジェクト名とサブジェクトの代替名はインターフェイス IP に解決する必要があります。
  - ISE CLI で **ip host x.x.x.x yyy.domain.com** を設定して、セカンダリ インターフェイス IP を FQDN にマッピングします。これは、証明書のサブジェクト名とサブジェクトの代替名と一致させるために使用されます。
  - ボンディングされた NIC のみが選択されている場合：PSN がポータルを設定しようとする、最初にボンディングインターフェイスを設定しようとしします。これが成功しない場合、おそらく、その PSN でボンディングが設定されていないために、PSN でエラーが記録されて終了します。PSN は物理インターフェイスでのポータルの開始を試みません。
  - **NIC チーミング**またはボンディングは、高可用性（耐障害性）のために 2 つの個別の NIC を設定できる、O/S 設定オプションです。どちらかの NIC に障害が発生すると、ボンディングされた接続の一部であるもう一方の NIC は、接続を続行します。1 つの NIC がポータル設定に基づきポータルに対して選択されます。
    - 物理 NIC と対応するボンディングされた NIC の両方が設定されている場合：PSN がポータルを設定しようとする、最初にボンディングインターフェイスへ接続しようとしします。これが成功しない場合、その PSN にボンドセットアップがなかったことが原因である可能性があるため、PSN は物理インターフェイスでポータルを開始しようとしします。
  - [証明書グループ タグ (Certificate group tag)]：ポータルの HTTPS トラフィックに使用する証明書を指定する証明書グループ タグを選択します。
  - エンドポイント ID グループ (Endpoint identity group)：ゲストのデバイスを追跡するためのエンドポイント ID グループを選択します。Cisco ISE はデフォルトとして使用する **GuestEndpoints** のエンドポイント ID グループを提供します。デフォルトを使用しない場合、追加のエンドポイント ID グループを作成することもできます。
- 従業員のデバイスを追跡するためのエンドポイント ID グループを選択します。Cisco ISE はデフォルトとして使用する **RegisteredDevices** のエンドポイント ID グループを提供します。デフォルトを使用しない場合、追加のエンドポイント ID グループを作成することもできます。
- \_\_日に達した場合にこの ID グループ内のエンドポイントを消去する (Purge endpoints in this identity group when they reach \_\_ days)：Cisco ISE データベースから消去されるまでの、ユーザのデバイスの登録からの日数を変更します。消去は毎日実行され、消去アクティビティは全体的な消去タイミングと同期されます。変更は、このエンドポイント ID グループ全体に適用されます。
- その他のポリシー条件に基づいてエンドポイント消去ポリシーに変更が加えられた場合、この設定は使用できなくなります。

### • 表示言語

- [ブラウザのロケールを使用する (Use browser locale)] : クライアントブラウザのロケール設定で指定された言語をポータルの表示言語として使用します。ブラウザロケールの言語がISEでサポートされていない場合は、フォールバック言語が言語ポータルとして使用されます。
- [フォールバック言語 (Fallback language)] : ブラウザロケールから言語を取得できない場合、またはブラウザロケール言語がISEでサポートされていない場合に使用する言語を選択します。
- [常に使用 (Always use)] : ポータルに使用する表示言語を選択します。この設定は、ユーザのブラウザのロケール オプションを上書きします。

[スポンサーに使用可能なSSID (SSIDs available to sponsors)] : ゲストの訪問にあたり、スポンサーが正しい接続先ネットワークとしてゲストに通知できる、ネットワークの名前またはSSID (セッション サービス識別子) を入力します。

## ホットスポット ゲスト ポータルの利用規定 (AUP) ページ設定

このページへのナビゲーションパスは、[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [ゲスト ポータル (Guest Portals)] > [作成、編集または複製 (Create, Edit or Duplicate)] > [ポータルの動作およびフローの設定 (Portal Behavior and Flow Settings)] > [利用規定 (AUP) ページ設定 (Acceptable Use Policy (AUP) Page Settings)] です。

- [AUP ページを含める (Include an AUP page)] : 会社のネットワーク使用諸条件を、別のページでユーザに表示します。
- [アクセスコードが必要 (Require an access code)] : 複数のゲストがネットワークへのアクセスを獲得ために使用する必要があるログイン クレデンシャルとして、アクセスコードを割り当てます。アクセスコードは、物理的に存在するゲストに対して指定される、主にローカルで認識されるコードです (ホワイトボードによって視覚的に、またはロビーアンバサダーにより口頭で)。これは、ネットワークにアクセスするために部外者に認知されることも使用されることもありません。

個別のゲストにログイン クレデンシャルとして提供されるユーザ名とパスワードに加えて、このオプションを使用できます。

- [AUP の最後までスクロールが必要 (Require scrolling to end of AUP)] : ユーザが AUP を完全に読んだことを確認します。[同意 (Accept)] ボタンは、ユーザが AUP の最後までスクロールするとアクティブになります。AUP がユーザに表示された場合に設定します。

## ホットスポット ポータルのポストアクセス バナー ページ設定

このページのナビゲーションパスは、[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [ゲスト ポータル (Guest Portals)] > [作成、編集または複製 (Create, Edit or Duplicate)] > [ポータルの動作およびフローの設定 (Portal Behavior and Flow Settings)] > [アクセス後のバナー ページ設定 (Post-Access Banner Page Settings)] です。

この設定を使用して、ゲストにアクセス ステータスおよび必要に応じてその他の追加アクションを通知します。

| フィールド                                                | 使用上のガイドライン                                   |
|------------------------------------------------------|----------------------------------------------|
| アクセス後バナー ページを含める (Include a Post-Access Banner page) | ゲストが正常に認証された後、ネットワーク アクセスを付与される前に追加情報を表示します。 |

## クレデンシャルを持つゲスト ポータルのポータル設定

このページへのナビゲーションパスは、[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [ゲスト ポータル (Guest Portals)] > [作成、編集または複製 (Create, Edit or Duplicate)] > [ポータルの動作およびフローの設定 (Portal Behavior and Flow Settings)] > [ポータル設定 (Portal Settings)] です。

- [HTTPS ポート (HTTPS port)] : 8000 ~ 8999 の範囲のポート値を入力します。デフォルト値はすべてのデフォルト ポータルで 8443 です。ただし、ブラックリスト ポータルは 8444 です。この範囲外のポート値を使用してアップグレードした場合は、このページで変更を加えるまで維持されます。このページを変更する場合は、この制限に従うようにポート設定を更新します。

ゲスト ポータルに非ゲスト ポータル (マイ デバイスなど) によって使用されるポートを割り当てると、エラー メッセージが表示されます。

ポスチャ評価と修復についてのみ、クライアントプロビジョニングポータルはポート 8905 および 8909 も使用します。それ以外の場合は、ゲスト ポータルへの割り当てと同じポートを使用します。

同じ HTTPS ポートに割り当てられたポータルは、同じギガビットイーサネットインターフェイスまたは別のインターフェイスを使用できます。これらのポータルが同じポートとインターフェイスの組み合わせを使用している場合、同じ証明書グループタグを使用する必要があります。次に例を示します。

- スポンサー ポータルを例として使用した有効な組み合わせを次に示します。
  - スポンサー ポータル : ポート **8443**、インターフェイス **0**、証明書タグ **A**、およびデバイス ポータル : ポート **8443**、インターフェイス **0**、証明書グループ **A**
  - スポンサー ポータル : ポート **8443**、インターフェイス **0**、証明書グループ **A**、およびデバイス ポータル : ポート **8445**、インターフェイス **0**、証明書グループ **B**

- スポンサー ポータル：ポート **8444**、インターフェイス **1**、証明書グループ **A**、およびブラックリスト ポータル：ポート **8444**、インターフェイス **0**、証明書グループ **B**
  - 無効な組み合わせには次が含まれます。
    - スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**、およびデバイス ポータル： **8443**、インターフェイス **0**、証明書グループ **B**
    - スポンサー ポータル：ポート **8444**、インターフェイス **0**、証明書タグ **A**、およびブラックリスト ポータル：ポート **8444**、インターフェイス **0**、証明書グループ **A**
  - [使用可能インターフェイス (Allowed interfaces)] : PAN がポータルの実行に使用できる PSN インターフェイスを選択します。ポータルを開く要求が PAN で行われると、PAN は PSN で使用可能なポートを探します。異なるサブネット上の IP アドレスを使用してイーサネット インターフェイスを設定する必要があります。
- これらのインターフェイスは、ポリシー サービスがオンになっているすべての PSN (VM ベースを含む) で使用可能である必要があります。これは、これらのすべての PSN がゲストセッションの開始時にリダイレクトに使用される可能性があるため、必須要件です。
- イーサネット インターフェイスは、異なるサブネット上の IP アドレスを使用する必要があります。
  - ここで有効にするインターフェイスは、ポリシー サービスがオンになっているときの VM ベースのものを含む、すべての PSN で使用できるものでなければなりません。これは、これらのすべての PSN がゲストセッションの開始時にリダイレクトに使用される可能性があるため必須です。
  - ポータルの証明書のサブジェクト名とサブジェクトの代替名はインターフェイス IP に解決する必要があります。
  - ISE CLI で **ip host x.x.x.x yyy.domain.com** を設定して、セカンダリ インターフェイス IP を FQDN にマッピングします。これは、証明書のサブジェクト名とサブジェクトの代替名と一致させるために使用されます。
  - ボンディングされた NIC のみが選択されている場合：PSN がポータルを設定しようとする、最初にボンディング インターフェイスを設定しようとしします。これが成功しない場合、おそらくは、その PSN でボンディングが設定されていないために、PSN でエラーが記録されて終了します。PSN は物理インターフェイスでのポータルの開始を試みません。
  - **NIC チーミング**またはボンディングは、高可用性 (耐障害性) のために2つの個別の NIC を設定できる、O/S 設定オプションです。どちらかの NIC に障害が発生すると、ボンディングされた接続の一部であるもう一方の NIC は、接続を続行します。1 つの NIC がポータル設定に基づきポータルに対して選択されます。
    - 物理 NIC と対応するボンディングされた NIC の両方が設定されている場合：PSN がポータルを設定しようとする、最初にボンディング インターフェイスへ接続

しようとします。これが成功しない場合、その PSN にボンドセットアップがなかったことが原因である可能性があるため、PSN は物理インターフェイスでポータルを開始しようとします。

- ポータルの証明書のサブジェクト名とサブジェクトの代替名はインターフェイス IP に解決する必要があります。
- [認証方式 (Authentication Method)] : ユーザ認証に使用する ID ソース順序 (ISS) または ID プロバイダー (IdP) を選択します。ISS は、ユーザ クレデンシャルを確認するために順番に検索される ID ストアのリストです。たとえば、内部ゲスト ユーザ、内部ユーザ、Active Directory、LDAP ディレクトリ などがあります。

Cisco ISE には、スポンサー ポータル Sponsor\_Portal\_Sequence 用のデフォルトのスポンサー ID ソース順序が含まれています。

IdP を設定するには、[管理 (Administration)] > [ID の管理 (Identity Management)] > [外部 ID ソース (External Identity Sources)] > [SAML ID プロバイダー (SAML Id Providers)] の順に選択します。

ID ソース順序を設定するには、[管理 (Administration)] > [ID の管理 (Identity Management)] > [ID ソース順序 (Identity Source Sequences)] の順に選択します。

- ゲストとしてこのポータルを使用する従業員のログイン オプションの継承元 (Employees using this portal as guests inherit login options from) : 従業員がこのポータルにログオンしたときに割り当てられるゲスト タイプを選択します。従業員のエンドポイント データは、そのゲスト タイプで属性 [エンドポイント ID グループにデバイス情報を保存する (Store device information in endpoint identity group)] に設定されたエンドポイント ID グループに保存されます。関連付けられたゲスト タイプの他の属性は継承されません。

#### • 表示言語

- [ブラウザのロケールを使用する (Use browser locale)] : クライアントブラウザのロケール設定で指定された言語をポータルの表示言語として使用します。ブラウザ ロケールの言語が ISE でサポートされていない場合は、フォールバック言語が言語ポータルとして使用されます。
- [フォールバック言語 (Fallback language)] : ブラウザロケールから言語を取得できない場合、またはブラウザロケール言語が ISE でサポートされていない場合に使用する言語を選択します。
- [常に使用 (Always use)] : ポータルに使用する表示言語を選択します。この設定は、ユーザのブラウザのロケール オプションを上書きします。

[スポンサーに使用可能な SSID (SSIDs available to sponsors)] : ゲストの訪問にあたり、スポンサーが正しい接続先ネットワークとしてゲストに通知できる、ネットワークの名前または SSID (セッション サービス識別子) を入力します。



## クレデンシャルを持つゲストポータルのログインページ設定

このページへのナビゲーションパスは、[ワークセンター (Work Centers)] > [ゲストアクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [ゲストポータル (Guest Portals)] > [作成、編集または複製 (Create, Edit or Duplicate)] > [ポータルの動作およびフローの設定 (Portal Behavior and Flow Settings)] > [ログインページの設定 (Login Page Settings)] です。

- [アクセスコードが必要 (Require an access code)] : 複数のゲストがネットワークへのアクセスを獲得ために使用する必要があるログインクレデンシャルとして、アクセスコードを割り当てます。アクセスコードは、物理的に存在するゲストに対して指定される、主にローカルで認識されるコードです (ホワイトボードによって視覚的に、またはロビーアンバサダーにより口頭で)。これは、ネットワークにアクセスするために部外者に認知されることも使用されることもありません。

個別のゲストにログインクレデンシャルとして提供されるユーザ名とパスワードに加えて、このオプションを使用できます。

- [頻度制限までの最大ログイン試行失敗数 (Maximum failed login attempts before rate limiting)] : Cisco ISE がアカウントのスロットルを開始するまでの単一のブラウザセッションからのログイン試行失敗回数を指定します。これにより、アカウントのロックアウトは起きません。スロットル率は、[頻度制限時のログイン試行間隔 (Time between login attempts when rate limiting)] で設定されます。
  - [頻度制限時のログイン試行間隔 (Time between login attempts when rate limiting)] : [頻度制限までの最大ログイン試行失敗数 (Maximum failed login attempts before rate limiting)] で定義された回数のログインの失敗後に、ユーザが再度ログインを試行するまでに待機する必要がある時間 (スロットル率) を分単位で設定します。
  - [AUP を含める (Include an AUP)] : フローに利用規約ページを追加します。AUP をページに追加したり、別のページへのリンクを設定することができます。これを追加すると、右側のフローの画像が変わります。
    - [同意が必要 (require acceptance)] : フローを続行する前に、ユーザが AUP に同意するように強制します。
  - [ゲストに自分自身のアカウントの作成を許可 (Allow guests to create their own accounts)] : このポータルの [ログイン (Login)] ページで、ゲストが自身を登録するためのオプションが提供されます。このオプションが選択されていない場合は、スポンサーがゲストアカウントを作成します。これを有効にすることで、このページのタブが有効になり、[アカウント登録ページの設定 (Self-Registration Page Settings)] および [アカウント登録成功ページの設定 (Self-Registration Success Page Settings)] を設定できます。
- ゲストがこのオプションを選択した場合、自身のゲストアカウントを作成するために必要な情報を入力できるアカウント登録フォームが示されます。
- [ゲストにログイン後のパスワード変更を許可 (Allow guests to change password after login)] : ゲストが正常に認証され、AUPに同意した後に、ゲストに必要なに応じてパスワードを変更することを許可します。

ゲストが自分のパスワードを変更した場合、スポンサーはゲストにログインクレデンシャル情報を提供できません。スポンサーは、ゲストのパスワードをランダムパスワードにリセットすることだけが可能です。

- [ログインに次の ID プロバイダ ゲスト ポータルの使用を許可 (Allow the following identity-provider guest portal to be used for login) ] : このオプションをオンにし、SAML Id ID プロバイダを選択すると、その SAML ID のリンクがこのポータルに追加されます。このサブ ポータルは、ユーザが証明書を提供している SAML IDP のように見えるように設定できます。

## アカウント登録ページの設定 (Self-Registration Page Settings)

このページへのナビゲーションパスは、[ワーク センター (Work Centers) ] > [ゲスト アクセス (Guest Access) ] > [ポータルとコンポーネント (Portal & Components) ] > [ゲスト ポータル (Guest Portals) ] > [作成、編集または複製 (Create, Edit or Duplicate) ] > [ポータルの動作およびフローの設定 (Portal Behavior and Flow Settings) ] > [アカウント登録ページの設定 (Self-Registration Page Settings) ] です。これらの設定を使用して、ゲストが自身を登録し、提供する必要がある情報をアカウント登録フォームで指定できるようにします。

- [アカウント登録ゲストに割り当てるゲスト タイプ (Assign self-registered guests to guest type) ] : このポータルを使用するすべてのアカウント登録ゲストに割り当てられるゲスト タイプを選択します。
- [アカウントの有効期間 (Account valid for) ] : アカウントの有効期間を、日、時間、または分で指定します。この期間を超過した場合、管理者またはスポンサーがスポンサー ポータルでアカウント有効期間を延長した場合を除き、アカウントは失効します。
- [アカウント登録に登録コードを必要とする (Require a registration code for self registration) ] : アカウント登録ゲストがアカウント登録フォームを正常に送信するために入力する必要があるコードを割り当てます。部外者がシステムにアクセスすることを防ぐために、アクセス コードと同様に、登録コードはオフラインで提供されます。
- [含めるフィールド (Fields to include) ] : アカウント登録ページ上で、アカウント登録フォームに表示するフィールドのチェックボックスをオンにします。その後、ゲストがこのフォームを送信してゲストアカウントを受信するために入力が必要であるフィールドのチェックボックスをオンにします。アカウント登録ゲストから重要な情報を収集するために、[SMS サービス プロバイダー (SMS Service Provider) ] および [訪問先担当者 (Person being Visited) ] フィールドを必須にすることができます。
  - [場所 (Location) ] : アカウント登録のゲストが定義済みリストを使用して登録時に選択できる場所を入力します。これにより、これらのゲストの有効なアクセス時間として自動的に関連するタイムゾーンが割り当てられます。場所の名前は、選択時に混乱を回避するために具体的にする必要があります (たとえば、ボストン オフィス、500 Park Ave New York、シンガポールなど)

ゲスト アクセスを時間で制限する予定の場合は、その時間を設定するときにタイムゾーンを使用します。アクセス時間が制御されたゲスト全員がサンノゼのタイムゾーンにいる場合を除き、各自のロケールのタイムゾーンを作成します。場所が1つだけ

である場合は、その場所がデフォルトの場所として自動的に割り当てられ、ポータルではこのフィールドがゲストに対して表示されません。また、[場所 (Location)] は、[含めるフィールド (Fields to include)] のリスト内で無効になります。

- **[SMS サービス プロバイダー (SMS Service Provider)]** : アカウント登録フォームに SMS プロバイダーを表示して、アカウント登録ゲストが自分の SMS プロバイダーを選択できるようにします。これで、会社の経費を最小化するために、ゲストの SMS サービスを使用して SMS 通知を送信できるようになります。ゲストが使用できる SMS プロバイダーを 1 つだけ選択した場合は、このフィールドはアカウント登録フォームに表示されません。
- **[訪問先担当者 (Person being Visited)]** : これはテキストフィールドであるため、このフィールドを使用する場合には、ゲストに対し、このフィールドに入力する情報について説明してください。
- **[カスタム フィールド (Custom Fields)]** : アカウント登録ゲストから追加のデータを収集するために作成したカスタムフィールドを選択します。その後、ゲストがアカウント登録フォームを送信してゲスト アカウントを受信するために入力が必要であるフィールドのチェックボックスをオンにします。これらのフィールドは名前のアルファベット順に表示されます。これらのフィールドは、カスタムフィールドを追加するため、**[ワーク センター (Work Centers)]** > **[ゲスト アクセス (Guest Access)]** > **[設定 (Settings)]** > **[カスタム フィールド (Custom Fields)]** で作成されます。
- **[AUP を含める (Include an AUP)]** : 会社のネットワーク使用の諸条件を、現在ユーザに表示されるページ上のテキストとして、または AUP テキストが含まれる新しいタブまたはウィンドウを開くリンクとして表示します。
  - **[同意が必要 (Require acceptance)]** : ユーザが AUP を最後まで読んだことを確認します。これにより、アカウント登録ページの **[同意する (Accept)]** ボタンが設定されます。AUP が **[ページ (as on page)]** として設定されている場合、ユーザが AUP の終わりまでスクロールするまでは **[同意する (Accept)]** ボタンを無効にするように設定できます。
- **[次の電子メール アドレスを持つゲストのみを許可 (Only allow guests with an email address from)]** : アカウント登録ゲストが電子メール アドレスを作成するときに **[電子メール アドレス (Email Address)]** で使用できるドメイン (例 : cisco.com) のホワイトリストを指定します。

このフィールドを空白のままにすると、**[次の電子メール アドレスを持つゲストを許可しない (Do not allow guests with email address from)]** にリストされているドメイン以外のすべての電子メール アドレスが有効になります。
- **[次の電子メール アドレスを持つゲストを許可しない (Do not allow guests with email address from)]** : アカウント登録ゲストが電子メール アドレスを作成するときに **[電子メール アドレス (Email Address)]** に使用できないドメイン (例 : czgtgj.com) のブラックリストを指定します。

- [アカウント登録ゲストが承認される必要がある (Require self-registered guests to be approved)] : このポータルを使用するアカウント登録ゲストは、ゲストのクレデンシャルを受信する前にスポンサーによる承認が必要であることを指定します。このオプションをクリックすると、スポンサーがアカウント登録ゲストを承認する方法に関する追加のオプションが表示されます。詳細については、[電子メールによるアカウント登録のアカウントの承認 \(552 ページ\)](#) を参照してください。
- [承認要求電子メール送信先 (Email approval request to)] : 次のいずれかを選択します。
  - [下に示すスポンサーの電子メールアドレス (sponsor email addresses listed below)] : 承認者として指名されたスポンサーの1つ以上の電子メールアドレス、またはすべてのゲストの承認要求の送信先となるメール ソフトウェアを入力します。
  - [訪問先担当者 (person being visited)] : [スポンサーに承認用クレデンシャルの入力を求める (Require sponsor to provide credentials for authentication)] フィールドが表示され、[含めるフィールド (Fields to include)] の [必須 (Required)] オプションが有効になります (以前は無効だった場合)。これらのフィールドはアカウント登録フォームに表示され、アカウント登録ゲストからこの情報を要求します。
- [承認/拒否のリンクの設定 (Approve/Deny Link Settings)] : このセクションでは次の内容を設定できます。
  - [リンクの有効期間 (Links are valid for)] : アカウント承認リンクの有効期間を設定できます。
  - [スポンサーに承認用クレデンシャルの入力を求める (Require sponsor to provide credentials for authentication)] : このセクションの設定でスポンサーによるアカウント承認用のクレデンシャルの入力が必須ではない場合にも、スポンサーにこの情報を入力させるには、このフィールドをオンにします。このフィールドは、[アカウント登録ゲストが承認される必要がある (Require self-registered guests to be approved)] が [訪問先担当者 (person being visited)] に設定されている場合にだけ表示されます。
  - [承認権限を検証するためスポンサーがスポンサーポータルと照合される (Sponsor is matched to a Sponsor Portal to verify approval privileges)] : [詳細 > (Details >)] をクリックして、スポンサーが有効なシステムユーザであり、スポンサーグループのメンバーであり、そのスポンサーグループのメンバーにアカウント承認権限があることを確認するために検索されるポータルを選択します。各スポンサーポータルには、スポンサーを識別するために使用される ID ソース シーケンスがあります。ポータルはリストされている順序で使用されます。リストの1番目のポータルは、スポンサーポータルで使用されているスタイルとカスタマイズ内容を決定します。
- [登録の送信後のゲストの誘導先 (After registration submission, direct guest to)] : 登録の正常完了後にアカウント登録ゲストを誘導する場所を選択します。

- [アカウント登録成功 (Self-Registration Success)] ページ : アカウント登録に成功したゲストを [アカウント登録成功 (Self-Registration Success)] ページに誘導します。このページには、[アカウント登録成功ページ設定 (Self-Registration Success Page Settings)] で指定したフィールドとメッセージが表示されます。

すべての情報を表示することが望ましくない場合があります。システムはアカウントの承認待ち（このページで有効になっている場合）であるか、またはこのページで指定されたホワイトリスト、ブラックリストドメインに基づいて電子メールアドレスまたは電話番号にログイン クレデンシャルを提供する可能性があるためです。

[アカウント登録成功ページの設定 (Self-Registration Success Page Settings)] で [ゲストのアカウント登録成功ページからの直接ログインを許可する (Allow guests to log in directly from the Self-Registration Success page)] を有効にした場合、アカウント登録に成功したゲストはこのページから直接ログインすることができます。これが有効になっていない場合、ゲストは [アカウント登録成功 (Self-Registration Success)] ページが表示された後にポータルログイン ページに誘導されます。

- [ログイン クレデンシャルを取得する方法の手順を含むログイン ページ (Login page with instructions about how to obtain login credentials)] : アカウント登録に成功したゲストをポータルログイン ページに再び誘導し、「ゲスト クレデンシャルが電子メール、SMS、または印刷物で提供されるのを待ってからログインに進んでください。」などのメッセージを表示します。

デフォルト メッセージをカスタマイズするには、[ポータル ページのカスタマイズ (Portal Page Customization)] タブをクリックして、[アカウント登録ページ設定 (Self-Registration Page Settings)] を選択します。

システムはアカウントの承認待ち（このページで有効になっている場合）であるか、またはこのページで指定されたホワイトリスト、ブラックリストドメインに基づいて電子メールアドレスまたは電話番号にログイン クレデンシャルを提供する可能性があります。

- [URL] : アカウント登録に成功したゲストを、アカウント クレデンシャルの提供を待機している間に、指定された URL に誘導します。

システムはアカウントの承認待ち（このページで有効になっている場合）であるか、またはこのページで指定されたホワイトリスト、ブラックリストドメインに基づいて電子メールアドレスまたは電話番号にログイン クレデンシャルを提供する可能性があります。

• [クレデンシャル通知自動送信手段 (Send credential notification automatically using)] :

- [電子メール (Email)] : アカウント登録に成功したゲストがログイン クレデンシャルを受信する手段のオプションとして電子メールを選択します。このオプションを選択した場合、[電子メールアドレス (Email address)] が [含めるフィールド (Fields to include)] のリストで必須フィールドになり、このオプションを無効にできなくなります。
- [SMS] : アカウント登録に成功したゲストがログイン クレデンシャルを受信する手段のオプションとして SMS を選択します。このオプションを選択した場合、[SMS サー

ビスプロバイダー (SMS Service Provider) ] が [ 含めるフィールド (Fields to include) ] のリストで必須フィールドになり、このオプションを無効にできなくなります。

## アカウント登録成功ページの設定

このページへのナビゲーションパスは、[ワーク センター (Work Centers) ] > [ゲスト アクセス (Guest Access) ] > [ポータルとコンポーネント (Portals & Components) ] > [ゲスト ポータル (Guest Portals) ] > [作成、編集または複製 (Create, Edit or Duplicate) ] > [ポータルの動作およびフローの設定 (Portal Behavior and Flow Settings) ] > [アカウント登録成功ページ設定 (Self Registration Success Page Settings) ] です。これらの設定を使用して、正常にアカウント登録したゲストに、ネットワークへのアクセスを獲得するために必要なクレデンシャルを通知します。

| フィールド                                                                                   | 使用上のガイドライン                                                                                                                                                                                                                                                             |
|-----------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| アカウント登録の成功ページにこの情報を含める (Include this information on the Self-Registration Success page) | <p>[アカウント登録成功 (Self-Registration Success) ] ページで正常に登録されたゲストに表示されるフィールドのチェックボックスをオンにします。</p> <p>スポンサーによるゲストの承認が必要ない場合は、[ユーザ名 (Username) ] と [パスワード (Password) ] のチェックボックスをオンにして、ゲストにこれらのクレデンシャルを表示します。スポンサーの承認が必要な場合、クレデンシャルはゲストが承認された後にのみ提供されるため、これらのフィールドを無効にします。</p> |
| ゲストは次の手段で情報を自分に送信できる (Allow guest to send information to self using)                    | <p>正常にアカウント登録したゲストが自分自身にクレデンシャル情報を送信するためのオプションのチェックボックスをオンにします。[印刷 (Print) ]、[電子メール (Email) ]、または [SMS]。</p>                                                                                                                                                           |
| AUP をページに含める/AUP をリンクとして含める (Include an AUP (on page/as link))                          | <p>会社のネットワーク使用の諸条件を、現在ユーザに表示されるページ上のテキストとして、または AUP テキストが含まれる新しいタブまたはウィンドウを開くリンクとして表示します。</p>                                                                                                                                                                          |

| フィールド                                                                                                      | 使用上のガイドライン                                                                                                                                                         |
|------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 同意が必要（Require acceptance）                                                                                  | ユーザのアカウントが完全に有効になる前に、ユーザはAUPに同意する必要があります。[ログイン（Login）] ボタンは、ユーザがAUPを受け入れない場合は有効になりません。ユーザがAUPに同意しない場合、ネットワークにアクセスできません。                                            |
| AUPの最後までスクロールが必要（Require scrolling to end of AUP）                                                          | このフィールドは、[ページ上の AUP（AUP on page）] オプションを選択した場合のみ表示されます。<br><br>ユーザがAUPを最後まで読んだことを確認します。[同意（Accept）] ボタンは、ユーザがAUPの最後までスクロールするとアクティブになります。                           |
| ゲストをアカウント登録の成功ページから直接ログインできるようにする（Allow guests to log in directly from the Self-Registration Success page） | [アカウント登録の成功（Self-Registration Success）] ページ下部に [ログイン（Login）] ボタンを表示します。これにより、ゲストはログインページをバイパスし、自動的にログイン クレデンシャルをポータルに提供して、ポータルフローの次のページ（たとえばAUP ページ）を表示できるようになります。 |

## クレデンシャルを持つゲストポータルの利用規定（AUP）ページ設定

このページへのナビゲーションパスは、[ワーク センター（Work Centers）] > [ゲスト アクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [ゲスト ポータル（Guest Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [利用規定（AUP）ページ設定（Acceptable Use Policy (AUP) Page Settings）] です。

- [AUP ページを含める（Include an AUP page）] : 会社のネットワーク使用諸条件を、別のページでユーザに表示します。
- [従業員に別の AUP を使用する（Use different AUP for employees）] : 従業員専用で別の AUP およびネットワーク使用諸条件を表示します。このオプションを選択すると、[従業員用の AUP をスキップ（Skip AUP for employees）] は選択できません。
- [従業員用の AUP をスキップ（Skip AUP for employees）] : 従業員は、ネットワークにアクセスする前に AUP に同意する必要はありません。このオプションを選択すると、[従業員に別の AUP を使用する（Use different AUP for employees）] は選択できません。
- [AUP の最後までスクロールが必要（Require scrolling to end of AUP）] : [AUP をページに含める（Include an AUP on page）] を有効にした場合にのみ、このオプションが表示されます。

ユーザが AUP を最後まで読んだことを確認します。[同意 (Accept)] ボタンは、ユーザが AUP の最後までスクロールするとアクティブになります。AUP がユーザに表示された場合に設定します。

- [初回のログインのみ (On first login only)] : ユーザが初めてネットワークまたはポータルにログインしたときに AUP を表示します。
- [ログインごと (On every login)] : ユーザがネットワークまたはポータルにログインするごとに、AUP を表示します。
- [\_\_ 日ごと (初回のログインから) (Every \_\_ days (starting at first login))] : ネットワークやポータルにユーザが初めてログインした後は、AUP を定期的に表示します。

## クレデンシャルを持つゲストポータルのゲストによるパスワード変更の設定

### ゲストのパスワード変更設定 (Guest Change Password Settings)

このページへのナビゲーションパスは、[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [ゲスト ポータル (Guest Portals)] > [作成、編集または複製 (Create, Edit or Duplicate)] > [ポータルの動作およびフローの設定 (Portal Behavior and Flow Settings)] > [ゲストによるパスワード変更設定 (Guest Change Password Settings)] です。

- [ゲストにログイン後のパスワード変更を許可 (Allow guests to change password after login)] : ゲストが正常に認証され、AUP に同意した後に、ゲストに必要なに応じてパスワードを変更することを許可します。

ゲストが自分のパスワードを変更した場合、スポンサーはゲストにログインクレデンシャル情報を提供できません。スポンサーは、ゲストのパスワードをランダムパスワードにリセットすることだけが可能です。

## クレデンシャルを持つゲスト ポータルのゲスト デバイス登録の設定

### ゲスト デバイス登録設定 (Guest Device Registration Settings)

このページへのナビゲーションパスは、[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [ゲスト ポータル (Guest Portals)] > [作成、編集または複製 (Create, Edit or Duplicate)] > [ポータルの動作およびフローの設定 (Portal Behavior and Flow Settings)] > [ゲスト デバイス登録設定 (Guest Device Registration Settings)] です。

これらの設定を使用して、ゲストがログインしたら Cisco ISE がゲストのデバイスを自動的に登録するようにするか、ゲストがログイン後に手動で自身のデバイスを登録することを許可できます。



各ゲスト タイプの最大デバイス数は、[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [ゲスト タイプ (Guest Types)] で指定されます。

- [ゲストのデバイスを自動登録 (Automatically register guest devices)] : ゲストがこのポータルにアクセスするデバイスのエンドポイントを自動的に作成します。エンドポイントは、このポータルに指定されたエンドポイント ID グループに追加され、。

許可ルールを作成が可能になり、該当 ID グループ内のエンドポイントへのアクセスが許可されます。そのため、Web 認証は不要になります。

登録済みデバイスの最大数に到達すると、システムは自動的に最初の登録デバイスを削除し、ゲストがログインしようとしているデバイスを登録し、このことをゲストに通知します。[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [ゲスト タイプ (Guest Types)] を選択し、ゲストが登録できるデバイスの最大数を変更します。

- [ゲストにデバイスの登録を許可 (Allow guests to register devices)] : ゲストは、名前、説明、および MAC アドレスを入力して、自分のデバイスを手動で登録できます。MAC アドレスはエンドポイント ID グループに関連付けられます。

登録済みデバイスの最大数に到達した場合に別のデバイスを登録できるようにするには、ゲストは少なくとも 1 個のデバイスを削除する必要があります。

## クレデンシャルを持つゲスト ポータルの BYOD 設定

このページへのナビゲーション パスは、[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [ゲスト ポータル (Guest Portals)] > [作成、編集または複製 (Create, Edit or Duplicate)] > [ポータルの動作およびフローの設定 (Portal Behavior and Flow Settings)] > [BYOD 設定 (BYOD Settings)] です。

この設定を使用して、従業員などゲスト以外の個人所有デバイスの持ち込み (BYOD) 機能を有効にし、クレデンシャルを持つゲスト ポータルを使用して企業ネットワークにアクセスできるようにします。

| フィールド                                                                                      | 使用上のガイドライン                                                                                                                                                                                                                                                              |
|--------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 従業員がネットワークでパーソナル デバイスを使用することを許可する (Allow employees to use personal devices on the network) | このポータルに [従業員の個人所有デバイス (BYOD) の登録 (Employee Bring Your Own Device (BYOD) Registration)] ページを追加して、従業員がデバイス登録プロセスを実行できるようにして、場合によってはネイティブ サプリカントおよび証明書のプロビジョニングを実行できるようにします。これは、従業員のパーソナル デバイス タイプ (iOS、Android、RT またはモバイルを除く Windows、OSX など) のクライアントプロビジョニングの設定に応じて異なります。 |

| フィールド                                                                       | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| エンドポイント ID グループ (Endpoint Identity Group)                                   | ゲストのデバイスを追跡するためのエンドポイント ID グループを選択します。Cisco ISE はデフォルトとして使用する <b>GuestEndpoints</b> のエンドポイント ID グループを提供します。デフォルトを使用しない場合、追加のエンドポイント ID グループを作成することもできます。                                                                                                                                                                                                                                                   |
| 従業員にゲスト アクセスの選択のみを許可する (Allow employees to choose to get guest access only) | 従業員をゲスト ネットワークにアクセスさせて、企業ネットワークへのアクセスに必要なことがある追加のプロビジョニングおよび登録を避けます。                                                                                                                                                                                                                                                                                                                                       |
| 登録時にデバイス ID フィールドを表示する (Display Device ID field during registration)        | 登録プロセス中に、デバイス ID をユーザに表示します。これは、デバイス ID が事前設定されており、BYOD ポータルを使用しているときに変更できない場合も含まれます。                                                                                                                                                                                                                                                                                                                      |
| 元の URL (Originating URL)                                                    | <p>ネットワークへの認証に成功すると、可能な場合はユーザのブラウザを、ユーザがアクセスしようとしていた元の Web サイトにリダイレクトします。リダイレクトできない場合は、認証成功ページが表示されます。リダイレクト URL が NAD のアクセスコントロールリストとその NAD の ISE で設定された許可プロファイルにより、PSN のポート 8443 で動作することを確認します。</p> <p>Windows、MAC、および Android デバイスの場合、制御はプロビジョニングを実行するセルフプロビジョニングウィザードアプリケーションに渡されます。そのため、これらのデバイスは元の URL にリダイレクトされません。ただし、iOS (dot1X) およびサポート対象外のデバイス (ネットワーク アクセスが許可されている) では、この URL にリダイレクトされます。</p> |
| 成功ページ (Success page)                                                        | デバイスの登録が成功したことを示すページを表示します。                                                                                                                                                                                                                                                                                                                                                                                |
| URL                                                                         | ネットワークへの認証に成功すると、ユーザのブラウザを指定された URL (会社の Web サイトなど) にリダイレクトします。                                                                                                                                                                                                                                                                                                                                            |

## クレデンシャルを持つゲスト ポータルのポストログイン バナー ページ設定

このページのナビゲーションパスは、[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [ゲスト ポータル または スポンサー ポータル (Guest Portals or Sponsor Portals)] > [作成、編集または複製 (Create, Edit or Duplicate)] > [ポータルの動作およびフローの設定 (Portal Behavior and Flow Settings)] > [ポストログインバナーページ設定 (Post-Login Banner Page Settings)] です。

これらの設定を使用して、正常なログイン後にユーザ（状況に応じてゲスト、スポンサーまたは従業員）に追加情報を通知します。

| フィールド                                                     | 使用上のガイドライン                                    |
|-----------------------------------------------------------|-----------------------------------------------|
| ポストログイン バナー ページを含める<br>(Include a Post-Login Banner page) | ユーザが正常にログインした後、ネットワーク アクセスを付与される前に追加情報を表示します。 |

## クレデンシャルを持つゲスト ポータルのゲスト デバイスのコンプライアンス設定

このページへのナビゲーションパスは、[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [ゲスト ポータル (Guest Portals)] > [作成、編集または複製 (Create, Edit or Duplicate)] > [ポータルの動作およびフローの設定 (Portal Behavior and Flow Settings)] > [ゲスト デバイスのコンプライアンス設定 (Guest Device Compliance Settings)] です。これらの設定を使用して、ネットワークにアクセスするためにデバイスのクライアントプロビジョニングを実行するようゲストおよびゲスト ポータルを使用する従業員に要求します。

- [ゲスト デバイス コンプライアンスが必要 (Require guest device compliance)] : ゲストをポスチャージェントのダウンロードを要求する [クライアントプロビジョニング (Client Provisioning)] ページにリダイレクトします。これにより、ウイルス対策ソフトウェアのチェックなど、ゲストのポスチャ ポリシーを設定するゲスト フローにクライアントプロビジョニングが追加されます。

ゲストが、ネットワークへのアクセスにクレデンシャルを持つゲストポータルを使用している従業員の場合：

- [BYOD 設定 (BYOD Settings)] で [従業員にネットワークでのパーソナルデバイスの使用を許可する (Allow employees to use personal devices on the network)] が有効になっている場合、従業員はBYODフローにリダイレクトされ、クライアントのプロビジョニングは実行されません。
- [BYOD 設定 (BYOD Settings)] で [従業員にネットワークでのパーソナルデバイスの使用を許可する (Allow employees to use personal devices on the network)] および [従業員にゲストアクセスの選択のみを許可する (Allow employees to choose to get guest access)]

only) ] が有効になっていて、従業員がゲストアクセスを選択する場合、[クライアントプロビジョニング (Client Provisioning) ] ページにルーティングされます。

## ゲストポータルの VLAN DHCP リリース ページ設定

このページへのナビゲーションパスは、[ワーク センター (Work Centers) ] > [ゲスト アクセス (Guest Access) ] > [ポータルとコンポーネント (Portals & Components) ] > [ゲスト ポータル (Guest Portals) ] > [作成、編集または複製 (Create, Edit or Duplicate) ] > [ポータルの動作およびフローの設定 (Portal Behavior and Flow Settings) ] > [VLAN DHCP リリース ページの設定 (VLAN DHCP Release Page Settings) ] です。

- [VLAN DHCP リリースを有効にする (Enable VLAN DHCP release) ] : 有線環境と無線環境の両方で VLAN が変更された後、Windows および Mac OS デバイスのゲストの IP アドレスを更新します。

これは、ネットワーク アクセスでゲスト VLAN が新しい VLAN に変更されたときに、最終的な許可処理時の中央 WebAuth (CWA) フローに影響します。ゲストの古い IP アドレスは VLAN の変更の前にリリースされる必要があります。ゲストが新しい VLAN に接続するときに新しいゲスト IP アドレスが DHCP を介して要求される必要があります。IP アドレスのリリースおよび更新操作は、使用しているブラウザおよびオペレーティングシステムによって異なります。Internet Explorer は ActiveX コントロールを使用し、Firefox と Google Chrome は Java アプレットを使用します。Internet Explorer 以外のブラウザでは、ブラウザで Java をインストールして有効にする必要があります。

VLAN DHCP リリース オプションは、モバイルデバイスでは動作しません。代わりに、ゲストが IP アドレスを手動でリセットする必要があります。この方法はデバイスによって異なります。たとえば、Apple iOS デバイスでは、ゲストは Wi-Fi ネットワークを選択して、[リースを更新 (Renew Lease) ] ボタンをクリックできます。

- [リリースを\_\_秒遅延 (Delay to release \_\_ seconds) ] : リリース遅延時間を入力します。リリースは、アプレットをダウンロードした直後から、Cisco ISE サーバが CoA 要求を再認証するよう NAD に指示するまでの間に行う必要があるため、この時間は短くすることを推奨します。
- [CoA を\_\_秒遅延 (Delay to CoA \_\_ seconds) ] : Cisco ISE が CoA の実行を遅延する時間を入力します。十分な時間を指定して (ガイドラインとしてデフォルト値を使用)、アプレットによるクライアント上での IP リリースのダウンロードと実行を可能にします。
- [更新を\_\_秒遅延 (Delay to renew \_\_ seconds) ] : 更新を遅延する値を入力します。この時間は IP リリース値に追加され、コントロールがダウンロードされるまで計時が開始されません。十分な時間を指定して (ガイドラインとしてデフォルト値を使用)、CoA の処理を可能にし、新しい VLAN アクセスが付与されるようにします。

## ゲスト ポータルの認証成功の設定

このページのナビゲーション パスは、[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [ゲスト ポータル (Guest Portals)] > [作成、編集または複製 (Create, Edit or Duplicate)] > [ポータルの動作およびフローの設定 (Portal Behavior and Flow Settings)] > [認証成功の設定 (Authentication Success Settings)] です。

これらの設定では、ユーザ（状況に応じてゲスト、スポンサーまたは従業員）に認証の成功が通知されるか、または URL が表示されます。[認証されたらゲストに次を表示： (Once authenticated, take guest to:)] で、次のフィールドを設定します。

- 元の URL (Originating URL) : ネットワークへの認証に成功すると、可能な場合はユーザのブラウザを、ユーザがアクセスしようとしていた元の Web サイトにリダイレクトします。リダイレクトできない場合は、認証成功ページが表示されます。リダイレクト URL が NAD のアクセス コントロール リストとその NAD の ISE で設定された許可プロファイルにより、PSN のポート 8443 で動作することを確認します。

Windows、MAC、および Android デバイスの場合、制御はプロビジョニングを実行するセルフプロビジョニング ウィザードアプリケーションに渡されます。そのため、これらのデバイスは元の URL にリダイレクトされません。ただし、iOS (dot1X) およびサポート対象外のデバイス（ネットワーク アクセスが許可されている）では、この URL にリダイレクトされます。

- 認証の成功ページ (Authentication Success page) : ユーザの認証に成功した通知。
- URL : ネットワークへの認証に成功すると、ユーザのブラウザを指定された URL（会社の Web サイトなど）にリダイレクトします。



(注) 認証後に外部 URL にゲストをリダイレクトする場合、URL アドレスを解決して、セッションがリダイレクトされるまでに遅延が生じることがあります。リダイレクト URL が NAD のアクセス コントロール リストとその NAD の ISE で設定された許可プロファイルにより、PSN のポート 8443 で動作することを確認します。

## ゲスト ポータルのサポート情報ページの設定

このページのナビゲーション パスは、[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [ゲスト ポータル (Guest Portals)] > [作成、編集または複製 (Create, Edit or Duplicate)] > [ポータルの動作およびフローの設定 (Portal Behavior and Flow Settings)] > [サポート情報ページの設定 (Support Information Page Settings)] です。

これらの設定を使用して、ヘルプデスクがユーザ（状況に応じてゲスト、スポンサーまたは従業員）が体験したアクセスの問題をトラブルシューティングするために使用できる情報を表示します。

| フィールド                                              | 使用上のガイドライン                                                                                                                                                                     |
|----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| サポート情報ページを含める (Include a Support Information Page) | 該当ポータルのすべての有効なページ上で、 <b>問い合わせ先</b> などの情報へのリンクを表示します。                                                                                                                           |
| MAC アドレス                                           | [サポート情報 (Support Information)] ページにデバイスの MAC アドレスを含めます。                                                                                                                        |
| IP アドレス                                            | [サポート情報 (Support Information)] ページにデバイスの IP アドレスを含めます。                                                                                                                         |
| ブラウザのユーザエージェント (Browser user agent)                | [サポート情報 (Support Information)] ページに、要求の発信元のユーザエージェントの製品名とバージョン、レイアウトエンジン、バージョンなど、ブラウザの詳細を含めます。                                                                                 |
| ポリシー サーバ (Policy server)                           | [サポート情報 (Support Information)] ページに、このポータルを提供している ISE ポリシーサービス ノード (PSN) の IP アドレスを含めます。                                                                                       |
| 障害コード (Failure code)                               | 可能な場合は、ログメッセージカタログ内の対応する番号を含めます。メッセージカタログにアクセスしてこれを表示するには、 <b>[管理 (Administration)] &gt; [システム (System)] &gt; [ロギング (Logging)] &gt; [メッセージ カタログ (Message Catalog)]</b> に移動します。 |
| フィールドを隠す (Hide field)                              | 含める情報が存在しない場合、[サポート情報 (Support Information)] ページ上の該当するフィールドラベルを表示しません。たとえば、障害コードが不明であるために空白である場合、[障害コード (Failure code)] は、選択されている場合でも表示されません。                                  |
| 値のないラベルを表示 (Display label with no value)           | 含める情報が存在しない場合でも、選択されているすべてのフィールドのラベルを [サポート情報 (Support Information)] ページに表示します。たとえば、障害コードが不明な場合、[障害コード (Failure code)] は空白であっても表示されます。                                         |

| フィールド                                            | 使用上のガイドライン                                                                                                                                                                                                 |
|--------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| デフォルト値でラベルを表示 (Display label with default value) | [サポート情報 (Support Information)] ページ上の選択されているフィールドに含まれる情報が存在しない場合、このテキストがこれらのすべてのフィールドに表示されます。たとえば、このフィールドに「Not Available」と入力した場合に障害コード不明が不明な場合は、[障害コード (Failure code)] に [使用できません (Not Available)] と表示されます。 |

## スポンサー ポータル アプリケーションの設定

### ポータル ID 設定

これらの設定へのナビゲーションパスは、[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [ゲスト ポータルまたはスポンサー ポータル (Guest Portals or Sponsor Portals)] > [作成、編集または複製 (Create, Edit or Duplicate)] > [ゲスト ポータルおよびスポンサー ポータルの設定とカスタマイズ (Guest Portals or Sponsor Portals Settings and Customization)] です。

- ポータル名 (Portal Name) : このポータルにアクセスするための一意のポータル名を入力します。このポータル名を、その他のスポンサーやゲスト ポータルおよび非ゲスト ポータル (ブラックリスト、個人所有デバイス持ち込み (BYOD)、クライアントプロビジョニング、モバイル デバイス管理 (MDM)、またはデバイスの各ポータル) に使用しないでください。

この名前は、許可プロファイルのポータルの選択でリダイレクションの選択肢として表示され、ポータルのリストで他のポータルの中から簡単に識別するために使用されます。

- [説明 (Description)] : 任意項目です。
- ポータル テスト URL (Portal test URL) : [保存 (Save)] をクリックした後にリンクとして表示されるシステムにより生成された URL。ポータルをテストするために使用します。

リンクをクリックすると、このポータルの URL を表示する新しいブラウザ タブが開きます。これを有効にするには、ポリシー サービスを含むポリシー サービス ノード (PSN) をオンにする必要があります。ポリシー サービスがオンになっていない場合、PSN は管理者用ポータルのみを表示します。



(注) テスト ポータルは RADIUS セッションをサポートしていないため、すべてのポータルに対するポータルフローの全体は表示されません。BYOD およびクライアントプロビジョニングは RADIUS セッションに依存するポータルの例です。たとえば、外部 URL へのリダイレクションは機能しません。

- 言語ファイル (Language File) : 各ポータル タイプは、デフォルトで 15 種類の言語をサポートします。これらの言語は、個々のプロパティファイルとして使用できます。これらのファイルは、圧縮された単一の言語ファイル内にまとめてバンドルされています。ポータルで使用する圧縮言語ファイルをエクスポートまたはインポートします。圧縮言語ファイルには、ポータルのテキストを表示するために使用可能な個別の言語ファイルがすべて含まれています。

言語ファイルには、その言語のポータル全体のすべての文字列設定に加え、特定のブラウザのロケール設定 (例: フランス語の場合は `fr`、`fr-fr`、`fr-ca`) へのマッピングが含まれています。1 つの言語ファイルには、翻訳およびローカリゼーションの目的に容易に使用できるように、サポートされるすべての言語が含まれています。

1 つの言語用のブラウザ ロケール設定を変更した場合、変更内容は他のすべてのエンドユーザ Web ポータルに適用されます。たとえば、ホットスポット ゲスト ポータルの `French.properties` ブラウザ ロケールを `fr,fr-fr,fr-ca` から `fr,fr-fr` に変更すると、この変更内容がデバイス ポータルにも適用されます。

[ポータルページのカスタマイズ (Portal Page Customizations)] タブでいずれかのポータル ページテキストをカスタマイズすると、警告アイコンが表示されます。警告メッセージは、ポータルのカスタマイズ時に 1 つの言語で行った変更をすべてのサポート対象の言語 プロパティファイルで更新するように注意を促します。ドロップダウンリストのオプションを使用して、手動で警告アイコンが表示されないようにします。また、警告アイコンは、更新された圧縮言語ファイルのインポート後に自動的に表示されなくなります。

## スポンサー ポータルのポータル設定

これらの設定を設定して、ポータルを特定し、すべてのポータルページで使用する言語ファイルを選択します。

- [HTTPS ポート (HTTPS port)] : 8000 ~ 8999 の範囲のポート値を入力します。デフォルト値はすべてのデフォルト ポータルで 8443 です。ただし、ブラックリスト ポータルは 8444 です。この範囲外のポート値を使用してアップグレードした場合は、このページで変更を加えるまで維持されます。このページを変更する場合は、この制限に従うようにポート設定を更新します。

ゲスト ポータルに非ゲスト ポータル (マイ デバイスなど) によって使用されるポートを割り当てると、エラー メッセージが表示されます。



ポスチャ評価と修復についてのみ、クライアントプロビジョニングポータルはポート 8905 および 8909 も使用します。それ以外の場合は、ゲスト ポータルへの割り当てと同じポートを使用します。

同じ HTTPS ポートに割り当てられたポータルは、同じギガビットイーサネットインターフェイスまたは別のインターフェイスを使用できます。これらのポータルが同じポートとインターフェイスの組み合わせを使用している場合、同じ証明書グループタグを使用する必要があります。次に例を示します。

- スポンサー ポータルを例として使用した有効な組み合わせを次に示します。
    - スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書タグ **A**、およびデバイス ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**
    - スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**、およびデバイス ポータル：ポート **8445**、インターフェイス **0**、証明書グループ **B**
    - スポンサー ポータル：ポート **8444**、インターフェイス **1**、証明書グループ **A**、およびブラックリストポータル：ポート **8444**、インターフェイス **0**、証明書グループ **B**
  - 無効な組み合わせには次が含まれます。
    - スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**、およびデバイス ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **B**
    - スポンサー ポータル：ポート **8444**、インターフェイス **0**、証明書タグ **A**、およびブラックリストポータル：ポート **8444**、インターフェイス **0**、証明書グループ **A**
  - [使用可能インターフェイス (Allowed interfaces)] : PAN がポータルの実行に使用できる PSN インターフェイスを選択します。ポータルを開く要求が PAN で行われると、PAN は PSN で使用可能なポートを探します。異なるサブネット上の IP アドレスを使用してイーサネット インターフェイスを設定する必要があります。
- これらのインターフェイスは、ポリシー サービスがオンになっているすべての PSN (VM ベースを含む) で使用可能である必要があります。これは、これらのすべての PSN がゲストセッションの開始時にリダイレクトに使用される可能性があるため、必須要件です。
- イーサネット インターフェイスは、異なるサブネット上の IP アドレスを使用する必要があります。
  - ここで有効にするインターフェイスは、ポリシー サービスがオンになっているときの VM ベースのものを含む、すべての PSN で使用できるものでなければなりません。これは、これらのすべての PSN がゲストセッションの開始時にリダイレクトに使用される可能性があるため必須です。
  - ポータルの証明書のサブジェクト名とサブジェクトの代替名はインターフェイス IP に解決する必要があります。

- ISE CLI で **ip host x.x.x.x yyy.domain.com** を設定して、セカンダリ インターフェイス IP を FQDN にマッピングします。これは、証明書のサブジェクト名とサブジェクトの代替名と一致させるために使用されます。
  - ボンディングされた NIC のみが選択されている場合：PSN がポータルを設定しようとする、最初にボンディング インターフェイスを設定しようとしています。これが成功しない場合、おそらくは、その PSN でボンディングが設定されていないために、PSN でエラーが記録されて終了します。PSN は物理 インターフェイスでのポータルの開始を試みません。
  - **NIC チーミング** またはボンディングは、高可用性（耐障害性）のために 2 つの個別の NIC を設定できる、O/S 設定オプションです。どちらかの NIC に障害が発生すると、ボンディングされた接続の一部であるもう一方の NIC は、接続を続行します。1 つの NIC がポータル設定に基づきポータルに対して選択されます。
    - 物理 NIC と対応するボンディングされた NIC の両方が設定されている場合：PSN がポータルを設定しようとする、最初にボンディング インターフェイスへ接続しようとしています。これが成功しない場合、その PSN にボンドセットアップがなかったことが原因である可能性があるため、PSN は物理 インターフェイスでポータルを開始しようとしています。
  - [証明書グループ タグ (Certificate group tag)]：ポータルの HTTPS トラフィックに使用する証明書を指定する証明書グループ タグを選択します。
  - [完全修飾ドメイン名 (FQDN) (Fully Qualified Domain Name (FQDN)) ]：スポンサーまたはデバイス ポータルに対応する 1 つの固有の FQDN またはホスト名を入力します。たとえば、**sponsorportal.yourcompany.com**、**sponsor** と入力することで、ユーザはブラウザにこれらのいずれかを入力すると、スポンサーポータルが表示されます。カンマを使用して名前を区切りますが、エントリ間にスペースを挿入しないでください。  
デフォルトの FQDN を変更する場合は、次を実行します。
    - DNS を更新して、新しい URL の FQDN が有効なポリシー サービス ノード (PSN) の IP アドレスに解決するようにします。PSN のプールを提供するロード バランサの仮想 IP アドレスを指定することもできます。
    - 名前の不一致による証明書の警告メッセージを回避するために、Cisco ISE PSN のローカル サーバ証明書のサブジェクト代替名 (SAN) 属性に、カスタマイズされた URL の FQDN またはワイルドカードを含めます。
  - [認証方式 (Authentication Method)]：ユーザ認証に使用する ID ソース順序 (ISS) または ID プロバイダー (IdP) を選択します。ISS は、ユーザ クレデンシャルを確認するために順番に検索される ID ストアのリストです。たとえば、内部ゲスト ユーザ、内部ユーザ、Active Directory、LDAP ディレクトリ などがあります。
- Cisco ISE には、スポンサー ポータル **Sponsor\_Portal\_Sequence** 用のデフォルトのスポンサー ID ソース順序が含まれています。

IdP を設定するには、[管理 (Administration)] > [ID の管理 (Identity Management)] > [外部 ID ソース (External Identity Sources)] > [SAML ID プロバイダー (SAML Id Providers)] の順に選択します。

ID ソース順序を設定するには、[管理 (Administration)] > [ID の管理 (Identity Management)] > [ID ソース順序 (Identity Source Sequences)] の順に選択します。

- [アイドル タイムアウト (Idle timeout)] : ポータルでアクティビティがない場合にユーザーをログアウトするまでに Cisco ISE が待機する時間 (分) を入力します。有効な範囲は 1 ～ 30 分です。
- [Kerberos を許可する (Allow Kerberos)] : スポンサー ポータルへアクセスするためのスポンサーの認証に Kerberos を使用します。ブラウザが ISE との SSL 接続を確立した後、セキュア トンネル内で Kerberos SSO が実行されます。



(注) Kerberos 認証には、同じドメイン内に存在する次の項目が必要です。

- スポンサーの PC
- ISE PSN
- このスポンサー ポータルに設定された FQDN



(注) ゲスト ポータルの Kerberos 認証はサポートされていません。

#### • 表示言語

- [ブラウザのロケールを使用する (Use browser locale)] : クライアント ブラウザのロケール設定で指定された言語をポータルの表示言語として使用します。ブラウザ ロケールの言語が ISE でサポートされていない場合は、フォールバック言語が言語ポータルとして使用されます。
- [フォールバック言語 (Fallback language)] : ブラウザ ロケールから言語を取得できない場合、またはブラウザ ロケール言語が ISE でサポートされていない場合に使用する言語を選択します。
- [常に使用 (Always use)] : ポータルに使用する表示言語を選択します。この設定は、ユーザーのブラウザのロケール オプションを上書きします。

[スポンサーに使用可能な SSID (SSIDs available to sponsors)] : ゲストの訪問にあたり、スポンサーが正しい接続先ネットワークとしてゲストに通知できる、ネットワークの名前または SSID (セッション サービス識別子) を入力します。

- [スポンサーに使用可能な SSID (SSIDs available to sponsors)] : ゲストの訪問にあたり、スポンサーが正しい接続先ネットワークとしてゲストに通知できる、ネットワークの名前または SSID (セッション サービス識別子) を入力します。

## スポンサー ポータルのログイン設定

### スポンサー ポータルのログイン ページ設定

このページへのナビゲーションパスは、[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [スポンサー ポータル (Sponsor Portals)] > [作成、編集または複製 (Create, Edit or Duplicate)] > [ポータルの動作およびフローの設定 (Portal Behavior and Flow Settings)] > [ログイン ページの設定 (Login Page Settings)] です。

- [頻度制限までの最大ログイン試行失敗数 (Maximum failed login attempts before rate limiting)] : Cisco ISE がアカウントのスロットルを開始するまでの単一のブラウザセッションからのログイン試行失敗回数を指定します。これにより、アカウントのロックアウトは起きません。スロットル率は、[頻度制限時のログイン試行間隔 (Time between login attempts when rate limiting)] で設定されます。
- [頻度制限時のログイン試行間隔 (Time between login attempts when rate limiting)] : [頻度制限までの最大ログイン試行失敗数 (Maximum failed login attempts before rate limiting)] で定義された回数のログインの失敗後に、ユーザが再度ログインを試行するまでに待機する必要がある時間 (スロットル率) を分単位で設定します。
- [AUP を含める (Include an AUP)] : フローに利用規約ページを追加します。AUP をページに追加したり、別のページへのリンクを設定することができます。これを追加すると、右側のフローの画像が変わります。
  - [同意が必要 (require acceptance)] : フローを続行する前に、ユーザが AUP に同意するように強制します。

## スポンサー ポータルの利用規定 (AUP) 設定

このページのナビゲーションパスは、[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [スポンサー ポータル (Sponsor Portals)] > [作成、編集または複製 (Create, Edit or Duplicate)] > [ポータルの動作およびフローの設定 (Portal Behavior and Flow Settings)] > [利用規定 (AUP) ページ設定 (Acceptable Use Policy (AUP) Page Settings)] です。

これらの設定を使用して、ユーザ (状況に応じてゲスト、スポンサーまたは従業員) に対して AUP エクスペリエンスを定義します。

| フィールド                             | 使用上のガイドライン                       |
|-----------------------------------|----------------------------------|
| AUP ページを含める (Include an AUP page) | 会社のネットワーク使用諸条件を、別のページでユーザに表示します。 |

| フィールド                                                        | 使用上のガイドライン                                                                     |
|--------------------------------------------------------------|--------------------------------------------------------------------------------|
| AUP の最後までスクロールが必要 (Require scrolling to end of AUP)          | ユーザが AUP を最後まで読んだことを確認します。[同意 (Accept)] ボタンは、ユーザが AUP の最後までスクロールするとアクティブになります。 |
| 初回のログインのみ (On first login only)                              | ユーザがネットワークまたはポータルに初めてログインしたときのみ、AUP を表示します。                                    |
| ログインごと (On every login)                                      | ユーザがネットワークまたはポータルにログインするごとに、AUP を表示します。                                        |
| __ 日ごと (初回のログインから) (Every __ days (starting at first login)) | ユーザがネットワークまたはポータルに初めてログインした後に、定期的に AUP を表示します。                                 |

## スポンサー ポータルのスポンサーのパスワード変更設定

このページへのナビゲーションパスは、[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [スポンサー ポータル (Sponsor Portals)] > [作成、編集または複製 (Create, Edit or Duplicate)] > [ポータルの動作およびフローの設定 (Portal Behavior and Flow Settings)] > [スポンサーによるパスワード変更設定 (Sponsor Change Password Settings)] です。スポンサー ポータルを使用してスポンサーのパスワード要件を定義するには、これらの設定を使用します。

スポンサーのパスワード ポリシーを設定するには、[管理 (Administration)] > [ID の管理 (Identity Management)] > [設定 (Settings)] > [ユーザパスワード ポリシー (User Password Policy)] を選択します。

| フィールド                                                              | 使用上のガイドライン                                                                                                              |
|--------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| スポンサーは自身のパスワードを変更可能 (Allow sponsors to change their own passwords) | スポンサーは、スポンサー ポータルにログインした後、自身のパスワードを変更できます。このオプションは、スポンサーが内部ユーザデータベースの一部である場合にだけ、[パスワードの変更 (Change Password)] ページを表示します。 |

## スポンサー ポータルのポストログイン バナー設定

このページのナビゲーションパスは、[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [ゲスト ポータルまたはスポンサー ポータル (Guest Portals or Sponsor Portals)] > [作成、編集または複製 (Create, Edit or Duplicate)] > [ポータルの動作およびフローの設定 (Portal Behavior and Flow Settings)] > [ポストログインバナーページ設定 (Post-Login Banner Page Settings)] です。

これらの設定を使用して、正常なログイン後にユーザ（状況に応じてゲスト、スポンサーまたは従業員）に追加情報を通知します。

| フィールド                                                     | 使用上のガイドライン                                    |
|-----------------------------------------------------------|-----------------------------------------------|
| ポストログイン バナー ページを含める<br>(Include a Post-Login Banner page) | ユーザが正常にログインした後、ネットワーク アクセスを付与される前に追加情報を表示します。 |

## スポンサー ポータルのサポート情報ページの設定

このページのナビゲーション パスは、[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [スポンサーポータル (Sponsor Portals)] > [作成、編集または複製 (Create, Edit or Duplicate)] > [ポータルの動作およびフローの設定 (Portal Behavior and Flow Settings)] > [サポート情報ページの設定 (Support Information Page Settings)] です。

これらの設定を使用して、ヘルプデスクがユーザ（状況に応じてゲスト、スポンサーまたは従業員）が体験したアクセスの問題をトラブルシューティングするために使用できる情報を表示します。

| フィールド                                              | 使用上のガイドライン                                                                                      |
|----------------------------------------------------|-------------------------------------------------------------------------------------------------|
| サポート情報ページを含める (Include a Support Information Page) | 該当ポータルのすべての有効なページ上で、問い合わせ先などの情報へのリンクを表示します。                                                     |
| MAC アドレス                                           | [サポート情報 (Support Information)] ページにデバイスの MAC アドレスを含めます。                                         |
| IP アドレス                                            | [サポート情報 (Support Information)] ページにデバイスの IP アドレスを含めます。                                          |
| ブラウザのユーザ エージェント (Browser user agent)               | [サポート情報 (Support Information)] ページに、要求の発信元のユーザ エージェントの製品名とバージョン、レイアウトエンジン、バージョンなど、ブラウザの詳細を含めます。 |
| ポリシー サーバ (Policy server)                           | [サポート情報 (Support Information)] ページに、このポータルを提供している ISE ポリシー サービス ノード (PSN) の IP アドレスを含めます。       |

| フィールド                                            | 使用上のガイドライン                                                                                                                                                                                                                       |
|--------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 障害コード (Failure code)                             | 可能な場合は、ログメッセージカタログ内の対応する番号を含めます。メッセージカタログにアクセスしてこれを表示するには、 <b>[管理 (Administration)] &gt; [システム (System)] &gt; [ロギング (Logging)] &gt; [メッセージカタログ (Message Catalog)]</b> に移動します。                                                    |
| フィールドを隠す (Hide field)                            | 含める情報が存在しない場合、 <b>[サポート情報 (Support Information)]</b> ページ上の該当するフィールドラベルを表示しません。たとえば、障害コードが不明であるために空白である場合、 <b>[障害コード (Failure code)]</b> は、選択されている場合でも表示されません。                                                                    |
| 値のないラベルを表示 (Display label with no value)         | 含める情報が存在しない場合でも、選択されているすべてのフィールドのラベルを <b>[サポート情報 (Support Information)]</b> ページに表示します。たとえば、障害コードが不明な場合、 <b>[障害コード (Failure code)]</b> は空白であっても表示されます。                                                                            |
| デフォルト値でラベルを表示 (Display label with default value) | <b>[サポート情報 (Support Information)]</b> ページ上の選択されているフィールドに含まれる情報が存在しない場合、このテキストがこれらのすべてのフィールドに表示されます。たとえば、このフィールドに「Not Available」と入力した場合に障害コード不明が不明な場合は、 <b>[障害コード (Failure code)]</b> に <b>[使用できません (Not Available)]</b> と表示されます。 |

## スポンサー ポータルのゲストへの通知のカスタマイズ

これらの設定へのナビゲーションパスは、**[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [スポンサー ポータル (Sponsor Portals)] > [作成、編集または複製 (Create, Edit or Duplicate)] > [ポータル ページのカスタマイズ (Portal Page Customization)] > [ゲストへの通知 (Notify Guests)]** です。

**[ページのカスタマイズ (Page Customizations)]** で、スポンサーがスポンサー ポータルからゲストに送信する通知に表示される、メッセージ、タイトル、コンテンツ、手順、およびフィールドやボタンのラベルをカスタマイズできます。

**[設定 (Settings)]** では、スポンサーが電子メールまたは SMS を使用してゲストにユーザ名とパスワードを個別に送信できるかどうかを指定できます。また、ヘルプデスクがアクセスの間

題をトラブルシューティングするために使用できる情報を提供するために、スポンサーがゲストに [サポート情報 (Support Information)] ページを表示できるかどうかを指定できます。

## スポンサー ポータルのカスタマイズの管理と承認

これらの設定へのナビゲーションパスは、[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [スポンサー ポータル (Sponsor Portals)] > [作成、編集または複製 (Create, Edit or Duplicate)] > [ポータル ページのカスタマイズ (Portal Page Customization)] > [管理と承認 (Manage and Approve)] です。

[ページのカスタマイズ (Page Customizations)] で、スポンサー ポータルの [管理と承認 (Manage and Approve)] タブに表示される、メッセージ、タイトル、コンテンツ、手順、およびフィールドやボタンのラベルをカスタマイズできます。

これらには、アカウント (登録済みおよび保留) の概要および詳細ビュー、スポンサーがゲストアカウントに対して実行する編集、拡張、一時停止などの操作に基づいて表示されるポップアップ ダイアログ、さらに汎用ポータルやアカウント アクション メッセージが含まれています。

## グローバル設定 (Global Settings)

### ゲストおよびスポンサー ポータルのグローバル設定

[ゲスト アクセス (Guest Access)] > [設定 (Settings)] を選択します。Cisco ISE 内のゲストポータル、スポンサー ポータル、ゲスト タイプ、およびスポンサー グループに適用される、次の一般設定を設定できます。

- ゲスト アカウントの消去、およびユーザ名とパスワードの生成のポリシー。
- 電子メールおよび SMS 通知をゲスト アカウントとスポンサーに送信するときに使用する SMTP サーバおよび SMS ゲートウェイ。
- アカウント登録ゲスト ポータルを使用したゲスト アカウントの作成およびゲストの登録時に選択する場所、タイムゾーン、SSID およびカスタム フィールド。

これらのグローバル設定を指定すると、特定のゲスト ポータルとスポンサー ポータル、ゲスト タイプおよびスポンサー グループの設定時にそれらを必要に応じて使用できます。

[ポータル設定 (Portal settings)] ページには、次のタブがあります。

- [ゲストアカウントの消去ポリシー (Guest Account Purge Policy)] : 期限が切れたゲストアカウントを消去する時期をスケジューリングします。詳細については、[期限切れのゲストアカウントを消去するスケジューリング設定 \(529 ページ\)](#) を参照してください。



- [カスタムフィールド (Custom Fields)] : ユーザから追加情報を取得するためにゲストポータルで使用するカスタムフィールドを追加します。詳細については、[ゲストアカウント作成用のカスタムフィールドの追加 \(530 ページ\)](#) を参照してください。
- [ゲスト電子メールの設定 (Guest Email Settings)] : アカウントの変更をゲストに電子メール通知するかどうかを決定します。詳細については、[電子メールでの通知用の電子メールアドレスおよび SMTP サーバの指定 \(531 ページ\)](#) を参照してください。
- [ゲストのロケーションおよびSSID (Guest Locations and SSIDs)] : ロケーションと、ゲストがそのロケーションで使えるネットワークのサービスセット識別子 (SSID) を設定します。詳細については、[ゲストのロケーションおよびSSIDの割り当て \(532 ページ\)](#) を参照してください。
- [ゲストユーザ名ポリシー (Guest Username Policy)] : ゲストユーザ名の作成方法を設定します。詳細については、[ゲストユーザ名ポリシーの設定 \(535 ページ\)](#) および[ゲストパスワードポリシーのルール \(533 ページ\)](#) を参照してください。
- [ゲストパスワードポリシー (Guest Password Policy)] : すべてのゲストポータルとスポンサーポータルのゲストパスワードポリシーを定義します。詳細については、[ゲストパスワードポリシーと有効期限の設定 \(534 ページ\)](#) を参照してください。
- [ロギング (Logging)] : ゲストユーザは、デバイスの MAC アドレスで追跡されます。ゲストユーザがレポートに表示される場合、ユーザ名は MAC アドレスです。このオプションを選択すると、ユーザ名として MAC アドレスではなく、ポータルユーザ ID がレポートに表示されます。

## ゲストタイプの設定

これらの設定のナビゲーションパスは、[ワークセンター (Work Centers)] > [ゲストアクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [ゲストタイプ (Guest Types)] です。これらの設定を使用して、ネットワークにアクセスできるゲストのタイプおよびそのアクセス権限を作成します。また、このタイプのゲストを作成できるスポンサーグループを指定できます。

- [ゲストタイプ名 (Guest type name)] : このゲストタイプを他のゲストタイプと区別する名前 (1 ~ 256 文字) を指定します。
- [説明 (Description)] : このゲストタイプの推奨される使用方法に関する追加情報 (最大 2000 文字) を指定します。たとえば、アカウント登録ゲスト用。ゲストアカウントの作成に使用しない、など。
- [言語ファイル (Language File)] : このフィールドでは、サポート対象のすべての言語で、電子メールの件名、電子メールメッセージ、および SMS メッセージの内容を含む言語ファイルをエクスポートおよびインポートできます。これらの言語とコンテンツは、アカウントが期限切れになった旨の通知に使用され、このゲストタイプに割り当てられているゲストに送信されます。新しいゲストタイプを作成すると、ゲストタイプを保存するまではこの機能は無効です。言語ファイルの編集の詳細については、[ポータル言語のカスタマイズ \(648 ページ\)](#) を参照してください。

- [追加データを収集 (Collect Additional Data)] : [カスタムフィールド... (Custom Fields...)] ボタンをクリックして、このゲストタイプを使用しているゲストから追加データを収集するために使用するカスタム フィールドを選択します。

カスタム フィールドを管理するには、[ワークセンター (Work Centers)] > [ゲストアクセス (Guest Access)] > [設定 (Settings)] > [カスタムフィールド (Custom Fields)] を選択します。

#### • 最大アクセス時間 (Maximum Access Time)

- [アカウント期間の開始 (Account duration starts)] : [最初のログインから (From first login)] を選択した場合、アカウントの開始時間は、ゲストユーザがゲストポータルに最初にログインしたときに開始され、終了時間は指定された期間に相当します。ゲストユーザがログインしなければ、アカウントがゲスト アカウント消去ポリシーによって削除されるまで、アカウントはAwaiting first login状態のままになります。

値は、1 から 999 日、時間、または分です。

アカウント登録ユーザのアカウントは、ユーザがアカウントを作成し、自分のアカウントにログオンしたときに開始されます。

[スポンサーが指定した日付から (From sponsor-specified date)] を選択した場合は、このゲスト タイプのゲストがネットワークにアクセスして接続を保持できる最大日数、時間数、または分数を入力します。

この設定を変更した場合、変更内容はこのゲストタイプを使用して作成された既存のゲスト アカウントには適用されません。

- [最大アカウント期間 (Maximum account duration)] : このゲスト タイプが割り当てられているゲストがログインできる期間 (日数、時間数、または分数) を入力します。



(注) アカウント消去ポリシーにより期限切れのゲストアカウントが確認され、期限切れ通知が送信されます。このポリシーは 20 分ごとに実行されるため、アカウント期間を 20 分未満に設定すると、アカウントの消去前に期限切れ通知が送信されることがあります。

[アクセスを許可する日付と時刻 (Allow access only on these days and times)] オプションを使用して、このゲストタイプのゲストにアクセスを提供する期間や曜日を指定できます。

- 選択した曜日によって、スポンサーのカレンダーで選択できる日付へのアクセスが制限されます。
- スポンサーが期間と日付を選択すると、スポンサーポータルで最大アカウント期間が適用されます。

ここで設定するアクセス時刻の設定は、ゲストアカウントの作成時にスポンサーポータルで利用できる時刻設定に影響します。詳細については、[スポンサーに対して使用可能な時間設定項目の設定（570 ページ）](#)を参照してください。

## • ログインオプション

- [最大同時ログイン数 (Maximum simultaneous logins)] : このゲストタイプに割り当てられたユーザが同時に実行できる最大ユーザセッション数を入力します。
- [ゲストが制限を超えた場合 (When guest exceeds limit)] : [最大同時ログイン数 (Maximum simultaneous logins)] を選択した場合は、その最大ログイン数に到達した後でユーザが接続したときに実行するアクションも選択する必要があります。
  - 最も古い接続を切断 (Disconnect the oldest connection)
  - [最も新しい接続を切断 (Disconnect the newest connection)] : [エラーメッセージを示すポータルページにユーザをリダイレクトする (Redirect user to a portal page showing an error message)] をオプションで選択 : 特定の時間にわたってエラーメッセージが表示され、その後セッションが切断されてユーザがゲストポータルにリダイレクトされます。エラーメッセージが表示される時間は設定可能です。エラーページの内容は、[メッセージ (Messages)] > [エラーメッセージ (Error Messages)] ページの [ポータルページのカスタマイズ (Portal Page Customization)] ダイアログで設定します。
- [ゲストが登録できるデバイスの最大数 (Maximum devices guests can register)] : 各ゲストに登録できるデバイスの最大数を入力します。そのゲストタイプのゲストに登録済みの値より小さい値を最大数として設定できます。この値は、新しく作成されたゲストアカウントにのみ適用されます。
- [ゲストデバイス登録のためのエンドポイントIDグループ (Endpoint identity group for guest device registration)] : ゲストのデバイスに割り当てるエンドポイントIDグループを選択します。Cisco ISE はデフォルトとして使用する **GuestEndpoints** のエンドポイントIDグループを提供します。デフォルトを使用しない場合、追加のエンドポイントIDグループを作成することもできます。
- [ゲストに対しゲストポータルのバイパスを許可する (Allow guest to bypass the Guest portal)] : クレデンシャルを持つゲストタイプのキャプティブポータル (Web 認証ページ) をバイパスし、有線およびワイヤレス (dot1x) サブリカントまたはVPNクライアントに認証情報を提供することでネットワークにアクセスすることをユーザに許可します。ゲストアカウントは、AUPが必要な場合でも、[初期ログインを待機 (Awaiting Initial Login)] 状態と AUP ページをバイパスして [アクティブ (Active)] 状態になります。

この設定を有効にしない場合、ユーザは初めにクレデンシャルを持つゲストのキャプティブポータルを使用してログインしないと、ネットワークの他の部分にアクセスできません。

## • アカウント有効期限通知

- [アカウント有効期限の \_\_ 日前にアカウント有効期限通知を送信する (Send account expiration notification \_\_ days before account expires) ] : アカウントが期限切れになる前にゲストに通知を送信します。有効期限前の日数、時間数、または分数を指定します。
- [メッセージ表示原語 (View messages in) ] : 電子メールまたは SMS 通知の表示言語を指定します。
- [電子メール (Email) ] : アカウント有効期限通知を電子メールで送信します。
- [次のポータルのカスタマイズを使用する (Use customization from) ] : 選択したポータルに対して設定した同一のカスタマイズ内容をこのゲストタイプのアカウント有効期限メールに適用します。
- [テキストのコピー元 (Copy text from) ] : 別のゲスト タイプのアカウント有効期限メールに、作成した電子メール テキストを再利用します。
- **テスト電子メールの送信先 (Send test email to me at)**
- [SMS] : アカウント有効期限通知を SMS で送信します。

SMS の設定は、電子メール通知の設定と同一ですが、[テスト SMS の送信 (Send test SMS to me) ] の SMS ゲートウェイを選択する点異なります。

- [スポンサーグループ (Sponsor Groups) ] : このゲスト タイプを使用してメンバーがゲスト アカウントを作成できるスポンサー グループを指定します。このゲスト タイプにアクセスできないようにするスポンサー グループは削除します。

## スポンサー グループ設定

これらの設定のナビゲーションパスは、[ワーク センター (Work Centers) ] > [ゲスト アクセス (Guest Access) ] > [ポータルとコンポーネント (Portals & Components) ] > [スポンサー グループ (Sponsor Groups) ] です。スポンサー グループにメンバーを追加したり、ゲストタイプおよびロケーション特権を定義したり、ゲストアカウントの作成と管理に関連する権限を設定したりする場合に、これらの設定を使用します。

- [スポンサー グループの無効化 (Disable Sponsor Group) ] : このスポンサー グループのメンバーがスポンサー ポータルにアクセスできないようにします。

たとえば、管理者ポータルで設定を変更している間、スポンサーが一時的にスポンサーポータルにログインできないようにします。あるいは、再びアクティブ化する必要があるまで、年次会議のスポンサーシップゲストなど、頻繁には発生しないアクティビティに関するスポンサー グループを無効にします。

- **スポンサー グループ名 (Sponsor group name)** : 一意の名前を入力します (1 ~ 256 文字) 。
- **[説明 (Description) ]** : このスポンサー グループで使用されるゲスト タイプなどの有益な情報を入力します (最大 2000 文字) 。

- [ゲスト タイプの設定 (Configure Guest Types)] : 必要とするゲスト タイプが使用可能でない場合は、[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [ゲスト タイプ (Guest Types)] の順にクリックし、新しいゲスト タイプを作成するか、または既存のゲスト タイプを編集します。

- **一致基準**

- メンバー (Members) : [スポンサー グループ メンバーの選択 (Select Sponsor Group Members)] ボックスを表示する場合にクリックします。ここでは、使用可能なユーザ ID グループを (内部および外部の ID ストアから) 選択し、このスポンサー グループのメンバーとして追加できます。
- スポンサー グループ メンバー (Sponsor Group Members) : 選択したスポンサー グループのリストを検索およびフィルタリングし、含めないグループを削除します。
- その他の条件 (Other conditions) : [新しい条件の作成 (Create New Condition)] をクリックして、このスポンサー グループに含まれるためにスポンサーが満たす必要がある条件を 1 つ以上構築します。Active Directory、LDAP、SAML、ODBC の ID ストアからの認証属性を使用できますが、RADIUS トークンまたは RSA SecurID ストアは使用できません。内部ユーザ属性も使用できます。条件には、属性、演算子、値があります。
- ディクショナリ属性 *Name* を使用して条件を作成するには、ID グループ名の前にユーザ ID グループを付けます。次に例を示します。

*InternalUser:Name EQUALS bsmith*

この場合、「bsmith」という名前の内部ユーザだけがこのスポンサー グループに所属できます。

- このスポンサー グループはこれらのゲスト タイプを使用してアカウントを作成可能 (This sponsor group can create accounts using these guest types) : このスポンサー グループのメンバーがゲスト アカウントの作成時に使用できるゲスト タイプを指定します。有効にするスポンサー グループには、使用できる少なくとも 1 つのゲスト タイプが設定されている必要があります。

このスポンサー グループに 1 つのゲスト タイプのみを割り当てる場合、それが使用可能な唯一の有効なゲストであるため、スポンサー ポータルに表示しないことを選択できます。[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [スポンサー ポータル (Sponsor Portal)] > [ページカスタマイズ (Page Customization)] > [アカウントの作成 (Create Accounts)] > [ゲスト タイプ (Guest Types)] > [設定 (Settings)] の順に選択します。このオプションを有効にするには、[スポンサーで 1 つのみ使用できる場合はゲスト タイプを非表示 (Hide guest type if only one is available to sponsor)] をオンにします。

- ゲストがアクセスするロケーションを選択 (Select the locations that guests will be visiting) : このグループのスポンサーがアカウントの作成時にゲストに割り当てることができるさま

さまざまなロケーションを選択します。このことは、これらのゲストアカウントの有効な時間帯を定義し、有効なアクセス時間などゲストに適用するすべての時間パラメータを指定する場合に役立ちます。このことによって、ゲストが他のロケーションからネットワークに接続できなくなることはありません。

有効にするスポンサーグループには、使用できる少なくとも1つのロケーションが設定されている必要があります。

このスポンサーグループに1つのロケーションのみを割り当てると、それが、メンバーが作成するゲストアカウントの唯一の有効な時間帯になります。デフォルトでは、スポンサーポータルに表示されません。

### スポンサーが作成可能 (Sponsor Can Create)

- 特定のゲストに割り当てられた複数のゲストアカウント (インポート) (Multiple guest accounts assigned to specific guests (Import)) : スポンサーは、ファイルから姓名などのゲストの詳細をインポートすることによって、複数のゲストアカウントを作成できます。

このオプションが有効である場合、[インポート (Import)] ボタンがスポンサーポータルの [アカウントの作成 (Create Accounts)] ページに表示されます。[インポート (Import)] オプションは、Internet Explorer、Firefox、Safari などのデスクトップブラウザだけで使用可能です (モバイルは不可)

- バッチ処理の制限 (Limit to batch of) : このスポンサーグループが複数のアカウントを同時に作成できる場合、単一のインポート操作で作成可能なゲストアカウントの数を指定します。

スポンサーは最大 10,000 個のアカウントを作成できますが、潜在的なパフォーマンスの問題があるため、作成するアカウントの数を制限することを推奨します。

- ゲストへの複数のゲストアカウントの割り当て (ランダム) (Multiple guest accounts to be assigned to any guests (Random)) : スポンサーが、未知のゲストのプレースホルダとして、または複数のアカウントをすばやく作成する必要がある場合に複数のランダムゲストアカウントを作成できるようにします。

このオプションが有効である場合、[ランダム (Random)] ボタンがスポンサーポータルの [アカウントの作成 (Create Accounts)] ページに表示されます。

- デフォルトユーザ名プレフィックス (Default username prefix) : スポンサーが複数のランダムなゲストアカウントを作成する場合に使用できるユーザ名プレフィックスを指定します。指定した場合、このプレフィックスはランダムなゲストアカウントを作成するときにスポンサーポータルに表示されます。また、[スポンサーにユーザ名プレフィックスの指定を許可 (Allow sponsor to specify a username prefix)] の設定により、次のようになります。

- 有効 : スポンサーは、スポンサーポータルでデフォルトのプレフィックスを編集できます。
- 無効 : スポンサーは、スポンサーポータルでデフォルトのプレフィックスを編集できません。

ユーザ名プレフィックスを指定しないか、またはスポンサーにユーザ名プレフィックスの指定を許可しない場合、スポンサーはスポンサー ポータルでユーザ名プレフィックスを割り当てることができません。

- スポンサーにユーザ名プレフィックスの指定を許可 (Allow sponsor to specify a username prefix) : このスポンサー グループが複数のアカウントを同時に作成できる場合、単一のインポート操作で作成可能なゲスト アカウントの数を指定します。

スポンサーは最大 10,000 個のアカウントを作成できますが、潜在的なパフォーマンスの問題があるため、作成するアカウントの数を制限することを推奨します。

- 開始日を\_\_日後より遅くすることはできない (Start date can be no more than \_\_ days into the future) : 有効にして日数を指定すると、作成した複数のゲスト アカウントの開始日をこの日数以内に設定する必要があります。

### スポンサーが管理可能 (Sponsor Can Manage)

- スポンサーが作成したアカウントのみ (Only accounts sponsor has created) : このグループのスポンサーは、スポンサーの電子メールアカウントに基づいて、スポンサーが作成したゲスト アカウントのみを表示および管理できます。
- このスポンサー グループのメンバーによって作成されたアカウント (Accounts created by members of this sponsor group) : このグループのスポンサーは、このスポンサー グループ内のスポンサーが作成したゲスト アカウントを表示および管理できます。
- すべてのゲスト アカウント (All guest accounts) : スポンサーはすべての保留中のゲスト アカウントを表示および管理できます。



(注) [アカウント登録ゲストからの要求の承認および表示 (Approve and view requests from self-registering guests)] にマークを付けて、[スポンサーが可能 (Sponsor Can)] の下で [このスポンサーに割り当てられた保留中のアカウントのみ (Only pending accounts assigned to this sponsor)] オプションを使用していない限り、グループメンバーシップにかかわらず、すべてのスポンサーがすべての保留中のアカウントを表示できます。

### スポンサーが可能 (Sponsor Can)

- ゲストの連絡先情報 (電子メール、電話番号) の更新 (Update guests' contact information (email, Phone Number)) : スポンサーは、自分が管理できるゲスト アカウントについて、ゲストの連絡先情報を変更できます
- ゲストのパスワードの表示/印刷 (View/print guests' passwords) : これをオンにすると、スポンサーはゲストのパスワードを印刷することができます。スポンサーは [アカウントの管理 (Manage Accounts)] ページおよびゲストの詳細で、ゲストのパスワードを表示できます。これがオフの場合、スポンサーはパスワードを印刷できませんが、ユーザは電子メールまたは SMS (設定済みの場合) を介してパスワードを取得できます。

- ゲストのクレデンシャルを含む SMS 通知の送信 (Send SMS notifications with guests' credentials) : スポンサーは、自分が管理できるゲスト アカウントについて、アカウントの詳細とログイン クレデンシャルとともにゲストに SMS (テキスト) 通知を送信できます。
- ゲスト アカウント パスワードのリセット (Reset guest account passwords) : スポンサーは、自分が管理できるゲスト アカウントについて、そのパスワードを Cisco ISE によって生成されたランダムなパスワードにリセットできます。
- ゲストのアカウントの延長 (Extend guests' accounts) : スポンサーは、自分が管理できるゲスト アカウントについて、その有効期限を延長できます。スポンサーは、アカウントの有効期限に関してゲストに送信される電子メール通知に自動的にコピーされます。
- ゲストのアカウントの削除 (Delete guests' accounts) : スポンサーは、自分が管理できるゲスト アカウントについて、アカウントを削除し、ゲストが企業のネットワークにアクセスすることを防ぐことができます。
- ゲストのアカウントの一時停止 (Suspend guests' accounts) : スポンサーは、自分が管理できるゲスト アカウントについて、アカウントを一時停止してゲストが一時的にログインすることを防ぐことができます。

また、このアクションは、許可変更 (CoA) 終了を発行して、一時停止されていたゲストをネットワークから排除できます。

- スポンサーに理由の入力を求める (Require sponsor to provide a reason) : ゲスト アカウントの一時停止に対する説明の入力をスポンサーに求めます。
- アカウント登録ゲストからの要求の承認および表示 (Approve and view requests from self-registering guests) : このスポンサー グループに含まれているスポンサーは、(承認が必要な) アカウント登録ゲストからのすべての保留中のアカウント要求を表示するか、アクセス先の担当者としてユーザがスポンサーの電子メールアドレスを入力した要求のみを表示できます。この機能では、アカウント登録ゲストによって使用されるポータルで [アカウント登録ゲストが承認される必要がある (Require self-registered guests to be approved)] にマークが付けられていて、スポンサーの電子メールが連絡先の担当者としてリストされている必要があります。
  - [保留中のすべてのアカウント (Any pending accounts)] : このグループに所属するスポンサーは、他のスポンサーによって作成されたアカウントを承認およびレビューします。
  - [このスポンサーに割り当てられている保留中のアカウントのみ (Only pending accounts assigned to this sponsor)] : このグループに所属するスポンサーは、スポンサー自身が作成したアカウントだけを表示および承認できます。
- プログラムによるインターフェイス (Guest REST API) を使用した Cisco ISE ゲスト アカウントへのアクセス (Access Cisco ISE guest accounts using the programmatic interface (Guest REST API)) : スポンサーは、自分が管理できるゲスト アカウントについて、Guest REST API プログラミングインターフェイスを使用してゲスト アカウントにアクセスできます。





## 第 32 章

# Web ポータルのカスタマイズのリファレンス

- [ポータル ページのタイトル、コンテンツおよびラベルの文字数制限](#) (1331 ページ)
- [ポータルのカスタマイズ](#) (1333 ページ)
- [ポータル言語ファイルの HTML サポート](#) (1335 ページ)

## ポータル ページのタイトル、コンテンツおよびラベルの文字数制限

[ポータル ページのカスタマイズ (Portal Page Customization)] タブのタイトル、テキスト ボックス、手順、フィールド、ボタンラベル、およびその他の視覚的な要素に入力できる文字数には上限および下限があります。

## ポータル ページのタイトル、コンテンツおよびラベルの文字数制限

ポータル ページの UI 要素へのナビゲーション パスは、次のとおりです。

- ゲスト ポータルの場合、[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [ゲスト ポータル (Guest Portals)] > [編集 (Edit)] > [ポータル ページのカスタマイズ (Portal Page Customization)] > [ページ (Pages)] を選択します。
- スポンサー ポータルの場合、[ワーク センター (Work Centers)] > [ゲスト アクセス (Guest Access)] > [ポータルとコンポーネント (Portals & Components)] > [スポンサー ポータル (Guest Portals)] > [編集 (Edit)] > [ポータル ページのカスタマイズ (Portal Page Customization)] > [ページ (Pages)] を選択します。
- デバイス ポータル。[管理 (Administration)] > [デバイス ポータル管理 (Device Portal Management)] > (任意のポータル) > [編集 (Edit)] > [ポータル ページのカスタマイズ (Portal Page Customization)] > [ページ (Pages)] を選択します。

タイトル、テキストボックス、手順、フィールドとボタンのラベル、およびカスタマイズしているポータルページのその他のビジュアル要素のコンテンツを入力する際に、この情報を使用します。これらの更新は、カスタマイズしている特定のページにのみ適用されます。



(注) シングルバイト文字とマルチバイト文字のどちらを入力するかにかかわらず、識別される最大文字数のみをフィールドに入力できます。マルチバイト文字は文字数制限には影響しません。

| フィールドのカテゴリ | フィールド                      | フィールドラベル：最小文字数 | フィールドラベル：最大文字数 | フィールドの入力値：最小文字数 | フィールドの入力値：最大文字数 |
|------------|----------------------------|----------------|----------------|-----------------|-----------------|
| 共通のページ要素   | バナー タイトル                   |                |                |                 | 256             |
|            | フッター要素                     |                |                | [0]             | 2000            |
|            | ブラウザページのタイトル               |                |                | [0]             | 256             |
|            | 説明テキスト                     |                |                | [0]             | 2000            |
|            | コンテンツ タイトル                 |                |                | [0]             | 256             |
|            | オプションコンテンツ 1               |                |                | [0]             | 2000            |
|            | オプションコンテンツ 2               |                |                | [0]             | 2000            |
|            | ボタン ラベル                    | [0]            | 64             |                 |                 |
|            | チェックボックスラベル                | [0]            | 64             |                 |                 |
|            | タブ ラベル                     | [0]            | 64             |                 |                 |
|            | リンク ラベル                    | [0]            | 256            |                 |                 |
| AUP        | AUP テキスト                   |                |                | [0]             | 50,000          |
| メッセージ テキスト | メッセージテキスト (ページに表示)         |                |                | [0]             | 2000            |
|            | メッセージテキスト (ポップアップウィンドウに表示) |                |                | [0]             | 256             |

| フィールドのカテゴリ     | フィールド                            | フィールドラベル：最小文字数 | フィールドラベル：最大文字数 | フィールドの入力値：最小文字数 | フィールドの入力値：最大文字数 |
|----------------|----------------------------------|----------------|----------------|-----------------|-----------------|
| フィールドラベル       | すべてのフィールドラベル                     | [0]            | 256            |                 |                 |
| フィールド入力（一般）    | 一般的なフィールド入力（次の特別な場合を参照）          |                |                | [0]             | 256             |
| フィールド入力（特別な場合） | [アクセスコード（Access Code）] フィールド     |                |                | 1               | 20              |
|                | [登録コード（Registration Code）] フィールド |                |                | 1               | 20              |
|                | [ユーザ名（Username）] フィールド           |                |                | 1               | 64              |
|                | [パスワード（Password）] フィールド          |                |                | 1               | 256             |
|                | [電話番号（Phone Number）] フィールド       |                |                | [0]             | 64              |
|                | [デバイス ID（Device ID）] フィールド       |                |                | 12              | 17              |

## ポータルのカスタマイズ

エンドユーザ Web ポータルおよびゲストエクスペリエンスの外観をカスタマイズできます。カスケーディングスタイルシート（CSS）言語と Javascript の使用経験がある場合、ポータルページのレイアウトを変更することで、jQuery Mobile ThemeRoller アプリケーションを使用してポータルのテーマをカスタマイズできます。

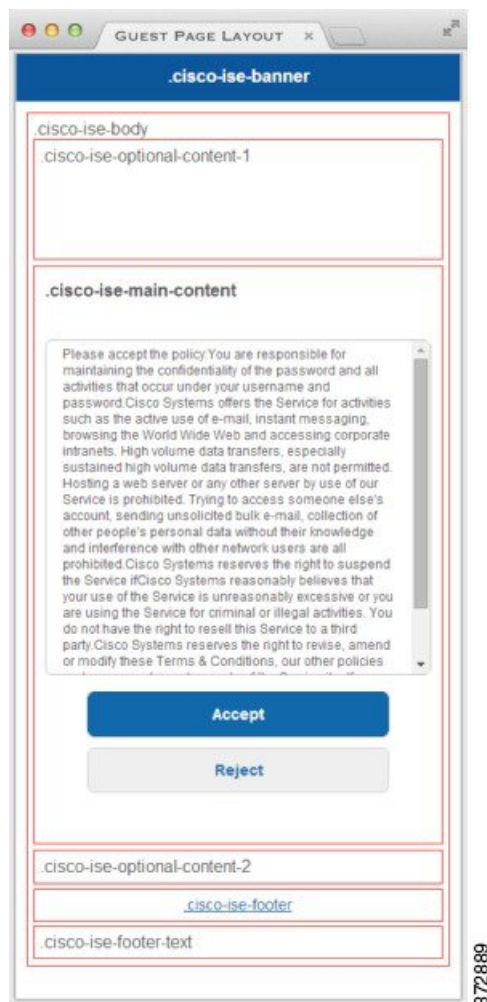
必要なポータルページから CSS テーマまたは言語プロパティをエクスポートすることで、すべてのフィールドを表示できます。詳細については、「[ポータルのデフォルトテーマ CSS ファイルのエクスポート](#)」を参照してください。

## エンドユーザ ポータルのページ レイアウトの CSS クラスと説明

Cisco ISE エンドユーザ Web ポータルのページ レイアウトを定義および変更するには、次の CSS クラスを使用します。

| CSS クラス名                     | 説明                                                                                                                                                                                                       |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| cisco-ise-banner             | <p>ロゴ、バナー イメージ、およびバナー テキストが含まれます。</p> <p>スポンサー ポータルおよびデバイス ポータルでは、このクラスにコンテキスト メニューをアクティブ化できるボタンも含まれます。たとえば、このメニューで [ログアウト (Log Out)]、[パスワードの変更 (Change Password)] などのオプションが含まれるポップアップ ウィンドウを表示できます。</p> |
| cisco-ise-body               | バナーの一部ではないすべてのページの要素が含まれます。                                                                                                                                                                              |
| cisco-ise-optional-content-1 | デフォルトでは空です。テキスト、リンク、および HTML コードと JavaScript コードを追加できます。                                                                                                                                                 |
| cisco-ise-main-content       | 説明テキスト、操作ボタン、および <b>cisco-ise-footer</b> コンテナなど、ポータル ページのメイン コンテンツが含まれます。                                                                                                                                |
| cisco-ise-optional-content-2 | デフォルトでは空です。テキスト、リンク、および HTML コードと JavaScript コードを追加できます。                                                                                                                                                 |
| cisco-ise-footer             | フッターの一部です。 <b>サポートへの問い合わせ</b> や <b>オンライン ヘルプ</b> などのリンクのプレースホルダーです。                                                                                                                                      |
| cisco-ise-footer-text        | デフォルトでは空です。著作権表示または免責事項など、ポータル ページの下部に表示するもののプレースホルダーです。                                                                                                                                                 |

図 67: エンドユーザ ポータルのページ レイアウトで使用する CSS クラス



## ポータル言語ファイルの HTML サポート

各ポータルの圧縮済み言語ファイルには、そのポータルのデフォルト言語プロパティファイルが含まれます。各プロパティファイルには、ポータルに表示される内容を定義するディクショナリ キーが含まれます。

[説明テキスト (Instructional Text)]、[コンテンツ (Content)]、[オプション コンテンツ 1 (Optional Content 1)]、[オプション コンテンツ 2 (Optional Content 2)] の各テキスト ボックスの内容など、ポータルに表示されるテキストをカスタマイズすることができます。これらのテキスト ボックスには、デフォルト コンテンツがあるものと空白のものがあります。

これらのテキスト ボックスに関連付けられたディクショナリ キーの一部でのみ、その値 (テキスト) で HTML がサポートされます。

## ブラックリスト ポータルの言語ファイルの HTML サポート

このポータルの [説明テキスト (Instructional Text)]、[コンテンツ (Content)]、[任意のコンテンツ 1 (Optional Content 1)]、および [任意のコンテンツ 2 (Optional Content 2)] テキストボックスへのナビゲーションパスは、[管理 (Administration)] > [デバイス ポータル管理 (Device Portal Management)] > [ブラックリスト ポータル (Blacklist Portal)] > [編集 (Edit)] > [ポータル ページのカスタマイズ (Portal Page Customization)] > [ページ (Pages)] です。テキストボックスのミニエディタの [HTML ソースの表示 (View HTML Source)] アイコンを使用して、コンテンツに HTML コードを追加できます。

ポータルの言語プロパティ ファイルの次のディクショナリ キーで、テキスト内の HTML がサポートされています。



(注) これは、ファイル内のディクショナリ キーの完全なリストではありません。

- key.blacklist.ui\_reject\_message

## 個人所有デバイスの持ち込みポータルの言語ファイルの HTML サポート

このポータルの [説明テキスト (Instructional Text)]、[コンテンツ (Content)]、[任意のコンテンツ 1 (Optional Content 1)]、および [任意のコンテンツ 2 (Optional Content 2)] テキストボックスへのナビゲーションパスは、[管理 (Administration)] > [デバイス ポータル管理 (Device Portal Management)] > [BYOD ポータル (BYOD Portals)] > [編集 (Edit)] > [ポータル ページのカスタマイズ (Portal Page Customization)] > [ページ (Pages)] です。テキストボックスのミニエディタの [HTML ソースの表示 (View HTML Source)] アイコンを使用して、コンテンツに HTML コードを追加できます。

ポータルの言語プロパティ ファイルの次のディクショナリ キーで、テキスト内の HTML がサポートされています。



(注) これは、ファイル内のディクショナリ キーの完全なリストではありません。

- key.guest.ui\_contact\_instruction\_message
- key.guest.ui\_byod\_welcome\_optional\_content\_1
- key.guest.ui\_byod\_welcome\_optional\_content\_2
- key.guest.ui\_byod\_reg\_limit\_message
- key.guest.ui\_byod\_reg\_content\_message
- key.guest.ui\_byod\_success\_manual\_reconnect\_message
- key.guest.ui\_byod\_install\_winmac\_instruction\_message

- key.guest.ui\_byod\_install\_optional\_content\_1
- key.guest.ui\_byod\_reg\_optional\_content\_2
- key.guest.ui\_byod\_install\_optional\_content\_2
- key.guest.ui\_byod\_reg\_optional\_content\_1
- key.guest.ui\_byod\_reg\_instruction\_message
- key.guest.ui\_byod\_welcome\_aup\_text
- key.guest.ui\_contact\_optional\_content\_2
- key.guest.ui\_contact\_optional\_content\_1
- key.guest.ui\_byod\_install\_ios\_instruction\_message
- key.guest.ui\_byod\_welcome\_instruction\_message
- key.guest.ui\_error\_optional\_content\_2
- key.guest.ui\_error\_optional\_content\_1
- key.guest.ui\_byod\_welcome\_renew\_cert\_message
- key.guest.ui\_byod\_install\_android\_instruction\_message
- key.guest.ui\_byod\_install\_instruction\_message
- key.guest.ui\_byod\_welcome\_config\_device\_message
- key.guest.ui\_byod\_success\_message
- key.guest.ui\_byod\_success\_unsupported\_device\_message
- key.guest.ui\_byod\_success\_optional\_content\_1
- key.guest.ui\_byod\_success\_optional\_content\_2
- key.guest.ui\_error\_instruction\_message

## 証明書プロビジョニング ポータルの言語ファイルの HTML サポート

このポータルの [説明テキスト (Instructional Text)]、[コンテンツ (Content)]、[任意のコンテンツ 1 (Optional Content 1)]、および [任意のコンテンツ 2 (Optional Content 2)] テキストボックスへのナビゲーションパスは、**[管理 (Administration)] > [デバイス ポータル管理 (Device Portal Management)] > [証明書プロビジョニング ポータル (Certificate Provisioning Portal)] > [編集 (Edit)] > [ポータル ページのカスタマイズ (Portal Page Customization)] > [ページ (Pages)]** です。テキスト ボックスのミニ エディタの [HTML ソースの表示 (View HTML Source)] アイコンを使用して、コンテンツに HTML コードを追加できます。

ポータルの言語プロパティ ファイルの次のディクショナリ キーで、テキスト内の HTML がサポートされています。



(注) これは、ファイル内のディクショナリ キーの完全なリストではありません。

- key.manualcertprov.ui\_login\_instruction\_message
- key.manualcertprov.ui\_aup\_instruction\_message
- key.manualcertprov.ui\_changepwd\_instruction\_message
- key.manualcertprov.ui\_post\_access\_instruction\_message
- key.manualcertprov.ui\_status\_csv\_invalid\_instruction\_message
- key.manualcertprov.ui\_login\_optional\_content\_1
- key.manualcertprov.ui\_login\_optional\_content\_2
- key.manualcertprov.ui\_aup\_optional\_content\_1
- key.manualcertprov.ui\_aup\_optional\_content\_2
- key.manualcertprov.ui\_changepwd\_optional\_content\_1
- key.manualcertprov.ui\_changepwd\_optional\_content\_2
- key.manualcertprov.ui\_post\_access\_optional\_content\_1
- key.manualcertprov.ui\_post\_access\_optional\_content\_2
- key.manualcertprov.ui\_landing\_instruction\_message
- key.manualcertprov.ui\_status\_page\_single\_generated\_content
- key.manualcertprov.ui\_status\_generated\_content

## クライアント プロビジョニング ポータルの言語ファイルの HTML サポート

このポータルの [説明テキスト (Instructional Text)]、[コンテンツ (Content)]、[任意のコンテンツ 1 (Optional Content 1)]、および [任意のコンテンツ 2 (Optional Content 2)] テキストボックスへのナビゲーションパスは、[管理 (Administration)] > [デバイス ポータル管理 (Device Portal Management)] > [クライアント プロビジョニング ポータル (Client Provisioning Portals)] > [編集 (Edit)] > [ポータル ページのカスタマイズ (Portal Page Customization)] > [ページ (Pages)] です。テキスト ボックスのミニ エディタの [HTML ソースの表示 (View HTML Source)] アイコンを使用して、コンテンツに HTML コードを追加できます。

ポータルの言語プロパティ ファイルの次のディクショナリ キーで、テキスト内の HTML がサポートされています。



(注) これは、ファイル内のディクショナリ キーの完全なリストではありません。



- key.guest.ui\_client\_provision\_agent\_installed\_instructions\_without\_java\_message
- key.guest.ui\_contact\_instruction\_message
- key.guest.ui\_success\_message
- key.guest.ui\_client\_provision\_unable\_to\_detect\_message
- key.guest.ui\_client\_provision\_instruction\_message
- key.guest.ui\_client\_provision\_agent\_installation\_message
- key.guest.ui\_client\_provision\_posture\_agent\_check\_message
- key.guest.ui\_vlan\_instruction\_message
- key.guest.ui\_client\_provision\_agent\_installation\_instructions\_with\_no\_java\_message
- key.guest.ui\_success\_instruction\_message
- key.guest.ui\_vlan\_optional\_content\_1
- key.guest.ui\_vlan\_optional\_content\_2
- key.guest.ui\_contact\_optional\_content\_2
- key.guest.ui\_contact\_optional\_content\_1
- key.guest.ui\_contact\_optional\_content\_1
- key.guest.ui\_client\_provision\_posture\_check\_compliant\_message
- key.guest.ui\_client\_provision\_optional\_content\_2
- key.guest.ui\_client\_provision\_optional\_content\_1
- key.guest.ui\_error\_optional\_content\_2
- key.guest.ui\_error\_optional\_content\_1
- key.guest.ui\_client\_provision\_posture\_check\_non\_compliant\_message
- key.guest.ui\_vlan\_install\_message
- key.guest.ui\_success\_optional\_content\_1
- key.guest.ui\_success\_optional\_content\_2
- key.guest.ui\_client\_provision\_posture\_agent\_scan\_message

## クレデンシャル ゲスト ポータルの言語ファイルの HTML サポート

このポータルの [説明テキスト (Instructional Test) ]、[コンテンツ (Content) ]、[オプションコンテンツ 1 (Optional Content 1) ]、および [オプション コンテンツ 2 (Optional Content 2) ] テキスト ボックスへのナビゲーションパスは、[ワーク センター (Work Centers) ] > [ゲスト アクセス (Guest Access) ] > [ポータルとコンポーネント (Portals & Components) ] > [ゲスト ポータル (Guest Portals) ] > [編集 (Edit) ] > [ポータル ページのカスタマイズ ( Portal Page Customization) ] > [ページ ( Pages) ] です。テキスト ボックスのミニ エディタの [HTML

ソースの表示 (View HTML Source) ] アイコンを使用して、コンテンツに HTML コードを追加できます。

ポータルの言語プロパティ ファイルの次のディクショナリ キーで、テキスト内の HTML がサポートされています。



(注) これは、ファイル内のディクショナリ キーの完全なリストではありません。

- key.guest.ui\_contact\_instruction\_message
- key.guest.ui\_login\_optional\_content\_1
- key.guest.ui\_login\_optional\_content\_2
- key.guest.ui\_client\_provision\_unable\_to\_detect\_message
- key.guest.ui\_client\_provision\_instruction\_message
- key.guest.ui\_device\_reg\_optional\_content\_2
- key.guest.ui\_device\_reg\_optional\_content\_1
- key.guest.ui\_byod\_success\_manual\_reconnect\_message
- key.guest.ui\_byod\_reg\_optional\_content\_2
- key.guest.ui\_byod\_reg\_optional\_content\_1
- key.guest.ui\_client\_provision\_agent\_installation\_instructions\_with\_no\_java\_message
- key.guest.ui\_success\_instruction\_message
- key.guest.ui\_max\_devices\_instruction\_message
- key.guest.ui\_max\_devices\_optional\_content\_1
- key.guest.ui\_self\_reg\_results\_instruction\_message
- key.guest.notification\_credentials\_email\_body
- key.guest.ui\_max\_devices\_optional\_content\_2
- key.guest.ui\_contact\_optional\_content\_2
- key.guest.ui\_contact\_optional\_content\_1
- key.guest.ui\_byod\_install\_ios\_instruction\_message
- key.guest.ui\_changepwd\_instruction\_message
- key.guest.ui\_client\_provision\_posture\_check\_compliant\_message
- key.guest.ui\_aup\_instruction\_message
- key.guest.ui\_changepwd\_optional\_content\_2
- key.guest.ui\_changepwd\_optional\_content\_1
- key.guest.ui\_self\_reg\_results\_optional\_content\_2

- key.guest.ui\_self\_reg\_results\_optional\_content\_1
- key.guest.ui\_device\_reg\_instruction\_message
- key.guest.ui\_byod\_welcome\_renew\_cert\_message
- key.guest.ui\_vlan\_execute\_message
- key.guest.ui\_byod\_install\_android\_instruction\_message
- key.guest.ui\_client\_provision\_posture\_check\_non\_compliant\_message
- key.guest.ui\_byod\_install\_instruction\_message
- key.guest.ui\_device\_reg\_max\_reached\_message
- key.guest.ui\_byod\_success\_message
- key.guest.ui\_byod\_success\_unsupported\_device\_message
- key.guest.ui\_byod\_success\_optional\_content\_1
- key.guest.ui\_byod\_success\_optional\_content\_2
- key.guest.ui\_aup\_employee\_text
- key.guest.ui\_client\_provision\_agent\_installed\_instructions\_without\_java\_message
- key.guest.ui\_success\_message
- key.guest.ui\_byod\_welcome\_optional\_content\_1
- key.guest.ui\_byod\_welcome\_optional\_content\_2
- key.guest.ui\_self\_reg\_optional\_content\_2
- key.guest.ui\_self\_reg\_optional\_content\_1
- key.guest.ui\_byod\_reg\_limit\_message
- key.guest.notification\_credentials\_print\_body
- key.guest.ui\_byod\_reg\_content\_message
- key.guest.ui\_client\_provision\_agent\_installation\_message
- key.guest.ui\_post\_access\_message
- key.guest.ui\_vlan\_instruction\_message
- key.guest.ui\_byod\_install\_winmac\_instruction\_message
- key.guest.ui\_aup\_guest\_text
- key.guest.ui\_byod\_install\_optional\_content\_1
- key.guest.ui\_byod\_install\_optional\_content\_2
- key.guest.ui\_byod\_reg\_instruction\_message
- key.guest.ui\_aup\_optional\_content\_1
- key.guest.ui\_aup\_optional\_content\_2

- key.guest.ui\_self\_reg\_aup\_text
- key.guest.ui\_login\_instruction\_message
- key.guest.ui\_vlan\_optional\_content\_1
- key.guest.ui\_vlan\_optional\_content\_2
- key.guest.ui\_self\_reg\_results\_aup\_text
- key.guest.ui\_device\_reg\_register\_message
- key.guest.ui\_byod\_welcome\_instruction\_message
- key.guest.ui\_client\_provision\_optional\_content\_2
- key.guest.ui\_self\_reg\_instruction\_message
- key.guest.ui\_vlan\_install\_message
- key.guest.ui\_success\_optional\_content\_1
- key.guest.ui\_success\_optional\_content\_2
- key.guest.ui\_post\_access\_instruction\_message
- key.guest.ui\_post\_access\_optional\_content\_2
- key.guest.ui\_post\_access\_optional\_content\_1
- key.guest.ui\_byod\_welcome\_config\_device\_message
- key.guest.ui\_client\_provision\_posture\_agent\_scan\_message

## ホットスポット ゲスト ポータルの言語ファイルの HTML サポート

このポータルの [説明テキスト (Instructional Test) ]、[コンテンツ (Content) ]、[オプションコンテンツ 1 (Optional Content 1) ]、および [オプションコンテンツ 2 (Optional Content 2) ] テキスト ボックスへのナビゲーションパスは、[ワーク センター (Work Centers) ] > [ゲスト アクセス (Guest Access) ] > [ポータルとコンポーネント (Portals & Components) ] > [ゲスト ポータル (Guest Portals) ] > [編集 (Edit) ] > [ポータル ページのカスタマイズ (Portal Page Customization) ] > [ページ (Pages) ] です。テキスト ボックスのミニ エディタの [HTML ソースの表示 (View HTML Source) ] アイコンを使用して、コンテンツに HTML コードを追加できます。

ポータルの言語プロパティ ファイルの次のディクショナリ キーで、テキスト内の HTML がサポートされています。



(注) これは、ファイル内のディクショナリ キーの完全なリストではありません。

- key.guest.ui\_contact\_instruction\_message
- key.guest.ui\_success\_message

- key.guest.ui\_post\_access\_message
- key.guest.ui\_vlan\_instruction\_message
- key.guest.ui\_success\_instruction\_message
- key.guest.ui\_aup\_optional\_content\_1
- key.guest.ui\_aup\_optional\_content\_2
- key.guest.ui\_vlan\_unsupported\_error\_message
- key.guest.ui\_vlan\_optional\_content\_1
- key.guest.ui\_vlan\_optional\_content\_2
- key.guest.ui\_contact\_optional\_content\_2
- key.guest.ui\_contact\_optional\_content\_1
- key.guest.ui\_aup\_instruction\_message
- key.guest.ui\_aup\_hotspot\_text
- key.guest.ui\_vlan\_execute\_message
- key.guest.ui\_vlan\_install\_message
- key.guest.ui\_success\_optional\_content\_1
- key.guest.ui\_success\_optional\_content\_2
- key.guest.ui\_post\_access\_instruction\_message
- key.guest.ui\_post\_access\_optional\_content\_2
- key.guest.ui\_post\_access\_optional\_content\_1

## モバイル デバイス管理ポータル言語ファイルの HTML サポート

このポータルの [説明テキスト (Instructional Text)]、[コンテンツ (Content)]、[オプション コンテンツ 1 (Optional Content 1)]、および [オプション コンテンツ 2 (Optional Content 2)] テキスト ボックスへのナビゲーションパスは、[管理 (Administration)] > [デバイス ポータル管理 (Device Portal Management)] > [MDM ポータル (MDM Portals)] > [編集 (Edit)] > [ポータル ページのカスタマイズ (Portal Page Customization)] > [ページ (Pages)] です。テキスト ボックスのミニ エディタの [HTML ソースの表示 (View HTML Source)] アイコンを使用して、コンテンツに HTML コードを追加できます。

ポータルの言語プロパティ ファイルの次のディクショナリ キーで、テキスト内の HTML がサポートされています。



(注) これは、ファイル内のディクショナリ キーの完全なリストではありません。

- key.mdm.ui\_contact\_instruction\_message

- key.mdm.ui\_mdm\_enrollment\_after\_message
- key.mdm.ui\_error\_optional\_content\_2
- key.mdm.ui\_error\_optional\_content\_1
- key.mdm.ui\_mdm\_enroll\_optional\_content\_1
- key.mdm.ui\_mdm\_enroll\_optional\_content\_1
- key.mdm.ui\_mdm\_enroll\_optional\_content\_2
- key.mdm.ui\_mdm\_enroll\_instruction\_message
- key.mdm.ui\_error\_instruction\_message
- key.mdm.ui\_mdm\_enrollment\_link\_message
- key.mdm.ui\_mdm\_not\_reachable\_message
- key.mdm.ui\_contact\_optional\_content\_2
- key.mdm.ui\_mdm\_continue\_message
- key.mdm.ui\_contact\_optional\_content\_1

## デバイス ポータルの言語ファイルの HTML サポート

このポータルの [説明テキスト (Instructional Text) ]、[コンテンツ (Content) ]、[任意のコンテンツ 1 (Optional Content 1) ]、および [任意のコンテンツ 2 (Optional Content 2) ] テキストボックスへのナビゲーションパスは、**[管理 (Administration) ] > [デバイス ポータル管理 (Device Portal Management) ] > [デバイス ポータル (My Devices Portals) ] > [編集 (Edit) ] > [ポータル ページのカスタマイズ (Portal Page Customization) ] > [ページ (Pages) ]** です。テキストボックスのミニ エディタの [HTML ソースの表示 (View HTML Source) ] アイコンを使用して、コンテンツに HTML コードを追加できます。

ポータルの言語プロパティ ファイルの次のディクショナリ キーで、テキスト内の HTML がサポートされています。



(注) これは、ファイル内のディクショナリ キーの完全なリストではありません。

- key.mydevices.ui\_add\_optional\_content\_1
- key.mydevices.ui\_add\_optional\_content\_2
- key.mydevices.ui\_post\_access\_instruction\_message
- key.mydevices.ui\_edit\_instruction\_message
- key.mydevices.ui\_contact\_optional\_content\_2
- key.mydevices.ui\_contact\_optional\_content\_1
- key.mydevices.ui\_changepwd\_optional\_content\_1

- key.mydevices.ui\_changepwd\_optional\_content\_2
- key.mydevices.ui\_post\_access\_message
- key.mydevices.ui\_home\_instruction\_message
- key.mydevices.ui\_edit\_optional\_content\_1
- key.mydevices.ui\_edit\_optional\_content\_2
- key.mydevices.ui\_add\_instruction\_message
- key.mydevices.ui\_post\_access\_optional\_content\_2
- key.mydevices.ui\_post\_access\_optional\_content\_1
- key.mydevices.ui\_error\_instruction\_message
- key.mydevices.ui\_actions\_instruction\_message
- key.mydevices.ui\_home\_optional\_content\_2
- key.mydevices.ui\_aup\_optional\_content\_1
- key.mydevices.ui\_aup\_optional\_content\_2
- key.mydevices.ui\_home\_optional\_content\_1
- key.mydevices.ui\_changepwd\_instruction\_message
- key.mydevices.ui\_contact\_instruction\_message
- key.mydevices.ui\_aup\_employee\_text
- key.mydevices.ui\_login\_optional\_content\_2
- key.mydevices.ui\_login\_optional\_content\_1
- key.mydevices.ui\_login\_instruction\_message
- key.mydevices.ui\_error\_optional\_content\_1
- key.mydevices.ui\_error\_optional\_content\_2
- key.mydevices.ui\_aup\_instruction\_message

## スポンサー ポータルの言語ファイルの HTML サポート

このポータルの [説明テキスト (Instructional Test) ]、[コンテンツ (Content) ]、[オプションコンテンツ 1 (Optional Content 1) ]、および [オプションコンテンツ 2 (Optional Content 2) ] テキスト ボックスへのナビゲーションパスは、[ワーク センター (Work Centers) ] > [ゲスト アクセス (Guest Access) ] > [ポータルとコンポーネント (Portals & Components) ] > [スポンサー ポータル (Sponsor Portals) ] > [編集 (Edit) ] > [ポータル ページのカスタマイズ (Portal Page Customization) ] > [ページ (Pages) ] です。テキスト ボックスのミニエディタの [HTML ソースの表示 (View HTML Source) ] アイコンを使用して、コンテンツに HTML コードを追加できます。

ポータルの言語プロパティ ファイルの次のディクショナリ キーで、テキスト内の HTML がサポートされています。



(注) これは、ファイル内のディクショナリ キーの完全なリストではありません。

- key.sponsor.ui\_aup\_instruction\_message
- key.sponsor.ui\_create\_random\_instruction\_message
- key.sponsor.ui\_home\_instruction\_message
- key.sponsor.ui\_post\_access\_instruction\_message
- key.sponsor.notification\_credentials\_print\_body
- key.sponsor.ui\_aup\_sponsor\_text
- key.sponsor.ui\_create\_accounts\_access\_info\_instruction\_message
- key.sponsor.ui\_login\_instruction\_message
- key.sponsor.notification\_credentials\_email\_body
- key.sponsor.ui\_create\_known\_instruction\_message
- key.sponsor.ui\_create\_import\_instruction\_message
- key.sponsor.ui\_suspend\_account\_instruction\_message
- key.sponsor.ui\_post\_access\_message
- key.sponsor.ui\_login\_optional\_content\_2
- key.sponsor.ui\_login\_optional\_content\_1
- key.sponsor.notification\_credentials\_email\_password\_body
- key.sponsor.ui\_contact\_optional\_content\_2
- key.sponsor.ui\_contact\_optional\_content\_1
- key.sponsor.ui\_login\_aup\_text
- key.sponsor.ui\_changepwd\_instruction\_message
- key.sponsor.ui\_create\_accounts\_guest\_type\_instruction\_message
- key.sponsor.ui\_changepwd\_optional\_content\_1
- key.sponsor.ui\_changepwd\_optional\_content\_2
- key.sponsor.notification\_credentials\_email\_username\_body
- key.sponsor.ui\_aup\_optional\_content\_1
- key.sponsor.ui\_aup\_optional\_content\_2
- key.sponsor.ui\_post\_access\_optional\_content\_1



- key.sponsor.ui\_post\_access\_optional\_content\_2
- key.sponsor.ui\_contact\_instruction\_message





## 第 33 章

# ポリシーのユーザ インターフェイスのリファレンス

- [認証 \(1349 ページ\)](#)
- [許可ポリシーの設定 \(1356 ページ\)](#)
- [エンドポイント プロファイリング ポリシーの設定 \(1358 ページ\)](#)
- [UDID 属性を使用するエンドポイント コンテキストの可視性 \(1365 ページ\)](#)
- [Dictionaries \(1366 ページ\)](#)
- [条件 \(1368 ページ\)](#)
- [結果 \(1400 ページ\)](#)

## 認証

ここでは、単純な認証ポリシーおよびルールベースの認証ポリシーを設定できる認証ポリシーページについて説明します。

## 簡易認証ポリシーの構成設定

次の表では、簡易認証ポリシーを設定できる、単純認証ポリシーページのフィールドについて説明します。このページへのナビゲーションパスは、**[ポリシー (Policy)] > [認証 (Authentication)]** です。

表 119: 簡易認証ポリシーの構成設定

| フィールド                                     | 使用上のガイドライン             |
|-------------------------------------------|------------------------|
| ネットワーク アクセス サービス (Network Access Service) | 作成済みの許可されるプロトコルを選択します。 |

| フィールド           | 使用上のガイドライン                                                                                                                                                                                                                                                       |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ID ソース          | <p>認証に使用する ID ソースを選択します。ID ソース順序が設定済みである場合、これを選択することも可能です。</p> <p>デフォルトの ID ソースを編集して、このルールで定義されたいずれの ID ソースも要求に一致しない場合に Cisco ISE が使用する ID ソースを指定できます。</p>                                                                                                       |
| オプション (Options) | <p>認証失敗、ユーザが見つからない、プロセス障害、の各イベントに対する今後のアクションのコースを定義します。次のいずれかのオプションを選択できます。</p> <ul style="list-style-type: none"> <li>• [拒否 (Reject)] : 拒否応答が送信されます。</li> <li>• [ドロップ (Drop)] : 応答は送信されません。</li> <li>• [続行 (Continue)] : Cisco ISE は認証ポリシーの処理を続行します。</li> </ul> |

#### 関連トピック

[簡易認証ポリシー](#) (678 ページ)

[簡易認証ポリシーのフロー](#) (680 ページ)

[簡易認証ポリシー設定のガイドライン](#) (681 ページ)

[簡易認証ポリシーの設定](#) (706 ページ)

## ルールベースの認証ポリシーの構成設定

次の表では、簡易認証ポリシーを設定できる、ルールベースの認証ポリシーページのフィールドについて説明します。このページへのナビゲーションパスは、**[ポリシー (Policy)] > [認証 (Authentication)] > [ルールベース (Rule-Based)]** です。

表 120: ルールベースの認証ポリシーの構成設定

| フィールド                 | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステータス (Status)        | <p>このポリシーのステータスを選択します。次のいずれかを設定できます。</p> <ul style="list-style-type: none"><li>• [有効 (Enabled)] : このポリシー条件はアクティブです。</li><li>• [無効 (Disabled)] : このポリシー条件は非アクティブであり、評価されません。</li><li>• [モニタのみ (Monitor Only)] : このポリシー条件は評価されますが、結果は実施されません。[ライブ ログ認証 (Live Log authentication)] ページでこのポリシー条件の結果を照会できます。ここでは、モニタされる手順と属性を含む詳細レポートを参照してください。たとえば、新しいポリシー条件を追加する場合に、条件がもたらす結果が正しいかどうかを判断できないことがあります。この場合、モニタ モードでポリシー条件を作成して、結果を確認できます。結果に問題がない場合はそのポリシー条件を有効化できます。</li></ul> |
| 標準ルール (Standard Rule) | <p>このポリシーの名前を入力し、条件および許可されるプロトコルを選択します。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                |

| フィールド           | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 条件 (Conditions) | <p>[条件 (Conditions)] 固定オーバーレイを拡大するにはプラス (+) 記号をクリックし、固定オーバーレイを閉じるにはマイナス (-) 記号または固定オーバーレイの外側をクリックします。</p> <ul style="list-style-type: none"> <li>• [既存の条件をライブラリから選択 (Select Existing Condition from Library)] または [新しい条件の作成 (高度なオプション) (Create New Condition (Advanced Option))] を選択します。</li> <li>• [既存の条件をライブラリから選択 (Select Existing Condition from Library)] : ポリシー要素ライブラリからシスコによって事前定義された条件を選択して、式を定義できます。</li> <li>• [新しい条件の作成 (高度なオプション) (Create New Condition (Advanced Option))] : さまざまなシステム定義またはユーザ定義のディクショナリから属性を選択することによって、式を定義できます。</li> </ul> |

| フィールド                                                    | 使用上のガイドライン |
|----------------------------------------------------------|------------|
| 既存の条件をライブラリから選択 (Select Existing Condition from Library) |            |

| フィールド | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       | <p>次を実行できます。</p> <ol style="list-style-type: none"> <li>事前定義された条件からポリシー要素の認証用に定義する条件を選択し、AND 演算子またはOR 演算子を使用して複数の条件を追加できます。</li> </ol> <p>次のディクショナリまたは属性を含む、事前定義された特定の条件を選択することはできません。</p> <ul style="list-style-type: none"> <li>ディクショナリ「Certificate」、および任意の属性</li> <li>ディクショナリ「Network Access」、および次の属性： <ul style="list-style-type: none"> <li>Device IP Address（デバイス IP アドレス）</li> <li>ISE Host Name</li> <li>NetworkDeviceName</li> <li>プロトコル</li> <li>UseCase</li> </ul> </li> </ul> <p>このような条件が使用できる場合、選択ボックスの最初のエントリは「関連する条件のみ選択可能」です。</p> <ol style="list-style-type: none"> <li>[操作 (Action)] アイコンをクリックして、後続のステップで次を実行します。 <ul style="list-style-type: none"> <li>[属性/値の追加 (Add Attribute/Value)] : アドホック属性/値の組み合わせを追加できます</li> <li>[ライブラリから条件を追加 (Add Condition from Library)] : シスコによって事前定義された条件を追加できます</li> <li>[複製 (Duplicate)] : 選択した条件のコピーを作成します</li> <li>[ライブラリに条件を追加 (Add Condition to Library)] : 作成したアドホック属性/値の組み合わせをポリシー</li> </ul> </li> </ol> |



| フィールド                                                          | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                | <p>要素ライブラリに保存できます</p> <ul style="list-style-type: none"><li>• [削除 (Delete)] : 選択した条件を削除します</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 新しい条件の作成 (高度なオプション)<br>(Create New Condition (Advance Option)) | <p>次を実行できます。</p> <ol style="list-style-type: none"><li>1. 式にアドホック属性/値の組み合わせを追加し、AND または OR 演算子を使用すると、複数の条件を追加できます。</li><li>2. [操作 (Action)] アイコンをクリックして、後続のステップで次を実行します。<ul style="list-style-type: none"><li>• [属性/値の追加 (Add Attribute/Value)] : アドホック属性/値の組み合わせを追加できます</li><li>• [ライブラリから条件を追加 (Add Condition from Library)] : シスコによって事前定義された条件を追加できます</li><li>• [複製 (Duplicate)] : 選択した条件のコピーを作成します</li><li>• [ライブラリに条件を追加 (Add Condition to Library)] : 作成したアドホック属性/値の組み合わせをポリシー要素ライブラリに保存できます</li><li>• [削除 (Delete)] : 選択した条件を削除します。ここでは、AND または OR 演算子を使用できます</li></ul></li></ol> |
| ネットワーク アクセスの選択 (Select Network Access)                         | 許可されるプロトコルまたは RADIUS サーバ順序から選択します。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| 矢印ボタン (Arrow Button)                                           | ID ソース選択条件を定義する場合にクリックします。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

| フィールド                               | 使用上のガイドライン                                                                                                                                                                                                                                                                                                 |
|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ID ソース順序 (Identity Source Sequence) | <p>次を実行できます。</p> <ol style="list-style-type: none"> <li>1. デフォルトの ID ソース行の [操作 (action)] アイコンをクリックし、[新規行を上挿入 (Insert new row above)] をクリックします。</li> <li>2. 作成した ID ソースルールの名前を入力します。</li> <li>3. ボタンをクリックして、選択する ID ソースに応じて条件を定義します。</li> <li>4. ID ソース順序または ID ソース、および Cisco ISE で実行する操作を選択します。</li> </ol> |

#### 関連トピック

[ルールベースの認証ポリシー \(681 ページ\)](#)

[ルールベースの認証ポリシー \(682 ページ\)](#)

[ルールベースの認証ポリシーの設定 \(707 ページ\)](#)

## 許可ポリシーの設定

次の表に、許可ポリシーを設定できるようにする許可ポリシー ページのフィールドを示します。このページへのナビゲーションパスは、[ポリシー (Policy)] > [許可 (Authorization)] です。

表 121: 許可ポリシーの設定

| フィールド                              | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステータス (Status)                     | <p>ポリシーを適用するには、次のいずれかを選択します。</p> <ul style="list-style-type: none"><li>• [有効 (Enabled)] : このポリシー条件はアクティブです。</li><li>• [無効 (Disabled)] : このポリシー条件は非アクティブであり、評価されません。</li><li>• [モニタのみ (Monitor Only)] : このポリシー条件は評価されますが、結果は実施されません。[ライブ ログ認証 (Live Log authentication)] ページでこのポリシー条件の結果を照会できます。ここでは、モニタされる手順と属性を含む詳細レポートを参照してください。たとえば、新しいポリシー条件を追加する場合に、条件がもたらす結果が正しいかどうかを判断できないことがあります。この場合、モニタ モードでポリシー条件を作成して、結果を確認できます。結果に問題がない場合はそのポリシー条件を有効化できます。</li></ul> |
| ルール名 (Rule Name)                   | ルール名に名前を入力します。                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 条件 (Conditions) (ID グループおよびその他の条件) | <p>最初のドロップダウンから ID グループを選択します。</p> <p>2 番目のドロップダウンから条件を選択します。</p> <p>既存の条件から選択することも、新しい条件を作成することもできます。</p>                                                                                                                                                                                                                                                                                                                                                         |
| 権限 (Permissions)                   | [標準 (Standard)] カテゴリから許可プロファイルを選択します。                                                                                                                                                                                                                                                                                                                                                                                                                              |

## 関連トピック

[Cisco ISE の許可ポリシー \(717 ページ\)](#)[許可ポリシーおよびプロファイルの設定のガイドライン \(721 ページ\)](#)[許可ポリシーの設定 \(728 ページ\)](#)

# エンドポイント プロファイリング ポリシーの設定

次の表では、[エンドポイントポリシー (Endpoint Policies)] ページのフィールドについて説明します。このページのナビゲーションパスは、[ポリシー (Policy)] > [プロファイリング (Profiling)] > [プロファイリング ポリシー (Profiling Policies)] です。

表 122: エンドポイント プロファイリング ポリシーの設定

| フィールド                              | 使用上のガイドライン                                                                                                                                                                                                            |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [名前 (Name)]                        | 作成するエンドポイントプロファイリングポリシーの名前を入力します。                                                                                                                                                                                     |
| 説明                                 | 作成するエンドポイントプロファイリングポリシーの説明を入力します。                                                                                                                                                                                     |
| ポリシー有効 (Policy Enabled)            | デフォルトでは [ポリシー有効 (Policy Enabled)] チェックボックスはオンになっており、エンドポイントのプロファイリング時に、一致するプロファイリングポリシーが関連付けられます。<br><br>オフになっている場合、エンドポイントのプロファイリング時に、エンドポイントプロファイリングポリシーは除外されます。                                                    |
| 最小確実度計数 (Minimum Certainty Factor) | プロファイリングポリシーに関連付ける最小値を入力します。デフォルト値は 10 です。                                                                                                                                                                            |
| 例外アクション (Exception Action)         | プロファイリングポリシー内のルールを定義するときに条件に関連付ける例外アクションを選択します。<br><br>デフォルトは [なし (NONE)] です。例外アクションは、[ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] > [プロファイリング (Profiling)] > [例外アクション (Exception Actions)] で定義されます。 |

| フィールド                                                       | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                              |
|-------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ネットワーク スキャン (NMAP) アクション<br>(Network Scan (NMAP) Action)    | <p>必要に応じて、プロファイリング ポリシー内のルールを定義するときに条件に関連付けるネットワーク スキャンアクションをリストから選択します。</p> <p>デフォルトは[なし (NONE)] です。例外アクションは、[ポリシー (Policy)] &gt; [ポリシー要素 (Policy Elements)] &gt; [結果 (Results)] &gt; [プロファイリング (Profiling)] &gt; [ネットワーク スキャンアクション (Network Scan (NMAP) Actions)] で定義されます。</p>                                                                        |
| ポリシーの ID グループの作成 (Create an Identity Group for the policy)  | <p>エンドポイント ID グループを作成するには、次のオプションのいずれかをオンにします。</p> <ul style="list-style-type: none"> <li>• はい、一致する ID グループを作成します (Yes, create matching Identity Group)</li> <li>• いいえ、既存の ID グループ階層を使用します (No, use existing Identity Group hierarchy)</li> </ul>                                                                                                       |
| はい、一致する ID グループを作成します (Yes, create matching Identity Group) | <p>既存のプロファイリング ポリシーを使用する場合、このオプションを選択します。</p> <p>このオプションは、これらのエンドポイントの一致する ID グループを作成します。エンドポイント プロファイルが既存のプロファイリングポリシーと一致した場合に、ID グループは <b>Profiled</b> エンドポイント ID グループの子になります。</p> <p>たとえば、ネットワーク上で検出されたエンドポイントが <b>Xerox-Device</b> プロファイルに一致する場合は、[エンドポイント ID グループ (Endpoint Identity Groups)] ページで <b>Xerox-Device</b> エンドポイント ID グループが作成されます。</p> |

| フィールド                                                                          | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>いいえ、既存の ID グループ階層を使用します<br/>(No, use existing Identity Group hierarchy)</p> | <p>プロファイリング ポリシーおよび ID グループの階層構造を使用して、一致する親エンドポイント ID グループにエンドポイントを割り当てるには、このチェックボックスをオンにします。</p> <p>このオプションを使用すると、エンドポイント プロファイリング ポリシー階層を利用することができ、エンドポイントはいずれかの一致する親エンドポイント ID グループ、さらに、親 ID グループに関連付けられたエンドポイント ID グループに割り当てられます。</p> <p>たとえば、既存のプロファイルに一致するエンドポイントは、適切な親エンドポイント ID グループの下にグループ化されます。ここで、不明プロファイルに一致するエンドポイントは、[不明 (Unknown)] の下にグループ化され、既存のプロファイルに一致するエンドポイントは、プロファイリングされたエンドポイント ID グループの下にグループ化されます。次の例を参考にしてください。</p> <ul style="list-style-type: none"> <li>• エンドポイントが <b>Cisco-IP-Phone</b> プロファイルに一致する場合、これらのエンドポイントは <b>Cisco-IP-Phone</b> エンドポイント ID グループの下でグループ化されます。</li> <li>• エンドポイントが <b>Workstation</b> プロファイルに一致する場合、これらのエンドポイントは、<b>Workstation</b> エンドポイント ID グループの下でグループ化されます。</li> </ul> <p><b>Cisco-IP-Phone</b> および <b>Workstation</b> エンドポイント ID グループは、システム内の <b>Profiled</b> エンドポイント ID グループに関連付けられます。</p> |
| <p>親ポリシー (Parent Policy)</p>                                                   | <p>新しいエンドポイントプロファイリングポリシーに関連付ける、システムで定義されている親プロファイリングポリシーを選択します。</p> <p>子にルールと条件を継承できる親プロファイリングポリシーを選択できます。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

| フィールド                            | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                    |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 関連 CoA タイプ (Associated CoA Type) | <p>エンドポイントプロファイリングポリシーと関連付ける次のいずれかの CoA タイプを選択します。</p> <ul style="list-style-type: none"><li>• CoA なし (No CoA)</li><li>• ポート バウンス</li><li>• 再認証 (Reauth)</li></ul> <p>• [グローバル設定 (Global Settings)] : [管理 (Administration)] &gt; [システム (System)] &gt; [設定 (Settings)] &gt; [プロファイリング (Profiling)] で設定されたプロファイラ設定から適用されます。</p> |
| ルール (Rule)                       | <p>エンドポイントプロファイリングポリシーで定義された 1 つ以上のルールにより、エンドポイントの一致するプロファイリングポリシーが決定されます。これにより、プロファイルに応じたエンドポイントのグループ化が可能になります。</p> <p>ポリシー要素ライブラリからの 1 つ以上のプロファイリング条件がルールに使用され、エンドポイント属性およびその値が、全体的な分類用に検証されます。</p>                                                                                                                         |

| フィールド           | 使用上のガイドライン |
|-----------------|------------|
| 条件 (Conditions) |            |



| フィールド | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       | <p>プラス (+) 記号をクリックして、条件の固定オーバーレイを展開します。マイナス (-) 記号をクリックするか、固定オーバーレイの外側をクリックして条件を閉じます。</p> <p>[既存の条件をライブラリから選択 (Select Existing Condition from Library) ] または [新しい条件の作成 (高度なオプション) (Create New Condition (Advanced Option)) ] をクリックします。</p> <p>[既存の条件をライブラリから選択 (Select Existing Condition from Library) ] : ポリシー要素ライブラリからシスコによって事前定義された条件を選択して、式を定義できます。</p> <p>[新しい条件の作成 (高度なオプション) (Create New Condition (Advanced Option)) ] : さまざまなシステム辞書またはユーザ定義辞書から属性を選択して、式を定義できます。</p> <p>プロファイリング条件と次のいずれかとを関連付けることができます。</p> <ul style="list-style-type: none"> <li>• 各条件の確実度係数の整数値</li> <li>• その条件の例外アクションまたはネットワーク スキャン アクション</li> </ul> <p>プロファイリング条件と関連付ける、次のいずれかの定義済み設定を選択します。</p> <ul style="list-style-type: none"> <li>• [確実度計数が増加する (Certainty Factor Increases) ] : 各ルールの確実度値を入力します。この値は、全体的な分類に関するすべての一致ルールに対して追加されます。</li> <li>• [例外の操作を行う (Take Exception Action) ] : このエンドポイント プロファイリング ポリシーの [例外アクション (Exception Action) ] フィールドで設定された例外アクションがトリガーされます。</li> <li>• [ネットワーク スキャンを行う (Take Network Scan Action) ] : このエンドポイント プロファイリング ポリシーの [ネットワーク スキャン (NMAP) アクション</li> </ul> |

| フィールド                                                           | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-----------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                 | <p>(Network Scan (NMAP) Action) ] フィールドで設定されたネットワーク スキャンアクションがトリガーされます。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <p>既存の条件をライブラリから選択 (Select Existing Condition from Library)</p> | <p>次を実行できます。</p> <ul style="list-style-type: none"> <li>• ポリシー要素ライブラリに存在するシスコによって事前定義された条件を選択できます。AND または OR 演算子を使用して複数の条件を追加できます。</li> <li>• [操作 (Action) ] アイコンをクリックして、後続のステップで次を実行します。 <ul style="list-style-type: none"> <li>• [属性/値の追加 (Add Attribute/Value) ] : アドホック属性/値の組み合わせを追加できます</li> <li>• [ライブラリから条件を追加 (Add Condition from Library) ] : シスコによって事前定義された条件を追加できます</li> <li>• [複製 (Duplicate) ] : 選択した条件のコピーを作成します</li> <li>• [ライブラリに条件を追加 (Add Condition to Library) ] : 作成したアドホック属性/値の組み合わせをポリシー要素ライブラリに保存できます</li> <li>• [削除 (Delete) ] : 選択した条件を削除します</li> </ul> </li> </ul> |

| フィールド                                                         | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 新しい条件の作成（高度なオプション）<br>(Create New Condition (Advance Option)) | <p>次を実行できます。</p> <ul style="list-style-type: none"> <li>• 式にアドホック属性/値の組み合わせを追加し、AND または OR 演算子を使用すると、複数の条件を追加できます。</li> <li>• [操作 (Action) ] アイコンをクリックして、後続のステップで次を実行します。 <ul style="list-style-type: none"> <li>• [属性/値の追加 (Add Attribute/Value) ] : アドホック属性/値の組み合わせを追加できます</li> <li>• [ライブラリから条件を追加 (Add Condition from Library) ] : シスコによって事前定義された条件を追加できます</li> <li>• [複製 (Duplicate) ] : 選択した条件のコピーを作成します</li> <li>• [ライブラリに条件を追加 (Add Condition to Library) ] : 作成したアドホック属性/値の組み合わせをポリシー要素ライブラリに保存できます</li> <li>• [削除 (Delete) ] : 選択した条件を削除します。ここでは、AND または OR 演算子を使用できます</li> </ul> </li> </ul> |

#### 関連トピック

[Cisco ISE プロファイリング サービス \(770 ページ\)](#)

[エンドポイント プロファイリング ポリシーの作成 \(797 ページ\)](#)

[UDID 属性を使用するエンドポイント コンテキストの可視性 \(1365 ページ\)](#)

## UDID 属性を使用するエンドポイント コンテキストの可視性

固有識別子 (UDID) は、エンドポイントに属する MAC アドレスを識別するエンドポイント属性です。エンドポイントには複数の MAC アドレスが含まれていることがあります（たとえば、有線インターフェイスに1つの MAC アドレス、ワイヤレス インターフェイスにもう1つの MAC アドレスなど）。AnyConnect がエンドポイントにインストールされている場合、AnyConnect エージェントがエンドポイントの UDID を生成します。UDID はエンドポイント

属性として保存され、UDID を使用してエンドポイントを照会できるようになります。エンドポイントの UDID は一定であり、AnyConnect のインストールまたはアンインストールに伴って変更されることはありません。これにより、[コンテキストの可視性 (Context Visibility)] ページ ([コンテキストの可視性 (Context Visibility)] > [エンドポイント (Endpoints)] > [コンプライアンス (Compliance)]) では、複数の NIC が装着されているエンドポイントの場合、複数のエントリではなく 1 つのエントリが表示されます。MAC アドレスではなく特定のエンドポイントに対してポスチャ制御を行うことができます。

## Dictionaries

ここでは、Cisco ISE で使用される RADIUS ベンダーのディクショナリについて説明します。

次の表に、RADIUS ベンダーのディクショナリ属性を設定できるようにする RADIUS ベンダーの [ディクショナリ (Dictionary)] ページのフィールドを示します。このページへのナビゲーションパスは、[ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [ディクショナリ (Dictionaries)] > [システム (System)] > [RADIUS] > [RADIUS ベンダー (RADIUS Vendors)] です。

表 123: RADIUS ベンダー ディクショナリ属性の設定

| フィールド                | 使用上のガイドライン                                                                                                                                                                             |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 属性名 (Attribute Name) | 選択した RADIUS ベンダーのベンダー固有属性名を入力します。                                                                                                                                                      |
| 説明                   | ベンダー固有属性のオプションの説明を入力します。                                                                                                                                                               |
| 内部名                  | 内部のデータベースで表されるベンダー固有属性の名前を入力します。                                                                                                                                                       |
| データ タイプ              | ベンダー固有属性に対して、次のデータ型のいずれかを選択します。 <ul style="list-style-type: none"> <li>• STRING</li> <li>• OCTET_STRING</li> <li>• UNIT32</li> <li>• UNIT64</li> <li>• IPV4</li> <li>• IPV6</li> </ul> |

| フィールド                                                                                | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                              |
|--------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MAC を有効にするオプション (Enable MAC option)                                                  | <p>MAC アドレスとしての RADIUS 属性の比較を有効にするには、このチェックボックスをオンにします。デフォルトで、RADIUS 属性 <b>Calling-Station-ID</b> に対して、このオプションは有効とマークされ、無効にできません。</p> <p>RADIUS ベンダーディクショナリ内の別のディクショナリ属性（文字列型）の場合は、このオプションを有効または無効にできます。</p> <p>このオプションを有効にした場合、認証および許可条件の設定中に、テキスト オプションを選択して比較をクリアな文字列にするか、または MAC アドレスオプションを選択して比較を MAC アドレスにするかを定義できます。</p>                                         |
| 方向 (Direction)                                                                       | RADIUS メッセージに適用するいずれかのオプションを選択します。                                                                                                                                                                                                                                                                                                                                      |
| ID                                                                                   | ベンダー属性 ID を入力します。有効な範囲は 0 ～ 255 です。                                                                                                                                                                                                                                                                                                                                     |
| タギングの許可 (Allow Tagging)                                                              | <p>RFC2868 で定義するように、タグを持つことが許可されるものとして属性をマークするには、このチェック ボックスをオンにします。タグの目的は、トンネル化されたユーザの属性のグループ化を許可することです。詳細については、RFC2868 を参照してください。</p> <p>タグ付けされた属性のサポートでは、特定のトンネルに関するすべての属性のそれぞれのタグ フィールドに同じ値が含まれ、各セットに <b>Tunnel-Preference</b> 属性の適切に評価されたインスタンスが含まれていることが保証されます。これは、マルチベンダー ネットワーク環境に使用すべきトンネル属性に適合しているため、複数のベンダーで製造されたネットワーク アクセス サーバ (NAS) 間の相互運用性の問題を解決します。</p> |
| プロファイルでこの属性の複数のインスタンスを許可する (Allow multiple instances of this attribute in a profile) | プロファイルでこの RADIUS ベンダー固有属性の複数のインスタンスが必要な場合は、このチェックボックスをオンにします。                                                                                                                                                                                                                                                                                                           |

#### 関連トピック

[システム定義のディクショナリとディクショナリ属性 \(307 ページ\)](#)

[ユーザ定義のディクショナリとディクショナリ属性](#) (308 ページ)

[RADIUS ベンダー ディクショナリ](#) (310 ページ)

[RADIUS ベンダー ディクショナリの作成](#) (310 ページ)

## 条件

ここでは、エンドポイント、ポスチャクライアントのプロファイリングに使用され、Cisco ISE リソースへのアクセス権を制限または拡張するためのポリシー条件について説明します。

## プロファイラ条件の設定

次の表では、[プロファイラ条件 (Profiler Condition)] ページのフィールドについて説明します。このページへのナビゲーションパスは、[ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [条件 (Conditions)] > [プロファイリング (Profiling)] です。

表 124: プロファイラ条件の設定

| フィールド                  | 使用上のガイドライン                                                                                                                                                                                                                                                                            |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [名前 (Name)]            | プロファイラ条件の名前。                                                                                                                                                                                                                                                                          |
| 説明                     | プロファイラ条件の説明。                                                                                                                                                                                                                                                                          |
| タイプ (Type)             | 事前定義済みタイプのいずれかを選択します。                                                                                                                                                                                                                                                                 |
| 属性名 (Attribute Name)   | プロファイラ条件が基づく属性を選択します。                                                                                                                                                                                                                                                                 |
| 演算子                    | 演算子を選択します。                                                                                                                                                                                                                                                                            |
| 属性値 (Attribute Value)  | 選択した属性の値を入力します。事前定義された属性値を含む属性名の場合、事前定義された値のドロップダウン リストが表示され、値を選択できます。                                                                                                                                                                                                                |
| システム タイプ (System Type) | <p>プロファイリング条件は、次のいずれかのタイプになります。</p> <ul style="list-style-type: none"> <li>[シスコ提供 (Cisco Provided)] : シスコ提供として識別され、展開時に Cisco ISE によって提供されるプロファイリング条件。システムから編集したり削除したりすることはできません。</li> <li>[管理者作成 (Administrator Created)] : 管理者作成として識別され、Cisco ISE の管理者として作成したプロファイリング条件。</li> </ul> |

### 関連トピック

- [Cisco ISE プロファイリング サービス \(770 ページ\)](#)
- [プロファイラ条件 \(662 ページ\)](#)
- [プロファイラ フィード サービス \(818 ページ\)](#)
- [プロファイラ条件の作成 \(663 ページ\)](#)

## ポスチャ条件の設定

ここでは、ポスチャに使用される単純条件および複合条件について説明します。

### 関連トピック

- [ポスチャ サービス \(932 ページ\)](#)
- [ポスチャ条件 \(663 ページ\)](#)
- [ポスチャのカスタム条件 \(951 ページ\)](#)
- [ポスチャ ポリシーの設定 \(948 ページ\)](#)
- [ポスチャ条件の作成 \(968 ページ\)](#)

## ファイル条件の設定

次の表では、[ファイル条件 (File Conditions)] ページのフィールドについて説明します。このページのナビゲーションパスは、[ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [条件 (Conditions)] > [ポスチャ (Posture)] > [ファイル条件 (File Condition)] です。

表 125: ファイル条件の設定

| フィールド                            | Windows OS での使用ガイドライン                     | Mac OS X での使用ガイドライン           |
|----------------------------------|-------------------------------------------|-------------------------------|
| [名前 (Name)]                      | ファイル条件の名前を入力します。                          | ファイル条件の名前を入力します。              |
| 説明                               | ファイル条件の説明を入力します。                          | ファイル条件の説明を入力します。              |
| オペレーティング システム (Operating System) | ファイル条件が適用される Windows オペレーティング システムを選択します。 | ファイル条件が適用される Mac OS X を選択します。 |

| フィールド                | Windows OS での使用ガイドライン                                                                                                                                                                                                                                                                                                                                                                                         | Mac OS X での使用ガイドライン                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ファイル タイプ (File Type) | <p>次のいずれか 1 つの事前定義済み設定を選択します。</p> <ul style="list-style-type: none"> <li>• <b>FileDate</b> : 特定のファイル作成日またはファイル更新日のファイルがシステムに存在するかどうかをチェックします。</li> <li>• <b>FileExistence</b> : システムにファイルが存在するかどうかを調べます。</li> <li>• <b>FileVersion</b> : 特定のバージョンのファイルがシステムに存在するかどうかを調べます。</li> <li>• <b>CRC32</b> : チェックサム関数を使用してファイルのデータ整合性をチェックします。</li> <li>• <b>SHA-256</b> : ハッシュ関数を使用してファイルのデータ整合性をチェックします。</li> </ul> | <p>次のいずれか 1 つの事前定義済み設定を選択します。</p> <ul style="list-style-type: none"> <li>• <b>FileDate</b> : 特定のファイル作成日またはファイル更新日のファイルがシステムに存在するかどうかをチェックします。</li> <li>• <b>FileExistence</b> : システムにファイルが存在するかどうかを調べます。</li> <li>• <b>CRC32</b> : チェックサム関数を使用してファイルのデータ整合性をチェックします。</li> <li>• <b>SHA-256</b> : ハッシュ関数を使用してファイルのデータ整合性をチェックします。</li> <li>• <b>PropertyList</b> :<br/>loginwindow.plist などの plist ファイルのプロパティ値をチェックします。</li> </ul> |



| フィールド                           | Windows OS での使用ガイドライン | Mac OS X での使用ガイドライン                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| データ型と演算子 (Data Type & Operator) | NA                    | <p>(ファイルタイプとして [PropertyList] を選択した場合に限り使用可能) plist ファイル内で検索するデータ型またはキーの値を選択します。各データ型には、一連の演算子が含まれています。</p> <ul style="list-style-type: none"><li>• [未指定 (Unspecified) ] : 指定したキーの存在をチェックします。演算子 (Exists、DoesNotExist) を入力します。</li><li>• [番号 (Number) ] : 指定した番号データ型のキーをチェックします。演算子 (equals、does not equal、greater than、less than、greater than または equal to、less than または equal to) と値を入力します。</li><li>• [文字列 (String) ] : 指定した文字列データ型のキーをチェックします。演算子 (equals、does not equal、equals (ignore case)、starts with、does not start with、contains、does not contain、ends with、does not end with) と値を入力します。</li><li>• [バージョン (Version) ] : バージョン文字列で指定したキーの値をチェックします。演算子 (earlier than、later than、same as) と値を入力します。</li></ul> |

| フィールド  | Windows OSでの使用ガイドライン | Mac OS Xでの使用ガイドライン                                                                        |
|--------|----------------------|-------------------------------------------------------------------------------------------|
| プロパティ名 | NA                   | (ファイルタイプとして [PropertyList] を選択した場合に限り使用可能) キーの名前 (たとえば BuildVersionStampAsNumber) を入力します。 |

| フィールド              | Windows OSでの使用ガイドライン | Mac OS Xでの使用ガイドライン                                                                                                                                                                                            |
|--------------------|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ファイルパス (File Path) |                      | <p>次のいずれか1つの事前定義済み設定を選択します。</p> <ul style="list-style-type: none"><li>• ルート (Root) : ルート (/) ディレクトリ内のファイルをチェックします。ファイルのパスを入力します。</li><li>• ホーム (Home) : ホーム (~) ディレクトリ内のファイルをチェックします。ファイルのパスを入力します。</li></ul> |

| フィールド | Windows OS での使用ガイドライン                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Mac OS X での使用ガイドライン |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
|       | <p>次のいずれか 1 つの事前定義済み設定を選択します。</p> <ul style="list-style-type: none"> <li>• <b>ABSOLUTE_PATH</b> : ファイルの完全修飾パスのファイルをチェックします。例 : C:\&lt;directory&gt;\file name。その他の設定では、ファイル名のみを入力します。</li> <li>• <b>SYSTEM_32</b> : C:\WINDOWS\system32 ディレクトリ内のファイルをチェックします。ファイル名を入力します。</li> <li>• <b>SYSTEM_DRIVE</b> : C:\ ドライブ内のファイルをチェックします。ファイル名を入力します。</li> <li>• <b>SYSTEM_PROGRAMS</b> : C:\Program Files 内のファイルをチェックします。ファイル名を入力します。</li> <li>• <b>SYSTEM_ROOT</b> : Windows システムのルートパス内のファイルをチェックします。ファイル名を入力します。</li> <li>• <b>USER_DESKTOP</b> : 指定したファイルが Windows ユーザのデスクトップにあるかどうかをチェックします。ファイル名を入力します。</li> <li>• <b>USER_PROFILE</b> : ファイルが Windows ユーザのローカルプロファイルディレクトリにあるかど</li> </ul> |                     |

| フィールド                                | Windows OS での使用ガイドライン                                                                                                                                                                                                                                                                                                                                                                                                                                      | Mac OS X での使用ガイドライン                                                                                                                                                                                                                                                                                                             |
|--------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                      | うかをチェックします。<br>ファイルのパスを入力します。                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                 |
| ファイル日付タイプ (File Date Type)           | (ファイル タイプとして [FileDate] を選択した場合に限り使用可能) [作成日 (Creation Date) ] または [変更日 (Modification Date) ] を選択します。                                                                                                                                                                                                                                                                                                                                                      | (ファイル タイプとして [FileDate] を選択した場合に限り使用可能) [作成日 (Creation Date) ] または [変更日 (Modification Date) ] を選択します。                                                                                                                                                                                                                           |
| ファイル演算子/演算子 (File Operator/Operator) | <p>[ファイル演算子 (File Operator) ] オプションは、[ファイルタイプ (File Type) ] で選択した設定に応じて変化します。次の設定を適切に選択します。</p> <p>FileDate</p> <ul style="list-style-type: none"> <li>• EarlierThan</li> <li>• LaterThan</li> <li>• EqualTo</li> </ul> <p>FileExistence</p> <ul style="list-style-type: none"> <li>• Exists</li> <li>• DoesNotExist</li> </ul> <p>FileVersion</p> <ul style="list-style-type: none"> <li>• EarlierThan</li> <li>• LaterThan</li> <li>• EqualTo</li> </ul> | <p>[ファイル演算子 (File Operator) ] オプションは、[ファイルタイプ (File Type) ] で選択した設定に応じて変化します。次の設定を適切に選択します。</p> <p>FileDate</p> <ul style="list-style-type: none"> <li>• EarlierThan</li> <li>• LaterThan</li> <li>• EqualTo</li> </ul> <p>FileExistence</p> <ul style="list-style-type: none"> <li>• Exists</li> <li>• DoesNotExist</li> </ul> |
| ファイルの CRC データ (File CRC Data)        | (ファイル タイプとして [CRC32] を選択した場合に限り使用可能) チェックサムの値 (たとえば 0x3c37fec3) を入力してファイルの整合性をチェックできます。チェックサム値は 16 進数の整数 0x で始まる必要があります。                                                                                                                                                                                                                                                                                                                                   | (ファイル タイプとして [CRC32] を選択した場合に限り使用可能) チェックサムの値 (たとえば 0x3c37fec3) を入力してファイルの整合性をチェックできます。チェックサム値は 16 進数の整数 0x で始まる必要があります。                                                                                                                                                                                                        |

| フィールド                                  | Windows OS での使用ガイドライン                                                                             | Mac OS X での使用ガイドライン                                                                               |
|----------------------------------------|---------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|
| ファイルのSHA-256データ<br>(File SHA-256 Data) | (ファイル タイプとして [SHA-256] を選択した場合に限り使用可能) 64 バイトの 16 進数のハッシュ値を入力してファイルの整合性をチェックできます。                 | (ファイル タイプとして [SHA-256] を選択した場合に限り使用可能) 64 バイトの 16 進数のハッシュ値を入力してファイルの整合性をチェックできます。                 |
| 日付および時刻 (Date and Time)                | (ファイル タイプとして <b>FileDate</b> を選択した場合に限り使用可能) クライアント システムの日付と時刻を、mm/dd/yyyy および hh:mm:ss 形式で入力します。 | (ファイル タイプとして <b>FileDate</b> を選択した場合に限り使用可能) クライアント システムの日付と時刻を、mm/dd/yyyy および hh:mm:ss 形式で入力します。 |

#### 関連トピック

[単純ポスチャ条件](#) (664 ページ)

[複合ポスチャ条件](#) (665 ページ)

[ポスチャ条件の作成](#) (968 ページ)

## ファイアウォール条件の設定

ファイアウォール条件により、特定のファイアウォール製品がエンドポイントで稼働しているかどうかを確認されます。サポートされているファイアウォール製品のリストは、OPSWAT サポート チャートに基づいています。初回ポスチャと定期的再評価 (PRA) の実行中にポリシーを適用できます。

| フィールド                            | 使用上のガイドライン                                                                  |
|----------------------------------|-----------------------------------------------------------------------------|
| [名前 (Name) ]                     | ファイアウォール条件の名前を入力します。                                                        |
| 説明                               | ファイアウォール条件の説明を入力します。                                                        |
| コンプライアンス モジュール                   | OESIS バージョン 4.x 以降をサポートします。                                                 |
| オペレーティング システム (Operating System) | 必要なファイアウォール製品がエンドポイントにインストールされているかどうかを確認します。Windows OS または Mac OSX を選択できます。 |

| フィールド                 | 使用上のガイドライン                                                                                                                                                  |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ベンダー                  | ドロップダウン リストからベンダー名を選択します。ベンダーのファイアウォール製品とそれらのチェック タイプが取得され、[選択したベンダーの製品 (Products for Selected Vendor) ] テーブルに表示されます。テーブル内のリストは、選択したオペレーティング システムによって変わります。 |
| チェック タイプ (Check Type) | [有効 (Enabled) ] : 特定のファイアウォールがエンドポイントで稼働しているかどうかをチェックします。ベンダーの製品が選択したチェック タイプをサポートしているかどうかを [選択したベンダーの製品 (Products for Selected Vendor) ] リストを参照することで確認します。 |

## レジストリ条件の設定

次の表では、[レジストリ条件 (Registry Conditions) ] ページのフィールドについて説明します。このページへのナビゲーションパスは、[ポリシー (Policy) ] > [ポリシー要素 (Policy Elements) ] > [条件 (Conditions) ] > [ポスチャ (Posture) ] > [レジストリ条件 (Registry Condition) ] です。

表 126: レジストリ条件の設定

| フィールド                            | 使用上のガイドライン                                                                                                                                                                                                |
|----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [名前 (Name) ]                     | レジストリ条件の名前を入力します。                                                                                                                                                                                         |
| 説明                               | レジストリ条件の説明を入力します。                                                                                                                                                                                         |
| レジストリ タイプ (Registry Type)        | レジストリ タイプとして事前定義済み設定の 1 つを選択します。                                                                                                                                                                          |
| レジストリ ルート キー (Registry Root Key) | レジストリ ルート キーとして事前定義済み設定の 1 つを選択します。                                                                                                                                                                       |
| サブ キー (Sub Key)                  | レジストリ ルート キーに指定されたパスのレジストリ キーをチェックするには、バックスラッシュ (「\」) なしでサブ キーを入力します。<br><br>たとえば、SOFTWARE\Symantec\Norton AntiVirus\version によって、次のパスのキーがチェックされます。<br><br>HKLM\SOFTWARE\Symantec\NortonAntiVirus\version |

| フィールド                            | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 値の名前 (Value Name)                | <p>([レジストリ タイプ (Registry Type)] として [RegistryValue] または [RegistryValueDefault] を選択した場合にのみ使用可能)</p> <p>[RegistryValue] をチェックするレジストリ キー値の名前を入力します。</p> <p>これは [RegistryValueDefault] のデフォルトフィールドです。</p>                                                                                                                                                                                                                         |
| 値データ型 (Value Data Type)          | <p>([レジストリ タイプ (Registry Type)] として [RegistryValue] または [RegistryValueDefault] を選択した場合にのみ使用可能) 次の設定の 1 つを選択します。</p> <ul style="list-style-type: none"> <li>• [未指定 (Unspecified)] : レジストリ キー値があるかどうかをチェックします。このオプションは、[RegistryValue] の場合にのみ使用できます。</li> <li>• [数字 (Number)] : レジストリ キー値の指定された数字をチェックします。</li> <li>• [文字列 (String)] : レジストリ キー値の文字列をチェックします</li> <li>• [バージョン (Version)] : レジストリ キー値のバージョンをチェックします。</li> </ul> |
| 値演算子 (Value Operator)            | 設定を適切に選択します。                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 値データ                             | <p>([レジストリ タイプ (Registry Type)] として [RegistryValue] または [RegistryValueDefault] を選択した場合にのみ使用可能) [値データ型 (Value Data Type)] で選択したデータ型に応じてレジストリ キーの値を入力します。</p>                                                                                                                                                                                                                                                                   |
| オペレーティング システム (Operating System) | レジストリ条件を適用する必要があるオペレーティング システムを選択します。                                                                                                                                                                                                                                                                                                                                                                                         |

#### 関連トピック

[単純ポスチャ条件](#) (664 ページ)

[複合ポスチャ条件](#) (665 ページ)

## 継続的なエンドポイント属性モニタリング

ポスチャ アセスメントの実行中に動的な変更が確認されるようにするため、AnyConnect エージェントを使用してさまざまなエンドポイント属性を継続的にモニタします。これによりエン



ドポイントの全体的な可視性が向上し、動作に基づいてポスチャポリシーを作成できるようになります。AnyConnect エージェントは、エンドポイントにインストールされ実行されているアプリケーションをモニタします。この機能をオンまたはオフにできます。また、データのモニタ頻度を設定できます。デフォルトでは、データは5分間隔で収集され、データベースに保存されます。初回ポスチャでは、AnyConnect がすべての実行中アプリケーションとインストールされているアプリケーションのリストを報告します。初回ポスチャの後に、AnyConnect エージェントはX分間隔でアプリケーションをスキャンし、最終スキャンでの差異をサーバに送信します。サーバはすべての実行中アプリケーションとインストールされているアプリケーションのリストを表示します。

## アプリケーション条件の設定

エンドポイントにインストールされているアプリケーションに対するアプリケーション条件クエリ。これにより、エンドポイントで配信されているソフトウェアの集約された可視性を確認できます。たとえば、この情報に基づいてポリシーを作成し、デスクトップチームと協力してソフトウェア ライセンスの数を減らすことができます。

次の表に、[アプリケーション条件 (Application Conditions)] ページのフィールドを示します。このページへのナビゲーションパスは [ワーク センター (Work Centers)] > [ポスチャ (Posture)] > [ポリシー要素 (Policy Elements)] > [アプリケーション条件 (Application Condition)] > [追加 (Add)] です。

| フィールド                            | 使用上のガイドライン                                                                                                                                                                                                                     |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [名前 (Name)]                      | アプリケーション条件の名前を入力します。                                                                                                                                                                                                           |
| 説明                               | アプリケーション条件の説明を入力します。                                                                                                                                                                                                           |
| オペレーティング システム (Operating System) | アプリケーション条件が適用される Windows OS または MAC OSX を選択します。                                                                                                                                                                                |
| コンプライアンス モジュール                   | OESIS バージョン 4.x 以降、3.x 以前、またはすべてのバージョンのサポート。                                                                                                                                                                                   |
| 次を確認 (Check By)                  | 次のいずれかを実行します。 <ul style="list-style-type: none"> <li>• [プロセス (Process)] : エンドポイントでプロセスが実行されているかどうかを確認するには、このオプションをオンにします。</li> <li>• [アプリケーション (Application)] : エンドポイントでアプリケーションが実行されているかどうかを確認するには、このオプションをオンにします。</li> </ul> |
| プロセス名                            | ([次を確認 (Check By)] オプションで [プロセス (Process)] を選択した場合に使用可能) 必要なプロセス名を入力します。                                                                                                                                                       |

| フィールド                              | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                         |
|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| アプリケーション演算子 (Application Operator) | <p>([次を確認 (Check By)] オプションで[プロセス (Process)] を選択した場合に使用可能) 次のいずれかを選択します。</p> <ul style="list-style-type: none"><li>• [実行中 (Running)] : エンドポイントでアプリケーションが実行されているかどうかを確認するには、このオプションを選択します。</li><li>• [実行されていない (Not Running)] : エンドポイントでアプリケーションが実行されていないかどうかを確認するには、このオプションをオンにします。</li></ul>                                                      |
| アプリケーションの状態 (Application State)    | <p>([次を確認 (Check By)] オプションで[アプリケーション (Application)] を選択した場合に使用可能) 次のいずれかを選択します。</p> <ul style="list-style-type: none"><li>• [インストール済み (Installed)] : クライアントのシステムに悪質なアプリケーションがインストールされているかどうかを調べるには、このオプションをオンにします。悪意のあるアプリケーションがある場合は、修復アクションがトリガーされます。</li><li>• [実行中 (Running)] : エンドポイントでアプリケーションが実行されているかどうかを確認するには、このオプションをオンにします。</li></ul> |

| フィールド                     | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 次をプロビジョニング (Provision By) | <p>([次を確認 (Check By)] オプションで[アプリケーション (Application)] を選択した場合に使用可能) 次のいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• [すべて (Everything)] : [ブラウザ (Browser)]、[パッチ管理 (Patch Management)] など、リストされているすべてのカテゴリを選択できます。</li> <li>• [名前 (Name)] : 1 つ以上のカテゴリを選択します。たとえば [ブラウザ (Browser)] カテゴリを選択すると、[ベンダー (Vendor)] ドロップダウン リストに対応するベンダーが表示されます。</li> <li>• [カテゴリ (Category)] : 1 つ以上のカテゴリ ([マルウェア対策 (Anti-Malware)]、[バックアップ (Backup)]、[ブラウザ (Browser)]、[データ ストレージ (Data Storage)] など) をオンにできます。</li> </ul> <p>(注) カテゴリは OPSWAT ライブラリから動的に更新されます。</p> |

[コンテキストの可視性 (Context Visibility)] > [エンドポイント (Endpoints)] > [コンプライアンス (Compliance)] ページで、各エンドポイントでインストールされているアプリケーションと実行中のアプリケーションの数を確認できます。

[ホーム (Home)] > [概要 (Summary)] > [コンプライアンス (Compliance)] ページに、ポスチャアセスメント対象であり準拠しているエンドポイントのパーセンテージが表示されます。

## サービス条件の設定

次の表では、[サービス条件 (Service Conditions)] ページのフィールドについて説明します。このページへのナビゲーションパスは、[ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [条件 (Conditions)] > [ポスチャ (Posture)] > [サービス条件 (Service Condition)] です。

表 127: サービス条件の設定

| フィールド       | 使用上のガイドライン       |
|-------------|------------------|
| [名前 (Name)] | サービス条件の名前を入力します。 |
| 説明          | サービス条件の説明を入力します。 |

| フィールド                             | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| オペレーティング システム (Operating Systems) | サービス条件を適用する必要があるオペレーティングシステムを選択します。Windows OS または Mac OSX のさまざまなバージョンを選択できます。                                                                                                                                                                                                                                                                                                                                                                        |
| サービス名 (Service Name)              | ルートとして動作するデーモンまたはユーザーエージェントサービスの名前を入力します (たとえば <code>com.apple.geod</code> )。AnyConnect エージェントは、コマンド <code>sudo launchctl list</code> を使用してサービス条件を確認します。                                                                                                                                                                                                                                                                                             |
| サービス タイプ (Service Type)           | <p>クライアントのコンプライアンスを確実にするために AnyConnect が調べる必要があるタイプ オブ サービスを選択します。</p> <ul style="list-style-type: none"><li>• [デーモン (Daemon)] : マルウェアに対するクライアント デバイスのスキャンなど、指定したサービスがクライアントのデーモンサービスの指定されたリストにあるかどうかをチェックします。</li><li>• [ユーザーエージェント (User Agent)] : マルウェアが検出された場合に実行するサービスなど、指定したサービスがクライアントのユーザ サービスの指定されたリストにあるかどうかをチェックします。</li><li>• [デーモンまたはユーザーエージェント (Daemon or User Agent)] : 指定したサービスがデーモンまたはユーザーエージェントのサービス リストにあるかどうかをチェックします。</li></ul> |

| フィールド                         | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| サービス オペレータ (Service Operator) | <p>クライアントでチェックするサービス ステータスを選択します。</p> <ul style="list-style-type: none"> <li>• Windows OS : サービスが [実行している (Running)] か、または [実行していない (Not Running)] かを確認します。</li> <li>• Mac OSX : サービスが [ロード済み (Loaded)] か、[ロードされていない (NotLoaded)] か、[ロード済みで実行している (Loaded &amp; Running)] か、[終了コード付きでロード済み (Loaded with Exit Code)] か、[ロード済みで実行しているまたは終了コードが付いている (Loaded &amp; running or with Exit code)] かどうかを確認します。</li> </ul> |

#### 関連トピック

[単純ポスチャ条件](#) (664 ページ)

[複合ポスチャ条件](#) (665 ページ)

## ポスチャ複合条件の設定

次の表では、[複合条件 (Compound Conditions)] ページのフィールドについて説明します。このページへのナビゲーションパスは、[ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [条件 (Conditions)] > [ポスチャ (Posture)] > [複合条件 (Compound Condition)] です。

表 128: ポスチャ複合条件の設定

| フィールド                            | 使用上のガイドライン                                                                            |
|----------------------------------|---------------------------------------------------------------------------------------|
| [名前 (Name)]                      | 作成する複合条件の名前を入力します。                                                                    |
| 説明                               | 作成する複合条件の説明を入力します。                                                                    |
| オペレーティング システム (Operating System) | 1 つ以上の Windows オペレーティング システムを選択します。これにより、条件が適用される Windows オペレーティング システムを関連付けることができます。 |
| カッコ ( ) (Parentheses ( ))        | ファイル、レジストリ、アプリケーション、サービス条件という単純な条件タイプから 2 つの単純条件を組み合わせるには、カッコをクリックします。                |

| フィールド                              | 使用上のガイドライン                                                                                                                                                                                                        |
|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| (&) : AND 演算子 (AND 演算子には「&」を使用します) | 複合条件内には AND 演算子 (アンパサンド (&)) を使用できます。たとえば、 <b>Condition1 &amp; Condition2</b> と入力します。                                                                                                                             |
| ( ) : OR 演算子 (OR 演算子には「 」を使用します)   | 複合条件内には OR 演算子 (縦線「 」) を使用できます。たとえば、 <b>Condition1 &amp; Condition2</b> と入力します。                                                                                                                                   |
| (!) : NOT 演算子 (NOT 演算子には「!」を使用します) | 複合条件内には NOT 演算子 (感嘆符 (!)) を使用できます。たとえば、 <b>Condition1 &amp; Condition2</b> と入力します。                                                                                                                                |
| 単純条件                               | <p>ファイル、レジストリ、アプリケーション、サービス条件という単純条件のリストから選択します。</p> <p>また、オブジェクトセレクトからファイル、レジストリ、アプリケーション、サービス条件という単純条件を作成できます。</p> <p>ファイル、レジストリ、アプリケーション、サービス条件という単純条件を作成するには、[操作 (Action)] ボタンのクイックピッカー (下向き矢印) をクリックします。</p> |

#### 関連トピック

[ポスチャ条件](#) (663 ページ)

[複合ポスチャ条件の作成](#) (667 ページ)

## ウイルス対策条件の設定

次の表では、[ウイルス対策条件 (Anti-Virus Condition)] ページのフィールドについて説明します。このページへのナビゲーションパスは、[ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [条件 (Conditions)] > [ポスチャ (Posture)] > [ウイルス対策条件 (Anti-Virus Condition)] です。

表 129: ウイルス対策条件の設定

| フィールド       | 使用上のガイドライン             |
|-------------|------------------------|
| [名前 (Name)] | 作成するウイルス対策条件の名前を入力します。 |
| 説明          | 作成するウイルス対策条件の説明を入力します。 |

| フィールド                                                                                                                                             | 使用上のガイドライン                                                                                                                                                                                                                                         |
|---------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| オペレーティング システム (Operating System)                                                                                                                  | オペレーティング システムを選択して、クライアント上のアンチウイルス プログラムのインストールをチェックするか、または条件が適用される最新のアンチウイルス定義ファイルの更新をチェックします。                                                                                                                                                    |
| ベンダー                                                                                                                                              | ドロップダウン リストからベンダーを選択します。ベンダーを選択すると、アンチウイルス製品およびバージョンが取得され、[選択したベンダーの製品 (Products for Selected Vendor)] テーブルに表示されます。                                                                                                                                |
| チェック タイプ (Check Type)                                                                                                                             | クライアント上でインストールをチェックするか、または最新の定義ファイルの更新をチェックするかを選択します。                                                                                                                                                                                              |
| インストール                                                                                                                                            | クライアント上のアンチウイルス プログラムのインストールのみをチェックする場合に選択します。                                                                                                                                                                                                     |
| 定義 (Definition)                                                                                                                                   | クライアント上のアンチウイルス製品の、最新の定義ファイルの更新のみをチェックする場合に選択します。                                                                                                                                                                                                  |
| 最新の AV 定義ファイルのバージョンに対してチェックします (使用可能な場合)。<br>(Check against latest AV definition file version, if available.) (それ以外の場合は、最新の定義ファイルの日付に対してチェックします)。 | ([定義 (Definition)] チェック タイプを選択した場合にのみ使用可能) クライアントのアンチウイルス定義ファイルのバージョンをチェックする場合に選択します。Cisco ISE でのポスチャ更新の結果として、最新のアンチウイルス定義ファイルのバージョンを使用できるときには、そのバージョンに対するチェックが行われます。それ以外の場合、このオプションを使用すると、クライアント上の定義ファイルの日付を、Cisco ISE の最新の定義ファイルの日付に対してチェックできます。 |

| フィールド                                                                  | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ウイルス定義ファイルを（有効）にすることを許可する（Allow virus definition file to be (Enabled)） | <p>（定義チェック タイプを選択した場合のみ使用可能） アンチウイルス定義ファイルのバージョンと、クライアント上の最新のアンチウイルス定義ファイルの日付をチェックする場合に選択します。最新の定義ファイルの日付が、製品の最新のアンチウイルス定義ファイルの日付または現在のシステム日付から、次のフィールド（[より古い日数（days older than）] フィールド）で定義した日数よりも古いことは許容されません。</p> <p>オフにした場合、[最新の AV 定義ファイルのバージョンに対してチェックします（使用可能な場合）。（Check against latest AV definition file version, if available.）] オプションを使用してアンチウイルス定義ファイルのバージョンのみをチェックすることができます。</p> |
| より古い日数（days older than）                                                | <p>クライアント上の最新のアンチウイルス定義ファイルの日付が、製品の最新のアンチウイルス定義ファイルの日付または現在のシステム日付よりも何日古いことが許容されるかを定義します。デフォルト値は 0 です。</p>                                                                                                                                                                                                                                                                                   |
| 最新のファイルの日付（latest file date）                                           | <p>[より古い日数（days older than）] クライアント上のアンチウイルス定義ファイルの日付をチェックすることを選択します。この日付は、フィールドで定義した日数だけ古いことが許容されます。</p> <p>日数をデフォルト値（0）に設定する場合、クライアント上のアンチウイルス定義ファイルの日付が、製品の最新のアンチウイルス定義ファイルの日付よりも古いことは許容されません。</p>                                                                                                                                                                                        |
| 現在のシステム日付（current system date）                                         | <p>[より古い日数（days older than）] クライアント上のアンチウイルス定義ファイルの日付をチェックすることを選択します。この日付は、フィールドで定義した日数だけ古いことが許容されます。</p> <p>日数をデフォルト値（0）に設定する場合、クライアント上のアンチウイルス定義ファイルの日付が、現在のシステム日付よりも古いことは許容されません。</p>                                                                                                                                                                                                     |



| フィールド                                      | 使用上のガイドライン                                                                                                                                                                                                                                                          |
|--------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 選択したベンダーの製品 (Products for Selected Vendor) | <p>テーブルからアンチウイルス製品を選択します。[新しいアンチウイルス条件 (New Anti-virus Compound Condition)] ページで選択したベンダーに基づいて、テーブルは、アンチウイルス製品およびバージョン、提供する修復のサポート、最新の定義ファイルの日付とバージョンに関する情報を取得します。</p> <p>テーブルから製品を選択すると、アンチウイルス プログラムのインストールをチェックしたり、最新のアンチウイルス定義ファイルの日付および最新バージョンをチェックしたりできます。</p> |

#### 関連トピック

[複合ポスチャ条件 \(665 ページ\)](#)

[シスコ事前設定済みアンチウイルスおよびアンチスパイウェア条件 \(665 ページ\)](#)

[アンチウイルスとアンチスパイウェア サポート表 \(666 ページ\)](#)

## アンチスパイウェア複合条件の設定

次の表に、[AS 複合条件 (AS Compound Conditions)] ページのフィールドを示します。このページへのナビゲーションパスは、[ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [条件 (Conditions)] > [AS 複合条件 (AS Compound Condition)] です。

表 130: アンチスパイウェア複合条件の設定

| フィールド                            | 使用上のガイドライン                                                                                                  |
|----------------------------------|-------------------------------------------------------------------------------------------------------------|
| [名前 (Name)]                      | 作成するアンチスパイウェア複合条件の名前を入力します。                                                                                 |
| 説明                               | 作成するアンチスパイウェア複合条件の説明を入力します。                                                                                 |
| オペレーティング システム (Operating System) | オペレーティング システムを選択すると、クライアント上のアンチスパイウェア プログラムのインストールをチェックするか、または条件が適用される最新のアンチスパイウェア 定義ファイルの更新をチェックすることができます。 |

| フィールド                                                                     | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ベンダー                                                                      | ドロップダウン リストからベンダーを選択します。ベンダーを選択すると、アンチスパイウェア製品およびバージョンが取得され、[選択したベンダーの製品 (Products for Selected Vendor)] テーブルに表示されます。                                                                                                                                                                                                                                                                                                     |
| チェック タイプ (Check Type)                                                     | クライアント上でインストールをチェックするか、または最新の定義ファイルの更新をチェックするか、いずれかのタイプを選択します。                                                                                                                                                                                                                                                                                                                                                            |
| インストール                                                                    | クライアント上のアンチスパイウェア プログラムのインストールのみをチェックする場合に選択します。                                                                                                                                                                                                                                                                                                                                                                          |
| 定義 (Definition)                                                           | クライアント上のアンチスパイウェア製品の、最新の定義ファイルの更新のみをチェックする場合に選択します。                                                                                                                                                                                                                                                                                                                                                                       |
| ウイルス定義ファイルを (有効) にすることを許可する (Allow virus definition file to be (Enabled)) | <p>このチェックボックスは、アンチスパイウェア定義チェック タイプを作成するときはオンにし、アンチスパイウェア インストール チェック タイプを作成するときはオフにします。</p> <p>オンにすると、その選択により、クライアント上のアンチスパイウェア定義ファイルのバージョンおよび最新のアンチスパイウェア定義ファイルの日付をチェックできます。最新の定義ファイルの日付が、現在のシステム日付から、[より古い日数 (days older than)] フィールドで定義した日数より古いことは許容されません。</p> <p>オフの場合、その選択により、[ウイルス定義ファイルを (有効) にすることを許可する (Allow virus definition file to be (Enabled))] チェックボックスがオフのときに、アンチスパイウェア定義ファイルのバージョンのみをチェックすることができます。</p> |
| より古い日数 (days older than)                                                  | クライアント上の最新のアンチスパイウェア定義ファイルの日付が、現在のシステム日付よりも何日古いことが許容されるかを定義します。デフォルト値は 0 です。                                                                                                                                                                                                                                                                                                                                              |

| フィールド                                      | 使用上のガイドライン                                                                                                                                                                                                                                                                        |
|--------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 現在のシステム日付 (current system date)            | <p>[より古い日数 (days older than) ] クライアント上のアンチスパイウェア定義ファイルの日付をチェックすることを選択します。この日付は、フィールドで定義した日数だけ古いことが許容されます。</p> <p>日数をデフォルト値 (0) に設定する場合、クライアント上のアンチスパイウェア定義ファイルの日付が、現在のシステム日付よりも古いことは許容されません。</p>                                                                                  |
| 選択したベンダーの製品 (Products for Selected Vendor) | <p>テーブルからアンチスパイウェア製品を選択します。[新しいアンチスパイウェア複合条件 (New Anti-spyware Compound Condition) ] ページで選択したベンダーに基づいて、テーブルは、アンチスパイウェア製品およびバージョン、提供する修復のサポート、最新の定義ファイルの日付とバージョンに関する情報を取得します。</p> <p>テーブルから製品を選択すると、アンチスパイウェアプログラムのインストールをチェックしたり、最新のアンチスパイウェア定義ファイルの日付および最新バージョンをチェックしたりできます。</p> |

#### 関連トピック

[複合ポスチャ条件 \(665 ページ\)](#)

[シスコ事前設定済みアンチウイルスおよびアンチスパイウェア条件 \(665 ページ\)](#)

[アンチウイルスとアンチスパイウェア サポート表 \(666 ページ\)](#)

## マルウェア対策条件の設定

マルウェア対策条件はスパイウェア対策条件とウイルス対策条件の組み合わせで、OESIS バージョン 4.x 以降のコンプライアンス モジュールでサポートされています。次の表では、[マルウェア対策条件 (Antimalware Conditions) ] ページのフィールドについて説明します。ナビゲーションパスは、[ワーク センター (Work Centers) ] > [ポスチャ (Posture) ] > [ポスチャ要素 (Posture Elements) ] > [条件 (Conditions) ] > [マルウェア対策 (Antimalware) ] です。また、[ポリシー (Policy) ] > [ポリシー要素 (Policy Elements) ] > [条件 (Conditions) ] > [ポスチャ (Posture) ] > [マルウェア対策条件 (Antimalware Condition) ] ページでもこのオプションにアクセスできます。

表 131: マルウェア対策条件の設定

| フィールド                            | 使用上のガイドライン                                                                                                                                           |
|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| [名前 (Name) ]                     | マルウェア対策条件の名前を入力します。                                                                                                                                  |
| 説明                               | マルウェア対策条件の説明を入力します。                                                                                                                                  |
| コンプライアンス モジュール                   | OESIS バージョン 4.x 以降のサポート。                                                                                                                             |
| オペレーティング システム (Operating System) | オペレーティング システムを選択して、クライアント上のマルウェア対策プログラムのインストールをチェックするか、または条件が適用される最新のマルウェア対策定義ファイルの更新をチェックします。MAC と Windows OS の両方をサポートしています。                        |
| ベンダー                             | ドロップダウン リストからベンダーを選択します。選択したベンダーのマルウェア対策製品、バージョン、最新の定義日、最新の定義バージョン、最小コンプライアンス モジュールバージョンが [選択したベンダーの製品 (Products for Selected Vendor) ] テーブルに表示されます。 |
| チェック タイプ (Check Type)            | クライアント上でインストールをチェックするか、または最新の定義ファイルの更新をチェックするかを選択します。                                                                                                |
| インストール                           | クライアント上のマルウェア対策プログラムのインストールのみをチェックする場合に選択します。                                                                                                        |
| 定義 (Definition)                  | クライアント上のマルウェア対策製品の、最新の定義ファイルの更新のみをチェックする場合に選択します。                                                                                                    |

| フィールド                                                                                                                                                      | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>最新の AV 定義ファイルのバージョンに対してチェックします（使用可能な場合）。</p> <p>(Check against latest AV definition file version, if available.)（それ以外の場合は、最新の定義ファイルの日付に対してチェックします）。</p> | <p>〔定義（Definition）〕チェック タイプを選択した場合にのみ使用可能）クライアントのマルウェア対策定義ファイルのバージョンをチェックする場合に選択します。Cisco ISE でのポスチャ更新の結果として、最新のマルウェア対策定義ファイルのバージョンを使用できるときには、そのバージョンに対するチェックが行われます。それ以外の場合、このオプションを使用すると、クライアント上の定義ファイルの日付を、Cisco ISE の最新の定義ファイルの日付に対してチェックできます。</p> <p>このチェックは、選択した製品の [最新の定義日（Latest Definition Date）] または [最新の定義バージョン（Latest Definition Version）] フィールドの Cisco ISE に値が記載されている場合にのみ機能します。そうでない場合は、[現在のシステム日付（Current System Date）] フィールドを使用する必要があります。</p> |
| <p>ウイルス定義ファイルを（有効）にすることを許可する（Allow Virus Definition File to be (Enabled)）</p>                                                                              | <p>（定義チェック タイプを選択した場合のみ使用可能）マルウェア対策定義ファイルのバージョンと、クライアント上の最新のマルウェア対策定義ファイルの日付をチェックする場合に選択します。最新の定義ファイルの日付が、製品の最新のマルウェア対策定義ファイルの日付または現在のシステム日付から、次のフィールド（[より古い日数（days older than）] フィールド）で定義した日数よりも古いことは許容されません。</p> <p>オフにした場合、[最新の AV 定義ファイルのバージョンに対してチェックします（使用可能な場合）。（Check against latest AV definition file version, if available.）] オプションを使用してマルウェア対策定義ファイルのバージョンのみをチェックすることができます。</p>                                                                  |
| <p>より古い日数（Days Older Than）</p>                                                                                                                             | <p>クライアント上の最新のマルウェア対策定義ファイルの日付が、製品の最新のマルウェア対策定義ファイルの日付または現在のシステム日付よりも何日古いことが許容されるかを定義します。デフォルト値は 0 です。</p>                                                                                                                                                                                                                                                                                                                                                   |

| フィールド                                      | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 最新のファイルの日付 (Latest File Date)              | <p>クライアント上のマルウェア対策定義ファイルの日付をチェックすることを選択します。この日付は、[より古い日数 (days older than) ] フィールドで定義した日数だけ古いことが許容されます。</p> <p>日数をデフォルト値 (0) に設定する場合、クライアント上のマルウェア対策定義ファイルの日付が、製品の最新のマルウェア対策定義ファイルの日付よりも古いことは許容されません。</p> <p>このチェックは、選択した製品の [最新の定義日 (Latest Definition Date) ] フィールドの Cisco ISE に値が記載されている場合にのみ機能します。そうでない場合は、[現在のシステム日付 (Current System Date) ] フィールドを使用する必要があります。</p> |
| 現在のシステム日付 (Current System Date)            | <p>クライアント上のマルウェア対策定義ファイルの日付をチェックすることを選択します。この日付は、[より古い日数 (days older than) ] フィールドで定義した日数だけ古いことが許容されます。</p> <p>日数をデフォルト値 (0) に設定する場合、クライアント上のマルウェア対策定義ファイルの日付が、現在のシステム日付よりも古いことは許容されません。</p>                                                                                                                                                                             |
| 選択したベンダーの製品 (Products for Selected Vendor) | <p>テーブルからマルウェア対策製品を選択します。[新しいマルウェア対策条件 (New Antimalware Condition) ] ページで選択したベンダーに基づいて、テーブルは、マルウェア対策製品およびバージョン、提供する修復のサポート、最新の定義ファイルの日付とバージョンに関する情報を取得します。</p> <p>テーブルから製品を選択すると、マルウェア対策プログラムのインストールをチェックしたり、最新のマルウェア対策定義ファイルの日付および最新バージョンをチェックしたりできます。</p>                                                                                                              |

## 関連トピック

[複合ポスチャ条件 \(665 ページ\)](#)

## ディクショナリ単純条件の設定

次の表に、[ディクショナリ単純条件（Dictionary Simple Conditions）] ページのフィールドを示します。このページへのナビゲーションパスは、[ポリシー（Policy）]>[ポリシー要素（Policy Elements）]>[条件（Conditions）]>[ポスチャ（Posture）]>[ディクショナリ単純条件（Dictionary Simple Conditions）] です。

表 132: ディクショナリ単純条件の設定

| フィールド         | 使用上のガイドライン                                            |
|---------------|-------------------------------------------------------|
| [名前（Name）]    | 作成するディクショナリ単純条件の名前を入力します。                             |
| 説明            | 作成するディクショナリ単純条件の説明を入力します。                             |
| 属性（Attribute） | ディクショナリから属性を選択します。                                    |
| 演算子           | 選択した属性に値に関連付ける演算子を選択します。                              |
| 値             | ディクショナリ属性に関連付ける値を入力するか、またはドロップダウンリストから事前定義済みの値を選択します。 |

### 関連トピック

[ディクショナリおよびディクショナリ属性](#)（307 ページ）

[単純条件と複合条件](#)（659 ページ）

[単純ポスチャ条件](#)（664 ページ）

[単純ポスチャ条件の作成](#)（664 ページ）

## ディクショナリ複合条件の設定

次の表に、[ディクショナリ複合条件（Dictionary Compound Conditions）] のページのフィールドを示します。このページへのナビゲーションパスは、[ポリシー（Policy）]>[ポリシー要素（Policy Elements）]>[条件（Conditions）]>[ポスチャ（Posture）]>[ディクショナリ複合条件（Dictionary Compound Conditions）] です。

表 133: ディクショナリ複合条件の設定

| フィールド      | 使用上のガイドライン                |
|------------|---------------------------|
| [名前（Name）] | 作成するディクショナリ複合条件の名前を入力します。 |
| 説明         | 作成するディクショナリ複合条件の説明を入力します。 |

| フィールド                                                       | 使用上のガイドライン                                                                                                                                                                                                                                                             |
|-------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 既存の条件をライブラリから選択 (Select Existing Condition from Library)    | ポリシー要素ライブラリから事前定義済みの条件を選択して式を定義するか、または後のステップでアドホック属性/値のペアを式に追加します。                                                                                                                                                                                                     |
| 条件名 (Condition Name)                                        | ポリシー要素ライブラリからすでに作成しているディクショナリ単純条件を選択します。                                                                                                                                                                                                                               |
| 式 (Expression)                                              | [条件名 (Condition Name)] ドロップダウン リストでの選択に基づいて式が更新されます。                                                                                                                                                                                                                   |
| AND または OR 演算子 (AND or OR operator)                         | <p>ライブラリから追加できるディクショナリ単純条件を論理的に組み合わせるには、AND または OR 演算子を選択します。</p> <p>次の操作を行うには、[操作 (Action)] アイコンをクリックします。</p> <ul style="list-style-type: none"> <li>属性/値の追加 (Add Attribute/Value)</li> <li>ライブラリから条件を追加 (Add Condition from Library)</li> <li>削除 (Delete)</li> </ul> |
| 新しい条件の作成 (高度なオプション) (Create New Condition (Advance Option)) | <p>さまざまなシステムディクショナリまたはユーザ定義ディクショナリから属性を選択します。</p> <p>後のステップで事前定義された条件をポリシー要素ライブラリから追加することもできます。</p>                                                                                                                                                                    |
| 条件名 (Condition Name)                                        | すでに作成したディクショナリ単純条件を選択します。                                                                                                                                                                                                                                              |
| 式 (Expression)                                              | [式 (Expression)] ドロップダウン リストから、ディクショナリ単純条件を作成できます。                                                                                                                                                                                                                     |
| 演算子                                                         | 属性に値に関連付ける演算子を選択します。                                                                                                                                                                                                                                                   |
| 値                                                           | ディクショナリ属性に関連付ける値を入力するか、またはドロップダウン リストから値を選択します。                                                                                                                                                                                                                        |

#### 関連トピック

[ディクショナリおよびディクショナリ属性](#) (307 ページ)

[単純条件と複合条件](#) (659 ページ)

[複合ポスチャ条件](#) (665 ページ)



[複合ポスチャ条件の作成](#) (667 ページ)

## パッチ管理条件の設定

次の表に、[パッチ管理条件 (Patch Management Conditions)] ページのフィールドを示します。ナビゲーションパスは、[ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [条件 (Conditions)] > [ポスチャ (Posture)] > [パッチ管理条件 (Patch Management Conditions)] です。

表 134: パッチ管理条件

| フィールド                            | 使用上のガイドライン                                                                                                                                                                           |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [名前 (Name)]                      | パッチ管理条件の名前を入力します。                                                                                                                                                                    |
| 説明                               | パッチ管理条件の説明を入力します。                                                                                                                                                                    |
| オペレーティング システム (Operating System) | オペレーティング システムを選択して、エンドポイント上のパッチ管理ソフトウェアのインストールをチェックするか、または条件が適用される最新のパッチ管理定義ファイルの更新をチェックします。Windows OS または Mac OSX を選択できます。また、パッチ管理条件を作成する複数のオペレーティング システムのバージョンを選択することもできます。        |
| ベンダー名 (Vendor Name)              | ドロップダウン リストからベンダー名を選択します。ベンダーのパッチ管理製品とそれらのサポート対象バージョン、チェックタイプ、および最小対応モジュールのサポートが取得され、[選択したベンダーの製品 (Products for Selected Vendor)] テーブルに表示されます。テーブル内のリストは、選択したオペレーティング システムによって変わります。 |

| フィールド                 | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| チェック タイプ (Check Type) | <p>次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• [インストール (Installation)] : 選択した製品がエンドポイントにインストールされているかどうかを確認します。 このチェック タイプは、すべてのベンダーでサポートされています。</li> <li>• [有効 (Enabled)] : 選択した製品がエンドポイントでイネーブルかどうかを確認します。 ベンダーの製品が選択したチェック タイプをサポートしているかどうかを[選択したベンダーの製品 (Products for Selected Vendor)] リストを参照することで確認します。</li> <li>• [最新 (Up to Date)] : 選択した製品に欠けているパッチがないかどうかを確認します。 ベンダーの製品が選択したチェック タイプをサポートしているかどうかを[選択したベンダーの製品 (Products for Selected Vendor)] リストを参照することで確認します。</li> </ul> <p>[ベンダー名 (Vendor Name)] で指定したベンダーがサポートする製品のリストを表示するには、[選択したベンダーの製品 (Products for Selected Vendor)] ドロップダウン矢印をクリックします。たとえば、製品 1 と 製品 2 の 2 つの製品を持つベンダー A を選択したとします。製品 1 は [有効 (Enabled)] オプションをサポートしているが、製品 2 はサポートしていない場合があります。または、製品 1 がチェック タイプのいずれもサポートしていない場合は、グレー表示されます。</p> |

#### 関連トピック

- [ソフトウェア パッチのインストール \(102 ページ\)](#)
- [ソフトウェア パッチのロールバック \(104 ページ\)](#)
- [パッチのインストールおよびロールバックの変更の表示](#)
- [パッチ管理条件の作成 \(668 ページ\)](#)

## ディスク暗号化条件の設定

次の表では、[ディスク暗号化条件（Disk Encryption Condition）] ページのフィールドについて説明します。ナビゲーションパスは、[ポリシー（Policy）]>[ポリシー要素（Policy Elements）]>[条件（Conditions）]>[ポスチャ（Posture）]>[ディスク暗号化条件（Disk Encryption Condition）] です。

表 135: ディスク暗号化条件の設定

| フィールド                           | 使用上のガイドライン                                                                                                                                                                              |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [名前（Name）]                      | 作成するディスク暗号化条件の名前を入力します。                                                                                                                                                                 |
| 説明                              | ディスク暗号化条件の説明を入力します。                                                                                                                                                                     |
| オペレーティング システム（Operating System） | ディスクを暗号化のためにチェックするエンドポイントのオペレーティング システムを選択します。Windows OS または Mac OSX を選択できます。また、ディスク暗号化条件を作成するための複数のバージョンのオペレーティング システムを選択することもできます。                                                    |
| ベンダー名（Vendor Name）              | ドロップダウン リストからベンダー名を選択します。ベンダーのデータ暗号化製品およびそれらのサポート対象バージョン、暗号化状態チェック、および最小対応モジュールサポートが取得され、[選択したベンダーの製品（Products for Selected Vendor）] テーブルに表示されます。テーブル内のリストは、選択したオペレーティング システムによって変わります。 |

| フィールド                    | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 参照先                      | <p>オプションが [選択したベンダーの製品 (Products for Selected Vendor) ] セクションでオンになっている場合にのみ有効です。次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• [特定のロケーション (Specific Location) ] : 指定したディスク ドライブがエンドポイントで暗号化されているか (たとえば Windows OS の場合は C:) 、または指定したボリューム ラベルが暗号化されているか (たとえば、Mac OSX の場合は Mackintosh HD) を確認します。</li> <li>• [システムロケーション (System Location) ] : デフォルトの Windows OS のシステム ドライブまたは Mac OSX のハード ドライブがエンドポイントで暗号化されているかを確認します。</li> </ul>                                                        |
| 暗号化状態 (Encryption State) | <p>[暗号化状態 (Encryption State) ] チェックボックスは、選択した製品が暗号化状態チェックをサポートしていない場合はディセーブルになっています。リピータは、チェックボックスがオンになっている場合のみ表示されます。[完全に暗号化済み (Fully Encrypted) ] オプションを選択して、クライアントのディスクドライブが完全に暗号化されているかどうかを確認できます。</p> <p>たとえば TrendMicro に対し条件を作成し、2 つのベンダー (一方のベンダーの [暗号化状態 (Encryption State) ] は「はい (Yes) 」でもう一方の [暗号化状態 (Encryption State) ] は「いいえ (No) 」) を選択した場合、ベンダーの暗号化状態の一方が「いいえ (No) 」になっているので [暗号化状態 (Encryption State) ] はディセーブルになります。</p> <p>(注) リピータをクリックすることで追加のロケーションを追加でき、各ロケーション間の関係は論理 AND 演算子です。</p> |

## 関連トピック

[ディスク暗号化条件の作成 \(669 ページ\)](#)

## USB 条件の設定

次の表では、[USB 条件 (USB Condition)] ページのフィールドについて説明します。ナビゲーションパスは、[ワーク センター (Work Centers)] > [ポスチャ (Posture)] > [ポリシー要素 (Policy Elements)] > [USB] です。また、[ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [条件 (Conditions)] > [ポスチャ (Posture)] > [USB 条件 (USB Condition)] ページに移動することもできます。

USB チェックは事前定義された条件で、Windows OS のみをサポートしています。

表 136: USB 条件の設定

| フィールド                            | 使用上のガイドライン                                        |
|----------------------------------|---------------------------------------------------|
| [名前 (Name)]                      | USB_Check                                         |
| 説明                               | シスコの事前定義チェック                                      |
| オペレーティング システム (Operating System) | Windows                                           |
| コンプライアンス モジュール                   | バージョン 4.x 以降向けの、ISE のポスチャ 準拠モジュールの表示専用フィールドのサポート。 |

### 関連トピック

[単純ポスチャ条件](#) (664 ページ)

## 時刻と日付の条件の設定

次の表では、[時刻と日付の条件 (Time and Date Conditions)] ページのフィールドについて説明します。このページへのナビゲーションパスは、[ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [条件 (Conditions)] > [共通 (Common)] > [時刻と日付 (Time and Date)] です。

表 137: 時刻と日付の条件の設定

| フィールド                    | 使用上のガイドライン                       |
|--------------------------|----------------------------------|
| 条件名 (Condition Name)     | 時刻と日付の条件の名前を入力します。               |
| 説明                       | 時刻と日付の条件の説明を入力します。               |
| 標準設定 (Standard Settings) |                                  |
| 終日 (All Day)             | (デフォルト) 全日用に設定します。               |
| 特定の時間 (Specific Hours)   | 時間、分、および AM/PM を設定して、時間範囲を設定します。 |

| フィールド                              | 使用上のガイドライン                                                                                                                                                                                                                                     |
|------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 毎日 (Every Day)                     | (デフォルト) 毎日用に設定します。                                                                                                                                                                                                                             |
| 特定の曜日 (Specific Days)              | 1 つ以上の特定の曜日を設定します。                                                                                                                                                                                                                             |
| 開始日と終了日なし (No Start and End Dates) | (デフォルト) 開始または終了日なしで設定します。                                                                                                                                                                                                                      |
| 特定の日付範囲 (Specific Date Range)      | 月、日、および年を設定して日付範囲を設定します。                                                                                                                                                                                                                       |
| 特定の日付 (Specific Date)              | 特定の月、日、年を設定します。                                                                                                                                                                                                                                |
| 例外                                 |                                                                                                                                                                                                                                                |
| 時間範囲 (Time Range)                  | 時間、分、および AM/PM を設定して、時間範囲を設定します。                                                                                                                                                                                                               |
| 曜日 (Week Days)                     | 1 つ以上の特定の曜日を設定します。                                                                                                                                                                                                                             |
| 日付の範囲 (Date Range)                 | 次の 2 つのいずれかのオプションを選択します。 <ul style="list-style-type: none"> <li>• [特定の日付範囲 (Specific Date Range)] : 月、日、および年で特定の日付範囲を設定するために使用できるドロップダウンリストが提供されます。</li> <li>• [特定の日付 (Specific Date)] : 特定の月、日、および年を設定するために使用できるドロップダウンリストが提供されます。</li> </ul> |

#### 関連トピック

[時刻と日付の条件](#) (730 ページ)

[時刻と日付の条件の作成](#) (672 ページ)

## 結果

ここでは、Cisco ISE サービスの要件について説明します。

## 許可されるプロトコル

次の表に、認証中に使用するプロトコルを設定できるようにする [許可されているプロトコル (Allowed Protocols)] ページのフィールドを示します。このページへのナビゲーションパス

は、[ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] > [認証 (Authentication)] > [許可されるプロトコル (Allowed Protocols)] です。

次の表で、PAC は Protected Access Credentials を意味します。

表 138: 許可されるプロトコル

| フィールド                                                                     | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [許可されているプロトコル (Allowed Protocols)] > [認証バイパス (Authentication Bypass)]     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| ホスト ルックアップの処理 (Process Host Lookup)                                       | <p>Cisco ISE がホスト ルックアップ要求を処理できるようにするには、このチェックボックスをオンにします。ホスト ルックアップ要求は、RADIUS Service-Type が 10 (Call-Check) に等しく、ユーザ名が Calling-Station-ID に等しい場合は PAP/CHAP プロトコルに対して処理されます。ホスト ルックアップ要求は、Service-Type が 1 (Framed) に等しく、ユーザ名が Calling-Station-ID に等しい場合は EAP-MD5 プロトコルに対して処理されます。Cisco ISE でホスト ルックアップ要求を無視し、認証にシステム ユーザ名属性の元の値を使用するには、このチェックボックスをオフにします。オフにすると、メッセージ処理はプロトコル (たとえば PAP) に従って行われます。</p> <p>(注) [ホスト ルックアップの処理 (Process Host Lookup)] ボックスをオフにすると、既存の MAB 認証が失敗する可能性があります。</p> |
| [許可されているプロトコル (Allowed Protocols)] > [認証プロトコル (Authentication Protocols)] |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| PAP/ASCII を許可 (Allow PAP/ASCII)                                           | このオプションによって、PAP/ASCII が有効になります。PAP は、平文パスワード (つまり暗号化されていないパスワード) を使用する最も安全性の低い認証プロトコルです。                                                                                                                                                                                                                                                                                                                                                                                                        |
| CHAP を許可 (Allow CHAP)                                                     | このオプションによって、CHAP 認証が有効になります。CHAP は、パスワードの暗号化とともにチャレンジ/レスポンス方式を使用します。CHAP は、Microsoft Active Directory では使用できません。                                                                                                                                                                                                                                                                                                                                                                                |
| MS-CHAPv1 を許可 (Allow MS-CHAPv1)                                           | MS-CHAPv1 を有効にするには、このチェックボックスをオンにします。                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

| フィールド                           | 使用上のガイドライン                                           |
|---------------------------------|------------------------------------------------------|
| MS-CHAPv2 を許可 (Allow MS-CHAPv2) | MS-CHAPv2を有効にするには、このチェックボックスをオンにします。                 |
| EAP-MD5 を許可 (Allow EAP-MD5)     | EAP ベースの MD5 パスワード ハッシュ認証を有効にするには、このチェックボックスをオンにします。 |



| フィールド                       | 使用上のガイドライン |
|-----------------------------|------------|
| EAP-TLS を許可 (Allow EAP-TLS) |            |

| フィールド | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       | <p>EAP-TLS 認証プロトコルを有効にする場合、およびEAP-TLS 設定値を設定する場合は、このチェックボックスをオンにします。エンドユーザクライアントからの EAP Identity 応答で提示されたユーザ ID を Cisco ISE が確認する方法を指定できます。ユーザ ID は、エンドユーザクライアントによって提示された証明書の情報に照らして確認されます。この比較は、Cisco ISE とエンドユーザクライアントとの間に EAP-TLS トンネルが確立された後に行われます。</p> <p>(注) EAP-TLS は、証明書ベースの認証プロトコルです。EAP-TLS 認証が行われるのは、証明書の設定に必要な手順を完了した場合に限られます。</p> <ul style="list-style-type: none"> <li>• [期限切れ証明書の認証を許可して、許可ポリシーの証明書の更新を許可する (Allow authentication of expired certificates to allow certificate renewal in Authorization Policy) ] : ユーザが証明書を更新できるようにする場合は、このチェックボックスをオンにします。このチェックボックスをオンにすると、要求をさらに処理する前に証明書が更新されたかどうかをチェックするように適切な許可ポリシールールを設定します。</li> <li>• [ステートレスセッション再開を有効にする (Enable Stateless Session Resume) ] : セッション状態をサーバに保存する必要なしで EAP-TLS セッションを再開できるようにするには、このチェックボックスをオンにします。Cisco ISE では RFC 5077 で記述されているセッションチケット拡張もサポートされます。Cisco ISE はチケットを作成して EAP-TLS クライアントにそのチケットを送信します。クライアントはセッションを再開するためにそのチケットを ISE に提示します。</li> <li>• [プロアクティブセッションチケット更新 (Proactive Session Ticket update) ] : セッションチケットが更新される前に経過す</li> </ul> |

| フィールド                | 使用上のガイドライン                                                                                                                                                                                                                                                                                  |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                      | <p>る必要がある存続可能時間（TTL）の量を示すパーセント値を入力します。たとえば、値に 60 を入力すると、セッションチケットは TTL の 60 パーセントが経過した後で更新されます。</p> <ul style="list-style-type: none"><li>• [セッションチケットの存続時間（Session ticket Time to Live）]：セッションチケットが期限切れになるまでの時間を入力します。この値は、セッションチケットがアクティブである期間を決定します。この値は秒、分、時、日数、または週数で入力できます。</li></ul> |
| LEAP を許可（Allow LEAP） | Lightweight Extensible Authentication Protocol（LEAP）認証を有効にするには、このチェックボックスをオンにします。                                                                                                                                                                                                           |

| フィールド                 | 使用上のガイドライン |
|-----------------------|------------|
| PEAP を許可 (Allow PEAP) |            |

| フィールド | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       | <p>PEAP 認証プロトコルおよび PEAP 設定値を有効にする場合は、このチェックボックスをオンにします。デフォルトの内部方式は、MS-CHAPv2 です。</p> <p>[PEAP を許可 (Allow PEAP)] チェックボックスをオンにすると、次の PEAP 内部方式を設定できます。</p> <ul style="list-style-type: none"> <li>• [EAP-MS-CHAPv2 を許可 (Allow EAP-MS-CHAPv2)] : 内部方式として EAP-MS-CHAPv2 を使用する場合は、このチェックボックスをオンにします。</li> <li>• [パスワード変更の許可 (Allow Password Change)] : Cisco ISE でパスワード変更をサポートする場合は、このチェックボックスをオンにします。</li> <li>• [再試行 (Retry Attempts)] : Cisco ISE でログイン失敗を返す前にユーザ クレデンシャルを要求する回数を指定します。有効な値は 0 ～ 3 です。</li> <li>• [EAP-GTC を許可 (Allow EAP-GTC)] : 内部方式として EAP-GTC を使用する場合は、このチェックボックスをオンにします。</li> <li>• [パスワード変更の許可 (Allow Password Change)] : Cisco ISE でパスワード変更をサポートする場合は、このチェックボックスをオンにします。</li> <li>• [再試行 (Retry Attempts)] : Cisco ISE でログイン失敗を返す前にユーザ クレデンシャルを要求する回数を指定します。有効な値は 0 ～ 3 です。</li> <li>• [EAP-TLS を許可 (Allow EAP-TLS)] : 内部方式として EAP-TLS を使用する場合は、このチェックボックスをオンにします。</li> </ul> <p>ユーザによる証明書の更新を許可する場</p> |

| フィールド | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       | <p>合は、[期限切れ証明書の認証を許可して、許可ポリシーの証明書の更新を許可する (Allow authentication of expired certificates to allow certificate renewal in Authorization Policy) ] チェックボックスをオンにします。このチェックボックスをオンにすると、要求をさらに処理する前に証明書が更新されたかどうかをチェックするように適切な許可ポリシー ルールを設定します。</p> <ul style="list-style-type: none"><li>• [暗号化バインド TLV を要求 (Require cryptobinding TLV) ] : EAP ピアと EAP サーバの両方が PEAP 認証の内部および外部 EAP 認証に参加する場合、このチェック ボックスをオンにします。</li><li>• [レガシー クライアントにのみ PEAPv0 を許可 (Allow PEAPv0 only for legacy clients) ] : PEAP サプリカントが PEAPv0 を使用してネゴシエーションできるようにするには、このチェックボックスをオンにします。一部のレガシー クライアントは PEAPv1 プロトコル規格に準拠しません。そのような PEAP カンパセーションがドロップされないようにするには、このチェックボックスをオンにします。</li></ul> |

| フィールド                         | 使用上のガイドライン |
|-------------------------------|------------|
| EAP-FAST を許可 (Allow EAP-FAST) |            |

| フィールド | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       | <p>EAP-FAST 認証プロトコルおよび EAP-FAST 設定を有効にする場合は、このチェックボックスをオンにします。EAP-FAST プロトコルは、同じサーバ上の複数の内部プロトコルをサポートできます。デフォルトの内部方式は、MS-CHAPv2 です。</p> <p>[EAP-FAST を許可 (Allow EAP-FAST)] チェックボックスをオンにすると、EAP-FAST を内部方式として設定できます。</p> <ul style="list-style-type: none"> <li>• EAP-MS-CHAPv2 を許可 (Allow EAP-MS-CHAPv2) <ul style="list-style-type: none"> <li>• [パスワード変更の許可 (Allow Password Change)] : Cisco ISE でパスワード変更をサポートする場合は、このチェックボックスをオンにします。</li> <li>• [再試行 (Retry Attempts)] : Cisco ISE でログイン失敗を返す前にユーザ クレデンシャルを要求する回数を指定します。有効な値は 0 ～ 3 です。</li> </ul> </li> <li>• EAP-GTC を許可 (Allow EAP-GTC) <p>[パスワード変更の許可 (Allow Password Change)] : Cisco ISE でパスワード変更をサポートする場合は、このチェックボックスをオンにします。</p> <p>[再試行 (Retry Attempts)] : Cisco ISE でログイン失敗を返す前にユーザ クレデンシャルを要求する回数を指定します。有効な値は 0 ～ 3 です。</p> </li> <li>• [PAC の使用 (Use PACs)] : EAP-FAST クライアントに認可 PAC をプロビジョニングするように Cisco ISE を設定する場合にこのオプションを選択します。追加の PAC オプションが表示されます。</li> <li>• [PAC を使用しない (Don't use PACs)] : トンネルまたはマシン PAC を発行したり受け入れたりしないで EAP-FAST を使用するように Cisco ISE を設定する場合にこ</li> </ul> |



| フィールド | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       | <p>のオプションを選択します。PAC のすべての要求は無視され、Cisco ISE は PAC を含まない Success-TLV で応答します。</p> <p>このオプションを選択すると、マシン認証を実行するように Cisco ISE を設定できます。</p> <ul style="list-style-type: none"><li>• [EAP-TLS を許可 (Allow EAP-TLS)] : 内部方式として EAP-TLS を使用する場合は、このチェックボックスをオンにします。</li></ul> <p>ユーザによる証明書の更新を許可する場合は、[期限切れ証明書の認証を許可して、許可ポリシーの証明書の更新を許可する (Allow authentication of expired certificates to allow certificate renewal in Authorization Policy)] チェックボックスをオンにします。このチェックボックスをオンにすると、要求をさらに処理する前に証明書が更新されたかどうかをチェックするように適切な許可ポリシー ルールを設定します。</p> |

| フィールド | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       | <ul style="list-style-type: none"> <li>• [EAP チェーンを有効化 (Enable EAP Chaining) ] : EAP チェーンを有効にするには、このチェックボックスをオンにします。</li> </ul> <p>EAP チェーンによって、Cisco ISE はユーザ認証とマシン認証の結果を関連付け、EAPChainingResult 属性を使用して適切な許可ポリシーを適用することができます。</p> <p>EAP チェーンには、クライアントデバイスで EAP チェーンをサポートするサブリカントが必要です。Cisco ISE は、AnyConnect 4.0 をサポートします。サブリカントで[ユーザ認証およびマシン認証 (User and Machine Authentication) ] オプションを選択します。</p> <p>EAP チェーンは、EAP-FAST プロトコル (PAC ベースモードおよび PAC レスモードの両方) を選択するときに使用できます。</p> <p>PAC ベースの認証では、ユーザ認可 PAC またはマシン認可 PAC のいずれかを使用するか、両方を使用して内部方式をスキップすることができます。</p> <p>証明書ベースの認証では、(許可されるプロトコルサービスの) EAP-FAST プロトコルに対して[プロビジョニングの受信クライアント証明書 (Accept Client Certificate for Provisioning) ] オプションが有効な場合、およびエンドポイント (AnyConnect) がトンネル内のユーザ証明書を送信するように設定されている場合、トンネルの確立中に、ISE が証明書を使用してユーザを認証し (内部方式はスキップされます)、マシン認証は内部方式によって実行されます。これらのオプションが設定されていない場合、EAP-TLS が内部方式としてユーザ認証に使用されます。</p> <p>EAP チェーンを有効にした後、許可ポリシーを更新し、NetworkAccess:EapChainingResult 属性を使</p> |

| フィールド | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                            |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       | <p>用して条件を追加し、適切な権限を割り当てます。次に例を示します。</p> <ul style="list-style-type: none"><li>• EapChainingResult = ユーザとマシンの両方が成功：フルアクセス</li><li>• EapChainingResult = ユーザは成功、マシンは失敗：アクセス制限</li><li>• EapChainingResult = ユーザは失敗、マシンは成功：アクセス制限</li><li>• EapChainingResult = ユーザとマシンの両方が失敗：認証の失敗。Cisco ISE は許可ポリシーを処理せず、アクセス拒否メッセージを送信しません。</li></ul> |

| フィールド                       | 使用上のガイドライン |
|-----------------------------|------------|
| EAP-TTLSを許可（Allow EAP-TTLS） |            |

| フィールド | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       | <p>EAP-TTLS プロトコルを有効にする場合に、このチェックボックスをオンにします。</p> <p>次の内部方式を設定できます。</p> <ul style="list-style-type: none"> <li>• [PAP/ASCIIを許可 (Allow PAP/ASCII)] : 内部方式として PAP/ASCII を使用する場合は、このチェックボックスをオンにします。EAP-TTLS PAP は、トークンおよび OTP ベースの認証で使用できます。</li> <li>• [CHAPを許可 (Allow CHAP)] : 内部方式として CHAP を使用する場合は、このチェックボックスをオンにします。CHAP は、パスワードの暗号化とともにチャレンジ/レスポンス方式を使用します。CHAP は、Microsoft Active Directory では使用できません。</li> <li>• [MS-CHAPv1を許可 (Allow MS-CHAPv1)] : 内部方式として MS-CHAPv1 を使用する場合は、このチェックボックスをオンにします。</li> <li>• [MS-CHAPv2を許可 (Allow MS-CHAPv2)] : 内部方式として MS-CHAPv2 を使用する場合は、このチェックボックスをオンにします。</li> <li>• [EAP-MD5を許可 (Allow EAP-MD5)] : 内部方式として EAP-MD5 を使用する場合は、このチェックボックスをオンにします。</li> <li>• [EAP-MS-CHAPv2 を許可 (Allow EAP-MS-CHAPv2)] : 内部方式として EAP-MS-CHAPv2 を使用する場合は、このチェックボックスをオンにします。 <ul style="list-style-type: none"> <li>• [パスワード変更の許可 (Allow Password Change)] : Cisco ISE でパスワード変更をサポートする場合は、このチェックボックスをオンにします。</li> <li>• [再試行 (Retry Attempts)] : Cisco ISE でログイン失敗を返す前にユーザクレデンシアルを要求する回数を指定</li> </ul> </li> </ul> |

| フィールド                                      | 使用上のガイドライン                                                                                                                                                                                                                                                                       |
|--------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                            | します。有効な値は 0 ～ 3 です。                                                                                                                                                                                                                                                              |
| 優先 EAP プロトコル (Preferred EAP protocol)      | EAP-FAST、PEAP、LEAP、EAP-TLS、EAP-TTLS、および EAP-MD5 から任意の優先 EAP プロトコルを選択するには、このチェックボックスをオンにします。優先プロトコルを指定しない場合、EAP-TLS がデフォルトで使用されます。                                                                                                                                                |
| EAP-TLS L ビット (EAP-TLS L-bit)              | デフォルトで、ISE からの TLS Change Cipher Spec メッセージと暗号化ハンドシェイクメッセージの L ビット フラグ（長さの含まれるフラグ）を予測するレガシー EAP サプリカントをサポートするには、このチェックボックスをオンにします。                                                                                                                                               |
| EAP の脆弱な暗号の許可 (Allow Weak Ciphers for EAP) | <p>このオプションを有効にすると、レガシー クライアントが脆弱な暗号（RSA_RC4_128_SHA、RSA_RC4_128_MD5 など）を使用してネゴシエートすることができます。レガシー クライアントが脆弱な暗号化だけをサポートしている場合に限り、このオプションを有効にすることを推奨します。</p> <p>このオプションはデフォルトでは無効になっています。</p> <p>（注） Cisco ISE は、EDH_RSA_DES_64_CBC_SHA および EDH_DSS_DES_64_CBC_SHA をサポートしていません。</p> |

| フィールド                                                                                     | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                              |
|-------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| すべての RADIUS 要求にメッセージオーセンティケーターが必要 (Require Message Authenticator for all RADIUS Requests) | <p>このオプションを有効にすると、Cisco ISE は、RADIUS メッセージ オーセンティケーター属性が RADIUS メッセージがあるかどうかを検証します。メッセージオーセンティケーター属性がない場合、RADIUS メッセージは破棄されます。</p> <p>このオプションを有効にすると、スプーフィングされたアクセス要求メッセージおよび RADIUS メッセージの改ざんに対する保護が提供されます。</p> <p>RADIUS メッセージ オーセンティケーター属性は、RADIUS メッセージ全体の Message Digest 5 (MD5) ハッシュです。</p> <p>(注) EAP はメッセージオーセンティケーター属性をデフォルトで使用するの<br/>で、これを有効にする必要はありません。</p> |

#### 関連トピック

[TACACS+ デバイス管理を許可された FIPS および非 FIPS モードのプロトコル](#) (236 ページ)

[ネットワーク アクセスの許可されるプロトコルの定義](#) (691 ページ)

## PAC オプション

次の表では、[許可されるプロトコル サービス リスト (Allowed Protocols Services List)] ページで [PAC を使用 (Use PAC)] を選択した後のフィールドについて説明します。このページへのナビゲーションパスは、[ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] > [認証 (Authentication)] > [許可されるプロトコル (Allowed Protocols)] です。

表 139: PAC オプション

| フィールド             | 使用上のガイドライン |
|-------------------|------------|
| PAC を使用 (Use PAC) |            |



| フィールド | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       | <ul style="list-style-type: none"> <li>• [トンネル PAC の存続可能時間 (Tunnel PAC Time To Live) ] : 存続可能時間 (TTL) の値によって PAC のライフタイムが制限されます。ライフタイム値と単位を指定します。デフォルトは 90 日です。範囲は 1 ~ 1825 日です。</li> <li>• [プロアクティブ PAC 更新の条件 : &lt;n%&gt; の PAC TTL が残っている場合 (Proactive PAC Update When: &lt;n%&gt; of PAC TTL is Left) ] : Update 値により、クライアントに有効な PAC が保持されます。Cisco ISE は、最初に認証が成功してから TTL によって設定された有効期限までに更新を開始します。update 値は、TTL の残り時間のパーセンテージです。デフォルトは 90% です。</li> <li>• [匿名インバンド PAC プロビジョニングを許可 (Allow Anonymous In-band PAC Provisioning) ] : Cisco ISE でクライアントとのセキュアな匿名 TLS ハンドシェイクを確立し、クライアントに PAC をプロビジョニングする場合にこのチェックボックスをオンにします。その際、EAP-FAST のフェーズ 0 と EAP-MSCHAPv2 が使用されます。匿名 PAC プロビジョニングを有効にするには、内部方式として EAP-MSCHAPv2 と EAP-GTC の両方を選択する必要があります。</li> <li>• [認証付きインバンド PAC プロビジョニングを許可 (Allow Authenticated In-band PAC Provisioning) ] : Cisco ISE は SSL サーバ側の認証を使用して、EAP-FAST のフェーズ 0 中にクライアントに PAC をプロビジョニングします。このオプションは匿名プロビジョニングよりもセキュアですが、サーバ証明書および信頼できるルート CA が Cisco ISE にインストールされている必要があります。<br/><br/>このオプションをオンにすると、認証された PAC プロビジョニングの成功後に Access-Accept メッセージをクライアント</li> </ul> |

| フィールド | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       | <p>に返すように Cisco ISE を設定できます。</p> <ul style="list-style-type: none"> <li>• [認証されたプロビジョニングの後にサーバから Access-Accept を返す (Server Returns Access Accept After Authenticated Provisioning)] : 認証された PAC プロビジョニングの後に Cisco ISE から access-accept パッケージを返す場合にこのチェックボックスをオンにします。</li> <li>• [マシン認証を許可 (Allow Machine Authentication)] : Cisco ISE でエンドユーザ クライアントにマシン PAC をプロビジョニングし、(マシン クレデンシャルを持たないエンドユーザ クライアントに対して) マシン認証を実行する場合にこのチェックボックスをオンにします。マシン PAC は、要求 (インバンド) によって、または管理者 (アウトオブバンド) によって、クライアントにプロビジョニングできます。Cisco ISE がエンドユーザ クライアントから有効なマシン PAC を受信すると、その PAC からマシン ID の詳細が抽出され、Cisco ISE 外部 ID ソースで確認されます。マシン認証の外部 ID ソースとして Cisco ISE によってサポートされるのは、Active Directory だけです。その詳細が正しいことが確認されると、その後の認証は実行されません。</li> </ul> <p>このオプションをオンにすると、マシン PAC を使用するために受け入れることができる期間の値を入力できます。Cisco ISE は、期限切れのマシン PAC を受け取ると、(エンドユーザ クライアントからの新規マシン PAC 要求を待たずに) エンドユーザ クライアントに新規マシン PAC を自動的に再プロビジョニングします。</p> |

| フィールド | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       | <ul style="list-style-type: none"> <li>• [ステートレスセッション再開の有効化 (Enable Stateless Session Resume)] : Cisco ISE で EAP-FAST クライアントに認可 PAC をプロビジョニングし、EAP-FAST のフェーズ 2 をスキップする場合にこのチェックボックスをオンにします (デフォルトはオン)。</li> </ul> <p>このチェックボックスは次の場合にオフにします。</p> <ul style="list-style-type: none"> <li>• Cisco ISE が EAP-FAST クライアントに認可 PAC をプロビジョニングしないようにする場合</li> <li>• EAP-FAST のフェーズ 2 を常に実行する場合</li> </ul> <p>このオプションをオンにすると、ユーザ認可 PAC の認可期間を入力できます。この期間の終了後、PAC は期限切れになります。Cisco ISE は期限切れの認可 PAC を受信すると、EAP-FAST 認証のフェーズ 2 を実行します。</p> |

#### 関連トピック

[OOB TrustSec PAC \(980 ページ\)](#)

[EAP-FAST の PAC の生成 \(687 ページ\)](#)

## 許可プロファイルの設定

次の表に、[標準許可プロファイル (Standard Authorization Profiles)] ページのフィールドを示します。このページへのナビゲーションパスは、[ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] > [許可 (Authorization)] > [許可プロファイル (Authorization Profiles)] です。

表 140: 許可プロファイルの設定

| フィールド       | 使用上のガイドライン                |
|-------------|---------------------------|
| [名前 (Name)] | 新しい許可プロファイルを識別する名前を入力します。 |
| 説明          | 許可プロファイルの説明を入力します。        |

| フィールド                          | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                               |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| アクセス タイプ (Access Type)         | アクセス タイプ オプション<br>([ACCESS_ACCEPT] または<br>[ACCESS_REJECT]) を選択します。                                                                                                                                                                                                                                                                       |
| サービス テンプレート (Service Template) | Cisco ISE で SAnet 対応デバイスから接続しているセッションをサポートできるようにする場合にこのチェックボックスをオンにします。<br>ISE は、サービス テンプレートを、「サービス テンプレート」 互換としてマークする特別なフラグを含む許可プロファイルとして実行します。このようにすると、認可プロファイルでもあるサービス テンプレートを 1 つのポリシーで使用して、SAnet および非 SAnet デバイスとの接続をサポートできます。                                                                                                      |
| 一般的なタスク                        |                                                                                                                                                                                                                                                                                                                                          |
| DACL 名 (DACL Name)             | デフォルト値 (PERMIT_ALL_TRAFFIC または DENY_ALL_TRAFFIC) を使用するか、次のディクショナリから属性を選択することができます。 <ul style="list-style-type: none"> <li>外部 ID ストア (属性) (External identity store (attributes))</li> <li>エンドポイント</li> <li>内部ユーザ</li> <li>内部エンドポイント</li> </ul>                                                                                            |
| VLAN                           | チェックボックスをオンにし、作成している新しい許可プロファイルに関連付ける仮想 LAN (VLAN) ID を識別する属性値を入力します (VLAN ID には整数値と文字列値の両方がサポートされます)。このエントリの形式は、Tunnel-Private-Group-ID:VLANnumber です。<br><br>(注) VLAN ID を選択しないと、Cisco ISE は、デフォルト値である VLAN ID = 1 を使用します。たとえば、VLAN 番号として 123 とのみ入力した場合、[属性詳細 (Attributes Details)] ペインは次の値を反映します。<br>Tunnel-Private-Group-ID = 1:123。 |

| フィールド                                        | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 音声ドメイン権限 (Voice Domain Permission)           | チェックボックスをオンにして「cisco-av-pair」のベンダー固有属性 (VSA) を有効にし、「device-traffic-class=voice」の値と関連付けます。複数ドメインの許可モードでは、ネットワークスイッチがこの VSA を受信した場合、エンドポイントは、許可後に音声ドメインに配置されます。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| ポスチャ検出 (Posture Discovery)                   | チェックボックスをオンにして Cisco ISE のポスチャ検出に使用されるリダイレクションプロセスを有効にし、この許可プロファイルに関連付けるデバイスの ACL を入力します。たとえば、入力した値が acl119 の場合、これは [属性詳細 (Attributes Details)] ペインで <code>cisco-av-pair = url-redirect-acl = acl119</code> として反映されます。[属性詳細 (Attributes Details)] ペインには、 <code>cisco-av-pair = url-redirect=https://ip:8443/guestportal/gateway?sessionId=SessionValueIdValue&amp;action=cpp</code> とも表示されます。                                                                                                                                                                                                                                                                      |
| 中央集中 Web 認証 (Centralized Web Authentication) | <p>チェックボックスをオンにして、ポスチャ検出と似ているがゲスト ユーザのアクセス要求を Cisco ISE のゲストサーバにリダイレクトするリダイレクションプロセスを有効にします。この許可プロファイルに関連付けるデバイスの ACL を入力し、redirect オプションとして [デフォルト (Default)] または [手動 (Manual)] を選択します。たとえば、入力した値が acl-999 の場合、これは [属性詳細 (Attributes Details)] ペインで <code>cisco-av-pair = url-redirect-acl = acl-99</code> として反映されます。[属性詳細 (Attributes Details)] ペインには、<code>cisco-av-pair = url-redirect=https://ip:8443/guestportal/gateway?sessionId=SessionValueIdValue&amp;action=cwa</code> も表示されます。</p> <p>ユーザをリダイレクトする正確な IP アドレスまたはホスト名を指定するには、[スタティック IP/ホスト名 (Static IP/Host Name)] チェックボックスをオンにします。このチェックボックスがオフの場合、ユーザはこの要求を受信したポリシー サービス ノードの FQDN にリダイレクトされます。</p> |

| フィールド                                                   | 使用上のガイドライン                                                                                                                                                                                                                                          |
|---------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Web リダイレクション (Web Redirection)<br>(CWA、DRW、MDM、NSP、CPP) |                                                                                                                                                                                                                                                     |
| Auto SmartPort                                          | チェックボックスをオンにして Auto SmartPort 機能を有効にし、対応するイベント名の値をテキストボックスに入力します。これにより、VSA cisco-av-pair が有効になり、このオプションの値が「auto-smart-port=event_name」になります。選択は [属性詳細 (Attributes Details)] ペインに反映されます。                                                             |
| フィルタ ID (Filter-ID)                                     | チェックボックスをオンにして、テキストボックスで定義した ACL 名（これには自動的に「.in」が付加されます）を送信する RADIUS フィルタ属性を有効にします。選択は [属性詳細 (Attributes Details)] ペインに反映されます。                                                                                                                      |
| 再認証 (Reauthentication)                                  | チェックボックスをオンにし、再認証中に接続を維持するために値を秒単位で入力します。[タイマー (Timer)] ドロップダウンリストから属性値を選択することもできます。デフォルト (値 0) または [RADIUS 要求 (RADIUS-Request)] (値 1) を使用することを選択して、再認証中に接続を維持することを選択します。これを [RADIUS 要求 (RADIUS-Request)] 値に設定すると、再認証プロセス中に接続が維持されます。               |
| MACSec ポリシー (MACSec Policy)                             | チェックボックスをオンにして、MACSec 対応クライアントが Cisco ISE に接続したときに必ず MACSec 暗号化ポリシーを有効にし、次の3つのオプションのいずれかを選択します。[must-secure]、[should-secure]、または [must-not-secure]。たとえば、選択肢は [属性詳細 (Attributes Details)] ペインに cisco-av-pair = linksec-policy=must-secure として反映されます。 |

| フィールド                                                      | 使用上のガイドライン                                                                                                                                                                                                                           |
|------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NEAT                                                       | チェックボックスをオンにして、ネットワーク間の ID 認識を拡張する機能であるネットワーク エッジ アクセス トポロジ (NEAT) を有効にします。このチェックボックスをオンにすると、[属性詳細 (Attributes Details)] ペインに、 <code>cisco-av-pair=device-traffic-class=switch</code> という値が表示されます。                                   |
| インターフェイステンプレート (Interface Template)                        | このチェックボックスをオンにして、認証のためにインターフェイス テンプレートを使用するテンプレート名を指定します。このオプションを選択すると、次の値が [属性詳細 (Attributes Details)] ペインに表示されます。<br><code>cisco-av-pair=interface-template-name=&lt;template_name&gt;</code>                                      |
| Web 認証 (ローカル Web 認証) (Web Authentication (Local Web Auth)) | チェックボックスをオンにしてこの許可プロファイルのローカル Web 認証を有効にします。この値では、Cisco ISE が DACL とともに VSA を送信することによって Web 認証の許可をスイッチが認識できます。VSA は <code>cisco-av-pair=priv-lvl=15</code> で、これは [属性詳細 (Attributes Details)] ペインで反映されます。                             |
| ワイヤレス LAN コントローラ (WLC) (Wireless LAN Controller (WLC))     | チェックボックスをオンにし、テキストフィールドに ACL 名を入力します。この値は、必須の [Airespace VSA] で使用され、ローカルで定義された ACL の WLC 上の接続への追加を許可します。たとえば、 <code>rsa-1188</code> と入力した場合、これは [属性詳細 (Attributes Details)] ペインに <code>Airespace-ACL-Name=rsa-1188</code> として反映されます。 |
| ASA VPN                                                    | チェックボックスをオンにして、適応型セキュリティアプライアンス (ASA) VPN グループポリシーを有効にします。[属性 (Attribute)] リストから値を選択してこの設定を行います。                                                                                                                                     |
| 高度な属性設定 (Advanced Attributes Settings)                     |                                                                                                                                                                                                                                      |
| Dictionaries                                               | 下矢印アイコンをクリックし、[ディクショナリ (Dictionaries)] ウィンドウに選択可能なオプションを表示します。目的のディクショナリおよび属性をクリックして選択し、最初のフィールドで設定します。                                                                                                                              |

| フィールド                     | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 属性値 (Attribute Values)    | <p>下矢印アイコンをクリックし、[属性値 (Attribute Values)] ウィンドウに選択可能なオプションを表示します。2 番目のフィールドに目的の属性グループおよび属性値をクリックして選択します。この値は、最初のフィールドで選択した値と一致します。設定する[高度な属性 (Advanced Attributes)] 設定が[属性詳細 (Attribute Details)] パネルに表示されます。</p> <p>(注) [属性詳細 (Attributes Details)] ペインに表示された読み取り専用値を変更または削除するには、対応する[共通タスク (Common Tasks)] フィールドまたは[高度な属性設定 (Advanced Attributes Settings)] ペインの[属性値 (Attribute Values)] テキストボックスで選択した属性でこれらの値を変更または削除する必要があります。</p> |
| 属性詳細 (Attributes Details) | <p>このペインは、[共通タスク (Common Tasks)] および[高度な属性 (Advanced Attributes)] に設定した設定済みの属性値を表示します。</p> <p>(注) [属性詳細 (Attributes Details)] ペインに表示される値は読み取り専用で、このペインでは編集または削除できません。</p>                                                                                                                                                                                                                                                              |



- (注) URL リダイレクトなしのクライアント プロビジョニングでは、ユーザが特定の VLAN にアクセスすることを制限して、制限付きアクセスを提供できます。[Web リダイレクション (Web Redirection)] チェックボックスをオフにし、[VLAN] チェックボックスをオンにして VLAN を設定する必要があります。

#### 関連トピック

[Cisco ISE の許可プロファイル \(717 ページ\)](#)

[許可プロファイルの権限 \(732 ページ\)](#)

[未登録のデバイスのリダイレクトのための許可プロファイルの設定 \(303 ページ\)](#)

[許可プロファイルの作成 \(554 ページ\)](#)



## プロファイリング例外アクションの設定

次の表では、[新規プロファイラ例外アクション（New Profiler Exception Action）] ページのフィールドについて説明します。このページへのナビゲーションパスは、[ポリシー（Policy）]>[ポリシー要素（Policy Elements）]>[結果（Results）]>[プロファイリング（Profiling）]>[例外アクション（Exception Actions）] です。

表 141: 例外アクションの作成

| フィールド                                          | 使用上のガイドライン                                                                                                                                                                                                                                                |
|------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [名前（Name）]                                     | 作成する例外アクションの名前を入力します。                                                                                                                                                                                                                                     |
| 説明                                             | 作成する例外アクションの説明を入力します。                                                                                                                                                                                                                                     |
| CoA を適用する CoA アクション（CoA Action to enforce CoA） | CoA を適用するには、[CoA アクション（CoA Action）] チェックボックスをオンにします。<br><br>エンドポイントプロファイリングポリシーで例外アクションを関連付けて CoA を適用する場合は、Cisco ISE で CoA をグローバルに設定する必要があります。これは、[管理（Administration）]>[システム（System）]>[設定（Settings）]>[プロファイリング（Profiling）] で実行できます。                       |
| ポリシー割り当て                                       | [ポリシー割り当て（Policy Assignment）] ドロップダウンリストをクリックして Cisco ISE に設定されたエンドポイントプロファイリングポリシーを表示し、例外アクションがトリガーされると一致した値に関係なくエンドポイントがプロファイリングされるプロファイリングポリシーを選択します。                                                                                                  |
| システム タイプ（System Type）                          | 例外アクションのタイプは次のいずれかになります。<br><br><ul style="list-style-type: none"> <li>• [シスコ提供（Cisco Provided）] : AuthorizationChange、EndpointDelete および FirstTimeProfile が含まれます。</li> <li>• [管理者作成（Administrator Created）] : Cisco ISE の管理者として作成されたものが含まれます。</li> </ul> |

### 関連トピック

[プロファイリング例外アクション（806 ページ）](#)

[例外アクションの作成（807 ページ）](#)

## ファイル修復

次の表では、[ファイル修復（File Remediation）] ページのフィールドについて説明します。このページのナビゲーションパスは、[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [ポスチャ（Posture）] > [修復アクション（Remediation Actions）] > [ファイル修復（File Remediation）] です。

表 142: ファイル修復

| フィールド                                   | 使用上のガイドライン                                                                                               |
|-----------------------------------------|----------------------------------------------------------------------------------------------------------|
| ファイルの修復名（File Remediation Name）         | ファイル修復の名前を入力します。作成して保存した後は、ファイル修復名を編集できません。                                                              |
| ファイル修復の説明（File Remediation Description） | ファイル修復の説明を入力します。                                                                                         |
| バージョン                                   | ファイル バージョンを入力します。                                                                                        |
| アップロードするファイル（File to upload）            | [参照（Browse）] をクリックして、Cisco ISE サーバにアップロードするファイル名を特定します。これは、ファイル修復アクションがトリガーされたときにクライアントにダウンロードされるファイルです。 |

### 関連トピック

[ファイル修復の追加](#) (952 ページ)

## ファイアウォール修復

次の表では、[ファイアウォール修復（Firewall Remediation）] ページのフィールドについて説明します。このページのナビゲーションパスは、[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [ポスチャ（Posture）] > [修復アクション（Remediation Actions）] > [ファイアウォール修復（Firewall Remediation）] です。

表 143: ファイアウォール修復

| フィールド                           | 使用上のガイドライン                     |
|---------------------------------|--------------------------------|
| [名前（Name）]                      | ファイアウォール修復の名前を入力します。           |
| 説明                              | ファイアウォール修復の説明を入力します。           |
| オペレーティング システム（Operating System） | Windows OS または Mac OSX を選択します。 |
| コンプライアンス モジュール                  | OESIS バージョン 4.x 以降のサポート。       |

| フィールド                            | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                              |
|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 修復タイプ (Remediation Type)         | <p>次のいずれかを実行します。</p> <ul style="list-style-type: none"><li>• [自動 (Automatic)] : [間隔 (Interval)] および [再試行回数 (Retry Count)] に値を入力します。ISE サーバは非準拠のクライアントを識別し、修復の通知方法を選択し、自動的にクライアントのファイアウォール アプリケーションを更新します。</li><li>• [手動 (Manual)] : ([間隔 (Interval)] および [再試行回数 (Retry Count)] フィールドは無効) 非準拠のクライアントはファイアウォール アプリケーションを手動でダウンロードし、適用する必要があります。</li></ul> |
| 間隔 (秒単位) (Interval (in seconds)) | <p>(自動修復タイプを選択した場合のみ使用可能) クライアントでスケジューリングされたパッチ更新が実行されるまでの時間間隔を秒単位で入力します。有効な範囲は 0 ～ 9999 です。</p>                                                                                                                                                                                                                                                        |
| 再試行回数 (Retry Count)              | <p>(自動修復タイプを選択した場合のみ使用可能) クライアントが重要なパッチの更新を試行できる回数を入力します。有効な範囲は 0 ～ 99 です。</p>                                                                                                                                                                                                                                                                          |
| ベンダー名 (Vendor Name)              | <p>ドロップダウンリストからベンダー名 (例: VMware Inc.) を選択します。</p> <p>(注) Cisco ISE および AnyConnect のサポート対象バージョンは次のとおりです。</p> <ul style="list-style-type: none"><li>• Cisco ISE バージョン 2.2 以降</li><li>• AnyConnect バージョン 4.4 以降</li></ul>                                                                                                                                  |

| フィールド                        | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 修復オプション (Remediation Option) | <p>[有効化 (Enable)] : エンドポイントでファイアウォールアプリケーションが無効になっている場合に、ファイアウォールアプリケーションを有効にします (ベンダーで有効化オプションがサポートされている場合)。</p> <p>[選択したベンダーの製品 (Products for Selected Vendor)] ドロップダウン矢印をクリックすると、[ベンダー名 (Vendor Name)] に指定したベンダーがサポートしている製品 (例: VMware vCentre Protect Agent)、バージョン (例: 8.x)、有効な修復サポート (例: [はい (Yes)]) のリストが表示されます。たとえば、製品 1 と製品 2 の 2 つの製品を持つベンダー A を選択したとします。製品 1 は [修復の有効化 (Enable remediation)] オプションをサポートしているが、製品 2 はサポートしていない場合があります。[選択したベンダーの製品 (Products for Selected Vendor)] テーブルは選択した修復オプションに応じて変わります。</p> |

## リンク修復

次の表では、[リンク修復 (Link Remediation)] ページのフィールドについて説明します。ナビゲーションパスは、[ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] > [ポスチャ (Posture)] > [修復アクション (Remediation Actions)] > [リンク修復 (Link Remediation)] です。

表 144: リンク修復

| フィールド                                   | 使用上のガイドライン      |
|-----------------------------------------|-----------------|
| リンク修復名 (Link Remediation Name)          | リンク修復の名前を入力します。 |
| リンク修復の説明 (Link Remediation Description) | リンク修復の説明を入力します。 |

| フィールド                            | 使用上のガイドライン                                                                                                                                                                                                                                            |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 修復タイプ (Remediation Type)         | 次のいずれかを実行します。 <ul style="list-style-type: none"> <li>• [自動 (Automatic)] : 選択されている場合、[間隔 (Interval)] および [再試行回数 (Retry Count)] の値を入力する必要があります。</li> <li>• [手動 (Manual)] : 選択されていると、[再試行回数 (Retry Count)] および [間隔 (Interval)] フィールドは編集できません。</li> </ul> |
| 再試行回数 (Retry Count)              | クライアントがリンクからの修復を試行できる回数を入力します。                                                                                                                                                                                                                        |
| 間隔 (秒単位) (Interval (in seconds)) | クライアントが前回の試行後にリンクからの修復を試行できる時間間隔を秒単位で入力します。                                                                                                                                                                                                           |
| URL                              | 修復のページまたはリソースへの有効な URL を入力します。                                                                                                                                                                                                                        |

#### 関連トピック

[リンク修復の追加](#) (952 ページ)

## アプリケーション修復

次の表では、[アプリケーション修復 (Application Remediation)] ページのフィールドについて説明します。ナビゲーションパスは、[ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] > [ポスチャ (Posture)] > [修復アクション (Remediation Actions)] > [アプリケーション修復 (Application Remediation)] です。

表 145: アプリケーション修復

| フィールド                            | 使用上のガイドライン                                        |
|----------------------------------|---------------------------------------------------|
| [名前 (Name)]                      | アプリケーション修復の名前を入力します。                              |
| 説明                               | アプリケーション修復の説明を入力します。                              |
| オペレーティング システム (Operating System) | アプリケーション修復条件が適用される Windows OS または MAC OSX を選択します。 |
| コンプライアンス モジュール                   | OESIS バージョン 4.x 以降のサポート。                          |

| フィールド                            | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                              |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 修復タイプ (Remediation Type)         | <p>次のいずれかを実行します。</p> <ul style="list-style-type: none"> <li>• [自動 (Automatic)] : [間隔 (Interval)] および [再試行回数 (Retry Count)] に値を入力します。ISE サーバは非準拠のクライアントを識別し、修復の通知方法を選択し、自動的にクライアントの最新のパッチを更新します。</li> <li>• [手動 (Manual)] : ([間隔 (Interval)] および [再試行回数 (Retry Count)] フィールドは無効) 非準拠のクライアントは最新のパッチを手動でダウンロードし、適用する必要があります。</li> </ul>                                    |
| 間隔 (秒単位) (Interval (in seconds)) | <p>(自動修復タイプを選択した場合のみ使用可能) クライアントでスケジューリングされたパッチ更新が実行されるまでの時間間隔を秒単位で入力します。有効な範囲は 0 ～ 9999 です。</p>                                                                                                                                                                                                                                                                        |
| 再試行回数 (Retry Count)              | <p>(自動修復タイプを選択した場合のみ使用可能) クライアントが重要なパッチの更新を試行できる回数を入力します。有効な範囲は 0 ～ 99 です。</p>                                                                                                                                                                                                                                                                                          |
| ベンダー名 (Vendor Name)              | <p>ドロップダウン リストからベンダー名を選択します。[選択したベンダーの製品 (Products for Selected Vendor)] テーブルに、アプリケーション名 (Internet Explorer など)、バージョン、ベンダー (Microsoft Corporation など)、実行中のプロセス、カテゴリ (フィッシング詐欺対策など) が表示されます。</p> <p>(注) Cisco ISE および AnyConnect のサポート対象バージョンは次のとおりです。</p> <ul style="list-style-type: none"> <li>• Cisco ISE バージョン 2.2 以降</li> <li>• AnyConnect バージョン 4.4 以降</li> </ul> |

| フィールド                        | 使用上のガイドライン |
|------------------------------|------------|
| 修復オプション (Remediation Option) |            |

| フィールド | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       | <p>次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• [アンインストール (Uninstall)] : アプリケーションをアンインストールします。たとえば、[コンテキスト ディレクトリ (Context Directory)] ページで、悪意のあるアプリケーションを実行している複数のエンドポイントがあることが確認されるとします。悪意のあるアプリケーションをアンインストールする要件を作成できます。</li> <li>(注) Cisco ISE 2.2 では、アプリケーション (Firefox 44.x など) がエンドポイントに存在していない場合でも、ポスチャフローが [コンプライアンス (Compliance)] に移動します。</li> <li>• [プロセス停止 (Kill Process)] : 必要な実行中のパッチ管理プロセスを停止します。たとえば、[コンテキスト ディレクトリ (Context Directory)] ページで、悪意のあるプロセスを実行している複数のエンドポイントがあることが確認されるとします。このような実行中の悪意のあるプロセスを停止する要件を作成できます。</li> </ul> <p>[パッチ管理ベンダー名 (Patch Management Vendor Name)] で指定したベンダーがサポートする製品のリストを表示するには、[選択したベンダーの製品 (Products for Selected Vendor)] ドロップダウン矢印をクリックします。たとえば、製品 1 と 製品 2 の 2 つの製品を持つベンダー A を選択したとします。製品 1 は [修復の有効化 (Enable remediation)] オプションをサポートしているが、製品 2 はサポートしていない場合があります。または、製品 1 が [有効 (Enable)] および [欠落したパッチの修復のインストール (Install missing patches remediation)] オプションをサポートしていない場合、製品 1 はディセーブル (グレー表示) になります。[選択したベンダーの製品 (Products for Selected Vendor)] テーブルは選択した修復オプションに応じて変わります。</p> |



## マルウェア対策修復

次の表に、[AV 修復 (AV Remediation)] ページのフィールドを示します。ナビゲーションパスは、[ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] > [ポスチャ (Posture)] > [修復アクション (Remediation Actions)] > [AV 修復 (AV Remediation)] です。

表 146: アンチウイルス修復

| フィールド                            | 使用上のガイドライン                                                                                                                                                                                                                                            |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [名前 (Name)]                      | マルウェア対策修復の名前を入力します。                                                                                                                                                                                                                                   |
| 説明                               | マルウェア対策修復の説明を入力します。                                                                                                                                                                                                                                   |
| オペレーティング システム (Operating System) | 次のいずれかを実行します。 <ul style="list-style-type: none"> <li>• <b>Windows</b></li> <li>• [Macintosh] : 選択されていると、[修復タイプ (Remediation Type)] フィールド、[間隔 (Interval)] フィールド、および [再試行回数 (Retry Count)] フィールドは編集できません</li> </ul>                                     |
| コンプライアンス モジュール                   | OESIS バージョン 4 はコンプライアンス モジュール 4.x および AnyConnect 4.3 以上をサポートします。                                                                                                                                                                                      |
| 修復タイプ (Remediation Type)         | 次のいずれかを実行します。 <ul style="list-style-type: none"> <li>• [自動 (Automatic)] : 選択されている場合、[間隔 (Interval)] および [再試行回数 (Retry Count)] の値を入力する必要があります。</li> <li>• [手動 (Manual)] : 選択されていると、[再試行回数 (Retry Count)] および [間隔 (Interval)] フィールドは編集できません。</li> </ul> |
| 間隔 (秒単位) (Interval (in seconds)) | クライアントが修復を試行した後で次の試行ができるようになるまでの時間間隔を秒単位で入力します。                                                                                                                                                                                                       |
| 再試行回数 (Retry Count)              | クライアントがマルウェア対策定義の更新を試行できる回数を入力します。                                                                                                                                                                                                                    |

| フィールド                                     | 使用上のガイドライン            |
|-------------------------------------------|-----------------------|
| アンチマルウェア ベンダー名 (Anti-Malware Vendor Name) | 必要なマルウェア対策ベンダーを選択します。 |

#### 関連トピック

[クライアントレス モードでのポストチャ要件の作成](#) (968 ページ)

## アンチウイルス修復

次の表では、[アンチウイルス修復 (Anti-Virus Remediation)] ページのフィールドについて説明します。ナビゲーションパスは、[ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] > [ポストチャ (Posture)] > [修復アクション (Remediation Actions)] > [アンチウイルス修復 (Anti-Virus Remediation)] です。

表 147: アンチウイルス修復

| フィールド                            | 使用上のガイドライン                                                                                                                                                                                                                                        |
|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [名前 (Name)]                      | アンチウイルス修復の名前を入力します。                                                                                                                                                                                                                               |
| 説明                               | アンチウイルス修復の説明を入力します。                                                                                                                                                                                                                               |
| 修復タイプ (Remediation Type)         | 次のいずれかを実行します。 <ul style="list-style-type: none"> <li>[自動 (Automatic)] : 選択されている場合、[間隔 (Interval)] および [再試行回数 (Retry Count)] の値を入力する必要があります。</li> <li>[手動 (Manual)] : 選択されていると、[再試行回数 (Retry Count)] および [間隔 (Interval)] フィールドは編集できません。</li> </ul> |
| 間隔 (秒単位) (Interval (in seconds)) | クライアントが修復を試行した後で次の試行ができるようになるまでの時間間隔を秒単位で入力します。                                                                                                                                                                                                   |
| 再試行回数 (Retry Count)              | クライアントがアンチウイルス定義の更新を試行できる回数を入力します。                                                                                                                                                                                                                |

| フィールド                            | 使用上のガイドライン                                                                                                                                                                                                       |
|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| オペレーティング システム (Operating System) | 次のいずれかを実行します。 <ul style="list-style-type: none"> <li>• <b>Windows</b></li> <li>• [Macintosh] : 選択されていると、[修復タイプ (Remediation Type)] フィールド、[間隔 (Interval)] フィールド、および[再試行回数 (Retry Count)] フィールドは編集できません</li> </ul> |
| AV ベンダー名 (AV Vendor Name)        | アンチウイルス ベンダーを選択します。                                                                                                                                                                                              |

#### 関連トピック

[アンチウイルス修復の追加](#) (953 ページ)

[クライアントレス モードでのポスチャ要件の作成](#) (968 ページ)

## アンチスパイウェア修復

次の表に、[AS 修復 (AS Remediation)] ページのフィールドを示します。ナビゲーションパスは、[ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] > [ポスチャ (Posture)] > [修復アクション (Remediation Actions)] > [AS 修復 (AS Remediation)] です。

表 148: アンチスパイウェア修復

| フィールド                            | 使用上のガイドライン                                                                                                                                                                                                                                          |
|----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [名前 (Name)]                      | アンチスパイウェア修復の名前を入力します。                                                                                                                                                                                                                               |
| 説明                               | アンチスパイウェア修復の説明を入力します。                                                                                                                                                                                                                               |
| 修復タイプ (Remediation Type)         | 次のいずれかを実行します。 <ul style="list-style-type: none"> <li>• [自動 (Automatic)] : 選択されている場合、[間隔 (Interval)] および[再試行回数 (Retry Count)] の値を入力する必要があります。</li> <li>• [手動 (Manual)] : 選択されていると、[再試行回数 (Retry Count)] および[間隔 (Interval)] フィールドは編集できません。</li> </ul> |
| 間隔 (秒単位) (Interval (in seconds)) | クライアントが修復を試行した後で次の試行ができるようになるまでの時間間隔を秒単位で入力します。                                                                                                                                                                                                     |

| フィールド                            | 使用上のガイドライン                                                                                                                                                                                                       |
|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 再試行回数 (Retry Count)              | クライアントがアンチスパイウェア定義の更新を試行できる試行回数を入力します。                                                                                                                                                                           |
| オペレーティング システム (Operating System) | 次のいずれかを実行します。 <ul style="list-style-type: none"> <li>• <b>Windows</b></li> <li>• [Macintosh] : 選択されていると、[修復タイプ (Remediation Type)] フィールド、[間隔 (Interval)] フィールド、および[再試行回数 (Retry Count)] フィールドは編集できません</li> </ul> |
| AS のベンダー名 (AS Vendor Name)       | アンチスパイウェア ベンダーを選択します。                                                                                                                                                                                            |

#### 関連トピック

[アンチスパイウェア修復の追加 \(954 ページ\)](#)

[クライアントレス モードでのポストチャ要件の作成 \(968 ページ\)](#)

## プログラム修復起動

次の表では、[プログラム修復起動 (Launch Program Remediation)] ページのフィールドについて説明します。ナビゲーションパスは、[ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] > [ポストチャ (Posture)] > [修復アクション (Remediation Actions)] > [プログラム修復起動 (Launch Program Remediation)] です。

表 149: プログラム修復起動

| フィールド                    | 使用上のガイドライン                                                                                                                                                                                                                                             |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [名前 (Name)]              | プログラム修復起動の名前を入力します。                                                                                                                                                                                                                                    |
| 説明                       | ユーザが作成するプログラム修復起動の説明を入力します。                                                                                                                                                                                                                            |
| 修復タイプ (Remediation Type) | 次のいずれかを実行します。 <ul style="list-style-type: none"> <li>• [自動 (Automatic)] : 選択した場合、[再試行回数 (Retry Count)] および [間隔 (Interval)] オプションに入力する必要があります。</li> <li>• [手動 (Manual)] : 選択されている場合、[間隔 (Interval)] および [再試行回数 (Retry Count)] フィールドは編集できません。</li> </ul> |

| フィールド                                     | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 間隔（秒単位）（Interval (in seconds)）            | クライアントが修復を試行した後で次の試行ができるようになるまでの時間間隔を秒単位で入力します。                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| 再試行回数（Retry Count）                        | 必要なプログラムを起動するためにクライアントが試行できる回数を入力します。                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| プログラムのインストールパス（Program Installation Path） | <p>ドロップダウンリストから、修復プログラムがインストールされるパスを選択します。</p> <ul style="list-style-type: none"><li>• <b>ABSOLUTE_PATH</b> : 修復プログラムは、ファイルの完全修飾パスにインストールされます。例 : C:\&lt;directory&gt;\</li><li>• <b>SYSTEM_32</b> : 修復プログラムは C:\WINDOWS\system32 ディレクトリにインストールされます。</li><li>• <b>SYSTEM_DRIVE</b> : 修復プログラムは C:\ ドライブにインストールされます。</li><li>• <b>SYSTEM_PROGRAMS</b> : 修復プログラムは C:\Program Files ファイルにインストールされます。</li><li>• <b>SYSTEM_ROOT</b> : 修復プログラムは Windows システムのルートパスにインストールされます。</li></ul> |
| プログラム実行ファイル（Program Executable）           | 修復プログラムの実行ファイルまたはインストール ファイルの名前を入力します。                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| プログラムパラメータ（Program Parameters）            | 修復プログラムに必要なパラメータを入力します。                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 既存プログラム（Existing Programs）                | <p>既存プログラム テーブルは修復プログラムのインストールパス、名前、およびパラメータ（存在する場合）を表示します。</p> <ul style="list-style-type: none"><li>• 既存プログラム リストに修復プログラムを追加するには、[追加（Add）] をクリックします。</li><li>• リストから修復プログラムを削除するには、削除アイコンをクリックします。</li></ul>                                                                                                                                                                                                                                                                    |

## 関連トピック

[プログラム修復起動の追加](#) (954 ページ)

[プログラム修復起動のトラブルシューティング](#) (955 ページ)

[クライアントレス モードでのポスチャ要件の作成](#) (968 ページ)

## Windows Update 修復

次の表では、[Windows Update 修復 (Windows Update Remediation)] ページのフィールドについて説明します。ナビゲーション パスは、[ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] > [ポスチャ (Posture)] > [修復アクション (Remediation Actions)] > [Windows Update 修復 (Windows Update Remediation)] です。

表 150: Windows Update 修復

| フィールド                            | 使用上のガイドライン                                                                                                                                                                                                                                         |
|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [名前 (Name)]                      | Windows Update 修復の名前を入力します。                                                                                                                                                                                                                        |
| 説明                               | Windows Update 修復の説明を入力します。                                                                                                                                                                                                                        |
| 修復タイプ (Remediation Type)         | 次のいずれかを実行します。 <ul style="list-style-type: none"> <li>[自動 (Automatic)] : 選択した場合、[再試行回数 (Retry Count)] および [間隔 (Interval)] オプションに入力する必要があります。</li> <li>[手動 (Manual)] : 選択されている場合、[間隔 (Interval)] および [再試行回数 (Retry Count)] フィールドは編集できません。</li> </ul> |
| 間隔 (秒単位) (Interval (in seconds)) | クライアントが修復を試行した後で次の試行ができるようになるまでの時間間隔を秒単位で入力します。                                                                                                                                                                                                    |
| 再試行回数 (Retry Count)              | Windows クライアントが Windows Update を試行できる回数を入力します。                                                                                                                                                                                                     |

| フィールド                                                                                          | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Windows Update 設定 (Windows Update Setting)                                                     | <p>次のオプションから選択します。</p> <ul style="list-style-type: none"><li>• [設定を変更しない (Do not change setting)] : Windows 自動更新のクライアント設定は、Windows Update 修復中または実行後に変更されません。</li><li>• [ダウンロードおよびインストールを通知 (Notify to download and install)] : Windows によってクライアントへの通知のみが行われ、ダウンロードやインストールは自動的には行われません。</li><li>• [自動的にダウンロードし、インストールを通知 (Automatically download and notify to install)] : Windows によってクライアントに更新プログラムがダウンロードされ、Windows Update をインストールするようにクライアントに通知されます。</li><li>• [自動的にダウンロードしてインストール (Automatically download and install)] : Windows によって自動的に Windows Update がダウンロードされてインストールされます。これは、Windows クライアントに対して強く推奨される設定です。</li></ul> |
| Windows Update 設定を管理者の設定でオーバーライド (Override User's Windows Update setting with administrator's) | <p>Windows Update 修復の実行中および実行後に、管理者が Windows 自動更新に対して指定した設定をすべてのクライアントマシンに適用するには、このチェックボックスをチェックします。</p> <p>このチェックボックスをオフにすると、次の設定が適用されます。</p> <ul style="list-style-type: none"><li>• 管理者が指定した設定 (Windows クライアントで自動更新が無効になっている場合のみ)。</li><li>• Windows クライアントが指定した設定 (クライアントで Windows 自動更新が有効になっている場合のみ)。</li></ul>                                                                                                                                                                                                                                                                                                            |

## 関連トピック

[Windows Update 修復の追加](#) (956 ページ)

クライアントレス モードでのポスチャ要件の作成 (968 ページ)

## Windows Server Update Services 修復

次の表では、[Windows Update 修復 (Windows Update Remediation)] ページのフィールドについて説明します。ナビゲーションパスは、[ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] > [ポスチャ (Posture)] > [修復アクション (Remediation Actions)] > [Windows Server Update Services 修復 (Windows Server Update Services Remediation)] です。

表 151: WSUS 修復

| フィールド                            | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                        |
|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [名前 (Name)]                      | WSUS 修復の名前を入力します。                                                                                                                                                                                                                                                                                                                                 |
| 説明                               | WSUS 修復の説明を入力します。                                                                                                                                                                                                                                                                                                                                 |
| 修復タイプ (Remediation Type)         | 次のオプションから選択します。 <ul style="list-style-type: none"> <li>[自動 (Automatic)] : NAC Agent は、Windows クライアントを最新の WSUS 更新で更新します。</li> <li>[手動 (Manual)] : 選択すると、[間隔 (Interval)] フィールドと [再試行回数 (Retry Count)] フィールドを編集できなくなります。ユーザは、コンプライアンスのために、Microsoft で管理されている WSUS サーバまたはローカルに管理されている WSUS サーバからの最新の WSUS 更新を使用して、Windows クライアントを手動で更新します。</li> </ul> |
| 間隔 (秒単位) (Interval (in seconds)) | NAC Agent と Web Agent が前回の試行後に再試行を試みるまでに WSUS 更新を遅延させる間隔を秒単位で入力します (デフォルトの間隔は 0 です)。                                                                                                                                                                                                                                                              |
| 再試行回数 (Retry Count)              | NAC Agent と Web Agent が WSUS 更新を使用して Windows クライアントの更新を再試行する回数を入力します。                                                                                                                                                                                                                                                                             |



| フィールド                                                  | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Windows Update の検証方法 (Validate Windows updates using)  | <p>次のオプションから選択します。</p> <ul style="list-style-type: none"><li>• [シスコルール (Cisco Rules)] : このオプションを選択すると、ポスチャ要件の条件としてカスタム ルールまたは事前設定済みルールを選択できます。</li><li>• [重大度レベル (Severity Level)] : このオプションを選択すると、ポスチャ要件の条件としてカスタム ルールまたは事前設定済みルールを選択できますが、いずれも使用されません。このため、WSUS 修復を指定するポスチャ要件内にはプレースホルダ条件 (ダミー条件) として pr_WSUSRule を使用できます。</li></ul>                                                                                                                                                                                                                   |
| Windows Update 重大度レベル (Windows Updates Severity Level) | <p>重大度レベルを選択します。</p> <ul style="list-style-type: none"><li>• [緊急 (Critical)] : 緊急の Windows Update のみをインストールします。</li><li>• [至急 (Express)] : 重要かつ重大な Windows Update をインストールします。</li><li>• [中 (Medium)] : 重大度および重要性が中程度のすべての Windows Update をインストールします。</li><li>• [すべて (All)] : 重大度および重要性が中程度および低程度のすべての Windows Update をインストールします。</li></ul> <p>(注) 重大度レベルオプションを使用してポスチャ要件に WSUS 修復アクションを関連付けて Windows Update を検証する場合は、ポスチャ要件に pr_WSUSRule (ダミー複合条件) 複合条件を選択する必要があります。ポスチャ要件が失敗すると、NAC Agent は、WSUS 修復で定義した重大度レベルに基づいて修復アクション (Windows Update) を適用します。</p> |

| フィールド                                                            | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 最新の OS サービス パックに更新 (Update to latest OS Service Pack)            | <p>クライアントのオペレーティング システムで<br/>使用できる最新のサービス パックを WSUS 修復が自動的にインストールできるようにするには、このチェックボックスをオンにします。</p> <p>(注) オペレーティング システムのサービス パックは、WSUS 修復で選択されている [中 (Medium) ] および [すべて (All) ] の重大度レベル オプションに関係なく、自動的に更新されます。</p>                                                                                                                                                                                                                       |
| Windows Update インストール ソース (Windows Updates Installation Source)  | <p>Windows クライアントに WSUS 更新をインストールするソースを指定します。</p> <ul style="list-style-type: none"> <li>• [Microsoft サーバ (Microsoft server) ] : Microsoft で管理されている WSUS サーバ</li> <li>• [管理対象サーバ (Managed server) ] : ローカルに管理されている WSUS サーバ</li> </ul>                                                                                                                                                                                                    |
| インストール ウィザード インターフェイス 設定 (Installation Wizard Interface Setting) | <p>WSUS 更新中にクライアントにインストール ウィザードを表示できるようにします。</p> <ul style="list-style-type: none"> <li>• [UI を表示 (Show UI) ] : Windows クライアントで Windows Update インストール ウィザードを表示します。ユーザは、クライアントに対して WSUS 更新中にインストール ウィザードを表示するための管理者権限を持っている必要があります。</li> <li>• [UI なし (No UI) ] : Windows クライアントで Windows Update インストール ウィザードを非表示にします。</li> </ul> <p>(注) 管理者権限のないユーザが WSUS 修復を使用して Windows アップデートをインストールできるようにするには、[UI なし (No UI) ] オプションを選択する必要があります。</p> |

## 関連トピック

[Windows Server Update Services 修復の追加 \(956 ページ\)](#)

[クライアントレス モードでのポストチャ要件の作成 \(968 ページ\)](#)

## パッチ管理修復

次の表に、[パッチ管理修復 (Patch Management Remediation)] ページのフィールドを示します。ナビゲーションパスは、[ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] > [ポスチャ (Posture)] > [修復アクション (Remediation Actions)] > [パッチ管理修復 (Patch Management Remediation)] です。

表 152: パッチ管理修復

| フィールド                            | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                 |
|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [名前 (Name)]                      | パッチ管理修復の名前を入力します。                                                                                                                                                                                                                                                                                                          |
| 説明                               | パッチ管理修復の説明を入力します。                                                                                                                                                                                                                                                                                                          |
| 修復タイプ (Remediation Type)         | 次のいずれかを実行します。 <ul style="list-style-type: none"><li>• [自動 (Automatic)] : [間隔 (Interval)] および [再試行回数 (Retry Count)] に値を入力します。ISE サーバは非準拠のクライアントを識別し、修復の通知方法を選択し、自動的にクライアントの最新のパッチを更新します。</li><li>• [手動 (Manual)] : ([間隔 (Interval)] および [再試行回数 (Retry Count)] フィールドは無効) 非準拠のクライアントは最新のパッチを手動でダウンロードし、適用する必要があります。</li></ul> |
| 間隔 (秒単位) (Interval (in seconds)) | (自動修復タイプを選択した場合のみ使用可能) クライアントでスケジューリングされたパッチ更新が実行されるまでの時間間隔を秒単位で入力します。                                                                                                                                                                                                                                                     |
| 再試行回数 (Retry Count)              | (自動修復タイプを選択した場合のみ使用可能) クライアントが重要なパッチの更新を試行できる回数を入力します。                                                                                                                                                                                                                                                                     |
| オペレーティング システム (Operating System) | サポートされる唯一の OS は Windows OS です。                                                                                                                                                                                                                                                                                             |

| フィールド                                     | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                |
|-------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| パッチ管理ベンダー名 (Patch Management Vendor Name) | <p>ドロップダウン リストからベンダー名を選択します。ベンダーのパッチ管理修復製品と、バージョン、修復の有効化、修復の更新、およびUI修復の表示に対する製品のサポートが [選択したベンダーの製品 (Products for Selected Vendor) ] テーブルに表示されます。</p> <p>(注) Cisco ISE および AnyConnect のサポート対象バージョンは次のとおりです。</p> <ul style="list-style-type: none"><li>• Cisco ISE バージョン 1.4 以降</li><li>• AnyConnect バージョン 4.1 以降</li></ul> |

| フィールド                        | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 修復オプション (Remediation Option) | <p>次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• [有効 (Enable)] : エンドポイントでディセーブルの場合は、パッチの管理ソフトウェアをイネーブルにします。</li> <li>• [欠落したパッチのインストール (Install Missing Patches)] : エンドポイントでパッチを更新します。</li> <li>• [パッチ管理ソフトウェアGUIのアクティブ化 (Activate Patch Management Software GUI)] : パッチ管理ソフトウェアのユーザインターフェイスを表示します。ソフトウェアの設定を変更したりソフトウェアアップデートを開始するには、このページの指示に従います。</li> </ul> <p>[パッチ管理ベンダー名 (Patch Management Vendor Name)] で指定したベンダーがサポートする製品のリストを表示するには、[選択したベンダーの製品 (Products for Selected Vendor)] ドロップダウン矢印をクリックします。たとえば、製品 1 と 製品 2 の 2 つの製品を持つベンダー A を選択したとします。製品 1 は [修復の有効化 (Enable remediation)] オプションをサポートしているが、製品 2 はサポートしていない場合があります。または、製品 1 が [有効 (Enable)] および [欠落したパッチの修復のインストール (Install missing patches remediation)] オプションをサポートしていない場合、製品 1 はディセーブル (グレー表示) になります。[選択したベンダーの製品 (Products for Selected Vendor)] テーブルは選択した修復オプションに応じて変わります。</p> |

#### 関連トピック

[パッチ管理修復の追加 \(953 ページ\)](#)

[クライアントレス モードでのポスチャ要件の作成 \(968 ページ\)](#)

## USB 大容量ストレージのチェックのワークフロー

ポスチャ ポリシーの USB\_Check 条件（シスコ事前定義済み）を使用して、USB 大容量ストレージデバイスがエンドポイントに接続されているかどうかを確認できます。USB 大容量ストレージのチェックと修復のフローは次のとおりです。

AnyConnect のエージェント：

- USB 接続があるかどうかを確認します。
- USB プラグインを検出して USB\_Block 修復（Cisco 事前定義済み）を適用します。  
AnyConnect エージェントが Cisco ISE に修復の障害を報告し、CoA を開始します。USB 大容量ストレージの修復は常にアクティブであり、アクセス時または定期的再評価（PRA）に限定されません。
- ユーザがネットワーク インターフェイスから接続解除すると、USB の検出の実行を停止します。
- エンドポイントの再接続時に、ポスチャフローを再実行します。ただし、エンドポイントがポスチャのリース期間内の場合、AnyConnect エージェントは、USB チェックを再び実行しません。



(注) AnyConnect は USB を検査し、修復を順に実行します。その結果、PRA を実行する際に、USB の動的な変更の処理に遅延が生じることがあります。USB のチェックが設定されると、他のチェックに対する PRA の猶予時間（[ワーク センター（Work Centers）]>[ポスチャ（Posture）]>[設定（Settings）]>[再評価設定（Reassessment Configurations）]）を最小化することをお勧めします。



(注) USB チェックには複合条件を作成できません。

### 関連トピック

- [USB 条件の設定](#)（1399 ページ）
- [単純ポスチャ条件](#)（664 ページ）

## USB 大容量ストレージ修復

次の表では、[USB 修復（USB Remediation）] ページのフィールドについて説明します。ナビゲーションパスは、[ワーク センター（Work Centers）]>[ポスチャ（Posture）]>[ポリシー要素（Policy Elements）]>[修復（Remediations）]>[USB] です。また、[ポリシー（Policy）]>[ポリシー要素（Policy Elements）]>[結果（Results）]>[ポスチャ（Posture）]>[修復アクション（Remediation Actions）]>[USB 修復（USB Remediation）] ページのオプションが表示されています。

表 153: USB 修復の設定

| フィールド                            | 使用上のガイドライン                                                   |
|----------------------------------|--------------------------------------------------------------|
| [名前 (Name) ]                     | USB 修復の名前を入力します。                                             |
| 説明                               | USB 修復の説明を入力します。                                             |
| コンプライアンス モジュール                   | バージョン 4.x 以降向けの、ISE のポスチャ準拠モジュールの表示専用フィールドのサポート。             |
| オペレーティング システム (Operating System) | Windows OS のサポートを示す表示専用フィールド。                                |
| 修復タイプ (Remediation Type)         | 修復が自動であることを示す表示専用フィールド。                                      |
| インターバル (Interval)                | クライアントでスケジュールされた USB 大容量ストレージのデバイス チェックが実行される時間間隔を秒単位で入力します。 |
| 再試行回数 (Retry Count)              | クライアントで USB 大容量ストレージのデバイスの再評価が実行される時間間隔を秒単位で入力します。           |

## 関連トピック

[単純ポスチャ条件](#) (664 ページ)

## クライアントのポスチャ要件

次の表に、[ポスチャ要件 (Posture Requirements) ] ページのフィールドを示します。ナビゲーションパスは、[ポリシー (Policy) ]>[ポリシー要素 (Policy Elements) ]>[結果 (Results) ]>[ポスチャ (Posture) ]>[要件 (Requirements) ] です。

表 154: ポスチャ要件

| フィールド         | 使用上のガイドライン                                                                                                                       |
|---------------|----------------------------------------------------------------------------------------------------------------------------------|
| [名前 (Name) ]  | 要件の名前を入力します。                                                                                                                     |
| オペレーティング システム | オペレーティング システムを選択します。<br><br>プラス記号 [+] をクリックして、複数のオペレーティング システムをポリシーに関連付けます。<br><br>マイナス記号 [-] をクリックして、ポリシーからオペレーティング システムを削除します。 |

| フィールド                         | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 条件 (Conditions)               | <p>リストから条件を選択します。</p> <p>[操作 (Action) ] アイコンをクリックして、ユーザ定義の条件を作成して、要件に関連付けることもできます。ユーザ定義の条件を作成中に関連する親オペレーティング システムは編集できません。</p> <p>pr_WSUSRule は、Windows Server Update Services (WSUS) 修復が関連付けられているポスチャ要件で使用される、ダミーの複合条件です。関連 WSUS 修復アクションは、重大度レベル オプションを使用して Windows Updates を検証するように設定する必要があります。この要件が失敗すると、Windows クライアントにインストールされている NAC Agent は、WSUS 修復で定義した重大度レベルに基づいて WSUS 修復アクションを適用します。</p> <p>pr_WSUSRule は複合条件のリストページには表示できません。条件ウィジェットからのみ pr_WSUSRule を選択できます。</p> |
| 修復アクション (Remediation Actions) | <p>リストから修復を選択します。</p> <p>修復アクションを作成して、要件に関連付けることもできます。</p> <p>Agent ユーザとの通信に使用できるすべての修復タイプのテキストボックスがあります。修復アクションに加えて、クライアントの非準拠に関してメッセージで Agent ユーザと通信することができます。</p> <p>[メッセージテキストのみ (Message Text Only) ] オプションで Agent ユーザに非準拠について通知します。また、詳細情報を得るためにヘルプ デスクに連絡したり、クライアントを手動で修復したりするオプションの手順がユーザに提供されています。このシナリオでは、NAC Agent は修復アクションをトリガーしません。</p>                                                                                                                          |

#### 関連トピック

[ポスチャ評価の利用規定の設定 \(941 ページ\)](#)

[クライアントのポスチャ要件の作成 \(959 ページ\)](#)





## 第 34 章

# 操作のユーザ インターフェイスのリファレンス

- [RADIUS ライブ ログ \(1451 ページ\)](#)
- [RADIUS ライブ セッション \(1454 ページ\)](#)
- [TACACS ライブ ログ \(1459 ページ\)](#)
- [診断ツール \(1461 ページ\)](#)

## RADIUS ライブ ログ

次の表では、最近の RADIUS 認証を表示する [RADIUS ライブ ログ (RADIUS Live Logs)] ページのフィールドについて説明します。このページへのナビゲーションパスは、[操作 (Operations)] > [RADIUS] > [ライブ ログ (Live Logs)] です。RADIUS ライブ ログはプライマリ PAN だけで表示されます。

表 155: RADIUS ライブ ログ

| オプション          | 使用上のガイドライン                                                                          |
|----------------|-------------------------------------------------------------------------------------|
| 時刻 (Time)      | モニタリングおよび収集エージェントがログを受信した時刻を表示します。このカラムは必須です。選択解除することはできません。                        |
| ステータス (Status) | 認証が成功したか失敗したかを示します。このカラムは必須です。選択解除することはできません。緑色は認証が成功したことを示します。赤色は認証が失敗したことを示します。   |
| 詳細 (Details)   | 虫眼鏡アイコンをクリックすると、選択した認証シナリオをドリルダウンし、詳細情報を確認できるレポートが表示されます。このカラムは必須です。選択解除することはできません。 |

| オプション                             | 使用上のガイドライン                                                                         |
|-----------------------------------|------------------------------------------------------------------------------------|
| 繰り返し回数 (Repeat Count)             | ID、ネットワーク デバイス、および許可のコンテキストで変更がなく、直近の 24 時間で認証要求が繰り返された回数を表示します。                   |
| ID (Identity)                     | ログイン済みの認証に関連付けられているユーザ名を示します。                                                      |
| エンドポイント ID (Endpoint ID)          | エンドポイントの一意の識別子を表示します。通常は MAC または IP アドレスです。                                        |
| エンドポイント プロファイル (Endpoint Profile) | プロファイリングされるエンドポイントのタイプを示します (たとえば、iPhone、Android、MacBook、Xbox になるようにプロファイリングされます)。 |
| 認証ポリシー (Authentication policy)    | 特定の認証に選択されているポリシーの名前を表示します。                                                        |
| 許可ポリシー                            | 特定の許可に選択されているポリシーの名前を表示します。                                                        |
| 認証プロファイル                          | 認証に使用された許可プロファイルを表示します。                                                            |
| [IP アドレス (IP Address) ]           | エンドポイントデバイスの IP アドレスを表示します。                                                        |
| ネットワーク デバイス (Network Device)      | ネットワーク アクセス デバイスの IP アドレスを表示します。                                                   |
| デバイス ポート (Device Port)            | エンドポイントが接続されているポート番号を表示します。                                                        |
| ID グループ                           | ログの生成対象となるユーザまたはエンドポイントに割り当てられる ID グループを表示します。                                     |
| ポスチャ ステータス (Posture Status)       | ポスチャ検証のステータスと認証の詳細を表示します。                                                          |
| サーバ                               | ログの生成元になったポリシー サービスが表示されます。                                                        |
| MDMサーバ名 (MDM Server Name)         | MDM サーバの名前を表示します。                                                                  |
| イベント                              | イベント ステータスを表示します。                                                                  |

| オプション                             | 使用上のガイドライン                                                                                                |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------|
| 失敗の理由 (Failure Reason)            | 認証が失敗した場合、その失敗の詳細な理由を表示します。                                                                               |
| 認証方式 (Auth Method)                | Microsoft チャレンジ ハンドシェイク 認証 プロトコル バージョン 2 (MS-CHAPv2)、IEE 802.1x、dot1x など、RADIUS プロトコルによって使用される認証方式を表示します。 |
| 認証プロトコル (Authentication Protocol) | Protected Extensible Authentication Protocol (PEAP) や拡張認証プロトコル (EAP) など、使用される認証プロトコルを表示します。               |
| セキュリティ グループ (Security Group)      | 認証ログによって識別されるグループを表示します。                                                                                  |
| セッション ID                          | セッション ID を表示します。                                                                                          |



- (注) [RADIUS ライブ ログ (RADIUS Live Logs)] と [TACACS+ ライブ ログ (TACACS+ Live Logs)] 詳細ペインでは、各ポリシー許可ルール の 1 番目の属性として [照会済み PIP (Queried PIP)] が表示されます。許可ルール内のすべての属性が、以前のルールについてすでに照会されているディクショナリに関連している場合、これ以外に [照会済み PIP (Queried PIP)] エントリは表示されません。

[RADIUS ライブ ログ (RADIUS Live Logs)] ページで、次を実行できます。

- データを csv または pdf ファイル形式でエクスポートします。
- 要件に基づいて列を表示または非表示にします。
- 簡易またはカスタムフィルタを使用してデータをフィルタリングします。後で使用するためにフィルタを保存することもできます。
- 列の順序を変更したり、列の幅を調整します。
- 列の値をソートします。



- (注) すべてのユーザのカスタマイズは、ユーザ設定として保存されます。

#### 関連トピック

[ライブ認証のモニタ](#) (1068 ページ)

[ライブ認証](#) (1068 ページ)

# RADIUS ライブセッション

次の表では、ライブ認証が表示される [RADIUS ライブセッション (RADIUS live sessions)] ページのフィールドについて説明します。このページへのナビゲーションパスは、[操作 (Operations)] > [RADIUS] > [ライブセッション (Live Sessions)] です。RADIUS ライブセッションはプライマリ PAN でしか表示できません。

表 156: RADIUS ライブセッション

| フィールド                               | 説明                                                                                       |
|-------------------------------------|------------------------------------------------------------------------------------------|
| 開始 (Initiated)                      | セッション開始時のタイムスタンプを表示します。                                                                  |
| 更新しました                              | 何らかの変更のためにセッションが最後に更新された時点のタイムスタンプを表示します。                                                |
| アカウントセッション時間 (Account Session Time) | ユーザセッションの期間 (秒単位) を表示します。                                                                |
| セッションステータス (Session Status)         | エンドポイントデバイスの現在のステータスを表示します。                                                              |
| アクション (CoA Action)                  | アクティブな RADIUS セッションを再認証するか、またはアクティブな RADIUS セッションを切断するには、[アクション (Actions)] アイコンをクリックします。 |
| 繰り返し回数 (Repeat Count)               | ユーザまたはエンドポイントの再認証回数を示します。                                                                |
| エンドポイント ID (Endpoint ID)            | エンドポイントの一意の識別子を表示します。通常は MAC または IP アドレスです。                                              |
| ID (Identity)                       | エンドポイントデバイスのユーザ名を表示します。                                                                  |
| [IP アドレス (IP Address)]              | エンドポイントデバイスの IP アドレスを表示します。                                                              |
| 監査セッション ID (Audit Session ID)       | 固有のセッション ID を表示します。                                                                      |
| アカウントセッション ID (Account Session ID)  | ネットワークデバイスから提供された固有 ID を表示します。                                                           |
| エンドポイントプロファイル (Endpoint Profile)    | デバイスのエンドポイントプロファイルを表示します。                                                                |

| フィールド                             | 説明                                                                                                      |
|-----------------------------------|---------------------------------------------------------------------------------------------------------|
| ポスチャ ステータス (Posture Status)       | ポスチャ 検証のステータスと認証の詳細を表示します。                                                                              |
| セキュリティ グループ (Security Group)      | 認証ログによって識別されるグループを表示します。                                                                                |
| サーバ                               | ログを生成したポリシーサービスを示します。                                                                                   |
| 認証方式 (Auth Method)                | パスワード認証プロトコル (PAP) 、チャレンジハンドシェイク認証プロトコル (CHAP) 、 IEE 802.1x、 dot1x など、 RADIUS プロトコルによって使用される認証方式を表示します。 |
| 認証プロトコル (Authentication Protocol) | Protected Extensible Authentication Protocol (PEAP) や拡張認証プロトコル (EAP) など、使用される認証プロトコルを表示します。             |
| 認証ポリシー (Authentication policy)    | 特定の認証に選択されているポリシーの名前を表示します。                                                                             |
| 許可ポリシー                            | 特定の許可に選択されているポリシーの名前を表示します。                                                                             |
| 認証プロファイル                          | 認証に使用された許可プロファイルを表示します。                                                                                 |
| NAS IP アドレス                       | ネットワーク デバイスの IP アドレスを表示します。                                                                             |
| デバイス ポート (Device Port)            | ネットワーク デバイスに接続されたポートを表示します。                                                                             |
| PRA アクション (PRA Action)            | ネットワークでのコンプライアンスのためにクライアントが正常にポスチャされた後、そのクライアントで実行される定期的な再評価アクションを表示します。                                |
| ANCステータス (ANC Status)             | [隔離 (Quarantine) ]、[隔離解除 (Unquarantine) ]、または [シャットダウン (Shutdown) ]としてデバイスの適応型ネットワーク制御のステータスを表示します。     |

| フィールド                             | 説明                                                                                                          |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------|
| WLC ローミング (WLC Roam)              | エンドポイントがローミング中に WLC 間でハンドオフされたことを追跡するために使用されるブール値 (Y/N) を表示します。<br>cisco-av-pair=nas-update の値は Y または N です。 |
| パケット入力                            | 受信したパケットの数を表示します。                                                                                           |
| パケット出力                            | 送信したパケットの数を表示します。                                                                                           |
| 受信バイト数 (Bytes In)                 | 受信したバイト数を表示します。                                                                                             |
| 送信バイト数 (Bytes Out)                | 送信したバイト数を表示します。                                                                                             |
| セッション送信元 (Session Source)         | RADIUS セッションまたは PassiveID セッションのいずれであるかを示します。                                                               |
| ユーザドメイン名 (User Domain Name)       | ユーザの登録済み DNS 名を示します。                                                                                        |
| ホストドメイン名 (Host Domain Name)       | ホストの登録済み DNS 名を示します。                                                                                        |
| ユーザ NetBIOS 名 (User NetBIOS Name) | ユーザの NetBIOS 名を示します。                                                                                        |
| ホスト NetBIOS 名 (Host NetBIOS Name) | ホストの NetBIOS 名を示します。                                                                                        |
| ライセンスのタイプ (License Type)          | 使用されているライセンスのタイプ (Base、Plus、Apex、または Plus and Apex) を表示します。                                                 |
| ライセンスの詳細 (License Details)        | ライセンスの詳細を表示します。                                                                                             |

| フィールド                                 | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| プロバイダー                                | <p>エンドポイント イベントはさまざまな syslog ソースから学習されます。これらの syslog ソースはプロバイダーと呼ばれます。</p> <ul style="list-style-type: none"><li>• <b>Windows Management Instrumentation (WMI)</b> : WMI は、オペレーティングシステム、デバイス、アプリケーション、およびサービスに関する管理情報にアクセスするための共通インターフェイスとオブジェクト モデルを提供する Windows サービスです。</li><li>• <b>エージェント</b> : クライアントまたは別のプログラムの代わりにクライアントで実行されるプログラム。</li><li>• <b>syslog</b> : クライアントがイベントメッセージを送信するロギング サーバ。</li><li>• <b>REST</b> : クライアントはターミナルサーバで認証されます。この syslog ソースの場合、[TS エージェント ID (TS Agent ID)]、[開始送信元ポート (Source Port Start)]、[終了送信元ポート (Source Port End)]、[最初の送信元ポート (Source First Port)] の値が表示されます。</li><li>• <b>SPAN</b> : ネットワーク情報は SPAN プロローブを使用して検出されます。</li><li>• <b>DHCP</b> : DHCP イベント。</li><li>• <b>エンドポイント (Endpoint)</b></li></ul> <p>異なるプロバイダーからの 2 つのイベントがエンドポイントセッションから学習されると、ライブセッションページにこれらのプロバイダーがカンマ区切り値として表示されます。</p> |
| MAC アドレス (MAC Address)                | クライアントの MAC アドレスを表示します。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| [エンドポイントチェック時刻 (Endpoint Check Time)] | エンドポイント プロローブによってエンドポイントが最後にチェックされた時刻を表示します。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

| フィールド                                        | 説明                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [エンドポイントチェック結果 (Endpoint Check Result) ]     | <p>エンドポイント プローブの結果が表示されます。設定可能な値は次のとおりです。</p> <ul style="list-style-type: none"> <li>• 到達不要</li> <li>• [ユーザ ログアウト (User Logout) ]</li> <li>• [アクティブ ユーザ (Active User) ]</li> </ul>                                                                                                                                                                                       |
| [送信元ポートの開始 (Source Port Start) ]             | (REST プロバイダーの場合にのみ値が表示されます。) ポート範囲の最初のポートの番号を示します。                                                                                                                                                                                                                                                                                                                       |
| [送信元ポートの終了 (Source Port End) ]               | (REST プロバイダーの場合にのみ値が表示されます。) ポート範囲の最後のポート番号を示します。                                                                                                                                                                                                                                                                                                                        |
| [最初の送信元ポート (Source First Port) ]             | <p>(REST プロバイダーの場合にのみ値が表示されます。) ターミナルサーバ (TS) エージェントにより割り当てられた最初のポートを示します。</p> <p>ターミナルサーバ (TS) は、複数のエンドポイントがモデムまたはネットワーク インターフェイスなしで接続でき、複数エンドポイントが LAN ネットワークに接続できるようにするサーバまたはネットワーク デバイスです。複数のエンドポイントに同一 IP アドレスが割り当てられている場合は、特定ユーザの IP アドレスを識別することが困難になります。このため、特定ユーザを識別する目的で TS エージェントがサーバにインストールされ、各ユーザにポート範囲が割り当てられます。これにより、IP アドレス - ポート - ユーザのマッピングが作成されます。</p> |
| [TS エージェント ID (TS Agent ID) ]                | (REST プロバイダーの場合にのみ値が表示されます。) エンドポイントにインストールされているターミナルサーバ (TS) エージェントの一意の ID を表示します。                                                                                                                                                                                                                                                                                      |
| [AD ユーザ解決 ID (AD User Resolved Identities) ] | (AD ユーザの場合にのみ値が表示されます。) 一致したアカウントの候補が表示されます。                                                                                                                                                                                                                                                                                                                             |



| フィールド                                | 説明                                                                             |
|--------------------------------------|--------------------------------------------------------------------------------|
| [AD ユーザ解決 DN (AD User Resolved DNs)] | (AD ユーザの場合にのみ値が表示されます。) AD ユーザの識別名 (例: CN=chris,CN=Users,DC=R1,DC=com) を表示します。 |

#### 関連トピック

[RADIUS セッションの許可の変更](#) (1101 ページ)

[Cisco ISE のアクティブな RADIUS セッション](#) (1100 ページ)

## TACACS ライブ ログ

次の表では、TACACS+ AAA の詳細を表示する [TACACS ライブ ログ (TACACS Live Logs)] ページのフィールドについて説明します。このページへのナビゲーションパスは、**[操作 (Operations)] > [TACACS ライブ ログ (TACACS Live Logs)]** です。TACACS ライブ ログはプライマリ PAN だけで表示されます。

表 157: TACACS ライブ ログ

| フィールド                    | 使用上のガイドライン                                                                          |
|--------------------------|-------------------------------------------------------------------------------------|
| 生成日時 (Generated Time)    | 特定のイベントがトリガーされた時点に基づいて、syslog の生成日時を示します。                                           |
| ログに記録された時刻 (Logged Time) | syslog がモニタリング ノードによって処理され、保存された時刻を示します。このカラムは必須です。選択解除することはできません。                  |
| ステータス (Status)           | 認証が成功したか失敗したかを示します。このカラムは必須です。選択解除することはできません。緑色は認証が成功したことを示します。赤色は認証が失敗したことを示します。   |
| 詳細 (Details)             | 虫眼鏡アイコンをクリックすると、選択した認証シナリオをドリルダウンし、詳細情報を確認できるレポートが表示されます。このカラムは必須です。選択解除することはできません。 |
| セッションキー (Session Key)    | ISE によってネットワーク デバイスに返される (EAP の成功メッセージまたは EAP の失敗メッセージにある) セッション キーを示します。           |

| フィールド                                    | 使用上のガイドライン                                                                                                                    |
|------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| [ユーザ名 (Username) ]                       | デバイス管理者のユーザ名を示します。このカラムは必須です。選択解除することはできません。                                                                                  |
| タイプ (Type)                               | [認証 (Authentication) ] および [承認 (Authorization) ] の 2 つのタイプで構成されます。認証、承認、またはその両方を通過または失敗したユーザ名を示します。このカラムは必須です。選択解除することはできません。 |
| 認証ポリシー (Authentication policy)           | 特定の認証に選択されているポリシーの名前を表示します。                                                                                                   |
| 許可ポリシー                                   | 特定の許可に選択されているポリシーの名前を表示します。                                                                                                   |
| ISE ノード (ISE Node)                       | アクセス要求が処理される ISE ノードの名前を示します。                                                                                                 |
| ネットワークデバイス名 (Network Device Name)        | ネットワーク デバイスの名前を示します。                                                                                                          |
| ネットワークデバイス IP (Network Device IP)        | アクセス要求を処理するネットワーク デバイスの IP アドレスを示します。                                                                                         |
| ネットワーク デバイス グループ (Network Device Groups) | ネットワーク デバイスが属する対応するネットワーク デバイス グループの名前を示します。                                                                                  |
| デバイスタイプ (Device Type)                    | 異なるネットワーク デバイスからのアクセス要求の処理に使用されるデバイスタイプポリシーを示します。                                                                             |
| 参照先                                      | ネットワーク デバイスからのアクセス要求の処理に使用されるロケーション ベースのポリシーを示します。                                                                            |
| デバイス ポート (Device Port)                   | アクセス要求が行われるデバイスのポート番号を示します。                                                                                                   |
| 失敗の理由 (Failure Reason)                   | ネットワーク デバイスによって行われたアクセス要求を拒否した理由を示します。                                                                                        |
| リモート アドレス (Remote Address)               | エンドステーションを一意に識別する IP アドレス、MAC アドレス、またはその他の任意の文字列を示します。                                                                        |

| フィールド                             | 使用上のガイドライン                                                                                        |
|-----------------------------------|---------------------------------------------------------------------------------------------------|
| 一致したコマンドセット (Matched Command Set) | MatchedCommandSet 属性値が存在する場合はその値を示し、MatchedCommandSet 属性値が空の場合、または属性自体が syslog に存在しない場合は空の値を示します。 |
| シェルプロファイル (Shell Profile)         | ネットワーク デバイスでコマンドを実行するためのデバイス管理者に付与された権限を示します。                                                     |

[TACACS ライブログ (TACACS Live Logs)] ページで、次を実行できます。

- データを csv または pdf ファイル形式でエクスポートします。
- 要件に基づいて列を表示または非表示にします。
- 簡易またはカスタムフィルタを使用してデータをフィルタリングします。後で使用するためにフィルタを保存することもできます。
- 列の順序を変更したり、列の幅を調整します。
- 列の値をソートします。



(注) すべてのユーザのカスタマイズは、ユーザ設定として保存されます。

#### 関連トピック

[TACACS+ デバイス管理](#) (9 ページ)

[TACACS+ のグローバル設定](#) (245 ページ)

## 診断ツール

### RADIUS 認証のトラブルシューティングの設定

次の表では、RADIUS 認証の問題を認識し、解決できる [RADIUS 認証のトラブルシューティング (RADIUS authentication troubleshooting)] ページのフィールドについて説明します。このページへのナビゲーションパスは、[操作 (Operations)] > [トラブルシューティング (Troubleshoot)] > [診断ツール (Diagnostic Tools)] > [一般ツール (General Tools)] > [RADIUS 認証のトラブルシューティング (RADIUS Authentication Troubleshooting)] です。

表 158: RADIUS 認証のトラブルシューティングの設定

| オプション                              | 使用上のガイドライン                                                                                                                                          |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| [ユーザ名 (Username) ]                 | 認証をトラブルシューティングするユーザのユーザ名を入力します。                                                                                                                     |
| MAC アドレス (MAC Address)             | トラブルシューティングするデバイスの MAC アドレスを入力します。                                                                                                                  |
| 監査セッション ID (Audit Session ID)      | トラブルシューティングする監査セッション ID を入力します。                                                                                                                     |
| NAS IP                             | NAS の IP アドレスを入力します。                                                                                                                                |
| NAS ポート (NAS Port)                 | NAS のポート番号を入力します。                                                                                                                                   |
| 認証状況 (Authentication Status)       | RADIUS 認証のステータスを選択します。                                                                                                                              |
| 失敗の理由 (Failure Reason)             | 失敗理由を入力するか、または [選択 (Select) ] をクリックしてリストから失敗理由を選択します。失敗理由をクリアするには、[クリア (Clear) ] をクリックします。                                                          |
| 時間範囲 (Time Range)                  | 時間範囲を選択します。この時間範囲に作成された RADIUS 認証レコードが使用されます。                                                                                                       |
| 開始日時 (Start Date-Time)             | [時間範囲 (Time Range) ] として [カスタム (Custom) ] を選択した場合は、開始日時を入力するか、またはカレンダーアイコンをクリックして開始日時を選択します。日付は <i>mm/dd/yyyy</i> 形式、時刻は <i>hh:mm</i> 形式である必要があります。 |
| 終了日時 (End Date-Time)               | [時間範囲 (Time Range) ] として [カスタム (Custom) ] を選択した場合は、終了日時を入力するか、またはカレンダーアイコンをクリックして終了日時を選択します。日付は <i>mm/dd/yyyy</i> 形式、時刻は <i>hh:mm</i> 形式である必要があります。 |
| レコード数の取得 (Fetch Number of Records) | 取得するレコードの数をドロップダウン リストから選択します。10、20、50、100、200、または 500 を選択できます。                                                                                     |

## 関連トピック

[予期せぬ RADIUS 認証結果のトラブルシューティング](#) (1075 ページ)

[RADIUS 認証のトラブルシューティング ツール](#) (1074 ページ)

## ネットワーク デバイス コマンドの実行の設定

次の表では、[ネットワークデバイスコマンドの実行 (Execute Network Device Command)] ページのフィールドについて説明します。これらのフィールドを使用して、ネットワーク デバイス上で **show** コマンドを実行します。このページのナビゲーションパスは、[操作 (Operations)] > [トラブルシューティング (Troubleshoot)] > [診断ツール (Diagnostic Tools)] > [一般ツール (General Tools)] > [ネットワーク デバイスの実行 (Execute Network Device)] です。

表 159: ネットワーク デバイス コマンドの実行の設定

| オプション                              | 使用上のガイドライン                           |
|------------------------------------|--------------------------------------|
| 情報の入力                              |                                      |
| ネットワーク デバイス IP (Network Device IP) | コマンドを実行するネットワーク デバイスの IP アドレスを入力します。 |
| コマンド (Command)                     | <b>show</b> コマンドを入力します。              |

### 関連トピック

[設定を確認する IOS show コマンドの実行](#) (1075 ページ)

[ネットワーク デバイス ツールの実行](#) (1075 ページ)

## 設定バリデータの評価の設定

次の表では、[設定バリデータの評価 (Evaluate Configuration Validator)] ページのフィールドについて説明します。これらのフィールドを使用してネットワーク デバイスの設定を評価して、設定の問題を特定します。このページのナビゲーションパスは、[操作 (Operations)] > [トラブルシューティング (Troubleshoot)] > [診断ツール (Diagnostic Tools)] > [一般ツール (General Tools)] > [設定バリデータの評価 (Evaluate Configuration Validator)] です。

表 160: 設定バリデータの評価の設定

| オプション                              | 使用上のガイドライン                         |
|------------------------------------|------------------------------------|
| 情報の入力                              |                                    |
| ネットワーク デバイス IP (Network Device IP) | 設定を評価するネットワーク デバイスの IP アドレスを入力します。 |
| 推奨テンプレートと比較する設定項目を、次のうちから選択します。    |                                    |
| AAA                                | このオプションは、デフォルトで選択されます。             |
| RADIUS                             | このオプションは、デフォルトで選択されます。             |

| オプション                             | 使用上のガイドライン                                                |
|-----------------------------------|-----------------------------------------------------------|
| デバイス検出 (Device Discovery)         | このオプションは、デフォルトで選択されます。                                    |
| ログ                                | このオプションは、デフォルトで選択されます。                                    |
| Web 認証 (Web Authentication)       | Web 認証の設定を比較する場合にこのチェックボックスをオンにします。                       |
| プロファイラ設定 (Profiler Configuration) | プロファイラの設定を比較する場合にこのチェックボックスをオンにします。                       |
| TrustSec                          | TrustSec 設定を比較する場合にこのチェックボックスをオンにします。                     |
| 802.1X                            | 802.1X 設定を比較する場合にこのチェックボックスをオンにします。使用可能ないずれかのオプションを選択します。 |

#### 関連トピック

[ネットワーク デバイス設定の問題のトラブルシューティング](#) (1076 ページ)

[設定バリデータ ツールの評価](#) (1076 ページ)

## ポスチャのトラブルシューティングの設定

次の表では、ネットワーク内のポスチャ問題の検出と解決に使用する [ポスチャのトラブルシューティング (Posture troubleshooting)] ページのフィールドについて説明します。このページへのナビゲーションパスは、[操作 (Operations)] > [トラブルシューティング (Troubleshoot)] > [診断ツール (Diagnostic Tools)] > [一般ツール (General Tools)] > [ポスチャのトラブルシューティング (Posture Troubleshooting)] です。

表 161: ポスチャのトラブルシューティングの設定

| オプション                          | 使用上のガイドライン                                             |
|--------------------------------|--------------------------------------------------------|
| トラブルシューティングが必要なポスチャ イベントの検索と選択 |                                                        |
| [ユーザ名 (Username)]              | フィルタリング基準として使用するユーザ名を入力します。                            |
| MAC アドレス (MAC Address)         | フィルタリング基準として使用する MAC アドレスを、xx-xx-xx-xx-xx-xx 形式で入力します。 |
| ポスチャ ステータス (Posture Status)    | フィルタリング基準として使用する認証ステータスを選択します。                         |

| オプション                              | 使用上のガイドライン                                                                                                                                                        |
|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 失敗の理由 (Failure Reason)             | 失敗理由を入力するか、または [選択 (Select)] をクリックしてリストから失敗理由を選択します。失敗理由をクリアするには、[クリア (Clear)] をクリックします。                                                                          |
| 時間範囲 (Time Range)                  | 時間範囲を選択します。この時間範囲に作成された RADIUS 認証レコードが使用されます。                                                                                                                     |
| 開始日時: (Start Date-Time:)           | ([時間範囲 (Time Range)] として [カスタム (Custom)] を選択した場合にのみ使用可能)<br>開始日時を入力するか、またはカレンダー アイコンをクリックして開始日時を選択します。<br>日付は <i>mm/dd/yyyy</i> 形式、時刻は <i>hh:mm</i> 形式である必要があります。 |
| 終了日時: (End Date-Time:)             | ([時間範囲 (Time Range)] として [カスタム (Custom)] を選択した場合にのみ使用可能)<br>終了日時を入力するか、またはカレンダー アイコンをクリックして終了日時を選択します。<br>日付は <i>mm/dd/yyyy</i> 形式、時刻は <i>hh:mm</i> 形式である必要があります。 |
| レコード数の取得 (Fetch Number of Records) | 表示するレコードの数を選択します。10、20、50、100、200、または 500 を選択できます。                                                                                                                |
| 検索結果                               |                                                                                                                                                                   |
| 時刻 (Time)                          | イベントの時刻                                                                                                                                                           |
| ステータス (Status)                     | ポスチャ ステータス                                                                                                                                                        |
| [ユーザ名 (Username)]                  | イベントに関連付けられたユーザ名                                                                                                                                                  |
| MAC アドレス (MAC Address)             | システムの MAC アドレス                                                                                                                                                    |
| 失敗の理由 (Failure Reason)             | イベントの障害理由                                                                                                                                                         |

#### 関連トピック

[エンドポイント ポスチャの障害のトラブルシューティング](#) (1076 ページ)

[ポスチャのトラブルシューティング ツール](#) (1076 ページ)

## TCP ダンプの設定

次の表では、ネットワーク インターフェイスのパケットの内容をモニタし、ネットワークで問題が発生したときにはトラブルシューティングするために使用する **tcpdump** ユーティリティ ページのフィールドについて説明します。このページへのナビゲーションパスは、[\[操作](#)

(Operations) ] > [トラブルシューティング (Troubleshoot) ] > [診断ツール (Diagnostic Tools) ] > [一般ツール (General Tools) ] > [TCP ダンプ (TCP Dump) ] です。

表 162: TCP ダンプの設定

| オプション                               | 使用上のガイドライン                                                                                                                                                                                                                                                      |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステータス (Status)                      | <ul style="list-style-type: none"> <li>• [停止済み (Stopped) ] : tcpdump ユーティリティは実行されていません。</li> <li>• [開始 (Start) ] : tcpdump ユーティリティによるネットワークのモニタリングを開始する場合にクリックします。</li> <li>• [停止 (Stop) ] : tcpdump ユーティリティを停止する場合にクリックします。</li> </ul>                         |
| ホスト名 (Host Name)                    | モニタするホストの名前をドロップダウン リストから選択します。                                                                                                                                                                                                                                 |
| ネットワーク インターフェイス (Network Interface) | <p>モニタするネットワーク インターフェイスの名前をドロップダウンリストから選択します。</p> <p>(注) IPv4 アドレスまたは IPv6 アドレスを持つすべてのネットワーク インターフェイスカード (NIC) を Cisco ISE 管理者ポータルに表示されるように設定する必要があります。</p>                                                                                                     |
| 無差別モード (Promiscuous Mode)           | <ul style="list-style-type: none"> <li>• [オン (On) ] : 無差別モードを有効にする場合にクリックします (デフォルト) 。</li> <li>• [オフ (Off) ] : 無差別モードを無効にする場合にクリックします。</li> </ul> <p>無差別モードがデフォルトのパケット スニッフィング モードです。有効に設定しておくことを推奨します。このモードでは、ネットワーク インターフェイスはすべてのトラフィックをシステムの CPU に渡します。</p> |
| フィルタ                                | <p>フィルタリング基準として使用するブール式を入力します。サポートされている標準 tcpdump フィルタ式 :</p> <pre>ip host 10.77.122.123 ip host 10.77.122.123 and not 10.177.122.119 ip host ISE123</pre>                                                                                                      |



| オプション                | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| フォーマット (Format)      | tcpdump ファイルのフォーマットを選択します。                                                                                                                                                                                                                                                                                                                                                                                                 |
| ダンプ ファイル (Dump File) | <p>最後のダンプ ファイルに記録された、次のようなデータを表示します。</p> <p>Last created on Wed Apr 27 20:42:38 UTC 2011 by admin</p> <p>File size: 3,744 bytes<br/>Format: Raw Packet Data<br/>Host Name: Positron<br/>Network Interface: GigabitEthernet 0<br/>Promiscuous Mode: On</p> <ul style="list-style-type: none"> <li>• [ダウンロード (Download)] : 最新のダンプ ファイルをダウンロードする場合にクリックします。</li> <li>• [削除 (Delete)] : 最新のダンプ ファイルを削除する場合にクリックします。</li> </ul> |

#### 関連トピック

[ネットワーク トラフィックのモニタリングでの TCP ダンプの使用](#) (1080 ページ)

[TCP ダンプ ファイルの保存](#) (1081 ページ)

[着信トラフィックを検証する TCP ダンプ ユーティリティ](#) (1080 ページ)

## SXP-IP マッピング

次の表では、デバイスとそのピア間のマッピングを比較するために使用する [SXP-IP マッピング (SXP-IP mappings)] ページのフィールドについて説明します。このページへのナビゲーションパスは、[操作 (Operations)] > [トラブルシューティング (Troubleshoot)] > [診断ツール (Diagnostic Tools)] > [TrustSec ツール (Trustsec Tools)] > [SXP-IP マッピング (SXP-IP mappings)] です。

#### ピア SXP デバイス

表 163: SXP-IP マッピングのピア SXP デバイス

| オプション                          | 使用上のガイドライン            |
|--------------------------------|-----------------------|
| ピア SXP デバイス (Peer SXP Devices) |                       |
| ピア IP アドレス (Peer IP Address)   | ピア SXP デバイスの IP アドレス。 |
| VRF                            | ピア デバイスの VRF インスタンス。  |

| オプション                                            | 使用上のガイドライン                                                                                                                                                                                        |
|--------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ピア SXP モード (Peer SXP Mode)                       | 送信者であるかまたは受信者であるかなどの、ピア デバイスの SXP モード。                                                                                                                                                            |
| セルフ SXP モード (Self SXP Mode)                      | 送信者であるかまたは受信者であるかなどの、ネットワーク デバイスの SXP モード。                                                                                                                                                        |
| 接続状態 (Connection State)                          | 接続のステータス。                                                                                                                                                                                         |
| 共通接続パラメータ (Common Connection Parameters)         |                                                                                                                                                                                                   |
| ユーザ共通接続パラメータ (User Common Connection Parameters) | <p>すべてのピア SXP デバイスの共通接続パラメータを有効にする場合にこのチェックボックスをオンにします。</p> <p>(注) 共通接続パラメータが指定されていない場合、または何らかの理由で共通接続パラメータが機能しない場合には、Expert Troubleshooter によって再度その特定のピアデバイスに対する接続パラメータの入力を要求するプロンプトが表示されます。</p> |
| [ユーザ名 (Username) ]                               | ピア SXP デバイスのユーザ名を入力します。                                                                                                                                                                           |
| [パスワード (Password) ]                              | ピア デバイスにアクセスするためのパスワードを入力します。                                                                                                                                                                     |
| プロトコル                                            | <ul style="list-style-type: none"> <li>プロトコルを選択します。</li> </ul> <p>(注) [Telnet] がデフォルトのオプションです。[SSHv2] を選択した場合は、ネットワーク デバイスで SSH 接続を有効にする必要があります。</p>                                              |
| [ポート (Port) ]                                    | <ul style="list-style-type: none"> <li>ポート番号を入力します。デフォルトのポート番号は、Telnet は 23、SSH は 22 です。</li> </ul>                                                                                               |
| パスワードを有効にする (Enable Password)                    | イネーブルパスワードがログインパスワードと異なる場合に入力します。                                                                                                                                                                 |
| ログインパスワードと同じ (Same as login password)            | 有効パスワードがログインパスワードと同じ場合は、このチェックボックスをオンにします。                                                                                                                                                        |

### 関連トピック

[SXP-IP マッピングを持つ TrustSec 対応ネットワークの接続問題のトラブルシューティング](#) (1083 ページ)

[SXP のサポート](#) (10 ページ)

## IP ユーザ SGT

次の表では、[IP ユーザ SGT (IP User SGT)] ページのフィールドについて説明します。これらのフィールドを使用して、デバイス上の IP-SGT 値を ISE が割り当てた SGT と比較します。このページへのナビゲーションパスは、[操作 (Operations)] > [トラブルシューティング (Troubleshoot)] > [診断ツール (Diagnostic Tools)] > [TrustSec ツール (TrustSec Tools)] > [IP ユーザ SGT (IP User SGT)] です。

表 164: IP ユーザ SGT

| オプション                              | 使用上のガイドライン                            |
|------------------------------------|---------------------------------------|
| 情報の入力                              |                                       |
| ネットワーク デバイス IP (Network Device IP) | ネットワーク デバイスの IP アドレスを入力します。           |
| 結果のフィルタリング                         |                                       |
| [ユーザ名 (Username)]                  | レコードをトラブルシューティングするユーザのユーザ名を入力します。     |
| ユーザ IP アドレス (User IP Address)      | レコードをトラブルシューティングするユーザの IP アドレスを入力します。 |
| SGT                                | ユーザ SGT 値を入力します。                      |

### 関連トピック

[IP-SGT マッピングを持つ TrustSec 対応ネットワークの接続問題のトラブルシューティング](#) (1083 ページ)

[セキュリティ グループの設定](#) (983 ページ)

## デバイス SGT の設定

次の表に、デバイス SGT を、割り当てられた最新の SGT 値と比較するために使用する [デバイス SGT (Device SGT)] ページのフィールドを示します。このページへのナビゲーションパスは、[操作 (Operations)] > [トラブルシューティング (Troubleshoot)] > [診断ツール (Diagnostic Tools)] > [TrustSec ツール (TrustSec Tools)] > [デバイス SGT (Device SGT)] です。

表 165: デバイス SGT の設定

| オプション                                            | 使用上のガイドライン                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 情報の入力                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| ネットワーク デバイス IP (Network Device IPs) (カンマ区切りのリスト) | ISE によって割り当てられたデバイス SGT と比較するデバイス SGT のネットワーク デバイス IP アドレスをカンマで区切って入力します。                                                                                                                                                                                                                                                                                                                                                                             |
| 共通接続パラメータ (Common Connection Parameters)         |                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| 共通接続パラメータを使用 (Use Common Connection Parameters)  | <p>比較時に次の共通接続パラメータを使用する場合にこのチェックボックスをオンにします。</p> <ul style="list-style-type: none"> <li>• [ユーザ名 (Username)] : ネットワーク デバイスのユーザ名を入力します。</li> <li>• [パスワード (Password)] : パスワードを入力します。</li> <li>• [プロトコル (Protocol)] : プロトコルを選択します。</li> </ul> <p>(注) [Telnet] がデフォルトのオプションです。[SSHv2] を選択した場合は、ネットワーク デバイスで SSH 接続を有効にする必要があります。</p> <ul style="list-style-type: none"> <li>• [ポート (Port)] : ポート番号を入力します。デフォルトのポート番号は、Telnet は 23、SSH は 22 です。</li> </ul> |
| パスワードを有効にする (Enable Password)                    | イネーブルパスワードがログインパスワードと異なる場合に入力します。                                                                                                                                                                                                                                                                                                                                                                                                                     |
| ログインパスワードと同じ (Same as login password)            | 有効パスワードがログインパスワードと同じ場合は、このチェックボックスをオンにします。                                                                                                                                                                                                                                                                                                                                                                                                            |

## 関連トピック

[デバイス SGT マッピングの比較による TrustSec 対応ネットワークの接続問題のトラブルシューティング](#) (1084 ページ)

[デバイス SGT ツール](#) (1084 ページ)

## 進行状況の詳細の設定

次の表では、いずれかの診断ツールの[ユーザ入力必須 (User Input Required)] ボタンをクリックすると表示される[進行状況詳細 (Progress Details)] ページのフィールドについて説明します。このページには、詳細なトラブルシューティング情報が表示されます。このページへのナビゲーションパスは、[操作 (Operations)] > [トラブルシューティング (Troubleshoot)] > [診断ツール (Diagnostic Tools)] > [任意の診断ツール (Any Diagnostic Tool)] です。

表 166: 進行状況の詳細の設定

| オプション                                                                               | 使用上のガイドライン                                                                                         |
|-------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|
| ネットワーク デバイス a.b.c.d の接続パラメータの指定                                                     |                                                                                                    |
| [ユーザ名 (Username)]                                                                   | ネットワーク デバイスにログインするためのユーザ名を入力します。                                                                   |
| [パスワード (Password)]                                                                  | パスワードを入力します。                                                                                       |
| プロトコル                                                                               | プロトコルを選択します。<br><br>(注) [Telnet] がデフォルトのオプションです。[SSHv2] を選択した場合は、ネットワーク デバイスで SSH 接続を有効にする必要があります。 |
| [ポート (Port)]                                                                        | ポート番号を入力します。                                                                                       |
| パスワードを有効にする (Enable Password)                                                       | イネーブル パスワードを入力します。                                                                                 |
| ログイン パスワードと同じ (Same As Login Password)                                              | イネーブルパスワードがログインパスワードと同じ場合は、このチェックボックスをオンにします。                                                      |
| コンソールサーバを使用 (Use Console Server)                                                    | コンソールサーバを使用する場合にこのチェックボックスをオンにします。                                                                 |
| コンソール IP アドレス (Console IP Address)                                                  | ([コンソールサーバを使用 (Use Console Server)] チェックボックスをオンにした場合) コンソールの IP アドレスを入力します。                        |
| 高度なオプション (「タイムアウトエラー (Expect timeout error)」が表示される場合や、デバイスから非標準のプロンプト文字列が返される場合に使用) |                                                                                                    |
| (注) 高度なオプションは、一部のトラブルシューティングツールに対してだけ表示されます。                                        |                                                                                                    |

| オプション                                           | 使用上のガイドライン                                                                      |
|-------------------------------------------------|---------------------------------------------------------------------------------|
| ユーザ名用文字列 (Username Expect String)               | Username: や Login: などの、ネットワーク デバイスによってユーザ名入力用プロンプトとして使用される文字列を入力します。            |
| パスワード用文字列 (Password Expect String)              | Password: などの、ネットワーク デバイスによってパスワード入力用プロンプトとして使用される文字列を入力します。                    |
| プロンプト用文字列 (Prompt Expect String)                | ネットワーク デバイスで使用されるプロンプトを入力します。たとえば、#、>、@ を入力します。                                 |
| 認証失敗用文字列 (Authentication Failure Expect String) | Incorrect password や Login invalid などの、認証エラーが発生した場合にネットワーク デバイスから返される文字列を入力します。 |

### 関連トピック

[予期せぬ RADIUS 認証結果のトラブルシューティング](#) (1075 ページ)

[設定を確認する IOS show コマンドの実行](#) (1075 ページ)

[ネットワーク デバイス設定の問題のトラブルシューティング](#) (1076 ページ)

[SXP-IP マッピングを持つ TrustSec 対応ネットワークの接続問題のトラブルシューティング](#) (1083 ページ)

[IP-SGT マッピングを持つ TrustSec 対応ネットワークの接続問題のトラブルシューティング](#) (1083 ページ)

[診断トラブルシューティング ツール](#) (1074 ページ)

## 結果概要 (Results Summary)

次の表では、診断ツールを使用したときに結果として表示される結果概要ページのフィールドについて説明します。

表 167: [RADIUS 認証のトラブルシューティング (RADIUS Authentication Troubleshooting)] : [結果概要 (Results Summary)]

| オプション                                    | 使用上のガイドライン            |
|------------------------------------------|-----------------------|
| 診断と解決策 (Diagnosis and Resolution)        |                       |
| 診断 (Diagnosis)                           | 問題の診断がここに表示されます。      |
| 解像度                                      | 問題の解決手順がここに詳細に表示されます。 |
| トラブルシューティングの概要 (Troubleshooting Summary) |                       |

| オプション | 使用上のガイドライン                                                                                     |
|-------|------------------------------------------------------------------------------------------------|
| 要約    | <p>トラブルシューティング情報の各ステップの概要がここに表示されます。任意のステップを展開して、詳細を表示できます。</p> <p>すべての設定エラーが赤いテキストで示されます。</p> |

**関連トピック**

[予期せぬ RADIUS 認証結果のトラブルシューティング](#) (1075 ページ)

[RADIUS 認証のトラブルシューティング ツール](#) (1074 ページ)







## 第 35 章

# ネットワーク アクセス フロー

- [パスワード ベースの認証 \(1475 ページ\)](#)
- [Cisco ISE の RADIUS プロトコルのサポート \(1476 ページ\)](#)
- [ユーザのネットワーク アクセス \(1476 ページ\)](#)

## パスワード ベースの認証

認証とは、ユーザ情報を検証してユーザ ID を確認することです。従来の認証方式では、名前とある決まったパスワードが使用されていました。これは、最も一般的かつ単純で、低コストの認証方式です。この方式の欠点は、ユーザ名やパスワードの情報が簡単に第三者に伝えられたり、推測または不正に取得されたりする可能性がある点です。単純な暗号化されていないユーザ名とパスワードを使用する方法は、強力な認証方式とは考えられていませんが、インターネットアクセスなど、許可または特権レベルが低い場合は十分に要件を満たす可能性があります。

## 暗号化されたパスワードと暗号化技術を使用したセキュアな認証

ネットワーク上でパスワードが不正に取得される危険性を低減するには、暗号化を使用する必要があります。RADIUS などのクライアント/サーバアクセス コントロール プロトコルでは、パスワードを暗号化することにより、ネットワーク内でパスワードが不正に取得される事態を防止します。ただし、RADIUS は認証、許可、およびアカウントティング (AAA) クライアントと Cisco ISE との間でだけ動作します。認証プロセスでは、このポイントの前で、許可されていないユーザが次のような例で暗号化されていないパスワードを入手する可能性があります。

- 電話回線を介してダイヤルアップ接続を行うエンドユーザ クライアントとの間の通信
- ネットワーク アクセス サーバで終了する ISDN 回線
- エンドユーザ クライアントとホスティング デバイスの間の Telnet セッションを介して行われる通信

さらに安全な方式では、チャレンジハンドシェイク認証プロトコル (CHAP)、ワンタイムパスワード (OTP)、および高度な EAP ベースのプロトコルの内部で使われるような暗号化技術を使用します。Cisco ISE は、これらのさまざまな認証方式をサポートしています。

## 認証方式と許可特権

認証と許可には基本的な暗黙の関係があります。ユーザに与えられる許可特権が多くなればなるほど、それに応じて認証を強化する必要があります。Cisco ISE では、さまざまな認証方式を提供することにより、この関係がサポートされています。

## Cisco ISE の RADIUS プロトコルのサポート

RADIUS は、クライアント/サーバプロトコルです。リモートアクセス サーバは、このプロトコルを使用して中央サーバと通信してダイヤルインユーザを認証し、要求されたシステムまたはサービスへのアクセスを許可します。RADIUS を使用すると、すべてのリモートサーバが共有できる中央データベースでユーザプロファイルを管理できます。このプロトコルはセキュリティを向上させます。また、このプロトコルを使用して、単一の管理ネットワーク ポイントで適用されるポリシーを設定できます。

RADIUS は、Cisco ISE の RADIUS クライアントとしても機能し、リモート RADIUS サーバへの要求をプロキシ処理します。また、アクティブセッション中に許可変更 (CoA) アクティビティを提供します。

Cisco ISE では、RFC 2865 と、その仕様および拡張仕様に記載されているすべての一般的な RADIUS 属性の包括的なサポートに従って、RADIUS プロトコルのフローがサポートされます。Cisco ISE では、Cisco ISE ディクショナリで定義されているベンダーだけを対象に、ベンダー固有属性の解析がサポートされます。

RADIUS インターフェイスでは、RFC 2865 で定義されている次の属性データ型がサポートされます。

- テキスト (Unicode Transformation Format (UTF) )
- 文字列 (バイナリ)
- アドレス (IP)
- 整数 (Integer)
- 時刻 (Time)

### ISE コミュニティ リソース

Cisco ISE でサポートされるネットワーク アクセス属性については、「[ISE Network Access Attributes](#)」を参照してください。

## ユーザのネットワーク アクセス

ネットワーク アクセスでは、ホストはネットワーク デバイスに接続し、ネットワーク リソースの使用を要求します。ネットワーク デバイスは、新しく接続されたホストを識別し、転送方式として RADIUS プロトコルを使用して、ユーザの認証および許可を Cisco ISE に要求します。

Cisco ISE では、RADIUS プロトコルを使用して転送されるプロトコルに応じて、ネットワーク アクセス フローがサポートされます。

## EAP を使用しない RADIUS ベースのプロトコル

EAP を含まない RADIUS ベースのプロトコルは、次のとおりです。

- Password Authentication Protocol (PAP)
- CHAP
- Microsoft Challenge Handshake Authentication Protocol version 1 (MS-CHAPv1)
- MS-CHAP バージョン 2 (MS-CHAPv2)

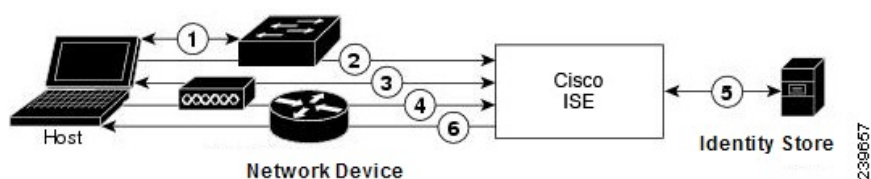
## RADIUS-Based Non-EAP 認証フロー

ここでは、EAP 認証を使用しない RADIUS ベースのフローについて説明します。PAP 認証を使用する RADIUS ベースのフローは、次のプロセスで発生します。

1. ホストがネットワーク デバイスに接続します。
2. ネットワーク デバイスが RADIUS 要求 (Access-Request) を Cisco ISE に送信します。この要求には、使用する特定のプロトコル (PAP、CHAP、MS-CHAPv1、または MS-CHAPv2) に適した RADIUS 属性が含まれます。
3. Cisco ISE では、ID ストアを使用してユーザ クレデンシアルを検証します。
4. RADIUS 応答 (Access-Accept または Access-Reject) が、決定を適用するネットワーク デバイスに送信されます。

次の図は、EAP を使用しない RADIUS ベースの認証を示しています。

図 68: EAP を使用しない RADIUS ベースの認証



Cisco ISE でサポートされる非 EAP プロトコルは次のとおりです。

## パスワード認証プロトコル

PAP では、ユーザが双方向ハンドシェイクを使用して ID を確立できる単純な方法が提供されます。PAP パスワードは共有秘密を使用して暗号化されるため、最もセキュリティ レベルの

低い認証プロトコルです。PAPは、反復的な試行錯誤攻撃に対する保護がほとんどないため、確実な認証方式ではありません。

## Cisco ISE の RADIUS-Based PAP 認証

Cisco ISE では、ID ストアに対してユーザ名とパスワードのペアをチェックし、最終的にその認証を確認するか、接続を終了します。

Cisco ISE では、異なるセキュリティ レベルを同時に使用して、さまざまな要件に対応できます。PAP は双方向ハンドシェイク手順を適用します。認証に成功した場合、Cisco ISE は確認応答を返します。認証に失敗した場合、Cisco ISE は接続を終了するか、認証の要求元にもう一度チャンスを与えます。

認証の要求元が、試行の頻度とタイミングを総合的に制御します。したがって、より強力な認証方式を使用できるサーバは、PAP よりも前にその方式のネゴシエーションを提案します。PAP は RFC 1334 で定義されています。

Cisco ISE では、RADIUS UserPassword 属性に基づく標準の RADIUS PAP 認証がサポートされます。RADIUS PAP 認証は、すべての ID ストアと互換性があります。

PAP 認証フローを使用する RADIUS には、試行の成功と失敗のログギングが含まれます。

## チャレンジハンドシェイク認証プロトコル

CHAPは、応答時に一方向の暗号化を使用するチャレンジ/レスポンス方式です。CHAPを使用することで、Cisco ISE は、セキュリティ レベルの高い順からセキュリティ暗号化方式をネゴシエートし、プロセス中に伝送されるパスワードを保護します。CHAPパスワードは再利用が可能です。Cisco ISE 内部データベースを認証に使用する場合は、PAP または CHAP のどちらかを使用できます。CHAP は、Microsoft ユーザデータベースでは使用できません。RADIUS PAP と比較した場合、エンドユーザ クライアントから AAA クライアントに通信するときに CHAPを使用すると、パスワードが暗号化されるため、高いセキュリティ レベルを確保できます。

Cisco ISE では、RADIUS ChapPassword 属性に基づく標準の RADIUS CHAP 認証がサポートされます。Cisco ISE では、外部 ID ストアを使用した RADIUS CHAP 認証だけがサポートされます。

## Microsoft Challenge Handshake Authentication Protocol Version 1

Cisco ISE では、RADIUS MS-CHAPv1 認証およびパスワード変更機能がサポートされます。RADIUS MS-CHAPv1 には、Change-Password-V1 と Change-Password-V2 の 2 つのバージョンのパスワード変更機能が含まれます。Cisco ISE は RADIUS MS-CHAP-CPW-1 属性に基づいた Change-Password-V1 パスワード変更をサポートせず、MS-CHAP-CPW-2 属性に基づいた Change-Password-V2 のみをサポートします。RADIUS MS-CHAPv1 認証およびパスワード変更機能は、次の ID ソースを使用してサポートされます。

- 内部 ID ストア
- Microsoft Active Directory ID ストア

## Microsoft Challenge Handshake Authentication Protocol Version 2

RADIUS MS-CHAPv2 認証およびパスワード変更機能は、次の ID ソースでサポートされます。

- 内部 ID ストア
- Microsoft Active Directory ID ストア

## RADIUS ベースの EAP プロトコル

EAP では、さまざまな認証タイプをサポートする拡張可能なフレームワークが提供されます。ここでは、Cisco ISE でサポートされる EAP 方式について説明します。次のトピックを扱います。

### 単純な EAP 方式

- EAP-Message Digest 5
- Lightweight EAP

### 認証に Cisco ISE サーバ証明書を使用する EAP 方式

- PEAP/EAP-MS-CHAPv2
- PEAP/EAP-GTC
- EAP-FAST/EAP-MS-CHAPv2
- EAP-FAST/EAP-GTC

上記にリストした方式とは別に、サーバ認証とクライアント認証の両方に証明書を使用する EAP 方式があります。

## RADIUS-Based EAP 認証フロー

認証プロセスで EAP が使用される場合は常に、そのプロセスよりも、具体的にどの EAP 方式（および該当する場合は内部方式）を使用する必要があるかを決定するネゴシエーションフェーズが先行します。EAP ベースの認証は、次のプロセスで発生します。

1. ホストがネットワーク デバイスに接続します。
2. ネットワーク デバイスが EAP 要求をホストに送信します。
3. ホストは、EAP 応答によって、ネットワーク デバイスに応答します。
4. ネットワーク デバイスは、ホストから受信した EAP 応答を RADIUS Access-Request 内に（EAP-Message RADIUS 属性を使用して）カプセル化し、RADIUS Access-Request を Cisco ISE に送信します。

5. Cisco ISE は、RADIUS パケットから EAP 応答を抽出して新しい EAP 要求を作成し、この EAP 要求を RADIUS Access-Challenge 内に（この場合も EAP-Message RADIUS 属性を使用して）カプセル化し、ネットワーク デバイスに送信します。
6. ネットワーク デバイスは、EAP 要求を抽出し、ホストへ送信します。

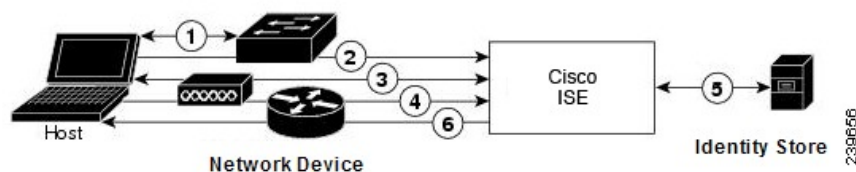
この方法で、ホストと Cisco ISE は間接的に EAP メッセージを交換します（EAP メッセージは、RADIUS を使用して転送され、ネットワーク デバイスを介して渡されます）。この方法で交換される EAP メッセージの最初のセットによって、特定の EAP 方式がネゴシエートされます。その後、認証を実行する場合に、この EAP 方式が使用されます。

その後交換される EAP メッセージは、実際の認証の実行に必要なデータを伝送するために使用されます。ネゴシエートされた特定の EAP 認証方式で必要な場合、Cisco ISE では ID ストアを使用してユーザ クレデンシャルを検証します。

Cisco ISE では、認証が成功か失敗かを決定した後、EAP-Success または EAP-Failure メッセージを、RADIUS Access-Accept または Access-Reject メッセージ内にカプセル化された状態で、ネットワーク デバイスに（最終的にはホストにも）送信します。

次の図は、EAP を使用する RADIUS ベースの認証を示しています。

図 69: EAP を使用する RADIUS ベースの認証



## Extensible Authentication Protocol-Message Digest 5

Extensible Authentication Protocol-Message Digest 5 (EAP-MD5) では、一方向のクライアント認証が提供されます。サーバは、クライアントにランダムチャレンジを送信します。クライアントは、チャレンジとそのパスワードを MD5 で暗号化することによって、応答でその ID を証明します。中間者がチャレンジと応答を見ることができると、EAP-MD5 は、公開メディアで使用される場合にはディクショナリ攻撃に対して脆弱です。サーバ認証が行われないため、スプーフィングに対しても脆弱です。Cisco ISE では、Cisco ISE 内部 ID ストアに対する EAP-MD5 認証がサポートされます。EAP-MD5 プロトコルを使用している場合は、ホストルックアップもサポートされます。

## Lightweight Extensible Authentication Protocol

Cisco ISE では現在、Lightweight Extensible Authentication Protocol (LEAP) を Cisco Aironet ワイヤレス ネットワーキングに対してだけ使用します。このオプションを有効にしないと、LEAP 認証を実行するように設定された Cisco Aironet エンドユーザクライアントは、ネットワークにアクセスできなくなります。Cisco Aironet エンドユーザクライアントすべてが Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) などの異なる認証プロトコルを使用する場合は、このオプションを無効にすることを推奨します。



- (注) [ネットワーク デバイス (Network Devices)] セクションで RADIUS (Cisco Aironet) デバイスとして定義された AAA クライアントを使用してユーザがネットワークにアクセスする場合は、LEAP、EAP-TLS、またはその両方を有効にする必要があります。これ以外の場合、Cisco Aironet ユーザは認証を受けることができません。

## 保護拡張認証プロトコル

保護拡張認証プロトコル (PEAP) では、相互認証が提供され、脆弱なユーザ クレデンシャルの機密性と整合性が保証されます。またこのプロトコルでは、自身をパッシブ (盗聴) およびアクティブ (中間者) 攻撃から保護し、セキュアに暗号キー関連情報を生成します。PEAP は、IEEE 802.1X 標準および RADIUS プロトコルと互換性があります。Cisco ISE では、Extensible Authentication Protocol-Microsoft Challenge Handshake Authentication Protocol (EAP-MS-CHAP)、Extensible Authentication Protocol-Generic Token Card (EAP-GTC)、および EAP-TLS 内部方式で PEAP バージョン 0 (PEAPv0) と PEAP バージョン 1 (PEAPv1) がサポートされます。Cisco Secure Services Client (SSC) サプリカントでは、Cisco ISE でサポートされるすべての PEAPv1 内部方式がサポートされます。

## PEAP の使用の利点

PEAP を使用すると、次のような利点があります。PEAP は、広く実装されセキュリティが細部にわたって確認された TLS に基づいています。キーを生成しない方式に対しては、キーを確立します。トンネル内で ID を送信します。内部方式の交換と結果メッセージを保護します。フラグメンテーションがサポートされます。

## PEAP プロトコルでサポートされているサプリカント

PEAP では、次のサプリカントがサポートされます。

- Microsoft Built-In Clients 802.1X XP
- Microsoft Built-In Clients 802.1X Vista
- Cisco Secure Services Client (SSC) Release 4.0
- Cisco SSC リリース 5.1
- Funk Odyssey Access Client リリース 4.72
- Intel リリース 12.4.0.0

## PEAP プロトコルのフロー

PEAP カンバセーションは、次の 3 つの部分に分かれます。

1. Cisco ISE とピアが TLS トンネルを構築します。Cisco ISE は自身の証明書を提示しますが、ピアは提示しません。ピアと Cisco ISE はキーを作成して、トンネル内のデータを暗号化します。
2. 内部方式によって、次のようにトンネル内のフローが決定されます。

- EAP-MS-CHAPv2 内部方式：EAP-MS-CHAPv2 パケットは、ヘッダーなしでトンネル内を移動します。ヘッダーの先頭のバイトにタイプ フィールドが含まれます。EAP-MS-CHAPv2 内部方式では、パスワード変更機能がサポートされます。ユーザが管理者ポータルでパスワードの変更を試行できる回数を設定できます。ユーザ認証の試行回数はこの数値によって制限されます。
- EAP-GTC 内部方式：PEAPv0 と PEAPv1 の両方で、EAP-GTC 内部方式がサポートされます。サポートされるサブリカントでは、EAP-GTC 内部方式を使用する PEAPv0 はサポートされません。EAP-GTC では、パスワード変更機能がサポートされます。ユーザが管理者ポータルでパスワードの変更を試行できる回数を設定できます。ユーザ認証の試行回数はこの数値によって制限されます。
- EAP-TLS 内部方式：Windows 組み込みサブリカントでは、トンネルが確立された後のメッセージのフラグメンテーションはサポートされず、このことは EAP-TLS 内部方式に影響を与えます。Cisco ISE では、トンネルが確立された後の外部 PEAP メッセージのフラグメンテーションはサポートされません。トンネルの確立中、フラグメンテーションは PEAP のマニュアルで指定されているとおりに動作します。PEAPv0 では EAP-TLS パケットのヘッダーが削除され、PEAPv1 では EAP-TLS パケットがそのまま送信されます。
- Extensible Authentication Protocol-type, length, value (EAP-TLV) 拡張：EAP-TLV パケットはそのまま送信されます。EAP-TLV パケットは、トンネル内をヘッダー付きで移動します。

3. カンバセーションが内部方式に到達した場合、保護された成功と失敗の確認応答があります。

クライアント EAP メッセージは常に RADIUS Access-Request メッセージで送信され、サーバ EAP メッセージは常に RADIUS Access-Challenge メッセージで送信されます。EAP-Success メッセージは、常に RADIUS Access-Accept メッセージで送信されます。EAP-Failure メッセージは、常に RADIUS Access-Reject メッセージで送信されます。クライアント PEAP メッセージをドロップすると、RADIUS クライアント メッセージがドロップされます。



- (注) Cisco ISE は、PEAPv1 通信中に EAP-Success または EAP-Failure メッセージの確認を要求します。ピアは、成功または失敗メッセージの受信を確認するために空の TLS データ フィールドを含む PEAP パケットを返送する必要があります。

## Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling

Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) は、相互認証を提供する認証プロトコルであり、共有秘密を使用してトンネルを確立します。このトンネルは、パスワードに基づく弱い認証方式を保護するために使用されます。Protected Access Credentials (PAC) キーと呼ばれる共有秘密は、トンネルのセキュリティを確保するときにクライアントとサーバを相互認証するために使用されます。



## EAP-FAST の利点

EAP-FAST は、他の認証プロトコルに比べて次の利点があります。

- 相互認証：EAP サーバはピアの ID と信頼性を確認できる必要があります、ピアは EAP サーバの信頼性を確認できる必要があります。
- パッシブ ディクショナリ攻撃に対する耐性：多くの認証プロトコルでは、ピアから EAP サーバにパスワードがクリアテキストまたはハッシュとして明示的に提供される必要があります。
- 中間者攻撃に対する耐性：相互認証された保護トンネルの確立時に、プロトコルは、ピアと EAP サーバとの間のカンバセーションに攻撃者が情報を挿入することを防ぐ必要があります。
- MS-CHAPv2 や汎用トークンカード (GTC) などの多くの異なるパスワード認証インターフェイスをサポートできる柔軟性：EAP-FAST は、同じサーバで複数の内部プロトコルをサポートできる拡張可能なフレームワークです。
- 効率性：無線メディアを使用する場合、ピアは計算資源と電源リソースを制限されます。EAP-FAST では、ネットワーク アクセス通信の計算を軽量化できます。
- 認証サーバのユーザごとの認証状態要件の最小化：大規模な展開では、通常、多くのサーバが多くのピアに対する認証サーバとして機能する必要があります。ユーザ名とパスワードを使用してネットワークにアクセスするのと同じように、ピアが同じ共有秘密を使用してトンネルのセキュリティを確保することも強く推奨されます。EAP-FAST により、サーバでキャッシュおよび管理する必要があるユーザごとおよびデバイスごとの状態を最小にすることができ、ピアによる強力な単一共有秘密の使用が容易になります。

## EAP-FAST フロー

EAP-FAST プロトコルのフローは常に、次のフェーズを組み合わせたものになります。

1. プロビジョニング フェーズ：これは EAP-FAST のフェーズ 0 です。このフェーズでは、Cisco ISE とピアとの間で共有される、PAC と呼ばれる一意の強力な秘密を使用して、ピアがプロビジョニングされます。
2. トンネル確立フェーズ：PAC を使用して新しいトンネルキーを確立することによって、クライアントとサーバを相互認証します。トンネルキーはその後、残りのカンバセーションを保護するために使用され、メッセージの機密性と信頼性を提供します。
3. 認証フェーズ：認証がトンネル内で処理され、セッションキーの生成と保護された終了が行われます。Cisco ISE では、EAP-FAST バージョン 1 および 1a がサポートされます。





## 第 36 章

# Cisco ISE の機能をサポートするために必要なスイッチとワイヤレス LAN コントローラの設定

Cisco ISE がネットワーク スイッチと相互運用し、Cisco ISE の機能がネットワーク セグメント全体で正常に動作することを保証するには、Cisco ISE との通信に必要な NTP、RADIUS/AAA、802.1X、MAB などの設定を使用して、ネットワーク スイッチを設定する必要があります。

- [スイッチでの標準 Web 認証のサポートの有効化 \(1486 ページ\)](#)
- [代理 RADIUS トランザクション用のローカルユーザ名とパスワードの定義 \(1486 ページ\)](#)
- [ログとアカウンティングのタイムスタンプの正確性を保証するための NTP サーバ設定 \(1486 ページ\)](#)
- [AAA 機能を有効にするコマンド \(1486 ページ\)](#)
- [スイッチ上の RADIUS サーバの設定 \(1487 ページ\)](#)
- [RADIUS 許可変更 \(CoA\) を有効にするコマンド \(1488 ページ\)](#)
- [デバイストラッキングと DHCP スヌーピングを有効にするコマンド \(1488 ページ\)](#)
- [802.1X ポートベースの認証を有効にするコマンド \(1489 ページ\)](#)
- [クリティカルな認証の EAP を有効にするコマンド \(1489 ページ\)](#)
- [リカバリ遅延を使用して AAA 要求をスロットリングするコマンド \(1489 ページ\)](#)
- [適用状態に基づく VLAN の定義 \(1489 ページ\)](#)
- [スイッチのローカル \(デフォルト\) ACL 定義 \(1490 ページ\)](#)
- [802.1X および MAB のスイッチ ポートを有効にする \(1492 ページ\)](#)
- [EPM ログギングを有効にするコマンド \(1494 ページ\)](#)
- [SNMP トラップを有効にするコマンド \(1494 ページ\)](#)
- [プロファイリング用の SNMP v3 クエリーを有効にするコマンド \(1494 ページ\)](#)
- [プロファイラによる収集を可能にするための MAC 通知トラップを有効にするコマンド \(1495 ページ\)](#)
- [スイッチ上での RADIUS Idle-timeout の設定 \(1495 ページ\)](#)
- [iOS サプリカントプロビジョニングのためのワイヤレス LAN コントローラ設定 \(1496 ページ\)](#)

- [MDM Interoperability のためのワイヤレス LAN コントローラでの ACL の設定](#) (1496 ページ)

## スイッチでの標準 Web 認証のサポートの有効化

認証時の URL リダイレクションのプロビジョニングなど、Cisco ISE 用の標準 Web 認証機能を有効にするには、次のコマンドをスイッチのコンフィギュレーションに含めます。

```
ip classless
```

```
ip route 0.0.0.0 0.0.0.0 10.1.2.3
```

```
ip http server
```

! Must enable HTTP/HTTPS for URL-redirection on port 80/443

```
ip http secure-server
```

## 代理 RADIUS トランザクション用のローカル ユーザ名とパスワードの定義

スイッチがこのネットワーク セグメントの RADIUS サーバであるかのように Cisco ISE ノードと通信するには、次のコマンドを入力します。

```
username test-radius password 0 abcde123
```

## ログとアカウンティングのタイムスタンプの正確性を保証するための NTP サーバ設定

次のコマンドを入力して、[管理 (Administration)] > [システム (System)] > [設定 (Settings)] > [システム時刻 (System Time)] で Cisco ISE に設定したのと同じ NTP サーバを指定していることを確認してください。

```
ntp server <IP_address>|<domain_name>
```

## AAA 機能を有効にするコマンド

802.1X および MAB 認証機能など、スイッチと Cisco ISE との間でさまざまな AAA 機能を有効にするには、次のコマンドを入力します。

```
aaa new-model
```

```
! Creates an 802.1X port-based authentication method list
aaa authentication dot1x default group radius

! Required for VLAN/ACL assignment

aaa authorization network default group radius

! Authentication & authorization for webauth transactions

aaa authorization auth-proxy default group radius

! Enables accounting for 802.1X and MAB authentications

aaa accounting dot1x default start-stop group radius

!

aaa session-id common

!

aaa accounting update periodic 5

! Update AAA accounting information periodically every 5 minutes

aaa accounting system default start-stop group radius

!

aaa server radius dynamic-author <cr>

client 10.0.56.17 server-key cisco

! Enables Cisco ISE to act as a AAA server when interacting with the client at IP address
10.0.56.17
```

## スイッチ上の RADIUS サーバの設定

Cisco ISE と相互運用し、RADIUS ソース サーバとして動作するようスイッチを設定するには、次のコマンドを入力します。

```
!
radius-server attribute 6 on-for-login-auth

! Include RADIUS attribute 8 in every Access-Request

radius-server attribute 8 include-in-access-req

! Include RADIUS attribute 25 in every Access-Request

radius-server attribute 25 access-request include

! Wait 3 x 30 seconds before marking RADIUS server as dead
```

```
radius-server dead-criteria time 30 tries 3

! Use RFC-standard ports (1812/1813)
radius-server host <Cisco_ISE_IP_address> auth-port 1812 acct-port 1813 test
username test-radius key 0 <RADIUS-KEY>

!
radius-server vsa send accounting
!
radius-server vsa send authentication
!
! send RADIUS requests from the MANAGEMENT VLAN

ip radius source-interface <VLAN_number>
```



(注) 3回の再試行を含む30秒のデッド基準時間を設定し、Active Directory を認証に使用する RADIUS 要求に対して、より長い応答時間を提供することを推奨します。

## RADIUS 許可変更 (CoA) を有効にするコマンド

スイッチが RADIUS 許可変更動作を適切に処理し、Cisco ISE のポスチャ機能をサポートできるようにするための設定を指定するには、次のコマンドを入力します。

```
aaa server radius dynamic-author
```

```
client <ISE-IP> server-key 0 abcde123
```



(注) Cisco ISE では、RFC の CoA 用デフォルトポート 3799 に対して、ポート 1700 (Cisco IOS ソフトウェアのデフォルト) を使用します。既存の Cisco Secure ACS 5.x ユーザは、既存の ACS の実装の一部として CoA を使用している場合、すでにこれをポート 3799 に設定している可能性があります。

## デバイス トラッキングと DHCP スヌーピングを有効にするコマンド

セキュリティに関連する Cisco ISE のオプション機能を提供できるようにするには、次のコマンドを入力することによって、デバイス トラッキングと DHCP スヌーピングを有効にし、スイッチ ポートのダイナミック ACL 内で IP 置換を実現します。

```
! Optional
```

```
ip dhcp snooping
```

```
! Required!
```

```
ip device tracking
```

RADIUS アカウンティングでは、DHCP スヌーピングが有効になっていても、DHCP 属性は IOS センサーによって Cisco ISE に送信されません。このような場合、DHCP スヌーピングを VLAN で有効にして DHCP をアクティブにする必要があります。

VLAN で DHCP スヌーピングを有効にするには、次のコマンドを使用します。

```
ip dhcp snooping
```

```
ip dhcp snooping vlan 1-100
```

(データおよび VLAN に使用する範囲を含める必要があります)

## 802.1X ポートベースの認証を有効にするコマンド

スイッチ ポートに対してグローバルに 802.1X 認証を有効にするには、次のコマンドを入力します。

```
dot1x system-auth-control
```

## クリティカルな認証の EAP を有効にするコマンド

サブリカントによる LAN 経由での認証要求をサポートするには、次のコマンドを入力することによって、EAP をクリティカルな認証（アクセスできない認証バイパス）に対して有効にします。

```
dot1x critical eapol
```

## リカバリ遅延を使用して AAA 要求をスロットリングするコマンド

クリティカルな認証リカバリ イベントが発生した場合、次のコマンドを入力することによって、自動的に遅延（秒単位）を発生させるようスイッチを設定し、Cisco ISE がリカバリ後にサービスを再起動できるようにすることが可能です。

```
authentication critical recovery delay 1000
```

## 適用状態に基づく VLAN の定義

ネットワーク内の既知の適用状態に基づいて VLAN 名、番号、および SVI を定義するには、次のコマンドを入力します。ネットワーク間のルーティングを有効にするには、それぞれの VLAN インターフェイスを作成します。これは特に、同じネットワーク セグメントを経由し

て渡される、複数のソースからのトラフィックを処理する場合に役立ちます。たとえば、PC とその PC がネットワークへの接続時に経由する IP 電話の両方からのトラフィックが考えられます。

```

vlan <VLAN_number>

name ACCESS!

vlan <VLAN_number>

name VOICE

!

interface <VLAN_number>

description ACCESS

ip address 10.1.2.3 255.255.255.0

ip helper-address <DHCP_Server_IP_address>

ip helper-address <Cisco_ISE_IP_address>

!

interface <VLAN_number>

description VOICE

ip address 10.2.3.4 255.255.255.0

ip helper-address <DHCP_Server_IP_address>

```

## スイッチのローカル（デフォルト）ACL 定義

このような機能を古いバージョンのスイッチ（Cisco IOS ソフトウェア リリースのバージョンが 12.2(55)SE よりも前）で有効にし、Cisco ISE が認証と許可に必要なダイナミック ACL の更新を実行できるようにするには、次のコマンドを入力します。

```

ip access-list extended ACL-ALLOW

permit ip any any

!

```



```
ip access-list extended ACL-DEFAULT

 remark DHCP

 permit udp any eq bootpc any eq bootps

 remark DNS

 permit udp any any eq domain

 remark Ping

 permit icmp any any

 remark Ping

 permit icmp any any

 remark PXE / TFTP

 permit udp any any eq tftp

 remark Allow HTTP/S to ISE and WebAuth portal

 permit tcp any host <Cisco_ISE_IP_address> eq www

 permit tcp any host <Cisco_ISE_IP_address> eq 443

 permit tcp any host <Cisco_ISE_IP_address> eq 8443

 permit tcp any host <Cisco_ISE_IP_address> eq 8905

 permit udp any host <Cisco_ISE_IP_address> eq 8905

 permit udp any host <Cisco_ISE_IP_address> eq 8906

 permit tcp any host <Cisco_ISE_IP_address> eq 8080
```

```
permit udp any host <Cisco_ISE_IP_address> eq 9996
```

```
remark Drop all the rest
```

```
deny ip any any log
```

```
!
```

```
! The ACL to allow URL-redirection for WebAuth
```

```
ip access-list extended ACL-WEBAUTH-REDIRECT
```

```
permit tcp any any eq www
```

```
permit tcp any any eq 443
```



(注) WLC でこの設定を行うと、CPU 使用率が増加し、システムが不安定になるリスクが高まります。これは IOS の問題で、Cisco ISE は悪影響を受けません。

## 802.1X および MAB のスイッチ ポートを有効にする

802.1X および MAB のスイッチ ポートを有効にするには、以下の手順を実行します。

- ステップ 1 すべてのアクセス スイッチ ポートのコンフィギュレーション モードを開始します。  
**interface range FastEthernet0/1-8**
- ステップ 2 次のように、（トランク モードではなく）アクセス モードのスイッチ ポートを有効にします。  
**switchport mode access**
- ステップ 3 静的にアクセス VLAN を設定します。アクセス VLAN のローカル プロビジョニングを提供するこの手順は、オープン モード認証に必要となります。  
**switchport access <VLAN\_number>**
- ステップ 4 静的に音声 VLAN を設定します。  
**switchport voice <VLAN\_number>**
- ステップ 5 オープンモード認証を有効にします。オープンモードを使用すると、認証が完了する前に、トラフィックをデータおよび音声 VLAN 上にブリッジングできます。実稼働環境では、ポートベースの ACL を使用して不正アクセスを防ぐことを強く推奨します。  
! Enables pre-auth access before AAA response; subject to port ACL  
**authentication open**
- ステップ 6 ポートベースの ACL を適用して、認証されていないエンドポイントからアクセス VLAN 上にデフォルトでどのトラフィックをブリッジングするかを決定します。最初にすべてのアクセスを許可してからポ

リシーを適用する必要があるため、ACL-ALLOW を適用して、スイッチ ポートを通過するすべてのトラフィックを許可する必要があります。すでに現時点のすべてのトラフィックを許可するデフォルトの ISE 許可を作成しましたが、この理由は、完全な可視性を実現し、既存のエンドユーザ環境にはまだ影響を与えないようにするためです。

! An ACL must be configured to prepend dACLs from AAA server.

**ip access-group ACL-ALLOW in**

(注) DSBUS スイッチ上に Cisco IOS Release 12.2(55)SE ソフトウェアを用意する前に、RADIUS AAA サーバからのダイナミック ACL を適用するためのポート ACL が必要です。デフォルトの ACL を用意できなかった場合、割り当てられた dACL はスイッチによって無視されます。Cisco IOS Release 12.2(55)SE ソフトウェアでは、デフォルトの ACL が自動的に生成および適用されます。

(注) テストの現段階では、ポートベースの 802.1X 認証を有効にし、さらに既存のネットワークへの影響を避けるために、ACL-ALLOW を使用しています。今後のテストでは、実稼働環境に必要なトラフィックをブロックする、異なる ACL-DEFAULT を適用する予定です。

**ステップ 7** マルチ認証ホストモードを有効にします。マルチ認証は、基本的には複数ドメイン認証 (MDA) のスーパーセットです。MDA では、データ ドメイン内の単一のエンドポイントだけが許可されます。マルチ認証を設定すると、音声ドメイン内では認証された単一の電話が (MDA の場合と同じように) 許可されますが、データ ドメイン内では認証できるデータ デバイスの数に制限がありません。

! Allow voice + multiple endpoints on same physical access port

**authentication host-mode multi-auth**

(注) IP 電話の背後で複数のデータ デバイス (仮想デバイスであるかハブに接続されている物理デバイスであるかにかかわらず) を使用すると、アクセス ポートの物理リンクステート認識度が低下する可能性があります。

**ステップ 8** 次のように、さまざまな認証方式オプションを有効にします。

! Enable re-authentication

**authentication periodic**

! Enable re-authentication via RADIUS Session-Timeout

**authentication timer reauthenticate server**

**authentication event fail action next-method**

**authentication event server dead action reinitialize** <VLAN\_number>

**authentication event server alive action reinitialize**

! IOS Flex-Auth authentication should do 802.1X then MAB

**authentication order dot1x mab**

**authentication priority dot1x mab**

**ステップ 9** 次のように、スイッチ ポートで 802.1X ポート制御を有効にします。

! Enables port-based authentication on the interface

**authentication port-control auto**

**authentication violation restrict**

**ステップ 10** 次のように、MAC 認証バイパス (MAB) を有効にします。

! Enable MAC Authentication Bypass (MAB)

**mab**

**ステップ 11** 次のように、スイッチ ポートで 802.1X を有効にします。

! Enables 802.1X authentication on the interface

**dot1x pae authenticator**

**ステップ 12** 次のように、再送信時間を 10 秒に設定します。

**dot1x timeout tx-period 10**

(注) dot1x tx-period のタイムアウトは、10 秒に設定する必要があります。この値を変更する場合は、その影響を理解したうえで行ってください。

**ステップ 13** 次のように、PortFast 機能を有効にします。

**spanning-tree portfast**

## EPM ロギングを有効にするコマンド

Cisco ISE の機能について発生する可能性があるトラブルシューティングや記録をサポートするには、次のように、スイッチに標準のロギング機能を設定します。

**epm logging**

## SNMP トラップを有効にするコマンド

次のように、スイッチがこのネットワーク セグメント内の適切な VLAN を経由して、Cisco ISE から SNMP トラップ転送を受信できるようにします。

**snmp-server community public RO**

**snmp-server trap-source <VLAN\_number>**

## プロファイリング用の SNMP v3 クエリーを有効にするコマンド

SNMP v3 プロファイリングが正常に発生し、Cisco ISE プロファイリング サービスがサポートされるように、スイッチを設定します。まず、[管理 (Administration)] > [ネットワーク リソース (Network Resources)] > [ネットワーク デバイス (Network Devices)] > [追加 (Add)] || [編集 (Edit)] > [SNMP 設定 (SNMP Settings)] を選択して、Cisco ISE の SNMP 設定を設定します。

```
Snmp-server user <name> <group> v3 auth md5 <string> priv des <string>
```

```
snmp-server group <group> v3 priv
```

```
snmp-server group <group> v3 priv context vlan-1
```



(注) `snmp-server group <group> v3 priv context vlan-1` コマンドは、コンテキストごとに設定する必要があります。`snmp show context` コマンドでは、すべてのコンテキスト情報がリストされます。

SNMP 要求がタイムアウトになり、接続の問題が発生していない場合は、タイムアウト値を増加させることができます。

## プロファイラによる収集を可能にするための MAC 通知トラップを有効にするコマンド

次のように、適切な MAC 通知トラップを送信するようスイッチを設定し、Cisco ISE のプロファイラ機能がネットワーク エンドポイントで情報を収集できるようにします。

```
mac address-table notification change
```

```
mac address-table notification mac-move
```

```
snmp trap mac-notification change added
```

```
snmp trap mac-notification change removed
```

## スイッチ上での RADIUS Idle-timeout の設定

スイッチに RADIUS Idle-timeout を設定するには、次のコマンドを使用します。

```
Switch(config-if) # authentication timer inactivity
```

`inactivity` は、クライアントアクティビティが不正と見なされるまでの非アクティブ間隔を秒単位で表したものです。

Cisco ISE では、そのようなセッションの非アクティブ タイマーを適用する必要がある許可ポリシーに対して、[ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] > [許可 (Authorization)] > [許可プロファイル (Authorization Profiles)] からこのオプションを有効にできます。

# iOS サプリカント プロビジョニングのためのワイヤレス LAN コントローラ設定

## シングル SSID の場合

同じワイヤレス アクセス ポイントで、Apple iOS ベースのデバイス (iPhone/iPad) が、ある SSID から別の SSID に切り替えることができるようにするには、「FAST SSID の変更」機能を有効にするようワイヤレス LAN コントローラ (WLC) を設定します。この機能によって、iOS ベースのデバイスがより迅速に SSID 間の切り替えを行うことができます。

## デュアル SSID BYOD の場合

デュアル SSID BYOD をサポートするには、Fast SSID が有効になっている必要があります。ワイヤレス コントローラで Fast SSID Change が有効になっている場合、クライアントは SSID 間を高速で移動できます。高速 SSID が有効になっている場合、クライアント エントリがクリアされず、遅延は適用されません。Fast SSID の詳細と、Cisco WLC での Fast SSID の設定の詳細については、[http://www.cisco.com/c/en/us/td/docs/wireless/controller/8-3/config-guide/b\\_cg83/b\\_cg83\\_chapter\\_0100001.html](http://www.cisco.com/c/en/us/td/docs/wireless/controller/8-3/config-guide/b_cg83/b_cg83_chapter_0100001.html)を参照してください。

## WLC の設定例

```
WLC (config)# FAST SSID change
```

一部の Apple iOS ベースのデバイスでは、ワイヤレス ネットワークに接続しようとする、次のエラー メッセージが表示される場合があります。

ワイヤレスネットワークをスキャンできませんでした。(Could not scan for Wireless Networks.)

デバイス認証に影響しないため、このエラー メッセージは無視できます。

# MDM Interoperability のためのワイヤレス LAN コントローラでの ACL の設定

未登録のデバイスおよび証明書プロビジョニングをリダイレクトするために許可ポリシーで使用する ACL をワイヤレス LAN コントローラで設定します。ACL は次の順序にする必要があります。

- 
- ステップ 1 サーバからクライアントへのすべての発信トラフィックを許可します。
  - ステップ 2 (任意) トラブルシューティングのためにクライアントからサーバへの ICMP 着信トラフィックを許可します。
  - ステップ 3 未登録および非準拠のデバイスが MDM エージェントをダウンロードし、コンプライアンス チェックに進むように MDM サーバへのアクセスを許可します。

- ステップ 4** Web ポータルおよびサブリカント用 ISE、および証明書プロビジョニングフローに対するクライアントからサーバへのすべての着信トラフィックを許可します。
- ステップ 5** 名前解決のためにクライアントからサーバへの着信 DNS トラフィックを許可します。
- ステップ 6** IP アドレスのためにクライアントからサーバへの着信 DHCP トラフィックを許可します。
- ステップ 7** ISE へのリダイレクションのための、クライアントからサーバへの企業リソースに対するすべての着信トラフィックを（会社のポリシーに応じて）拒否します。
- ステップ 8** （任意）残りのトラフィックを許可します。

## 例

次の例では、未登録のデバイスを BYOD フローにリダイレクトするための ACL を示しています。この例では、Cisco ISE IP アドレスは 10.35.50.165 で、社内ネットワークの IP アドレスは 192.168.0.0 および 172.16.0.0（リダイレクト用）で、MDM サーバサブネットは 204.8.168.0 です。

図 70: 登録されていないデバイスをリダイレクトするための ACL

| General          |        |                |                     |          |             |             |      |           |                |  |
|------------------|--------|----------------|---------------------|----------|-------------|-------------|------|-----------|----------------|--|
| Access List Name |        | NSP-ACL        |                     |          |             |             |      |           |                |  |
| Deny Counters    |        | 0              |                     |          |             |             |      |           |                |  |
| Seq              | Action | Source IP/Mask | Destination IP/Mask | Protocol | Source Port | Dest Port   | DSCP | Direction | Number of Hits |  |
| 1                | Permit | 0.0.0.0 /      | 0.0.0.0 /           | Any      | Any         | Any         | Any  | Outbound  | 150720         |  |
| 2                | Permit | 0.0.0.0 /      | 0.0.0.0 /           | ICMP     | Any         | Any         | Any  | Inbound   | 7227           |  |
| 3                | Permit | 0.0.0.0 /      | 204.8.168.0 /       | Any      | Any         | Any         | Any  | Any       | 17626          |  |
| 4                | Permit | 0.0.0.0 /      | 255.255.255.0 /     | Any      | Any         | Any         | Any  | Inbound   | 7505           |  |
| 5                | Permit | 0.0.0.0 /      | 10.35.50.165 /      | Any      | Any         | Any         | Any  | Inbound   | 2864           |  |
| 6                | Permit | 0.0.0.0 /      | 255.255.255.255 /   | UDP      | Any         | DNS         | Any  | Inbound   | 0              |  |
| 7                | Permit | 0.0.0.0 /      | 0.0.0.0 /           | UDP      | Any         | DHCP Server | Any  | Inbound   | 0              |  |
| 8                | Deny   | 0.0.0.0 /      | 0.0.0.0 /           | Any      | Any         | Any         | Any  | Inbound   | 0              |  |
| 9                | Deny   | 0.0.0.0 /      | 192.168.0.0 /       | Any      | Any         | Any         | Any  | Inbound   | 4              |  |
| 10               | Deny   | 0.0.0.0 /      | 255.240.0.0 /       | Any      | Any         | Any         | Any  | Inbound   | 457            |  |
| 11               | Deny   | 0.0.0.0 /      | 10.0.0.0 /          | Any      | Any         | Any         | Any  | Inbound   | 1256           |  |
| 12               | Deny   | 0.0.0.0 /      | 255.0.0.0 /         | Any      | Any         | Any         | Any  | Inbound   | 11310          |  |
| 13               | Deny   | 0.0.0.0 /      | 173.194.0.0 /       | Any      | Any         | Any         | Any  | Any       | 0              |  |
| 14               | Permit | 0.0.0.0 /      | 255.255.0.0 /       | Any      | Any         | Any         | Any  | Any       | 71819          |  |
| 15               | Permit | 0.0.0.0 /      | 171.68.0.0 /        | Any      | Any         | Any         | Any  | Any       | 0              |  |
| 16               | Permit | 0.0.0.0 /      | 255.252.0.0 /       | Any      | Any         | Any         | Any  | Any       | 0              |  |
| 17               | Permit | 0.0.0.0 /      | 171.71.181.0 /      | Any      | Any         | Any         | Any  | Any       | 0              |  |
| 18               | Permit | 0.0.0.0 /      | 255.255.255.0 /     | Any      | Any         | Any         | Any  | Any       | 0              |  |
| 19               | Permit | 0.0.0.0 /      | 0.0.0.0 /           | Any      | Any         | Any         | Any  | Any       | 0              |  |
| 20               | Permit | 0.0.0.0 /      | 0.0.0.0 /           | Any      | Any         | Any         | Any  | Any       | 0              |  |







## 第 37 章

# Cisco ISE でサポートされる管理情報ベース

- [IF-MIB \(1499 ページ\)](#)
- [SNMPv2-MIB \(1500 ページ\)](#)
- [IP-MIB \(1500 ページ\)](#)
- [CISCO-CDP-MIB \(1501 ページ\)](#)
- [CISCO-VTP-MIB \(1502 ページ\)](#)
- [CISCO-STACK-MIB \(1502 ページ\)](#)
- [BRIDGE-MIB \(1502 ページ\)](#)
- [OLD-CISCO-INTERFACE-MIB \(1502 ページ\)](#)
- [CISCO-LWAPP-AP-MIB \(1503 ページ\)](#)
- [CISCO-LWAPP-DOT11-CLIENT-MIB \(1504 ページ\)](#)
- [CISCO-AUTH-FRAMEWORK-MIB \(1505 ページ\)](#)
- [EEE8021-PAE-MIB: RFC IEEE 802.1X \(1505 ページ\)](#)
- [HOST-RESOURCES-MIB \(1506 ページ\)](#)
- [LLDP-MIB \(1506 ページ\)](#)

## IF-MIB

表 168 :

| オブジェクト        | OID                 |
|---------------|---------------------|
| ifIndex       | 1.3.6.1.2.1.2.2.1.1 |
| ifDescr       | 1.3.6.1.2.1.2.2.1.2 |
| ifType        | 1.3.6.1.2.1.2.2.1.3 |
| ifSpeed       | 1.3.6.1.2.1.2.2.1.5 |
| ifPhysAddress | 1.3.6.1.2.1.2.2.1.6 |
| ifAdminStatus | 1.3.6.1.2.1.2.2.1.7 |

| オブジェクト       | OID                 |
|--------------|---------------------|
| ifOperStatus | 1.3.6.1.2.1.2.2.1.8 |

## SNMPv2-MIB

表 169:

| オブジェクト          | OID               |
|-----------------|-------------------|
| system          | 1.3.6.1.2.1.1     |
| sysDescr        | 1.3.6.1.2.1.1.1.0 |
| sysObjectID     | 1.3.6.1.2.1.1.2.0 |
| sysUpTime       | 1.3.6.1.2.1.1.3.0 |
| sysContact      | 1.3.6.1.2.1.1.4.0 |
| sysName         | 1.3.6.1.2.1.1.5.0 |
| sysLocation     | 1.3.6.1.2.1.1.6.0 |
| sysServices     | 1.3.6.1.2.1.1.7.0 |
| sysORLastChange | 1.3.6.1.2.1.1.8.0 |
| sysORTable      | 1.3.6.1.2.1.1.9.0 |

## IP-MIB

表 170:

| オブジェクト                     | OID                  |
|----------------------------|----------------------|
| ipAdEntIfIndex             | 1.3.6.1.2.1.4.20.1.2 |
| ipAdEntNetMask             | 1.3.6.1.2.1.4.20.1.3 |
| ipNetToMediaPhysAddress    | 1.3.6.1.2.1.4.22.1.2 |
| ipNetToPhysicalPhysAddress | 1.3.6.1.2.1.4.35.1.4 |

# CISCO-CDP-MIB

表 171:

| オブジェクト                        | OID                           |
|-------------------------------|-------------------------------|
| cdpCacheEntry                 | 1.3.6.1.4.1.9.9.23.1.2.1.1    |
| cdpCacheIfIndex               | 1.3.6.1.4.1.9.9.23.1.2.1.1.1  |
| cdpCacheDeviceIndex           | 1.3.6.1.4.1.9.9.23.1.2.1.1.2  |
| cdpCacheAddressType           | 1.3.6.1.4.1.9.9.23.1.2.1.1.3  |
| cdpCacheAddress               | 1.3.6.1.4.1.9.9.23.1.2.1.1.4  |
| cdpCacheVersion               | 1.3.6.1.4.1.9.9.23.1.2.1.1.5  |
| cdpCacheDeviceId              | 1.3.6.1.4.1.9.9.23.1.2.1.1.6  |
| cdpCacheDevicePort            | 1.3.6.1.4.1.9.9.23.1.2.1.1.7  |
| cdpCachePlatform              | 1.3.6.1.4.1.9.9.23.1.2.1.1.8  |
| cdpCacheCapabilities          | 1.3.6.1.4.1.9.9.23.1.2.1.1.9  |
| cdpCacheVTPMgmtDomain         | 1.3.6.1.4.1.9.9.23.1.2.1.1.10 |
| cdpCacheNativeVLAN            | 1.3.6.1.4.1.9.9.23.1.2.1.1.11 |
| cdpCacheDuplex                | 1.3.6.1.4.1.9.9.23.1.2.1.1.12 |
| cdpCacheApplianceID           | 1.3.6.1.4.1.9.9.23.1.2.1.1.13 |
| cdpCacheVlanID                | 1.3.6.1.4.1.9.9.23.1.2.1.1.14 |
| cdpCachePowerConsumption      | 1.3.6.1.4.1.9.9.23.1.2.1.1.15 |
| cdpCacheMTU                   | 1.3.6.1.4.1.9.9.23.1.2.1.1.16 |
| cdpCacheSysName               | 1.3.6.1.4.1.9.9.23.1.2.1.1.17 |
| cdpCacheSysObjectID           | 1.3.6.1.4.1.9.9.23.1.2.1.1.18 |
| cdpCachePrimaryMgmtAddrType   | 1.3.6.1.4.1.9.9.23.1.2.1.1.19 |
| cdpCachePrimaryMgmtAddr       | 1.3.6.1.4.1.9.9.23.1.2.1.1.20 |
| cdpCacheSecondaryMgmtAddrType | 1.3.6.1.4.1.9.9.23.1.2.1.1.21 |
| cdpCacheSecondaryMgmtAddr     | 1.3.6.1.4.1.9.9.23.1.2.1.1.22 |
| cdpCachePhysLocation          | 1.3.6.1.4.1.9.9.23.1.2.1.1.23 |

| オブジェクト             | OID                           |
|--------------------|-------------------------------|
| cdpCacheLastChange | 1.3.6.1.4.1.9.9.23.1.2.1.1.24 |

## CISCO-VTP-MIB

表 172:

| オブジェクト         | OID                             |
|----------------|---------------------------------|
| vtpVlanIfIndex | 1.3.6.1.4.1.9.9.46.1.3.1.1.18.1 |
| vtpVlanName    | 1.3.6.1.4.1.9.9.46.1.3.1.1.4.1  |
| vtpVlanState   | 1.3.6.1.4.1.9.9.46.1.3.1.1.2.1  |

## CISCO-STACK-MIB

表 173:

| オブジェクト       | OID                         |
|--------------|-----------------------------|
| portIfIndex  | 1.3.6.1.4.1.9.5.1.4.1.1.11  |
| vlanPortVlan | 1.3.6.1.4.1.9.5.1.9.3.1.3.1 |

## BRIDGE-MIB

表 174:

| オブジェクト               | OID                    |
|----------------------|------------------------|
| dot1dTpFdbPort       | 1.3.6.1.2.1.17.4.3.1.2 |
| dot1dBasePortIfIndex | 1.3.6.1.2.1.17.1.4.1.2 |

## OLD-CISCO-INTERFACE-MIB

表 175:

| オブジェクト      | OID                      |
|-------------|--------------------------|
| locIfReason | 1.3.6.1.4.1.9.2.2.1.1.20 |

# CISCO-LWAPP-AP-MIB

表 176:

| オブジェクト                             | OID                          |
|------------------------------------|------------------------------|
| cLApEntry                          | 1.3.6.1.4.1.9.9.513.1.1.1    |
| cLApSysMacAddress                  | 1.3.6.1.4.1.9.9.513.1.1.1.1  |
| cLApIfMacAddress                   | 1.3.6.1.4.1.9.9.513.1.1.1.2  |
| cLApMaxNumberOfDot11Slots          | 1.3.6.1.4.1.9.9.513.1.1.1.3  |
| cLApEntPhysicalIndex               | 1.3.6.1.4.1.9.9.513.1.1.1.4  |
| cLApName                           | 1.3.6.1.4.1.9.9.513.1.1.1.5  |
| cLApUpTime                         | 1.3.6.1.4.1.9.9.513.1.1.1.6  |
| cLLwappUpTime                      | 1.3.6.1.4.1.9.9.513.1.1.1.7  |
| cLLwappJoinTakenTime               | 1.3.6.1.4.1.9.9.513.1.1.1.8  |
| cLApMaxNumberOfEthernetSlots       | 1.3.6.1.4.1.9.9.513.1.1.1.9  |
| cLApPrimaryControllerAddressType   | 1.3.6.1.4.1.9.9.513.1.1.1.10 |
| cLApPrimaryControllerAddress       | 1.3.6.1.4.1.9.9.513.1.1.1.11 |
| cLApSecondaryControllerAddressType | 1.3.6.1.4.1.9.9.513.1.1.1.12 |
| cLApSecondaryControllerAddress     | 1.3.6.1.4.1.9.9.513.1.1.1.13 |
| cLApTertiaryControllerAddressType  | 1.3.6.1.4.1.9.9.513.1.1.1.14 |
| cLApTertiaryControllerAddress      | 1.3.6.1.4.1.9.9.513.1.1.1.15 |
| cLApLastRebootReason               | 1.3.6.1.4.1.9.9.513.1.1.1.16 |
| cLApEncryptionEnable               | 1.3.6.1.4.1.9.9.513.1.1.1.17 |
| cLApFailoverPriority               | 1.3.6.1.4.1.9.9.513.1.1.1.18 |
| cLApPowerStatus                    | 1.3.6.1.4.1.9.9.513.1.1.1.19 |
| cLApTelnetEnable                   | 1.3.6.1.4.1.9.9.513.1.1.1.20 |
| cLApSshEnable                      | 1.3.6.1.4.1.9.9.513.1.1.1.21 |
| cLApPreStdStateEnabled             | 1.3.6.1.4.1.9.9.513.1.1.1.22 |
| cLApPwrInjectorStateEnabled        | 1.3.6.1.4.1.9.9.513.1.1.1.23 |

| オブジェクト                      | OID                          |
|-----------------------------|------------------------------|
| cLApPwrInjectorSelection    | 1.3.6.1.4.1.9.9.513.1.1.1.24 |
| cLApPwrInjectorSwMacAddr    | 1.3.6.1.4.1.9.9.513.1.1.1.25 |
| cLApWipsEnable              | 1.3.6.1.4.1.9.9.513.1.1.1.26 |
| cLApMonitorModeOptimization | 1.3.6.1.4.1.9.9.513.1.1.1.27 |
| cLApDomainName              | 1.3.6.1.4.1.9.9.513.1.1.1.28 |
| cLApNameServerAddressType   | 1.3.6.1.4.1.9.9.513.1.1.1.29 |
| cLApNameServerAddress       | 1.3.6.1.4.1.9.9.513.1.1.1.30 |
| cLApAMSDUEnable             | 1.3.6.1.4.1.9.9.513.1.1.1.31 |
| cLApEncryptionSupported     | 1.3.6.1.4.1.9.9.513.1.1.1.32 |
| cLApRogueDetectionEnabled   | 1.3.6.1.4.1.9.9.513.1.1.1.33 |

## CISCO-LWAPP-DOT11-CLIENT-MIB

表 177:

| オブジェクト                    | OID                            |
|---------------------------|--------------------------------|
| cldcClientEntry           | 1.3.6.1.4.1.9.9.599.1.3.1.1    |
| cldcClientMacAddress      | 1.3.6.1.4.1.9.9.599.1.3.1.1.1  |
| cldcClientStatus          | 1.3.6.1.4.1.9.9.599.1.3.1.1.2  |
| cldcClientWlanProfileName | 1.3.6.1.4.1.9.9.599.1.3.1.1.3  |
| cldcClientWgbStatus       | 1.3.6.1.4.1.9.9.599.1.3.1.1.4  |
| cldcClientWgbMacAddress   | 1.3.6.1.4.1.9.9.599.1.3.1.1.5  |
| cldcClientProtocol        | 1.3.6.1.4.1.9.9.599.1.3.1.1.6  |
| cldcAssociationMode       | 1.3.6.1.4.1.9.9.599.1.3.1.1.7  |
| cldcApMacAddress          | 1.3.6.1.4.1.9.9.599.1.3.1.1.8  |
| cldcIfType                | 1.3.6.1.4.1.9.9.599.1.3.1.1.9  |
| cldcClientIPAddress       | 1.3.6.1.4.1.9.9.599.1.3.1.1.10 |
| cldcClientNacState        | 1.3.6.1.4.1.9.9.599.1.3.1.1.11 |
| cldcClientQuarantineVLAN  | 1.3.6.1.4.1.9.9.599.1.3.1.1.12 |

| オブジェクト                     | OID                            |
|----------------------------|--------------------------------|
| cldcClientAccessVLAN       | 1.3.6.1.4.1.9.9.599.1.3.1.1.13 |
| cldcClientLoginTime        | 1.3.6.1.4.1.9.9.599.1.3.1.1.14 |
| cldcClientUpTime           | 1.3.6.1.4.1.9.9.599.1.3.1.1.15 |
| cldcClientPowerSaveMode    | 1.3.6.1.4.1.9.9.599.1.3.1.1.16 |
| cldcClientCurrentTxRateSet | 1.3.6.1.4.1.9.9.599.1.3.1.1.17 |
| cldcClientDataRateSet      | 1.3.6.1.4.1.9.9.599.1.3.1.1.18 |

## CISCO-AUTH-FRAMEWORK-MIB

表 178:

| オブジェクト                     | OID                            |
|----------------------------|--------------------------------|
| cafPortConfigEntry         | 1.3.6.1.4.1.9.9.656.1.2.1.1    |
| cafSessionClientMacAddress | 1.3.6.1.4.1.9.9.656.1.4.1.1.2  |
| cafSessionStatus           | 1.3.6.1.4.1.9.9.656.1.4.1.1.5  |
| cafSessionDomain           | 1.3.6.1.4.1.9.9.656.1.4.1.1.6  |
| cafSessionAuthUserName     | 1.3.6.1.4.1.9.9.656.1.4.1.1.10 |
| cafSessionAuthorizedBy     | 1.3.6.1.4.1.9.9.656.1.4.1.1.12 |
| cafSessionAuthVlan         | 1.3.6.1.4.1.9.9.656.1.4.1.1.14 |

## EEE8021-PAE-MIB: RFC IEEE 802.1X

表 179:

| オブジェクト                             | OID                    |
|------------------------------------|------------------------|
| dot1xAuthAuthControlledPortStatus  | 1.0.8802.1.1.1.2.1.1.5 |
| dot1xAuthAuthControlledPortControl | 1.0.8802.1.1.1.2.1.1.6 |
| dot1xAuthSessionUserName           | 1.0.8802.1.1.1.2.4.1.9 |

## HOST-RESOURCES-MIB

表 180:

| オブジェクト         | OID                    |
|----------------|------------------------|
| hrDeviceDescr  | 1.3.6.1.2.1.25.3.2.1.3 |
| hrDeviceStatus | 1.3.6.1.2.1.25.3.2.1.5 |

## LLDP-MIB

表 181:

| オブジェクト                       | OID                       |
|------------------------------|---------------------------|
| lldpEntry                    | 1.0.8802.1.1.2.1.4.1.1    |
| lldpTimeMark                 | 1.0.8802.1.1.2.1.4.1.1.1  |
| lldpLocalPortNum             | 1.0.8802.1.1.2.1.4.1.1.2  |
| lldpIndex                    | 1.0.8802.1.1.2.1.4.1.1.3  |
| lldpChassisIdSubtype         | 1.0.8802.1.1.2.1.4.1.1.4  |
| lldpChassisId                | 1.0.8802.1.1.2.1.4.1.1.5  |
| lldpPortIdSubtype            | 1.0.8802.1.1.2.1.4.1.1.6  |
| lldpPortId                   | 1.0.8802.1.1.2.1.4.1.1.7  |
| lldpPortDescription          | 1.0.8802.1.1.2.1.4.1.1.8  |
| lldpSystemName               | 1.0.8802.1.1.2.1.4.1.1.9  |
| lldpSystemDescription        | 1.0.8802.1.1.2.1.4.1.1.10 |
| lldpCapabilitiesMapSupported | 1.0.8802.1.1.2.1.4.1.1.11 |
| lldpCacheCapabilities        | 1.0.8802.1.1.2.1.4.1.1.12 |