Cisco AnyConnect Secure Mobility Client リリース 4.6 管理者ガイド

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

目 次

第 1 章

AnyConnect の展開 1

展開前の作業 1

AnyConnect 展開の概要 2

AnyConnect のためのエンドポイントの準備 4

AnyConnect とモバイル ブロードバンド カードの使用方法 4

Windows での Internet Explorer 信頼済みサイトのリストへの ASA の追加 5

Internet Explorer でのプロキシ変更のブロック 6

AnyConnect による Windows RDP セッションの処理方法の設定 6

Windows での DES-only SSL 暗号化 8

Linux 上での NVM の使用 8

AnyConnect カーネル モジュールを構築するための必要条件 8

NVM の構築済み AnyConnect Linux カーネル モジュール とのパッケージ化 9

AnyConnect の事前展開 10

事前展開と Web 展開向けの AnyConnect モジュール実行可能ファイル 11

AnyConnect プロファイルを事前展開する場所 12

スタンドアロン アプリケーションとしての AnyConnect モジュールの事前展開 17

Windows での SMS によるスタンドアロン モジュールの展開 17

スタンドアロン アプリケーションとしての AnyConnect モジュールの展開 17

スタンドアロン モジュールのユーザ インストール 18

Windows への事前展開 19

zip ファイルを使用した AnyConnect の配布 19

AnyConnect zip ファイルの内容 19

SMS を使用した AnyConnect の配布 20

Windows 事前展開セキュリティ オプション 23

Windows での AnyConnect モジュールのインストールおよび削除の順序 23
macOS への事前展開 24
macOS での AnyConnect のインストールおよびアンインストール 24
macOS への AnyConnect モジュールのスタンドアロン アプリケーションとしてのインストール 24
macOS 上のアプリケーションの制限 26
Linux への事前展開 26
Linux 用モジュールのインストール 26
Linux 用モジュールのアンインストール 26
Linux デバイスへの NVM の手動インストール/アンインストール 27
Firefox でのサーバ証明書検証の初期化 27
Linux デバイスへの DART の手動インストール 28
Web 展開 AnyConnect 28
ASA での Web 展開の設定 30
WebLaunch のブラウザの制限 30
AnyConnect パッケージのダウンロード 30
ASA での AnyConnect パッケージのロード 31
追加の AnyConnect モジュールの有効化 31
ASDM でのクライアント プロファイルの作成 32
ISE での Web 展開の設定 32
ISE アップロードのための AnyConnect ファイルの準備 34
AnyConnect を展開するための ISE の設定 34
FTD での Web 展開の設定 36
AnyConnect ソフトウェアおよびプロファイルの更新 37
AnyConnect 自動更新の無効化 39
ユーザに WebLaunch 中に AnyConnect のダウンロードを求めるプロンプトの表示 40
ユーザに対するアップグレード遅延の許可 40
更新ポリシーの設定 43
更新ポリシーの概要 43
許可されたサーバ更新ポリシーの動作 44
不正なサーバ更新ポリシーの動作 44

更新ポリシーのガイドライン 45
更新ポリシーの例 46
AnyConnect 参照情報 48
ローカル コンピュータ上のユーザ プリファレンス ファイルの場所 48
AnyConnect およびレガシー VPN クライアントで使用されるポート 48

第 2 章 **AnyConnect クライアントとインストーラのカスタマイズとローカライズ 51**
AnyConnect インストール動作の変更 51
カスタマー エクスペリエンス フィードバックの無効化 51
インストール動作の変更、Windows 52
クライアント インストールをカスタマイズする Windows インストーラ プロパティ 53
AnyConnect モジュール用の Windows インストーラ プロパティ 54
適応型セキュリティ アプライアンスへのカスタマイズされたインストーラ トランスフォームのインポート 55
AnyConnect インストーラ画面のローカライズ 56
適応型セキュリティ アプライアンスへのローカライズされたインストーラ トランスフォームのインポート 57
インストール動作の変更、macOS 59
ACTransforms.xml による macOS でのインストーラ動作のカスタマイズ 59
カスタマー エクスペリエンス フィードバック モジュールの無効化 59
インストール動作の変更、Linux 60
ACTransform.xml による Linux でのインストーラ動作のカスタマイズ 60
DSCP の保存の有効化 60
パブリック DHCP サーバ ルートの設定 61
AnyConnect GUI テキストとメッセージのカスタマイズ 61
AnyConnect のテキストとメッセージの追加または編集 63
適応型セキュリティ アプライアンスへの変換テーブルのインポート 66
エンタープライズ展開用のメッセージ カタログの作成 66
ASA のカスタマイズした変換テーブルへの新しいメッセージの統合 67
クライアントでの Windows のデフォルト言語の選択 69
AnyConnect GUI のカスタム アイコンおよびロゴの作成 69

AnyConnect GUI コンポーネントの置き換え 70
Windows 用 AnyConnect アイコンとロゴ 71
Linux 用 AnyConnect アイコンとロゴ 75
macOS 用 AnyConnect アイコンとロゴ 77
AnyConnect クライアントのヘルプ ファイルの作成とアップロード 78
スクリプトの作成および展開 79
スクリプトの作成、テスト、および展開 81
スクリプトに関する AnyConnect プロファイルの設定 82
スクリプトのトラブルシューティング 83
AnyConnect API によるカスタム アプリケーションの作成と展開 84
AnyConnect CLI コマンドの使用 85
クライアント CLI プロンプトの起動 85
クライアント CLI コマンドの使用 85
ASA によるセッション終了時に Windows ポップアップ メッセージが表示されないようにする 87
ISE 展開のための AnyConnect カスタマイズおよびローカリゼーションの準備 88
AnyConnect ローカリゼーション バンドルの準備 88
AnyConnect カスタマイゼーション バンドルの準備 90

第 3 章 **AnyConnect プロファイル エディタ 93**
プロファイル エディタについて 93
ASDM からの新しいプロファイルの追加 93
スタンドアロン プロファイル エディタ 94
スタンドアロン AnyConnect プロファイル エディタのインストール 95
スタンドアロン プロファイル エディタを使用したクライアント プロファイルの編集 96
AnyConnect VPN プロファイル 97
AnyConnect プロファイル エディタ、プリファレンス（Part 1） 97
AnyConnect プロファイル エディタ、プリファレンス（Part 2） 101
AnyConnect プロファイル エディタのバックアップ サーバ 108
AnyConnect プロファイル エディタの証明書照合 109
AnyConnect プロファイル エディタの証明書の登録 112

AnyConnect プロファイル エディタの証明書ピン 113
証明書ピン留めウィザード 114
AnyConnect プロファイル エディタのモバイル ポリシー 114
AnyConnect プロファイル エディタのサーバ リスト 114
AnyConnect プロファイル エディタのサーバ リストの追加/編集 115
AnyConnect プロファイル エディタのモバイル設定 118
AnyConnect ローカル ポリシー 120
ローカル ポリシー パラメータと値 120
ローカル ポリシー パラメータの手動変更 124
MST ファイルでのローカル ポリシー パラメータの有効化 125
Enable FIPS ツールによるローカル ポリシー パラメータの有効化 126

第 4 章 VPN アクセスの設定 127
VPN への接続と接続解除 127
AnyConnect VPN 接続オプション 127
VPN 接続サーバの設定 129
ログイン前の Windows VPN 接続の自動開始 131
Start Before Logon について 131
Start Before Logon の制限 132
Start Before Logon の設定 132
Start Before Logon のトラブルシューティング 134
AnyConnect 起動時の VPN 接続の自動開始 134
Windows システムにおける Start Before Logon（PLAP）の設定 135
PLAP のインストール 135
PLAP を使用した Windows PC へのログオン 136
PLAP を使用した AnyConnect からの接続解除 136
VPN 接続の自動リスタート 137
Trusted Network Detection を使用した接続または接続解除 137
Trusted Network Detection について 137
Trusted Network Detection のガイドライン 138
Trusted Network Detection の設定 139

Always-Onを使用した VPN 接続の必要性 141
Always-On VPN について 141
Always-On VPN の制限事項 142
Always-On VPN のガイドライン 142
Always-On VPN の設定 143
キャプティブ ポータル ホットスポットの検出と修復の使用 147
キャプティブ ポータルについて 147
キャプティブ ポータル修復の設定 148
キャプティブ ポータルの検出と修復のトラブルシューティング 149
AnyConnect over L2TP または PPTP の設定 150
ユーザに対する PPP 除外上書きの指示 151
AnyConnect プロキシ接続の設定 151
AnyConnect プロキシ接続について 151
AnyConnect プロキシ接続の要件 153
プロキシ接続の制限 153
ローカル プロキシ接続の許可 153
パブリック プロキシ 153
プライベート プロキシ接続の設定 155
プロキシ設定の確認 156
VPN トラフィックの選択および除外 156
VPN をバイパスするための IPv4 または IPv6 トラフィックの設定 156
ローカル プリンタおよびテザー デバイスをサポートしたクライアント ファイアウォールの設定 158
スプリット トンネリングの設定 158
ダイナミック スプリット トンネリングについて 158
スタティック スプリット トンネリングとダイナミック スプリット トンネリングの相互運用性 159
スプリット トンネリング設定をともなう重複シナリオの結果 160
ダイナミック スプリット トンネリングの使用状況の通知 160
ダイナミック スプリット除外トンネリングの設定 161
拡張ダイナミック スプリット除外トンネリングの設定 162

ダイナミック スプリット包含トンネリングの設定 162
拡張ダイナミック スプリット包含トンネリングの設定 163
スプリット DNS 164
スプリット DNS の要件 164
スプリット DNS の設定 164
AnyConnect ログを使用したスプリット DNS の確認 165
スプリット DNS を使用しているドメインの確認 165
VPN 認証の管理 166
重要なセキュリティ上の考慮事項 166
サーバ証明書処理の設定 166
サーバ証明書の確認（Server Certificate Verification） 166
無効なサーバ証明書の処理 167
Certificate-Only 認証の設定 170
証明書登録の設定 171
SCEP プロキシの登録と動作 171
認証局の要件 172
証明書登録のガイドライン 172
SCEP プロキシ証明書登録の設定 173
SCEP 用の Windows 2008 Server の認証局の設定 174
証明書失効通知の設定 176
証明書選択の設定 177
使用する証明書ストアの設定 177
Windows ユーザに認証証明書の選択を求めるプロンプトの表示 180
macOS および Linux での PEM 証明書ストアの作成 181
証明書照合の設定 182
SAML を使用した VPN 認証 185
SDI トークン（SoftID）統合を使用した VPN 認証 186
SDI 認証交換のカテゴリ 188
ネイティブ SDI と RADIUS SDI の比較 190
RADIUS/SDI メッセージをサポートするための ASA の設定 191
証明書のピン留めについて 193

グローバル ピンとホストごとのピン 194

第 5 章 ネットワーク アクセス マネージャの設定 195

ネットワーク アクセス マネージャについて 195

Suite B および FIPS 196

シングル サインオンの「シングル ユーザ」の適用 197

シングル サインオンのシングル ユーザの適用の設定 197

ネットワーク アクセス マネージャの展開 198

DHCP 接続テストの無効化 199

ネットワーク アクセス マネージャ プロファイル 200

[クライアント ポリシー（Client Policy）] ウィンドウ 200

[認証ポリシー（Authentication Policy）] ウィンドウ 203

[ネットワーク（Networks）] ウィンドウ 204

[ネットワーク（Networks）]、[メディア タイプ（Media Type）] ページ 205

[ネットワーク（Networks）]、[セキュリティ レベル（Security Level）] ページ 207

認証ネットワークの設定 207

オープン ネットワークの設定 210

共有キー ネットワークの設定 210

[ネットワーク（Networks）]、[ネットワーク接続タイプ（Network Connection Type）] ページ 211

[ネットワーク（Networks）]、[ユーザまたはマシンの認証（User or Machine Authentication）] ページ 213

EAP の概要 213

EAP-GTC 214

EAP-TLS 214

EAP-TTLS 215

PEAP オプション 217

EAP-FAST 設定 219

LEAP 設定 221

ネットワーク クレデンシャルの定義 221

[ネットワーク グループ（Network Groups）] ウィンドウ 228

第 6 章 ポスチャの設定 231

ISE ポスチャ モジュールの提供内容 232

ポスチャ チェック 232

必要な修復 232

エンドポイント コンプライアンスの再評価 234

シスコ テンポラル エージェント 235

オプション モードのポスチャ ポリシー拡張機能 236

ハードウェア インベントリの可視性 236

ステルス モード 237

ポスチャ ポリシーの適用 237

UDID 統合 238

アプリケーション監視 238

USB ストレージ デバイス検出 238

自動コンプライアンス 239

VLAN のモニタリングと遷移 239

AnyConnect ISE フローを中断する操作 240

ISE ポスチャのステータス 241

ポスチャとマルチホーミング 243

エンドポイントの同時ユーザ 243

ポスチャ モジュールのロギング 244

ポスチャ モジュールのログ ファイルと場所 244

ISE ポスチャ プロファイル エディタ 245

[詳細（Advanced）] パネル 247

VPN ポスチャ（HostScan）モジュールの提供内容 248

HostScan 248

基本的機能 249

エンドポイント アセスメント 249

Advanced Endpoint Assessment：マルウェア対策およびファイアウォールの修復 250

HostScan 用のアンチマルウェア アプリケーションの設定 250

ダイナミック アクセス ポリシーとの統合 250

DAP の BIOS シリアル番号 251
DAP エンドポイント属性としての BIOS の指定 251
BIOS シリアル番号の取得方法 251
ASA で有効にされたホスト スキャン イメージの判別 252
HostScan のアップグレード 252
OPSWAT サポート 252

第 7 章 Web セキュリティの設定 257
Web セキュリティ モジュールについて 257
一般的な Web セキュリティの設定 258
クライアント プロファイルでの Cisco Cloud Web Security スキャニング プロキシ 258
ユーザがスキャニング プロキシを選択する方法 259
スキャニング プロキシ リストの更新 260
ユーザに対するスキャニング プロキシの表示または非表示 260
デフォルトのスキャニング プロキシの選択 262
HTTP(S) トラフィック リスニング ポートの指定 262
パブリック プロキシを設定するための Windows インターネット オプションの設定 263
Web スキャニング サービスでのエンドポイント トラフィックの除外または包含 264
ホスト例外の除外と包含 265
プロキシ例外の除外 266
静的な例外の除外 267
ユーザ制御の設定および最も早いスキャニング プロキシ応答時間の計算 268
Secure Trusted Network Detection の使用 270
Secure Trusted Network Detection の不使用 271
認証の設定および Cisco Cloud Web Security プロキシへのグループ メンバーシップの送信 272
Web セキュリティの詳細設定 274
KDF リスニング ポートの設定 274
ポートが着信接続を受信する方法の設定 275
タイムアウトと再試行が発生するタイミングの設定 276
DNS ルックアップ 276

デバッグの設定 277
トラフィックのブロックと許可 277
他のカスタマイズ可能な Web セキュリティ オプション 277
エクスポート オプション 277
Web セキュリティのためのスプリット トンネル除外の設定 279
Cisco Cloud Web Security ホステッド プロファイルの使用 280
Cisco AnyConnect Web セキュリティ エージェントの無効化および有効化 282
Windows を使用したフィルタの無効化と有効化 282
Mac OS X を使用したフィルタの無効化と有効化 282
Web セキュリティ ロギング 283

第 8 章 **AMP イネーブラの設定 285**
AMP イネーブラについて 285
AMP イネーブラの導入 285
AMP イネーブラ プロファイル エディタ 286
AMP イネーブラのステータス 287

第 9 章 **ネットワーク可視性モジュール 289**
ネットワーク可視性モジュールについて 289
デスクトップ AnyConnect での NVM 290
モバイル AnyConnect での NVM 291
NVM の使用方法 291
NVM プロファイル エディタ 292
NVM のコレクション パラメータ 295
カスタマー フィードバック モジュールによる NVM ステータスの提供 298

第 10 章 **Umbrella ローミング セキュリティ 299**
Umbrella ローミング クライアントと Umbrella ローミング セキュリティ モジュールの非互換性 300
Cisco Umbrella アカウントの取得 300
ダッシュボードからの OrgInfo ファイルのダウンロード 300

Umbrella ローミング セキュリティの起動と実行 301
OrgInfo.json ファイルの設定 301
クラウド最新情報 302
セキュリティ ポリシーの設定とレポートの確認 303
エンドポイントに表示される UI の変更内容解説 303
診断の解釈 309

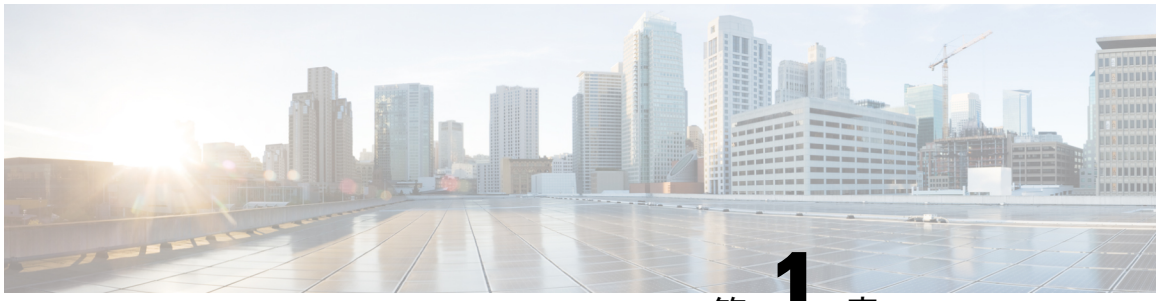
第 11 章 ローカル ポリシーでの FIPS の有効化 311
FIPS、NGE、および AnyConnect について 311
AnyConnect の FIPS 機能 312
AnyConnect FIPS の要件 313
AnyConnect FIPS の制限事項 313
AnyConnect FIPS のガイドライン 313
AnyConnect コア VPN クライアントのための FIPS の設定 315
AnyConnect コア VPN のための FIPS の有効化 315
Windows インストール時の FIPS の有効化 315
ネットワーク アクセス マネージャのための FIPS の設定 316
ネットワーク アクセス マネージャのための FIPS の有効化 316
ネットワーク アクセス マネージャに対する FIPS モードの適用 317

第 12 章 Cisco AnyConnect カスタマー エクスペリエンス フィードバック モジュール 319
カスタマー エクスペリエンス フィードバックの設定 320

第 13 章 AnyConnect のトラブルシューティング 321
トラブルシューティングに必要な情報の収集 321
統計詳細情報の表示 321
トラブルシューティング用にデータを収集するための DART の実行 322
インストールまたはアンインストールの問題についてデータを収集するためのログの収集（Windows） 323
コンピュータ システム情報の取得 324
systeminfo ファイル ダンプの取得 324

レジストリ ファイルの確認 324
AnyConnect ログ ファイルの場所 324
AnyConnect 接続または接続解除の問題 325
AnyConnect が初期接続を確立しないか、接続解除しない 325
AnyConnect がトラフィックを通過させない 327
VPN サービスの障害 328
VPN サービス接続に失敗 328
何がサービスと競合しているかの特定 329
VPN クライアント ドライバで（Microsoft Windows アップデート後に）エラーが発生する 330
VPN クライアント ドライバ エラーの修復 330
ドライバのクラッシュ 330
VPNVA.sys でのドライバ クラッシュの修復 330
vpnagent.exe でのドライバ クラッシュの修復 331
ネットワーク アクセス マネージャに関するリンク/ドライバの問題 331
その他のクラッシュ 331
AnyConnect のクラッシュ 331
.log ファイルまたは .dmp ファイルのバックアップ方法 332
AnyConnect が vpndownloader でクラッシュする（Layered Service Provider（LSP）モジュールおよび NOD32 AV） 332
ブルー スクリーン（AT & T Dialer） 332
セキュリティの警告 333
Microsoft Internet Explorer のセキュリティの警告 333
「不明な機関による認証」アラート 333
クライアントでの信頼できるルート証明書のインストール 333
接続のドロップ 334
有線接続が導入された場合のワイヤレス接続のドロップ（Juniper Odyssey クライアント） 334
Odyssey クライアントの設定 334
ASA への接続に失敗（Kaspersky AV Workstation 6.x） 335
UDP DTLS 接続なし（McAfee Firewall 5） 335

ホスト デバイスへの接続に失敗（Microsoft ルーティングとリモート アクセス サーバ） 335
接続障害/クレデンシャル不足（ロード バランサ） 335
インストールの失敗 336
AnyConnect がダウンロードに失敗する（Wave EMBASSY Trust Suite） 336
非互換性の問題 336
ルーティング テーブルの更新に失敗（Bonjour Printing Service） 336
TUN のバージョンに互換性がない（OpenVPN クライアント） 336
Winsock カタログの競合（LSP 症状 2 競合） 336
データ スループット低下（LSP 症状 3 競合） 336
SSL プロトコル スキャンの無効化 337
DPD 障害（EVDO ワイヤレス カードおよび Venturi ドライバ） 337
DTLS トラフィック障害（DSL ルータ） 337
NETINTERFACE_ERROR（CheckPoint と、Kaspersky などの他のサードパーティ製ソフトウェア） 338
パフォーマンスの問題（Virtual Machine Network Service ドライバ） 338
既知のサードパーティ製アプリケーション競合 338



第 1 章

AnyConnect の展開

- 展開前の作業 （1 ページ）
- AnyConnect 展開の概要 （2 ページ）
- AnyConnect のためのエンドポイントの準備 （4 ページ）
- Linux 上での NVM の使用 （8 ページ）
- AnyConnect の事前展開 （10 ページ）
- Web 展開 AnyConnect （28 ページ）
- AnyConnect ソフトウェアおよびプロファイルの更新 （37 ページ）

展開前の作業

Umbrella ローミング セキュリティ モジュールを展開している場合は、Umbrella ローミング クライアントのすべての既存のインストールが検出され、競合を防ぐために自動的に削除されます。Umbrella ローミング クライアントの既存インストールを Umbrella サービス サブスクリプションに関連付けている場合は、OrgInfo.json ファイルを AnyConnect インストーラと同じ場所に配置して Umbrella モジュールのディレクトリで Web 展開または事前展開を設定していない限り、Umbrella ローミング セキュリティ モジュールに自動的に移行されます。Umbrella ローミング セキュリティ モジュールを展開する前に、手動で Umbrella ローミング クライアントをアンインストールすることができます。

Umbrella ローミング セキュリティ モジュールを使用している場合は、次の前提条件も満たす必要があります。

- **Umbrella ローミング アカウントを取得する。**Umbrella ダッシュボード（http://dashboard.umbrella.com）は、AnyConnect Umbrella ローミング セキュリティ モジュールの操作に必要な情報を取得するログイン ページです。ローミング クライアント アクティビティのレポートを制御するためにもこのサイトを使用します。
- **ダッシュボードから OrgInfo ファイルをダウンロードする。**AnyConnect Umbrella ローミング セキュリティ モジュールの導入準備を行うには、Umbrella ダッシュボードから OrgInfo.json ファイルを取得します。[ID（Identities）] メニュー ストラクチャで [ローミング コンピュータ（Roaming Computers）] をクリックし、続いて、ページ左上隅の [+] 記号をクリックします。AnyConnect Umbrella ローミング セキュリティ モジュールまでスクロールし、[モジュール プロファイル（Module Profile）] をクリックします。

OrgInfo.json ファイルには、ローミング セキュリティ モジュールにレポートの送信先と適用するポリシーを知らせる、Umbrella サービス サブスクリプションについての詳細が含まれています。

AnyConnect 展開の概要

AnyConnect の展開は、AnyConnect クライアントと関連ファイルのインストール、設定、アップグレードを意味します。

Cisco AnyConnect Secure Mobility Client は、次の方法によってリモート ユーザに展開できます。

- 事前展開：新規インストールとアップグレードは、エンドユーザによって、または社内のソフトウェア管理システム（SMS）を使用して実行されます。
- Web 展開：AnyConnect パッケージは、ヘッドエンド（ASA もしくは FTD ファイアウォール、または ISE サーバ）にロードされます。ユーザがファイアウォールまたは ISE に接続すると、AnyConnect がクライアントに展開されます。
  - 新規インストールの場合、ユーザはヘッドエンドに接続して AnyConnect クライアントをダウンロードします。クライアントは、手動でインストールするか、または自動（Web 起動）でインストールされます。
  - アップデートは、AnyConnect がすでにインストールされているシステムで AnyConnect を実行することにより、またはユーザを ASA クライアントレス ポータルに誘導することによって行われます。
- クラウド更新：Umbrella ローミング セキュリティ モジュールの展開後に、上記およびクラウド更新のいずれかの方法を使用して AnyConnect モジュールを更新できます。クラウド更新では、ソフトウェア アップグレードは Umbrella クラウド インフラストラクチャから自動的に得られます。更新トラックは管理者のアクションではなくこれによって決まります。デフォルトでは、クラウド更新からの自動更新は無効です。

（注） クラウド更新に関して以下を検討してください。

- 現在インストールされているソフトウェア モジュールのみが更新されます。
- カスタマイズ、ローカリゼーション、およびその他の展開タイプはサポートされません。
- 更新は、デスクトップにログインしたときにのみ実行され、VPN が確立されているときは実行されません。
- 更新を無効にすると、最新のソフトウェア機能と更新を利用できません。
- クラウド更新を無効にしても、他の更新メカニズムや設定（Web 展開、遅延更新など）には影響しません。
- クラウド更新は、AnyConnect のより新しいバージョンや未公開バージョン（暫定リリース、修繕公開されたバージョンなど）があっても無視します。

AnyConnect を展開する場合に、追加機能を含めるオプションのモジュール、および VPN やオプション機能を設定するクライアント プロファイルを含めることができます。

ASA、IOS、Microsoft Windows、Linux、および macOS のシステム、管理、およびエンドポイントの要件については、AnyConnect のリリース ノートを参照してください。

AnyConnect のインストール方法の決定

AnyConnect は、ISE 2.0（またはそれ以降）および ASA ヘッドエンドによる Web 展開または事前展開が可能です。

Web 展開

- ASA または FTD デバイスからの Web 展開：ユーザは、ヘッドエンド デバイス上の AnyConnect クライアントレス ポータルに接続して、AnyConnect のダウンロードを選択します。ASA は、AnyConnect ダウンローダをダウンロードします。AnyConnect ダウンローダがクライアントをダウンロードし、クライアントをインストールし、VPN 接続を開始します。
- ISE からの Web 展開：ユーザは、ASA、ワイヤレス コントローラ、またはスイッチなどのネットワーク アクセス デバイス（NAD）に接続します。NAD はユーザを許可し、ISE ポータルにユーザをリダイレクトします。AnyConnect ダウンローダがクライアントにインストールされ、パッケージの抽出およびインストールを管理します。ただし、VPN 接続は開始しません。

事前展開

- Windows トランスフォームなどの、社内のソフトウェア管理システム（SMS）を使用します。
- AnyConnect ファイルのアーカイブを手動で配布し、インストール方法に関する指示をユーザに提供します。ファイルのアーカイブ形式は、zip（Windows）、DMG（Mac OS X）、gzip（Linux）です。

システム要件およびライセンスの依存関係の詳細については、『AnyConnect Secure Mobility Client Features, License, and OS Guide』を参照してください。

（注） Mac または Linux プラットフォームでルート権限のアクティビティを実行するために AnyConnect ポスチャ（HostScan）を使用している場合は、AnyConnect ポスチャを事前展開することを推奨します。

AnyConnect のインストールに必要なリソースの決定

AnyConnect 展開は、複数の種類のファイルで構成されています。

- AnyConnect コア クライアント。AnyConnect パッケージに含まれています。
- 追加機能をサポートするモジュール。AnyConnect パッケージに含まれています。
- AnyConnect および追加機能を設定するクライアント プロファイル。自分で作成します。
- 言語ファイル、画像、スクリプト、およびヘルプ ファイル（展開をカスタマイズまたはローカライズする場合）。
- AnyConnect ISE ポスチャおよびコンプライアンス モジュール（OPSWAT）。

AnyConnect のためのエンドポイントの準備

AnyConnect とモバイル ブロードバンド カードの使用方法

一部の 3G カードには、AnyConnect を使用する前に必要な設定手順があります。たとえば、VZAccess Manager には次の 3 種類の設定があります。

- モデム手動接続（modem manually connects）
- ローミング時を除くモデム自動接続（modem auto connect except when roaming）
- LAN アダプタ自動接続（LAN adapter auto connect）

[LAN アダプタ自動接続（LAN adapter auto connect）] を選択した場合は、プリファレンスを NDIS モードに設定します。NDIS は、VZAccess Manager が終了されても接続を続行できる、

常時接続です。VZAccess Manager では、AnyConnect をインストールする準備が整うと、自動接続 LAN アダプタをデバイス接続のプリファレンスとして表示します。AnyConnect インターフェイスが検出されると、3G マネージャはインターフェイスをドロップし、AnyConnect 接続を許可します。

優先順位の高い接続に移動する場合（有線ネットワークが最も優先順位が高く、次に WiFi、モバイル ブロードバンドの順になります）、AnyConnect は、古い切断を解除する前に新しい接続を確立します。

Windows での Internet Explorer 信頼済みサイトのリストへの ASA の追加

Active Directory 管理者が Internet Explorer の信頼済みサイトのリストに ASA を追加するには、グループ ポリシーを使用できます。この手順は、ローカル ユーザが Internet Explorer の信頼済みサイトに追加する方法とは異なります。

手順

ステップ 1 Windows ドメイン サーバで、ドメイン管理者グループのメンバーとしてログインします。

ステップ 2 [Active Directory ユーザとコンピュータ（Active Directory Users and Computers）] MMC スナップインを開きます。

ステップ 3 グループ ポリシー オブジェクトを作成するドメインまたは組織ユニットを右クリックして、**[プロパティ（Properties）]** をクリックします。

ステップ 4 **[グループ ポリシー（Group Policy）]** タブを選択して、**[新規（New）]** をクリックします。

ステップ 5 新しいグループ ポリシー オブジェクトの名前を入力して、**Enter** を押します。

ステップ 6 一部のユーザまたはグループにこの新しいポリシーが適用されないようにするには、**[プロパティ（Properties）]** をクリックします。**[セキュリティ]** タブを選択します。このポリシーを適用しないユーザまたはグループを追加し、[許可] カラムの [読み取り] チェックボックスと [グループ ポリシーの適用] チェックボックスをオフにします。[OK] をクリック

ステップ 7 **[編集（Edit）]** をクリックし、**[ユーザの構成（User Configuration）]** > **[Windows の設定（Windows Settings）]** > **[Internet Explorer メンテナンス（Internet Explorer Maintenance）]** > **[セキュリティ（Security）]** を選択します。

ステップ 8 右側のペインで **[セキュリティ ゾーンおよびコンテンツの規則（Security Zones and Content Ratings）]** を右クリックし、**[プロパティ（Properties）]** をクリックします。

ステップ 9 [現行のセキュリティ ゾーンとプライバシーの設定をインポートする（Import the current security zones and privacy settings）] を選択します。プロンプトが表示されたら、**[続行（Continue）]** をクリックします。

ステップ 10 **[設定の変更（Modify Settings）]** をクリックし、**[信頼されたサイト（Trusted Sites）]** を選択して、**[サイト（Sites）]** をクリックします。

ステップ 11 信頼済みサイトのリストに追加するセキュリティ アプライアンスの URL を入力し、**[追加（Add）]** をクリックします。形式は、ホスト名（https://vpn.mycompany.com) または IP アドレ

ス (https://192.168.1.100) を含めることができます。 完全一致 (https://vpn.mycompany.com) またはワイルドカード (https://*.mycompany.com) でも構いません。

ステップ 12 **[閉じる（Close）]** をクリックし、すべてのダイアログボックスが閉じるまで **[OK]** をクリックします。

ステップ 13 ドメインまたはフォレスト全体にポリシーが伝搬されるまで待ちます。

ステップ 14 [インターネット オプション（Internet Options）] ウィンドウで **[OK]** をクリックします。

Internet Explorer でのプロキシ変更のブロック

手順

ステップ 1 ASDM で、**[設定（Configuration）]** > **[リモート アクセス VPN（Remote Access VPN）]** > **[ネットワーク（クライアント）アクセス（Network (Client) Access）]** > **[グループ ポリシー（Group Policies）]** に移動します。

ステップ 2 グループ ポリシーを選択し、新しいグループ ポリシーの **[編集（Edit）]** または **[追加（Add）]** をクリックします。

ステップ 3 ナビゲーション ペインで、**[詳細（Advanced）]** > **[ブラウザ プロキシ（Browser Proxy）]** に移動します。[プロキシ サーバ ポリシー（Proxy Server Policy）] ペインが表示されます。

ステップ 4 [プロキシ ロックダウン（Proxy Lockdown）] をクリックして、その他のプロキシ設定を表示します。

ステップ 5 [継承（Inherit）] をオフにし、次のいずれかを選択します。

- [はい（Yes）] を選択して、AnyConnect セッションの間、プロキシのロックダウンを有効にし、Internet Explorer の [接続（Connections）] タブを非表示にします。
- [いいえ（No）] を選択して、AnyConnect セッションの間、プロキシのロックダウンを無効にし、Internet Explorer の [接続（Connections）] タブを公開します。

ステップ 6 [OK] をクリックして、プロキシ サーバ ポリシーの変更を保存します。

ステップ 7 [適用（Apply）] をクリックして、グループ ポリシーの変更を保存します。

AnyConnect による Windows RDP セッションの処理方法の設定

AnyConnect は、Windows RDP セッションからの VPN 接続を許可するように設定できます。デフォルトでは、RDP によりコンピュータに接続されているユーザは、Cisco AnyConnect Secure Mobility Client を使用して VPN 接続を開始できません。次の表に、RDP セッションからの VPN 接続のログインとログアウトのオプションを示します。これらのオプションは、VPN クライアント プロファイルで設定されます。

設定名	値	SBL モードで使用での使用可否
	• [シングル ローカル ログイン（Single Local Logon）]（デフォルト）：VPN 接続全体で、ログインできるローカル ユーザは 1 人だけです。また、クライアント PC に複数のリモート ユーザがログインしている場合でも、ローカル ユーザが VPN 接続を確立することはできます。この設定は、VPN 接続を介した企業ネットワークからのリモート ユーザ ログインに対しては影響を与えません。 （注） VPN 接続が排他的トンネリング用に設定されている場合、VPN 接続用のクライアント PC のルーティング テーブルが変更されるため、リモート ログインは接続解除されます。VPN 接続がスプリット トンネリング用に設定されている場合、リモート ログインが接続解除されるかどうかは、VPN 接続のルーティング設定によって異なります。 • [シングル ログイン（Single Logon）]：VPN 接続全体で、ログインできるユーザは 1 人だけです。VPN 接続の確立時に、ローカルまたはリモートで複数のユーザがログインしている場合、接続は許可されません。VPN 接続中にローカルまたはリモートで第 2 のユーザがログインすると、VPN 接続が終了します。VPN 接続中の追加のログインは許可されません。そのため、VPN 接続によるリモート ログインは行えません。 （注） 複数同時ログオンはサポートされません。	○

設定名	値	SBL モードで使用での使用可否
[Windows VPN 確立（Windows VPN Establishment）]：	• [ローカルユーザのみ（Local Users Only）]（デフォルト）：リモート ログインしたユーザは、VPN 接続を確立できません。これは、以前のバージョンの AnyConnect と同じ機能です。 • [リモートユーザを許可（Allow Remote Users）]：リモート ユーザは VPN 接続を確立できます。ただし、設定された VPN 接続ルーティングによってリモート ユーザが接続解除された場合は、リモート ユーザがクライアント PC に再アクセスできるように、VPN 接続が終了します。リモート ユーザが VPN 接続を終了せずにリモート ログイン セッションを接続解除するには、VPN を確立した後、90 秒間待つ必要があります。	×

その他の VPN セッションの接続オプションについては、「AnyConnect VPN 接続オプション」を参照してください。

Windows での DES-only SSL 暗号化

デフォルトでは、Windows は DES SSL 暗号化をサポートしません。ASA に DES-only を設定した場合、AnyConnect 接続は失敗します。これらのオペレーティング システムの DES 対応設定は難しいため、ASA には、DES-only SSL 暗号化を設定しないことをお勧めします。

Linux 上での NVM の使用

NVM を Linux 上で使用する場合は、事前にカーネル ドライバ フレームワーク（KDF）をセットアップする必要があります。AnyConnect カーネル モジュールを事前構築するか、ターゲット上にドライバを構築するか、選択できます。ターゲット上に構築する場合、アクションは不要です。構築は、展開時またはリブート時に自動的に処理されます。

AnyConnect カーネル モジュールを構築するための必要条件

ターゲット デバイスを準備します。

- GNU Make Utility がインストールされていることを確認します。
- 次のカーネル ヘッダー パッケージをインストールします。

- RHEL の場合は、kernel-devel-2.6.32-642.13.1.el6.x86_64 などのパッケージ **kernel-devel-$(uname -r)** をインストールします。
- Ubuntu の場合は、linux-headers-4.2.0-27-generic などのパッケージ **linux-headers-$(uname -r)** をインストールします。

- GCC コンパイラがインストールされていることを確認します。インストールされた GCC コンパイラの *major.minor* バージョンが、カーネルの構築に使用されている GCC のバージョンと一致している必要があります。これは、/proc/version ファイルで確認できます。

NVM の構築済み AnyConnect Linux カーネル モジュール とのパッケージ化

始める前に

AnyConnect カーネル モジュールを構築するための必要条件 （8 ページ）に記載されている前提条件を満たす必要があります。

（注） NVM は、セキュア ブートが有効になっているデバイスではサポートされません。

AnyConnect NVM は、構築済みの AnyConnect Linux カーネル モジュールとパッケージ化することができます。こうすると、特にターゲット デバイスの OS カーネル バージョンが同一である場合、すべてのターゲットデバイスに構築する必要がなくなります。事前構築の選択肢を使用しないことにした場合、構築は、展開時またはリブート時に、管理者による入力がなくても自動的に実行され、ターゲット上で使用できるようになります。

（注） 構築済み AnyConnect Linux カーネル モジュールでは、Web 展開はサポートされていません。

手順

ステップ 1 AnyConnect 事前展開パッケージ、anyconnect-linux64-<*version*>-predeploy-k9.tar.gz を解凍します。

ステップ 2 nvm ディレクトリに移動します。

ステップ 3 次のスクリプトを呼び出します。**$sudo ./build_and_package_ac_ko.sh**

スクリプトを実行すると、構築済みの AnyConnect Linux カーネル モジュールを含む anyconnect-linux64-<*version*>-**ac_kdf_ko**-k9.tar.gz が作成されます。このファイルは、事前展開にのみ使用することができます。

次のタスク

ターゲット デバイスの OS カーネルがアップグレードされたら、更新された Linux カーネル モジュールで AnyConnect NVM を再展開する必要があります。

AnyConnect の事前展開

AnyConnect は、SMS を使用した手動による事前展開が可能です。この場合、エンド ユーザがインストールできるファイルを配布するか、AnyConnect ファイル アーカイブにユーザが接続できるようにします。

AnyConnect をインストールするためのファイル アーカイブを作成する場合、「AnyConnect プロファイルを事前展開する場所 （12 ページ）」で説明するように、アーカイブのディレクトリ構造が、クライアントにインストールされるファイルのディレクトリ構造と一致する必要があります。

始める前に

- 手動で VPN プロファイルを展開している場合、ヘッドエンドにもプロファイルをアップロードする必要があります。クライアント システムが接続する場合、クライアントのプロファイルがヘッドエンドのプロファイルに一致することを AnyConnect が確認します。プロファイルのアップデートを無効にしており、ヘッドエンド上のプロファイルがクライアントと異なる場合、手動で展開したプロファイルは動作しません。
- 手動で AnyConnect ISE ポスチャ プロファイルを展開する場合、ISE にもそのファイルをアップロードする必要があります。

手順

ステップ 1 AnyConnect 事前展開パッケージをダウンロードします。

事前展開用の AnyConnect ファイルは cisco.com で入手できます。

OS	AnyConnect 事前展開パッケージ名
Windows	anyconnect-win-*version*-predeploy-k9.zip
macOS	anyconnect-macos-*version*-predeploy-k9.dmg
Linux（64 ビット）	anyconnect-linux64-*version*-predeploy-k9.tar.gz

Umbrella ローミング セキュリティ モジュールは、Linux オペレーティング システムでは使用できません。

ステップ 2 クライアント プロファイルを作成します。一部のモジュールおよび機能にはクライアント プロファイルが必要です。

クライアント プロファイルを必要とするモジュールは次のとおりです。

- AnyConnect VPN
- AnyConnect ネットワーク アクセス マネージャ
- AnyConnect Web セキュリティ
- AnyConnect ISE ポスチャ
- AnyConnect AMP イネーブラ
- ネットワーク可視性モジュール
- Umbrella ローミング セキュリティ モジュール

AnyConnect クライアント プロファイルを必要としないモジュールは次のとおりです。

- AnyConnect VPN Start Before Logon
- AnyConnect Diagnostic and Reporting Tool
- AnyConnect ポスチャ
- AnyConnect カスタマー エクスペリエンス フィードバック

ASDM でクライアント プロファイルを作成して、PC にこれらのファイルをコピーできます。または、Windows PC 上のスタンドアロン プロファイル エディタを使用できます。Windows 上のスタンドアロン エディタの詳細については、「プロファイル エディタについて」を参照してください。

ステップ 3 任意で、AnyConnect クライアントとインストーラのカスタマイズとローカライズ （51 ページ）を行います。

ステップ 4 配布用ファイルを準備します。ファイルのディレクトリ構造は、「AnyConnect プロファイルを事前展開する場所」で説明されています。

ステップ 5 AnyConnect インストール用ファイルをすべて作成したら、これらをアーカイブ ファイルで配布するか、クライアントにファイルをコピーできます。同じ AnyConnect ファイルが、接続する予定のヘッドエンド、ASA、および ISE にも存在することを確認します。

事前展開と Web 展開向けの AnyConnect モジュール実行可能ファイル

次の表に、Windows コンピュータに Umbrella ローミング セキュリティ モジュール、ネットワーク アクセス マネージャ、AMP イネーブラ、ISE ポスチャ、Web セキュリティ、およびネットワーク可視性モジュールの各クライアントを事前展開または Web 展開する際のエンドポイント コンピュータ上のファイル名を示します。

表 *1 : Web* 展開または事前展開のモジュールのファイル名

モジュール	Web 展開インストーラ（ダウンロード）	事前展開インストーラ
ネットワーク アクセス マネージャ	anyconnect-win-*version*-nam-webdeploy-k9.msi	anyconnect-win-*version*-nam-predeploy-k9.msi
Web セキュリティ	anyconnect-win-*version*-websecurity-webdeploy-k9.exe	anyconnect-win-*version*-websecurity-predeploy-k9.msi
ISE ポスチャ	anyconnect-win-*version*-iseposture-webdeploy-k9.msi	anyconnect-win-*version*-iseposture-predeploy-k9.msi
AMP イネーブラ	anyconnect-win-*version*-amp-webdeploy-k9.msi	anyconnect-win-*version*-amp-predeploy-k9.exe
ネットワーク可視性モジュール	anyconnect-win-*version*-nvm-webdeploy-k9.exe	anyconnect-win-*version*-nvm-predeploy-k9.msi
Umbrella ローミング セキュリティ モジュール	anyconnect-win-*version*-umbrella-webdeploy-k9.exe	anyconnect-win-*version*-umbrella-predeploy-k9.msi

AnyConnect 4.3（およびそれ以降）は Visual Studio 2015 ビルド環境に移行しており、そのネットワーク アクセス マネージャ モジュールが機能するためには VS 再頒布可能ファイルが必要です。これらのファイルは、インストールパッケージの一部としてインストールされます。.msi ファイルを使用して、4.3（またはそれ以降）にネットワーク アクセス マネージャ モジュールをアップグレードできますが、最初に AnyConnect セキュア モビリティ クライアントをアップグレードし、リリース 4.3（またはそれ以降）を実行する必要があります。

（注） Windows サーバ OS が存在する場合、AnyConnect ネットワーク アクセス マネージャをインストールするときに、インストール エラーが発生することがあります。WLAN サービスはサーバのオペレーティング システムにデフォルトではインストールされないため、このソフトウェアをインストールし、PC をリブートする必要があります。WLANAutoconfig サービスは、ネットワーク アクセス マネージャがすべての Windows オペレーティング システムで機能するための要件です。

AnyConnect プロファイルを事前展開する場所

クライアント システムにファイルをコピーする場合は、次の表に示す場所にファイルを配置する必要があります。

表 *2 : AnyConnect* コア ファイル

ファイル	説明
anyfilename.xml	AnyConnect プロファイル。このファイルは、特定のユーザ タイプに対して設定される機能および属性値を指定します。

ファイル	説明
AnyConnectProfile.xsd	XML スキーマ フォーマットを定義します。AnyConnect はこのファイルを使用して、プロファイルを検証します。

表 *3:* すべてのオペレーティング システムに対するプロファイルの場所

オペレーティング システム	モジュール	参照先
Windows	VPN を使用するコア クライアント	%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Profile
	ネットワーク アクセス マネージャ	%ProgramData%\Cisco\ Cisco AnyConnect Secure Mobility Client\Network AccessManager\newConfigFiles
	Web セキュリティ	%ProgramData%\Cisco\ Cisco AnyConnect Secure Mobility Client\Web Security
	カスタマー エクスペリエンスのフィードバック	%ProgramData%\Cisco\ Cisco AnyConnect Secure Mobility Client\CustomerExperienceFeedback
	OPSWAT	%PROGRAMFILES%\Cisco\Cisco AnyConnect Secure Mobility Client\opswat
	ISE ポスチャ	%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\ISE Posture
	AMP イネーブラ	%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\AMP Enabler
	ネットワーク可視性モジュール	%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\NVM
	Umbrella ローミング セキュリティ モジュール	

オペレーティング システム	モジュール	参照先
		%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Umbrella （注） Umbrella ローミング セキュリティ モジュールを有効にするためには、Umbrella ダッシュボードから OrgInfo.json ファイルをコピーして、名前を変更しないでこの対象ディレクトリに配置する必要があります。または、インストールする前にファイルを \Profiles\umbrella に配置して、OrgInfo.json ファイルと Umbrella ローミング セキュリティ モジュールインストーラを同じ場所に置くこともできます。

オペレーティング システム	モジュール	参照先
macOS	その他のすべてのモジュール	/opt/cisco/anyconnect/profile
	カスタマー エクスペリエンスのフィードバック	/opt/cisco/anyconnect/CustomerExperienceFeedback
	バイナリ	/opt/cisco/anyconnect/bin
	OPSWAT	/opt/cisco/anyconnect/lib/opswat
	ライブラリ	/opt/cisco/anyconnect/lib
	UI リソース	/Applications/Cisco/Cisco AnyConnect Secure Mobility Client.app/Contents/Resources/
	ISE ポスチャ	/opt/cisco/anyconnect/iseposture/
	AMP イネーブラ	/opt/cisco/anyconnect/ampenabler/
	ネットワーク可視性モジュール	/opt/cisco/anyconnect/NVM/
	Umbrella ローミング セキュリティ モジュール	/opt/cisco/anyconnect/umbrella （注） Umbrella ローミング セキュリティ モジュールを有効にするためには、Umbrella ダッシュボードから OrgInfo.json ファイルをコピーして、名前を変更しないでこの対象ディレクトリに配置する必要があります。または、インストールする前にファイルを \Profiles\umbrella に配置して、OrgInfo.json ファイルと Umbrella ローミング セキュリティ モジュールインストーラを同じ場所に置くこともできます。

オペレーティング システム	モジュール	参照先
Linux	NVM	/opt/cisco/anyconnect/NVM
	その他のすべてのモジュール	/opt/cisco/anyconnect/profile

スタンドアロン アプリケーションとしての AnyConnect モジュールの事前展開

ネットワーク アクセス マネージャ、Web セキュリティ、および Umbrella ローミング セキュリティ モジュールは、スタンドアロン アプリケーションとして実行できます。コア AnyConnect クライアントがインストールされていますが、VPN および AnyConnect UI は使用されません。

Windows での SMS によるスタンドアロン モジュールの展開

手順

ステップ 1 ソフトウェア管理システム（SMS）を設定して MSI プロパティ PRE_DEPLOY_DISABLE_VPN=1 を設定し、VPN 機能を無効にします。次に例を示します。

```
msiexec /package anyconnect-win-version-predeploy-k9.msi /norestart /passive
PRE_DEPLOY_DISABLE_VPN=1 /lvx* <log_file_name>
```

MSI は、MSI に埋め込まれた VPNDisable_ServiceProfile.xml ファイルを VPN 機能のプロファイルに指定されたディレクトリにコピーします。

ステップ 2 モジュールをインストールします。たとえば、次の CLI コマンドは、Web セキュリティをインストールします。

msiexec /package anyconnect-win-*version*-websecurity-predeploy-k9.msi /norestart /passive /lvx* c:\test.log

ステップ 3 （任意）DART をインストールします。

misexec /package annyconnect-win-*version*-dart-predeploy-k9.msi /norestart /passive /lvx* c:\test.log

ステップ 4 難解化 クライアント プロファイルのコピーを、正しい Windows フォルダに保存します。

ステップ 5 Cisco AnyConnect サービスを再起動します。

スタンドアロン アプリケーションとしての AnyConnect モジュールの展開

AnyConnect のネットワーク アクセス マネージャ、Web セキュリティ、および Umbrella ローミング セキュリティ モジュールは、ユーザ コンピュータ上にスタンドアロン アプリケーションとして展開できます。これらのアプリケーションでは、DART がサポートされます。

要件

VPNDisable_ServiceProfile.xml ファイルは、VPN クライアント プロファイル ディレクトリにある唯一の AnyConnect プロファイルである必要もあります。

スタンドアロン モジュールのユーザ インストール

個別のインストーラを取得して、手動で配布できます。

zip イメージをユーザが使用できるようにし、それをインストールするように要求する場合は、スタンドアロン モジュールだけをインストールするように指示してください。

（注） コンピュータ上にネットワーク アクセス マネージャが事前にインストールされていなかった場合、ユーザは、ネットワーク アクセス マネージャのインストールを完了するためにコンピュータをリブートする必要があります。一部のシステム ファイルのアップグレードを必要とする、アップグレード インストールの場合も、ユーザはリブートを必要とします。

手順

ステップ 1 ユーザに AnyConnect ネットワーク アクセス マネージャ、AnyConnect Web セキュリティ モジュール、または Umbrella ローミング セキュリティ モジュールを確認するように指示します。

ステップ 2 [Cisco AnyConnect VPN モジュール（Cisco AnyConnect VPN Module）] チェックボックスをオフにするようユーザに指示します。

このようにすると、コア クライアントの VPN 機能が無効になり、ネットワーク アクセス マネージャ、Web セキュリティ、または Umbrella ローミング セキュリティ モジュールが、インストール ユーティリティによって、VPN 機能なしのスタンドアロン アプリケーションとしてインストールされます。

ステップ 3 （任意）[ロックダウン コンポーネント サービス（Lock Down Component Services）] チェックボックスをオンにします。ロックダウン コンポーネント サービスによって、ユーザは、Windows サービスを無効または停止できなくなります。

ステップ 4 オプション モジュール用のインストーラを実行するようにユーザに指示します。このインストーラでは、VPN サービスなしで AnyConnect GUI を使用できます。ユーザが [選択してインストール（Install Selected）] ボタンをクリックすると、次の処理が行われます。

a) スタンドアロン ネットワーク アクセス マネージャ、スタンドアロン Web セキュリティ モジュール、または Umbrella ローミング セキュリティ モジュールの選択を確認するポップアップ ダイアログボックスが表示されます。
b) ユーザが [OK] をクリックすると、設定値 PRE_DEPLOY_DISABLE_VPN=1 を使用して、インストール ユーティリティにより、AnyConnect コア インストーラが起動されます。
c) インストール ユーティリティは、既存のすべての VPN プロファイルを削除してから VPNDisable_ServiceProfile.xml をインストールします。

d) インストール ユーティリティは、指定に応じて、ネットワーク アクセス マネージャ インストーラ、Web セキュリティ インストーラ、または Umbrella ローミング セキュリティ インストーラを起動します。
e) 指定に応じて、ネットワーク アクセス マネージャ、Web セキュリティ モジュール、または Umbrella ローミング セキュリティ モジュールが、コンピュータ上で VPN サービスなしで有効になります。

Windows への事前展開

zip ファイルを使用した AnyConnect の配布

この zip パッケージ ファイルは、インストール ユーティリティ、個々のコンポーネント インストーラを起動するセレクタ メニュー プログラム、AnyConnect のコア モジュールとオプション モジュール用の MSI を含みます。zip パッケージ ファイルをユーザに対して使用可能にすると、ユーザはセットアップ プログラム（setup.exe）を実行します。このプログラムでは、インストール ユーティリティ メニューが表示されます。このメニューから、ユーザはインストールする AnyConnect モジュールを選択します。多くの場合、ロードするモジュールをユーザが選択しないようにする必要があります。したがって、zip ファイルを使用して配布する場合は、zip を編集し、使用されないようにするモジュールを除外して、HTA ファイルを編集します。

ISO を配布する 1 つの方法は、SlySoft や PowerIS などの仮想 CD マウント ソフトウェアを使用することです。

事前展開 zip の変更

- ファイルをバンドルしたときに作成したすべてのプロファイルを使用して zip ファイルを更新し、配布しないモジュールのインストーラをすべて削除します。
- HTA ファイルを編集して、インストール メニューをカスタマイズし、配布しないモジュールのインストーラへのリンクをすべて削除します。

AnyConnect zip ファイルの内容

ファイル	目的
GUI.ico	AnyConnect アイコン イメージ。
Setup.exe	インストール ユーティリティを起動します。
anyconnect-win-*version*-dart-predeploy-k9.msi	DART モジュール用 MSI インストーラ ファイル。
anyconnect-win-*version*-gina-predeploy-k9.msi	SBL モジュール用 MSI インストーラ ファイル。
anyconnect-win-*version*-iseposture-predeploy-k9.msi	ISE ポスチャ モジュール用 MSI インストーラ。

ファイル	目的
anyconnect-win-*version*-amp-predeploy-k9.exe	AMP イネーブラ用 MSI インストーラ ファイル。
anyconnect-win-*version*-nvm-predeploy-k9.msi	ネットワーク可視性モジュール用 MSI インストーラ ファイル。
anyconnect-win-*version*-umbrella-predeploy-k9.msi	Umbrella ローミング セキュリティ モジュール用 MSI インストーラ ファイル。
anyconnect-win-*version*-nam-predeploy-k9.msi	ネットワーク アクセス マネージャ モジュール用 MSI インストーラ ファイル。
anyconnect-win-*version*-posture-predeploy-k9.msi	ポスチャ モジュール用 MSI インストーラ ファイル。
anyconnect-win-*version*-websecurity-predeploy-k9.msi	Web セキュリティ モジュール用 MSI インストーラ ファイル。
anyconnect-win-*version*-core-vpn-predeploy-k9.msi	AnyConnect コア クライアント用 MSI インストーラ ファイル。
autorun.inf	setup.exe の情報ファイル。
eula.html	Acceptable Use Policy（アクセプタブル ユース ポリシー）の略。
setup.hta	サイトに合わせてカスタマイズできる、インストール ユーティリティ HTML アプリケーション（HTA）。

SMS を使用した AnyConnect の配布

展開するモジュールのインストーラ（*.msi）を zip イメージから抽出した後で、これらを手動で配布できます。

要件

- AnyConnect を Windows にインストールする場合、AlwaysInstallElevated または Windows User Account Control（UAC）グループ ポリシー設定のいずれかを無効にする必要があります。無効にしないと、AnyConnect インストーラはインストールに必要な一部のディレクトリにアクセスできない場合があります。
- Microsoft Internet Explorer（MSIE）ユーザは、信頼済みサイト リストにヘッドエンドを追加するか、Java をインストールする必要があります。信頼済みサイトのリストへの追加により、最低限のユーザ操作で ActiveX コントロールによるインストールが可能になります。

プロファイルの展開プロセス

- MSI インストーラを使用する場合、MSI が Profiles\vpn フォルダに配置されている任意のプロファイルを選択し、インストール中に適切なフォルダに配置します。適切なフォルダパスは、CCO で使用可能な事前展開 MSI ファイルに含まれています。
- インストール後にプロファイルを手動で事前展開する場合は、手動か、Altiris などの SMS を使用してプロファイルをコピーすることにより、適切なフォルダにプロファイルを展開します。
- クライアントに事前展開したプロファイルと同じクライアントプロファイルを、必ずヘッドエンドにも配置してください。このプロファイルは、ASA で使用されるグループ ポリシーに結合する必要もあります。クライアントプロファイルがヘッドエンドのものと一致しないか、グループポリシーに結合されていない場合は、アクセスの拒否など、一貫性のない動作を招く可能性があります。

Windows 事前展開 MSI の例

インストールされるモジュール	コマンドおよびログ ファイル
VPN なしの AnyConnect コア クライアント機能。 スタンドアロン ネットワーク アクセス マネージャまたは Web セキュリティ モジュールをインストールするときに使用します。	msiexec /package anyconnect-win-*version*-core-vpn-predeploy-k9.msi /norestart /passive PRE_DEPLOY_DISABLE_VPN=1 /lvx* anyconnect-win-*version*-core-vpn-predeploy-k9-install-datetimestamp.log
VPN ありの AnyConnect コア クライアント機能。	msiexec /package anyconnect-win-*version*-core-vpn-predeploy-k9.msi /norestart /passive /lvx* anyconnect-win-*version*-core-vpn-predeploy-k9-install-datetimestamp.log
カスタマー エクスペリエンスのフィードバック	msiexec /package anyconnect-win-*version*-core-vpn-predeploy-k9.msi /norestart /passive DISABLE_CUSTOMER_EXPERIENCE_FEEDBACK=1 /lvx* anyconnect-win-*version*-core-vpn-predeploy-k9-install-datetimestamp.log
Diagnostic and Reporting Tool（DART）	msiexec /package anyconnect-win-*version*-dart-predeploy-k9.msi /norestart /passive /lvx* anyconnect-win-*version*-dart-predeploy-k9-install-datetimestamp.log
SBL	msiexec /package anyconnect-win-*version*-gina-predeploy-k9.msi /norestart /passive /lvx* anyconnect-win-*version*-gina-predeploy-k9-install-datetimestamp.log

インストールされるモジュール	コマンドおよびログ ファイル
ネットワーク アクセス マネージャ	msiexec /package anyconnect-win-*version*-nam-predeploy-k9.msi /norestart /passive /lvx* anyconnect-win-*version*-nam-predeploy-k9-install-datetimestamp.log
Web セキュリティ	msiexec /package anyconnect-win-*version*-websecurity-predeploy-k9.msi /norestart/passive /lvx* anyconnect-win-*version*-websecurity-predeploy-k9-install-datetimestamp.log
VPN ポスチャ（HostScan）	msiexec /package anyconnect-win-*version*-posture-predeploy-k9.msi /norestart/passive /lvx* anyconnect-win-*version*-posture-predeploy-k9-install-datetimestamp.log
ISE ポスチャ	msiexec /package anyconnect-win-*version*-iseposture-predeploy-k9.msi /norestart/passive /lvx* anyconnect-win-*version*-iseposture-predeploy-k9-install-datetimestamp.log
AMP イネーブラ	msiexec /package anyconnect-win-*version*-amp-predeploy-k9.msi / norestart/passive /lvx* anyconnect-win-*version*-amp-predeploy-k9-install-datetimestamp.log
ネットワーク可視性モジュール	msiexec /package anyconnect-win-*version*-nvm-predeploy-k9.msi / norestart/passive /lvx* anyconnect-win-*version*-nvm-predeploy-k9-install-datetimestamp.log
Umbrella ローミング セキュリティ	msiexec /package anyconnect-win-*version*-umbrella-predeploy-k9.msi / norestart/passive /lvx* anyconnect-*version*-umbrella-predeploy-k9-install-datetimestamp.log

AnyConnect サンプル Windows トランスフォーム

サンプルの Windows トランスフォームが、その使用方法を説明したドキュメントとともに用意されています。下線文字（_）で始まるトランスフォームは、一般的な Windows トランスフォームで、特定のモジュールインストーラに特定のトランスフォームのみを適用できます。英文字で始まるトランスフォームは VPN トランスフォームです。各トランスフォームには、その使用方法を説明したマニュアルがあります。トランスフォーム ダウンロードは sampleTransforms-*x.x.x*.zip です。

Windows 事前展開セキュリティ オプション

Cisco AnyConnect Secure Mobility Client をホストするデバイスでは、エンド ユーザに限定的なアクセス権を与えることを推奨します。エンドユーザに追加の権限を与える場合、インストーラでは、エンドポイントでロックダウン済みとして設定されている Windows サービスをユーザとローカル管理者がオフにしたり停止したりできないようにするロックダウン機能を提供できます。Web セキュリティ モジュールでは、サービス パスワードを使用してクライアントをバイパス モードにすることができます。また、ユーザが AnyConnect をアンインストールできないようにすることもできます。

Windows ロックダウン プロパティ

各MSIインストーラでは、共通のプロパティ（LOCKDOWN）がサポートされます。これは、ゼロ以外の値に設定されている場合に、そのインストーラに関連付けられた Windows サービスがエンドポイントデバイスでユーザまたはローカル管理者によって制御されないようにします。インストール時に提供されるサンプルのトランスフォーム（anyconnect-vpn-transforms-X.X.xxxxx.zip）を使用して、このプロパティを設定し、ロックダウンする各 MSI インストーラにトランスフォームを適用することを推奨します。ロックダウン オプションも ISO インストール ユーティリティ内のチェックボックスです。

[プログラムの追加と削除（Add/Remove Program List）] リストでの AnyConnect の非表示

Windows の [プログラムの追加と削除（Add/Remove Program List）] リストを表示するユーザに対して、インストールされている AnyConnect モジュールを非表示にできます。ARPSYSTEMCOMPONENT=1 を使用して任意のインストーラを起動した場合、そのモジュールは、Windows の [プログラムの追加と削除（Add/Remove Program List）] リストに表示されません。

サンプルのトランスフォーム（anyconnect-vpn-transforms-X.X.xxxxx.zip）を使用して、このプロパティを設定することを推奨します。非表示にするモジュールごとに、各 MSI インストーラにトランスフォームを適用します。

Windows での AnyConnect モジュールのインストールおよび削除の順序

モジュールのインストーラは、インストールを開始する前に、インストーラがコア クライアントと同じバージョンであることを確認します。バージョンが一致しない場合は、モジュールはインストールされず、不一致がユーザに通知されます。インストールユーティリティを使用する場合は、パッケージ内のモジュールが、まとめてビルドおよびパッケージ化されるため、バージョンは常に一致します。

手順

ステップ 1 AnyConnect モジュールは次の順番でインストールします。

a) AnyConnect コア クライアント モジュールをインストールします。このモジュールは、GUI および VPN 機能（SSL、IPsec の両方）をインストールします。

b) AnyConnect Diagnostic and Reporting Tool（DART）モジュールをインストールします。このモジュールは、AnyConnect コア クライアント インストールに関する有用な診断情報を提供します。
c) Umbrella ローミング セキュリティ モジュール、ネットワーク可視性モジュール、AMP イネーブラ、SBL、ネットワーク アクセス マネージャ、Web セキュリティ、ポスチャ モジュール、ISE 準拠モジュールを任意の順序でインストールします。

ステップ 2 AnyConnect モジュールは次の順番でアンインストールします。

a) Umbrella ローミング セキュリティ モジュール、ネットワーク可視性モジュール、AMP イネーブラ、ネットワーク アクセス マネージャ、Web セキュリティ、ポスチャ、ISE 準拠モジュール、または SBL を任意の順序でアンインストールします。
b) AnyConnect コア クライアントをアンインストールします。
c) 最後に DART をアンインストールします。

DART 情報は、万一アンインストール プロセスが失敗した場合に役立ちます。

（注） 設計上、一部の XML ファイルは AnyConnect のアンインストール後もそのままの状態です。

macOS への事前展開

macOS での AnyConnect のインストールおよびアンインストール

macOS 向け AnyConnect は、すべての AnyConnect モジュールを含む DMG ファイルで配布されます。ユーザが DMG ファイルを開き、AnyConnect.pkg ファイルを実行すると、インストール ダイアログが開始され、インストール方法が手順を追って説明されます。[インストール タイプ（Installation Type）] 画面で、ユーザはインストールするパッケージ（モジュール）を選択できます。

いずれかの AnyConnect モジュールを配布から除外するには、Apple pkgutil ツールを使用し、変更後にパッケージに署名します。ACTransforms.xml を使用してインストーラを変更することもできます。言語と外観をカスタマイズし、その他のインストール アクションを変更できます。これについては、ACTransforms.xml による macOS でのインストーラ動作のカスタマイズ（59 ページ）のカスタマイズの章で説明されています。

macOS への AnyConnect モジュールのスタンドアロン アプリケーションとしてのインストール

VPN なしで、Web セキュリティ モジュール、ネットワーク可視性モジュール、または Umbrella ローミング セキュリティ モジュールのみをインストールできます。VPN および AnyConnect UI は使用されません。

次の手順では、スタンドアロン プロファイル エディタをインストールして、プロファイルを作成し、そのプロファイルを DMG パッケージに追加することによって、モジュールをカスタ

マイズする方法について説明します。また、ブート時に自動的に起動するように AnyConnect ユーザインターフェイスを設定し、モジュールに必要なユーザおよびグループ情報を AnyConnect が提供できるようにします。

手順

ステップ 1 Cisco.com から Cisco AnyConnect Secure Mobility Client DMG ファイルをダウンロードします。

ステップ 2 ファイルを開いて、インストーラにアクセスします。ダウンロードしたイメージは読み取り専用ファイルです。

ステップ 3 ディスク ユーティリティを実行するか、次のようにターミナルアプリケーションを使用して、インストーラ イメージを書き込み可能にします。

```
hdiutil 変換 <source dmg>：UDRW o のフォーマット<output dmg>
```

ステップ 4 Windows オペレーティング システムが実行されているコンピュータにスタンドアロンのプロファイル エディタをインストールします。カスタム インストールまたは完全インストールの一部として、必要な AnyConnect モジュールを選択する必要があります。デフォルトではインストールされていません。

ステップ 5 プロファイル エディタを起動して、プロファイルを作成します。

ステップ 6 セキュアな場所に、`WebSecurity_ServiceProfile.xml`、`NVM_ServiceProfile.xml`、または `OrgInfo.json`（ダッシュボードから取得します）としてプロファイルを適切に保存します。

これらのモジュールについて、プロファイルエディタが Web セキュリティ用に難解化バージョンのプロファイル（`WebSecurity_ServiceProfile.wso` など）を作成し、Web セキュリティ用のファイル（`WebSecurity_ServiceProfile.xml` など）を保存したのと同じ場所に保存します。難解化を完了するには、以下のステップに従います。

a) 指定した .wso ファイルを Windows デバイスから Web セキュリティ用の適切なフォルダ パス（`AnyConnect x.x.x /Profiles/websecurity` など）の macOS インストーラ パッケージにコピーします。または、Web セキュリティ インスタンスに対して以下のような端末アプリケーションを使用します。

```
cp <path to the wso> \Volumes\"AnyConnect <VERSION>"\Profiles\websecurity\
```

b) macOS インストーラで、`AnyConnect x.x.x/Profiles` ディレクトリに移動し、編集用に TextEdit で `ACTransforms.xml` ファイルを開きます。VPN 機能がインストールされないように、`<DisableVPN>` 要素を true に設定します。

```
<ACTransforms>
<DisableVPN>true</DisableVPN>
</ACTransforms>
```

c) これで、AnyConnect DMG パッケージをユーザに配布する準備ができました。

macOS 上のアプリケーションの制限

ゲートキーパーは、システムでの実行を許可するアプリケーションを制限します。次からダウンロードされたアプリケーションを許可するか選択できます。

- Mac App Store
- Mac App Store and identified developers
- あらゆる場所

デフォルト設定は Mac App Store and identified developers（署名付きアプリケーション）です。

最新バージョンの AnyConnect は、Apple 証明書を使用した署名付きアプリケーションです。ゲートキーパーが Mac App Store（のみ）に設定されている場合、事前展開されたインストールから AnyConnect をインストールして実行するには、[あらゆる場所（Anywhere）] 設定を選択するか、またはCtrlキーを押しながらクリックして選択した設定をバイパスする必要があります。詳細については、http://www.apple.com/macosx/mountain-lion/security.html を参照してください。

Linux への事前展開

Linux 用モジュールのインストール

Linux 用の個々のインストーラを取り出して、手動で配布できます。事前展開パッケージ内の各インストーラは、個別に実行できます。tar.gz ファイル内のファイルの表示および解凍には、圧縮ファイル ユーティリティを使用します。

手順

ステップ 1 AnyConnect コア クライアント モジュールをインストールします。このモジュールは、GUI および VPN 機能（SSL、IPsec の両方）をインストールします。

ステップ 2 DART モジュールをインストールします。このモジュールは、AnyConnect コア クライアントインストールに関する、有用な診断情報を提供します。

ステップ 3 ポスチャ モジュールまたは ISE 準拠モジュールをインストールします。

ステップ 4 NVM をインストールします。

Linux 用モジュールのアンインストール

ユーザが AnyConnect をアンインストールする順序は重要です。

DART 情報は、アンインストール プロセスが失敗した場合に役立ちます。

手順

ステップ 1 NVM をアンインストールします。
ステップ 2 ポスチャ モジュールまたは ISE 準拠モジュールをアンインストールします。
ステップ 3 AnyConnect コア クライアントをアンインストールします。
ステップ 4 DART をアンインストールします。

Linux デバイスへの NVM の手動インストール/アンインストール

手順

ステップ 1 AnyConnect 事前展開パッケージを解凍します。
ステップ 2 nvm ディレクトリに移動します。
ステップ 3 次のスクリプトを呼び出します。**$sudo ./nvm_install.sh**

/opt/cisco/anyconnect/bin/nvm_uninstall.sh を使用して、NVM をアンインストールできます。

Firefox でのサーバ証明書検証の初期化

AnyConnect でサーバ証明書を使用する場合は、AnyConnect が証明書にアクセスして信頼済みとして検証できるように、証明書ストアを使用可能にする必要があります。デフォルトでは、AnyConnect は Firefox 証明書ストアを使用します。

Firefox 証明書ストアをアクティブにする方法

AnyConnect を Linux デバイスにインストールした後、AnyConnect 接続を初めて試行する前に、Firefox ブラウザを開始します。Firefox を開くと、プロファイルが作成され、そこに証明書ストアが含まれます。

Firefox 証明書ストアを使用しない場合

Firefox を使用しない場合、Firefox 証明書ストアを除外するローカル ポリシーを設定し、PEM ストアを設定する必要があります。

複数モジュールの要件

1 つ以上のオプション モジュールに加えてコア クライアントを展開する場合、ロックダウン プロパティを各インストーラに適用する必要があります。ロックダウンについては、Windows 事前展開 MSI の例 （21 ページ）で説明しています。

このアクションは、VPN インストーラ、ネットワーク アクセス マネージャ、Web セキュリティ、ネットワーク可視化モジュール、および Umbrella ローミング セキュリティ モジュールに使用できます。

（注） VPN インストーラのロックダウンをアクティブにすると、その結果として AMP イネーブラもロックダウンされます。

Linux デバイスへの DART の手動インストール

1. anyconnect-dart-linux-(ver)-k9.tar.gz をローカルに保存します。
2. 端末から、**tar -zxvf <***path to tar.gz file including the file name* コマンドを使用して tar.gz ファイルを抽出します。
3. 端末から、抽出したフォルダに移動し、**sudo ./dart_install.sh** コマンドを使用して dart_install.sh を実行します。
4. ライセンス契約書に同意し、インストールが完了するまで待機します。

（注） DART のアンインストールには、**/opt/cisco/anyconnect/dart/dart_uninstall.sh** しか使用できません。

Web 展開 AnyConnect

Web 展開とは、クライアント システム上の AnyConnect ダウンローダがヘッドエンドから AnyConnect ソフトウェアを取得するか、またはヘッドエンドのポータルを使用して AnyConnect をインストールまたは更新することです。ブラウザのサポート（および Java と ActiveX の要件）にあまりにも大きく依存していた従来の Web 起動に代わり、自動 Web 展開のフローを改善しました。このフローは、クライアントレス ページからの初期ダウンロードおよび開始時に提示されます。

ASA での Web 展開

ASA のクライアントレス ポータルは、AnyConnect を Web 展開します。プロセス フローは次のとおりです。

ユーザがブラウザを開き、ASA のクライアントレス ポータルに接続します。ポータルで、ユーザが **[AnyConnect クライアントの起動（Start AnyConnect Client）]** ボタンをクリックします。これで、AnyConnect パッケージを手動でダウンロードできます。NPAPI（Netscape プラグイン アプリケーション プログラミング インターフェイス）プラグインをサポートするブラウザを実行している場合は、タブを使用して、weblaunch（ActiveX または Java）で自動 Web プロビジョニングを開始することもできます。

ASA Web 展開の制限

- 同じ OS 用の複数の AnyConnect パッケージを ASA にロードすることはサポートされていません。
- OPSWAT 定義は、Web 展開時には VPN ポスチャ（HostScan）モジュールに含まれません。OPSWAT 定義をクライアントに配信するには、HostScan モジュールを手動で展開するか、または ASA にロードする必要があります。
- ASA にデフォルトの内部フラッシュ メモリ サイズしかない場合、ASA に複数の AnyConnect クライアント パッケージを保存およびロードすると問題が生じる可能性があります。フラッシュ メモリにパッケージ ファイルを保持するために十分な容量がある場合でも、クライアント イメージの unzip とロードのときに ASA のキャッシュ メモリが不足する場合があります。AnyConnect 展開時および ASA メモリのアップグレード時の ASA メモリ要件の詳細については、VPN アプライアンスの最新のリリース ノートを参照してください。
- ユーザは IP アドレスまたは DNS を使用して ASA に接続できますが、リンクローカル セキュア ゲートウェイ アドレスはサポートされていません。
- Internet Explorer の信頼済みサイトのリストに Web 起動をサポートするセキュリティ アプライアンスの URL を追加する必要があります。これは、「Windows での Internet Explorer 信頼済みサイトのリストへの ASA の追加」の説明に従って、グループ ポリシーを使用して行うことができます。

ISE による Web 展開

ISE のポリシーでは、AnyConnect クライアントをいつ展開するかを指定します。ユーザがブラウザを開き、ISE によって制御されるリソースに接続すると、ユーザは AnyConnect クライアント ポータルにリダイレクトされます。その ISE ポータルでは、ユーザが AnyConnect をダウンロードし、インストールできます。Internet Explorer では、ActiveX コントロールに従ってインストールを進めます。他のブラウザでは、ポータルによって Network Setup Assistant がダウンロードされ、ユーザがそれを使用して AnyConnect をインストールします。

ISE 展開の制限

- ISE と ASA の両方が AnyConnect を Web 展開する場合は、設定が両方のヘッドエンドで一致する必要があります。
- ISE サーバが AnyConnect ISE ポスチャ エージェントによって検出されるのは、そのエージェントが ISE クライアント プロビジョニング ポリシーに設定されている場合だけです。ISE 管理者は、[エージェント設定（Agent Configuration）] > [ポリシー（Policy）] > [クライアント プロビジョニング（Client Provisioning）] で NAC Agent または AnyConnect ISE ポスチャ モジュールを設定します。

ASA での Web 展開の設定

WebLaunch のブラウザの制限

表 *4:* オペレーティング システムによる *WebLaunch* 用の *AnyConnect* ブラウザ サポート

オペレーティング システム	ブラウザ
現在の Microsoft Windows 10 x86 (32 ビット) と x64 (64 ビット) のバージョンのサポート	Internet Explorer 11
Windows 8.x x86（32 ビット）および x64（64 ビット）	Internet Explorer 11
Windows 7 SP1 x86（32 ビット）および x64（64 ビット）	Internet Explorer 11
macOS 10.11、10.12、10.13、および 10.14 （64 ビット）	Safari 11

（注） EDGE ブラウザは Active-X をサポートしていないため、プロビジョニング ページでは自動プロビジョニング オプションが表示されません。

（注） Web 起動は、NPAPI（Netscape プラグイン アプリケーション プログラミング インターフェイス）プラグインをサポートするすべてのブラウザで機能します。

また、AnyConnect Umbrella ローミング セキュリティ モジュールの追加には、Microsoft .NET 4.0 が必要です。

AnyConnect パッケージのダウンロード

Cisco AnyConnect Software Download の Web ページから最新の Cisco AnyConnect Secure Mobility Client パッケージをダウンロードします。

OS	AnyConnect Web 展開パッケージ名
Windows	anyconnect-win-*version*-webdeploy-k9.pkg
macOS	anyconnect-macos-*version*-webdeploy-k9.pkg
Linux（64 ビット）	anyconnect-linux64-*version*-webdeploy-k9.pkg

（注） ASA で同じオペレーティング システムの異なるバージョンを使用してはなりません。

ASA での AnyConnect パッケージのロード

手順

ステップ 1 **[設定（Configuration）] > [リモート アクセス（Remote Access）] > [VPN] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [AnyConnect クライアント ソフトウェア（AnyConnect Client Software）]** に移動します。[AnyConnect クライアント イメージ（AnyConnect Client Images）] パネルに、現在 ASA にロードされている AnyConnect イメージが表示されます。イメージが表示される順序は、ASA がリモート コンピュータにイメージをダウンロードした順序です。

ステップ 2 AnyConnect イメージを追加するには、[追加（Add）] をクリックします。

- ASA にアップロードした AnyConnect イメージを選択するには、[フラッシュの参照（Browse Flash）] をクリックします。
- コンピュータ上にローカルに保存した AnyConnect イメージを参照して選択するには、[アップロード（Upload）] をクリックします。

ステップ 3 [OK] または [アップロード（Upload）] をクリックします。

ステップ 4 [Apply] をクリックします。

追加の AnyConnect モジュールの有効化

追加機能を有効にするには、グループ ポリシーまたはローカル ユーザ設定で新しいモジュール名を指定します。追加モジュールの有効化は、ダウンロード時間に影響することに注意してください。機能を有効にすると、AnyConnect は VPN エンドポイントにそれらのモジュールをダウンロードする必要があります。

（注） Start Before Logon を選択した場合は、AnyConnect クライアント プロファイルでもこの機能を有効にする必要があります。

手順

ステップ 1 ASDM で、**[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [グループ ポリシー（Group Policies）]** に移動します。

ステップ 2 グループ ポリシーを選択し、新しいグループ ポリシーの **[編集（Edit）]** または **[追加（Add）]** をクリックします。

ステップ 3 ナビゲーション ペインで、**[VPN ポリシー（VPN Policy）]** > **[AnyConnect クライアント（AnyConnect Client）]** の順に選択します。[ダウンロードするクライアント モジュール（Client Modules to Download）] で [追加（Add）] をクリックし、このグループ ポリシーに追加する各モジュールを選択します。使用可能なモジュールは、ASA に追加またはアップロードしたモジュールです。

ステップ 4 [適用（Apply）] をクリックし、変更をグループ ポリシーに保存します。

ASDM でのクライアント プロファイルの作成

ASA でクライアント プロファイルを作成する前に、AnyConnect Web 展開パッケージを追加する必要があります。

手順

ステップ 1 **[設定（Configuration）]** > **[リモートアクセスVPN（Remote Access VPN）]** > **[ネットワーク(クライアント)アクセス（Network (Client) Access）]** > **[AnyConnectクライアントプロファイル（AnyConnect Client Profile）]** に移動します。

ステップ 2 グループと関連付けるクライアント プロファイルを選択し、[グループ ポリシーの変更（Change Group Policy）] をクリックします。

ステップ 3 [プロファイル ポリシー名のポリシーの変更（Change Policy for Profile policy name）] ウィンドウで、[使用可能なグループ ポリシー（Available Group Policies）] フィールドからグループ ポリシーを選択し、右矢印をクリックして [ポリシー（Policies）] フィールドに移動します。

ステップ 4 [OK] をクリックします。

ステップ 5 [AnyConnect クライアント プロファイル（AnyConnect Client Profile）] ページで、[適用（Apply）] をクリックします。

ステップ 6 [保存（Save）] をクリックします。

ステップ 7 設定が終了したら、[OK] をクリックします。

ISE での Web 展開の設定

ISE は、ISE のポスチャをサポートするために、AnyConnect コア、ISE ポスチャ モジュール、および OPSWAT（コンプライアンス モジュール）を設定して展開できます。また、ISE は、ASA に接続する場合に使用可能なすべての AnyConnect モジュールおよびリソースを展開できます。ユーザが ISE によって制御されるリソースを参照すると次のようになります。

- ISE が ASA の背後にある場合、ユーザは ASA に接続し、AnyConnect をダウンロードし、VPN 接続を確立します。AnyConnect ISE ポスチャが ASA によってインストールされてい

ない場合、ISE ポスチャをインストールするために、ユーザは AnyConnect クライアント ポータルにリダイレクトされます。

- ISE が ASA の背後にない場合、ユーザは AnyConnect クライアント ポータルに接続し、ISE 上の AnyConnect 設定で定義された AnyConnect リソースをインストールするように誘導されます。一般的な設定では、ISE ポスチャ ステータスが不明な場合、ブラウザが AnyConnect クライアント プロビジョニング ポータルにリダイレクトされます。
- ユーザが ISE 内の AnyConnect クライアント プロビジョニング ポータルに誘導されると次のようになります。
  - ブラウザが Internet Explorer の場合、ISE は AnyConnect ダウンローダをダウンロードし、ダウンローダが AnyConnect をロードします。
  - 他のすべてのブラウザの場合、ISEはクライアントプロビジョニング リダイレクション ポータルを開きます。ここには、Network Setup Assistant（NSA）ツールをダウンロードするためのリンクが表示されます。ユーザはNSAを実行します。これにより、ISE サーバが検出され、AnyConnect ダウンローダがダウンロードされます。

    NSA が Windows での実行を終了した場合、自動的に削除されます。macOS での実行を終了した場合は、手動で削除する必要があります。

ISE のマニュアルでは、次の方法について説明しています。

- ISE で AnyConnect 設定プロファイルを作成する
- ローカル デバイスから ISE に AnyConnect リソースを追加する
- リモート サイトから AnyConnect プロビジョニング リソースを追加する
- AnyConnect クライアントおよびリソースを展開する

（注） AnyConnect ISE ポスチャ モジュールでは、検出時に Web プロキシ ベースのリダイレクションはサポートされていないため、非リダイレクションベースの検出を使用することをお勧めします。詳細については、『Cisco Identity Services Engine Administrator Guide』の「Client Provisioning Without URL Redirection for Different Networks」セクションを参照してください。

ISE では、次の AnyConnect リソースの設定および展開が可能です。

- AnyConnect コアおよびモジュール（ISE ポスチャ モジュールを含む）
- プロファイル：ネットワーク可視性モジュール、AMP イネーブラ、VPN、ネットワーク アクセス マネージャ、Webセキュリティ、カスタマーフィードバック、およびAnyConnect ISE ポスチャ
- カスタマイズ用ファイル
  - UI リソース
  - バイナリ、接続スクリプト、およびヘルプ ファイル

- ローカリゼーション ファイル
  - メッセージのローカリゼーション用 AnyConnect gettext 変換
  - Windows インストーラ トランスフォーム

ISE アップロードのための AnyConnect ファイルの準備

- オペレーティング システムの AnyConnect パッケージ、およびローカル PC に展開する他の AnyConnect リソースをダウンロードします。

（注） ASA を使用すると、インストールは VPN のダウンローダによって行われます。ダウンロードでは、ISE ポスチャ プロファイルは ASA によってプッシュされ、後続のプロファイルのプロビジョニングに必要なホスト検出が利用可能になってから、ISE ポスチャ モジュールが ISE に接続します。その一方、ISE では、ISE ポスチャ モジュールは ISE が検出された後にのみプロファイルを取得し、これがエラーの原因になることがあります。したがって、VPN に接続するとき ASA を ISE ポスチャ モジュールにプッシュすることを推奨します。

- 展開するモジュールのプロファイルを作成します。最低でも、AnyConnect ISE ポスチャ プロファイルを作成します。
- ISE バンドルと呼ばれる ZIP アーカイブにカスタマイズおよびローカリゼーション リソースを統合します。バンドルには次を含めることができます。
  - AnyConnect UI リソース
  - VPN 接続スクリプト
  - ヘルプ ファイル
  - インストーラ トランスフォーム

  AnyConnect ローカリゼーション バンドルには、次を含めることができます。
  - バイナリ形式の AnyConnect gettext 変換
  - インストーラ トランスフォーム

ISE バンドルの作成については、「ISE 展開のための AnyConnect カスタマイズおよびローカリゼーションの準備」で説明します。

AnyConnect を展開するための ISE の設定

追加の AnyConnect リソースをアップロードして作成する前に、AnyConnect パッケージを ISE にアップロードする必要があります。

（注） ISE で AnyConnect 設定オブジェクトを設定する場合、[AnyConnect モジュールの選択（AnyConnect Module Selection）] の下にある VPN モジュールの選択を解除しても、展開された、またはプロビジョニングされたクライアントの VPN は無効になりません。

1. ISE で、**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（results）]** > を選択します。[クライアント プロビジョニング（Client Provisioning）] を展開して [リソース（Resources）] を表示して、[リソース（Resources）] を選択します。
2. **[追加（Add）]** > **[ローカル ディスクからのエージェント リソース（Agent resources from local disk）]** を選択して、AnyConnect パッケージ ファイルをアップロードします。展開を計画しているその他の AnyConnect リソースについて、ローカル ディスクからのエージェント リソースの追加を繰り返して行ってください。
3. **[追加（Add）]** > **[AnyConnect設定（AnyConnect Configuration）]** > を選択します。この AnyConnect 設定は、次の表に示すように、モジュール、プロファイル、カスタマイズ/言語パッケージ、および OPSWAT パッケージを設定します。

   AnyConnect ISE ポスチャ プロファイルは、ISE、ASA、または Windows AnyConnect プロファイル エディタで作成および編集できます。次の表では、ISE の各 AnyConnect リソースの名前およびリソース タイプの名前について説明します。

   表 *5 : ISE* の *AnyConnect* リソース

プロンプト	ISE リソース タイプと説明
AnyConnect パッケージ	AnyConnectDesktopWindows AnyConnectDesktopOSX AnyConnectWebAgentWindows AnyConnectWebAgentOSX
コンプライアンス モジュール	AnyConnectComplianceModuleWindows AnyConnectComplianceModuleOSX
AnyConnect プロファイル	AnyConnectProfile ISE により、アップロードされた AnyConnect パッケージで提供される各プロファイルのチェックボックスが表示されます。
カスタマイゼーション バンドル	AnyConnectCustomizationBundle
ローカリゼーション バンドル	AnyConnectLocalizationBundle

4. ロールまたは OS ベースのクライアント プロビジョニング ポリシーを作成します。AnyConnect および ISE レガシー NAC/MAC エージェントを、クライアント プロビジョニングのポスチャ エージェントに選択できます。各 CP ポリシーは、AnyConnect エージェン

トまたはレガシー NAC/MAC エージェントのいずれか 1 つのエージェントのみをプロビジョニングできます。AnyConnect エージェントを設定する場合、ステップ 2 で作成した AnyConnect 設定を 1 つ選択します。

FTD での Web 展開の設定

Firepower Threat Defense（FTD）デバイスは、ASA と同様のセキュア ゲートウェイ機能を提供する次世代ファイアウォール（NGFW）です。FTD デバイスは、AnyConnect セキュア モビリティ クライアントを使用する リモート アクセス VPN（RA VPN）のみをサポートしており、その他のクライアントまたはクライアントレス VPN アクセスはサポートしていません。トンネルの確立と接続は、IPsec IKEv2 または SSL で行われます。FTD デバイスに接続するときには、IKEv1 はサポートされません。

Windows、Mac、および Linux の AnyConnect クライアントは FTD ヘッドエンド上で設定され、接続時に展開されます。すると、リモートユーザは、クライアント ソフトウェアのインストールおよび設定不要で、SSL または IKEv2 IPsec VPN クライアントの利点を利用できるようになります。以前からインストールされているクライアントの場合は、ユーザの認証時に、FTD ヘッドエンドによってクライアントのリビジョンが点検され、必要に応じてアップグレードされます。

以前にインストールされたクライアントがない場合、リモートユーザは、設定されているインターフェイスの IP アドレスを入力し、AnyConnect クライアントをダウンロードおよびインストールします。FTD ヘッドエンドは、リモート コンピュータのオペレーティング システムに適合するクライアントをダウンロードおよびインストールして、セキュリティで保護された接続を確立します。

Apple iOS デバイスおよび Android デバイス用の AnyConnect アプリは、当該プラットフォームのアプリ ストアからインストールされます。これらは、必要最小限の設定で、FTD ヘッドエンドへの接続を確立します。AnyConnect ソフトウェアの配布には、他のヘッドエンド デバイスおよび環境と同様、この章で説明する代替的な展開方法が使用できます。

現在、FTD での設定およびエンドポイントへの配布が可能なのは、中核的な AnyConnect VPN モジュールと、AnyConnect VPN プロファイルのみです。Firepower Management Center（FMC）のリモート アクセス VPN ポリシー ウィザードを使用すると、これらの基本的 VPN 機能を迅速かつ簡単にセットアップできます。

AnyConnect および FTD の注意事項と制約事項

- サポートされている VPN クライアントは、Cisco AnyConnect セキュア モビリティ クライアントのみです。それ以外のクライアントまたはネイティブ VPN はサポートされていません。クライアントレス VPN は、AnyConnect クライアントの展開に使用されるだけで、エンティティ自体としてはサポートされていません。
- FTD で AnyConnect を使用するには、バージョン 4.0 以降の AnyConnect と、バージョン 6.2.1 以降の FMC が必要です。

- FMC 自体は AnyConnect プロファイル エディタをサポートしていません。VPN プロファイルを別途で設定する必要があります。VPN プロファイル および AnyConnect VPN パッケージはFMC にファイル オブジェクトとして追加され、RA VPN 設定の一部となります。
- セキュア モビリティ、ネットワーク アクセス マネジメント、およびその他すべての AnyConnect モジュールと、それらのコア VPN 機能を超えたプロファイルは、現在サポートされていません。
- VPN ロード バランシングはサポートされません。
- ブラウザ プロキシはサポートされません。
- すべてのポスチャ派生機能（HostScan、エンドポイント ポスチャ アセスメント、および ISE）と、クライアント ポスチャに基づくダイナミック アクセス ポリシーは、サポートされていません。
- Firepower Threat Defense デバイスは、AnyConnect のカスタマイズまたはローカライズに必要なファイルの設定または展開を行いません。
- デスクトップ クライアントでの遅延アップグレードやモバイル クライアントでのアプリごとの VPN など、AnyConnect クライアント上でカスタム属性を必要とする機能は、FTD ではサポートされません。
- FTDヘッドエンドでローカルに認証を行うことはできません。したがって、設定されているユーザは、リモート接続に使用できません。FTD が認証局の役割を果たすことはできません。また、次の認証機能はサポートされていません。
  - セカンダリ認証または二重認証
  - SAML 2.0 を使用するシングル サインオン
  - TACACS、Kerberos（KCD 認証）および RSA SDI
  - LDAP 認証（LDAP 属性マップ）
  - RADIUS CoA

FTD 上での AnyConnect の設定および展開の詳細については、適切なリリース（リリース 6.2.1 以降）の『Firepower Management Center Configuration Guide』の「*Firepower Threat Defense Remote Access VPN*」の章を参照してください。

AnyConnect ソフトウェアおよびプロファイルの更新

AnyConnect は、いくつかの方法で更新できます。

- AnyConnect クライアント：AnyConnect が ASA に接続する場合、AnyConnect ダウンローダは新しいソフトウェアまたはプロファイルが ASA にロードされたかどうかを確認します。それらの更新はクライアントにダウンロードされ、VPN トンネルが確立されます。

- クラウド更新：Umbrella ローミング セキュリティ モジュールは、Umbrella クラウド インフラストラクチャからインストールされたすべての AnyConnect モジュールの自動更新を提供できます。クラウド更新では、ソフトウェア アップグレードは Umbrella クラウド インフラストラクチャから自動的に得られます。更新トラックは管理者のアクションではなくこれによって決まります。デフォルトでは、クラウド更新からの自動更新は無効です。
- ASA または FTD ポータル：ASA のクライアントレス ポータルに接続して更新を取得するように、ユーザに指示します。FTD は、コア VPN モジュールのみをダウンロードします。
- ISE：ユーザが ISE に接続すると、ISE は AnyConnect 設定を使用して、更新されたコンポーネントまたは新しいポスチャ要件があるかどうかを確認します。更新を利用できる場合、ユーザは、ASA、ワイヤレス コントローラ、またはスイッチなどのネットワーク アクセス デバイス（NAD）に接続します。認証時、ユーザは NAD によって ISE ポータルにリダイレクトされ、パッケージの抽出とインストールを管理するために、AnyConnect のダウンローダがクライアントにインストールされます。

エンドユーザに遅延更新を許可することができ、ヘッドエンドに更新をロードしてもクライアントの更新を回避することもできます。

アップグレード例のフロー

前提条件

ここでの例の前提は次のとおりです。

- クライアントのポスチャ ステータスを使用してどのタイミングでクライアントを ISE の AnyConnect クライアント プロビジョニング ポータルにリダイレクトするかを決定する Dynamic Authorization Control List（DACL）を ISE に作成し、ASA にプッシュしておきます。
- ISE は、ASA の背後にあります。

AnyConnect がクライアントにインストールされている

1. ユーザが AnyConnect を起動し、クレデンシャルを入力し、[接続（Connect）] をクリックします。
2. ASA がクライアントとの SSL 接続を開いて認証クレデンシャルを ISE に渡し、ISE がクレデンシャルを検証します。
3. AnyConnect が AnyConnect ダウンローダを起動し、ダウンローダがアップグレードを実行し、VPN トンネルを開始します。

ISE ポスチャが ASA によってインストールされなかった場合は、次のようになります。

1. ユーザが任意のサイトを参照し、DACL によって ISE の AnyConnect クライアント プロビジョニング ポータルにリダイレクトされます。
2. ブラウザが Internet Explorer の場合、ActiveX コントロールが AnyConnect ダウンローダを起動します。その他のブラウザの場合、ユーザが Network Setup Assistant（NSA）をダウンロードして実行し、NSA が AnyConnect ダウンローダをダウンロードして起動します。

3. AnyConnect ダウンローダが ISE に設定された AnyConnect アップグレード（これには、AnyConnect ISE ポスチャ モジュールが含まれています）を実行します。
4. クライアントの ISE ポスチャ エージェントがポスチャを起動します。

AnyConnect がインストールされていない

1. ユーザがサイトを参照して、ASA クライアントレス ポータルへの接続を開始します。
2. ユーザが認証クレデンシャルを入力し、これが ISE に渡されて検証されます。
3. AnyConnect ダウンローダが、Internet Explorer では ActiveX コントロールによって起動され、他のブラウザでは Java アプレットによって起動されます。
4. AnyConnect ダウンローダが ASA に設定されたアップグレードを実行し、VPN トンネルを開始します。ダウンローダが完了します。

ISE ポスチャが ASA によってインストールされなかった場合は、次のようになります。

1. ユーザがサイトを再度参照し、ISE の AnyConnect クライアント プロビジョニング ポータルにリダイレクトされます。
2. Internet Explorer では、ActiveX コントロールが AnyConnect ダウンローダを起動します。その他のブラウザの場合、ユーザが Network Setup Assistant をダウンロードして実行し、これが AnyConnect ダウンローダをダウンロードして起動します。
3. AnyConnect ダウンローダが、既存の VPN トンネルによって ISE に設定されたアップグレード（これには、AnyConnect ISE ポスチャ モジュールの追加が含まれています）を実行します。
4. ISE ポスチャ エージェントがポスチャ評価を開始します。

AnyConnect 自動更新の無効化

クライアント プロファイルを設定し、配布することによって、AnyConnect 自動更新を無効にしたり、制限したりできます。

- VPN クライアント プロファイル：
  - 自動更新では、自動更新を無効にします。このプロファイルは、AnyConnect の Web 展開インストールに含めるか、既存のクライアント インストールに追加できます。ユーザがこの設定を切り替えられるようにすることもきます。
- VPN ローカル ポリシー プロファイル：
  - ダウンローダのバイパスにより、ASA の更新されたコンテンツがクライアントにダウンロードされないようにします。
  - 更新ポリシーにより、さまざまなヘッドエンドへの接続時のソフトウェアおよびプロファイルの更新をきめ細かく制御できます。

ユーザに WebLaunch 中に AnyConnect のダウンロードを求めるプロンプトの表示

リモート ユーザに対して Web 展開の開始を求めるプロンプトを表示するように ASA を設定し、ユーザが AnyConnect をダウンロードするか、クライアントレス ポータル ページを表示するかを選択できる期間を設定できます。

ユーザに AnyConnect のダウンロードを求めるプロンプトの表示は、グループ ポリシーまたはユーザ アカウントで設定されます。次の手順は、グループ ポリシーでこの機能を有効にする方法を示しています。

手順

ステップ 1 ASDM で、**[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [グループ ポリシー（Group Policies）]** に移動します。

ステップ 2 グループ ポリシーを選択し、新しいグループ ポリシーの **[編集（Edit）]** または **[追加（Add）]** をクリックします。

ステップ 3 ナビゲーション ペインで、**[詳細（Advanced）] > [AnyConnect クライアント（AnyConnect Client）] > [ログイン設定（Login Settings）]** を選択します。必要に応じて [継承（Inherit）] チェックボックスをオフにし、[ログイン後の設定（Post Login setting）] を選択します。

ユーザにプロンプトを表示する場合は、タイムアウト時間を指定し、その時間経過後のデフォルト動作を [デフォルトのログイン後選択（Default Post Login Selection）] 領域で選択します。

ステップ 4 [OK] をクリックし、変更をグループ ポリシーに適用して、[保存（Save）] をクリックします。

ユーザに対するアップグレード遅延の許可

「AnyConnect 自動更新の無効化」の説明に従って AutoUpdate を無効にし、ユーザに AnyConnect の更新の受け入れを強制できます。AutoUpdate はデフォルトでオンになっています。

遅延アップデートを設定して、ユーザがクライアントのアップデートを後で行うことを許可できます。遅延アップデートが設定されている場合に、クライアントのアップデートが利用可能になると、AnyConnect は更新を実行するか延期するかをユーザに尋ねるダイアログを開きます。遅延アップグレードは、すべての Windows、Linux、および OS X でサポートされます。

ASA での遅延アップデートの設定

ASA では、遅延アップデートはカスタム属性を追加し、グループ ポリシーでその属性を参照および設定することで有効になります。遅延アップデートを使用するには、**すべての**カスタム属性を作成し、設定する必要があります。

ASA 設定にカスタム属性を追加するための手順は、実行中の ASA/ASDM のリリースによって異なります。カスタム属性の設定手順については、ASA/ASDM の展開リリースに対応した

『*Cisco ASA Series VPN ASDM Configuration Guide*』および『*Cisco ASA Series VPN CLI Configuration Guide*』を参照してください。

次の属性と値により、ASDM に遅延アップデートを設定します。

カスタム属性 *	有効な値	デフォルト値	注記
DeferredUpdateAllowed	true false	false	true は遅延アップデートを有効にします。遅延アップデートが無効（false）の場合、次の設定は無視されます。
DeferedUpdateMinimumVersion	*x.x.x*	0.0.0	アップデートを遅延できるようにインストールする必要がある AnyConnect の最小バージョン。 最小バージョンチェックは、ヘッドエンドで有効になっているすべてのモジュールに適用されます。有効になっているモジュール（VPN を含む）がインストールされていないか、最小バージョンを満たしていない場合、接続は遅延アップデートの対象になりません。 この属性が指定されていない場合、エンドポイントにインストールされているバージョンに関係なく、遅延プロンプトが表示されます（または自動消去されます）。

カスタム属性 *	有効な値	デフォルト値	注記
DeferredUpdateDismissTimeout	0 ～ 300（秒）	150 秒	遅延アップデートプロンプトが表示され、自動的に消去されるまでの秒数。この属性は、遅延アップデートプロンプトが表示される場合に限り適用されます（最小バージョン属性が最初に評価されます）。 この属性がない場合、自動消去機能が無効になり、ユーザが応答するまでダイアログが表示されます（必要な場合）。 この属性を 0 に設定すると、次に基づいて強制的に自動遅延またはアップグレードが実施されます。 • インストールされているバージョンおよび DeferredUpdateMinimumVersion の値。 • DeferredUpdateDismissResponse の値。
DeferredUpdateDismissResponse	defer update	update	DeferredUpdateDismissTimeout が発生した場合に実行するアクション。

* カスタム属性値は大文字と小文字を区別します。

ISE での遅延アップデートの設定

手順

ステップ 1 次のナビゲーションに従ってください。

a) **[ポリシー（Policy）]** > **[結果（Results）]** を選択します。

b) [クライアント プロビジョニング（Client Provisioning）] を展開します。
c) [リソース（Resources）] を選択し、**[追加（Add）] > [ローカル ディスクからのエージェント リソース（Agent Resources from Local Disk）]** をクリックします。
d) AnyConnect pkg ファイルをアップロードして、[送信（Submit）] を選択します。

ステップ 2 作成したその他の AnyConnect リソースもアップロードします。

ステップ 3 [リソース（Resources）] で、アップロードした AnyConnect パッケージを使用して [AnyConnect 設定（AnyConnect Configuration）] を追加します。[AnyConnect 設定（AnyConnect Configuration）] には遅延アップデートを設定するフィールドがあります。

遅延アップデートの GUI

次の図は、更新が可能で、遅延アップデートが設定されている場合に表示される UI を示します。図の右側は [DeferredUpdateDismissTimeout] が設定されている場合の UI を示しています。

更新ポリシーの設定

更新ポリシーの概要

AnyConnect ソフトウェアおよびプロファイルの更新は、ヘッドエンドへの接続時に使用可能で、かつクライアントによって許可されている場合に発生します。ヘッドエンドに対して AnyConnect 更新の設定を行うと、更新を使用できるようになります。VPN ローカル ポリシー ファイルの更新ポリシー設定によって、更新が許可されるかどうかが決まります。

更新ポリシーは、ソフトウェア ロックと呼ばれることもあります。複数のヘッドエンドが設定されている場合、更新ポリシーはマルチ ドメイン ポリシーとも呼ばれます。

デフォルトでは、更新ポリシー設定ではすべてのヘッドエンドからのソフトウェアおよびプロファイルの更新を許可します。これを制限するには、次のように更新ポリシー パラメータを設定します。

- **Server Name** リストにヘッドエンドを指定することで、特定のヘッドエンドにすべての AnyConnect ソフトウェアおよびプロファイルの更新を許可（認証）します。

  ヘッドエンドのサーバ名は FQDN または IP アドレスで指定できます。また、*.example.com のようにワイルドカードにすることもできます。

  更新がどのように発生するかの詳細については、下記の「許可されたサーバ更新ポリシーの動作」を参照してください。

- 他のすべての無指定または認証されていないヘッドエンドの場合：
  - **Allow Software Updates From Any Server** オプションを使用して、VPN コア モジュールおよびその他のオプション モジュールのソフトウェア更新を許可または拒否します。
  - **Allow VPN Profile Updates From Any Server** オプションを使用して、VPN プロファイルの更新を許可または拒否します。

- **Allow Service Profile Updates From Any Server** オプションを使用して、その他のサービス モジュールのプロファイルの更新を許可または拒否します。
- [任意のサーバからの ISE ポスチャ プロファイル更新を許可（Allow ISE Posture Profile Updates From Any Server）] オプションを使用して ISE ポスチャ プロファイルの更新を許可または拒否します。
- [任意のサーバからのコンプライアンス モジュール更新を許可（Allow Compliance Module Updates From Any Server）] オプションを使用して、コンプライアンス モジュールの更新を許可または拒否します。

  更新がどのように発生するかの詳細については、下記の「不正なサーバ更新ポリシーの動作」を参照してください。

許可されたサーバ更新ポリシーの動作

Server Name リストで識別されている、許可されたヘッドエンドに接続する場合は、他の更新ポリシー パラメータは適用されず、次のようになります。

- ヘッドエンド上の AnyConnect パッケージのバージョンがクライアント上のバージョンと比較され、ソフトウェアの更新が必要かどうかが判断されます。
  - AnyConnect パッケージのバージョンがクライアント上のバージョンより古い場合、ソフトウェアは更新されません。
  - AnyConnect パッケージのバージョンがクライアント上のバージョンと同じである場合、ヘッドエンドでダウンロード対象として設定され、クライアントに存在しないソフトウェア モジュールのみがダウンロードされてインストールされます。
  - AnyConnectパッケージのバージョンがクライアント上のバージョンより新しい場合、ヘッドエンドでダウンロード対象として設定されたソフトウェアモジュール、およびすでにクライアントにインストールされているソフトウェアモジュールがダウンロードされてインストールされます。
- ヘッドエンド上の VPN プロファイル、ISE ポスチャ プロファイル、および各サービス プロファイルが、クライアント上の該当プロファイルと比較され、更新が必要かどうかが判断されます。
  - ヘッドエンド上のプロファイルがクライアント上のプロファイルと同じ場合は、プロファイルは更新されません。
  - ヘッドエンド上のプロファイルがクライアント上のプロファイルと異なる場合、プロファイルがダウンロードされます。

不正なサーバ更新ポリシーの動作

非正規のヘッドエンドに接続すると、次のような、**Allow ... Updates From Any Server** オプションを使用して AnyConnect の更新方法が決定されます。

- **Allow Software Updates From Any Server:**

- このオプションがオンの場合、この認証されていない ASA に対してソフトウェア更新が許可されます。更新は、認証されたヘッドエンドに対する、上記のようなバージョン比較に基づきます。
- このオプションがオフの場合、ソフトウェア更新は行われません。また、バージョン比較に基づく更新を行う必要があった場合、VPN 接続の試行は終了します。

- **Allow VPN Profile Updates From Any Server:**
  - このオプションがオンの場合、VPN プロファイルは、ヘッドエンドの VPN プロファイルがクライアントのものと異なる場合に更新されます。
  - このオプションがオフの場合、VPNプロファイルは更新されません。また、差異に基づくVPNプロファイル更新を行う必要があった場合、VPN接続の試行は終了します。
- **Allow Service Profile Updates From Any Server:**
  - このオプションがオンの場合、各サービスプロファイルは、ヘッドエンドのプロファイルがクライアントのものと異なる場合に更新されます。
  - このオプションがオフの場合、サービス プロファイルは更新されません。
- **Allow ISE Posture Profile Updates From Any Server:**
  - このオプションがオンの場合、ISE ポスチャ プロファイルは、ヘッドエンドの ISE ポスチャ プロファイルがクライアントのものと異なる場合に更新されます。
  - このオプションがオフの場合、ISE ポスチャ プロファイルは更新されません。ISE ポスチャ プロファイルは、ISE ポスチャ エージェントを機能させるために必要です。
- **Allow Compliance Module Updates From Any Server:**
  - このオプションがオンの場合、コンプライアンス モジュールは、ヘッドエンドのコンプライアンス モジュールがクライアントのものと異なる場合に更新されます。
  - このオプションがオフの場合、コンプライアンス モジュールは更新されません。コンプライアンス モジュールは、ISE ポスチャ エージェントを機能させるために必要です。

更新ポリシーのガイドライン

- 認証された **Server Name** リストにサーバの IP アドレスを表示することで、リモート ユーザはヘッドエンドにその対応する IP アドレスを使用して接続できます。ユーザが IP アドレスを使用して接続しようとしたときに、ヘッドエンドが FQDN でリストされている場合、この試行は、認証されていないドメインへの接続として扱われます。
- ソフトウェア更新には、カスタマイズ、ローカリゼーション、スクリプト、およびトランスフォームのダウンロードが含まれます。ソフトウェア更新が許可されていない場合、これらの項目はダウンロードされません。一部のクライアントがスクリプトの更新を許可しない場合、ポリシーの適用にスクリプトを使用しないでください。

- Always-Onを有効にした状態でVPNプロファイルをダウンロードすると、クライアントの他のすべての VPN プロファイルが削除されます。認証されていない、または社外のヘッドエンドからの VPN プロファイルの更新を許可するかどうかを決定する場合は、このことを考慮してください。
- インストールおよび更新ポリシーによってVPNプロファイルがクライアントにダウンロードされない場合、次の機能は使用できません。

サービス無効化	信頼されていないネットワーク ポリシー
証明書ストアの上書き	信頼できる DNS ドメイン
事前接続メッセージの表示	信頼できる DNS サーバ
ローカル LAN へのアクセス	Always-On
Start Before Logon	キャプティブ ポータル修復
ローカル プロキシ接続	スクリプティング
PPP 除外	ログオフ時の VPN の保持
自動 VPN ポリシー	必要なデバイス ロック
信頼されたネットワーク ポリシー	自動サーバ選択

- ダウンローダは、ダウンロード履歴を記録する個別のテキスト ログ（UpdateHistory.log）を作成します。このログは、更新時刻、クライアントを更新したASA、更新されたモジュール、インストールされているバージョン（アップグレードの前および後）を含みます。このログ ファイルは、次の場所に保存されます。

  `%AllUsers%\Application Data\Cisco\Cisco AnyConnect Secure Mobility Client\Logs` ディレクトリ。

更新ポリシーの例

この例では、クライアントの AnyConnect バージョンがさまざまな ASA ヘッドエンドと異なる場合のクライアントの更新動作を示します。

VPN ローカル ポリシー XML ファイルでの更新ポリシーが次のようになっているとします。

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectLocalPolicy acversion="2.4.140"
xmlns=http://schemas.xmlsoap.org/encoding/
xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectLocalPolicy.xsd">
<FipsMode>false</FipsMode>
<BypassDownloader>false</BypassDownloader><RestrictWebLaunch>false</RestrictWebLaunch>
<StrictCertificateTrust>false</StrictCertificateTrust>
<RestrictPreferenceCaching>false</RestrictPreferenceCaching>
<RestrictTunnelProtocols>false</RestrictTunnelProtocols>
<UpdatePolicy>
<AllowSoftwareUpdatesFromAnyServer>true</AllowSoftwareUpdatesFromAnyServer>
<AllowVPNProfileUpdatesFromAnyServer>true</AllowVPNProfileUpdatesFromAnyServer>
<AllowServiceProfileUpdatesFromAnyServer>true</AllowServiceProfileUpdatesFromAnyServer>
<AllowISEProfileUpdatesFromAnyServer>false</AllowISEProfileUpdatesFromAnyServer>
```

```
<AllowComplianceModuleUpdatesFromAnyServer>true</AllowComplianceModuleUpdatesFromAnyServer>
<AuthorizedServerList>
    <ServerName>seattle.example.com</ServerName>
    <ServerName>newyork.example.com</ServerName>
     </AuthorizedServerList>
</UpdatePolicy>
</AnyConnectLocalPolicy>
```

ASA ヘッドエンド設定は次のようになっています。

ASA ヘッドエンド	ロードされている AnyConnect パッケージ	ダウンロードするモジュール
seattle.example.com	バージョン 3.1.05182	VPN、ネットワーク アクセス マネージャ、Web セキュリティ
newyork.example.com	バージョン 3.1.06079	VPN、ネットワーク アクセス マネージャ
raleigh.example.com	バージョン 3.1.07021	VPN、ポスチャ

次の更新シーケンスは、クライアントが現在 AnyConnect VPN およびネットワーク アクセス マネージャ モジュールを実行している場合に実行可能です。

- クライアントは、同じバージョンの AnyConnect が設定された、認証されたサーバである seattle.example.com に接続します。Web セキュリティ プロファイル、および、可能な場合は、Web セキュリティ ソフトウェア モジュールがダウンロードおよびインストールされます。VPN およびネットワーク アクセス マネージャ プロファイルがダウンロード可能で、かつクライアントのものとは異なる場合、それらのプロファイルもダウンロードされます。
- 次に、クライアントは、AnyConnect の新しいバージョンが設定された、認証された ASA である newyork.example.com に接続します。VPN、ネットワーク アクセス マネージャ、および Web セキュリティ モジュールがダウンロードおよびインストールされます。ダウンロード可能で、かつクライアントのものとは異なるプロファイルもダウンロードされます。
- 次に、クライアントは、認証されていない ASA である raleigh.example.com に接続します。ソフトウェア更新が許可されるため、VPN、ネットワーク アクセス マネージャ、Web セキュリティ、およびポスチャ モジュールはすべてアップグレードされます。VPN プロファイルとサービス プロファイルの更新は許可されないため、ダウンロードされません。VPN プロファイルが（差異に基づいて）更新可能であった場合、接続は終了します。

AnyConnect 参照情報

ローカル コンピュータ上のユーザ プリファレンス ファイルの場所

AnyConnect は、一部のプロファイル設定をユーザ コンピュータ上のユーザ プリファレンス ファイルおよびグローバル プリファレンス ファイルに保存します。AnyConnect は、ローカル ファイルを使用して、クライアント GUI の [プリファレンス（Preferences）] タブでユーザ制御可能設定を行い、ユーザ、グループ、ホストなど直近の接続に関する情報を表示します。

AnyConnect は、Start Before Logon や起動時自動接続など、ログイン前に実行するアクションにグローバル ファイルを使用します。

次の表に、クライアント コンピュータ上のユーザ プリファレンス ファイルのファイル名およびインストールされたパスを示します。

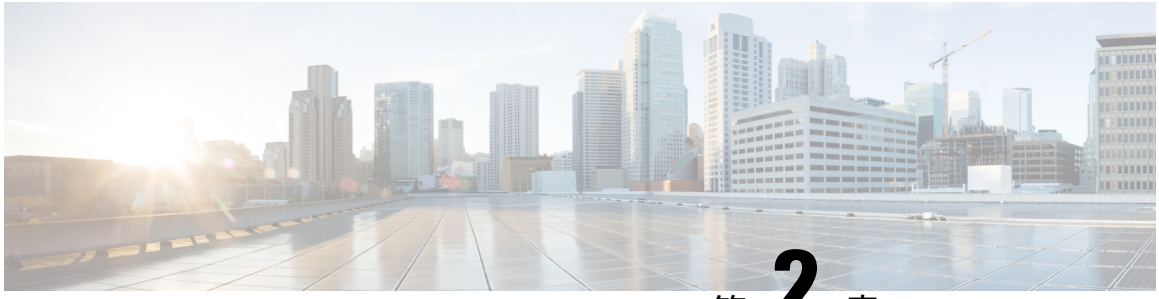
オペレーティング システム	タイプ	ファイルおよびパス
Windows	ユーザ（User）	C:\Users\username\AppData\Local\Cisco\Cisco AnyConnect VPN Client\preferences.xml
	グローバル	C:\ProgramData\Cisco\Cisco AnyConnect VPN Client\preferences_global.xml
macOS	ユーザ（User）	/Users/username/.anyconnect
	グローバル	/opt/cisco/anyconnect/.anyconnect_global
Linux	ユーザ（User）	/home/username/.anyconnect
	グローバル	/opt/cisco/anyconnect/.anyconnect_global

AnyConnect およびレガシー VPN クライアントで使用されるポート

次の表に、レガシー Cisco VPN Client および Cisco AnyConnect Secure Mobility Client で使用されるポートをプロトコルごとに示します。

プロトコル	Cisco AnyConnect Client ポート
TLS（SSL）	TCP 443
SSL リダイレクション	TCP 80（任意）
DTLS	UDP 443（任意、ただし強く推奨）
IPsec/IKEv2	UDP 500、UDP 4500

プロトコル	Cisco VPN Client（IPsec）ポート
IPsec/NATT	UDP 500、UDP 4500
IPsec/NATT	UDP 500、UDP 4500
IPsec/TCP	TCP（設定可能）
IPsec/UDP	UDP 500、UDP X（設定可能）



第 2 章

AnyConnect クライアントとインストーラのカスタマイズとローカライズ

- AnyConnect インストール動作の変更 （51 ページ）
- DSCP の保存の有効化 （60 ページ）
- パブリック DHCP サーバ ルートの設定 （61 ページ）
- AnyConnect GUI テキストとメッセージのカスタマイズ （61 ページ）
- AnyConnect GUI のカスタム アイコンおよびロゴの作成 （69 ページ）
- AnyConnect クライアントのヘルプ ファイルの作成とアップロード （78 ページ）
- スクリプトの作成および展開 （79 ページ）
- AnyConnect API によるカスタム アプリケーションの作成と展開 （84 ページ）
- AnyConnect CLI コマンドの使用 （85 ページ）
- ISE 展開のための AnyConnect カスタマイズおよびローカリゼーションの準備 （88 ページ）

AnyConnect インストール動作の変更

ガイドライン

- Web 展開では、クライアントレス SSL ポータルの一部である AnyConnect Web 起動を使用します。クライアントレス SSL ポータルはカスタマイズできますが、このポータルの AnyConnect 部分はカスタマイズできません。たとえば、[AnyConnect の起動（Start AnyConnect）] ボタンはカスタマイズできません。

カスタマー エクスペリエンス フィードバックの無効化

カスタマー エクスペリエンス フィードバック モジュールは、デフォルトで有効になっています。このモジュールは、カスタマーがどの機能およびモジュールを有効にし、使用しているかという匿名の情報をシスコに提供します。この情報によりユーザエクスペリエンスを把握できるため、シスコは品質、信頼性、パフォーマンス、ユーザエクスペリエンスを継続して改善できます。

カスタマー エクスペリエンス フィードバック モジュールを手動で無効にするには、スタンドアロン プロファイル エディタを使用して CustomerExperience_Feedback.xml ファイルを作成します。AnyConnect サービスを停止し、ファイルの名前を CustomerExperience_Feedback.xml にし、C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\CustomerExperienceFeedback\ ディレクトリにそのファイルを配置する必要があります。ファイルが無効フラグを設定して作成されると、AnyConnect に手動で展開できます。結果を確認するには、[AnyConnect について（AnyConnect About）] メニューを開き、カスタマーエクスペリエンス フィードバック モジュールが [インストール済みモジュール（Installed Module）] セクションにリストされていないことを確認します。

カスタマー エクスペリエンス フィードバックは、次を使用して無効にできます。

- カスタマー エクスペリエンス フィードバック モジュールのクライアント プロファイル：[カスタマーエクスペリエンス フィードバック サービスの有効化（Enable Customer Experience Feedback Service）] をオフにして、プロファイルを配布します。
- MST ファイル：anyconnect-vpn-transforms-X.X.xxxxx.zip から、anyconnect-win-disable-customer-experience-feedback.mst を抽出します。

インストール動作の変更、Windows

- AnyConnect のインストール動作を変更するには、Windows インストーラのプロパティを使用します。これらのプロパティは次で使用できます。
  - コマンド ライン パラメータ：1 つ以上のプロパティが、コマンド ライン インストーラ msiexec のパラメータとして渡されます。この方法は、事前展開に使用します。Web 展開ではサポートされません。
  - インストーラ トランスフォーム：トランスフォームを使用して、インストーラのプロパティ テーブルを変更できます。トランスフォームの作成には、いくつかのツールを使用できます。一般的なツールの 1 つが Microsoft Orca です。Orca ツールは、Microsoft Windows Installer Software Development Kit（SDK）の一部で、Microsoft Windows SDK に同梱されています。Windows SDK を入手するには、http://msdn.microsoft.com を参照し、使用している Windows のバージョンに対応する SDK を探します。

    トランスフォームは、事前展開のみに使用できます。（ダウンローダがインストーラを呼び出したときに、シスコによって署名されたトランスフォームのみが Web 展開を実行します。）アウトオブバンドの方法で、自分のトランスフォームを適用できますが、詳細は、このガイドの範囲外です。

- ISO イメージでは、インストーラ プログラム `setup.hta` は HTML であり、編集可能です。

制限事項

AnyConnect アンインストール プロンプトはカスタマイズできません。

クライアント インストールをカスタマイズする Windows インストーラ プロパティ

次の Windows インストーラ プロパティで、AnyConnect インストールをカスタマイズします。他にも Microsoft によってサポートされる数多くの Windows インストーラ プロパティがあることに留意してください。

- システム MTU のリセット：VPN インストーラ プロパティ（RESET_ADAPTER_MTU）が 1 に設定されている場合、すべての Windows ネットワーク アダプタの MTU 設定がデフォルト値にリセットされます。変更を有効にするには、システムをリブートする必要があります。

- Windows ロックダウンの設定：デバイスの Cisco AnyConnect Secure Mobility Client に対するエンド ユーザのアクセス権は制限することを推奨します。エンド ユーザに追加の権限を与える場合、インストーラでは、AnyConnect サービスをユーザとローカル管理者がオフにしたり停止したりできないようにするロックダウン機能を提供できます。また、サービス パスワードを使用して、コマンド プロンプトからサービスを停止できます。

  VPN、ネットワーク アクセス マネージャ、Web セキュリティ、ネットワーク可視化モジュール、および Umbrella ローミング セキュリティ モジュールの MSI インストーラは、共通のプロパティ（LOCKDOWN）をサポートします。LOCKDOWN が 0 以外の値に設定されている場合、インストーラに関連付けられた Windows サービスをエンドポイント デバイスでユーザまたはローカル管理者が制御することはできません。サンプルのトランスフォームを使用して、このプロパティを設定し、ロックダウンした各 MSI インストーラにトランスフォームを適用することを推奨します。サンプルのトランスフォームは、Cisco AnyConnect Secure Mobility Client ソフトウェア ダウンロード ページからダウンロードできます。

  1 つ以上のオプション モジュールに加えてコア クライアントを展開する場合、LOCKDOWN プロパティを各インストーラに適用する必要があります。この操作は片方向のみであり、製品を再インストールしない限り削除できません。

  （注） AMP イネーブラ インストーラには、VPN インストーラが組み合わされています。

- ActiveX コントロールの有効化：AnyConnect 事前展開 VPN パッケージの以前のバージョンでは、VPN WebLaunch ActiveX コントロールがデフォルトでインストールされていました。AnyConnect 3.1 以降では、VPN ActiveX コントロールのインストールはデフォルトでオフになっています。この変更は、最もセキュアな設定をデフォルトにするために行われました。

  AnyConnect クライアントとオプション モジュールを事前展開する際、VPN ActiveX コントロールを AnyConnect でインストールする必要がある場合には、msiexec またはトランスフォームとともに NOINSTALLACTIVEX=0 オプションを使用する必要があります。

- [プログラムの追加と削除（Add/Remove Program List）] リストでの AnyConnect の非表示：インストールした AnyConnect モジュールをユーザの Windows コントロール パネルの [プログラムの追加と削除（Add/Remove Program List）] リストに表示されないようにするこ

とができます。インストーラに ARPSYSTEMCOMPONENT=1 を渡すと、そのモジュールはインストール済みプログラムのリストに表示されなくなります。

サンプルのトランスフォームを使用して、このプロパティを設定し、非表示にする各モジュールの MSI インストーラごとにトランスフォームを適用することを推奨します。サンプルのトランスフォームは、Cisco AnyConnect Secure Mobility Client ソフトウェア ダウンロード ページからダウンロードできます。

AnyConnect モジュール用の Windows インストーラ プロパティ

次の表に、MSI インストール コマンド ライン コールの例およびプロファイルの展開先を示します。

インストールされるモジュール	コマンドおよびログ ファイル
VPN なしの AnyConnect コア クライアント機能 （スタンドアロン モジュールのインストール時に使用）	msiexec /package anyconnect-win-*version*-predeploy-k9.msi /norestart /passive PRE_DEPLOY_DISABLE_VPN=1 /lvx* anyconnect-win-*version*-predeploy-k9-install-datetimestamp.log
VPN ありの AnyConnect コア クライアント機能	msiexec /package anyconnect-win-*version*-predeploy-k9.msi /norestart /passive /lvx* anyconnect-win-*version*-predeploy-k9-install-datetimestamp.log
カスタマー エクスペリエンスのフィードバック	msiexec /package anyconnect-win-*version*-predeploy-k9.msi /norestart /passive DISABLE_CUSTOMER_EXPERIENCE_FEEDBACK=1 /lvx* anyconnect-win-*version*-predeploy-k9-install-datetimestamp.log
Diagnostic and Reporting Tool（DART）	msiexec /package anyconnect-win-*version*-dart-predeploy-k9.msi /norestart /passive /lvx* anyconnect-win-*version*-dart-predeploy-k9-install-datetimestamp.log
SBL	msiexec /package anyconnect-win-*version*-gina-predeploy-k9.msi /norestart /passive /lvx* anyconnect-win-*version*-gina-predeploy-k9-install-datetimestamp.log
ネットワーク アクセス マネージャ	msiexec /package anyconnect-win-*version*-nam-predeploy-k9.msi /norestart /passive /lvx* anyconnect-win-*version*-nam-predeploy-k9-install-datetimestamp.log

インストールされるモジュール	コマンドおよびログ ファイル
Web セキュリティ	msiexec /package anyconnect-win-*version*-websecurity-predeploy-k9.msi /norestart/passive /lvx* anyconnect-win-*version*-websecurity-predeploy-k9-install-datetimestamp.log
ポスチャ（Posture）	msiexec /package anyconnect-win-*version*-posture-predeploy-k9.msi /norestart/passive /lvx* anyconnect-win-*version*-posture-predeploy-k9-install-datetimestamp.log
ISE ポスチャ	msiexec /package anyconnect-win-*version*-iseposture-predeploy-k9.msi /norestart/passive /lvx* anyconnect-win-*version*-iseposture-predeploy-k9-install-datetimestamp.log
AMP イネーブラ	msiexec /package anyconnect-win-*version*-amp-predeploy-k9.msi /norestart/ passive /lvx* anyconnect-win-*version*-amp-predeploy-k9-install-datetimestamp.log
ネットワーク可視性モジュール	msiexec /package anyconnect-win-*version*-nvm-predeploy-k9.msi /norestart/ passive /lvx* anyconnect-win-*version*-nvm-predeploy-k9-install-datetimestamp.log
Umbrella ローミング セキュリティ モジュール	msiexec /package anyconnect-win-*version*-umbrella-predeploy-k9.msi/norestart/ passive /lvx* anyconnect-win-*version*-predeploy-k9-install-datetimestamp.log

適応型セキュリティ アプライアンスへのカスタマイズされたインストーラ トランスフォームのインポート

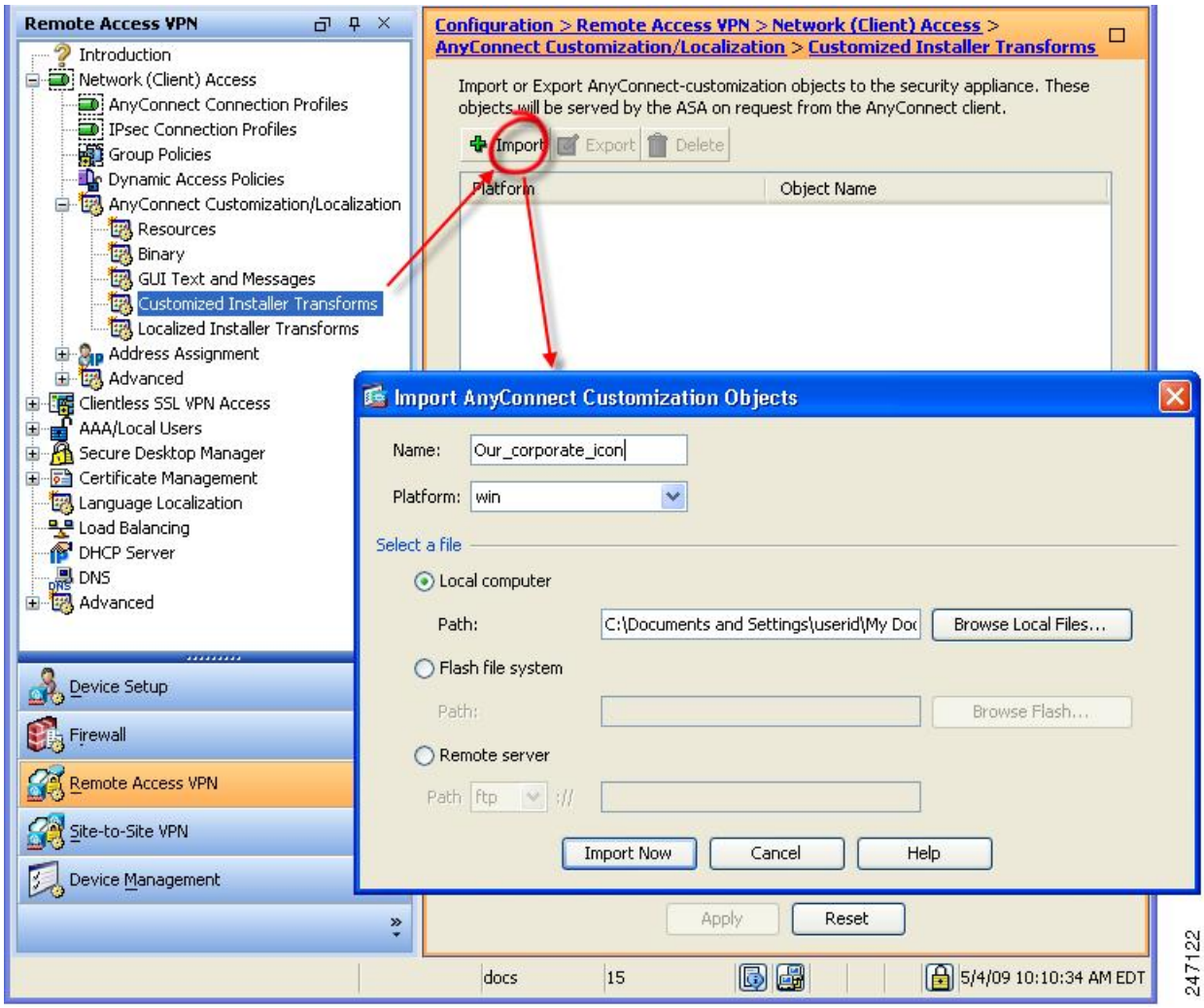
シスコが提供する Windows トランスフォームを適応型セキュリティ アプライアンスにインポートすると、Web 展開に使用できます。

手順

ステップ 1 ASDM で、**[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [AnyConnect カスタマイゼーション/ローカリゼーション（AnyConnect Customization/LocalizationScript）] > [カスタマイズされたインストーラ トランスフォーム（Customized Installer Transforms）]** に移動します。

ステップ 2 [インポート（Import）] をクリックします。

[AnyConnect カスタマイゼーション オブジェクトのインポート（Import AnyConnect Customization Objects）] ウィンドウが表示されます。



ステップ 3 インポートするファイルの名前を入力します。他のカスタマイズ用オブジェクトの名前とは異なり、この名前は ASA にとって重要ではないため、自由に指定できます。

ステップ 4 プラットフォームを選択し、インポートするファイルを指定します。[今すぐインポート（Import Now）] をクリックします。インストーラ トランスフォームのテーブルにファイルが表示されます。

AnyConnect インストーラ画面のローカライズ

AnyConnect インストーラに表示されるメッセージを翻訳できます。ASA はトランスフォームを使用して、インストーラに表示されるメッセージを翻訳します。トランスフォームによってインストレーションが変更されますが、元のセキュリティ署名 MSI は変化しません。これら

のトランスフォームではインストーラ画面だけが翻訳され、クライアント GUI 画面は翻訳されません。

（注） AnyConnect のすべてのリリースには、ローカライズされたトランスフォームが含まれています。このトランスフォームは、管理者が、新しいソフトウェアを含む AnyConnect パッケージをアップロードするときに必ず、適応型セキュリティ アプライアンス（ASA）にアップロードできます。ローカリゼーション トランスフォームを使用している場合は、新しい AnyConnect パッケージをアップロードする際に、必ず cisco.com の最新リリースでローカリゼーション トランスフォームをアップデートしてください。

現時点では、30 の言語に対応するトランスフォームが用意されています。これらのトランスフォームは、cisco.com の AnyConnect ソフトウェア ダウンロード ページから、次の .zip ファイルで入手できます。

```
anyconnect-win-<VERSION>-webdeploy-k9-lang.zip
```

このファイルの <VERSION> は、AnyConnect のリリース バージョン（4.3.xxxxx など）を表します。

アーカイブには使用可能な翻訳用のトランスフォーム（.mst ファイル）が含まれています。用意されている 30 以外の言語をリモート ユーザに表示する必要がある場合は、独自のトランスフォームを作成し、それを新しい言語として ASA にインポートすることができます。Microsoft のデータベース エディタ Orca を使用して、既存のインストレーションおよび新規ファイルを修正できます。Orca は、Microsoft Windows Installer Software Development Kit（SDK）の一部で、Microsoft Windows SDK に同梱されています。

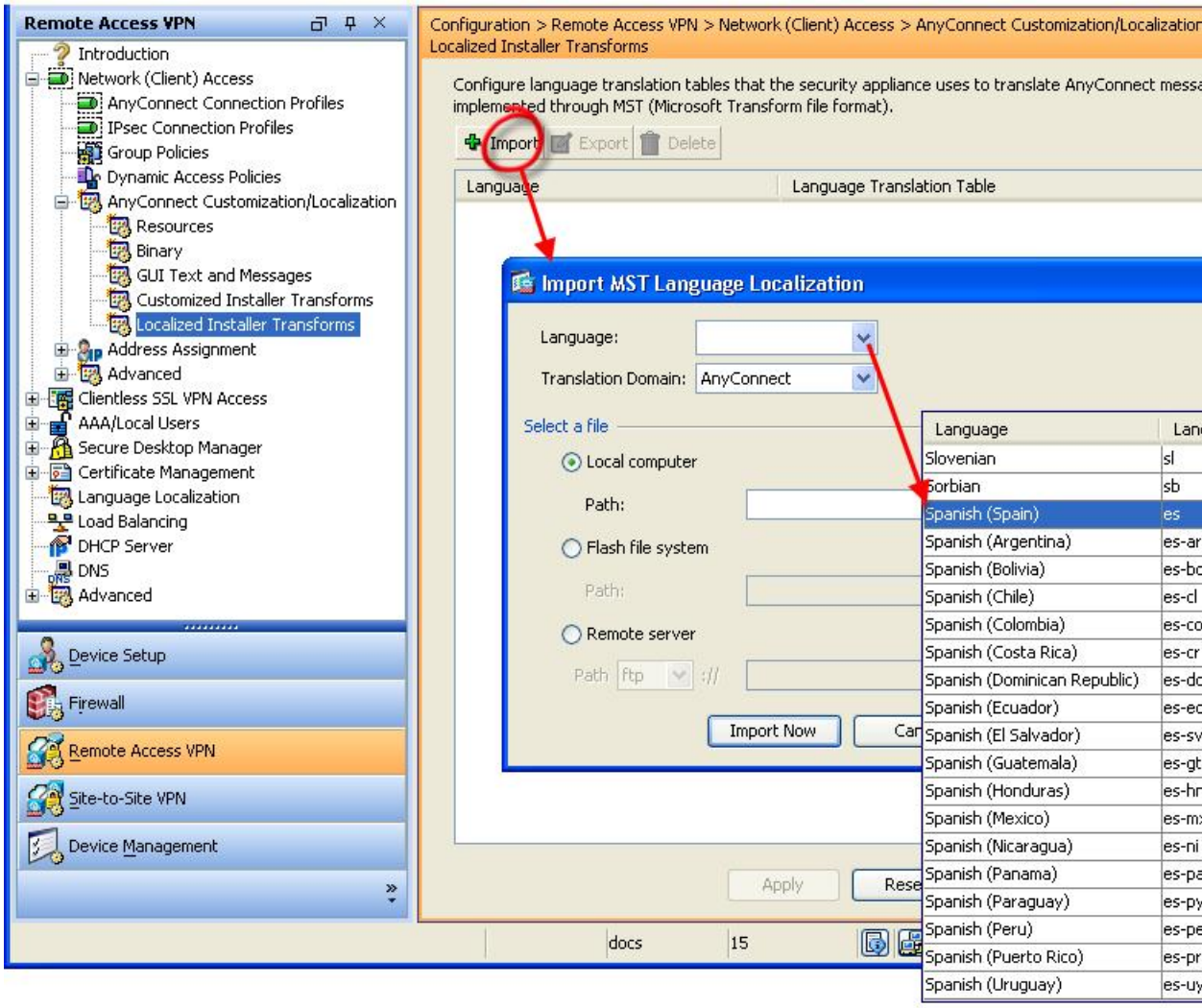
適応型セキュリティ アプライアンスへのローカライズされたインストーラ トランスフォームのインポート

ここでは、ASDM を使用してトランスフォームを ASA にインポートする方法について説明します。

手順

ステップ 1 ASDM で、**[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [AnyConnect カスタマイゼーション/ローカリゼーション（AnyConnect Customization/LocalizationScript）] > [ローカライズされたインストーラ トランスフォーム（Localized Installer Transforms）]** に移動します。

ステップ 2 [インポート（Import）] をクリックします。[MST 言語ローカライズのインポート（Import MST Language Localization）] ウィンドウが表示されます。



ステップ 3 [言語（Language）] ドロップダウン リストをクリックして、このトランスフォーム用の言語（および業界で認められている略称）を選択します。手動で略称を入力する場合は、ブラウザおよびオペレーティング システムが認識できる略称を使用してください。

ステップ 4 [今すぐインポート（Import Now）] をクリックします。
テーブルが正常にインポートされたことを示すメッセージが表示されます。

ステップ 5 [適用（Apply）] をクリックして変更を保存します。

この手順では、言語にスペイン語（es）を指定しました。次の図は、AnyConnectの言語リストのスペイン語の新しいトランスフォームを示しています。

インストール動作の変更、macOS

制限事項

AnyConnect インストーラはローカライズできません。インストーラによって使用される文字列は、Mac インストーラ アプリケーションから取得され、AnyConnect インストーラからは取得されません。

ACTransforms.xml による macOS でのインストーラ動作のカスタマイズ

macOS については .pkg の動作をカスタマイズする標準の方法が提供されていないため、ACTransforms.xml を作成しました。この XML ファイルをインストーラとともに配置すると、インストーラはインストールを実行する前にこのファイルを読み取ります。ファイルをインストーラからの特定の相対パスに配置する必要があります。インストーラは、次の場所で変更が見つかるかどうかこの順序で検索します。

1. .pkg インストーラ ファイルと同じディレクトリにある「Profile」ディレクトリ内。
2. マウント済みディスク イメージ ボリュームのルートにある「Profile」ディレクトリ内。
3. マウント済みディスク イメージ ボリュームのルートにある「Profile」ディレクトリ内。

XML ファイルの形式は次のとおりです。

```
<ACTransforms>
<PropertyName1>Value</PropertyName1>
<PropertyName2>Value</PropertyName2>
</ACTransforms>
```

たとえば、macOS ACTransforms.xml プロパティは、Web セキュリティの「スタンドアロン」展開を作成する場合 DisableVPN です。ACTransforms.xml は、DMG ファイルの Profiles ディレクトリ内にあります。

カスタマー エクスペリエンス フィードバック モジュールの無効化

カスタマー エクスペリエンス フィードバック モジュールは、デフォルトで有効になっています。Mac OS X でこの機能を無効に切り替えるには、次の手順に従います。

手順

ステップ 1 ディスク ユーティリティまたは hdiutil を使用して、dmg パッケージを読み取り専用から読み取り/書き込みに変換します。次に例を示します。

```
hdiutil convert anyconnect-macosx-i386-ver-k9.dmg -format UDRW -o
anyconnect-macosx-i386-ver-k9-rw.dmg
```

ステップ 2 まだ設定されていない場合は、ACTransforms.xml を編集し、次の値を設定または追加します。

```
<DisableCustomerExperienceFeedback>false</DisableCustomerExperienceFeedback>
```

インストール動作の変更、Linux

ACTransform.xml による Linux でのインストーラ動作のカスタマイズ

Linux については .pkg の動作をカスタマイズする標準の方法が提供されていないため、ACTransforms.xml を作成しました。この XML ファイルをインストーラとともに配置すると、インストーラはインストールを実行する前にこのファイルを読み取ります。ファイルをインストーラからの特定の相対パスに配置する必要があります。インストーラは、次の場所で変更が見つかるかどうかこの順序で検索します。

- .pkg インストーラ ファイルと同じディレクトリにある「Profile」ディレクトリ内
- マウント済みディスク イメージ ボリュームのルートにある「Profile」ディレクトリ内
- .dmg ファイルと同じディレクトリにある「Profile」ディレクトリ内

事前展開パッケージ内の Profiles ディレクトリの XML ファイルである ACTransforms.xml の形式は次のとおりです。

```
<ACTransforms>
<PropertyName1>Value</PropertyName1>
<PropertyName2>Value</PropertyName2>
</ACTransforms>
```

DSCP の保存の有効化

Windows または OS X プラットフォームでは、DTLS 接続でのみ DiffServ コード ポイント（DSCP）を制御するカスタム属性を設定できます。DSCP の保存により、デバイスは遅延の影響を受けやすいトラフィックを優先することができます。ルータでは、これが設定されているかどうかが反映され、アウトバウンド接続品質の向上のために優先トラフィックがマークされます。

カスタム属性タイプは DSCPPreservationAllowed であり、有効な値は True または False です。

（注） デフォルトでは、AnyConnectはDSCPの保存を実行します（True）。無効にするには、ヘッドエンドでカスタム属性値を false に設定し、接続を再初期化します。

この機能は、ASDMの[設定（Configuration）]>[リモートアクセスVPN（Remote Access VPN）]>[ネットワーク(クライアント)アクセス（Network (Client) Access）]>[グループポリシー（Group Policies）]>[追加/編集（Add/Edit）]>[詳細（Advanced）]>[AnyConnectクライアント（AnyConnect Client）]>[カスタム属性（Custom Attributes）]で設定します。設定プロセスについては、適切なバージョンの『Cisco ASA Series VPN Configuration Guide』の「*Enable DSCP Preservation*」の項を参照してください。

パブリック DHCP サーバ ルートの設定

AnyConnect は、すべてのネットワークのトンネルが設定されているときにローカル DHCP トラフィックを暗号化せずに流せるようにするために、AnyConnect クライアント接続時にローカル DHCP サーバに特殊なルートを追加します。また、このルートでのデータ漏えいを防ぐため、AnyConnect はホスト デバイスの LAN アダプタに暗黙的なフィルタを適用し、DHCP トラフィックを除く、そのルートのすべてのトラフィックをブロックします。外部インターフェイスに接続し、ローカル DHCP サーバを使用して接続が確立されると、そのサーバへの特殊なルートが作成され、非仮想アダプタではなく NIC をポイントします。同じサーバで他のサービス（WINS、DNS など）が実行されている場合は、VPN セッションが確立されると、このルートがこれらのサービスを中断します。

Windows では、グループ ポリシーのカスタム属性を設定することで、パブリックな DHCP サーバ ルートの作成を制御できます。トンネル確立時のパブリック DHCP サーバ ルート作成を避けるために、no-dhcp-server-route カスタム属性が存在し、これを true に設定する必要があります。

この機能は、ASDMの[設定（Configuration）]>[リモートアクセスVPN（Remote Access VPN）]>[ネットワーク(クライアント)アクセス（Network (Client) Access）]>[グループポリシー（Group Policies）]>[追加/編集（Add/Edit）]>[詳細（Advanced）]>[AnyConnectクライアント（AnyConnect Client）]>[カスタム属性（Custom Attributes）]で設定します。設定プロセスについては、適切なリリースの『Cisco ASA Series VPN Configuration Guide』を参照してください。

AnyConnect GUI テキストとメッセージのカスタマイズ

適応型セキュリティ アプライアンス（ASA）は、変換テーブルを使用して AnyConnect に表示されるユーザ メッセージを翻訳します。変換テーブルとは、翻訳されたメッセージ テキストの文字列を含むテキスト ファイルです。ASDM またはトランスフォーム（Windows の場合）を使用して、既存のメッセージを編集したり、言語を追加したりできます。

ローカリゼーション用の次の Windows サンプル トランスフォームは、www.cisco.com で入手できます。

- Windows プラットフォームの事前展開パッケージ用言語ローカリゼーション トランスフォーム ファイル
- Windows プラットフォームの Web 展開パッケージ用言語ローカリゼーション トランスフォーム ファイル

Windows 用 AnyConnect パッケージ ファイルには、AnyConnect メッセージのデフォルトの英語の言語テンプレートが含まれます。AnyConnect パッケージを ASA にロードすると、ASA はこのファイルを自動的にインポートします。このテンプレートには、AnyConnect ソフトウェア内のメッセージ文字列の最新の変更が含まれています。これを使用すると、別の言語用の変換テーブルを新しく作成できます。または、www.cisco.com から入手可能な次の変換テーブルのいずれかをインポートすることができます（適応型セキュリティ アプライアンスへの変換テーブルのインポート （66 ページ）を参照）。

- 中国語（簡体字）
- 中国語（繁体字）
- チェコ語
- Dutch
- フランス語
- フランス語（カナダ）
- ドイツ語
- ハンガリー語
- イタリア語
- 日本語
- Korean
- ポーランド語
- ポルトガル語（ブラジル）
- ロシア語
- スペイン語（ラテンアメリカ）

次の項では、目的の言語が利用できない場合や、インポートした変換テーブルをさらにカスタマイズしたい場合などに、GUI テキストおよびメッセージを翻訳するための手順を説明します。

- AnyConnect のテキストとメッセージの追加または編集。メッセージ ファイルを追加または編集して、1 つ以上のメッセージ ID のメッセージ テキストを次の方法で変更して、メッセージ ファイルに変更を加えることができます。

- 開いたダイアログのテキストに変更内容を入力します。
- 開いたダイアログのテキストをテキストエディタにコピーし、変更を行い、そのテキストを元のダイアログに貼り付けます。

- 適応型セキュリティ アプライアンスへの変換テーブルのインポート（66 ページ）。[ファイルに保存（Save to File）] をクリックして、そのファイルを編集し、ファイルを ASDM にもう一度インポートすることで、メッセージ ファイルをエクスポートできます。

ASA の変換テーブルを更新した後、クライアントをリスタートして別の接続に成功するまでは、更新したメッセージは適用されません。

（注） クライアントを ASA から展開せずに、Altiris Agent などの社内のソフトウェア展開システムを使用する場合は、Gettext などのカタログ ユーティリティを使用して、手動で AnyConnect 変換テーブル（anyconnect.po）を .mo ファイルに変換し、その .mo ファイルをクライアント コンピュータの適切なフォルダにインストールします。詳細については、「エンタープライズ展開用のメッセージ カタログの作成」（3-22 ページ）を参照してください。

注意事項と制約事項

AnyConnect は、すべての国際化の要件に完全には準拠していません。次の例外があります。

- 日付/時刻の形式は、ロケールの要件に従わない場合があります。
- 右から左への言語はサポートされません。
- 一部の文字列はハードコードされたフィールド長により UI で切り捨てられます。
- 次のようないくつかのハードコードされた英語文字列は、そのまま維持されます。
  - 更新時のステータス メッセージ。
  - 信頼できないサーバ メッセージ。
  - 遅延アップデート メッセージ。

AnyConnect のテキストとメッセージの追加または編集

英語変換テーブルを追加または編集し、1 つ以上のメッセージ ID のメッセージ テキストを変更することによって、AnyConnect GUI に表示される英語のメッセージを変更できます。メッセージ ファイルを開いたら、次の操作でそれを編集できます。

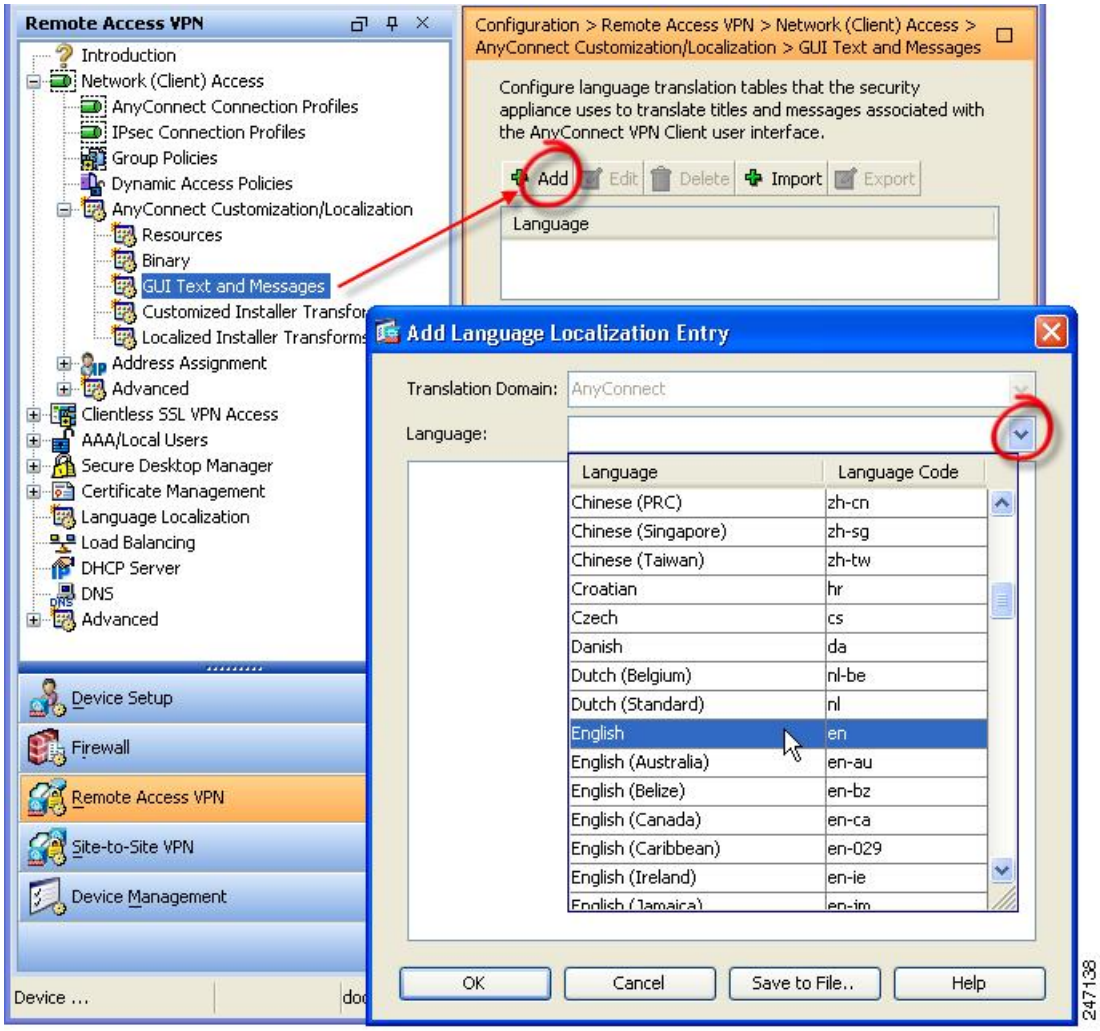
- 開いたダイアログのテキストに変更内容を入力します。
- 開いたダイアログのテキストをテキストエディタにコピーし、変更を行い、そのテキストを元のダイアログに貼り付けます。

- [ファイルに保存（Save to File）] をクリックしてメッセージ ファイルをエクスポートし、そのファイルを編集し、ファイルを ASDM にインポートします。

手順

ステップ 1 ASDM で、**[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [AnyConnect カスタマイゼーション/ローカリゼーション（AnyConnect Customization/Localization）] > [GUI テキストおよびメッセージ（GUI Text and Messages）]** に移動します。

ステップ 2 [追加（Add）] をクリックします。[言語ローカリゼーション エントリの追加（Add Language Localization Entry）] ウィンドウが表示されます。

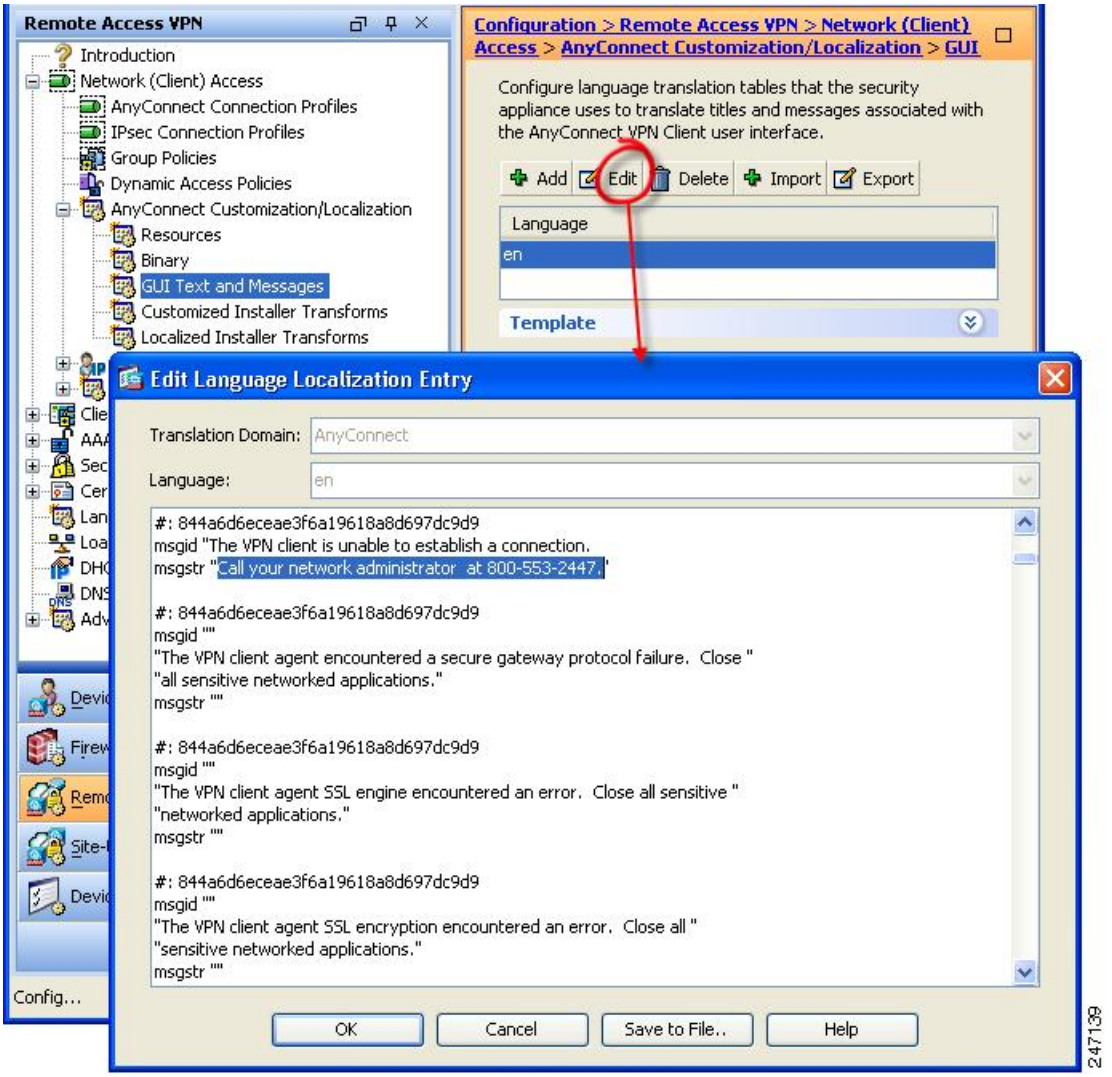


ステップ 3 [言語（Language）] ドロップ リストをクリックし、言語として [英語（en）（English (en)）] を指定します。英語の変換テーブルが、ペインの言語リストに表示されます。

ステップ 4 [編集（Edit）] をクリックして、メッセージの編集を開始します。

[言語のローカライズ エントリの編集（Edit Language Localization Entry）] ウィンドウが表示されます。msgid の引用符で囲まれたテキストは、クライアントに表示されるデフォルトの英語テキストです。変更してはいけません。msgstr の文字列には、msgid のデフォルト テキストを置き換えるために、クライアントで使用されるテキストが含まれます。msgstr の引用符の間に、使用するテキストを挿入します。

次の例では、「Call your network administrator at 800-553-2447」が挿入されています。



ステップ 5 [OK]、[適用（Apply）] の順にクリックし、変更内容を保存します。

適応型セキュリティ アプライアンスへの変換テーブルのインポート

手順

ステップ 1 www.cisco.com から目的の変換テーブルをダウンロードします。

ステップ 2 ASDM で、**[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [AnyConnect カスタマイゼーション/ローカリゼーション（AnyConnect Customization/Localization）] > [GUI テキストおよびメッセージ（GUI Text and Messages）]** に移動します。

ステップ 3 [インポート（Import）] をクリックします。[言語ローカリゼーション エントリのインポート（Import Language Localization Entry）] ウィンドウが表示されます。

ステップ 4 ドロップダウン リストから適切な言語を選択します。

ステップ 5 変換テーブルのインポート元を指定します。

ステップ 6 [今すぐインポート（Import Now）] をクリックします。この変換テーブルが、この優先言語で AnyConnect クライアントに展開されます。ローカリゼーションは、AnyConnect がリスタートし、再接続した後に適用されます。

（注） 非モバイル デバイスで実行される AnyConnect の場合、Cisco Secure Desktop が使用されていない場合でも、ホストスキャンメッセージがローカライズされるためには、適応型セキュリティ アプライアンスに Cisco Secure Desktop 変換テーブルもインポートする必要があります。

エンタープライズ展開用のメッセージ カタログの作成

クライアントを ASA から展開せずに、Altiris Agent などの社内のソフトウェア展開システムを使用する場合は、Gettext などのユーティリティを使用して、手動で AnyConnect 変換テーブルをメッセージ カタログに変換できます。テーブルを .po ファイルから .mo ファイルに変換後、そのファイルをクライアント コンピュータ上の該当するフォルダに配置します。

（注） GetText と PoeEdit は、サードパーティ製ソフトウェア アプリケーションです。AnyConnect GUI をカスタマイズする推奨方法は、ASA からデフォルトの .mo ファイルを取得し、クライアントへの展開での必要に応じてそのファイルを編集する方法です。デフォルトの .mo ファイルを使用することによって、GetText や PoeEdit などのサードパーティ製アプリケーションに起因する潜在的な変換に関する問題を回避することができます。

Gettext は GNU プロジェクトのユーティリティであり、コマンド ウィンドウで実行できます。詳しくは、GNU の Web サイト（gnu.org）を参照してください。また、Poedit などの、Gettext を使用する GUI ベースのユーティリティを使用することもできます。このソフトウェアは

poedit.net から入手できます。Gettext を使用してメッセージ カタログを作成する手順は、次のとおりです。

AnyConnect メッセージ テンプレートのディレクトリ

AnyConnect メッセージ テンプレートは、各オペレーティング システムで、次に示すフォルダにあります。

（注） \l10n ディレクトリは、次に示す各ディレクトリ パスの一部です。このディレクトリ名のスペルは、小文字の l（「エル」）、1、0、小文字の n です。

- Windows の場合：<DriveLetter>:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\l10n\<LANGUAGE-CODE>\LC_MESSAGES
- macOS および Linux の場合：/opt/cisco/anyconnect/l10n/<LANGUAGE-CODE>/LC_MESSAGES

手順

ステップ 1 Gettext ユーティリティを http://www.gnu.org/software/gettext/ からダウンロードし、管理用のコンピュータ（リモートのユーザ コンピュータ以外）にインストールします。

ステップ 2 AnyConnect がインストールされたコンピュータにある、AnyConnect メッセージ テンプレート AnyConnect.po のコピーを取得します。

ステップ 3 この AnyConnect.po ファイルを編集し（notepad.exe または任意のプレーン テキスト エディタを使用）、必要に応じて文字列を変更します。

ステップ 4 Gettext のメッセージ ファイル コンパイラを実行して、次のように .po ファイルから .mo ファイルを作成します。

msgfmt -o AnyConnect.mo AnyConnect.po

ステップ 5 ユーザのコンピュータ上の正しいメッセージ テンプレート ディレクトリに .mo ファイルのコピーを格納します。

ASA のカスタマイズした変換テーブルへの新しいメッセージの統合

新しいユーザ メッセージが、AnyConnect の一部のリリースに追加されています。これらの新しいメッセージの翻訳を有効にするために、新しいメッセージ文字列は、最新のクライアント イメージとともにパッケージ化された翻訳テンプレートに追加されています。以前のクライアントに含まれていたテンプレートに基づいて変換テーブルを作成した場合、リモート ユーザには新しいメッセージが自動的には表示されません。最新のテンプレートを既存の変換テーブルに統合し、変換テーブルに新しいメッセージを含める必要があります。

統合を実行するための無料のサードパーティ製ツールがあります。GNUプロジェクトのGettextユーティリティにはWindows版があり、コマンドウィンドウで実行できます。詳しくは、GNUの Web サイト（gnu.org）を参照してください。また、Poedit などの、Gettext を使用する GUI ベースのユーティリティを使用することもできます。このソフトウェアは poedit.net から入手できます。両方の手順を次に示します。

（注） この手順は、すでに最新の AnyConnect イメージ パッケージを ASA にロードしてあることが前提になっています。まだロードしていない場合は、テンプレートをエクスポートできません。

手順

ステップ 1 **[リモート アクセス VPN（Remote Access VPN）] > [言語のローカライズ（Language Localization）] > [テンプレート（Templates）]** を選択し、最新の AnyConnect 翻訳テンプレートをエクスポートします。`AnyConnect.pot` というファイル名で、テンプレートをエクスポートします。このファイル名にすると、msgmerge.exe プログラムからこのファイルがメッセージ カタログ テンプレートとして認識されます。

ステップ 2 AnyConnect テンプレートおよび変換テーブルを統合します。

Windows 版の Gettext ユーティリティを使用している場合は、コマンド プロンプト ウィンドウを開き、次のコマンドを実行します。このコマンドでは、次のように、AnyConnect 変換テーブル（.po）とテンプレート（.pot）が統合され、`AnyConnect_merged.po` ファイルが新しく作成されます。

```
msgmerge -o AnyConnect_merged.po AnyConnect.po AnyConnect.pot
```

このコマンドの実行結果の例を次に示します。

```
C:\Program Files\GnuWin32\bin> msgmerge -o AnyConnect_merged.po AnyConnect.po
AnyConnect.pot

..................................... done.
```

Poedit を使用している場合は、初めに AnyConnect.po ファイルを開きます。それには、[ファイル（File）] > [オープン（Open）] > <AnyConnect.po> の順に選択します。次に、POT ファイル <AnyConnect.pot> から、[カタログ（Catalog）] > [更新（Update）] の順に選択して、テンプレートと統合します。新しい文字列と使用されなくなった文字列の両方を示す、[更新概要（Update Summary）] ウィンドウが表示されます。ファイルを保存します。このファイルを次の手順でインポートします。

ステップ 3 統合した変換テーブルを、**[リモート アクセス VPN（Remote Access VPN）] > [言語のローカライズ（Language Localization）]** にインポートします。[インポート（Import）] をクリックし、言語を指定して、変換ドメインとして [AnyConnect] を選択します。インポートするファイルとして `AnyConnect_merged.po` を指定します。

クライアントでの Windows のデフォルト言語の選択

リモート ユーザが ASA に接続してクライアントをダウンロードすると、AnyConnect がコンピュータの優先言語を検出し、指定されたシステム ロケールを検出して適切な変換テーブルを適用します。

Windows で指定されているシステム ロケールを表示または変更するには、次の手順に従います。

手順

ステップ 1 **[コントロール パネル]** > **[地域と言語]** ダイアログボックスに移動します。コントロール パネルをカテゴリ別に表示している場合は、**[時計、言語、および地域（Clock, Language, and Region）]** > **[表示言語の変更（Change display language）]** を選択します。

ステップ 2 言語/ロケール設定を指定し、これらの設定がすべてのユーザ アカウントのデフォルト設定として使用されることを指定します。

ステップ 3 Web Security を使用して展開している場合、Web Security エージェントをリスタートし、新しい翻訳内容を取得します。

（注） 場所が指定されていない場合、AnyConnect はデフォルトで言語のみが設定されます。たとえば、「fr-ca」ディレクトリが見つからないと、AnyConnect は「fr」ディレクトリを調べます。翻訳内容を表示するのに、表示言語、場所、またはキーボードを変更する必要はありません。

AnyConnect GUI のカスタム アイコンおよびロゴの作成

この項の表は、置き換えることができる AnyConnect ファイルをオペレーティング システムごとに示しています。表に含まれるイメージは、AnyConnect VPN クライアント、ネットワーク アクセス マネージャ、および Web セキュリティ モジュールにより使用されます。

制約事項

- カスタム コンポーネントのファイル名は、AnyConnect GUI で使用されるファイル名と一致している必要があります。これはオペレーティング システムによって異なり、macOS および Linux では大文字と小文字が区別されます。たとえば、Windows クライアント用の企業ロゴを置き換えるには、独自の企業ロゴを company_logo.png としてインポートする必要があります。別のファイル名でインポートすると、AnyConnect インストーラはそのコンポーネントを変更しません。ただし、独自の実行ファイルを展開して GUI をカスタマイズする場合は、その実行ファイルから任意のファイル名のリソース ファイルを呼び出すことができます。

- イメージをソース ファイルとして（たとえば、company_logo.bmp）インポートする場合、インポートしたイメージは、同じファイル名を使用して別のイメージを再インポートするまで、AnyConnect をカスタマイズします。たとえば、company_logo.bmp をカスタムイメージに置き換えて、このイメージを削除する場合、同じファイル名を使用して新しいイメージ（または元のシスコ ロゴイメージ）をインポートするまで、クライアントはこのイメージの表示を継続します。

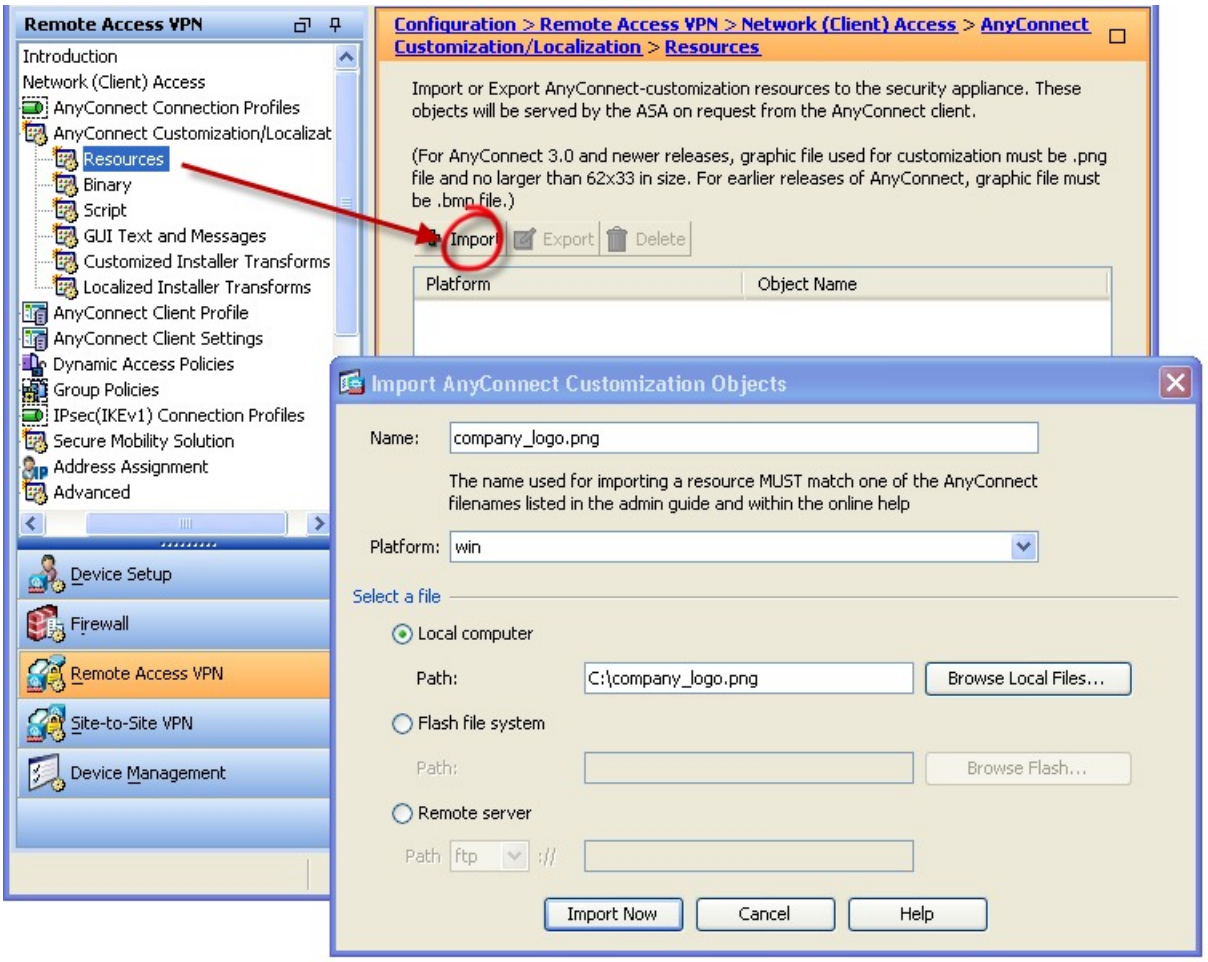
AnyConnect GUI コンポーネントの置き換え

独自のカスタム ファイルをセキュリティ アプライアンスにインポートし、その新しいファイルをクライアントに展開することによって、AnyConnect をカスタマイズできます。

手順

ステップ 1 ASDM で、**[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [AnyConnect カスタマイゼーション/ローカリゼーション（AnyConnect Customization/LocalizationScript）] > [リソース（Resources）]** に移動します。

ステップ 2 [インポート（Import）] をクリックします。[AnyConnect カスタマイゼーション オブジェクトのインポート（Import AnyConnect Customization Objects）] ウィンドウが表示されます。



ステップ 3 インポートするファイルの名前を入力します。

ステップ 4 プラットフォームを選択し、インポートするファイルを指定します。[今すぐインポート（Import Now）] をクリックします。オブジェクトのリストにファイルが表示されます。

Windows 用 AnyConnect アイコンとロゴ

Windows 用のファイルはすべて次の場所に格納されています。

```
%PROGRAMFILES%\Cisco\Cisco AnyConnect Secure Mobility Client\res\
```

（注） %PROGRAMFILES% は、同じ名前の環境変数を指します。ほとんどの Windows インストレーションでは、`C:\Program Files` です。

Windows インストレーションでのファイル名および説明	イメージ サイズ（ピクセル、長さ X 高さ）およびタイプ
about.png [詳細（Advanced）] ダイアログの右上にある [バージョン情報（About）] ボタン。 サイズは調整できません。 	24 x 24 PNG
about_hover.png [詳細（Advanced）] ダイアログの右上にある [バージョン情報（About）] ボタン。 サイズは調整できません。 	24 x 24 PNG
app_logo.png 最大サイズは 128 x 128 です。ご使用のカスタム ファイルがこのサイズ以外の場合は、アプリケーションで 128 x 128 にサイズ変更されます。比率が異なる場合は、引き伸ばされます。 	128 x 128 PNG
attention.ico 注意または操作が必要な状態をユーザに通知するシステム トレイ アイコン。たとえば、ユーザ クレデンシャルについてのダイアログです。 サイズは調整できません。 	16 x 16 ICO

Windows インストレーションでのファイル名および説明	イメージ サイズ（ピクセル、長さ X 高さ）およびタイプ
company_logo.png トレイ フライアウトおよび[詳細（Advanced）]ダイアログの左上に表示される企業ロゴ。 最大サイズは 97 x 58 です。ご使用のカスタム ファイルがこのサイズ以外の場合は、アプリケーションで 97 x 58 にサイズ変更されます。比率が異なる場合は、引き伸ばされます。 	97 x 58（最大） PNG
company_logo_alt.png [バージョン情報（About）]ダイアログ右下に表示される企業ロゴ。 最大サイズは 97 x 58 です。ご使用のカスタム ファイルがこのサイズ以外の場合は、アプリケーションで 97 x 58 にサイズ変更されます。比率が異なる場合は、引き伸ばされます。 	97 x 58 PNG
cues_bg.jpg トレイ フライアウト、[詳細（Advanced）]ウィンドウ、および[バージョン情報（About）]ダイアログの背景イメージ。 イメージが引き伸ばされることはないため、過度に小さい置換イメージを使用すると、領域が黒くなります。 	1260 x 1024 JPEG

Windows インストレーションでのファイル名および説明	イメージ サイズ（ピクセル、長さ X 高さ）およびタイプ
error.ico 1 つ以上のコンポーネントで致命的な問題が発生していることをユーザに通知するシステム トレイ アイコン。 サイズは調整できません。 	16 x 16 ICO
neutral.ico クライアントのコンポーネントが正常に動作していることを示すシステム トレイ アイコン。 サイズは調整できません。 	16 x 16 ICO
transition_1.ico transition_2.ico および transition_3.ico と一緒に使用されるシステム トレイ アイコンで、1 つ以上のクライアント コンポーネントが状態遷移中であることを示します（たとえば、VPN に接続中、ネットワーク アクセス マネージャに接続中など）。3 つのアイコン ファイルが次々に表示されます。これは、左から右に移動する 1 つのアイコンのように見えます。 サイズは調整できません。 	16 x 16 ICO
transition_2.ico transition_1.ico および transition_3.ico と一緒に使用されるシステム トレイ アイコンで、1 つ以上のクライアント コンポーネントが状態遷移中であることを示します（たとえば、VPN に接続中、ネットワーク アクセス マネージャに接続中など）。3 つのアイコン ファイルが次々に表示されます。これは、左から右に移動する 1 つのアイコンのように見えます。 サイズは調整できません。 	16 x 16 ICO

Windows インストレーションでのファイル名および説明	イメージ サイズ（ピクセル、長さ X 高さ）およびタイプ
transition_3.ico transition_1.ico および transition_2.ico と一緒に使用されるシステム トレイ アイコンで、1 つ以上のクライアント コンポーネントが状態遷移中であることを示します（たとえば、VPN に接続中、ネットワーク アクセス マネージャに接続中など）。3 つのアイコン ファイルが次々に表示されます。これは、左から右に移動する 1 つのアイコンのように見えます。 サイズは調整できません。 	16 x 16 ICO
vpn_connected.ico VPN が接続中であることを示すシステム トレイアイコン。 サイズは調整できません。 	16 x 16 ICO

Linux 用 AnyConnect アイコンとロゴ

Linux 用のファイルはすべて次の場所に格納されています。

```
/opt/cisco/anyconnect/pixmaps/
```

次の表に、置換できるファイルと影響を受けるクライアント GUI エリアを示します。

Linux インストレーションでのファイル名および説明	イメージ サイズ（ピクセル、長さ X 高さ）およびタイプ
company-logo.png ユーザ インターフェイスの各タブに表示される企業ロゴ。 AnyConnect 3.0 以降の場合は、62 x 33 ピクセル以下の PNG イメージを使用してください。 	142 x 92 PNG

Linux インストレーションでのファイル名および説明	イメージ サイズ（ピクセル、長さ X 高さ）およびタイプ
cvc-about.png [バージョン情報（About）] タブに表示されるアイコン。 	16 X 16 PNG
cvc-connect.png [接続（Connect）] ボタンの隣、および [接続（Connection）] タブに表示されるアイコン。 	16 X 16 PNG
cvc-disconnect.png [接続解除（Disconnect）] ボタンの隣に表示されるアイコン。 	16 X 16 PNG
cvc-info.png [統計情報（Statistics）] タブに表示されるアイコン。 	16 X 16 PNG
systray_connected.png クライアントが接続中のときに表示されるトレイ アイコン。 	16 X 16 PNG
systray_notconnected.png クライアントが接続中でないときに表示されるトレイ アイコン。 	16 X 16 PNG
systray_disconnecting.png クライアントが接続解除の処理中のときに表示されるトレイ アイコン。 	16 X 16 PNG

Linux インストレーションでのファイル名および説明	イメージ サイズ（ピクセル、長さ X 高さ）およびタイプ
systray_quarantined.png クライアントが隔離中のときに表示されるトレイ アイコン。 	16 x 16 PNG
systray_reconnecting.png クライアントが再接続中のときに表示されるトレイ アイコン。 	16 X 16 PNG
vpnui48.png メイン プログラム アイコン。 	48 x 48 PNG

macOS 用 AnyConnect アイコンとロゴ

macOS 用のファイルはすべて次の場所に格納されています。

/Cisco AnyConnect Secure Mobility Client/Contents/Resources

次の表に、置換できるファイルと影響を受けるクライアント GUI エリアを示します。

macOS インストレーションでのファイル名および説明	イメージ サイズ（ピクセル数、長さ X 高さ）
bubble.png クライアントが接続または接続解除したときに表示される通知バブル。 	142 x 92 PNG
logo.png メイン画面の右上に表示されるロゴアイコン。 	50 x 33 PNG

macOS インストレーションでのファイル名および説明	イメージ サイズ（ピクセル数、長さ X 高さ）
vpngui.icns すべてのアイコン サービス（Dock、Sheets、Finder など）で使用される macOS アイコンのファイル形式。 	128 X 128 ICNS
macOS ステータス アイコン。 	16 X 16 PNG

AnyConnectクライアントのヘルプファイルの作成とアップロード

AnyConnect のユーザにヘルプを提供するために、サイトに関する手順を含むヘルプ ファイルを作成し、適応型セキュリティ アプライアンスにロードします。ユーザが AnyConnect に接続すると、AnyConnect がヘルプ ファイルをダウンロードし、AnyConnect ユーザ インターフェイス上にヘルプ アイコンを表示します。ユーザがヘルプ アイコンをクリックすると、ブラウザにヘルプ ファイルが開きます。PDF および HTML ファイルがサポートされています。

手順

ステップ 1 `help_AnyConnect.html` という名前の HTML ファイルを作成します。

ステップ 2 ASDM で、**[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [AnyConnect カスタマイゼーション/ローカリゼーション（AnyConnect Customization/LocalizationScript）] > [バイナリ（Binary）]** に移動します。

ステップ 3 **help_AnyConnect.xxx** ファイルをインポートします。サポートされる形式は、PDF、HTML、HTM、および MHT です。

ステップ 4 PC 上で AnyConnect を起動し、適応型セキュリティ アプライアンスに接続します。ヘルプ ファイルがクライアント PC にダウンロードされます。
ヘルプ アイコンが自動的に UI に追加されたことがわかるはずです。

ステップ 5 ヘルプ アイコンをクリックすると、ヘルプ ファイルがブラウザに表示されます。

ヘルプ アイコンが表示されない場合は、ヘルプのディレクトリを確認し、AnyConnect のダウンローダがヘルプ ファイルを取得できたかどうかを確認します。

ファイル名の「help_」の部分はダウンローダにより削除されるので、ご使用のオペレーティング システムに応じて、次のいずれかのディレクトリの中に AnyConnect.html が保存されているはずです。

- Windows：`C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Help`
- macOS：`/opt/cisco/anyconnect/help`

スクリプトの作成および展開

AnyConnect では、次のイベントが発生したときに、スクリプトをダウンロードして実行できます。

- セキュリティ アプライアンスで新しいクライアント VPN セッションが確立された。このイベントによって起動するスクリプトを *OnConnect* スクリプトと呼びます。スクリプトには、このファイル名プレフィックスが必要です。
- セキュリティ アプライアンスでクライアント VPN セッションが切断された。このイベントによって起動するスクリプトを *OnDisconnect* スクリプトと呼びます。スクリプトには、このファイル名プレフィックスが必要です。

Trusted Network Detection によって開始された新しいクライアント VPN セッションが確立すると、OnConnect スクリプトがトリガーされます（スクリプトを実行するための要件が満たされている場合）が、ネットワーク中断後に永続 VPN セッションを再接続しても、OnConnect スクリプトはトリガーされません。

この機能には次のような使用例があります。

- VPN 接続時にグループ ポリシーを更新する。
- VPN 接続時にネットワーク ドライブをマッピングし、接続解除後にマッピングを解除する。
- VPN 接続時にサービスにログインし、接続解除後にログオフする。

AnyConnect は、WebLaunch の起動中およびスタンドアロン起動中でのスクリプトの起動をサポートします。

ここでの説明は、スクリプトの作成方法と、ターゲット エンドポイントのコマンド ラインからスクリプトを実行し、テストする方法についての知識があることを前提としています。

（注） AnyConnect のソフトウェア ダウンロード サイトでは、サンプル スクリプトがいくつか提供されています。これらを確認する場合は、単なるサンプルであることに留意してください。これらのサンプル スクリプトは、スクリプトを実行するために必要なローカル コンピュータの要件を満たしていない場合があります。また、ご使用のネットワークおよびユーザのニーズに応じてカスタマイズしてからでないと使用できません。シスコでは、サンプル スクリプトまたはユーザ作成スクリプトはサポートしていません。

スクリプトの要件と制限

次のスクリプトの要件と制限事項に留意してください。

- サポートされるスクリプトの数：AnyConnect は、1 つの OnConnect スクリプトおよび 1 つの OnDisconnect スクリプトのみを実行します。ただし、これらのスクリプトが別のスクリプトを起動する場合があります。
- ファイル形式：AnyConnect は、ファイル名で OnConnect スクリプトおよび onDisconnect スクリプトを識別します。また、ファイル拡張子に関係なく、OnConnect または OnDisconnect で始まるファイルを検索します。照合プレフィックスに関連する最初のスクリプトが実行されます。解釈されたスクリプト（VBS、Perl、Bash など）または実行可能ファイルを認識します。
- スクリプト言語：クライアントでは、スクリプトを特定の言語で作成する必要はありません。ただし、スクリプトを実行可能なアプリケーションが、クライアント コンピュータにインストールされている必要があります。クライアントでスクリプトを起動するためには、このスクリプトがコマンド ラインから実行可能であることが必要です。
- Windows セキュリティ環境によるスクリプトの制限：Microsoft Windows では、AnyConnect はユーザが Windows にログインし、VPN セッションを確立した後でのみスクリプトを起動できます。そのため、ユーザのセキュリティ環境に伴う制限が、これらのスクリプトに適用されます。スクリプトが実行できる機能は、ユーザが起動権限を持つ機能に限られます。AnyConnect は、Windows でスクリプトを実行中は CMD ウィンドウを非表示にします。したがって、テストの目的で、.bat ファイル内のメッセージを表示するスクリプトを実行しても機能しません。
- スクリプトの有効化：デフォルトでは、クライアントはスクリプトを起動しません。スクリプトを有効にするには、AnyConnect プロファイルの EnableScripting パラメータを使用します。これにより、クライアントではスクリプトが存在する必要がなくなります。
- クライアント GUI 終了：クライアント GUI を終了しても、必ずしも VPN セッションは終了しません。OnDisconnect スクリプトは、セッションが終了した後で実行されます。
- 64 ビット Windows でのスクリプトの実行：AnyConnect クライアントは、32 ビット アプリケーションです。64 ビット Windows バージョンで実行すると、cmd.exe の 32 ビット バージョンが使用されます。

  32 ビットの cmd.exe では、64 ビットの cmd.exe でサポートされているコマンドの一部が欠けているため、一部のスクリプトについては、サポートされていないコマンドの実行を試

行したときにスクリプトの実行が停止したり、一部実行されてから停止したりする場合があります。たとえば、64 ビットの cmd.exe でサポートされている msg コマンドは、32 ビット バージョンの Windows 7（%WINDIR%\SysWOW64 に含まれる）では理解されない場合があります。

そのため、スクリプトを作成する場合は、32 ビットの cmd.exe でサポートされているコマンドを使用してください。

スクリプトの作成、テスト、および展開

対象のオペレーティング システムでスクリプトを作成およびテストします。ネイティブ オペレーティング システムのコマンド ラインからスクリプトを正しく実行できない場合は、AnyConnect でも正しく実行できません。

手順

ステップ 1 スクリプトを作成およびテストします。

ステップ 2 スクリプトの展開方法を選択します。

- ASDM を使用して、スクリプトをバイナリ ファイルとして ASA にインポートします。

  [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [AnyConnect カスタマイゼーション/ローカリゼーション（AnyConnect Customization/Localization）] > [スクリプト（Script）] に進みます。

  ASDM バージョン 6.3 以降を使用している場合、ASA では、ファイルをスクリプトとして識別できるように、プレフィックス scripts_ とプレフィックス OnConnect または OnDisconnect がユーザのファイル名に追加されます。クライアントが接続すると、セキュリティ アプライアンスは、リモート コンピュータ上の適切なターゲット ディレクトリにスクリプトをダウンロードし、scripts_ プレフィックスを削除し、OnConnect プレフィックスまたは OnDisconnect プレフィックスを残します。たとえば、myscript.bat スクリプトをインポートする場合、スクリプトは、セキュリティ アプライアンス上では scripts_OnConnect_myscript.bat となります。リモート コンピュータ上では、スクリプトは OnConnect_myscript.bat となります。

  6.3 よりも前の ASDM バージョンを使用している場合には、次のプレフィックスでスクリプトをインポートする必要があります。

  - scripts_OnConnect
  - scripts_OnDisconnect

    スクリプトの実行の信頼性を確保するために、すべての ASA で同じスクリプトを展開するように設定します。スクリプトを修正または置換する場合は、旧バージョンと同じ名前を使用し、ユーザが接続する可能性のあるすべての ASA に置換スクリプトを割り当てます。ユーザが接続すると、新しいスクリプトにより同じ名前のスクリプトが上書きされます。

- 社内のソフトウェア展開システムを使用して、VPNエンドポイントにスクリプトを手動で展開します。

  この方式を使用する場合は、次のスクリプト ファイル名プレフィックスを使用します。

  - OnConnect
  - OnDisconnect

  次のディレクトリにスクリプトをインストールします。

  表 *6*：スクリプトの所定の場所

OS	ディレクトリ
Microsoft Windows	%ALLUSERSPROFILE%\Cisco\Cisco AnyConnect Secure Mobility Client\Script
Linux （Linux では、User、Group、Other にファイルの実行権限を割り当てます）	/opt/cisco/anyconnect
macOS	/opt/cisco/anyconnect/script

スクリプトに関する AnyConnect プロファイルの設定

手順

ステップ 1 VPN プロファイル エディタを開き、ナビゲーション ペインから [プリファレンス（Part 2）（Preferences (Part 2)）] を選択します。

ステップ 2 [スクリプトの有効化（Enable Scripting）] をオンにします。クライアントでは、VPN 接続の接続時または接続解除時にスクリプトが起動します。

ステップ 3 [ユーザ制御可（User Controllable）] をオンにして、OnConnect スクリプトおよび OnDisconnect スクリプトの実行をユーザが有効または無効にすることができるようにします。

ステップ 4 [次のイベント時にスクリプトを終了する（Terminate Script On Next Event）] をオンにして、スクリプト処理可能な別のイベントへの遷移が発生した場合に、実行中のスクリプトプロセスをクライアントが終了できるようにします。たとえば、VPNセッションが終了すると、クライアントでは実行中の OnConnect スクリプトが終了し、AnyConnect で新しい VPN セッションが開始すると、実行中の OnDisconnect スクリプトが終了します。Microsoft Windows 上のクライアントでは OnConnect スクリプトまたは OnDisconnect スクリプトによって起動した任意のスクリプト、およびその従属スクリプトもすべて終了します。macOS および Linux 上のクライアントでは、OnConnect スクリプトまたは OnDisconnect スクリプトのみ終了し、子スクリプトは終了しません。

ステップ 5 [Post SBL OnConnect スクリプトを有効にする（Enable Post SBL On Connect Script）] をオンにして（デフォルトでオン）、SBL で VPN セッションが確立された場合にクライアントにより OnConnect スクリプトが（存在すれば）起動するようにします。

（注） 必ずクライアント プロファイルを ASA のグループ ポリシーに追加し、それを VPN エンドポイントにダウンロードしてください。

スクリプトのトラブルシューティング

スクリプトの実行に失敗した場合は、次のようにして問題を解決してください。

手順

ステップ 1 スクリプトに、`OnConnect` または `OnDisconnect` のプレフィックス名が付いていることを確認します。各オペレーティング システムで必要なスクリプト ディレクトリについては、「スクリプトの作成、テスト、および展開」を参照してください。

ステップ 2 スクリプトをコマンド ラインから実行してみます。コマンド ラインから実行できないスクリプトは、クライアントでも実行できません。コマンドラインでスクリプトの実行に失敗する場合は、スクリプトを実行するアプリケーションがインストールされていることを確認し、そのオペレーティング システムでスクリプトを作成し直してください。

ステップ 3 VPN エンドポイントのスクリプト ディレクトリに、OnConnect スクリプトと OnDisconnect スクリプトがそれぞれ 1 つのみ存在していることを確認してください。クライアントが ASA から OnConnect スクリプトをダウンロードして、別の ASA 用の異なるファイル名サフィックスを持つ 2 番目の OnConnect スクリプトをダウンロードした場合、クライアントは意図されたスクリプトを実行しない可能性があります。スクリプト パスに複数の OnConnect スクリプトまたは OnDisconnect スクリプトが含まれており、かつスクリプトの展開に ASA を使用している場合は、スクリプト ディレクトリ内のファイルを削除し、VPN セッションを再確立します。スクリプト パスに複数の OnConnect スクリプトまたは OnDisconnect スクリプトが含まれており、かつ手動展開を使用している場合は、不要なスクリプトを削除し、VPNセッションを再確立します。

ステップ 4 オペレーティング システムが Linux の場合は、スクリプト ファイルに実行権限が設定されていることを確認します。

ステップ 5 クライアント プロファイルでスクリプトが有効になっていることを確認します。

AnyConnect API によるカスタム アプリケーションの作成と展開

Windows、Linux、macOS のコンピュータでは、AnyConnect API を使用して独自の実行可能なユーザ インターフェイス（UI）を開発できます。AnyConnect バイナリ ファイルを置き換えることで UI を展開します。

次の表に、オペレーティング システムごとのクライアント実行可能ファイルのファイル名を示します。

クライアント OS	クライアント GUI ファイル	クライアント CLI ファイル
Windows	vpnui.exe	vpncli.exe
Linux	vpnui	vpn
macOS	ASA 展開ではサポートされません。ただし、Altiris Agent などの他の手段によって、クライアント GUI を置き換える Mac 用の実行ファイルを展開できます。	vpn

実行可能ファイルは、ASA にインポートされたリソース ファイル（ロゴ イメージなど）を呼び出すことができます。独自の実行可能ファイルを展開する場合、リソース ファイルに任意のファイル名を使用できます。

制約事項

- 適応型セキュリティ アプライアンスから最新の AnyConnect ソフトウェアを展開することはできません。適応型セキュリティ アプライアンスに AnyConnect パッケージの最新バージョンを配置すると、AnyConnect クライアントはその更新をダウンロードして、カスタム UI を置き換えます。カスタム クライアントおよび関連する AnyConnect ソフトウェアの配布を管理する必要があります。ASDM でバイナリをアップロードして AnyConnect クライアントを置き換えることができる場合でも、この展開機能は、カスタム アプリケーションを使用しているときにはサポートされません。
- Web セキュリティまたはネットワーク アクセス マネージャを展開する場合は、Cisco AnyConnect Secure Mobility Client GUI を使用します。
- Start Before Logon はサポートされていません。

AnyConnect CLI コマンドの使用

Cisco AnyConnect VPN Client には、グラフィカル ユーザ インターフェイスを使用せずにクライアント コマンドを入力することを希望するユーザ向けに、コマンドライン インターフェイス（CLI）があります。ここでは、CLI コマンド プロンプトの起動方法、および CLI を介して使用できるコマンドについて説明します。

- クライアント CLI プロンプトの起動 （85 ページ）
- クライアント CLI コマンドの使用 （85 ページ）
- ASA によるセッション終了時に Windows ポップアップ メッセージが表示されないようにする （87 ページ）

クライアント CLI プロンプトの起動

CLI コマンド プロンプトを起動するには、以下の手順を実行します。

- （Windows）Windows フォルダ C:/Program Files/Cisco/Cisco AnyConnect Secure Mobility Client にある *vpncli.exe* ファイルを見つけます。vpncli.exe をダブル クリックします。
- （Linux および macOS）/opt/cisco/anyconnect/bin/ フォルダにある *vpn* ファイルを見つけます。*vpn* ファイルを実行します。

クライアント CLI コマンドの使用

インタラクティブ モードで CLI を実行する場合、独自のプロンプトが表示されます。コマンド ラインを使用することもできます。

- connect *IP address* または *alias*：クライアントは特定の ASA との接続を確立します。
- disconnect：クライアントは以前に確立した接続を閉じます。
- stats：確立された接続に関する統計情報を表示します。
- quit：CLI インタラクティブ モードを終了します。
- exit：CLI インタラクティブ モードを終了します。

次の例は、ユーザがコマンド ラインから接続を確立し、終了する例です。

Windows

```
connect 209.165.200.224
```

アドレスが 209.165.200.224 のセキュリティ アプライアンスへの接続を確立します。要求されたホストにアクセスすると、AnyConnect クライアントに、ユーザが属するグループが表示され、ユーザ名とパスワードが要求されます。オプションのバナーを表示するよう指定されてい

る場合、ユーザはバナーに応答する必要があります。デフォルトの応答は、接続の試行を終了する「n」です。次に例を示します。

```
VPN > connect 209.165.200.224
>>contacting host (209.165.200.224) for login information...
>>Please enter your username and password.
Group: testgroup
Username: testuser
Password: ********
>>notice: Please respond to banner.
VPN>
STOP! Please read. Scheduled system maintenance will occur tonight from 1:00-2:00 AM for
 one hour.
The system will not be available during that time.

accept? [y/n] y
>> notice: Authentication succeeded. Checking for updates...
>> state: Connecting
>> notice: Establishing connection to 209.165.200.224.
>> State: Connected
>> notice: VPN session established.
VPN>
```

stats

現在の接続の統計情報を表示します。以下に例を示します。

```
VPN > stats
[Tunnel information]

Time Connected: 01:17:33
Client Address: 192.168.23.45
Server Address: 209.165.200.224

[Tunnel Details]

Tunneling Mode: All traffic
Protocol: DTLS
Protocol Cipher: RSA_AES_256_SHA1
Protocol Compression: None

[Data Transfer]

Bytes (sent/received): 1950410/23861719
Packets (sent/received): 18346/28851
Bypassed (outbound/inbound): 0/0
Discarded (outbound/inbound): 0/0

[Secure Routes]

Network Subnet
0.0.0.0 0.0.0.0
VPN>
```

disconnect

以前に確立した接続を閉じます。以下に例を示します。

```
VPN > disconnect
>> state: Disconnecting
>> state: Disconnected
>> notice: VPN session ended.
VPN>
```

quit または exit

いずれのコマンドも CLI のインタラクティブ モードを終了します。以下に例を示します。

```
quit
goodbye
>>state: Disconnected
```

Linux または Mac OS X

```
/opt/cisco/anyconnect/bin/vpn connect 1.2.3.4
```

アドレスが 1.2.3.4 の ASA への接続を確立します。

```
/opt/cisco/anyconnect/bin/vpn connect some_asa_alias
```

プロファイルを読み込み、エイリアス *some_asa_alias* を検索してアドレスを探し、ASA への接続を確立します。

```
/opt/cisco/anyconnect/bin/vpn stats
```

vpn 接続に関する統計情報を表示します。

```
/opt/cisco/anyconnect/bin/vpn disconnect
```

存在する場合、VPN セッションを切断します。

ASA によるセッション終了時に Windows ポップアップ メッセージが表示されないようにする

ASA からセッション リセットを発行することによって AnyConnect セッションを終了すると、エンド ユーザに次の Windows ポップアップ メッセージが表示されます。

```
The secure gateway has terminated the vpn connection. The following message was received
 for the gateway: Administrator Reset
```

このメッセージを表示させたくないと思う場合があるかもしれません（たとえば、CLI コマンドを使用して VPN トンネルを開始するときなど）。クライアントが接続した後に、クライアント CLI を再起動することによって、このメッセージを表示さないようにすることができます。次に、この処理を行った場合の CLI 出力例を示します。

```
C:/Program Files (x86)\Cisco\Cisco AnyConnect Secure Mobility Client>vpncli
Cisco AnyConnect Secure Mobility Client (version 4.x).
Copyright (c) 2016 Cisco Systems, Inc.
All Rights Reserved.
>> state: Connected
>> state: Connected
>> notice: Connected to asa.cisco.com.
>> notice: Connected to asa.cisco.com.
>> registered with local VPN subsystem.
>> state: Connected
>> notice: Connected to asa.cisco.com.
>> state: Disconnecting
>> notice: Disconnect in progress, please wait...
>> state: Disconnected
>> notice: On a trusted network.
>> error: The secure gateway has terminated the VPN connection.
The following message was received from the secure gateway: Administrator Reset
VPN>
```

または、次の場所にあるエンドポイント デバイスでは、Windows レジストリに SuppressModalDialogs という名前の 32 ビットの倍精度値を作成できます。クライアントは名前の有無を検査しますが、値は無視します。

- 64 ビット Windows：

  HKEY_LOCAL_MACHINE/SOFTWARE\Wow6432Node\Cisco\ Cisco AnyConnect Secure Mobility Client

- 32 ビット Windows：

  HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\Cisco AnyConnect Secure Mobility Client

ISE 展開のための AnyConnect カスタマイズおよびローカリゼーションの準備

AnyConnect ローカリゼーション バンドルの準備

AnyConnect ローカリゼーション バンドルは、AnyConnect をローカライズするために使用される変換テーブル ファイルとインストーラ トランスフォーム ファイルを含む zip ファイルです。この zip ファイルは、ISE からユーザに AnyConnect を展開するために使用される ISE AnyConnect リソースの一部です。この zip ファイルの内容は、次の手順に従って AnyConnect 展開でサポートする言語によって定義されます。

始める前に

ISE は、AnyConnect ローカリゼーション バンドル内のコンパイル済みのバイナリ変換テーブルを必要とします。gettext には、編集で使用されるテキスト .po とランタイムに使用されるコンパイル済みのバイナリ .mo の 2 つのファイル形式があります。コンパイルは、gettext ツールの msgfmt を使用して行われます。gettext ユーティリティを http://www.gnu.org/software/gettext/ からダウンロードし、管理に使用するローカル コンピュータ（リモートのユーザ コンピュータ以外）にインストールします。

手順

ステップ 1 AnyConnect 展開で使用する変換テーブル ファイルを取得して準備します。

a) www.cisco.com の Cisco AnyConnect Secure Mobility Client ソフトウェア ダウンロード ページから `AnyConnect-translations-`*`(date)`*`.zip` ファイルをダウンロードしてこれを開きます。

   この zip ファイルには、シスコによって提供されるすべての言語変換用 *.po ファイルが含まれます。

b) （任意） 現在の環境用にカスタマイズまたは作成した変換テーブル ファイル（*.po ファイル）があれば、それを特定します。

c) gettext メッセージ ファイル コンパイラを実行して、使用している各 *.po ファイルから *.mo ファイルを作成します。

msgfmt -o AnyConnect.mo AnyConnect.po

ステップ 2 AnyConnect 展開で使用する変換テーブルを収集します。

a) ローカル コンピュータの作業領域に l10n という名前のディレクトリを作成します。

b) l10n ディレクトリの下に、含める各言語のディレクトリを作成します。ディレクトリの名前は各言語コードです。

たとえば、フランス語（カナダ）の場合は fr-ch です。

c) 含めるコンパイル済み変換テーブル ファイルを、適切な名前のディレクトリに配置します。

コンパイル済み変換テーブルに *.po ファイルを含めないでください。*.mo ファイルのみをこのファイルに含める必要があります。

ディレクトリ構造は、フランス語（カナダ）、ヘブライ語、および日本語の変換テーブルを含む次のディレクトリ構造と同様になります。

```
l10n\fr-ch\AnyConnect.mo
    \he\AnyConnect.mo
    \ja\AnyConnect.mo
```

ステップ 3 （Windows の場合のみ）AnyConnect 展開で使用する言語ローカリゼーション変換ファイルを取得して準備します。

a) www.cisco.com の Cisco AnyConnect Secure Mobility Client ソフトウェア ダウンロード ページから、展開に適用する言語ローカリゼーション変換ファイルを含む zip ファイルをダウンロードしてこれを開きます。

zip ファイルの名前は anyconnect-win-*(version)*-webdeploy-k9-lang.zip または anyconnect-win-*(version)*-gina-webdeploy-k9-lang.zip です。

（注） 言語ローカリゼーション ファイルのバージョンは、現在の環境で使用する AnyConnect のバージョンに一致する必要があります。AnyConnect を新しいバージョンにアップグレードする場合は、ローカリゼーションバンドルで使用される言語ローカリゼーションファイルも同じバージョンにアップグレードする必要があります。

b) 現在の環境用にカスタマイズまたは作成した言語ローカリゼーション変換ファイルがあれば、それを特定します。

ステップ 4 （Windows の場合のみ）AnyConnect 展開で使用する言語ローカリゼーション ファイルを収集します。

a) ローカル コンピュータの同じ作業領域に mst いう名前のディレクトリを作成します。

b) mstディレクトリの下に、含める各言語のディレクトリを作成します。ディレクトリの名前は各言語コードです。

たとえば、フランス語（カナダ）の場合は fr-ch です。

c) 含める言語ローカリゼーション ファイルを、適切な名前のディレクトリに配置します。

ディレクトリ構造は、次のようになります。

```
l10n\fr-ch\AnyConnect.mo
    \he\AnyConnect.mo
    \ja\AnyConnect.mo
mst\fr-ch\AnyConnect_fr-ca.mst
   \he\AnyConnect_he.mst
   \ja\AnyConnect_ja.mst
```

ステップ 5 標準圧縮ユーティリティを使用して、このディレクトリ構造を `AnyConnect-Localization-Bundle-(release).zip` などの適切な名前のファイルに ZIP 圧縮して、AnyConnect ローカリゼーション バンドルを作成します。

次のタスク

AnyConnect ローカリゼーション バンドルを、AnyConnect をユーザに展開するために使用する ISE AnyConnect リソースの一部として ISE にアップロードします。

AnyConnect カスタマイゼーション バンドルの準備

AnyConnect カスタマイゼーション バンドルは、カスタム AnyConnect GUI リソース、カスタム ヘルプ ファイル、VPN スクリプト、およびインストーラ トランスフォームを含む zip ファイルです。この zip ファイルは、ISE からユーザに AnyConnect を展開するために使用される ISE AnyConnect リソースの一部です。このファイルのディレクトリ構造は次のとおりです。

```
win\resource\
   \binary
   \transform
mac-intel\resource
         \binary
         \transform
```

カスタマイズされた AnyConnect コンポーネントは、次のように Windows および macOS プラットフォームの `resource`、`binary`、および `transform` サブディレクトリに含まれています。

- 各 `resource` サブディレクトリには、そのプラットフォーム用のすべてのカスタム AnyConnect GUI コンポーネントが含まれます。

  これらのリソースを作成する方法については、「AnyConnect GUI のカスタム アイコンおよびロゴの作成 （69 ページ）」を参照してください。

- 各 `binary` サブディレクトリには、そのプラットフォーム用のカスタム ヘルプ ファイルおよび VPN スクリプトが含まれます。

  - AnyConnect ヘルプ ファイルを作成する方法については、「AnyConnect クライアントのヘルプ ファイルの作成とアップロード （78 ページ）」を参照してください。

  - VPN スクリプトを作成する方法については、「スクリプトの作成および展開 （79 ページ）」を参照してください。

- 各 transform サブディレクトリには、そのプラットフォーム用のインストーラ トランスフォームが含まれます。
  - Windows のカスタム インストーラ トランスフォームの作成方法については、次の項を参照してください。 インストール動作の変更、Windows （52 ページ）
  - macOS のインストーラ トランスフォームの作成方法については、次の項を参照してください。 ACTransforms.xml による macOS でのインストーラ動作のカスタマイズ （59 ページ）

始める前に

AnyConnect カスタマイゼーション バンドルを準備する前に、必要なすべてのカスタム コンポーネントを作成します。

手順

ステップ 1 説明されているディレクトリ構造を、ローカル コンピュータの作業領域に作成します。

ステップ 2 resources ディレクトリに、各プラットフォーム用のカスタム AnyConnect GUI ファイルを含めます。ファイルにはすべて適切に名前が付けられ、アイコン、およびロゴのサイズが適切に調整されていることを確認します。

ステップ 3 binary ディレクトリに、カスタム help_AnyConnect.html ファイルを含めます。

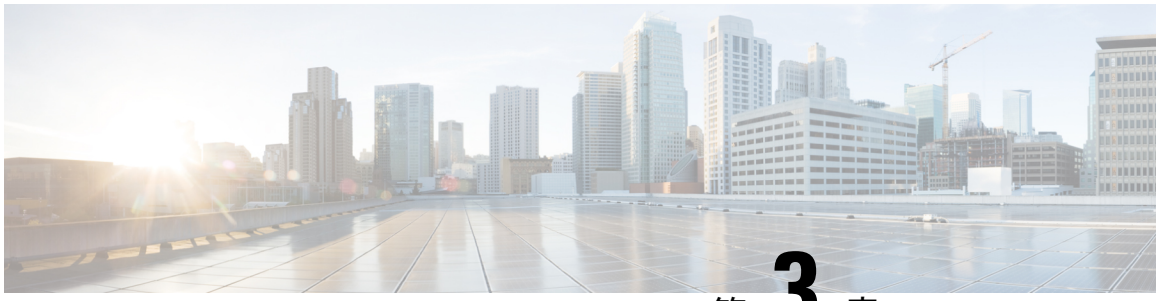
ステップ 4 binary ディレクトリに、VPN の OnConnect および OnDisconnect スクリプト、およびこれらが呼び出すその他のスクリプトを含めます。

ステップ 5 transform ディレクトリに、プラットフォーム固有のインストーラ トランスフォームを含めます。

ステップ 6 標準圧縮ユーティリティを使用して、このディレクトリ構造を AnyConnect-Customization-Bundle.zip などの適切な名前のファイルに ZIP 圧縮して、AnyConnect カスタマイゼーション バンドルを作成します。

次のタスク

AnyConnect カスタマイゼーション バンドルを、AnyConnect をユーザに展開するために使用する ISE AnyConnect リソースの一部として ISE にアップロードします。



第 3 章

AnyConnect プロファイル エディタ

- プロファイル エディタについて （93 ページ）
- スタンドアロン プロファイル エディタ （94 ページ）
- AnyConnect VPN プロファイル （97 ページ）
- AnyConnect ローカル ポリシー （120 ページ）

プロファイル エディタについて

Cisco AnyConnect Secure Mobility Client ソフトウェア パッケージには、すべてのオペレーティング システム用のプロファイル エディタが含まれています。AnyConnect クライアント イメージを ASA にロードすると、ASDM はプロファイル エディタをアクティブ化します。ローカルまたはフラッシュからクライアント プロファイルをアップロードできます。

複数の AnyConnect パッケージをロードした場合は、最新の AnyConnect パッケージのクライアント プロファイル エディタがアクティブ化されます。これによりエディタには、旧バージョンのクライアントで使用される機能に加え、ロードされた最新の AnyConnect で使用される機能が表示されます。

Windows で動作するスタンドアロン プロファイル エディタもあります。

ASDM からの新しいプロファイルの追加

（注） クライアント プロファイルを作成する前に、まずクライアント イメージをアップロードする必要があります。

プロファイルが AnyConnect の一部としてエンドポイント上の管理者定義のエンド ユーザ要件および認証ポリシーに展開され、これにより、エンド ユーザが設定済みのネットワーク プロファイルを使用できるようになります。1 つ以上のプロファイルを作成および設定するには、プロファイル エディタを使用します。AnyConnect には ASDM の一部であるプロファイル エディタが、スタンドアロン Windows プログラムとして組み込まれています。

新しいクライアント プロファイルを ASDM から ASA に追加するには、次の手順を実行します。

手順

ステップ 1 ASDM で、**[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [AnyConnect クライアント プロファイル（AnyConnect Client Profile）]** を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 プロファイル名を入力します。

ステップ 4 [プロファイルの使用（Profile Usage）] ドロップダウン リストから、プロファイルを作成するモジュールを選択します。

ステップ 5 （任意）[プロファイルの場所（Profile Location）] フィールドで [フラッシュの参照（Browse Flash）] をクリックし、ASA の XML ファイルのデバイス ファイル パスを選択します。

ステップ 6 （任意）スタンドアロン エディタを使用してプロファイルを作成した場合、[アップロード（Upload）] をクリックして、そのプロファイル定義を使用します。

ステップ 7 （任意）ドロップダウン リストから AnyConnect グループ ポリシーを選択します。

ステップ 8 [OK] をクリックします。

スタンドアロン プロファイル エディタ

ASDM のプロファイル エディタに加えて、Windows のプロファイル エディタのスタンドアロンバージョンを使用できます。クライアントを事前展開する場合は、ソフトウェア管理システムを使用してコンピュータに展開する、VPNサービス用のプロファイルおよびその他のモジュールを、スタンドアロン プロファイル エディタを使用して作成します。

[プログラムの追加と削除（Add or Remove Programs）] を使用して、スタンドアロンの Cisco AnyConnect Profile Editor のインストールを変更したり、VPN やその他のプロファイル エディタをアンインストールしたりできます。

要件

- Java：最低でも JRE 1.6 がプロファイル エディタの前提条件ですが、管理者は自分でこれを展開する必要があります。

（注） スタンドアロン プロファイル エディタをアンインストールするときに、JRE 1.6 は自動的にアンインストールされません。別途自分でアンインストールする必要があります。

- サポートされるオペレーティング システム：このアプリケーションは、Windows 7 でテスト済みです。MSI は、Windows 上でだけ実行されます。
- サポートされるブラウザ：このアプリケーションに含まれているヘルプファイルは、Firefox および Internet Explorer でサポートされています。その他のブラウザではテストされていません。
- 必要なハード ドライブ容量：Cisco AnyConnect プロファイル エディタ アプリケーションは、最大 5 MB のハード ドライブ容量を必要とします。JRE 1.6 は、最大 100 MB のハード ドライブ容量を必要とします。
- 最初の接続に関するユーザ制御可能なすべての設定をクライアント GUI に表示するには、VPN プロファイルのサーバ リストに ASA を含める必要があります。ASA のアドレスまたは FQDN をホスト エントリとしてプロファイルに追加していない場合、フィルタがセッションに適用されません。たとえば、証明書照合を作成し、証明書が基準と適切に一致した場合でも、プロファイルに ASA をホスト エントリとして追加しなかった場合、この証明書照合は無視されます。

スタンドアロン AnyConnect プロファイル エディタのインストール

スタンドアロンの AnyConnect プロファイル エディタは、AnyConnect の ISO ファイルおよび .pkg ファイルとは別に Windows 実行 msi ファイルとして配布され、ファイルの命名規則は `tools-anyconnect-win-<version>-profileeditor-k9.msi` となっています。

手順

ステップ 1 `tools-anyconnect-win-<version>-profileeditor-k9.smi` を https://software.cisco.com/download/home/286281283/type/282364313/release/4.0.00061 からダウンロードします。

ステップ 2 `tools-anyconnect-win-<version>-profileeditor-k9.msi` をダブルクリックして、インストール ウィザードを起動します。

ステップ 3 [セットアップへようこそ（Welcome）] 画面で、[次へ（Next）] をクリックします。

ステップ 4 [セットアップ タイプの選択（Choose Setup Type）] ウィンドウで、次のいずれかのボタンをクリックし、[次へ（Next）] をクリックします。

- [一般（Typical）]：ネットワーク アクセス マネージャ プロファイル エディタのみを自動的にインストールします。
- [カスタム（Custom）]：インストールするプロファイル エディタを選択できます。
- [完全（Complete）]：すべてのプロファイル エディタが自動的にインストールされます。

ステップ 5 前の手順で [一般（Typical）] または [完全（Complete）] をクリックした場合は、次の手順に進みます。前の手順で [カスタム（Custom）] をクリックした場合は、インストールするスタンドアロン プロファイル エディタのアイコンをクリックし、[ローカルのハード ドライブにインストールする（Will be installed on local hard drive）] を選択するか、[すべての機能を利用し

ない（Entire Feature will be unavailable）] をクリックして、そのスタンドアロン プロファイル エディタがインストールされないようにします。[次へ（Next）] をクリックします。

ステップ 6 [インストール準備完了（Ready to Install）] 画面で [インストール（Install）] をクリックします。

ステップ 7 [終了（Finish）] をクリックします。

- スタンドアロン AnyConnect プロファイル エディタは、`C:\Program Files\Cisco\Cisco AnyConnect プロファイル エディタ` ディレクトリにインストールされます。
- プロファイル エディタを起動するには、**[スタート（Start）] > [すべてのプログラム（All Programs）] > [Cisco] > [Cisco AnyConnect プロファイル エディタ（Cisco AnyConnect Profile Editor）]** を選択してから、サブメニューで目的のスタンドアロン プロファイル エディタをクリックするか、デスクトップ上にインストールされる該当するプロファイル エディタ ショートカット アイコンをクリックします。

スタンドアロン プロファイル エディタを使用したクライアント プロファイルの編集

セキュリティ上の理由から、スタンドアロン プロファイル エディタ以外でクライアント プロファイル XML ファイルを手動で編集することはできません。スタンドアロン プロファイル エディタ以外で編集されたプロファイル XML ファイルは、ASA によって受け入れられません。

手順

ステップ 1 デスクトップ上のショートカット アイコンをダブルクリックするか、**[スタート] > [すべてのプログラム] > [Cisco] > [Cisco AnyConnect プロファイル エディタ（Cisco AnyConnect Profile Editor）]** の順に選択し、サブメニューから目的のプロファイル エディタを選択して、起動します。

ステップ 2 **[ファイル（File）] > [オープン（Open）]** を選択し、編集するクライアント プロファイル XML ファイルまで移動します。

たとえば、Web セキュリティ機能のクライアント プロファイルを、誤って、VPN など別の機能のプロファイル エディタを使用して開こうとすると、「スキーマの検証に失敗しました（Schema Validation failed）」というメッセージが表示され、プロファイルを編集できません。

誤って、同じ種類のプロファイル エディタのインスタンスを 2 つ使用して、同じクライアント プロファイルを編集しようとした場合は、そのクライアント プロファイルに加えた最後の変更が保存されます。

ステップ 3 プロファイルに変更を加え、**[ファイル（File）] > [保存（Save）]** を選択して変更を保存します。

AnyConnect VPN プロファイル

Cisco AnyConnect Secure Mobility Client 機能は、AnyConnect プロファイルで有効になります。これらのプロファイルには、コア クライアント VPN 機能とオプション クライアント モジュールであるネットワーク アクセス マネージャ、ISE ポスチャ、カスタマー エクスペリエンス フィードバック、Web セキュリティの構成設定が含まれています。ASA は、AnyConnect のインストールと更新中にプロファイルを展開します。ユーザがプロファイルの管理や修正を行うことはできません。

ASA または ISE は、すべての AnyConnect ユーザにグローバルにプロファイルを展開するか、ユーザのグループ ポリシーに基づいて展開するように設定できます。通常、ユーザは、インストールされている AnyConnect モジュールごとに 1 つのプロファイル ファイルを持ちます。場合により、1 人のユーザに複数の VPN プロファイルを割り当てることがあります。複数の場所で作業するユーザには、複数の VPN プロファイルが必要になります。

一部のプロファイル設定は、ユーザのコンピュータ上のユーザ プリファレンス ファイルまたはグローバル プリファレンス ファイルにローカルに保存されます。ユーザ ファイルには、AnyConnect クライアントが、クライアント GUI の [プリファレンス（Preferences）] タブにユーザ制御可能設定を表示するうえで必要となる情報、およびユーザ、グループ、ホストなど、直近の接続に関する情報が保存されます。

グローバル ファイルには、ユーザ制御可能設定に関する情報が保存されます。これにより、ログイン前でも（ユーザがいなくても）それらの設定を適用できます。たとえば、クライアントでは Start Before Logon や起動時自動接続が有効になっているかどうかをログイン前に認識する必要があります。

AnyConnect プロファイル エディタ、プリファレンス（Part 1）

- [Start Before Logon の使用（Use Start Before Logon）]（Windows のみ）：Windows のログイン ダイアログボックスが表示される前に AnyConnect を開始することにより、ユーザを Windows へのログイン前に VPN 接続を介して企業インフラへ強制的に接続させます。認証後、ログイン ダイアログボックスが表示され、ユーザは通常どおりログインします。
- [事前接続メッセージの表示（Show Pre-connect Message）]：管理者は、ユーザが初めて接続を試行する前にワンタイム メッセージを表示させることができます。たとえば、メッセージを表示して、ユーザにスマート カードをリーダに挿入するよう促すことができます。このメッセージは、AnyConnect メッセージ カタログに表示され、ローカライズされています。
- [証明書ストア（Certificate Store）]：AnyConnect がどの証明書ストアで証明書を保存し、読み取るかを制御します。セキュア ゲートウェイは、適切に設定し、複数の証明書認証の組み合わせのうちどれが特定の VPN 接続で許容されるかをクライアントに指定する必要があります。

VPN プロファイルの CertificateStore 設定の値は、セキュア ゲートウェイに許容される証明書のタイプによって異なります。証明書のタイプは、2 ユーザ証明書か、1 マシンおよび 1 ユーザ証明書のどちらかです。

macOS 上で AnyConnect がアクセスできる証明書ストアをさらに絞りこめるようにするには、Windows 用または macOS 用のドロップダウンから証明書ストアを設定できます。macOS のための新しいプロファイル プリファレンスは CertificateStoreMac といい、次の追加された値をサポートします。

- [すべて（All）]（Windows 用）：1 マシンおよび 1 ユーザ証明書が ASA 設定によって許容されます。
- [ユーザ（User）]（Windows 用）：2 ユーザ証明書が ASA 設定によって許容されます。
- [すべて（All）]（macOS 用）：利用可能なすべての macOS キーチェーンおよびファイル ストアからの証明書を使用します。
- [システム（System）]（macOS 用）：macOS システム キーチェーンおよびシステム ファイル/PEM ストアからの証明書のみを使用します。
- [ログイン（Log in）]（macOS 用）：ユーザ ファイル/PEM ストアに加え、macOS ログイン キーチェーンおよびダイナミック スマートカード キーチェーンからの証明書のみを使用します。

- [**証明書ストアの上書き**（Certificate Store Override）]：ユーザに自分のデバイスに対する管理者権限がない場合、管理者は Windows マシン証明書ストアで証明書を検索するように AnyConnect に指示できます。証明書ストアの上書きは、デフォルトでは UI プロセスによって接続が開始される SSL にのみ適用されます。IPSec/IKEv2 を使用している場合、AnyConnect プロファイルのこの機能は適用されません。

  （注） マシン証明書を使用して Windows に接続するには、このオプションが有効にされている事前展開されたプロファイルが必要です。接続する前に Windows デバイスにこのプロファイルが存在しない場合、証明書はマシン ストアにアクセスできず、接続は失敗します。

  - True：AnyConnect は、Windows マシン証明書ストア内の証明書を検索します。CertificateStore を [すべて（all）] に設定する場合、CertificateStoreOverride は true に設定する必要があります。
  - False：AnyConnect は、Windows マシン証明書ストア内の証明書を検索しません。

- AutomaticCertSelection：セキュア ゲートウェイで複数証明書の認証を設定するときは、この値を true に設定する必要があります。

- [起動時に自動接続（Auto Connect on Start）]：AnyConnect の起動時に、プロファイルで指定されたセキュア ゲートウェイまたはクライアントが最後に接続していたゲートウェイとの VPN 接続が自動的に確立されます。
- [接続時に最小化（Minimize On Connect）]：VPN 接続の確立後、AnyConnect GUI が最小化されます。
- [ローカル LAN アドレス（Local LAN Access）]：ASA への VPN セッション中にリモート コンピュータへ接続したローカル LAN に対してユーザが無制限にアクセスできるようになります。

（注） ローカル LAN アクセスを有効にすると、パブリック ネットワークからユーザ コンピュータを経由して、社内ネットワークにセキュリティの脆弱性が生じる可能性があります。代替手段として、セキュリティ アプライアンス（バージョン 8.4(1) 以降）で、デフォルト グループ ポリシーに含まれている AnyConnect クライアント ローカル印刷ファイアウォール ルールを使用した SSL クライアント ファイアウォールを展開するように設定することもできます。このファイアウォール ルールを有効にするには、このエディタ [プリファレンス（Part 2）（Preferences (Part 2)）] で、[自動 VPN ポリシー（Automatic VPN Policy）]、[常にオン（Always on）]、および [VPN の接続解除を許可（Allow VPN Disconnect）] も有効にする必要があります。

- [キャプティブポータル検出を無効にする（Disable Captive Portal Detection）]：AnyConnect クライアントが受信する証明書の共通名が、ASA 名と一致しない場合、キャプティブ ポータルが検出されます。この動作により、ユーザによる認証が促されます。自己署名証明書を使用する一部のユーザは、HTTP キャプティブ ポータルで保護されている企業リソースへの接続を有効にすることを望むことがあるため、[キャプティブポータル検出を無効にする（Disable Captive Portal Detection）] チェックボックスをオンにする必要があります。管理者は、このオプションをユーザが設定できるようにするかどうかを判断し、判断に基づいてチェックボックスをオンにすることもできます。ユーザが設定できるようにした場合は、AnyConnect Secure Mobility Client UI の [プリファレンス（Preferences）] タブにチェックボックスが表示されます。
- [自動再接続（Auto Reconnect）]：接続が解除された場合、AnyConnect により VPN 接続の再確立が試行されます。[自動再接続（Auto Reconnect）] を無効にすると、接続解除の原因にかかわらず、再接続は試行されません。

（注） 自動再接続は、ユーザがクライアントの動作を制御するシナリオで使用します。この機能は、AlwaysOn ではサポートされません。

- **自動再接続の動作**

- DisconnectOnSuspend：AnyConnect では、システムの一時停止時に VPN セッションに割り当てられたリソースが解放され、システムの再開後も再接続は試行されません。
- ReconnectAfterResume（デフォルト）：接続が解除された場合、AnyConnect により VPN 接続の再確立が試行されます。

- [自動更新（Auto Update）]：オンにすると、クライアントの自動アップデートが有効になります。[ユーザ制御可（User Controllable）]チェックボックスをオンにすると、クライアントのこの設定を無効にできます。
- [RSA セキュア ID 連携（RSA Secure ID Integration）]（Windows のみ）：ユーザが RSA とどのように対話するかを制御します。デフォルトでは、AnyConnect が RSA の適切な対話方法を決定します（自動設定：ソフトウェア トークンとハードウェア トークンの両方を受け入れます）。
- [Windows ログインの強制（Windows Logon Enforcement）]：Remote Desktop Protocol（RDP）セッションから VPN セッションを確立することを許可します。スプリット トンネリングはグループ ポリシーで設定する必要があります。VPN 接続を確立したユーザがログオフすると、その VPN 接続は AnyConnect により解除されます。接続がリモート ユーザによって確立されていた場合、そのリモート ユーザがログオフすると、VPN 接続は終了します。
  - [シングル ローカル ログイン（Single Local Logon）]（デフォルト）：VPN 接続全体で、ログインできるローカル ユーザは 1 人だけです。また、クライアント PC に複数のリモート ユーザがログインしている場合でも、ローカル ユーザが VPN 接続を確立することはできます。この設定は、VPN 接続を介した企業ネットワークからのリモート ユーザ ログインに対しては影響を与えません。

    （注） VPN 接続が排他的トンネリング用に設定されている場合、VPN 接続用のクライアント PC のルーティング テーブルが変更されるため、リモート ログインは接続解除されます。VPN 接続がスプリット トンネリング用に設定されている場合、リモート ログインが接続解除されるかどうかは、VPN 接続のルーティング設定によって異なります。

  - [シングル ログイン（Single Logon）]：VPN 接続全体で、ログインできるユーザは 1 人だけです。VPN 接続の確立時に、ローカルまたはリモートで複数のユーザがログインしている場合、接続は許可されません。VPN 接続中にローカルまたはリモートで第 2 のユーザがログインすると、VPN 接続が終了します。VPN 接続中の追加のログインは許可されません。そのため、VPN 接続によるリモート ログインは行えません。

    （注） 複数同時ログオンはサポートされません。

- **[Windows VPN 確立（Windows VPN Establishment）]**：クライアント PC にリモート ログインしたユーザが VPN 接続を確立した場合の AnyConnect の動作を決定します。設定可能な値は次のとおりです。
  - [ローカルユーザのみ（Local Users Only）]（デフォルト）：リモート ログインしたユーザは、VPN 接続を確立できません。これは、以前のバージョンの AnyConnect と同じ機能です。
  - [リモートユーザを許可（Allow Remote Users）]：リモート ユーザは VPN 接続を確立できます。ただし、設定された VPN 接続ルーティングによってリモート ユーザが接続解除された場合は、リモート ユーザがクライアント PC に再アクセスできるように、VPN 接続が終了します。リモート ユーザが VPN 接続を終了せずにリモート ログイン セッションを接続解除するには、VPN を確立した後、90 秒間待つ必要があります。
- **スマートカードのピンのクリア（Clear SmartCard PIN）**
- [サポートされている IP プロトコル（IP Protocol Supported）]：IPv4 アドレスおよび IPv6 アドレスの両方で AnyConnect を使用して ASA に接続しようとしているクライアントの場合、AnyConnect は接続の開始に際してどの IP プロトコルを使用するか決定する必要があります。デフォルトで、AnyConnect は最初に IPv4 を使用して接続しようとします。接続が成功しない場合、IPv6 を使用して接続を開始しようとします。

  このフィールドでは、最初の IP プロトコルとフォールバックの順序を設定します。
  - [IPv4]：ASA に対して IPv4 接続のみ可能です。
  - [IPv6]：ASA に対して IPv6 接続のみ可能です。
  - [IPv4, IPv6]：最初に ASA に IPv4 接続しようとします。クライアントが IPv4 を使用して接続できない場合、IPv6 接続をしようとします。
  - [IPv6, IPv4]：最初に ASA に IPv6 接続しようとします。クライアントが IPv6 を使用して接続できない場合、IPv4 接続をしようとします。

  （注） IPv4 から IPv6、IPv6 から IPv4 プロトコルへのフェールオーバーも VPN セッション中に行うことができます。プライマリ IP プロトコルが失われると、可能な場合に、セカンダリ IP プロトコルを介して VPN セッションが再確立されます。

AnyConnect プロファイル エディタ、プリファレンス（Part 2）

- [自動証明書選択の無効化（Disable Automatic Certificate Selection）]（Windows のみ）：クライアントによる自動証明書選択を無効にし、ユーザに対して認証証明書を選択するためのプロンプトを表示します。

関連項目：証明書選択の設定

- [プロキシ設定（Proxy Settings）]：プロキシ サーバへのクライアント アクセスを制御するために AnyConnect プロファイルにポリシーを指定します。これは、プロキシ設定によってユーザが社内ネットワークの外からトンネルを確立できない場合に使用します。
  - [ネイティブ（Native）]：クライアントは、AnyConnect によって以前に設定されたプロキシ設定とブラウザに設定されたプロキシ設定の両方を使用します。グローバル ユーザ プリファレンスに設定されたプロキシ設定は、ブラウザのプロキシ設定に追加されます。
  - [プロキシを無視（IgnoreProxy）]：ユーザのコンピュータのブラウザのプロキシ設定を無視します。
  - [上書き（Override）]：パブリック プロキシ サーバのアドレスを手動で設定します。パブリック プロキシは、Linux でサポートされている唯一のプロキシです。Windows も、パブリック プロキシをサポートしています。[ユーザ制御可（User Controllable）] になるようにパブリック プロキシ アドレスを設定できます。

- [ローカルプロキシ接続を許可（Allow Local Proxy Connections）]：デフォルトでは、Windows ユーザは AnyConnect でローカル PC 上のトランスペアレントまたは非トランスペアレントのプロキシ サービスを介して VPN セッションを確立するようになっています。ローカル プロキシ接続のサポートを無効にする場合は、このパラメータをオフにします。トランスペアレント プロキシ サービスを提供する要素の例として、一部のワイヤレス データ カードによって提供されるアクセラレーション ソフトウェアや、一部のアンチウイルス ソフトウェアに備えられたネットワーク コンポーネントなどがあります。

- [最適なゲートウェイの選択を有効化（Enable Optimal Gateway Selection）]（OGS）、（IPv4 クライアントのみ）：AnyConnect では、ラウンド トリップ時間（RTT）に基づいて接続または再接続に最適なセキュア ゲートウェイが特定され、それが選択されます。これにより、ユーザが介入することなくインターネット トラフィックの遅延を最小限に抑えることができます。OGS はセキュリティ機能ではなく、セキュア ゲートウェイ クラスタ間またはクラスタ内部でのロード バランシングは実行されません。OGS のアクティブ化/非アクティブ化を制御し、エンドユーザがこの機能そのものを制御できるようにするかどうかを指定します。クライアント GUI の [接続（Connection）] タブにある [接続先（Connect To）] ドロップダウン リストには [自動選択（Automatic Selection）] が表示されます。
  - [一時停止時間しきい値（時間）（Suspension Time Threshold (hours)）]：新しいゲートウェイ選択の計算を呼び出す前に VPN を一時停止しておく必要がある最小時間を（時間単位で）入力します。次の設定可能パラメータ（パフォーマンス向上しきい値（Performance Improvement Threshold））と組み合わせてこの値を最適化することで、最適なゲートウェイの選択と、クレデンシャルの再入力を強制する回数の削減の間の適切なバランスを見つけることができます。
  - [パフォーマンス向上しきい値（%）（Performance Improvement Threshold (%)）]：システムの再開後にクライアントが別のセキュア ゲートウェイに再接続する際の基準となるパフォーマンス向上率。特定のネットワークに対してこれらの値を調整すれば、最

適なゲートウェイを選択することと、クレデンシャルを強制的に入力させる回数を減らすこととの間で適切なバランスを取ることができます。デフォルトは 20% です。

OGS が有効な場合は、この機能の設定をユーザが行えるようにすることも推奨します。

OGS には次の制約事項があります。

- Always-On を設定した状態では動作できません
- 自動プロキシ検出を設定した状態では動作できません。
- プロキシ自動設定（PAC）ファイルを設定した状態では動作できません。
- AAA が使用されている場合は、別のセキュア ゲートウェイへの遷移時にユーザがそれぞれのクレデンシャルを再入力しなければならないことがあります。この問題は、証明書を使用すると解消されます。

- [自動 VPN ポリシー（Automatic VPN Policy）]（Windows および macOS のみ）：Trusted Network Detection を有効にして、AnyConnect が信頼ネットワーク ポリシーと非信頼ネットワーク ポリシーに従って VPN 接続をいつ開始または停止するかを自動的に管理できるようにします。無効の場合、VPN 接続の開始および停止は手動でのみ行うことができます。[自動 VPN ポリシー（Automatic VPN Policy）] を設定しても、ユーザは VPN 接続を手動で制御できます。
  - [信頼されたネットワーク ポリシー（Trusted Network Policy）]：ユーザが社内ネットワーク（信頼ネットワーク）に存在する場合に AnyConnect が VPN 接続で自動的に実行するアクション。
    - [接続解除（Disconnect）]（デフォルト）：信頼ネットワークが検出されると VPN 接続が解除されます。
    - [接続（Connect）]：信頼ネットワークが検出されると VPN 接続が開始されます。
    - [何もしない（Do Nothing）]：非信頼ネットワークでは動作はありません。[信頼されたネットワークポリシー（Trusted Network Policy）] と [信頼されていないネットワークポリシー（Untrusted Network Policy）] の両方を [何もしない（Do Nothing）] に設定すると、Trusted Network Detection は無効となります。
    - [一時停止（Pause）]：ユーザが信頼ネットワークの外で VPN セッションを確立した後に、信頼済みとして設定されたネットワークに入った場合、AnyConnect は VPN セッションを接続解除するのではなく、一時停止します。ユーザが再び信頼ネットワークの外に出ると、そのセッションは AnyConnect により再開されます。この機能を使用すると、信頼ネットワークの外へ移動した後に新しい VPN セッションを確立する必要がなくなるため、ユーザにとっては有用です。
  - [信頼されていないネットワークポリシー（Untrusted Network Policy）]：ユーザが社内ネットワークの外（非信頼ネットワーク）に存在する場合、AnyConnect により VPN 接続が自動的に開始されます。この機能を使用すると、ユーザが信頼ネットワークの

外にいるときに VPN 接続を開始することによって、セキュリティ意識を高めることができます。

- [接続（Connect）]（デフォルト）：非信頼ネットワークが検出されると、VPN接続が開始されます。
- [何もしない（Do Nothing）]：信頼ネットワークでは動作はありません。このオプションは、Always-On VPN を無効にします。[信頼されたネットワークポリシー（Trusted Network Policy）] と [信頼されていないネットワークポリシー（Untrusted Network Policy）] の両方を [何もしない（Do Nothing）] に設定すると、Trusted Network Detection は無効となります。

- [信頼された DNS ドメイン（Trusted DNS Domains）]：クライアントが信頼ネットワーク内に存在する場合にネットワーク インターフェイスに割り当てることができる DNS サフィックス（カンマ区切りの文字列）。*.cisco.com などがこれに該当します。DNS サフィックスでは、ワイルドカード（*）がサポートされます。
- [信頼された DNS サーバ（Trusted DNS Servers）]：クライアントが信頼ネットワーク内に存在する場合にネットワーク インターフェイスに割り当てることができる DNS サーバ アドレス（カンマ区切りの IP アドレス）。たとえば、192.168.1.2, 2001:DB8::1 です。IPv4 または IPv6 DNS サーバ アドレスでは、ワイルドカード（*）がサポートされています。
- **Trusted Servers @ https://<server>[:<port>]**：信頼できる URL として追加するホスト URL。信頼できる証明書を使用してアクセス可能なセキュア Web サーバが、信頼できるサーバとして見なされる必要があります。[追加（Add）]をクリックすると、URL が追加され、証明書ハッシュに事前にデータが取り込まれます。ハッシュが見つからない場合は、ユーザに対して証明書ハッシュを手動で入力して [設定（Set）] をクリックするように求めるエラー メッセージが表示されます。

（注） このパラメータを設定できるのは、信頼された DNS ドメインまたは信頼された DNS サーバを 1 つ以上を定義する場合だけです。信頼された DNS ドメインまたは信頼された DNS サーバが定義されていない場合、このフィールドは無効になります。

- [常時接続（Always On）]：対応している Windows または macOS オペレーティング システムのいずれかを実行しているコンピュータにユーザがログインした場合、AnyConnect が VPN へ自動的に接続するかどうかを判断します。コンピュータが信頼ネットワーク内に存在しない場合にはインターネット リソースへのアクセスを制限することによってセキュリティ上の脅威からコンピュータを保護するという企業ポリシーを適用できます。グループ ポリシーおよびダイナミック アクセス ポリシーに Always-On VPN パラメータを設定し、ポリシーの割り当てに使用される一致基準に基づいて例外を指定することにより、この設定を上書きすることもできます。AnyConnect ポリシーでは Always-On VPN が有効になっているが、ダイナミック アクセス ポリシーまたはグループ ポリシーでは無効になっている場合、各新規セッションの確立に関す

るダイナミック アクセス ポリシーまたはグループ ポリシーが基準と一致すれば、クライアントでは現在以降の VPN セッションに対して無効の設定が保持されます。有効にした後に、追加のパラメータを設定できます。

（注） AlwaysOn は、ユーザによる設定なしで接続が確立し冗長性が動作するシナリオで使用します。そのため、この機能を使用しているときは、[プリファレンス,パート 1（Preferences, part 1）] で自動再接続を有効に設定する必要はありません。

関連項目：Always-Onを使用した VPN 接続の必要性

- [VPN の接続解除を許可（Allow VPN Disconnect）]：AnyConnect でAlways-On VPN セッション用の [接続解除（Disconnect）] ボタンが表示されるようにするかどうかを指定します。VPN セッションの中断後に現在の VPN セッションまたは再接続で問題が発生し、パフォーマンスが低下したなどの理由により、Always-On VPN セッションのユーザは [接続解除（Disconnect）] をクリックして代替のセキュア ゲートウェイを選択できます。

  [接続解除（Disconnect）]ボタンを使用すると、すべてのインターフェイスがロックされます。これにより、データの漏えいを防ぐことができる以外に、VPN セッションの確立には必要のないインターネットアクセスからコンピュータを保護することができます。上述した理由により、[接続解除（Disconnect）] ボタンを無効にすると、VPN アクセスが妨害または阻止されることがあります。

- [接続エラー ポリシー（Connect Failure Policy）]：AnyConnect が VPN セッションを確立できない場合（ASA が到達不能の場合など）に、コンピュータがインターネットにアクセスできるようにするかどうかを指定します。このパラメータは、[Always-On] および [VPN の接続解除を許可（Allow VPN Disconnect）] が有効の場合にだけ適用されます。[Always-On] を選択した場合、フェールオープン ポリシーはネットワーク接続を許可し、フェールクローズ ポリシーはネットワーク接続を無効にします。

  - [クローズド（Closed）]：VPN が到達不能の場合にネットワーク アクセスを制限します。この設定の目的は、エンドポイントを保護するプライベート ネットワーク内のリソースが使用できない場合に、企業の資産をネットワークに対する脅威から保護することにあります。

  - [オープン（Open）]：VPN が到達不能の場合でもネットワーク アクセスを許可します。

注意 AnyConnect が VPN セッションの確立に失敗した場合は、接続障害クローズド ポリシーによりネットワーク アクセスは制限されます。このポリシーは、主にネットワークに常時アクセス可能なことよりも、セキュリティが持続することを重視する非常にセキュリティの高い組織向きです。このポリシーでは、スプリット トンネリングによって許可され、ACL によって制限されたすべてのプリンタやテザード デバイスなどのローカル リソース以外のネットワーク アクセスを防止します。ユーザが VPN を越えてインターネットにアクセスする必要がある場合に、セキュア ゲートウェイを利用できないときには、このポリシーを適用すると生産性が低下する可能性があります。AnyConnectは、ほとんどのキャプティブ ポータルを検出します。キャプティブ ポータルを検出できない場合、接続障害クローズドポリシーによりすべてのネットワーク接続が制限されます。

クローズド接続ポリシーの展開は、段階的に行うことを強く推奨します。たとえば、最初に接続障害オープンポリシーを使用して Always-On VPN を展開し、ユーザを通じて AnyConnect がシームレスに接続できない頻度を調査します。さらに、新機能に関心を持つユーザを対象に、小規模な接続障害クローズドポリシーを試験的に展開しそのフィードバックを依頼します。引き続きフィードバックを依頼しながら試験的なプログラムを徐々に拡大したうえで、全面的な展開を検討します。接続障害クローズドポリシーを展開する場合は必ず、VPNユーザに対して接続障害クローズドポリシーのメリットだけでなく、ネットワークアクセスの制限についても周知してください。

関連項目：キャプティブ ポータルについて

[接続エラー ポリシー（Connect Failure Policy）] が [クローズド（Closed）] である場合、次の設定を行うことができます。

- [キャプティブポータルの修復を許可（Allow Captive Portal Remediation）]：クライアントによりキャプティブ ポータル（ホットスポット）が検出された場合、クローズ接続障害ポリシーにより適用されるネットワーク アクセスの制限が AnyConnect により解除されます。ホテルや空港では、ユーザがブラウザを開いてインターネットアクセスの許可に必要な条件を満たすことができるようにするため、キャプティブ ポータルを使用するのが一般的です。デフォルトの場合、このパラメータはオフになっており、セキュリティは最高度に設定されます。ただし、クライアントから VPN へ接続する必要があるにもかかわらず、キャプティブ ポータルによりそれが制限されている場合は、このパラメータをオンにする必要があります。
- [修復タイムアウト（Remediation Timeout）]：AnyConnect によりネットワーク アクセスの制限が解除されるまでの時間（分）。このパラメータは、[キャ

プティブポータルの修復を許可（Allow Captive Portal Remediation）]パラメータがオンになっており、かつクライアントによりキャプティブポータルが検出された場合に適用されます。キャプティブポータルの通常の要求を満たすことができるだけの十分な時間を指定します（5 分など）。

- [最新の VPN ローカル リソース ルールを適用（Apply Last VPN Local Resource Rules）]：VPN が到達不能の場合、クライアントでは ASA から受信した最後のクライアント ファイアウォールが適用されます。この中には、ローカル LAN 上のリソースへのアクセスを許可する ACL が含まれている場合もあります。

関連項目：接続障害ポリシーの設定

- [手動でのホスト入力を許可する（Allow Manual Host Input）]：ユーザが、AnyConnect UI のドロップダウン ボックスにリストされていない VPN アドレスを入力できるようにします。このチェックボックスをオフにすると、VPN接続の選択項目は、ドロップダウンボックスに表示されているものに限定され、ユーザによる新しい VPN アドレスの入力が制限されます。
- [PPP 除外（PPP Exclusion）]：PPP 接続上の VPN トンネルの場合、除外ルートを決定するかどうかとその方法を指定します。クライアントでは、セキュア ゲートウェイより先を宛先としてトンネリングされたトラフィックから、このセキュア ゲートウェイを宛先とするトラフィックを除外できます。除外ルートは、セキュアでないルートとして AnyConnect GUI の [ルートの詳細（Route Details）] 画面に表示されます。この機能をユーザ設定可能にした場合、ユーザは PPP 除外設定の読み取りや変更を行うことができます。
  - [自動（Automatic）]：PPP 除外を有効にします。AnyConnect は、PPP サーバの IP アドレスを自動的に使用します。この値は、自動検出による IP アドレスの取得に失敗した場合にのみ変更するよう、ユーザに指示してください。
  - [無効（Disabled）]：PPP 除外は適用されません。
  - [上書き（Override）]：同様に PPP 除外を有効にします。自動検出による PPP サーバの IP アドレスの取得に失敗し、PPP 除外をユーザ制御可能として設定した場合に選択します。

  [PPP 除外（PPP Exclusion）] を有効にした場合は、次も設定します。
  - [PPP 除外サーバ IP（PPP Exclusion Server IP）]：PPP 除外に使用されるセキュリティ ゲートウェイの IP アドレス。
- [スクリプトの有効化（Enable Scripting）]：OnConnect スクリプトおよび OnDisconnect スクリプトがセキュリティ アプライアンスのフラッシュ メモリに存在する場合はそれらを起動します。
  - [次のイベント時にスクリプトを終了する（Terminate Script On Next Event）]：スクリプト処理可能な別のイベントへの遷移が発生した場合に、実行中のスクリプト プロセスを終了します。たとえば、VPN セッションが終了すると、AnyConnect では実行中

の OnConnect スクリプトが終了し、クライアントで新しい VPN セッションが開始すると、実行中の OnDisconnect スクリプトが終了します。Microsoft Windows 上のクライアントでは OnConnect スクリプトまたは OnDisconnect スクリプトによって起動した任意のスクリプト、およびその従属スクリプトもすべて終了します。macOS および Linux 上のクライアントでは、OnConnect スクリプトまたは OnDisconnect スクリプトのみ終了し、子スクリプトは終了しません。

- [Post SBL OnConnect スクリプトを有効にする（Enable Post SBL On Connect Script）]：SBL で VPN セッションが確立された場合に OnConnect スクリプトが（存在すれば）起動されるようにします（VPN エンドポイントで Microsoft Windows を実行している場合にのみサポート）。

- [ログオフ時に VPN を保持（Retain VPN On Logoff）]：ユーザが Windows または Mac OS からログオフした場合に、VPN セッションを維持するかどうかを指定します。
  - [ユーザの強制設定（User Enforcement）]：別のユーザがログインした場合に VPN セッションを終了するかどうかを指定します。このパラメータが適用されるのは、[ログオフ時に VPN を保持（Retain VPN On Logoff）] がオンになっており、かつ VPN セッションが確立されている間に元のユーザが Windows または Mac OS X からログオフした場合のみです。

- [認証タイムアウト値（Authentication Timeout Values）]：デフォルトでは、AnyConnect は接続試行を終了するまでに、セキュア ゲートウェイからの認証を最大 12 秒間待ちます。その時間が経過すると、認証がタイムアウトになったことを示すメッセージが表示されます。10 ～ 120 の範囲で秒数を入力します。

AnyConnect プロファイル エディタのバックアップ サーバ

ユーザが選択したサーバで障害が発生した場合にクライアントが使用するバックアップ サーバのリストを設定できます。ユーザが選択したサーバで障害が発生した場合、クライアントはリストの先頭にある最適なサーバのバックアップに接続しようとします。それが失敗した場合、クライアントは選択結果の順序に従って [最適なゲートウェイの選択（Optimal Gateway Selection）] リストの残りの各サーバを試します。

（注） ここで設定するバックアップ サーバは、AnyConnect プロファイル エディタのサーバ リストの追加/編集 （115 ページ）でバックアップ サーバが定義されていないときに**のみ**、試行されます。サーバのリストで設定されるサーバが優先され、ここにリストされているバックアップ サーバは上書きされます。

[ホスト アドレス（Host Address）]：バックアップ サーバ リストに表示する IP アドレスまたは完全修飾ドメイン名（FQDN）を指定します。

- [追加（Add）]：バックアップ サーバ リストにホスト アドレスを追加します。

- [上に移動（Move Up）]：選択したバックアップ サーバをリストの上方向に移動します。ユーザが選択したサーバで障害が発生した場合、クライアントではまずリストの先頭にあるバックアップサーバに対して接続が試行され、必要に応じてリストの下方向に移動します。
- [下に移動（Move Down）]：選択したバックアップ サーバをリストの下方向に移動します。
- [削除（Delete）]：サーバ リストからバックアップ サーバを削除します。

AnyConnect プロファイル エディタの証明書照合

このペインでは、クライアント証明書の自動選択の詳細設定に使用できるさまざまな属性の定義を有効にします。

証明書一致基準を指定しない場合、AnyConnect は、次の証明書照合ルールを適用します。

- キーの使用状況：Digital_Signature
- 拡張キーの使用状況：Client Auth

仕様に一致する任意の条件がプロファイルで作成される場合、プロファイルに明記されない限り、上記一致ルールのいずれも適用されません。

- [キーの使用状況（Key Usage）]：受け入れ可能なクライアント証明書を選択する場合は、次のような証明書キー属性を使用できます。
  - Decipher_Only：データを復号化します。他のビットは設定されません（Key_Agreement は除く）。
  - Encipher_Only：データを暗号化します。他のビットは設定されません（Key_Agreement は除く）。
  - CRL_Sign：CRL の CA 署名を確認します。
  - Key_Cert_Sign：証明書の CA 署名を確認します。
  - Key_Agreement：キー共有。
  - Data_Encipherment：Key_Encipherment 以外のデータを暗号化します。
  - Key_Encipherment：キーを暗号化します。
  - Non_Repudiation：一部のアクションを誤って拒否しないように、Key_Cert_sign および CRL_Sign 以外のデジタル署名を確認します。
  - Digital_Signature：Non_Repudiation、Key_Cert_Sign、および CRL_Sign 以外のデジタル署名を確認します。
- [拡張キーの使用状況（Extended Key Usage）]：次の拡張キーの使用状況設定を使用します。OID は丸カッコ内に記載してあります。

- ServerAuth（1.3.6.1.5.5.7.3.1）
- ClientAuth（1.3.6.1.5.5.7.3.2）
- CodeSign（1.3.6.1.5.5.7.3.3）
- EmailProtect（1.3.6.1.5.5.7.3.4）
- IPSecEndSystem（1.3.6.1.5.5.7.3.5）
- IPSecTunnel（1.3.6.1.5.5.7.3.6）
- IPSecUser（1.3.6.1.5.5.7.3.7）
- TimeStamp（1.3.6.1.5.5.7.3.8）
- OCSPSign（1.3.6.1.5.5.7.3.9）
- DVCS（1.3.6.1.5.5.7.3.10）
- IKE Intermediate

- [カスタム拡張照合キー（最大 10）（Custom Extended Match Key (Max 10)）]：カスタム拡張照合キー（もしあれば）を指定します（最大 10 個）。証明書は入力したすべての指定キーに一致する必要があります。OID 形式でキーを入力します（1.3.6.1.5.5.7.3.11 など）。

（注） カスタム拡張照合キーを 30 文字を超える OID サイズで作成すると、[OK] ボタンのクリック時に拒否されます。OID の最大文字数は、30 文字です。

- [拡張キーの使用状況が設定されている証明書のみを適合（Match only certificates with Extended key usage）]：以前の動作では、証明書識別名（DN）の照合ルールが設定されると、クライアントは特定の EKU OID が設定されている証明書と、EKU が設定されていないすべての証明書とを適合させていました。一貫性を保ちながら、より明確にするため、EKU が設定されていない証明書との適合を拒否できます。デフォルトでは、お客様が予想している従来の動作が保持されます。新しい動作を有効にし、適合を拒否するには、チェックボックスをオンにする必要があります。

- [識別名（最大 10）（Distinguished Name (Max 10)）]：受け入れ可能なクライアント証明書を選択する際に完全一致基準として使用する識別名（DN）を指定します。
  - [名前（Name）]：照合に使用する識別名（DN）。
    - CN：サブジェクトの一般名
    - C：サブジェクトの国
    - DC：ドメイン コンポーネント
    - DNQ：サブジェクトの DN 修飾子

- EA：サブジェクトの電子メール アドレス
- GENQ：サブジェクトの GEN 修飾子
- GN：サブジェクトの名
- I：サブジェクトのイニシャル
- L：サブジェクトの都市
- N：サブジェクトの非構造体名
- O：サブジェクトの会社
- OU：サブジェクトの部署
- SN：サブジェクトの姓
- SP：サブジェクトの州
- ST：サブジェクトの州
- T：サブジェクトの敬称
- ISSUER-CN：発行元の一般名
- ISSUER-DC：発行元のコンポーネント
- ISSUER-SN：発行元の姓
- ISSUER-GN：発行元の名
- ISSUER-N：発行元の非構造体名
- ISSUER-I：発行元のイニシャル
- ISSUER-GENQ：発行元の GEN 修飾子
- ISSUER-DNQ：発行元の DN 修飾子
- ISSUER-C：発行元の国
- ISSUER-L：発行元の都市
- ISSUER-SP：発行元の州
- ISSUER-ST：発行元の州
- ISSUER-O：発行元の会社
- ISSUER-OU：発行元の部署
- ISSUER-T：発行元の敬称
- ISSUER-EA：発行元の電子メール アドレス

- [パターン（Pattern）]：照合する文字列を指定します。 照合するパターンには、目的の文字列部分のみ含まれている必要があります。パターン照合構文や正規表現構文を入力する必要はありません。入力した場合、その構文は検索対象の文字列の一部と見なされます。

  abc.cisco.com という文字列を例とした場合、cisco.com で照合するためには、入力するパターンを cisco.com とする必要があります。

- [演算子（Operator）]：この DN で照合する場合に使用する演算子です。
  - [等しい（Equal）]：== と同等
  - [等しくない（Not Equal）]：!= と同等
- [ワイルドカード（Wildcard）]：[有効（Enabled）] を指定するとワイルドカード パターン照合が含まれます。ワイルドカードが有効であれば、パターンは文字列内のどの場所でも使用できます。
- [大文字と小文字を区別（Match Case）]：大文字と小文字を区別したパターン照合を有効にする場合はオンにします。

関連トピック

証明書照合の設定 （182 ページ）

AnyConnect プロファイル エディタの証明書の登録

証明書登録により、AnyConnect は Simple Certificate Enrollment Protocol（SCEP）を使用してクライアント認証のために証明書をプロビジョニングし、更新できます。

- [証明書失効しきい値（Certificate Expiration Threshold）]：AnyConnect が、証明書の有効期限の何日前にユーザに対して証明書の失効が近づいていることを警告する日数（RADIUS パスワード管理ではサポートされません）。デフォルトは 0（警告は表示しない）です。値の範囲は 0 ～ 180 日です。
- [証明書インポート ストア（Certificate Import Store）]：どの Windows 証明書ストアに登録証明書を保存するかを選択します。
- [証明書の内容（Certificate Contents）]：SCEP 登録要求に含める証明書の内容を指定します。
  - Name (CN)：証明書での一般名。
  - Department (OU)：証明書に指定されている部署名。
  - Company (O)：証明書に指定されている会社名。
  - State (ST)：証明書に指定されている州 ID。
  - State (SP)：別の州 ID。

- Country (C)：証明書に指定されている国 ID。
- Email (EA)：電子メール アドレス。次の例では、[Email (EA)] は %USER%@cisco.com です。%USER% は、ユーザの ASA ユーザ名ログイン クレデンシャルに対応します。
- Domain (DC)：ドメイン コンポーネント。次の例では、[Domain (DC)] は cisco.com に設定されています。
- SurName (SN)：姓または名。
- GivenName (GN)：通常は名。
- UnstructName (N)：定義されていない名前。
- Initials (I)：ユーザのイニシャル。
- Qualifier (GEN)：ユーザの世代修飾子。たとえば、「Jr.」や「III」です。
- Qualifier (DN)：完全 DN の修飾子。
- City (L)：都市 ID。
- Title (T)：個人の敬称。たとえば、Ms.、Mrs.、Mr. など。
- CA Domain：SCEP 登録に使用されます。通常は CA ドメイン。
- Key size：登録する証明書用に生成された RSA キーのサイズ。

- [証明書取得ボタンを表示（Display Get Certificate Button）]：次の条件下で AnyConnect GUI が [証明書を取得（Get Certificate）] ボタンを表示できるようにします。
  - 証明書は [証明書失効しきい値（Certificate Expiration Threshold）] で定義された期間内に期限が切れるよう設定されている（RADIUS ではサポートされません）。
  - 証明書の期限が切れています。
  - 証明書が存在しません。
  - 証明書を照合できません。

関連トピック

証明書登録の設定 （171 ページ）

AnyConnect プロファイル エディタの証明書ピン

前提条件

証明書のピン留めを開始する前のベストプラクティスについては、証明書のピン留めについて（193 ページ）を参照してください。

プリファレンスの有効化とグローバルおよびホストごとの証明書ピンの設定には、VPN プロファイル エディタを使用します。[グローバル ピン（Global Pins）] セクション内のプリファレ

ンスが有効になっている場合は、サーバ リスト内のホストごとの証明書のみピン留めできます。プリファレンスを有効にすると、クライアントが証明書ピン検証に使用するグローバル ピンのリストを設定できます。[サーバ リスト（Server List）] セクションでのホストごとのピンの追加は、グローバル ピンの追加と同様です。証明書チェーン内の任意の証明書をピン留めでき、証明書は、ピン留めのために必要な情報を計算するため、プロファイル エディタにインポートされます。

[ピンを追加（Add Pin）]：証明書のプロファイル エディタへのインポートおよびピン留めを手引きする証明書ピン留めウィザードが開始します。

ウィンドウの [証明書の詳細（Certificate Details）] 部分では、[件名（Subject）] 列および [発行元（Issuer）] 列を視覚的に確認することができます。

証明書ピン留めウィザード

ピン留めに必要な情報を指定するため、サーバ証明書チェーンからの任意の証明書をプロファイル エディタにインポートすることができます。プロファイル エディタは、次の 3 つの証明書インポート オプションをサポートしています。

- ローカルのファイルを参照：お使いのコンピュータにローカルに存在している証明書を選択します。
- URL からファイルをダウンロード：任意のファイル ホスティング サーバから証明書をダウンロードします。
- PEM 形式の情報をペースト：証明書の開始および終了ヘッダーを含む PEM 形式の情報を挿入します。

（注） インポートできるのは、データ形式が DER、PEM、および PKCS7 の証明書のみです。

AnyConnect プロファイル エディタのモバイル ポリシー

AnyConnect のバージョン 3.0 以降では、Windows Mobile デバイスをサポートしません。Windows Mobile デバイスに関する情報は、『*Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 2.5*』を参照してください。

AnyConnect プロファイル エディタのサーバ リスト

クライアント GUI に表示されるサーバ リストの設定を行うことができます。ユーザは、VPN 接続を確立する際、このリストでサーバを選択することができます。

[サーバ リスト（Server List）] テーブルの列は次のとおりです。

- [ホスト名（Hostname）]：ホスト、IP アドレス、または完全修飾ドメイン名（FQDN）を参照する際に使用するエイリアス。

- [ホスト アドレス（Host Address）]：サーバの IP アドレスまたは FQDN。
- [ユーザ グループ（User Group）]：[ホスト アドレス（Host Address）] と組み合わせて使用することによりグループ ベースの URL が構成されます。
- [自動 SCEP ホスト（Automatic SCEP Host）]：クライアント認証に使用する証明書のプロビジョニング用および更新用として指定された Simple Certificate Enrollment Protocol。
- [CA URL]：このサーバが認証局（CA）へ接続する際に使用する URL。
- [証明書ピン（Certificate Pins）]：ピン検証の際にクライアントによって使用されるホストごとのピン。AnyConnect プロファイル エディタの証明書ピン （113 ページ） を参照してください。

（注） クライアントは、ピン検証の際に、グローバル ピンおよび対応するホストごとのピンを使用します。ホストごとのピンの設定は、証明書ピン留めウィザードの使用によるグローバル ピンの設定と同様に行います。

[追加/編集（Add/Edit）]：上記のサーバのパラメータを指定できる [サーバ リスト エントリ（Server List Entry）] ダイアログを起動します。

[削除（Delete）]：サーバ リストからサーバを削除します。

[詳細（Details）]：サーバのバックアップ サーバまたは CA URL に関する詳細情報を表示します。

関連トピック

VPN 接続サーバの設定 （129 ページ）

AnyConnect プロファイル エディタのサーバ リストの追加/編集

- [ホスト表示名（Host Display Name）]：ホスト、IP アドレス、または完全修飾ドメイン名（FQDN）を参照する際に使用するエイリアスを入力します。
- [FQDN または IP アドレス（FQDN or IP Address）]：サーバの IP アドレスまたは FQDN を指定します。
  - [ホスト アドレス（Host Address）] フィールドに IP アドレスまたは FQDN を指定すると、[ホスト名（Host Name）] フィールドのエントリが AnyConnect Client トレイ フライアウト内の接続ドロップダウン リストに表示されるサーバのラベルになります。
  - [ホスト名（Hostname）] フィールドで FQDN のみを指定し、[ホスト アドレス（Host Address）] フィールドでは IP アドレスを指定しない場合、[ホスト名（Hostname）] フィールドの FQDN が DNS サーバによって解決されます。
  - IP アドレスを入力する場合、セキュア ゲートウェイのパブリック IPv4 アドレスまたはグローバル IPv6 アドレスを使用します。リンクローカル セキュア ゲートウェイ アドレスの使用はサポートしていません。

- [ユーザ グループ（User Group）]：ユーザ グループを指定します。

  このユーザ グループとホスト アドレスを組み合わせてグループ ベースの URL が構成されます。プライマリ プロトコルを IPsec として指定した場合、ユーザ グループは接続プロファイル（トンネル グループ）の正確な名前である必要があります。SSL の場合、ユーザ グループは接続プロファイルの group-url または group-alias です。

- [モバイル専用追加設定（Additional mobile-only settings）]：Apple iOS および Android モバイル デバイスを設定する場合に選択します。

- **バックアップ サーバ リスト**

  ユーザが選択したサーバで障害が発生した場合にクライアントが使用するバックアップ サーバのリストを設定することをお勧めします。サーバで障害が発生した場合、クライアントではまずリストの先頭にあるサーバに対して接続が試行され、必要に応じてリストの下方向に移動します。

  （注） 逆の面から述べれば、AnyConnect プロファイル エディタのバックアップ サーバ（108 ページ）で設定されるバックアップ サーバは、すべての接続エントリのグローバル項目です。バックアップ サーバの場所に配置したエントリは、ここで、個々のエントリ サーバ リスト エントリとして入力した内容によって上書きされます。この設定は優先され、推奨される方法です。

  - [ホスト アドレス（Host Address）]：バックアップ サーバ リストに表示する IP アドレスまたは FQDN を指定します。クライアントでは、ホストに接続できない場合には、バックアップ サーバへの接続が試行されます。
  - [追加（Add）]：バックアップ サーバ リストにホスト アドレスを追加します。
  - [上に移動（Move Up）]：選択したバックアップ サーバをリストの上方向に移動します。ユーザが選択したサーバで障害が発生した場合、クライアントではまずリストの先頭にあるバックアップ サーバに対して接続が試行され、必要に応じてリストの下方向に移動します。
  - [下に移動（Move Down）]：選択したバックアップ サーバをリストの下方向に移動します。
  - [削除（Delete）]：サーバ リストからバックアップ サーバを削除します。

- **ロード バランシング サーバ リスト**

  このサーバ リスト エントリのホストがセキュリティ アプライアンスのロード バランシング クラスタであり、かつAlways-On機能が有効になっている場合は、このリストでクラスタのバックアップ デバイスを指定します。指定しなかった場合、ロード バランシング クラスタ内にあるバックアップ デバイスへのアクセスはAlways-On機能によりブロックされます。

- [ホスト アドレス（Host Address）]：ロードバランシング クラスタにあるバックアップ デバイスの IP アドレスまたは FQDN を指定します。
- [追加（Add）]：ロード バランシング バックアップ サーバ リストにアドレスを追加します。
- [削除（Delete）]：ロード バランシング バックアップ サーバをリストから削除します。

- [プライマリ プロトコル（Primary Protocol）]：このサーバも接続するプロトコル（SSL または IKEv2 を使用した IPsec）を指定します。デフォルトは SSL です。
  - [標準認証のみ（IOS ゲートウェイ）（Standard Authentication Only (IOS Gateways)）]：プロトコルとして IPsec を選択した場合、このオプションを選択して、IOS サーバへの接続の認証方式を制限できます。

（注） このサーバが ASA である場合、認証方式を独自の AnyConnect EAP から標準ベースの方式に変更すると、ASA でセッション タイムアウト、アイドル タイムアウト、接続解除タイムアウト、スプリット トンネリング、スプリット DNS、MSIE プロキシ設定、およびその他の機能を設定できなくなります。

  - [IKE ネゴシエーション中の認証方式（Auth Method During IKE Negotiation）]：標準ベースの認証方式の 1 つを選択します。
    - [IKE ID（IKE Identity）]：標準ベースの EAP 認証方式を選択した場合、このフィールドにグループまたはドメインをクライアント アイデンティティとして入力できます。クライアントは、文字列を ID_GROUP タイプ IDi ペイロードとして送信します。デフォルトでは、文字列は *$AnyConnectClient$* です。

- [CA URL]：SCEP CA サーバの URL を指定します。FQDN または IP アドレスを入力します。たとえば、http://ca01.cisco.com などです。
- [証明書ピン（Certificate Pins）]：ピン検証の際にクライアントによって使用されるホストごとのピン。AnyConnect プロファイル エディタの証明書ピン（113 ページ）を参照してください。
- [チャレンジ PW のプロンプト（Prompt For Challenge PW）]：有効にすると、証明書をユーザが手動で要求できるようになります。 ユーザが [証明書を取得（Get Certificate）] をクリックすると、クライアントではユーザに対してユーザ名および 1 回限定利用のパスワードに関するプロンプトが表示されます。
- [CA サムプリント（CA Thumbprint）]：CA の証明書サムプリント。SHA1 ハッシュまたは MD5 ハッシュを使用します。

（注） CA URL およびサムプリントを用意することができるのは CA サーバ管理者です。サムプリントは、発行元の証明書の「fingerprint」属性フィールドや「thumbprint」属性フィールドではなく、サーバから直接取得する必要があります。

関連トピック

VPN 接続サーバの設定 （129 ページ）

AnyConnect プロファイル エディタのモバイル設定

Apple iOS/Android の設定

- [証明書認証（Certificate Authentication）]：接続エントリに関連付けられた証明書認証ポリシー属性は、証明書がこの接続にどのように処理されるかを指定します。有効な値は次のとおりです。
  - [自動（Automatic）]：AnyConnect は、接続がいつなされるかを認証するクライアント証明書を自動で選択します。この場合、インストールされているすべての証明書が確認されて期限切れの証明書が無視され、VPN クライアント プロファイルに定義された基準に一致する証明書が適用されます。次に、基準に一致する証明書を使用して認証されます。これは、デバイス ユーザが VPN 接続の確立を試行するたびに実行されます。
  - [手動（Manual）]：AnyConnect は、プロファイルがダウンロードされ、次のいずれかを行うときに、Android デバイスの AnyConnect 証明書ストアで証明書を検索します。
    - AnyConnect は、VPN クライアント プロファイルで定められる基準に一致している証明書に基づく証明書を見つけた場合、証明書を接続エントリに割り当て、接続が確立されたときにその証明書を使用します。
    - 一致する証明書が見つからない場合、証明書認証ポリシーが [自動（Automatic）] に設定されます。
    - 割り当てられた証明書が、何らかの理由で AnyConnect 証明書ストアから削除された場合、AnyConnect は [自動（Automatic）] に証明書認証ポリシーをリセットします。
  - [無効（Disabled）]：クライアント証明書は認証に使用されません。
- [プロファイルがインポートされたときにサーバ リスト エントリをアクティブ化（Make this Server List Entry active when profile is imported）]：VPN 接続がデバイスにダウンロードされたら、サーバ リスト エントリをデフォルトとして定義します。この宛先を設定できるのは、1 つのサーバ リスト エントリのみです。デフォルトでは、無効に設定されています。

Apple iOS のみの設定

- [3G/WiFi ネットワーク間のローミング時に再接続（Reconnect when roaming between 3G/Wifi networks）]：有効（デフォルト）の場合、AnyConnect は、接続が解除された後やデバイスが起動した後、もしくは接続種別（EDGE（2G）、1xRTT（2G）、3G または Wi-Fi など）が変更になった後で、再接続にかかる時間を制限しません。この機能は、ネットワーク全体とのセキュアな接続を維持することで、シームレスなモビリティを提供します。企業への接続が必要で、かつバッテリ寿命の消費が多いアプリケーションには有用です。

  [ネットワーク ローミング（Network Roaming）] が無効で、AnyConnect の接続が切断された場合、必要に応じて最大 20 秒まで再接続を試みます。接続できない場合は、デバイス ユーザまたはアプリケーションは、必要な場合は新しい VPN 接続を開始する必要があります。

  （注） ネットワーク ローミングは、データ ローミングや複数のモバイル サービス プロバイダーの使用には影響しません。

- [Connect on Demand（証明書の認証が必要）（Connect on Demand (requires certificate authorization)）]：このフィールドでは、Apple iOS で提供される Connect on Demand 機能を設定できます。その他のアプリケーションが、ドメイン ネーム システム（DNS）を使用して解決されるネットワーク接続を開始したときに、毎回チェックされるルールのリストを作成できます。

  [Connect on Demand] は、[証明書認証（Certificate Authentication）] フィールドが [手動（Manual）] または [自動（Automatic）] に設定されている場合にのみ使用できるオプションです。[証明書認証（Certificate Authentication）] フィールドが [無効（Disabled）] に設定されている場合は、このチェックボックスはグレー表示されます。[ドメインまたはホストと一致（Match Domain or Host）] フィールドおよび [オンデマンドアクション（On Demand Action）] フィールドで定義される Connect on Demand ルールは、チェックボックスがグレー表示されている場合でも、設定および保存できます。

- [ドメインまたはホストと一致（Match Domain or Host）]：ユーザが Connect on Demand ルールを作成するホスト名（host.example.com）、ドメイン名（.example.com）、またはドメインの一部（.internal.example.com）を入力します。このフィールドには、IP アドレス（10.125.84.1）を入力しないでください。

- [オンデマンドアクション（On Demand Action）]：デバイス ユーザが前の手順で定義されたドメインまたはホストに接続しようとしたときに実行するアクションを次の中から 1 つ指定します。

  - [接続しない（Never Connect）]：このリストのルールに一致しても、iOS は絶対に VPN 接続を開始しません。このリストのルールは他のどのリストよりも優先されます

（注） Connect On Demand が有効の場合、アプリケーションは自動的にこのリストにサーバアドレスを追加します。これにより、Web ブラウザを使用してサーバのクライアントレス ポータルへのアクセスを試行する場合は、VPN 接続が自動的に確立されなくなります。この動作が望ましくない場合にはこのルールを削除します。

- [必要に応じて接続（Connect if Needed）]：このリストのルールに一致したときに、システムが DNS を使用してアドレスを解決できなかった場合に限り、iOS は VPN 接続を開始します。
- [常に接続（Always Connect）]：常時接続動作は、リリースに依存します。
  - Apple iOS 6 では、iOS はこのリスト ルールが一致したときに常に VPN 接続を開始します。
  - iOS 7.x では、常時接続はサポートされません。このリストのルールが一致しても、[必要に応じて接続（Connect if Needed）] のルールとして動作します。
  - 以降のリリースでは、常時接続は使用されません。設定されたルールは [必要に応じて接続（Connect if Needed）] リストに移動され、それに合わせて動作します。
- [追加または削除（Add or Delete）]：[ドメインまたはホストと一致（Match Domain or Host）] フィールドおよび [オンデマンドアクション（On Demand Action）] フィールドに指定されたルールをルール テーブルに追加するか、または選択したルールをルール テーブルから削除します。

AnyConnect ローカル ポリシー

AnyConnectLocalPolicy.xml は、セキュリティ設定を含む、クライアント上の XML ファイルです。このファイルは、ASA によって展開されません。手動でインストールするか、社内のソフトウェア展開システムを使用してユーザ コンピュータに展開する必要があります。ユーザのシステムで既存のローカル ポリシー ファイルに変更を加えた場合は、そのシステムをリブートする必要があります。

ローカル ポリシー パラメータと値

次のパラメータは、VPN ローカル ポリシー エディタおよび `AnyConnectLocalPolicy.xml` ファイル内の要素です。XML 要素は、山カッコで囲んで表示しています。

（注） ファイルを手動で編集し、ポリシーパラメータを省略した場合、この機能にはデフォルトの動作が適用されます。

- <acversion>

  このファイルのすべてのパラメータを解釈できるAnyConnectクライアントの最小バージョンを指定します。このバージョンよりも古いバージョンの AnyConnect を実行しているクライアントがファイルを読み込むと、イベント ログに警告が記録されます。

  形式は acversion="<version number>" です。

- [FIPS モード（FIPS Mode）] <FipsMode>

  クライアントの FIPS モードを有効にします。この設定は、FIPS 標準で承認されているアルゴリズムおよびプロトコルだけを使用するようにクライアントに強制します。

- [ダウンローダのバイパス（Bypass Downloader）] <BypassDownloader>

  オンにすると、ダイナミック コンテンツのローカル バージョンの存在を検出し、アップデートする VPNDownloader.exe モジュールの起動を無効にします。クライアントは、変換、カスタマイズ、オプション モジュール、コア ソフトウェア更新など、ASA のダイナミック コンテンツをチェックしません。

  [ダウンローダのバイパス（Bypass Downloader）] をオンにすると、ASA へのクライアント接続時に、次の 2 つの事態のいずれかが発生します。

  - ASA 上の VPN クライアント プロファイルがクライアント上のものと異なる場合、クライアントは接続の試行を中断します。
  - ASA に VPN クライアント プロファイルが存在しない場合でもクライアントは VPN 接続を行いますが、クライアントにハードコードされた VPN クライアント プロファイル設定を使用します。

    （注） ASA で VPN クライアント プロファイルを設定する場合は、BypassDownloader を true に設定した ASA に接続する前に、クライアントプロファイルをクライアントにインストールしておく必要があります。プロファイルには管理者が定義したポリシーを含めることができるため、BypassDownloader 設定 true は、ASA を使用してクライアントプロファイルを集中管理しない場合に限りお勧めします。

- [CLRチェックの有効化（Enable CRL Check）] <EnableCRLCheck>

  この機能は *Windows* デスクトップでのみ実装されます。SSL 接続と IPsec VPN 接続の両方で、証明書失効リスト（CRL）チェックを実行するオプションがあります。この設定を有効にすると、AnyConnect はチェーン内のすべての証明書を対象とした最新の CRL を取得します。AnyConnect は次に、当該証明書がこれらの信頼できなくなった失効証明書に含

まれているかどうかを確認します。認証局（CA）によって失効された証明書であることが判明すると、AnyConnect は接続しません。

CRL チェックは、デフォルトでは無効です。AnyConnect が CRL チェックを実行するのは、[CLRチェックの有効化（Enable CRL Check）] がオンである場合（有効な場合）だけであるため、エンド ユーザに対し次のような状況が発生することがあります。

- CRL によって証明書が失効した場合、AnyConnect ローカル ポリシー ファイルで [厳格な証明書トラスト（Strict Certificate Trust）] が無効になっている場合でも、セキュア ゲートウェイへの接続は無条件で失敗します。
- 到達できない CRL 配布ポイントなどが原因で CRL を取得できない場合、AnyConnect ローカル ポリシー ファイルで [厳格な証明書トラスト（Strict Certificate Trust）] が有効になっていると、セキュア ゲートウェイへの接続は無条件で失敗します。[厳格な証明書トラスト（Strict Certificate Trust）] が無効な場合は、ユーザに対しエラーを無視するように求められることがあります。

（注） AnyConnect は、[常時接続（Always On）] が有効な場合は CRL チェックを実行できません。CRL配布ポイントがパブリックに到達不能な場合、AnyConnectでサービスの中断が発生することがあります。

- [Web起動の制限（Restrict Web Launch）] <RestrictWebLaunch>

  ユーザは、FIPS 準拠のブラウザを使用して、WebLaunch を開始できません。これを行うためには、AnyConnect トンネルを開始するために使用されるセキュリティ Cookie をクライアントが取得できないようにします。クライアントからユーザに情報メッセージが表示されます。

- [厳格な証明書トラスト（Strict Certificate Trust）] <StrictCertificateTrust>

  選択すると、リモート セキュリティ ゲートウェイを認証するときに、AnyConnect は確認できない証明書を許可しません。ユーザにこれらの証明書を受け入れるように求める代わりに、クライアントは自己署名証明書を使用したセキュリティ ゲートウェイの接続に失敗し、「Local policy prohibits the acceptance of untrusted server certificates. 接続を確立できません。.オフにすると、クライアントはユーザに証明書を受け入れるように求めます。これはデフォルトの動作です。

  以下の理由があるため、AnyConnect クライアントに対する厳格な証明書トラストを有効にすることを、強くお勧めします。

  - 明確な悪意を持った攻撃が増えているため、ローカルポリシーで厳格な証明書トラストを有効にすると、パブリック アクセス ネットワークなどの非信頼ネットワークからユーザが接続している場合に「中間者」攻撃を防ぐために役立ちます。
  - 完全に検証可能で信頼できる証明書を使用する場合でも、AnyConnect クライアントは、デフォルトでは、未検証の証明書の受け入れをエンドユーザに許可します。エンドユーザが中間者攻撃の対象になった場合は、悪意のある証明書を受け入れるようエ

ンドユーザに求めます。エンドユーザによるこの判断を回避するには、厳格な証明書トラストを有効にします。

- [プリファレンス キャッシングの制限（Restrict Preference Caching）] <RestrictPreferenceCaching>

  AnyConnect は機密情報をディスクにキャッシュしないように設計されています。このパラメータを有効にすると、AnyConnect プリファレンスに保存されているすべての種類のユーザ情報に、このポリシーが拡張されます。

  - [クレデンシャル（Credentials）]：ユーザ名および第2ユーザ名はキャッシュされません。
  - [サムプリント（Thumbprints）]：クライアントおよびサーバ証明書のサムプリントはキャッシュされません。
  - [クレデンシャルとサムプリント（CredentialsAndThumbprints）]：証明書のサムプリントおよびユーザ名はキャッシュされません。
  - [すべて（All）]：自動プリファレンスはいずれもキャッシュされません。
  - [false]：すべてのプリファレンスがディスクに書き込まれます（デフォルト）。

- [PEM ファイル証明書ストアの除外（Exclude Pem File Cert Store）]（Linux および macOS）<ExcludePemFileCertStore>

  サーバ証明書の検証とクライアント証明書の検索にクライアントが PEM ファイル証明書ストアを使用できないようにします。

  FIPS 対応の OpenSSL を使用するストアには、クライアント証明書認証用の証明書の取得場所に関する情報があります。PEM ファイル証明書ストアを許可することで、リモートユーザは FIPS 準拠の証明書ストアを使用することになります。

- [Mac のネイティブ証明書ストアの除外（Exclude Mac Native Cert Store）]（macOS のみ）<ExcludeMacNativeCertStore>

  サーバ証明書の検証とクライアント証明書の検索にクライアントが Mac ネイティブ（キーチェーン）証明書ストアを使用できないようにします。

- [Firefox の NSS 証明書ストアの除外（Exclude Firefox NSS Cert Store）]（Linux および macOS）<ExcludeFirefoxNSSCertStore>

  サーバ証明書の検証とクライアント証明書の検索にクライアントが Firefox NSS 証明書ストアを使用できないようにします。

  ストアには、クライアント証明書認証用の証明書の取得場所に関する情報があります。

- [更新ポリシー（Update Policy）] <UpdatePolicy>

  クライアントがどのヘッドエンドからソフトウェア更新またはプロファイル更新を取得できるかを制御します。

  - **[任意のサーバからのソフトウェア更新を許可**（Allow Software Updates From Any Server）] <AllowSoftwareUpdatesFromAnyServer>

不正なサーバ（[サーバ名（Server Name）] リストに記載されていないもの）からの VPN コア モジュールおよびその他のオプション モジュールのソフトウェア更新を許可または禁止します。

- [任意のサーバからの VPN プロファイル更新を許可（Allow VPN Profile Updates From AnyServer）]<AllowVPNProfileUpdatesFromAnyServer>

  不正なサーバ（[サーバ名（Server Name）] リストに記載されていないもの）からの VPN プロファイル更新を許可または禁止します。

- [**任意のサーバからのサービス プロファイル更新を許可**（Allow Service Profile Updates From AnyServer）] <AllowServiceProfileUpdatesFromAnyServer>

  不正なサーバ（[サーバ名（Server Name）] リストに記載されていないもの）からのその他のサービス モジュール プロファイル更新を許可または禁止します。

- [任意のサーバからの ISE ポスチャ プロファイル更新を許可（Allow ISE Posture Profile Updates From Any Server）] <AllowISEProfileUpdatesFromAnyServer>

  不正なサーバ（[サーバ名（Server Name）] リストに記載されていないもの）からの ISE ポスチャ プロファイル更新を許可または禁止します。

- [任意のサーバからのコンプライアンス モジュール更新を許可（Allow Compliance Module Updates From Any Server）] <AllowComplianceModuleUpdatesFromAnyServer>

  不正なサーバ（[サーバ名（Server Name）] リストに記載されていないもの）からのコンプライアンス モジュール更新を許可または禁止します。

- [サーバ名（Server Name）] <ServerName>

  このリストに認証されたサーバを指定します。これらのヘッドエンドには、VPN接続時にすべてのAnyConnectソフトウェアとプロファイルの完全な更新が許可されます。ServerNameには、FQDN、IPアドレス、ドメイン名、またはワイルドカードを含むドメイン名を使用できます。

ローカル ポリシー パラメータの手動変更

手順

ステップ 1 クライアント インストールから、AnyConnect ローカル ポリシー ファイル（AnyConnectLocalPolicy.xml）のコピーを取得します。

表 *7:* オペレーティング システムと *AnyConnect* ローカル ポリシー ファイルのインストール パス

オペレーティング システム	インストール パス
Windows	C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client

オペレーティング システム	インストール パス
Linux	/opt/cisco/anyconnect
macOS	/opt/cisco/anyconnect

ステップ 2 パラメータ設定を編集します。AnyConnectLocalPolicy ファイルを手動で編集するか、AnyConnect プロファイル エディタのインストーラとともに配布される VPN ローカル ポリシー エディタを使用できます。

ステップ 3 ファイルを `AnyConnectLocalPolicy.xml` として保存し、社内のソフトウェア展開システムを使用してこのファイルをリモート コンピュータに展開します。

ステップ 4 ローカル ポリシー ファイルへの変更が反映されるように、リモート コンピュータをリブートします。

MST ファイルでのローカル ポリシー パラメータの有効化

設定できる説明および値については、「ローカル ポリシー パラメータと値」を参照してください。

ローカル ポリシー パラメータを変更するには、MST ファイルを作成します。MST パラメータ名は、AnyConnect ローカル ポリシー ファイル（AnyConnectLocalPolicy.xml）の次のパラメータに対応しています。

- LOCAL_POLICY_BYPASS_DOWNLOADER
- LOCAL_POLICY_FIPS_MODE
- LOCAL_POLICY_RESTRICT_PREFERENCE_CACHING
- LOCAL_POLICY_RESTRICT_TUNNEL_PROTOCOLS
- LOCAL_POLICY_RESTRICT_WEB_LAUNCH
- LOCAL_POLICY_STRICT_CERTIFICATE_TRUST

（注） AnyConnect インストールは、ユーザ コンピュータ上にある既存のローカル ポリシー ファイルを自動的には上書きしません。クライアント インストーラが新しいポリシー ファイルを作成できるようにするには、その前にユーザ コンピュータ上の既存のポリシー ファイルを削除しておく必要があります。

（注） ローカル ポリシー ファイルへのすべての変更には、システムのリブートが必要になります。

Enable FIPS ツールによるローカル ポリシー パラメータの有効化

すべてのオペレーティング システムで、シスコの Enable FIPS ツールを使用して、FIPS が有効な AnyConnect ローカル ポリシー ファイルを作成できます。Enable FIPS ツールはコマンド ライン ツールで、実行するには、Windows では管理者権限が必要です。Linux および macOS では、root ユーザとして実行する必要があります。

Enable FIPS ツールのダウンロード元の詳細については、FIPS クライアント用に受け取ったライセンシング情報を参照してください。

Enable FIPS ツールを実行するには、コンピュータのコマンド ラインから EnableFIPS <arguments> コマンドを入力します。Enable FIPS ツールを使用するときは、次のことに注意してください。

- 引数を何も指定しなかった場合、ツールによって FIPS が有効にされ、vpnagent サービス（Windows）または vpnagent デーモン（macOS および Linux）がリスタートされます。
- 複数の引数はスペースで区切ります。

Windows コンピュータ上で実行する Enable FIPS ツールのコマンド例を次に示します。

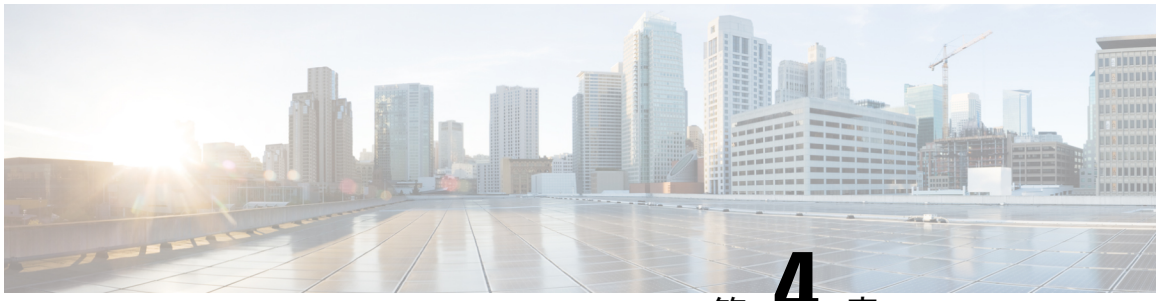
```
EnableFIPS rwl=false sct=true bd=true fm=false
```

Linux または macOS コンピュータ上で実行するコマンド例を次に示します。

```
./EnableFIPS rwl=false sct=true bd=true fm=false
```

次の表に、Enable FIPS ツールで設定できるポリシー設定の例を示します。引数は、AnyConnect ローカル ポリシー ファイルのパラメータに対応します。

ポリシー設定	引数および構文
FIPS モード	fm=[true | false]
ダウンローダのバイパス	bd=[true | false]
WebLaunch の制限	rwl=[true | false]
厳格な証明書トラスト	sct=[true | false]
プリファレンス キャッシングの制限	rpc=[Credentials | Thumbprints | CredentialsAndThumbprints | All | false]
FireFox の NSS 証明書ストアの除外（Linux および macOS）	efn=[true | false]
PEM ファイル証明書ストアの除外 （Linux および macOS）	epf=[true | false]
Mac のネイティブ証明書ストアの除外 （macOS のみ）	emn=[true | false]



第 4 章

VPN アクセスの設定

- VPN への接続と接続解除 （127 ページ）
- VPN トラフィックの選択および除外 （156 ページ）
- VPN 認証の管理 （166 ページ）

VPN への接続と接続解除

AnyConnect VPN 接続オプション

AnyConnect クライアントには、自動的に VPN セッションを接続、再接続、または切断するための多数のオプションが用意されています。これらのオプションは、ユーザが VPN に接続するために便利な方法を提供し、同時にネットワーク セキュリティの要件をサポートします。

AnyConnect 接続の開始とリスタート

VPN 接続サーバの設定を行い、ユーザが手動で接続するセキュア ゲートウェイの名前とアドレスを提供します。

便利な自動 VPN 接続を提供するための AnyConnect 機能を次から選択します。

- ログイン前の Windows VPN 接続の自動開始
- AnyConnect 起動時の VPN 接続の自動開始
- VPN 接続の自動リスタート

また、強力なネットワーク セキュリティを適用したり、ネットワーク アクセスを VPN のみに制限したりするために、次の自動 VPN ポリシー オプションの使用を検討してください。

- Trusted Network Detection について
- Always-Onを使用した VPN 接続の必要性
- キャプティブ ポータル ホットスポットの検出と修復の使用

AnyConnect 接続の再ネゴシエートと維持

アクティビティが発生していない場合でも、ASA がユーザに対して AnyConnect VPN 接続を維持する長さを制限できます。VPN セッションがアイドルになった場合、接続を終了するか、または接続を再ネゴシエートできます。

- キープアライブ：ASA はキープアライブ メッセージを定期的に送信します。これらのメッセージは、ASA によって無視されますが、クライアントと ASA の間の、デバイスを使用した接続の維持に役立ちます。

  ASDM または CLI でキープアライブを設定する手順については、『Cisco ASA Series VPN Configuration Guide』の「*Enable Keepalive*」の項を参照してください。

- デッド ピア検出：ASA および AnyConnect クライアントは、「R-U-There」メッセージを送信します。これらのメッセージは、IPsec のキープアライブ メッセージよりも少ない頻度で送信されます。ASA（ゲートウェイ）および AnyConnect クライアントの両方で DPD メッセージの送信を有効にして、タイムアウト間隔を設定できます。

  - クライアントが ASA の DPD メッセージに応答しない場合、ASA はもう 1 回試行してから、セッションを「再開待機」モードに移行します。このモードでは、ユーザはネットワークをローミングしたり、スリープ モードに移行してから後で接続を回復したりできます。アイドル タイムアウトが発生する前にユーザが再接続しなかった場合、ASA はトンネルを終了します。推奨されるゲートウェイ DPD 間隔は 300 秒です。

  - ASA がクライアントの DPD メッセージに応答しない場合、クライアントはもう 1 回試行してから、トンネルを終了します。推奨されるクライアント DPD 間隔は 30 秒です。

    ASDM 内で DPD を設定する手順については、適切なリリースの『Cisco ASA Series VPN Configuration Guide』の「*Configure Dead Peer Detection*」の項を参照してください。

- ベスト プラクティス：

  - クライアント DPD を 30 秒に設定します（[グループ ポリシー（Group Policy）] > [詳細（Advanced）] > [AnyConnect 接続（AnyConnect Client）] > [デッド ピア検出（Dead Peer Detection）]）。

  - サーバ DPD を 300 秒に設定します（[グループ ポリシー（Group Policy）] > [詳細（Advanced）] > [AnyConnect 接続（AnyConnect Client）] > [デッド ピア検出（Dead Peer Detection）]）。

  - SSL および IPsec の両方のキー再生成を 1 時間に設定します（[グループ ポリシー（Group Policy）] > [詳細（Advanced）] > [AnyConnect 接続（AnyConnect Client）] > [キー再作成（Key Regeneration）]）。

AnyConnect 接続の終了

AnyConnect 接続を終了するには、ユーザはセキュア ゲートウェイに対してエンドポイントを再認証し、新しい VPN 接続を作成する必要があります。

次の接続パラメータは、タイムアウトに基づいて、VPN セッションを終了します。

- 最大接続時間：ユーザの最大接続時間を分単位で設定します。ここで指定した時間が経過すると、システムは接続を終了します。また、無制限の接続時間（デフォルト）を許可することもできます。
- VPN アイドル タイムアウト：セッションが指定した時間非アクティブである場合は、ユーザのセッションを終了します。VPN アイドル タイムアウトを設定しない場合は、デフォルトのアイドル タイムアウトが使用されます。
- デフォルト アイドル タイムアウト：セッションが指定した時間非アクティブである場合は、ユーザのセッションを終了します。デフォルト値は 30 分（1800 秒）です。

これらのパラメータを設定するには、適切なリリースの『Cisco ASA Series VPN Configuration Guide』の「*Specify a VPN Session Idle Timeout for a Group Policy*」の項を参照してください。

VPN 接続サーバの設定

AnyConnect VPN サーバ リストは、VPN ユーザが接続するセキュア ゲートウェイを識別するホスト名とホストアドレスのペアで構成されます。ホスト名は、エイリアス、FQDN、または IP アドレスで指定できます。

サーバ リストに追加されたホストは、AnyConnect GUI の [接続先（Connect to）] ドロップダウン リストに表示されます。その後、ユーザはドロップダウン リストから選択して VPN 接続を開始できます。リストの最上位にあるホストはデフォルト サーバで、GUI のドロップダウン リストの先頭に表示されます。ユーザがリストから代替サーバを選択した場合、その選択されたサーバが新しいデフォルト サーバになります。

サーバ リストにサーバを追加すると、その詳細を表示し、サーバ エントリを編集または削除するようになります。サーバ リストにサーバを追加するには、次の手順を実行します。

手順

ステップ 1 VPN プロファイル エディタを開き、ナビゲーション ペインから [サーバ リスト（Server List）] を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 サーバのホスト名およびアドレスを設定します。

a) [ホスト表示名（Host Display Name）]、ホストの参照に使用されるエイリアス、FQDN、または IP アドレスを入力します。名前に「&」または「<」文字を使用しないでください。FQDN または IP アドレスを入力した場合、次の手順で [FQDN] または [IP アドレス（IP Address）] を入力する必要はありません。

IP アドレスを入力する場合、セキュア ゲートウェイのパブリック IPv4 アドレスまたはグローバル IPv6 アドレスを使用します。リンクローカル セキュア ゲートウェイ アドレスの使用はサポートしていません。

b) （任意）[ホスト表示名（Host Display Name）] に入力していない場合、ホストの [FQDN] または [IP アドレス（IP Address）] を入力します。
c) （任意）[ユーザ グループ（User Group）] を指定します。

AnyConnect は、ユーザ グループとともに FQDN または IP アドレスを使用してグループ URL を形成します。

ステップ 4 [バックアップ サーバ リスト（Backup Server List）] に、バックアップ サーバとしてフォールバックするサーバを入力します。名前に「&」または「<」文字を使用しないでください。

（注） 逆の面から述べれば、[サーバ（Server）] メニューの [バックアップ サーバ（Backup Server）] タブは、すべての接続エントリのグローバル項目です。バックアップ サーバの場所に配置したエントリは、ここで、個々のエントリ サーバ リスト エントリとして入力した内容によって上書きされます。この設定は優先され、推奨される方法です。

ステップ 5 （任意）[ロード バランシング サーバ リスト（Load Balancing Server List）] .に、ロード バランシング サーバ を追加します。名前に「&」または「<」文字を使用しないでください。

このサーバ リスト エントリのホストにセキュリティ アプライアンスのロード バランシング クラスタを指定し、かつ Always-On 機能が有効になっている場合は、このリストにクラスタのロード バランシング デバイスを追加します。指定しなかった場合、ロード バランシング クラスタ内にあるバックアップ デバイスへのアクセスは Always-On 機能によりブロックされます。

ステップ 6 クライアントがこの ASA に使用する [プライマリ プロトコル（Primary Protocol）] を指定します。

a) SSL（デフォルト）または IPSec を選択します。

IPsec を指定した場合、ユーザ グループは接続プロファイル（トンネル グループ）の正確な名前である必要があります。SSL の場合、ユーザ グループは接続プロファイルの group-url または group-alias です。

b) IPSec を指定した場合は、[標準認証のみ（Standard Authentication Only）] を選択してデフォルトの認証方式（独自の AnyConnect EAP）を無効にし、ドロップダウン リストからいずれかの方式を選択します。

（注） 認証方式を独自の AnyConnect EAP から標準ベースの方式に変更すると、ASA でセッション タイムアウト、アイドル タイムアウト、接続解除タイムアウト、スプリット トンネリング、スプリット DNS、MSIE プロキシ設定、およびその他の機能を設定できなくなります。

ステップ 7 （任意）このサーバ用の SCEP を設定します。

a) SCEP CA サーバの URL を指定します。FQDN または IP アドレスを入力します。たとえば、http://ca01.cisco.com などです。
b) [チャレンジ PW のプロンプト（Prompt For Challenge PW）] をオンにして、ユーザが証明書を手動で要求できるようにします。ユーザが [証明書を取得（Get Certificate）] をクリックすると、クライアントではユーザに対してユーザ名および 1 回限定利用のパスワードに関するプロンプトが表示されます。

c) CA の証明書サムプリントを入力します。SHA1 ハッシュまたは MD5 ハッシュを使用します。CA URL およびサムプリントを用意することができるのは CA サーバ管理者です。サムプリントは、発行した証明書の「fingerprint」属性フィールドや「thumbprint」属性フィールドではなく、サーバから直接取得する必要があります。

ステップ 8 [OK] をクリックします。

関連トピック

AnyConnect プロファイル エディタのサーバ リスト （114 ページ）
AnyConnect プロファイル エディタのサーバ リストの追加/編集 （115 ページ）

ログイン前の Windows VPN 接続の自動開始

Start Before Logon について

Start Before Logon（SBL）と呼ばれるこの機能によりユーザは、Windows へのログイン前に、企業インフラへの VPN 接続を確立できます。

SBL がインストールされ、有効になると、[ネットワーク接続（Network Connect）] ボタンは AnyConnect VPN および ネットワーク アクセス マネージャ UI を起動します。

SBL には、ネットワーク アクセス マネージャ タイルも含まれており、ユーザが設定したホーム ネットワーク プロファイルを使用した接続を可能にします。SBL モードで許可されるネットワーク プロファイルには、非 802.1X 認証モードを採用するすべてのメディア タイプ（オープン WEP、WPA/WPA2 パーソナル、および静的キー（WEP）ネットワークなど）が含まれます。

SBL は Windows システムのみで利用でき、Windows のバージョンによって異なるメカニズムを使用して実装されます。

- Windows では、Pre-Login Access Provider（PLAP）が AnyConnect SBL を実装するために使用されます。

  PLAP では、Ctrl キー、Alt キー、および Del キーを同時に押すとウィンドウが表示され、そこでシステムにログインするか、ウィンドウの右下隅にある [ネットワーク接続（Network Connect）] ボタンでネットワーク接続（PLAP コンポーネント）を起動するかを選択できます。

  PLAP は Windows の 32 ビット版と 64 ビット版をサポートします。

SBL を有効にする理由としては、次のものがあります。

- ユーザのコンピュータに Active Directory インフラストラクチャを導入済みである。
- ネットワークでマッピングされるドライブを使用し、Microsoft Active Directory インフラストラクチャの認証を必要とする。
- コンピュータのキャッシュにクレデンシャルを入れることができない（グループ ポリシーでキャッシュのクレデンシャル使用が許可されない場合）。このシナリオでは、コンピュー

タへのアクセスが許可される前にユーザのクレデンシャルが確認されるようにするため、ユーザは社内ネットワーク上のドメイン コントローラと通信できることが必要です。

- ネットワーク リソースから、またはネットワーク リソースへのアクセスを必要とする場所からログイン スクリプトを実行する必要がある。SBL を有効にすると、ユーザは、ローカル インフラストラクチャおよび通常はオフィスにいるときに実行されるログイン スクリプトにアクセスできます。これには、ドメイン ログイン スクリプト、グループ ポリシー オブジェクト、およびユーザがシステムにログインするときに通常実行されるその他の Active Directory 機能が含まれます。
- インフラストラクチャとの接続が必要な場合があるネットワーキング コンポーネント（MS NAP/CS NAC など）が存在する。

Start Before Logon の制限

- AnyConnect は、高速ユーザ切り替えとの互換性がありません。
- AnyConnect は、サードパーティの Start Before Logon アプリケーションでは起動できません。

Start Before Logon の設定

手順

ステップ 1 AnyConnect Start Before Logon モジュールのインストール。
ステップ 2 AnyConnect プロファイルでの SBL の有効化。

AnyConnect Start Before Logon モジュールのインストール

AnyConnect インストーラは、基盤となるオペレーティング システムを検出し、システム ディレクトリに AnyConnect SBL モジュールから適切な AnyConnect DLL を配置します。Windows 7 または Windows Server 2008 では、インストーラは、32 ビット版と 64 ビット版のどちらのオペレーティング システムが使用されているかを判別して、該当する PLAP コンポーネント（vpnplap.dll または vpnplap64.dll）をインストールします。

（注） VPNGINA または PLAP コンポーネントがインストールされたまま AnyConnect をアンインストールすると、VPNGINA または PLAP のコンポーネントは無効となり、リモート ユーザの画面に表示されなくなります。

SBL モジュールを事前展開するか、SBL モジュールをダウンロードするように ASA を設定することができます。AnyConnect を事前展開する場合は、Start Before Logon モジュールよりも先にコア クライアント ソフトウェアをインストールする必要があります。MSI ファイルを使

用して AnyConnect コアおよび Start Before Logon コンポーネントを事前展開する場合は、正しい順序で実行する必要があります。

手順

ステップ 1 ASDM で、**[設定（Configuration）]** > **[リモート アクセス VPN（Remote Access VPN）]** > **[ネットワーク（クライアント）アクセス（Network (Client) Access）]** > **[グループ ポリシー（Group Policies）]** に移動します。

ステップ 2 グループ ポリシーを選択し、新しいグループ ポリシーの **[編集（Edit）]** または **[追加（Add）]** をクリックします。

ステップ 3 左側のナビゲーション ペインで **[詳細（Advanced）]** > **[AnyConnect クライアント（AnyConnect Client）]** を選択します。

ステップ 4 [ダウンロードするオプションのクライアント モジュール（Optional Client Module for Download）] 設定の [継承（Inherit）] をオフにします。

ステップ 5 ドロップダウン リストから **AnyConnect SBL** モジュールを選択します。

AnyConnect プロファイルでの SBL の有効化

始める前に

- SBL は、呼び出されたときにネットワークに接続されている必要があります。場合によっては、ワイヤレス接続がワイヤレス インフラストラクチャに接続するユーザのクレデンシャルに依存するために、接続できないことがあります。このシナリオでは、ログインのクレデンシャル フェーズよりも SBL モードが優先されるため、接続できません。このような場合に SBL を機能させるには、ログインを通してクレデンシャルをキャッシュするようにワイヤレス接続を設定するか、その他のワイヤレス認証を設定する必要があります。
- ネットワーク アクセス マネージャがインストールされている場合、デバイス接続を展開して、適切な接続を確実に使用できるようにする必要があります。

手順

ステップ 1 VPN プロファイル エディタを開き、ナビゲーション ペインから [プリファレンス（Part 1）（Preferences (Part 1)）] を選択します。

ステップ 2 [ログイン前の起動の使用（Use Start Before Logon）] を選択します。

ステップ 3 （任意）リモート ユーザが SBL を制御できるようにする場合は、[ユーザ制御可（User Controllable）] をオンにします。

（注） SBL を有効にする場合は、その前にユーザがリモート コンピュータをリブートする必要があります。

Start Before Logon のトラブルシューティング

手順

ステップ 1 AnyConnect プロファイルが ASA にロードされており、展開できるようになっていることを確認します。

ステップ 2 以前のプロファイルを削除します（*.xml と指定してハード ドライブ上の格納場所を検索します）。

ステップ 3 Windows の [プログラムの追加と削除（Add/Remove Programs）] を使用して SBL コンポーネントをアンインストールします。コンピュータをリブートして、再テストします。

ステップ 4 イベント ビューアでユーザの AnyConnect ログをクリアし、再テストします。

ステップ 5 セキュリティ アプライアンスを再度参照して、AnyConnect を再インストールします。

ステップ 6 いったんリブートします。次回リブート時には、[ログイン前の起動（Start Before Logon）] プロンプトが表示されます。

ステップ 7 DART バンドルを収集し、AnyConnect 管理者に送付します。

ステップ 8 次のエラーが表示された場合は、ユーザの AnyConnect プロファイルを削除します。

```
Description: Unable to parse the profile C:\Documents and Settings\All Users\Application
 Data
\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\VABaseProfile.xml. Host data not
 available.
```

ステップ 9 .tmpl ファイルに戻って、コピーを .xml ファイルとして保存し、その XML ファイルをデフォルト プロファイルとして使用します。

AnyConnect 起動時の VPN 接続の自動開始

[起動時に自動接続（Auto Connect on Start）] とも呼ばれるこの機能は、AnyConnect が開始されると、VPN クライアント プロファイルで指定されたセキュア ゲートウェイへの VPN 接続を自動的に確立します。

[起動時に自動接続（Auto Connect on Start）] はデフォルトでは無効であり、ユーザはセキュア ゲートウェイを指定または選択する必要があります。

手順

ステップ 1 VPN プロファイル エディタを開き、ナビゲーション ペインから [プリファレンス（Part 1）（Preferences (Part 1)）] を選択します。

ステップ 2 [起動時に自動接続（Auto Connect on Start）] を選択します。

ステップ 3 （任意）[起動時に自動接続（Auto Connect on Start）] をユーザが制御できるようにするには、[ユーザ制御可（User Controllable）] を選択します。

Windows システムにおける Start Before Logon（PLAP）の設定

Start Before Logon（SBL）機能によって、ユーザが Windows にログインする前に VPN 接続が開始されます。これにより、ユーザは自分のコンピュータにログインする前に、企業のインフラストラクチャに接続されます。

SBL AnyConnect 機能は「Pre-Login Access Provider（PLAP）」と呼ばれます。これは、接続可能なクレデンシャルプロバイダーです。この機能を使用すると、プログラマチック ネットワークの管理者は、クレデンシャルの収集やネットワーク リソースへの接続など特定のタスクをログオン前に実行することができます。PLAP では、サポートされている Windows オペレーティング システムすべてに対して SBL 機能を提供します。PLAP は、vpnplap.dll を使用する 32 ビット版のオペレーティング システムと、vpnplap64.dll を使用する 64 ビット版のオペレーティング システムをサポートしています。PLAP 機能は、x86 および x64 をサポートしています。

PLAP のインストール

vpnplap.dll および vpnplap64.dll の両コンポーネントは、既存のインストール済み環境の一部になっているため、単一のアドオン SBL パッケージをセキュリティ アプライアンスにロードできます。ロードされると、該当するコンポーネントがターゲット プラットフォームにインストールされます。PLAP はオプションの機能です。インストーラ ソフトウェアは、基盤のオペレーティング システムを検出して該当する DLL をシステム ディレクトリに配置します。Windows 7 以降、または Windows Server 2008 では、インストーラは、32 ビット版と 64 ビット版のどちらのオペレーティング システムが使用されているかを判別して、該当する PLAP コンポーネントをインストールします。

（注） PLAP コンポーネントがインストールされたまま AnyConnect をアンインストールすると、PLAP のコンポーネントは無効となり、リモート ユーザの画面に表示されなくなります。

PLAP は、インストールされた後でも、SBL がアクティブ化されるようにユーザ プロファイル <profile.xml> ファイルが変更されるまでアクティブ化されません。AnyConnect プロファイルでの SBL の有効化 （133 ページ）を参照してください。アクティブ化後に、ユーザは [ユーザのスイッチ（Switch User）] をクリックし、さらに画面下右側の [ネットワーク接続（Network Connect）] アイコンをクリックして Network Connect コンポーネントを呼び出します。

（注） 誤ってユーザ インターフェイスの画面表示を最小化した場合は、Alt+Tab キーの組み合わせで元に戻ります。

PLAP を使用した Windows PC へのログオン

手順

ステップ 1 Windows のスタート画面で、**Ctrl+Alt+Del** キーの組み合わせを押します。

[ユーザのスイッチ（Switch User）] ボタンが表示されたログイン ウィンドウが表示されます。

ステップ 2 ユーザが [ユーザのスイッチ（Switch User）] をクリックします。[ネットワーク接続（Network Connect）] ウィンドウが表示されます。AnyConnect 接続によってすでに接続済みのユーザが [ユーザのスイッチ（Switch User）] をクリックしても、VPN 接続は解除されません。[ネットワーク接続（Network Connect）] をクリックすると、元の VPN 接続が終了します。[キャンセル（Cancel）] をクリックすると、VPN 接続が終了します。

ステップ 3 ウィンドウの右下にある [ネットワーク接続（Network Connect）] ボタンをクリックして、AnyConnect を起動します。AnyConnect のログオン ウィンドウが表示されます。

ステップ 4 この GUI を使用して通常どおりログインします。
この例は、AnyConnect がただ 1 つのインストール済み接続プロバイダーであることを前提としたものです。複数のプロバイダーをインストールしている場合は、このウィンドウに表示される項目の中から、ユーザが使用するものをいずれか 1 つ選択する必要があります。

ステップ 5 接続されると、[ネットワーク接続（Network Connect）] ウィンドウとほぼ同じ画面が表示されます。異なるのは、右下隅に表示されるのが Microsoft の [接続解除（Disconnect）] ボタンである点です。このボタンは、正常に接続されたことを通知するためだけのものです。

ステップ 6 各ユーザのログオン用アイコンをクリックします。
接続が確立したら、数分間以内にログオンします。約 2 分のアイドル タイムアウト後にユーザ ログオン セッションがタイムアウトし、AnyConnect PLAP コンポーネントに対して接続解除が発行され、VPN トンネルが接続解除されます。

PLAP を使用した AnyConnect からの接続解除

VPN セッションが正常に確立されると、PLAP コンポーネントは元のウィンドウに戻ります。このときウィンドウの右下隅には [接続解除（Disconnect）] ボタンが表示されます。

[接続解除（Disconnect）] をクリックすると、VPN トンネルが接続解除されます。

トンネルは、[接続解除（Disconnect）] ボタンの操作によって明示的に接続解除される以外に、次のような状況でも接続解除されます。

- ユーザが PLAP を使用して PC にログインした後で [キャンセル（Cancel）] を押した。
- ユーザがシステムへログインする前に PC がシャットダウンした。

- Windows でユーザ ログオン セッションがタイムアウトになり、[ログオンするには CTRL+ALT+DELを押してください（Press CTRL + ALT + DEL to log on）] 画面に戻った。

この動作は、Windows PLAP アーキテクチャの機能であり、AnyConnect の機能ではありません。

VPN 接続の自動リスタート

[自動再接続（Auto Reconnect）] が有効（デフォルト）になっている場合、AnyConnect は初期接続に使用したメディアに関係なく、VPNセッションの中断から回復し、セッションを再確立します。たとえば、有線、ワイヤレス、または3Gのセッションを再確立できます。[自動再接続（Auto Reconnect）] が有効になっている場合は、システムの一時停止またはシステムの再開が発生した場合の再接続動作も指定します。システムの一時停止とは、Windows の「休止状態」や macOS または Linux の「スリープ」など、低電力スタンバイのことです。システムの再開とは、システムの一時停止からの回復のことです。

[自動再接続（Auto Reconnect）] を無効にすると、クライアントでは接続解除の原因にかかわらず、再接続が試行されません。この機能のデフォルト設定（有効）を使用することを強く推奨します。この設定を無効にすると、不安定な接続では VPN 接続の中断が発生することがあります。

手順

ステップ 1 VPN プロファイル エディタを開き、ナビゲーション ペインから [プリファレンス（Part 1）（Preferences (Part 1)）] を選択します。

ステップ 2 [自動再接続（Auto Reconnect）] を選択します。

ステップ 3 自動再接続の動作を選択します。

- [中断時に接続解除（Disconnect On Suspend）]：（デフォルト）AnyConnect では、システムが一時停止すると VPN セッションに割り当てられたリソースが解放され、システムの再開後も再接続は試行されません。
- [再開後に再接続（Reconnect After Resume）]：クライアントでは、システムが一時停止すると VPN セッションに割り当てられたリソースが保持され、システムの再開後は再接続が試行されます。

Trusted Network Detection を使用した接続または接続解除

Trusted Network Detection について

Trusted Network Detection（TND）を使用すると、ユーザが社内ネットワークの中（信頼ネットワーク）にいる場合は AnyConnect により自動的に VPN 接続が解除され、社内ネットワークの

外（非信頼ネットワーク）にいる場合は自動的に VPN 接続が開始されるようにすることができます。

TND を使用している場合でも、ユーザが手動で VPN 接続を確立することは可能です。信頼ネットワークの中でユーザが手動で開始した VPN 接続は解除されません。TND で VPN セッションが接続解除されるのは、最初に非信頼ネットワークにいたユーザが信頼ネットワークに移動した場合だけです。たとえば、ユーザが自宅で VPN 接続を確立した後で会社に移動すると、この VPN セッションは TND によって接続解除されます。

（注） Web セキュリティ モジュールにおける同等の機能については、「*Web* セキュリティの設定」の章の「Secure Trusted Network Detection の使用」を参照してください。

TND は AnyConnect VPN クライアント プロファイルで設定します。ASA の設定の変更は必要ありません。AnyConnect が信頼ネットワークと非信頼ネットワークの間の遷移を認識したときに実施するアクションまたはポリシーを指定する必要があります。また、信頼ネットワークおよび信頼サーバを特定する必要があります。

Trusted Network Detection のガイドライン

- TND 機能は AnyConnect GUI を制御し、接続を自動的に開始するため、GUI を常に実行している必要があります。ユーザが GUI を終了した場合、TND によって VPN 接続が自動的に開始されることはありません。
- さらに AnyConnect で Start Before Logon（SBL）が実行されている場合は、ユーザが信頼ネットワークの中に移動した時点で、コンピュータ上に表示されている SBL ウィンドウが自動的に閉じます。
- Always-Onが設定されているかどうかにかかわらず、Trusted Network Detection は、IPv4 ネットワークおよび IPv6 ネットワーク経由での ASA への IPv6 および IPv4 VPN 接続でサポートされています。
- ユーザ コンピュータ上に複数のプロファイルがあると、TND 設定が異なっている場合には問題になることがあります。

  ユーザが過去に TND 対応のプロファイルを受け取っていた場合、システムをリスタートすると、AnyConnect は最後に接続されたセキュリティ アプライアンスへの接続を試みますが、これが目的の動作ではないことがあります。別のセキュリティ アプライアンスに接続するには、そのヘッドエンドを手動で接続解除してから、再接続する必要があります。この問題を回避する手段としては、次のような対策が考えられます。

  - 社内ネットワーク上にあるすべての ASA にロードされるクライアント プロファイルで、TND を有効にする。
  - すべての ASA がリストされた 1 つのプロファイルをホスト エントリ セクションに作成し、このプロファイルをすべての ASA にロードする。
  - 複数の異なるプロファイルが必要ない場合は、すべての ASA のプロファイルに同じプロファイル名を使用する。既存のプロファイルは各 ASA により上書きされます。

- Linux 上で TND を使用するには、ネットワーク マネージャがインストールされてターゲット（RHEL/Ubuntu）デバイス上で正しく実行されていることと、ネットワーク インターフェイスがネットワーク マネージャによって管理されていることが必要です。

Trusted Network Detection の設定

手順

ステップ 1 VPN プロファイル エディタを開き、ナビゲーション ペインから [プリファレンス（Part 2）（Preferences (Part 2)）] を選択します。

ステップ 2 [自動 VPN ポリシー（Automatic VPN Policy）] を選択します。

ステップ 3 [信頼されたネットワークポリシー（Trusted Network Policy）] を選択します。

これは、ユーザが社内ネットワーク（信頼ネットワーク）内に存在する場合にクライアントが実行するアクションです。次のオプションがあります。

- [接続解除（Disconnect）]：（デフォルト）クライアントは、信頼ネットワークで VPN 接続を終了します。
- [接続（Connect）]：クライアントは、信頼ネットワークで VPN 接続を開始します。
- [何もしない（Do Nothing）]：クライアントは、信頼ネットワークでアクションを実行しません。[信頼されたネットワークポリシー（Trusted Network Policy）] と [信頼されていないネットワークポリシー（Untrusted Network Policy）] の両方を [何もしない（Do Nothing）] に設定すると、Trusted Network Detection（TND）は無効となります。
- [一時停止（Pause）]：ユーザが信頼ネットワークの外で VPN セッションを確立した後に、信頼済みとして設定されたネットワークに入った場合、AnyConnect は（VPN セッションを接続解除するのではなく）一時停止します。ユーザが再び信頼ネットワークの外に出ると、そのセッションは AnyConnect により再開されます。この機能を使用すると、信頼ネットワークの外へ移動した後に新しい VPN セッションを確立する必要がなくなるため、ユーザにとっては有用です。

ステップ 4 [信頼されていないネットワークポリシー（Untrusted Network Policy）] を選択します。

これは、ユーザが社内ネットワーク外に存在する場合にクライアントが実行するアクションです。次のオプションがあります。

- [接続（Connect）]：非信頼ネットワークが検出されるとクライアントにより VPN 接続が開始されます。
- [何もしない（Do Nothing）]：クライアントは、非信頼ネットワークの検出時にアクションを実行しません。このオプションを指定すると、Always-On VPN が無効になります。[信頼されたネットワークポリシー（Trusted Network Policy）] と [信頼されていないネットワークポリシー（Untrusted Network Policy）] の両方を [何もしない（Do Nothing）] に設定すると、Trusted Network Detection は無効となります。

ステップ 5 [信頼された DNS ドメイン（Trusted DNS Domains）] を指定します。

クライアントが信頼ネットワーク内に存在する場合にネットワーク インターフェイスに割り当てることができる DNS サフィックス（カンマ区切りの文字列）を指定します。split-dns リストに複数の DNS サフィックスを追加し、ASA でデフォルト ドメインを指定した場合、複数の DNS サフィックスを割り当てることができます。

AnyConnect クライアントは、次の順序で DNS サフィックスのリストを構築します。

- ヘッド エンドから渡されたドメイン。
- ヘッド エンドから渡されたスプリット DNS リスト。
- パブリック インターフェイスの DNS サフィックス（設定されている場合）。設定されていない場合は、プライマリ DNS サフィックスの親サフィックスを伴うプライマリおよび接続固有のサフィックス（対応するボックスが拡張 TCP/IP 設定でオンの場合）。

照合する DNS サフィックス	TrustedDNSDomains に使用する値
example.com（のみ）	*example.com
example.com と anyconnect.example.com	*.example.com または example.com、anyconnect.example.com
asa.example.com と anyconnect.example.com	*.example.com または asa.example.com、anyconnect.example.com

ステップ 6 [信頼された DNS サーバ（Trusted DNS Servers）] を指定します。

クライアントが信頼ネットワーク内に存在する場合にネットワーク インターフェイスに割り当てることができるすべての DNS サーバ アドレス（カンマ区切りの文字列）。たとえば、203.0.113.1,2001:DB8::1 です。IPv4 および IPv6 DNS サーバ アドレスでは、ワイルドカード（*）がサポートされています。

DNS で解決できるヘッドエンド サーバの DNS エントリが必要です。IP アドレスによる接続の場合、mus.cisco.com を解決できる DNS サーバが必要です。mus.cisco.com が DNS で解決できない場合、キャプティブ ポータルの検出が期待どおりに動作しません。

（注） TrustedDNSDomains、TrustedDNSServers、またはその両方を設定できます。TrustedDNSServers を設定する場合は、DNS サーバをすべて入力してください。その結果、サイトはすべて信頼ネットワークの一部になります。

アクティブ インターフェイスは、VPN プロファイルのすべてのルールが一致した場合に、信頼ネットワークに含まれると見なされます。

ステップ 7 信頼できる URL として追加するホスト URL を指定します。信頼できる証明書を使用してアクセス可能なセキュア Web サーバが、信頼できるサーバとして見なされる必要があります。[追加（Add）] をクリックすると、URL が追加され、証明書ハッシュに事前にデータが取り込まれます。ハッシュが見つからない場合は、ユーザに対して証明書ハッシュを手動で入力して [設定（Set）] をクリックするように求めるエラー メッセージが表示されます。

（注） このパラメータを設定できるのは、信頼された DNS ドメインまたは信頼された DNS サーバを 1 つ以上を定義する場合だけです。信頼された DNS ドメインまたは信頼された DNS サーバが定義されていない場合、このフィールドは無効になります。

Always-Onを使用した VPN 接続の必要性

Always-On VPN について

Always-On操作により、VPNセッションがアクティブでない限り、コンピュータが信頼ネットワーク上にない場合にはインターネット リソースにアクセスできなくなります。この状況で VPN を常に適用すると、コンピュータがセキュリティに対する脅威から保護されます。

Always-Onが有効になっている場合、ユーザがログインした後、および非信頼ネットワークが検出されたときに、VPN セッションが自動的に確立されます。VPN セッションは、ユーザがコンピュータからログアウトするか、（ASA グループ ポリシーに指定された）セッション タイマーまたはアイドル セッション タイマーが期限に達するまではオープンした状態が維持されます。AnyConnect では、セッションがオープンしている場合は、それを再アクティブ化するために接続の再確立が継続して試行され、それ以外の場合は、新しい VPN セッションの確立が継続的に試行されます。

VPNプロファイルでAlways-Onが有効になっている場合、AnyConnectは他のダウンロードされたすべての AnyConnect プロファイルを削除してエンドポイントを保護し、ASA に接続するように設定されているパブリック プロキシを無視します。

Always-Onを有効にする場合は、次の AnyConnect オプションも考慮する必要があります。

- [ユーザにAlways-On VPN セッションの接続解除を許可（Allowing the user to Disconnect the VPN session）]：AnyConnect では、ユーザがAlways-On VPN セッションの接続を解除できます。**Allow VPN Disconnect** を有効にすると、AnyConnect では VPN セッションが確立された時点で [接続解除（Disconnect）] ボタンが表示されます。Always-On VPN を有効にすると、プロファイル エディタでは、[接続解除（Disconnect）] ボタンがデフォルトで有効になります。

  [接続解除（Disconnect）]ボタンを押すと、すべてのインターフェイスがロックされます。これにより、データの漏えいを防ぐことができる以外に、VPNセッションの確立には必要のないインターネットアクセスからコンピュータを保護することができます。現在のVPNセッションでパフォーマンスが低下したり、VPNセッションの中断後に再接続で問題が発生したりした場合、Always-On VPN セッションのユーザは [接続解除（Disconnect）] をクリックして代替のセキュア ゲートウェイを選択できます。

- [接続障害ポリシーの設定（Setting a Connect Failure Policy）]：接続障害ポリシーにより、Always-On VPN が有効で、AnyConnect が VPN セッションを確立できない場合に、コンピュータがインターネットにアクセスできるかどうかが決まります。「常時接続の接続障害ポリシーの設定」を参照してください。

- [キャプティブ ポータル ホットスポットの処理（Handling Captive Portal Hotspots）]：「キャプティブ ポータル ホットスポットの検出と修復の使用」を参照してください。

Always-On VPN の制限事項

- Always-Onがオンであっても、ユーザがログインしていない場合は、AnyConnect は VPN 接続を確立しません。AnyConnect が VPN 接続を確立するのは、ログイン後に限られます。
- Always-On VPN では、プロキシを介した接続はサポートされていません。

Always-On VPN のガイドライン

脅威に対する保護を強化するためにも、Always-On VPN の設定を行う場合は、次のような追加的な保護対策を講じることを推奨します。

- 認証局（CA）からデジタル証明書を購入し、それをセキュア ゲートウェイ上に登録することを強く推奨します。ASDM では、[アイデンティティ証明書（Identity Certificates）] パネル（[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [証明書の管理（Certificate Management）] > [アイデンティティ証明書（Identity Certificates）]）に、公開証明書を容易に登録するための [ASA SSL VPN を Entrust で登録（Enroll ASA SSL VPN with Entrust）] ボタンが用意されています。
- フェールオーバー モードで常時接続の VPN を使用している場合、外部 SAML IdP はサポートされていません（ただし、内部 SAML IdP を使用すると、ASA はすべてのトラフィックを IdP にプロキシします。また、ASA はサポートされています）。
- Always-On が設定されたプロファイルをエンドポイントに事前に展開し、事前定義された ASA への接続を制限します。事前展開により、不正なサーバへのアクセスを防止することができます。
- ユーザが処理を終了できないように管理者権限を制限します。管理者権限を持つ PC ユーザは、エージェントを停止することにより、Always-Onポリシーを無視することができます。Always-Onの安全性を十分に確保する必要がある場合は、ユーザに対してローカル管理者権限を付与しないでください。
- Windows コンピュータ上の Cisco サブフォルダ（通常は `C:\ProgramData`）へのアクセスを制限します。
- 限定的な権限または標準的な権限を持つユーザは、それぞれのプログラム データ フォルダに対して書き込みアクセスを実行できる場合があります。このアクセスを使用すれば、AnyConnectプロファイル ファイルを削除できるため、Always-On機能を無効にすることができます。
- Windows ユーザのグループ ポリシー オブジェクト（GPO）を事前に展開して、限定的な権限を持つユーザが GUI を終了できないようにします。macOS ユーザに対してもこれに相当するものを事前に展開します。

Always-On VPN の設定

手順

ステップ 1 AnyConnect VPN クライアント プロファイルでのAlways-Onの設定 （143 ページ）。
ステップ 2 （任意）サーバ リストへのロード バランシング バックアップ クラスタ メンバーの追加。
ステップ 3 （任意）常時接続 VPN からのユーザの除外。

AnyConnect VPN クライアント プロファイルでのAlways-Onの設定

始める前に

Always-On VPN を使用するには、ASA 上に有効な信頼できるサーバ証明書が設定されている必要があります。設定されていない場合、VPN 常時接続は失敗し、その証明書が無効であることを示すイベントがログに記録されます。また、サーバ証明書が厳格な証明書トラスト モードを通過できるようにすると、Always-On VPN プロファイルのダウンロードを防止して不正なサーバへの VPN 接続をロックできます。

手順

ステップ 1 VPN プロファイル エディタを開き、ナビゲーション ペインから [プリファレンス（Part 2）（Preferences (Part 2)）] を選択します。
ステップ 2 [自動 VPN ポリシー（Automatic VPN Policy）] を選択します。
ステップ 3 Trusted Network Detection の設定 （139 ページ）
ステップ 4 [常時接続（Always On）] を選択します。
ステップ 5 （任意）[VPN の接続解除を許可（Allow VPN Disconnect）] を選択または選択解除します。
ステップ 6 （任意）接続障害ポリシーの設定。
ステップ 7 （任意）キャプティブ ポータル修復の設定。

サーバ リストへのロード バランシング バックアップ クラスタ メンバーの追加

Always-On VPN は、AnyConnect VPN セッションのロード バランシングに影響を与えます。Always-On VPN を無効にした状態では、クライアントからロード バランシング クラスタ内のプライマリ デバイスに接続すると、クライアントはプライマリ デバイスから任意のバックアップ クラスタ メンバーにリダイレクションされます。Always-On を有効にすると、クライアント プロファイルのサーバ リスト内にバックアップ クラスタ メンバーのアドレスが指定されていない限り、クライアントがプライマリ デバイスからリダイレクトされることはありません。このため、サーバ リストにはいずれかのバックアップ クラスタ メンバーを必ず追加するようにしてください。

クライアント プロファイルにバックアップ クラスタ メンバーのアドレスを指定する場合は、ASDM を使用してロード バランシング バックアップ サーバ リストを追加します。手順は次のとおりです。

手順

ステップ 1 VPN プロファイル エディタを開き、ナビゲーション ペインから [サーバ リスト（Server List）] を選択します。

ステップ 2 ロードバランシング クラスタのプライマリ デバイスであるサーバを選択し、[編集（Edit）] をクリックします。

ステップ 3 いずれかのロード バランシング クラスタ メンバーの FQDN または IP アドレスを入力します。

常時接続 VPN からのユーザの除外

Always-Onポリシーに優先して適用される除外規定を設定できます。たとえば、特定のユーザに対して他社とのVPNセッションを確立できるようにしつつ、企業外資産に対してはAlways-On VPN ポリシーを除外するという場合があります。

ASA のグループ ポリシーおよびダイナミック アクセス ポリシーで設定された除外規定は Always-On ポリシーを上書きします。ポリシーの割り当てに使用される一致基準に従って例外を指定します。AnyConnect ポリシーでは Always-On が有効になっているが、ダイナミック アクセス ポリシーまたはグループ ポリシーでは無効になっている場合、各新規セッションの確立に関するダイナミック アクセス ポリシーまたはグループ ポリシーが基準と一致すれば、クライアントでは現在以降の VPN セッションに対して無効の設定が保持されます。

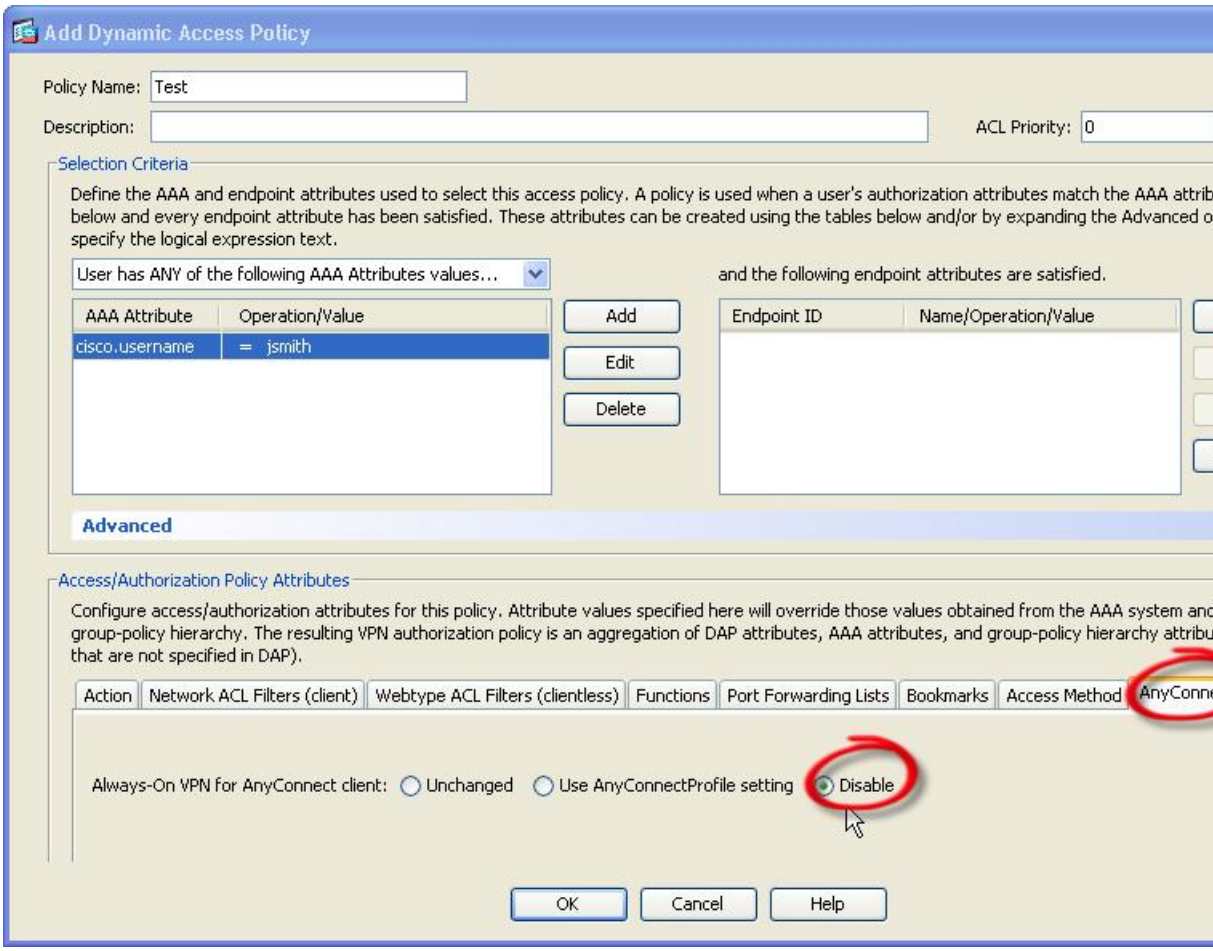
この手順では、AAA エンドポイント条件を使用して企業外資産にセッションを照合するダイナミック アクセス ポリシーを設定します。

手順

ステップ 1 [設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [ダイナミック アクセス ポリシー（Dynamic Access Policies）] > [追加（Add）] または [編集（Edit）] を選択します。

ステップ 2 ユーザをAlways-On VPN から除外する条件を設定します。たとえば、[選択基準（Selection Criteria）] 領域を使用して、ユーザのログイン ID に一致する AAA 属性を指定します。

ステップ 3 [ダイナミック アクセス ポリシーの追加（Add Dynamic Access Policy）] ウィンドウまたは [ダイナミック アクセス ポリシーの編集（Edit Dynamic Access Policy）] ウィンドウの下半分にある [AnyConnect] タブをクリックします。



ステップ 4 [AnyConnect クライアントのAlways-On VPN（Always-On VPN for AnyConnect client）] の横にある [無効（Disable）] をクリックします。

常時接続の接続障害ポリシーの設定

接続障害ポリシーについて

接続障害ポリシーは、Always-On VPN が有効で、AnyConnect が VPN セッションを確立できない場合に、コンピュータがインターネットにアクセスできるかどうかを決定します。これは、セキュア ゲートウェイに到達不能な場合、または AnyConnect がキャプティブ ポータル ホットスポットの存在を検出できない場合に発生する可能性があります。

オープン ポリシーは、最大限のネットワーク アクセスを許可します。これにより、インターネット リソースやその他のローカル ネットワーク リソースへのアクセスが必要なタスクをユーザが継続して実行できるようにします。

クローズド ポリシーは、VPN セッションが確立されるまで、すべてのネットワーク接続を無効にします。AnyConnect では、エンドポイントから、コンピュータが接続を許可されている

セキュア ゲートウェイ宛以外のトラフィックをすべてブロックするパケット フィルタを有効にすることで、この制限が実現されています。

AnyConnect では、接続障害ポリシーの内容にかかわらず、VPN 接続の確立が継続的に試行されます。

接続障害ポリシーを設定するためのガイドライン

最大限のネットワーク アクセス権を許可するオープン ポリシーを使用する場合は、次の点を考慮してください。

- VPNセッションが確立されるまでセキュリティと保護は提供されません。したがって、エンドポイント デバイスが Web ベースのマルウェアに感染したり、センシティブ データが漏えいしたりする可能性があります。
- [接続解除（Disconnect）] ボタンが有効で、かつユーザが [接続解除（Disconnect）] をクリックした場合は、オープン接続障害ポリシーは適用されません。

VPNセッションが確立されるまですべてのネットワーク接続を無効にする終了ポリシーを使用する場合は、次の点を考慮してください。

- ユーザが VPN の外部へのインターネット アクセスを必要とする場合に、クローズド ポリシーを適用すると、生産性が低下する可能性があります。
- クローズドの目的は、エンドポイントを保護するプライベート ネットワークのリソースが使用できない場合に、ネットワークの脅威から企業資産を保護することです。スプリット トンネリングによって許可されたプリンタやテザー デバイスなどのローカル リソースを除き、すべてのネットワーク アクセスが禁止されるため、エンドポイントは Web ベースのマルウェアとセンシティブ データ漏えいから常に保護されます。
- このオプションは、主にネットワークに常時アクセス可能なことよりも、セキュリティが持続することを重視する組織向きです。
- クローズドポリシーは、特に有効にしない限り、キャプティブ ポータルを修復しません。
- クライアント プロファイルで [最新の VPN ローカル リソースを適用（Apply Last VPN Local Resources）] が有効になっている場合は、直近の VPN セッションにより適用されたローカル リソース ルールを適用できます。たとえば、これらのルールにより、アクティブ シンクやローカル印刷へのアクセスを規定することができます。
- AnyConnect ソフトウェアのアップグレード中、Always-Onが有効であると、ネットワークはクローズド ポリシーに関係なくブロックが解除され、開かれます。
- クローズド接続ポリシーの展開は、段階的に行うことを強く推奨します。たとえば、最初に接続障害オープン ポリシーを使用してAlways-Onを展開し、ユーザを通じて AnyConnect がシームレスに接続できない頻度を調査します。さらに、新機能に関心を持つユーザを対象に、小規模な接続障害クローズドポリシーを試験的に展開しそのフィードバックを依頼します。引き続きフィードバックを依頼しながら試験的なプログラムを徐々に拡大したうえで、全面的な展開を検討します。接続障害クローズドポリシーを展開する場合は必ず、VPN ユーザに対して接続障害クローズド ポリシーのメリットだけでなく、ネットワーク アクセスの制限についても周知してください。

注意 AnyConnect が VPN セッションの確立に失敗した場合は、接続障害クローズド ポリシーによりネットワーク アクセスは制限されます。接続障害クローズドポリシーは、細心の注意を払って実装してください。

接続障害ポリシーの設定

Always-On 機能を有効にする場合にのみ、接続障害ポリシーを設定します。デフォルトでは、接続障害ポリシーはクローズされており、VPN が到達不能な場合にはインターネットにアクセスできません。この状況でインターネットへのアクセスを許可するには、オープンするように接続障害ポリシーを設定する必要があります。

手順

ステップ 1 VPN プロファイル エディタを開き、ナビゲーション ペインから [プリファレンス（Part 2）（Preferences (Part 2)）] を選択します。

ステップ 2 [Connect Failure Policy（接続エラーポリシー）] パラメータを次のいずれかに設定します。

- [クローズド（Closed）]：（デフォルト）セキュア ゲートウェイに接続できない場合、ネットワーク アクセスが制限されます。
- [オープン（Open）]：クライアントがセキュア ゲートウェイに接続できない場合、ブラウザなどのアプリケーションによるネットワーク アクセスが許可されます。

ステップ 3 クローズド ポリシーを指定した場合は、次の手順を実行します。

a) キャプティブ ポータル修復の設定。

b) ネットワーク アクセスが無効になっている間、最後の VPN セッションのローカル デバイス ルールを保持する場合は、[最新の VPN ローカル リソースを適用（Apply Last VPN Local Resources）] を選択します。

キャプティブ ポータル ホットスポットの検出と修復の使用

キャプティブ ポータルについて

空港、喫茶店、ホテルなど、Wi-Fi や有線アクセスを提供している施設では、アクセスする前に料金を支払ったり、アクセプタブル ユース ポリシーを順守することに同意したりする必要があります。こうした施設では、キャプティブ ポータルと呼ばれる技術を使用することにより、ユーザがブラウザを開いてアクセス条件に同意するまではアプリケーションの接続が行えないようにしています。キャプティブポータルの検出はこの制限を認識することであり、キャ

プティブ ポータル修復はネットワーク アクセスを取得するためにキャプティブ ポータルのホットスポット要件を満たすプロセスです。

キャプティブ ポータルは、VPN 接続が開始されると AnyConnect によって自動的に検出され、追加設定は必要ありません。また、AnyConnect は、キャプティブ ポータルの検出中にブラウザの設定を変更せず、キャプティブ ポータルを自動的に修復しません。修復は、エンド ユーザが実行します。AnyConnect は、現在の設定に応じてキャプティブ ポータルの検出に対応します。

- Always-On が無効の場合、または Always-On が有効で接続障害ポリシーが開いている場合、各接続試行時に次のメッセージが表示されます。

```
The service provider in your current location is restricting access to the Internet.
 You need to log on with the service provider before you can establish a VPN session.
 You can try this by visiting any website with your browser.
```

  エンドユーザは、ホットスポットプロバイダーの要件を満たすことで、キャプティブ ポータル修復を実行する必要があります。これらの要件には、ネットワークにアクセスするための料金の支払い、アクセプタブル ユース ポリシーへの署名、その両方、またはプロバイダーが定義するその他の要件などがあります。

- Always-On が有効で、接続障害ポリシーが閉じている場合、キャプティブ ポータル修復を明示的に有効にする必要があります。有効の場合、エンドユーザは修復を前述のように実行できます。無効の場合、各接続試行時に次のメッセージが表示され、VPN に接続できません。

```
The service provider in your current location is restricting access to the Internet.
 The AnyConnect protection settings must be lowered for you to log on with the service
 provider. Your current enterprise security policy does not allow this.
```

キャプティブ ポータル修復の設定

Always-On 機能を有効にし、接続障害ポリシーをクローズドに設定する場合にのみ、キャプティブ ポータル修復を設定します。この場合、キャプティブ ポータルのために VPN に接続できないときは、キャプティブ ポータル修復を設定すると、AnyConnect は VPN に接続できます。

（注） このプラットフォームでは常時接続がサポートされていないため、キャプティブ ポータルの修復の設定は Linux に適用されません。したがって、プロファイル エディタでの [キャプティブ ポータルの修復を常に許可（Allow Captive Portal Remediation Aloways On）] の設定に関係なく、Linux ユーザはキャプティブ ポータルを修復できます。

接続障害ポリシーがオープンに設定されているか、または Always-On が有効でない場合、ユーザはネットワーク アクセスが制限されないため、AnyConnect VPN クライアント プロファイルに特定の設定がなくてもキャプティブ ポータルを修復できます。

デフォルトでは、セキュリティを最大化するために、常時接続をサポートしているプラットフォーム（Windows と macOS）上ではキャプティブ ポータルの修復は無効になっています。

手順

ステップ 1 VPN プロファイル エディタを開き、ナビゲーション ペインから [プリファレンス（Part 1）（Preferences (Part 1)）] を選択します。

ステップ 2 [キャプティブ ポータルの修復を許可（Allow Captive Portal Remediation）] .を選択します。

この設定は、クローズ接続障害ポリシーによるネットワーク アクセス制限を解除します。

ステップ 3 修復タイムアウトを指定します。

AnyConnect がネットワーク アクセス制限を解除する時間（分単位）を入力します。ユーザには、キャプティブ ポータルの要件を満たすことができるだけの十分な時間が必要です。

キャプティブ ポータルの検出と修復のトラブルシューティング

次のような状況では、誤ってキャプティブ ポータルと見なされる場合があります。

- AnyConnectが、サーバ名が正しくない証明書（CN）を持ったASAに接続しようとしている場合、AnyConnect クライアントは、その環境を「キャプティブ ポータル」環境と見なします。

  これを回避するには、ASA 証明書が正しく設定されていることを確認します。証明書の CN 値は、VPN クライアント プロファイルの ASA サーバの名前と一致する必要があります。

- ASA の前に別のデバイスがネットワーク上に存在し、そのデバイスが ASA への HTTPS アクセスをブロックして、クライアントによる ASA への接続に応答すると、AnyConnect クライアントは、その環境を「キャプティブ ポータル」環境と見なします。これは、ユーザが内部ネットワークに存在し、ファイアウォールを介して ASA に接続している場合に発生する可能性があります。

  企業内から ASA へのアクセスを制限する必要がある場合、ASA のアドレスへの HTTP および HTTPS トラフィックが HTTP ステータスを返さないようにファイアウォールを設定します。ASA への HTTP/HTTPS アクセスは許可するか、完全にブロック（ブラック ホール化とも呼ばれます）し、ASA に送信された HTTP/HTTPS 要求が予期しない応答を返さないようにします。

ユーザがキャプティブ ポータル修復ページにアクセスできない場合は、次のことを試すようにユーザに指示してください。

- 修復を実行するためのブラウザを 1 つだけ残し、インスタント メッセージング プログラム、電子メール クライアント、IP フォン クライアントなど、HTTP を使用するその他のアプリケーションをすべて終了します。

  キャプティブ ポータルは、接続の反復試行を無視し、結果的にクライアント側でタイムアウトにすることで、DoS 攻撃を積極的に阻止することができます。HTTP 接続が多数のアプリケーションによって試行された場合、この問題の深刻度は大きくなります。

- ネットワーク インターフェイスを無効にした後、再度有効にします。このアクションにより、キャプティブ ポータルの検出が再試行されます。
- コンピュータを再起動します。

AnyConnect over L2TP または PPTP の設定

一部の国の ISP では、Layer 2 Tunneling Protocol（L2TP）や Point-to-Point Tunneling Protocol（PPTP）のサポートが必要です。

セキュア ゲートウェイを宛先としたトラフィックを Point-to-Point Tunneling Protocol（PPP）接続上で送信するため、AnyConnect は外部トンネルが生成したポイントツーポイント アダプタを使用します。PPP 接続上で VPN トンネルを確立する場合、クライアントでは ASA より先を宛先としてトンネリングされたトラフィックから、この ASA を宛先とするトラフィックが除外される必要があります。除外ルートを特定するかどうかや、除外ルートを特定する方法を指定する場合は、AnyConnect プロファイルの [PPP 除外（PPP Exclusion）] 設定を使用します。除外ルートは、セキュアでないルートとして AnyConnect GUI の [ルートの詳細（Route Details）] 画面に表示されます。

手順

ステップ 1 VPN プロファイル エディタを開き、ナビゲーション ペインから [プリファレンス（Part 2）（Preferences (Part 2)）] を選択します。

ステップ 2 [PPP 除外（PPP Exclusion）] でその方式を選択します。また、このフィールドに対する [ユーザ制御可（User Controllable）] をオンにして、ユーザがこの設定を表示および変更できるようにします。

- [自動（Automatic）]：PPP 除外を有効にします。AnyConnect は、PPP サーバの IP アドレスを自動的に使用します。この値は、自動検出による IP アドレスの取得に失敗した場合にのみ変更するよう、ユーザに指示してください。
- [上書き（Override）]：同様に PPP 除外を有効にします。自動検出で PPP サーバの IP アドレスを取得できず、[PPP 除外（PPP Exclusion）] の [ユーザ制御可（User Controllable）] の値が true である場合は、次項の説明に従ってこの設定を使用するよう、ユーザに指示してください。
- [無効（Disabled）]：PPP 除外は適用されません。

ステップ 3 [PPP 除外サーバ IP（PPP Exclusion Server IP）] フィールドに、接続に使用する PPP サーバの IP アドレスを入力します。このフィールドに対する [ユーザ制御可（User Controllable）] をオンにして、ユーザが preferences.xml ファイルを利用して PPP サーバの IP アドレスを変更できるようにします。

次のタスク

preferences.xml ファイルの変更については、「ユーザに対する *PPP* 除外上書きの指示」の項を参照してください。

ユーザに対する PPP 除外上書きの指示

自動検出が機能しない場合に、PPP除外フィールドをユーザ設定可能に設定すると、ユーザはローカル コンピュータ上で AnyConnect プリファレンス ファイルを編集することにより、これらの設定を上書きすることができます。

手順

ステップ 1 メモ帳などのエディタを使用して、プリファレンス XML ファイルを開きます。

このファイルは、ユーザのコンピュータ上で次のいずれかのパスにあります。

- Windows：%LOCAL_APPDATA%\Cisco\Cisco AnyConnect Secure Mobility Client\preferences.xml。次に例を示します。
- macOS：/Users/username/.anyconnect
- Linux：/home/username/.anyconnect

ステップ 2 PPPExclusion の詳細を `<ControllablePreferences>` の下に挿入して、Override 値と PPP サーバの IP アドレスを指定します。アドレスは、完全な形式の IPv4 アドレスにする必要があります。次に例を示します。

```
<AnyConnectPreferences>
<ControllablePreferences>
<PPPExclusion>Override
<PPPExclusionServerIP>192.168.22.44</PPPExclusionServerIP></PPPExclusion>
</ControllablePreferences>
</AnyConnectPreferences>
```

ステップ 3 ファイルを保存します。

ステップ 4 AnyConnect を終了して、リスタートします。

AnyConnect プロキシ接続の設定

AnyConnect プロキシ接続について

AnyConnect は、ローカル プロキシ、パブリック プロキシ、プライベート プロキシで VPN セッションをサポートしています。

- ローカル プロキシ接続：

ローカル プロキシは、AnyConnect と同じ PC 上で動作し、トランスペアレント プロキシとして使用されることもあります。トランスペアレント プロキシ サービスの例として、一部のワイヤレス データ カードによって提供されるアクセラレーション ソフトウェアや、一部のアンチウイルス ソフトウェア（Kaspersky など）に搭載のネットワーク コンポーネントなどがあります。

ローカル プロキシの使用は、AnyConnect VPN クライアント プロファイルで有効または無効にします。「ローカル プロキシ接続の許可」を参照してください。

- パブリック プロキシ接続：

  通常、パブリック プロキシは Web トラフィックの匿名化に使用されます。Windows がパブリック プロキシを使用するように設定されている場合、AnyConnect はその接続を使用します。パブリック プロキシは macOS と Linux でネイティブと上書きの両方をサポートしています。

  パブリック プロキシの設定については、パブリック プロキシ接続の設定（Windows）に関する説明を参照してください。

- プライベート プロキシ接続：

  プライベート プロキシ サーバは、企業の使用ポリシーに基づいて企業ユーザが特定の Web サイト（たとえば、アダルト、ギャンブル、ゲームなどのサイト）にアクセスできないようにするために社内ネットワークで使用されます。

  トンネルの確立後にブラウザにプライベート プロキシ設定をダウンロードするようにグループ ポリシーを設定します。VPN セッションが終了すると、設定は元の状態に復元されます。プライベート プロキシ接続の設定 （155 ページ）を参照してください。

（注） プロキシ サーバを経由する AnyConnect SBL 接続は、Windows オペレーティング システムのバージョン、システム（マシン）の設定、またはその他のサードパーティ プロキシ ソフトウェア機能に依存します。このため、Microsoft または使用するすべてのサードパーティ プロキシ アプリケーションによって提供される、システム全体のプロキシ設定を参照してください。

VPN クライアント プロファイルによるクライアント プロキシの制御

VPN クライアント プロファイルでは、クライアント システムのプロキシ接続をブロックしたり、リダイレクトしたりできます。Windows および Linux の場合、パブリック プロキシ サーバのアドレスを自分で設定したり、ユーザに設定を許可したりできます。

VPN クライアント プロファイルにプロキシ設定を設定する方法の詳細については、「AnyConnect プロファイル エディタ、プリファレンス（Part 2）」を参照してください。

クライアントレス サポートのためのプロキシ自動設定ファイルの生成

ASA の一部のバージョンでは、AnyConnect セッションが確立された後も、プロキシ サーバを経由するクライアントレス ポータル アクセスをサポートするために、AnyConnect 設定が必要です。AnyConnect では、この設定が行われるように、プロキシ自動設定（PAC）ファイルを使用してクライアント側プロキシ設定が修正されます。AnyConnect でこのファイルが生成されるのは、ASA でプライベート側プロキシ設定が指定されていない場合だけです。

AnyConnect プロキシ接続の要件

プロキシ接続の OS サポートは次のようになります。

プロキシ接続タイプ	Windows	macOS	Linux
ローカル プロキシ	○	可（上書きおよびネイティブ）	○
プライベートプロキシ	可（Internet Explorer）	可（システムプロキシ設定として設定）	なし
パブリック プロキシ	可（IEおよび上書き）	可（上書きおよびネイティブ	可（上書きおよびネイティブ）

プロキシ接続の制限

- IPv6 プロキシは、プロキシ接続のどのタイプでもサポートされません。
- プロキシ経由の接続は、Always-On機能が有効になっている場合にはサポートされません。
- ローカル プロキシへのアクセスを許可するには、VPN クライアント プロファイルが必要です。

ローカル プロキシ接続の許可

手順

ステップ 1 VPN プロファイル エディタを開き、ナビゲーション ペインから [プリファレンス（Part 2）（Preferences (Part 2)）] を選択します。

ステップ 2 [ローカル プロキシ接続を許可（Allow Local Proxy Connections）] を選択（デフォルト）または選択解除します。ローカル プロキシはデフォルトで無効になっています。

パブリック プロキシ

パブリック プロキシは Windows および Linux の各プラットフォームでサポートされています。プロキシ サーバは、クライアント プロファイルで設定されるプリファレンスに基づいて選択

されます。プロキシ オーバーライドの場合、AnyConnect はプロファイルからプロキシ サーバを取得します。リリース 4.1 では、Linux および macOS でのネイティブ プロキシ設定とともに Mac でのプロキシ サポートが追加されました。

Linux では、AnyConnect の実行前にネイティブ プロキシ設定がエクスポートされます。設定を変更した場合は、再起動が必要です。

プロキシ サーバの認証には、ユーザ名とパスワードが必要です。AnyConnect は、プロキシ サーバが認証を必要とするように設定されている場合、基本認証および NTLM 認証をサポートします。AnyConnect ダイアログが認証プロセスを管理します。プロキシ サーバに対する認証に成功すると、AnyConnect は ASA ユーザ名およびパスワードの入力を求めます。

パブリック プロキシ接続の設定（Windows）

Windows でパブリック プロキシ接続を設定するには、次の手順を実行します。

手順

ステップ 1 Internet Explorer またはコントロール パネルから [インターネット オプション（Internet Options）] を開きます。

ステップ 2 [接続（Connections）] タブを選択し、[LAN 設定（LAN Settings）] ボタンをクリックします。

ステップ 3 プロキシ サーバを使用するように LAN を設定し、プロキシ サーバの IP アドレスを入力します。

パブリック プロキシ接続の設定（macOS）

手順

ステップ 1 システム設定に移動し、接続している適切なインターフェイスを選択します。

ステップ 2 [詳細設定（Advanced）] をクリックします。

ステップ 3 新しいウィンドウで [プロキシ（Proxies）] タブを選択します。

ステップ 4 HTTPS プロキシを有効にします。

ステップ 5 右側のパネルの [セキュアプロキシサーバ（Secure Proxy Server）] フィールドに、プロキシ サーバのアドレスを入力します。

パブリック プロキシ接続の設定（Linux）

Linux でパブリック プロキシ接続を設定するには、環境変数を設定します。

プライベート プロキシ接続の設定

手順

ステップ 1 ASA グループ ポリシーにプライベート プロキシ情報を設定します。『*Cisco ASA Series VPN Configuration Guide*』の「Configuring a Browser Proxy for an Internal Group Policy」の項を参照してください。

（注） macOS 環境では、（VPN 接続時に）ASA からプッシュダウンされたプロキシ情報は、端末を開いて **scutil --proxy** を発行するまで、ブラウザに表示されません。

ステップ 2 （任意）ブラウザのプロキシ設定を無視するためのクライアントの設定。

ステップ 3 （任意）Internet Explorer の [接続（Connections ）] タブのロックダウン。

ブラウザのプロキシ設定を無視するためのクライアントの設定

AnyConnect プロファイルでは、ユーザの PC 上で Microsoft Internet Explorer または Safari のプロキシ設定が無視されるようにポリシーを指定できます。これにより、ユーザは社内ネットワークの外部からトンネルを確立できなくなり、AnyConnect は望ましくないまたは違法なプロキシ サーバ経由で接続できなくなります。

手順

ステップ 1 VPN プロファイル エディタを開き、ナビゲーション ペインから [プリファレンス（Part 2）（Preferences (Part 2)）] を選択します。

ステップ 2 [プロキシ設定（Proxy Settings）] ドロップダウン リストで、[プロキシを無視（Ignore Proxy）] を選択します。[プロキシを無視（Ignore Proxy）] を選択すると、クライアントはすべてのプロキシ設定を無視します。ASA からダウンロードされるプロキシに対してアクションが実行されません。

Internet Explorer の [接続（Connections ）] タブのロックダウン

ある条件下では、AnyConnect により、Internet Explorer の [ツール（Tools ）] > [インターネット オプション] > [接続（Connections ）] タブが非表示にされます。このタブが表示されている場合、ユーザはプロキシ情報を設定できます。このタブを非表示にすると、ユーザが意図的または偶発的にトンネルを迂回することを防止できます。タブのロックダウンは接続解除すると反転され、このタブに適用される管理者定義のポリシーの方が優先されます。このロックダウンは、次のいずれかの条件で行われます。

- ASA の設定で、[接続（Connections ）] タブのロックダウンが指定されている。
- ASA の設定で、プライベート側プロキシが指定されている。

- Windows のグループ ポリシーにより、以前に [接続（Connections ）] タブがロックダウンされている（ロックダウンしない ASA グループ ポリシー設定の上書き）。

グループ ポリシーで、プロキシのロックダウンを許可する、または許可しないように ASA を設定できます。ASDM を使用してこれを設定する手順は次のとおりです。

手順

ステップ 1 ASDM で、**[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [グループ ポリシー（Group Policies）]** に移動します。

ステップ 2 グループ ポリシーを選択し、新しいグループ ポリシーの **[編集（Edit）]** または **[追加（Add）]** をクリックします。

ステップ 3 ナビゲーション ペインで、**[詳細（Advanced）] > [ブラウザ プロキシ（Browser Proxy）]** に移動します。[プロキシ サーバ ポリシー（Proxy Server Policy）] ペインが表示されます。

ステップ 4 **[プロキシ ロックダウン（Proxy Lockdown）]** をクリックして、その他のプロキシ設定を表示します。

ステップ 5 プロキシのロックダウンを有効にして、AnyConnect のセッション中は Internet Explorer の [接続（Connections ）] タブを非表示にするには、**[継承（Inherit）]** をオフにして **[はい（Yes）]** を選択します。または、プロキシのロックダウンを無効にして、AnyConnect のセッション中は Internet Explorer の [接続（Connections ）] タブを表示するには、**[いいえ（No）]** を選択します。

ステップ 6 **[OK]** をクリックして、プロキシ サーバ ポリシーの変更を保存します。

ステップ 7 **[適用（Apply）]** をクリックして、グループ ポリシーの変更を保存します。

プロキシ設定の確認

- Windows の場合：次の場所でレジストリのプロキシ設定を検索します。

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
```

- macOS の場合：ターミナル ウィンドウを開き、次を入力します。

```
scutil --proxy
```

VPN トラフィックの選択および除外

VPN をバイパスするための IPv4 または IPv6 トラフィックの設定

ASA が IPv6 トラフィックのみを待機している場合は AnyConnect クライアントが IPv4 トラフィックをどのように管理するかを設定し、ASA がクライアント バイパス プロトコル設定を

使用して IPv4 トラフィックのみを待機している場合は AnyConnect クライアントが IPv6 トラフィックをどのように管理するかを設定できます。

AnyConnect クライアントで ASA に VPN 接続をする場合、ASA はクライアントに IPv4、IPv6、または IPv4 および IPv6 両方のアドレスを割り当てる場合があります。

クライアント バイパス プロトコルが IP プロトコルに対して有効であり、かつ、あるアドレス プールがそのプロトコルに対して設定されていない（つまり、そのプロトコルの IP アドレスが ASA によってクライアントに割り当てられていない）場合、そのプロトコルを使用する IP トラフィックは VPN トンネルを介して送信されません。これは、トンネル外で送信されます。

クライアント バイパス プロトコルが無効であり、かつ、あるアドレス プールがそのプロトコル用に設定されていない場合、VPN トンネルが確立された後、クライアントではその IP プロトコルのすべてのトラフィックをドロップします。

たとえば、IPv4 アドレスのみ AnyConnect 接続に割り当てられ、エンドポイントがデュアル スタックされていると想定します。エンドポイントが IPv6 アドレスへの到達を試みた場合、クライアント バイパス プロトコルが無効になっていると、IPv6 トラフィックはドロップされます。クライアント バイパス プロトコルが有効になっていると、IPv6 トラフィックはクライアントからクリア テキストで送信されます。

クライアント バイパス プロトコルを ASA でグループ ポリシーに設定します。

手順

ステップ 1 ASDM で、**[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [グループ ポリシー（Group Policies）]** に移動します。

ステップ 2 グループ ポリシーを選択し、新しいグループ ポリシーの **[編集（Edit）]** または **[追加（Add）]** をクリックします。

ステップ 3 **[詳細（Advanced）] > [AnyConnect]** を選択します。

ステップ 4 デフォルト グループ ポリシー以外のグループ ポリシーの場合、[クライアント バイパス プロトコル（Client Bypass Protocol）] の隣にある [継承（Inherit）] チェックボックスをオフにします。

ステップ 5 次のオプションのいずれかを選択します。

- ASA がアドレスを割り当てなかった IP トラフィックをドロップする場合は、[無効（Disable）] をクリックします。
- その IP トラフィックをクリア テキストで送信する場合は、[有効（Enable）] をクリックします。

ステップ 6 [OK] をクリックします。

ステップ 7 [Apply] をクリックします。

ローカル プリンタおよびテザー デバイスをサポートしたクライアント ファイアウォールの設定

『*Cisco ASA Series Configuration Guide*』の「Client Firewall with Local Printer and Tethered Device Support」の項を参照してください。

スプリット トンネリングの設定

スプリット トンネリングは、[ネットワーク（クライアント）アクセス（Network (Client) Access）] グループ ポリシーに設定します。『Cisco ASA Series VPN Configuration Guide』の「*Configure Split Tunneling for AnyConnect Traffic*」の項を参照してください。

ASDM でグループ ポリシーに変更を加えたら、[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [AnyConnect 接続プロファイル（AnyConnect Connection Profiles）] > [追加/編集（Add/Edit）] > [グループ ポリシー（Group Policy）] で、グループ ポリシーを接続プロファイルに関連付けてください。

ダイナミック スプリット トンネリングについて

ダイナミック スプリット トンネリングは、ASDM グループ ポリシー設定で [次のネットワークリストを除外（Exclude Network List Below）] または [次のネットワークリストをトンネリング（Tunnel Network List Below）] オプションを使用して設定される現在のスプリット トンネリング オプションを強化するために設計されました。スプリット トンネリングを定義するために通常使用される静的な包含または除外と違い、ダイナミック スプリット トンネリングでの包含または除外は、特定のサービスに関するトラフィックを VPN トンネリングから除外するまたは VPN トンネリングに包含する必要があるシナリオに対応しています。IP プロトコルごとに個別のスプリット トンネリング設定を構成できます。たとえば、IPv4 にダイナミック スプリット包含トンネリング（IPv4 スプリット包含ドメインやダイナミック スプリット包含ドメインなど）を有効にし、IPv6 にダイナミック スプリット除外トンネリング（IPv6 トンネル オール ドメインやダイナミック スプリット除外ドメインなど）を有効にできます。さらに、AnyConnect リリース 4.6 では、拡張ダイナミック スプリット トンネリングが追加されました。ダイナミック スプリット除外ドメインとダイナミック スプリット包含ドメインの両方が拡張ドメイン名の一致に指定されています。

ダイナミック スプリット除外トンネリング：複数のクラウドベースのサービスが同じ IP プールにホストされており、ユーザの場所またはクラウド上のコンピュータ資源の負荷に応じて異なる IP アドレスへと解決される場合があります。そのようなサービスのうち 1 つだけを VPN トンネルから除外したい場合、管理者が静的な除外を使用してそのためのポリシーを定義するのは、特に ISP NAT、6to4、4to6 などのネットワーク変換スキームも考慮される場合は困難です。ダイナミック スプリット除外トンネリングでは、トンネルの確立後に、ホストの DNS ドメイン名に基づいて動的にスプリット除外トンネリングをプロビジョニングできます。たとえば、VPN 管理者は、実行時に example.com を VPN トンネルから除外するように設定できます。VPN トンネルがアップしているときにアプリケーションが mail.example.com に接続しようとす

ると、VPN クライアントは、自動的にシステム ルーティング テーブルとフィルタを変更し、トンネル外部への接続を許可します。

拡張ダイナミック スプリット除外トンネリング：ダイナミック スプリット除外トンネリングがダイナミック スプリット除外ドメインとダイナミック スプリット包含ドメインの両方で設定されている場合、VPN トンネルから動的に除外されたトラフィックは少なくとも 1 つのダイナミック スプリット除外ドメインに一致する必要がありますが、ダイナミック スプリット包含ドメインに一致する必要はありません。たとえば、VPN 管理者がダイナミック スプリット除外ドメイン example.com とダイナミック スプリット包含ドメイン mail.example.com を設定した場合、mail.example.com 以外のすべての example.com トラフィックはトンネリングから除外されます。

ダイナミック スプリット包含トンネリング：ダイナミック スプリット包含トンネリングでは、トンネルの確立後に、ホストの DNS ドメイン名に基づいて動的にスプリット包含トンネリングをプロビジョニングできます。たとえば、VPN 管理者は、実行時に domain.com を VPN トンネルに含めるように設定できます。VPN トンネルがアップしているときにアプリケーションが www.domain.com に接続しようとすると、VPN クライアントは、自動的にシステム ルーティング テーブルとフィルタを変更し、VPN トンネル内部での接続を許可します。

拡張ダイナミック スプリット包含トンネリング：ダイナミック スプリット包含トンネリングがダイナミック スプリット包含ドメインとダイナミック スプリット除外ドメインの両方で設定されている場合、VPN トンネルに動的に包含されたトラフィックは少なくとも 1 つのダイナミック スプリット包含ドメインに一致する必要がありますが、ダイナミック スプリット除外ドメインに一致する必要はありません。たとえば、VPN 管理者が domain.com をスプリット包含ドメインとして、www.domain.com をスプリット除外ドメインとして設定した場合、www.domain.com 以外のすべての domain.com トラフィックがトンネリングされます。

（注） ダイナミック スプリット トンネリングは、Linux ではサポートされていません。

スタティック スプリット トンネリングとダイナミック スプリット トンネリングの相互運用性

静的な除外と動的な除外は共存可能です。スタティック スプリット トンネリングはトンネルの確立時に適用され、ダイナミック スプリット トンネリングは、トンネルが接続済みとなっているときにドメインへのトラフィックが発生すると適用されます。

ダイナミック スプリット除外トンネリング

ダイナミック スプリット除外トンネリングは、「tunnel all」、「split include」、および「split exclude」トンネリングに適用されます。

- すべてのネットワークをトンネリングする：VPN トンネルからの除外は、すべて動的です。
- 特定のネットワークを除外する：事前設定された静的な除外に動的な除外が追加されます。

- 特定のネットワークを包含する：除外されるホスト名の IP アドレスのうち、スプリットを含むネットワークと重複する場合のみ、動的な除外が適用されます。それ以外の場合、トラフィックは VPN トンネルからすでに除外されているため、動的な除外は行われません。

拡張ダイナミック スプリット除外トンネリングは、「tunnel all」および「split exclude」トンネリングに適用されます。ダイナミック スプリット除外ドメインとダイナミック スプリット包含ドメインの両方、およびスプリット包含トンネリングが設定されている場合、その結果の設定は拡張ダイナミック スプリット包含トンネリングになります。

ダイナミック スプリット包含トンネリング

ダイナミック スプリット包含トンネリングは、スプリット包含設定にのみ適用されます。

拡張ダイナミック スプリット包含トンネリングは、スプリット包含設定にのみ適用されます。

（注） Umbrella ローミング セキュリティによる保護は、スタティックまたはダイナミック スプリット トンネリングのいずれかが有効になっていると、アクティブになります。Umbrella クラウド リゾルバは、到達可能であり、かつ、VPN トンネルによるプローブが可能である場合を除き、VPN トンネルから静的に包含または除外することが必要となる場合があります。

スプリット トンネリング設定をともなう重複シナリオの結果

動的な包含または除外の対象は、まだ包含または除外されていない IP アドレスのみです。静的トンネリングおよび何らかの形式の動的トンネリングの両方が適用されており、新たな包含または除外を強制する必要がある場合、すでに適用された包含または除外との衝突が発生する可能性があります。動的な除外（除外されるドメイン名と一致する DNS 応答の一部となっているすべての IP アドレスが対象）が実行される場合、除外において考慮されるのは、まだ除外されていないアドレスのみです。同様に、動的な包含（包含されるドメイン名と一致する DNS 応答の一部となっているすべての IP アドレスが対象）が実行される場合、包含において考慮されるのは、まだ包含されていないアドレスのみです。

静的なパブリック ルート（セキュア ゲートウェイ ルートなどのスプリット除外ルートやクリティカル ルートなど）は、ダイナミック スプリット包含ルートよりも優先されます。そのため、動的な包含の少なくとも 1 つの IP アドレスが静的なパブリック ルートと一致する場合、動的な包含は強制されません。

同様に、静的スプリット包含ルートはダイナミック スプリット除外ルートよりも優先されます。そのため、動的な除外の少なくとも 1 つの IP アドレスが静的スプリット包含ルートと一致する場合、動的な除外は強制されません。

ダイナミック スプリット トンネリングの使用状況の通知

VPN トンネルの接続中は、ダイナミック スプリット トンネリングに何が設定されているかをいくつかの方法で確認できます。

- [統計（Statistics）] タブ：ASN グループ ポリシーで設定されている VPN トンネルから除外された、または VPN トンネルに包含されたドメイン名を含むダイナミック トンネル除外およびダイナミック トンネル包含が表示されます。
- [エクスポート統計（Export Stats）]：VPN トンネリングから除外された、または VPN トンネリングに包含されたドメイン名と、IPv4 と IPv6 の両方のトンネル モードを含むファイルが生成されます。ダイナミック ルートもエクスポートされた統計に含まれます。
- [ルートの詳細（Route Details）] タブ：除外または包含された各 IP アドレスに対応するホスト名を持つ IPv4 および IPv6 ダイナミック スプリット除外および包含ルートが表示されます。

（注） AnyConnect UI には、AnyConnect VPN が実現する保護されたルートまたは保護されていないルートが、IP プロトコルにつき最大 200 個表示されます。ルートの数が 200 を超えると、切り捨てが発生します。すべてのルートを表示するには、Windows では **route print** を実行し、Linux または macOS では **netstat -rn** を実行します。

- VPN の設定ログ メッセージ：VPN トンネルから除外された、または VPN トンネルに包含されたドメインの数が示されます。

ダイナミック スプリット除外トンネリングの設定

始める前に

ダイナミック スプリット トンネリングについて （158 ページ） を参照してください。

ダイナミック スプリット トンネリングでは、トンネルの確立後に、DNS ドメイン名に基づいて動的にスプリット除外トンネリングを行うことができます。ダイナミック スプリット トンネリングを設定するには、ASA 上でカスタム属性を作成し、グループ ポリシーに追加します。GUI の手順については、『*Cisco ASA Series VPN ASDM Configuration Guide*』の「Configure Dynamic Split Tunneling」を参照してください。

1. 次のコマンドを使用して、WebVPN コンテキストでカスタム属性タイプを定義します。

```
anyconnect-custom-attr dynamic-split-exclude-domains description dynamic split exclude
 domains
```

2. VPN トンネル外部のクライアントによるアクセスが必要な各クラウド/Web サービスについて、属性名を定義します。たとえば、Google Web サービスに関する DNS ドメイン名のリストとして、Google_domains を追加します。この属性値には、VPN トンネルから除外するドメイン名のリストが含まれており、例として次のようにカンマ区切り値（CSV）形式にする必要があります。

```
anyconnect-custom-data dynamic-split-exclude-domains example_service_domains
example1.com, example2.com
```

3. 次のコマンドを使用して、以前に定義されているカスタム属性を特定のポリシー グループに追加します。これは、group-policy 属性のコンテキストで実行されます。

```
anyconnect-custom dynamic-split-exclude-domains value example_service_domains
```

拡張ダイナミック スプリット除外トンネリングの設定

始める前に

ダイナミック スプリット トンネリングについて （158 ページ） を参照してください。

ダイナミック スプリット除外トンネリングがダイナミック スプリット除外ドメインとダイナミック スプリット包含ドメインの両方で設定されている場合、拡張ドメイン名照合がサポートされています。拡張ダイナミック スプリット除外トンネリングを設定するには、ASA 上で 2 つのカスタム属性を作成し、グループ ポリシーに追加します。GUI の手順については、『*Cisco ASA Series VPN ASDM Configuration Guide*』の「Configure Dynamic Split Tunneling」を参照してください。

1. 次のコマンドを使用して、WebVPN コンテキストでカスタム属性タイプを定義します。

```
anyconnect-custom-attr dynamic-split-exclude-domains description dynamic split exclude
 domains
```

2. VPN トンネル外部のクライアントによるアクセスが必要な各クラウド/Web サービスについて、属性名を定義します。たとえば、example.com がダイナミック スプリット除外ドメインで、www.example.com がダイナミック スプリット包含ドメインである場合、examples.com へのすべてのトラフィックは www.example.com を除いて除外されます。この属性値には、VPN トンネルから除外する（またはしない）ドメイン名のリストが含まれており、例として次のようにカンマ区切り値（CSV）形式にする必要があります。

```
anyconnect-custom-data dynamic-split-exclude-domains example_service_domains
example1.com, example2.com
```

```
anyconnect-custom-data dynamic-split-include-domains example_service_domains_tunneled
 www.example1.com, www.example2.com
```

3. 次のコマンドを使用して、以前に定義されているカスタム属性を特定のポリシー グループに追加します。これは、group-policy 属性のコンテキストで実行されます。

```
anyconnect-custom dynamic-split-exclude-domains value
```

```
example_service_domains
```

```
anyconnect-custom dynamic-split-include-domains value
```

```
example_service_domains_tunneled
```

ダイナミック スプリット包含トンネリングの設定

始める前に

ダイナミック スプリット トンネリングについて （158 ページ） を参照してください。

ダイナミック スプリット トンネリングでは、トンネルの確立後に、ホストの DNS ドメイン名に基づいて動的にスプリット包含トンネリングをプロビジョニングできます。ダイナミック ス

プリット トンネリングを設定するには、ASA 上でカスタム属性を作成し、グループ ポリシーに追加します。GUI の手順については、『*Cisco ASA Series VPN ASDM Configuration Guide*』の「Configure Dynamic Split Tunneling」を参照してください。

1. 次のコマンドを使用して、WebVPN コンテキストでカスタム属性タイプを定義します。

```
anyconnect-custom-attr dynamic-split-include-domains description dynamic split include
 domains
```

2. VPN トンネルによるクライアント アクセスが必要な各クラウド/Web サービスについて、カスタム属性名を定義します。この属性値には、VPN トンネルに包含するドメイン名のリストが含まれており、例として次のようにカンマ区切り値（CSV）形式にする必要があります。

```
anyconnect-custom-data dynamic-split-include-domains corporate_service_domains
domain1.com, domain2.com
```

（注） カスタム属性は421 文字以内である必要があります。制限を超えると、動的に包含されたドメインのリスト（CSV 形式）を 小さな値に分割する必要がある場合があります。

3. 次のコマンドを使用して、以前に定義されているカスタム属性を特定のポリシー グループに追加します。これは、group-policy 属性のコンテキストで実行されます。

```
anyconnect-custom dynamic-split-include-domains value
corporate_service_domains
```

拡張ダイナミック スプリット包含トンネリングの設定

始める前に

ダイナミック スプリット トンネリングについて （158 ページ） を参照してください。

ダイナミック スプリット包含トンネリングがダイナミック スプリット包含ドメインとダイナミック スプリット除外ドメインの両方で設定されている場合、拡張ドメイン名照合がサポートされています。拡張ダイナミック スプリット包含トンネリングを設定するには、ASA 上で 2 つのカスタム属性を作成し、グループ ポリシーに追加します。GUI の手順については、『*Cisco ASA Series VPN ASDM Configuration Guide*』の「Configure Dynamic Split Tunneling」を参照してください。

1. 次のコマンドを使用して、WebVPN コンテキストでカスタム属性タイプを定義します。

```
anyconnect-custom-attr dynamic-split-exclude-domains description dynamic split exclude
 domains
```

2. VPN トンネルからのクライアント アクセスが必要な各クラウド/Web サービスについて、カスタム属性名を定義します。たとえば、domain.com がダイナミック スプリット包含ドメインであり、www.domain.com がダイナミック スプリット除外ドメインである場合、domain.com へのすべてのトラフィックは www.domain.com を除いて包含されます。属性値には、VPN トンネルに包含する（またはしない）ドメイン名のリストが含まれており、例として次のようにカンマ区切り値（CSV）形式にする必要があります。

```
anyconnect-custom-data dynamic-split-include-domains corporate_service_domains
domain1.com, domain2.com

anyconnect-custom-data dynamic-split-include-domains corporate_service_domains_excluded
 www.domain1.com, www.domain2.com
```

3. 次のコマンドを使用して、以前に定義されているカスタム属性を特定のポリシー グループに追加します。これは、group-policy 属性のコンテキストで実行されます。

```
anyconnect-custom dynamic-split-include-domains value

corporate_service_domains

anyconnect-custom dynamic-split-exclude-domains value

corporate_service_domains_excluded
```

スプリット DNS

スプリット DNS が [ネットワーク（クライアント）アクセス（Network (Client) Access）] グループ ポリシーに設定されている場合、AnyConnect は、特定の DNS クエリーをプライベート DNS サーバ（同様にグループ ポリシーに設定）にトンネルします。他の DNS クエリーはすべて DNS 解決のためのクライアント オペレーティング システムの DNS リゾルバにクリア テキストで送信されます。スプリット DNS が設定されていない場合、AnyConnect はすべての DNS クエリーをトンネルします。

スプリット DNS の要件

スプリット DNS は、標準クエリーおよび更新クエリー（A、AAAA、NS、TXT、MX、SOA、ANY、SRV、PTR、CNAME など）をサポートしています。トンネリングされたネットワークのいずれかに一致する PTR クエリーは、トンネル経由で許可されます。

AnyConnect スプリット DNS は、Windows と macOS プラットフォームでサポートされています。

macOS の場合、AnyConnect は、次のいずれかの条件を満たす場合のみ、ある IP プロトコルのトゥルー スプリット DNS を使用できます。

- グループ ポリシーで、スプリット DNS が 1 つの IP プロトコル（IPv4 など）に設定されており、クライアント バイパス プロトコルがもう片方の IP プロトコル（IPv6 など）に設定されている（後者の IP プロトコルにはアドレス プールは設定されていない）。
- スプリット DNS が両方の IP プロトコルに設定されている。

スプリット DNS の設定

グループ ポリシーにスプリット DNS を設定するには、次の手順を実行します。

手順

ステップ 1 少なくとも 1 つの DNS サーバを設定します。

『Cisco ASA Series VPN Configuration Guide』の「*Configure Server Attributes for an Internal Group Policy*」の項を参照してください。

指定したプライベート DNS サーバが、クライアント プラットフォームに設定されている DNS サーバとオーバーラップしていないことを確認します。オーバーラップしていると、名前解決が正しく動作せず、クエリーがドロップされる可能性があります。

ステップ 2 Split-Include トンネリングを設定します。

[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [グループ ポリシー（Group Policies）] > [詳細（Advanced）] > [スプリット トンネリング（Split Tunneling）] ペインで、[次のトンネル ネットワーク リスト（Tunnel Network List Below）] を選択し、[ネットワーク リスト（Network List）] にトンネルするアドレスを指定します。

スプリット DNS は、[次のネットワーク リストを除外（Exclude Network List Below）] スプリット トンネリング ポリシーをサポートしません。[次のトンネル ネットワーク リスト（Tunnel Network List Below）] スプリット トンネリング ポリシーを使用して、スプリット DNS を設定します。

ステップ 3 スプリット DNS を設定します。

[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [グループ ポリシー（Group Policies）] > [詳細（Advanced）] > [スプリット トンネリング（Split Tunneling）] ペインで、[トンネルですべての DNS ルックアップを送信する（Send All DNS lookups through tunnel）] をオフにし、クエリーがトンネルされるドメインの名前を [DNS 名（DNS Names）] に指定します。

次のタスク

ASDM でグループ ポリシーに変更を加えたら、[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [AnyConnect 接続プロファイル（AnyConnect Connection Profiles）] > [追加/編集（Add/Edit）] > [グループ ポリシー（Group Policy）] で、グループ ポリシーを接続プロファイルに関連付けてください。

AnyConnect ログを使用したスプリット DNS の確認

スプリット DNS が有効であることを確認するには、AnyConnect のログで、「Received VPN Session Configuration Settings」が含まれたエントリを検索します。このエントリは、スプリット DNS が有効であることを示します。IPv4 と IPv6 のスプリット DNS 用に別々のログ エントリがあります。

スプリット DNS を使用しているドメインの確認

ドメイン名解決には、オペレーティング システムの DNS リゾルバに依存するあらゆるツールまたはアプリケーションを使用できます。たとえば、ping または Web ブラウザを使用してス

プリット DNS ソリューションをテストできます。nslookup または dig などのその他のツールは、OS DNS リゾルバを回避します。

クライアントを使用して、どのドメインがスプリット DNS に使用されているかを確認する手順は次のとおりです。

手順

ステップ 1 **ipconfig/all** を実行して、DNS サフィックス検索リストの横にリストされたドメインを記録します。

ステップ 2 VPN 接続を確立し、DNS サフィックス検索リストの横にリストされたドメインを再度確認します。

トンネルを確立した後に追加されたドメインは、スプリット DNS で使用されるドメインです。

（注） このプロセスは、ASA からプッシュされたドメインと、クライアント ホストで設定済みのドメインがオーバーラップしていないことを前提としています。

VPN 認証の管理

重要なセキュリティ上の考慮事項

- セキュア ゲートウェイ上での自己署名証明書の使用はお勧めしません。理由は、ユーザが誤って不正なサーバ上の証明書を信頼するようにブラウザを設定する可能性があるため、また、ユーザがセキュア ゲートウェイに接続する際に、セキュリティ警告に応答する手間がかかるためです。
- 以下の理由があるため、AnyConnect クライアントに対する厳格な証明書トラストを有効にすることを、強くお勧めします。

  を設定するには、ローカルポリシーパラメータと値（120ページ）の「ローカルポリシーパラメータと値」の項を参照してください。

サーバ証明書処理の設定

サーバ証明書の確認（Server Certificate Verification）

- （Windows のみ）SSL 接続と IPsec VPN 接続の両方で、証明書失効リスト（CRL）チェックを実行するオプションがあります。プロファイルエディタで有効にすると、AnyConnect はチェーン内のすべての証明書を対象とした最新の CRL を取得します。AnyConnect は次に、当該証明書がこれらの信頼できなくなった失効証明書に含まれているかどうかを確認

します。認証局によって失効された証明書であることが判明すると、AnyConnect は接続しません。詳細は、ローカル ポリシー パラメータと値 （120 ページ）を参照してください。

- サーバ証明書が設定された ASA にユーザが接続する場合、信頼チェーン（ルートや中間など）に問題があっても、その証明書を信頼し、インポートするためのチェックボックスは表示されます。証明書にそれ以外の問題がある場合、そのチェックボックスは表示されません。
- FQDN によって実行される SSL 接続では、FQDN を使用した初期検証に失敗した場合、名前検証のために FQDN が IP アドレスに解決されず、セカンダリ サーバの証明書検証が行われません。
- IPSec および SSL 接続では、サーバ証明書にキーの使用状況が含まれる場合、属性に DigitalSignature および（KeyAgreement または KeyEncipherment）が含まれている必要があります。サーバ証明書に EKU が含まれている場合は、属性に serverAuth（SSL および IPSec の場合）または ikeIntermediate（IPsec の場合のみ）が含まれている必要があります。サーバ証明書がなくても、KU または EKU を受け入れることができることに注意してください。
- IPsec および SSL 接続は、サーバ証明書で名前の検証を実行します。IPsec および SSL 名前検証のために次のルールが適用されます。
  - Subject Alternative Name 拡張子が関連する属性に含まれる場合、名前検証は Subject Alternative Name に対してのみ実行されます。関連する属性には、すべての証明書の DNS Name 属性や、接続が IP アドレスに対して実行される場合は、IP アドレスの属性などが含まれます。
  - Subject Alternative Name 拡張子がない場合、または、あっても関連する属性が含まれていない場合、名前検証は、証明書の Subject で見つかった Common Name 属性に対して実行されます。
  - 証明書が名前検証の目的でワイルドカードを使用する場合、そのワイルドカードは最初（左端）のサブドメインのみに含まれなければならず、他に追加する場合はサブドメインの最後（右端）の文字でなければなりません。このルールに準拠していないワイルドカードのエントリは、名前検証の目的では無視されます。
- OS X の場合、期限切れの証明書は、キーチェーン アクセスで [有効期限の切れた証明書を表示（Show Expired Certificates）] が設定されている場合にのみ表示されます。期限切れの証明書は、ユーザの混乱を招く可能性があるため、デフォルトでは表示されません。

無効なサーバ証明書の処理

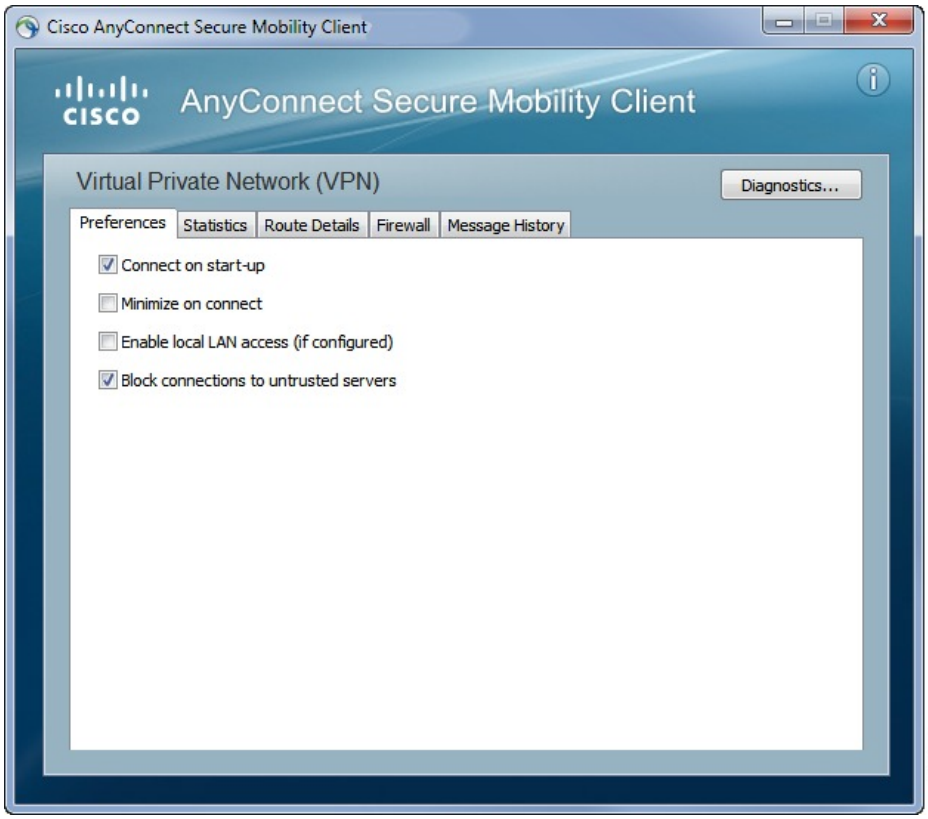
非信頼ネットワーク上のモバイル ユーザを狙った攻撃の増加に対応して、シスコは重大なセキュリティ違反を防ぐため、クライアントのセキュリティ保護を強化しました。デフォルトのクライアントの動作は、中間者攻撃に対する追加の防御レイヤを提供するように変更されました。

ユーザ対話

ユーザがセキュア ゲートウェイに接続しようとしたときに証明書エラーがある場合（期限切れ、無効な日付、キーの誤用、またはCNの不一致による）、[設定の変更（Change Settings）] および [安全を確保（Keep Me Safe）] ボタンを含む赤色のダイアログがユーザに表示されます。

（注） Linux のダイアログは、このマニュアルに示すものと異なる場合があります。

- [安全を確保（Keep Me Safe）] をクリックすると、接続が解除されます。
- [設定の変更（Change Settings）] をクリックすると、AnyConnect の [詳細（Advanced）] > [VPN] > [プリファレンス（Preferences）] ダイアログが開きます。ここで、ユーザは非信頼サーバへの接続を有効にできます。現在の接続の試行がキャンセルされます。



ユーザが、[信頼されていないサーバへの接続をブロック（Block connections to untrusted servers）] をオフにして、証明書に関する問題が CA が信頼できないことのみである場合、次回ユーザがこのセキュア ゲートウェイに接続しようとするときは、ユーザに証明書ブロック エラーのダイアログは表示されず、次のダイアログのみが表示されます。

ユーザが [常にこの VPN サーバを信頼し、証明書をインポートする（Always trust this VPN server and import the certificate）] をオンにしている場合、このセキュア ゲートウェイへの今後の接続時に、ユーザの続行を確認するプロンプトは表示されません。

（注） ユーザが、AnyConnect の [詳細（Advanced）] > [VPN] > [設定（Preferences）] で [信頼されていないサーバへの接続をブロック（Block connections to untrusted servers）] をオンにしている場合、または、ユーザの設定が注意事項と制約事項の項で説明されているモードのリストのいずれかの条件と一致する場合、AnyConnect は無効なサーバ証明書を拒否します。

改善されたセキュリティ動作

クライアントが無効なサーバ証明書を受け入れると、その証明書はクライアントの証明書ストアに保存されます。以前は、証明書のサムプリントだけが保存されました。ユーザが無効なサーバ証明書を常に信頼してインポートすることを選択した場合のみ、無効な証明書が保存されることに注意してください。

エンドユーザの安全性が自動的に損なわれる管理上の優先操作はありません。先行するセキュリティ上の判断をエンド ユーザから完全に排除するには、ユーザのローカル ポリシー ファイルで [厳格な証明書トラスト（Strict Certificate Trust）] を有効にします。[厳格な証明書トラスト（Strict Certificate Trust）] が有効である場合、ユーザにはエラー メッセージが表示され、接続が失敗します。ユーザ プロンプトは表示されません。

ローカルポリシーファイルでの厳格な証明書トラストの有効化については、ローカルポリシーパラメータと値 （120 ページ）の「*AnyConnect* ローカル ポリシー パラメータと値」の項を参照してください。

注意事項と制約事項

無効なサーバ証明書は、次の場合に拒否されます。

- AnyConnect VPN クライアント プロファイルで [常時接続（Always On）] が有効になっており、適用されたグループ ポリシーまたは DAP によりオフにされていない。
- クライアントに、厳格な証明書トラストが有効なローカル ポリシーがある。
- AnyConnect でログイン前の起動が設定されている。
- マシン証明書ストアからのクライアント証明書が認証に使用されている。

Certificate-Only 認証の設定

ユーザ名とパスワードを使用して AAA でユーザを認証するか、デジタル証明書で認証するか（または、その両方を使用するか）を指定する必要があります。証明書のみの認証を設定すると、ユーザはデジタル証明書で接続でき、ユーザ ID とパスワードを入力する必要がなくなります。

複数のグループを使用する環境で証明書のみの認証をサポートする場合は、複数のグループ URL をプロビジョニングします。各グループ URL には、さまざまなクライアント プロファイルとともに、グループ固有の証明書マップを作成するためのカスタマイズ済みデータの一部が含まれます。たとえば、ASA に開発部の Department_OU 値をプロビジョニングし、このプロ

セスによる証明書が ASA に提供されたときに、このグループにユーザを配置するようにできます。

（注） セキュア ゲートウェイに対してクライアントを認証するために使用される証明書は有効であり、（CA によって署名された）信頼できるものである必要があります。自己署名されたクライアント証明書は受け入れられません。

手順

ステップ 1 **[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [AnyConnect 接続プロファイル（AnyConnect Connection Profiles）]** を選択します。接続プロファイルを選択し、[編集（Edit）] をクリックします。[AnyConnect 接続プロファイルの編集（Edit AnyConnect Connection Profile）] ウィンドウが開きます。

ステップ 2 選択されていない場合は、ウィンドウの左ペインにあるナビゲーションツリーの [基本（Basic）] ノードをクリックします。ウィンドウの右ペインにある [認証（Authentication）] 領域で、[証明書（Certificate）] 方式を有効にします。

ステップ 3 [OK] をクリックし、変更を適用します。

証明書登録の設定

Cisco AnyConnect Secure Mobility Clientは、Simple Certificate Enrollment Protocol（SCEP）を使用して、クライアント認証の一部として証明書をプロビジョニングおよび更新します。SCEP を使用した証明書の登録は、ASA への AnyConnect IPsec および SSL VPN 接続で次のようにサポートされます。

- SCEP プロキシ：ASA はクライアントと認証局（CA）間の SCEP 要求と応答のプロキシとして機能します。
  - クライアントが CA に直接アクセスしないため、CA は、AnyConnect クライアントではなく ASA にアクセスできる必要があります。
  - 登録は、クライアントにより常に自動的に開始されます。ユーザの介入は必要ありません。

関連トピック

AnyConnect プロファイル エディタの証明書の登録 （112 ページ）

SCEP プロキシの登録と動作

次の手順では、AnyConnect および ASA が SCEP プロキシ用に設定されている場合に、証明書が取得され、証明書ベースの接続が確立された方法について説明します。

1. ユーザは、証明書と AAA 認証の両方用に設定された接続プロファイルを使用して、ASA ヘッドエンドに接続します。ASA は、クライアントからの認証用に証明書と AAA クレデンシャルを要求します。
2. ユーザが AAA クレデンシャルを入力しますが、有効な証明書は使用可能ではありません。この状況は、入力された AAA クレデンシャルを使用してトンネルが確立された後で、クライアントが自動 SCEP 登録要求を送信するトリガーになります。
3. ASA が CA に対して登録要求を転送し、CA の応答をクライアントに返します。
4. SCEP 登録が成功すると、クライアントにユーザに対する（設定可能な）メッセージが表示され、現行のセッションが接続解除されます。ユーザは、証明書認証を使用して、ASA トンネル グループに接続できます。

   SCEP 登録に失敗した場合、クライアントにユーザに対する（設定可能な）メッセージが表示され、現行のセッションが接続解除されます。ユーザは自分の管理者に連絡する必要があります。

他の SCEP プロキシの動作上の考慮事項：

- そうするように設定されている場合、ユーザが介入することなく、期限切れになる前に証明書がクライアントにより自動的に更新されます。
- SCEP プロキシ登録は、SSL と IPSec トンネルの両方の証明書認証に SSL を使用します。

認証局の要件

- IOS CS、Windows Server 2003 CA、および Windows Server 2008 CA を含め、すべての SCEP 準拠 CA がサポートされています。
- CA は自動付与モードである必要があります。証明書のポーリングはサポートされません。
- 一部の CA について、セキュリティを強化するために、電子メールで登録パスワードをユーザに送信するように設定できます。CA パスワードは、ユーザを識別するための認証局に送信されるチャレンジ パスワードまたはトークンです。このパスワードはその後、AnyConnect クライアント プロファイルで設定できます。これは、CA が証明書を付与する前に確認する、SCEP 要求の一部になります。

証明書登録のガイドライン

- ASA へのクライアントレス（ブラウザ ベース）VPN アクセスは、SCEP プロキシをサポートしていませんが、WebLaunch（クライアントレス起動 AnyConnect）がサポートされます。
- ASA ロード バランシングは、SCEP 登録でサポートされます。
- ASA は、クライアントから受信した要求を記録しますが、登録が失敗した理由は表示しません。接続の問題は、CA またはクライアントでデバッグされる必要があります。
- 証明書のみの認証および ASA での証明書マッピング：

複数のグループを使用する環境で証明書のみの認証をサポートする場合は、複数のグループ URL をプロビジョニングします。各グループ URL には、さまざまなクライアント プロファイルとともに、グループ固有の証明書マップを作成するためのカスタマイズ済みデータの一部が含まれます。たとえば、ASA に開発部の Department_OU 値をプロビジョニングし、このプロセスによる証明書が ASA に提供されたときに、このトンネル グループにユーザを配置するようにできます。

- ポリシーを適用するための登録接続の特定：

  ASA で、登録接続を捕捉し、選択された DAP レコードの適切なポリシーを適用するために、aaa.cisco.sceprequired 属性が使用されます。

- Windows 証明書の警告：

  Windows クライアントが最初に認証局から証明書を取得しようとした際に、警告される可能性があります。プロンプトが表示されたら、[はい（Yes）] をクリックしてください。これにより、ルート証明書をインポートできます。クライアント証明書との接続に影響しません。

SCEP プロキシ証明書登録の設定

SCEP プロキシ登録用 VPN クライアント プロファイルの設定

手順

ステップ 1 VPN プロファイル エディタを開き、ナビゲーション ペインから [証明書の登録（Certificate Enrollment）] を選択します。

ステップ 2 [証明書の登録（Certificate Enrollment）] を選択します。

ステップ 3 登録証明書で、要求する [証明書の内容（Certificate Contents）] を設定します。証明書フィールドの定義については、「AnyConnect プロファイル エディタの証明書の登録」を参照してください。

（注）
- %machineid% を使用した場合は、デスクトップ クライアントに Hostscan/Posture がロードされます。
- モバイル クライアントの場合、証明書フィールドのうち少なくとも 1 つを指定する必要があります。

SCEP プロキシ登録をサポートするための ASA の設定

SCEP プロキシのため、1 つの ASA 接続プロファイルは、証明書登録および認証された VPN 接続をサポートします。

手順

ステップ 1 グループ ポリシー（例：cert_group）を作成します。次のフィールドを設定します。

- [一般（General）] で、[SCEP フォワーディング URL（SCEP Forwarding URL）] に CA への URL を入力します。
- [詳細（Advanced）] > [AnyConnect クライアント（AnyConnect Client）] ペインで、[ダウンロードするクライアント プロファイルの継承（Inherit for Client Profiles to Download）] をオフにし、SCEP プロキシ用に設定されたクライアント プロファイルを指定します。たとえば、ac_vpn_scep_proxy クライアント プロファイルを指定します。

ステップ 2 証明書の登録および接続を認証した証明書（例：cert_tunnel）用の接続プロファイルを作成します。

- [認証（Authentication）]：Both（AAA および Certificate）。
- デフォルトのグループ ポリシー：cert_group。
- [詳細（Advanced）] > [一般（General）] で、[この接続プロファイルへの SCEP 登録を有効にする（Enable SCEP Enrollment for this Connction Profile）] をオンにします。
- [詳細（Advanced）] > [グループエイリアス/グループ URL（GroupAlias/Group URL）] で、この接続プロファイルのグループ（cert_group）が含まれるグループ URL を作成します。

SCEP 用の Windows 2008 Server の認証局の設定

認証局ソフトウェアが Windows 2008 サーバで実行されている場合、AnyConnect で SCEP がサポートされるように次のいずれかの設定変更を行う必要があります。

認証局での SCEP パスワードの無効化

次の手順は、クライアントが SCEP 登録の前にアウトオブバンドパスワードを提供せずに済むように、SCEP チャレンジ パスワードを無効にする方法について説明します。

手順

ステップ 1 認証局サーバで、レジストリ エディタを起動します。これを行うには、**[スタート（Start）]** > **[ファイル名を指定して実行（Run）]** を選択し、**regedit** と入力して [OK] をクリックします。

ステップ 2 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP\EnforcePassword に移動します。

EnforcePassword キーが存在しない場合は、新しいキーとして作成します。

ステップ 3 EnforcePassword を編集し、「0」に設定します。存在しない場合は、REG-DWORD として作成します。

ステップ 4 regedit を終了し、認証局サーバをリブートします。

認証局での SCEP テンプレートの設定

以下の手順では、証明書のテンプレートを作成する方法、およびこれをデフォルト SCEP テンプレートとして割り当てる方法について説明します。

手順

ステップ 1 サーバ マネージャを起動します。これは、[スタート（Start）] > [管理ツール（Admin Tools）] > [サーバ マネージャー（Server Manager）] を選択することで実行できます。

ステップ 2 [役割（Expand Roles）] > [証明書サービス（Certificate Services）]（または [Active Directory 証明書サービス（AD Certificate Services）]）を展開します。

ステップ 3 CA の名前 > [証明書テンプレート（Certificate Templates）] に移動します。

ステップ 4 [証明書テンプレート（Certificate Templates）] > [管理（Manage）] を右クリックします。

ステップ 5 [証明書テンプレート コンソール（Cert Templates Console）] から、ユーザ テンプレートを右クリックして [複製（Duplicate）] を選択します。

ステップ 6 新しいテンプレートの [Windows Server 2008] バージョンを選択して、[OK] をクリックします。

ステップ 7 テンプレートの表示名を、NDES IPsec SSL など、具体的な説明に変更します。

ステップ 8 サイトの有効期間を調整します。ほとんどのサイトでは、証明書の期限切れを避けるために 3 年以上を選択します。

ステップ 9 [Cryptography] タブで、展開の最小キー サイズを設定します。

ステップ 10 [サブジェクト名（Subject Name）] タブで、[要求に含まれる（Supply in Request）] を選択します。

ステップ 11 [拡張機能（Extensions）] タブで、[アプリケーションのポリシー（Application Policies ）] に少なくとも次が含まれるように設定します。

- クライアント認証
- IP セキュリティ末端システム
- IP セキュリティ IKE 中間
- IP セキュリティ トンネル終端
- IP セキュリティ ユーザ

これらの値は、SSL または IPSec に有効です。

ステップ 12 [適用（Apply）] をクリックして、次に [OK] をクリックして新しいテンプレートを保存します。

ステップ 13 サーバ マネージャから [証明書サービス（Certificate Services）] に移動して CA の名前を選択し、[証明書テンプレート（Certificate Templates）] を右クリックします。[新規（New ）] > [発

行する証明書テンプレート（Certificate Template to Issue）] を選択し、作成した新しいテンプレートを選択します（この例では NDES-IPSec-SSL）。次に、[OK] をクリックします。

ステップ 14 レジストリを編集します。これは、[スタート（Start）]>[ファイル名を指定して実行（Run）] で regedit と入力し、[OK] をクリックすることで実行できます。

ステップ 15 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP に移動します。

ステップ 16 次の 3 つのキーの値を、NDES-IPSec-SSL に設定します。

- EncryptionTemplate
- GeneralPurposeTemplate
- SignatureTemplate

ステップ 17 [保存（Save）] をクリックして、認証局サーバをリブートします。

証明書失効通知の設定

認証証明書が間もなく期限切れになることをユーザに警告するよう AnyConnect を設定します。[証明書失効しきい値（Certificate Expiration Threshold）] の設定では、AnyConnect がユーザに対して証明書の失効が近づいていることを証明書の有効期限の何日前に警告するかを指定します。AnyConnect は、証明書が実際に期限切れか、新しい証明書が取得されるまで、ユーザが接続するたびに警告します。

（注） RADIUS 登録では、[証明書失効しきい値（Certificate Expiration Threshold）] 機能は使用できません。

手順

ステップ 1 VPN プロファイル エディタを開き、ナビゲーション ペインから [証明書の登録（Certificate Enrollment）] を選択します。

ステップ 2 [証明書の登録（Certificate Enrollment）] を選択します。

ステップ 3 [証明書失効しきい値（Certificate Expiration Threshold）] を指定します。

AnyConnect がユーザに対して証明書の失効が近づいていることを証明書の有効期限の何日前に警告するかを示す数字です。

デフォルトは 0（警告は表示しない）です。範囲は 0 ～ 180 日です。

ステップ 4 [OK] をクリックします。

証明書選択の設定

次の手順では、クライアント システムで証明書を検索する方法および証明書を選択する方法を設定する、AnyConnect プロファイル内のすべての場所を示します。いずれの手順も必須ではなく、条件を指定しなかった場合、AnyConnect はデフォルトのキー照合を使用します。

Windows では、AnyConnect はブラウザの証明書ストアを読み取ります。Linux の場合、プライバシー強化メール（PEM）形式のファイル ストアを作成する必要があります。macOS の場合、プライバシー強化メール（PEM）形式のファイル ストアまたはキーチェーンを使用できます。

手順

ステップ 1 Windows および macOS の場合：使用する証明書ストアの設定 （177 ページ）

VPN クライアント プロファイルに AnyConnect で使用される証明書ストアを指定します。

ステップ 2 Windows のみ：Windows ユーザに認証証明書の選択を求めるプロンプトの表示 （180 ページ）

ユーザに有効な証明書のリストを示すように AnyConnect を設定し、ユーザがセッションの認証にその証明書を選択できるようにします。

ステップ 3 macOS および Linux 環境の場合：macOS および Linux での PEM 証明書ストアの作成 （181 ページ）

ステップ 4 macOS および Linux 環境の場合：VPN ローカル ポリシー プロファイルで除外する証明書ストアを選択します。

ステップ 5 証明書照合の設定 （182 ページ）

ストアの証明書を検索する場合に、AnyConnect が照合を試みるキーを設定します。キー（拡張キー）を指定し、カスタム拡張キーを追加できます。また、AnyConnect が照合する識別名に演算子の値のパターンを指定できます。

使用する証明書ストアの設定

Windows および macOS では、AnyConnect が VPN クライアント プロファイルで使用するための別の証明書ストアが提供されます。1 つまたは複数の証明書認証の組み合わせが可能で、複数の証明書認証の選択肢のうち特定の VPN 接続において許容されるものをクライアントに指定するようにセキュア ゲートウェイを設定できます。たとえば、ローカル ポリシー ファイルで ExcludeMacNativeCertStore を *true* に設定（AnyConnect がユーザ ファイル証明書ストアやシステム ファイル証明書ストアなどのファイル証明書ストアのみを使用するよう強制）し、プロファイル ベースの証明書ストアを [ログイン（Login）] に設定（AnyConnect が、ユーザ ファイル ストアに加え、ログイン キーチェーンおよびダイナミック スマートカード キーチェーンなどの証明書ストアのみを使用するよう強制）すると、その組み合わせによるフィルタリングにより、AnyConnect は、厳格にユーザ ファイル証明書ストアを使用するようになります。

コンピュータ上で管理者権限を持つユーザは、両方の証明書ストアにアクセスできます。管理者権限を持たないユーザがアクセスできるのは、ユーザ証明書ストアのみです。通常、Windows

ユーザには管理者権限がありません。[証明書ストアの上書き（Certificate Store Override）] を選択すると、ユーザに管理者権限がない場合でも、AnyConnect はマシン ストアにアクセスできます。

（注） マシン ストアのアクセス制御は、Windows のバージョンとセキュリティ設定によって異なる場合があります。このため、ユーザは管理者権限を持つ場合にも、マシン ストアの証明書を使用できない可能性があります。この場合、[証明書ストアの上書き（Certificate Store Override）] を選択してマシン ストアへのアクセスを許可します。

次の表に、検索対象の [証明書ストア（Certificate Store）] および [証明書ストアの上書き（Certificate Store Override）] のオン/オフに基づいて AnyConnect がクライアントで証明書を検索する方法について説明します。

[証明書ストア（Certificate Store）] の設定	**[証明書ストアの上書き（Certificate Store Override）] の設定**	**AnyConnect の検索方法**
[すべて（All）]（Windows 用）	オフ	AnyConnect は、すべての証明書ストアを検索します。ユーザに管理者権限がない場合、AnyConnect は、マシン ストアにアクセスできません。 この設定は、デフォルトです。この設定は、ほとんどの状況に適しています。変更が必要となる特別な理由またはシナリオ要件がある場合を除いて、この設定は変更しないでください。
[すべて（All）]（Windows 用）	オン	AnyConnect は、すべての証明書ストアを検索します。ユーザに管理者権限がない場合、AnyConnect は、マシン ストアにアクセスできます。
[すべて（All）]（macOS 用）	オン	AnyConnect は、利用可能なすべての macOS キーチェーンおよびファイル ストアからの証明書を使用します。

[証明書ストア（Certificate Store）] の設定	[証明書ストアの上書き（Certificate Store Override）] の設定	AnyConnect の検索方法
[ユーザ（User）]（Windows 用）	適用せず	AnyConnect は、ユーザ証明書ストア内のみ検索します。管理者権限のないユーザがこの証明書ストアにアクセスできるため、証明書ストアの上書きは適用されません。
[システム（System）]（macOS 用）	オン	AnyConnect は macOS システム キーチェーンとシステム ファイル/PEM ストアからの証明書のみを使用します。macOS システム キーチェーンとシステム ファイル/PEM ストアからの証明書のみを使用します。
[ログイン（Log in）]（macOS 用）	オン	AnyConnect は、ユーザ ファイル/PEM ストアに加え、macOS ログイン キーチェーンおよびダイナミック スマートカード キーチェーンからの証明書のみを使用します。

複数証明書認証の使用

始める前に

- デスクトップ プラットフォーム（Windows、OS X、Linux）でのみサポートされます。
- VPN プロファイルで *AutomaticCertSelection* を有効にしている必要があります。
- VPNプロファイルで設定した証明書照合設定によって、複数証明書認証で使用できる証明書が制限されます。

（注） SCEP はサポートされていません。

手順

ステップ 1 [証明書ストア（Certificate Store）] を設定します。

- 1 マシンおよび 1 ユーザ証明書の場合は、VPN プロファイルで CertificateStore を [すべて（All）] に設定し、ステップ 2 の説明に従って *CertficateStoreOverride* を有効にします。
- 2 ユーザ証明書の場合は、VPN プロファイルで CertificateStore を [すべて（All）] または [ユーザ（User）] に設定しますが、ステップ 2 の説明に従って *CertificateStoreOverride*.はそのままにします。

ステップ 2 ユーザに管理者権限がない場合に AnyConnect にマシン証明書ストアの検索を許可するには、**証明書ストアの上書き** を選択します。

基本的な証明書認証の使用

手順

ステップ 1 [証明書ストア（Certificate Store）] を設定します。

- [すべて（All）] :（デフォルト）すべての証明書ストアを使用して証明書を検索するよう AnyConnect クライアントに指示します。
- [マシン（Machine）] : 証明書ルックアップを Windows ローカル マシン証明書ストアに制限するように AnyConnect クライアントに指示します。
- [ユーザ（User）] : 証明書ルックアップをローカル ユーザ証明書ストアに制限するように AnyConnect クライアントに指示します。

ステップ 2 ユーザに管理者権限がない場合に AnyConnect にマシン証明書ストアの検索を許可するには、**証明書ストアの上書き** を選択します。

Windows ユーザに認証証明書の選択を求めるプロンプトの表示

ユーザに対して有効な証明書のリストを表示し、セッションの認証に使用する証明書をユーザが選択できるように AnyConnect を設定できます。期限切れの証明書は必ずしも無効として見なされるわけではありません。たとえば SCEP を使用している場合、サーバが新しい証明書をクライアントに発行することがあります。期限切れの証明書を削除すると、クライアントがまったく接続できなくなることがあります。この場合、手動による介入とアウトオブバンド証明書配布が必要になります。AnyConnect では、設定されている証明書一致ルールに基づき、セキュリティ関連プロパティ（キーの使用状況、キーのタイプと強度など）に基づいて、クライアント証明書が制限されるだけです。この設定は Windows でのみ使用できます。デフォルトでは、ユーザによる証明書の選択は無効です。

手順

ステップ 1 VPN プロファイル エディタを開き、ナビゲーション ペインから [プリファレンス（Part 2）（Preferences (Part 2)）] を選択します。

ステップ 2 証明書の選択を有効にするには、[証明書選択を無効にする（Disable Certificate Selection）] チェックボックスをオフにします。

ステップ 3 **[詳細（Advanced）] > [VPN] > [プリファレンス（Preferences）]** ペインでユーザが自動証明書の選択のオン/オフを切り替えられるようにする場合を除き、[ユーザ制御可（User Controllable）] チェックボックスをオフにします。

macOS および Linux での PEM 証明書ストアの作成

AnyConnect では、プライバシー強化メール（PEM）形式のファイル ストアからの証明書取得がサポートされています。AnyConnect はリモート コンピュータのファイル システムから PEM 形式の証明書ファイルを読み取り、確認と署名を行います。

始める前に

あらゆる条件下でクライアントが適切な証明書を取得するためには、ファイルが次の要件を満たしている必要があります。

- すべての証明書ファイルは、拡張子 .pem で終わっていること。
- すべての秘密キー ファイルは、拡張子 .key で終わっていること。
- クライアント証明書と、それに対応する秘密キーのファイル名が同じであること（client.pem と client.key など）。

ヒント PEM ファイルのコピーを保持する代わりに、PEM ファイルへのソフト リンクを使用できます。

PEM ファイル証明書ストアを作成する場合は、次に示すパスとフォルダを作成します。これらのフォルダに、適切な証明書を配置してください。

PEM ファイル証明書ストアのフォルダ	保存される証明書のタイプ
~/.cisco/certificates/ca （注） .cisco/ はホーム ディレクトリにあります。	信頼できる CA とルート証明書
~/.cisco/certificates/client	クライアント証明書
~/.cisco/certificates/client/private	秘密キー

マシン証明書は、ルート ディレクトリ以外は PEM ファイル証明書と同じです。マシン証明書の場合は、~/.cisco を /opt/.cisco に置き換えてください。それ以外は、パス、フォルダ、および証明書のタイプが適用されます。

証明書照合の設定

AnyConnect では、特定のキーのセットに一致するこれらの証明書に証明書の検索を限定できます。証明書照合は、[証明書照合（Certificate Matching）] ペインの AnyConnect VPN クライアント プロファイルで設定できるグローバル基準です。基準は次のとおりです。

- [キーの使用状況（Key Usage）]
- [拡張キーの使用状況（Extended Key Usage）]
- [識別名（Distinguished Name）]

関連トピック

AnyConnect プロファイル エディタの証明書照合 （109 ページ）

キーの使用状況の設定

[キーの使用状況（Key Usage）] キーを選択すると、AnyConnect で使用できる証明書が、選択したキーの少なくとも 1 つを持つ証明書に制限されます。サポート対象のセットは、VPN クライアント プロファイルの [キーの使用状況（Key Usage）] リストに一覧表示されており、次が含まれています。

- DECIPHER_ONLY
- ENCIPHER_ONLY
- CRL_SIGN
- KEY_CERT_SIGN
- KEY_AGREEMENT
- DATA_ENCIPHERMENT
- KEY_ENCIPHERMENT
- NON_REPUDIATION
- DIGITAL_SIGNATURE

1 つ以上の基準が指定されている場合、証明書が一致すると見なされるには、少なくとも 1 つの基準が一致している必要があります。

拡張キーの使用状況の設定

[拡張キーの使用状況（Extended Key Usage）] キーを選択すると、AnyConnect で使用できる証明書がこれらのキーを持つ証明書に限定されます。次の表は、既知の制約のセットと、それに対応するオブジェクト ID（OID）をリストにまとめたものです。

制約	OID
ServerAuth	1.3.6.1.5.5.7.3.1
ClientAuth	1.3.6.1.5.5.7.3.2
CodeSign	1.3.6.1.5.5.7.3.3
EmailProtect	1.3.6.1.5.5.7.3.4
IPSecEndSystem	1.3.6.1.5.5.7.3.5
IPSecTunnel	1.3.6.1.5.5.7.3.6
IPSecUser	1.3.6.1.5.5.7.3.7
TimeStamp	1.3.6.1.5.5.7.3.8
OCSPSign	1.3.6.1.5.5.7.3.9
DVCS	1.3.6.1.5.5.7.3.10
IKE Intermediate	1.3.6.1.5.5.8.2.2

カスタム拡張照合キーの設定

その他の OID（本書の例で使用している 1.3.6.1.5.5.7.3.11 など）はすべて、「カスタム」と見なされます。管理者は、既知のセットの中に必要な OID がない場合、独自の OID を追加できます。

証明書識別名の設定

[識別名（Distinguished Name）] の表には、クライアントが使用できる証明書を指定の条件に一致する証明書に限定する証明書 ID、および一致条件が含まれています。条件をリストに追加したり、追加した条件の内容と照合するための値またはワイルドカードを設定したりするには、[追加（Add）] ボタンをクリックします。

ID	説明
CN	SubjectCommonName
SN	SubjectSurName
GN	SubjectGivenName
N	SubjectUnstructName
I	SubjectInitials
GENQ	SubjectGenQualifier
DNQ	SubjectDnQualifier
C	SubjectCountry

ID	説明
L	SubjectCity
SP	SubjectState
ST	SubjectState
O	SubjectCompany
OU	SubjectDept
T	SubjectTitle
EA	SubjectEmailAddr
DC	DomainComponent
ISSUER-CN	IssuerCommonName
ISSUER-SN	IssuerSurName
ISSUER-GN	IssuerGivenName
ISSUER-N	IssuerUnstructName
ISSUER-I	IssuerInitials
ISSUER-GENQ	IssuerGenQualifier
ISSUER-DNQ	IssuerDnQualifier
ISSUER-C	IssuerCountry
ISSUER-L	IssuerCity
ISSUER-SP	IssuerState
ISSUER-ST	IssuerState
ISSUER-O	IssuerCompany
ISSUER-OU	IssuerDept
ISSUER-T	IssuerTitle
ISSUER-EA	IssuerEmailAddr
ISSUER-DC	IssuerDomainComponent

[識別名（Distinguished Name）] には、0 個以上の一致基準を含めることができます。証明書が一致すると見なされるには、指定されているすべての基準に一致している必要があります。[識別名（Distinguished Name）] の一致では、証明書に指定の文字列が含まれている必要があるかどうか、および文字列にワイルドカードを許可するかどうかを指定します。

SAML を使用した VPN 認証

最初のセッション認証にASAリリース9.7.1と統合されたSAML2.0を使用できます。AnyConnect 4.6では、組み込みブラウザとのSAML統合が拡張され、これが以前のリリースからのネイティブ（外部）ブラウザ統合に置き換わります。SAML認証用に設定されたトンネル グループに接続するときに、AnyConnectは組み込みブラウザ ウィンドウを開いて認証プロセスを完了します。SAML試行のたびに新しいブラウザ セッションが使用され、ブラウザ セッションはAnyConnectに固有のものとなります（セッション状態は、他のどのブラウザとも共有されません）。各SAML認証試行はセッション状態なしで始まりますが、試行間で永続クッキーが保持されます。

プラットフォーム固有の要件

組み込みブラウザでSAMLを使用するためには、次のシステム要件を満たす必要があります。

- Windows：Windows 7（またはそれ以降）、Internet Explorer 11（またはそれ以降）
- macOS：macOS 10.10（またはそれ以降）（AnyConnectは、macOS 10.11以降を公式にサポートしています）
- Linux：WebKitGTK+ 2.1x（それ以降）、Red Hat 7.4（それ以降）およびUbuntu 16.04（それ以降）の公式パッケージ

アップグレード プロセス

ネイティブ（外部）ブラウザ搭載のSAML 2.0は、AnyConnect 4.4とAnyConnect 4.5、およびASAリリース9.7.x、9.8.x、および9.9.1で使用できます。組み込みブラウザを搭載した新しい拡張バージョンを使用するには、AnyConnect 4.6およびASA 9.7.1.24（またはそれ以降）、9.8.2.28（またはそれ以降）、または9.9.2.1（またはそれ以降）へのアップグレードが必要です。

組み込みブラウザSAML統合を備えたヘッドエンドまたはクライアント デバイスをアップグレードまたは展開するときには、次のシナリオに注意してください。

- AnyConnect 4.6を最初に展開した場合は、他に何も操作しなくても、ネイティブ（外部）ブラウザと組み込みブラウザの両方のSAML統合が想定どおりに機能します。AnyConnectを最初に展開するときでも、AnyConnect 4.6は既存のASAバージョンも更新されたASAバージョンもサポートします。
- 更新されたASAバージョン（組み込みブラウザSAML統合を搭載）を最初に展開する場合は、続いてAnyConnectをアップグレードする必要があります。デフォルトでは、更新されたASAリリースは、AnyConnect 4.6よりも前のリリースのネイティブ（外部）ブラウザSAML統合と後方互換性がないためです。認証後に既存のAnyConnect 4.4または4.5クライアントのアップグレードが発生し、このアップグレードを行うためには、トンネルグループ設定で **saml external-browser** コマンドを有効にする必要があります。

SAMLを使用する場合は、次の注意事項に従ってください。

- フェールオーバー モードで常時接続の VPN を使用している場合、外部 SAML IdP はサポートされていません（ただし、内部 SAML IdP を使用すると、ASA はすべてのトラフィックを IdP にプロキシします。また、ASA はサポートされています）。
- 信頼できないサーバ証明書は、組み込みブラウザでは許可されません。
- 組み込みブラウザ SAML 統合は、CLI モードまたは SBL モードではサポートされません。
- （モバイルのみ）単一ログアウトはサポートされていません。
- Web ブラウザに確立された SAML 認証は AnyConnect と共有されず、その逆も同じです。
- 設定に応じて、組み込みブラウザ搭載のヘッドエンドに接続するときに、さまざまな方法が使用されます。たとえば、AnyConnect では IPv6 接続よりも IPv4 接続の方が好ましく、組み込みブラウザでは IPv6 の方が好ましい場合もあります。あるいは、その逆もあります。同じく、プロキシを試して障害が発生したのに AnyConnect がどのプロキシにもフォールバックしない場合もあれば、プロキシを試して障害が発生した後で組み込みブラウザがナビゲーションを停止する場合もあります。
- SAML 機能を使用するためには、ASA の Network Time Protocol（NTP）サーバを IdP NTP サーバと同期する必要があります。
- ASDM の VPN ウィザードは現在、SAML 設定をサポートしていません。
- SAML IdP *NameID* 属性は、ユーザのユーザ名を特定し、認証、アカウンティング、および VPN セッション データベースに使用されます。
- ユーザが SAML 経由で VPN セッションを確立するたびにアイデンティティ プロバイダー（IdP）による再認証を行う場合は、AnyConnect プロファイル エディタ、プリファレンス（Part 1） （97 ページ）で [自動再接続（Auto Reconnect）] を *ReconnectAfterResume* に設定する必要があります。
- 組み込みブラウザ搭載の AnyConnect は VPN 試行のたびに新しいブラウザ セッションを使用するため、IDP が HTTP セッション クッキーを使用してログオン状態を追跡している場合には、毎回ユーザの再認証が必要になります。この場合、**[設定（Configuration）] > [リモートアクセスVPN（Remote Access VPN）] > [クライアントレスSSL VPNアクセス（Clientless SSL VPN Access）] > [詳細（Advanced）] > [シングルサインオンサーバ（Single Sign On Servers）]** > の [強制再認証（Force Re-Authentication）] は、AnyConnect が開始した SAML 認証には影響しません。

設定の詳細については、適切なリリース（9.7 以降）の『Cisco ASA Series VPN Configuration Guide』の「*SSO Using SAML 2.0*」の項を参照してください。

SDI トークン（SoftID）統合を使用した VPN 認証

AnyConnect は、Windows 7 x86（32 ビット）および x64（64 ビット）で動作する RSA SecurID クライアント ソフトウェア バージョン 1.1 以降のサポートを統合します。

RSA SecurID ソフトウェア オーセンティケータは、企業の資産へのセキュアなアクセスのために必要となる管理項目数を減らします。リモート デバイスに常駐する RSA SecurID Software

Token は、1 回限定で使用可能なパスコードを 60 秒ごとにランダムに生成します。SDI は Security Dynamics 社製テクノロジーの略称で、ハードウェアとソフトウェアの両方のトークンを使用する、この 1 回限定利用のパスワード生成テクノロジーを意味します。

通常、ユーザはツール トレイの [AnyConnect] アイコンをクリックし、接続する接続プロファイルを選択してから、認証ダイアログボックスに適切なクレデンシャルを入力することで AnyConnect に接続します。ログイン（チャレンジ）ダイアログボックスは、ユーザが属するトンネル グループに設定されている認証タイプと一致しています。ログイン ダイアログボックスの入力フィールドには、どのような種類の入力が認証に必要か明確に示されます。

SDI 認証では、リモート ユーザは AnyConnect ソフトウェア インターフェイスに PIN（個人識別番号）を入力して RSA SecurID パスコードを受け取ります。セキュアなアプリケーションにパスコードを入力すると、RSA Authentication Manager がこのパスコードを確認してユーザにアクセスを許可します。

RSA SecurID ハードウェアまたはソフトウェアのトークンを使用するユーザには、パスコードまたは PIN、PIN、パスコードのいずれかを入力する入力フィールドが表示されます。ダイアログボックス下部のステータス行には、さらにこの点に関連する情報が表示されます。ユーザは、ソフトウェア トークンの PIN またはパスコードを AnyConnect ユーザ インターフェイスに直接入力します。

最初に表示されるログイン ダイアログボックスの外観は、セキュア ゲートウェイの設定によって異なります。セキュア ゲートウェイには、メインのログイン ページ、メインのインデックス URL、トンネル グループのログイン ページ、またはトンネル グループの URL（URL/トンネル グループ）からアクセスできます。メインのログイン ページからセキュア ゲートウェイにアクセスするには、[ネットワーク（クライアント）アクセス（Network (Client) Access）] の [AnyConnect 接続プロファイル（AnyConnect Connection Profiles）] ページで [ユーザに接続の選択を許可する（Allow user to select connection）] チェックボックスをオンにする必要があります。いずれの方法でも、セキュア ゲートウェイはクライアントにログイン ページを送信します。メインのログイン ページにはドロップダウン リストがあり、ここからトンネル グループを選択します。トンネルグループ ログイン ページにはこの表示はありません。トンネルグループは URL で指定されるためです。

（接続プロファイルまたはトンネル グループのドロップダウン リストが表示される）メインのログイン ページの場合、デフォルト トンネル グループの認証タイプによって、パスワードの入力フィールド ラベルの初期設定が決まります。たとえば、デフォルト トンネル グループが SDI 認証を使用する場合、フィールド ラベルは [パスコード（Passcode）] になります。一方で、デフォルト トンネル グループが NTLM 認証を使用する場合、フィールド ラベルは [パスワード（Password）] になります。リリース 2.1 以降では、異なるトンネル グループをユーザが選択しても、フィールド ラベルが動的に更新されることはありません。トンネルグループのログイン ページでは、フィールド ラベルはトンネルグループの要件に一致します。

クライアントは、パスワード入力フィールドへの RSA SecurID Software Token の PIN の入力をサポートします。RSA SecurID Software Token ソフトウェアがインストールされており、トンネルグループ認証タイプが SDI の場合、フィールド ラベルは [パスコード（Passcode）] となり、ステータス バーには、「ユーザ名およびパスコードまたはソフトウェア トークンPINを入力してください（Enter a username and passcode or software token PIN）」と表示されます。PIN を使用すると、同じトンネル グループおよびユーザ名で行う次回のログインからは、フィール

ド ラベルが [PIN] になります。クライアントは、入力された PIN を使用して RSA SecurID Software Token DLL からパスコードを取得します。認証が成功するたびにクライアントはトンネル グループ、ユーザ名、認証タイプを保存し、保存されたトンネル グループが新たにデフォルトのトンネル グループとなります。

AnyConnect では、すべての SDI 認証でパスコードを使用できます。パスワード入力ラベルが [PIN] の場合でも、ユーザはステータス バーの指示どおりにパスコードを入力することができます。クライアントは、セキュア ゲートウェイにパスコードをそのまま送信します。パスコードを使用すると、同じトンネル グループおよびユーザ名で行う次回のログインからは、ラベルが [Passcode] のフィールドが表示されます。

RSASecureIDIntegration プロファイル設定は、次の 3 つの値のいずれかになります。

- Automatic：クライアントはまず 1 つの方式を試行し、それが失敗したら別の方式を試行します。デフォルトでは、ユーザ入力がトークン パスコード（HardwareToken）として処理され、これが失敗したら、ユーザ入力がソフトウェア トークン PIN（SoftwareToken）として処理されます。認証が成功すると、成功した方式が新しい SDI トークン タイプとして設定され、ユーザ プリファレンス ファイルにキャッシュされます。SDI トークン タイプは、次回の認証試行でいずれの方式が最初に試行されるかを定義します。通常、現行の認証試行には、最後に成功した認証試行で使用されたトークンと同じものが使用されます。ただし、ユーザ名またはグループの選択を変更した場合は、入力フィールド ラベルに示されている、デフォルトの方式が最初に試行される状態に戻ります。

  （注） SDI トークン タイプは、設定が自動の場合のみ、意味を持ちます。認証モードが自動以外の場合は、SKI トークン タイプのログを無視できます。HardwareToken がデフォルトの場合、次のトークン モードはトリガーされません。

- SoftwareToken：クライアントは、ユーザ入力を常にソフトウェア トークン PIN として解釈し、入力フィールド ラベルは [PIN:] になります。
- HardwareToken：クライアントは、ユーザ入力を常にトークン パスコードとして解釈し、入力フィールド ラベルは [Passcode:] になります。

（注） AnyConnect では、RSA Software Token クライアント ソフトウェアにインポートした複数のトークンからの、トークンの選択はサポートされていません。その代わりに、クライアントは RSA SecurID Software Token GUI を介してデフォルト選択のトークンを使用します。

SDI 認証交換のカテゴリ

すべての SDI 認証交換は次のいずれかのカテゴリに分類されます。

- 通常の SDI 認証ログイン
- 新規ユーザ モード

- 新規 PIN モード
- PIN クリア モード
- 次のトークン コード モード

通常の SDI 認証ログイン

通常ログイン チャレンジは、常に最初のチャレンジです。SDI認証ユーザは、ユーザ名およびトークン パスコード（ソフトウェア トークンの場合は PIN）を、ユーザ名とパスコードまたはPINフィールドにそれぞれ指定する必要があります。クライアントはユーザの入力に応じてセキュア ゲートウェイ（中央サイトのデバイス）に情報を返し、セキュア ゲートウェイはこの認証を認証サーバ（SDI または RADIUS プロキシ経由の SDI）で確認します。

認証サーバが認証要求を受け入れた場合、セキュア ゲートウェイは認証が成功したページをクライアントに送信します。これで認証交換が完了します。

パスコードが拒否された場合は認証は失敗し、セキュア ゲートウェイは、エラー メッセージとともに新しいログイン チャレンジ ページを送信します。SDI サーバでパスコード失敗しきい値に達した場合、SDI サーバはトークンを次のトークン コード モードに配置します。

新規ユーザ モード、PIN クリア モード、および新規 PIN モード

PIN のクリアは、ネットワーク管理者だけの権限で、SDI サーバでのみ実行できます。

新規ユーザ モード、PIN クリア モード、新規 PIN モードでは、AnyConnect は、後の「next passcode」ログイン チャレンジで使用するために、ユーザ作成 PIN またはシステムが割り当てた PIN をキャッシュに入れます。

PIN クリア モードと新規ユーザ モードは、リモート ユーザから見ると違いがなく、また、セキュア ゲートウェイでの処理も同じです。いずれの場合も、リモート ユーザは新しい PIN を入力するか、SDI サーバから割り当てられる新しい PIN を受け入れる必要があります。唯一の相違点は、最初のチャレンジでのユーザの応答です。

新規PINモードでは、通常のチャレンジと同様に、既存のPINを使用してパスコードが生成されます。PIN クリア モードでは、ユーザがトークン コードだけを入力するハードウェア トークンとして PIN が使用されることはありません。RSA ソフトウェア トークンのパスコードを生成するために 0 が 8 つ並ぶ PIN（00000000）が使用されます。いずれの場合も、SDI サーバ管理者は、使用すべき PIN 値（ある場合）をユーザに通知する必要があります。

新規ユーザをSDIサーバに追加すると、既存ユーザのPINをクリアする場合と同じ結果になります。いずれの場合も、ユーザは新しいPINを指定するか、SDIサーバから割り当てられる新しい PIN を受け入れる必要があります。これらのモードでは、ユーザはハードウェア トークンとして、RSA デバイスのトークン コードのみ入力します。いずれの場合も、SDI サーバ管理者は、使用すべき PIN 値（ある場合）をユーザに通知する必要があります。

新規 PIN の作成

現行の PIN がない場合、システム設定に応じて、次の条件のいずれかを満たすことが、SDI サーバによって要求されます。

- システムがユーザに新規 PIN を割り当てる必要がある（デフォルト）。
- ユーザは新規 PIN を作成する必要がある。
- ユーザは、PIN を作成するか、システムの割り当てを受け入れるかを選択できる。

PIN をリモート ユーザ自身で作成する方法とシステムで割り当てる方法を選択できるように SDI サーバを設定している場合、ログイン画面にはオプションを示すドロップダウン リストが表示されます。ステータス行にプロンプト メッセージが表示されます。

システムが割り当てる PIN の場合、ユーザがログイン ページで入力したパスコードを SDI サーバが受け入れると、セキュア ゲートウェイはシステムが割り当てた PIN をクライアントに送信します。クライアントは、ユーザが新規 PIN を確認したことを示す応答をセキュア ゲートウェイに返し、システムは「next passcode」チャレンジに進みます。

ユーザが新しく PIN を作成するように選択した場合、AnyConnect にこの PIN を入力するためのダイアログボックスが表示されます。PIN は 4 ～ 8 桁の長さの数値にする必要があります。PIN は一種のパスワードであるため、ユーザがこの入力フィールドに入力する内容はアスタリスクで表示されます。

RADIUS プロキシを使用する場合、PIN の確認は、最初のダイアログボックスの次に表示される、別のチャレンジで行われます。クライアントは新しい PIN をセキュア ゲートウェイに送信し、セキュア ゲートウェイは「next passcode」チャレンジに進みます。

「next passcode」チャレンジと「next Token Code」チャレンジ

「next passcode」チャレンジでは、クライアントが新規 PIN の作成または割り当て時にキャッシュに入れられた PIN 値を使用して RSA SecurID Software Token DLL から次のパスコードを取得し、ユーザにプロンプト表示せずにこれをセキュア ゲートウェイに返します。同様に、ソフトウェア トークン用の「next Token Code」チャレンジでは、クライアントは RSA SecurID Software Token DLL から次のトークン コードを取得します。

ネイティブ SDI と RADIUS SDI の比較

ネットワーク管理者は、SDI認証を可能にするセキュア ゲートウェイを次のいずれかのモードで設定することができます。

- ネイティブ SDI：SDI サーバと直接通信して SDI 認証を処理できるセキュア ゲートウェイのネイティブ機能です。
- RADIUS SDI：RADIUS SDI プロキシを使用して SDI サーバと通信することで SDI 認証を行うセキュア ゲートウェイのプロセスです。

リモート ユーザからは、ネイティブ SDI と RADIUS SDI は同一です。SDI メッセージは SDI サーバ上で設定が可能なため、これには、ASA 上のメッセージ テキストは、SDI サーバ上のメッセージテキストに一致する必要があります。一致しない場合、リモートクライアントユーザに表示されるプロンプトが、認証中に必要なアクションに対して適切でない場合があります。この場合、AnyConnect が応答できずに認証に失敗することがあります。

RADIUS SDI チャレンジは、少数の例外はありますが、基本的にはミラー ネイティブの SDI 交換です。両者とも最終的には SDI サーバと通信するため、クライアントからの必要な情報と要求される情報の順序は同じです。

認証の間に、RADIUS サーバは ASA にアクセス チャレンジ メッセージを提示します。これらのチャレンジ メッセージ内に、SDI サーバからのテキストを含む応答メッセージがあります。このメッセージ テキストは、ASA が SDI サーバと直接通信している場合と RADIUS プロキシを経由して通信している場合とで異なります。そのため、AnyConnect にネイティブ SDI サーバとして認識させるために、ASA は RADIUS サーバからのメッセージを解釈する必要があります。

また、SDI メッセージは SDI サーバで設定可能であるため、ASA のメッセージ テキストの全体または一部が、SDI サーバのメッセージテキストと一致する必要があります。一致しない場合、リモート クライアント ユーザに表示されるプロンプトが、認証中に必要とされるアクションに対して適切でない場合があります。この場合、AnyConnect が応答できずに認証に失敗することがあります。

RADIUS/SDI メッセージをサポートするための ASA の設定

SDI 固有の RADIUS 応答メッセージを解釈し、適切なアクションを AnyConnect ユーザに求めるように ASA を設定するには、SDI サーバとの直接通信をシミュレートする方法で RADIUS 応答メッセージを転送するように接続プロファイル（トンネル グループ）を設定する必要があります。SDI サーバに認証されるユーザは、この接続プロファイルを介して接続する必要があります。

手順

ステップ 1 **[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [AnyConnect 接続プロファイル（AnyConnect Connection Profiles）]** を選択します。

ステップ 2 SDI 固有の RADIUS 応答メッセージを解釈するために設定する接続プロファイルを選択して、[編集（Edit）] をクリックします。

ステップ 3 [AnyConnect 接続プロファイルの編集（Edit AnyConnect Connection Profile）] ウィンドウで、左側のナビゲーション ペインにある [詳細（Advanced）] ノードを展開して、[グループ エイリアス/グループ URL（Group Alias / Group URL）] を選択します。

ステップ 4 [ログイン画面への SecurID メッセージの表示を有効にする（Enable the display of SecurID messages on the login screen）] をオンにします。

ステップ 5 [OK] をクリックします。

ステップ 6 **[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [AAA/ローカル ユーザ（AAA/Local Users）] > [AAA サーバ グループ（AAA Server Groups）]** を選択します。

ステップ 7 [追加（Add）] をクリックして、AAA サーバ グループを追加します。

ステップ 8 [AAA サーバ グループの編集（Edit AAA Server Group）] ダイアログで AAA サーバ グループを設定して、[OK] をクリックします。

ステップ 9 [AAA サーバ グループ（AAA Server Groups）] 領域で作成した AAA サーバ グループを選択し、[選択したグループ内のサーバ（Servers in the Selected Group）] 領域で [追加（Add）] をクリックします。

ステップ 10 [SDI メッセージ（SDI Messages）] 領域で [メッセージ テーブル（Message Table）] 領域を展開します。メッセージテキストフィールドをダブルクリックするとメッセージを編集できます。RADIUS サーバから送信されたメッセージとテキストの一部または全体が一致するように、RADIUS 応答メッセージ テキストを ASA で設定します。

次の表に、メッセージコード、デフォルトの RADIUS 応答メッセージテキスト、および各メッセージの機能を示します。

（注） ASA が使用するデフォルトのメッセージテキストは、Cisco Secure Access Control Server（ACS）で使用されるデフォルトのメッセージ テキストです。Cisco Secure ACS を使用していて、デフォルトのメッセージテキストを使用している場合、ASA でメッセージ テキストを設定する必要はありません。

セキュリティ アプライアンスは、テーブルでの出現順に文字列を検索するため、メッセージテキスト用に使用する文字列が別の文字列のサブセットでないことを確認する必要があります。たとえば、「new PIN」が new-pin-sup と next-ccode-and-reauth の両方に対するデフォルトのメッセージテキストのサブセットであるとします。new-pin-sup を「new PIN」として設定した場合、セキュリティ アプライアンスは RADIUS サーバから「new PIN with the next card code」を受信すると、next-ccode-and-reauth コードではなく new-pin-sup コードとテキストを照合します。

メッセージ コード	デフォルトの RADIUS 応答メッセージ テキスト	機能
next-code	Enter Next PASSCODE	ユーザは PIN を入力せずに次のトークンコードを入力する必要があることを示します。
new-pin-sup	Please remember your new PIN	新しいシステムの PIN が提供されており、ユーザにその PIN を表示することを示します。
new-pin-meth	Do you want to enter your own pin	新しい PIN の作成にどの新しい PIN 方式を使用するかをユーザに尋ねます。
new-pin-req	Enter your new Alpha-Numerical PIN	ユーザ生成の PIN を入力することを要求することを示します。
new-pin-reenter	Reenter PIN:	ユーザが提供した PIN の確認のために ASA が内部的に使用します。ユーザにプロンプトを表示せずに、クライアントが PIN を確認します。

メッセージ コード	デフォルトの RADIUS 応答メッセージ テキスト	機能
new-pin-sys-ok	New PIN Accepted	ユーザが提供した PIN が受け入れられたことを示します。
next-ccode-and-reauth	new PIN with the next card code	PIN操作後、次のトークンコードを待ってから、認証のために新しい PIN と次のトークンコードの両方を入力する必要があることをユーザに示します。
ready-for-sys- pin	ACCEPT A SYSTEM GENERATED PIN	ユーザがシステム生成の PIN に対する準備ができていることを示すために ASA が内部的に使用します。

ステップ 11 [OK]、[適用（Apply）]、[保存（Save）] の順にクリックします。

証明書のピン留めについて

AnyConnect の証明書のピン留めは、サーバ証明書チェーンが実際に接続しているサーバから来たものであるか検出するのに役立ちます。この機能は VPN プロファイル設定に基づくもので、AnyConnect サーバ証明書検証ポリシーへの追加機能です。AnyConnect のローカル ポリシー ファイルでの厳格な証明書トラストの設定は、証明書のピン留めチェックに影響しません。ピンは、VPNプロファイルで、グローバルにまたはホストごとに設定できます。プライマリ ホストについて設定されたピンは、サーバ リスト内のバックアップ ホストに対しても有効です。証明書のピン留めチェックを実行するプリファレンスをユーザが制御することはできません。ピン検証が失敗すると、VPN 接続が終了します。

（注） AnyConnect は、プリファレンスが有効になっており、接続サーバの VPN プロファイルにピンがあるときのみ、ピン検証を実行します。

プリファレンスの有効化とグローバルおよびホストごとの証明書ピンの設定は、VPNプロファイル エディタ（AnyConnect プロファイル エディタの証明書ピン （113 ページ））で行うことができます。

証明書のピン留めを設定および維持するにあたっては、注意が必要です。プリファレンスを設定するときは、次の推奨事項を考慮してください。

- ルート証明書および/または中間証明書をピン留めする。理由は、これらはオペレーティング システムにおいて CA ベンダーによって十分に管理されているためです。

- CA が侵害された場合のバックアップとなるよう、別の CA からの複数のルート証明書および/または中間証明書をピン留めする。
- CAの移行が容易になるよう、複数のルート証明書および/または中間証明書をピン留めする。
- リーフ証明書がピン留めされている場合は、証明書の更新時に公開キーを保持するため、同一の証明書署名要求を使用する。
- サーバ リスト内のすべての接続ホストをピン留めする。

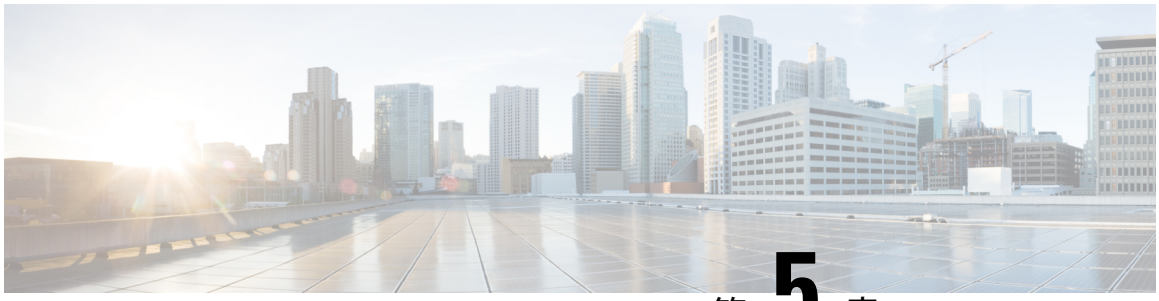
グローバル ピンとホストごとのピン

証明書ピンは、グローバルまたはホストごとに設定できます。大部分の接続ホストに対して有効なピンは、グローバル ピンとして設定されます。ルート証明書、中間証明機関の証明書、およびワイルドカード リーフ証明書は、VPN プロファイルのグローバル ピンの下に設定することを推奨します。1 つの接続ホストに対してのみ有効なピンは、ホストごとのピンと見なされます。リーフ証明書、自己署名の証明書は、VPNプロファイルのホストごとのピンの下に設定することを推奨します。

（注） AnyConnect は、ピン検証において、対応する接続サーバのグローバル ピンおよびホストごとのピンをチェックします。

（注） 複数の VPN プロファイルにまたがるグローバル ピンは、マージされません。ピンは、VPN 接続のためのファイル接続サーバから厳格に考慮されます。

（注） ホストごとの証明書のピン留めができるのは、[グローバル ピン（Global Pins）] セクションで証明書ピン留めのプリファレンスが有効になっている場合のみです。



第 5 章

ネットワーク アクセス マネージャの設定

この章では、ネットワーク アクセスマネージャ設定の概要について、ならびにユーザ ポリシーおよびネットワーク プロファイルの追加と設定の手順について説明します。

- ネットワーク アクセス マネージャについて （195 ページ）
- ネットワーク アクセス マネージャの展開 （198 ページ）
- DHCP 接続テストの無効化 （199 ページ）
- ネットワーク アクセス マネージャ プロファイル （200 ページ）

ネットワーク アクセス マネージャについて

ネットワーク アクセス マネージャは、ポリシーに従ってセキュアなレイヤ 2 ネットワークを提供するクライアント ソフトウェアです。最適なレイヤ 2 アクセス ネットワークを検出して選択し、有線ネットワークとワイヤレス ネットワークの両方へのアクセスに対してデバイス認証を実行します。ネットワーク アクセス マネージャは、セキュアなアクセスに必要なユーザおよびデバイス アイデンティティならびにネットワーク アクセス プロトコルを管理します。管理者定義のポリシーに違反する接続をエンドユーザが確立しないように、インテリジェントに動作します。

ネットワーク アクセス マネージャは、単一ホーム（一度に 1 つのネットワーク接続を許可する）になるよう設計されています。また、有線接続がワイヤレス接続によりも優先されます。そのため、有線接続を使用してネットワークに接続した場合、ワイヤレス アダプタは IP アドレスを失い無効になります。

（注） ネットワーク アクセス マネージャは Mac OS X または Linux には対応していません。

（注） Windows OS で ISE ポスチャを使用する場合は、AnyConnect ISE ポスチャを開始する前に Network Access Manager をインストールする必要があります。

Cisco AnyConnect Secure Mobility Client のネットワーク アクセス マネージャ コンポーネントは、次の主要な機能に対応しています。

- 有線（IEEE 802.3）およびワイヤレス（IEEE 802.11）ネットワーク アダプタ。
- Windows 7 以降でのモバイル ブロードバンド（3G）ネットワーク アダプタ（Microsoft モバイル ブロードバンド API をサポートする WAN アダプタが必要です）。
- Windows マシン クレデンシャルを使用した事前ログイン認証。
- Windows ログイン クレデンシャルを使用するシングル サインオン ユーザ認証。
- 簡素化された IEEE 802.1X 設定。
- IEEE MACsec 有線暗号化および企業ポリシー制御。
- EAP 方式：
  - EAP-FAST、PEAP、EAP-TTLS、EAP-TLS、および LEAP（IEEE 802.3 有線のみ EAP-MD5、EAP-GTC、および EAP-MSCHAPv2）。
- 内部 EAP 方式：
  - PEAP：EAP-GTC、EAP-MSCHAPv2、および EAP-TLS。
  - EAP-TTLS：EAP-MD5 および EAP-MSCHAPv2 およびレガシー方式（PAP、CHAP、MSCHAP、および MSCHAPv2）。
  - EAP-FAST：GTC、EAP-MSCHAPv2、および EAP-TLS。
- 暗号化モード：スタティック WEP（オープンまたは共有）、ダイナミック WEP、TKIP、および AES。
- キー確立プロトコル：WPA、WPA2/802.11i。
- AnyConnect は、次の環境でスマートカードにより提供されるクレデンシャルに対応します。
  - Windows の Microsoft CAPI 1.0 および CAPI 2.0（CNG）。
  - Windows ログインは ECDSA 証明書に対応していないため、ネットワーク アクセス マネージャのシングル サインオン（SSO）は ECDSA クライアント証明書に対応していません。

Suite B および FIPS

次の機能は、Windows 7 以降で FIPS 認定されています。例外を次に示します。

- ACS および ISE は Suite B には対応していませんが、OpenSSL 1.x 搭載の FreeRADIUS 2.x は対応しています。Microsoft NPS 2008 は Suite B に一部対応しています（NPS の証明書は RSA でなければなりません）。

- 802.1X/EAP は、Suite B の遷移プロファイルのみをサポートします（RFC 5430 の定義どおり）。TLS 1.2 はサポートされていません。
- MACsec は FIPS 準拠です。
- 楕円曲線 Diffie-Hellman（ECDH）キー交換はサポートされています。
- ECDSA クライアント証明書はサポートされています。
- OS ストアの ECDSA CA 証明書はサポートされています。
- ネットワーク プロファイルの（PEM エンコードされた）ECDSA CA 証明書はサポートされています。
- サーバの ECDSA 証明書チェーン検証はサポートされています。

シングル サインオンの「シングル ユーザ」の適用

Microsoft Windows では複数のユーザが同時にログインできますが、Cisco AnyConnect ネットワーク アクセス マネージャではシングル ユーザにネットワーク認証を制限します。AnyConnect ネットワーク アクセス マネージャは、ログインしているユーザの数に関係なく、デスクトップまたはサーバ当たり 1 人のユーザをアクティブにできます。シングル ユーザ ログインの適用は、いつでもシステムにログインできるユーザは1人のみで、管理者は現在ログインしているユーザを強制的にログオフできないことを示しています。

ネットワーク アクセス マネージャ クライアント モジュールが Windows デスクトップにインストールされている場合、デフォルト動作はシングル ユーザ ログインを適用することです。サーバにインストールされている場合、デフォルト動作はシングル ユーザ ログインの適用を緩和することです。いずれの場合も、デフォルトの動作を変更するようにレジストリを変更または追加できます。

制約事項

- Windows 管理者は、現在ログインしているユーザの強制ログオフが制限されています。
- 接続されたワークステーションへの RDP は同一ユーザにサポートされています。
- 同一ユーザと見なされるためには、クレデンシャルを同じフォーマットにする必要があります。たとえば、user/example は user@example.com と同じではありません。
- また、スマートカードユーザが同じPINを持っている場合、同一ユーザと見なされます。

シングル サインオンのシングル ユーザの適用の設定

Windows ワークステーションまたはサーバで複数のユーザを処理する方法を変更するには、レジストリの EnforceSingleLogon の値を変更します。

Windows では、レジストリ キーは **EnforceSingleLogon** で、OverlayIcon レジストリ キーと同じ場所にあります。

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential
Providers\{B12744B8-5BB7-463a-B85E-BB7627E73002}
```

1 つまたは複数のユーザ ログインを設定するには、EnforceSingleLogon という名前の DWORD を追加し、1 または 0 の値を指定します。

Windows の場合：

- 1 は、シングル ユーザにログインを制限します。
- 0 は、複数のユーザにログインを許可します。

ネットワーク アクセス マネージャの展開

ネットワーク アクセス マネージャは AnyConnect の一部として展開されます。AnyConnect をネットワーク アクセス マネージャやその他のモジュールとともにインストールする方法については、「AnyConnect 展開の概要」を参照してください。

ガイドライン

- Windows のネットワーク ステータス タスク トレイ アイコンの混同：ネットワーク アクセス マネージャは、Windows のネットワーク管理より優先します。したがって、ネットワーク アクセス マネージャのインストール後、ネットワークに接続するためにネットワーク ステータスのアイコンを使用できません。

  推奨アクション：Windows グループ ポリシーの [ネットワーク アイコンを削除する（Remove the networking icon）] を設定することで、タスク トレイから Windows ネットワーク アイコンを削除します。この設定は、トレイ アイコンだけに影響します。ユーザは、コントロール パネルを使用してネイティブのワイヤレス ネットワークを確立できます。

- Windows 7 以降の非表示のネットワークおよびネットワークの選択：ネットワーク アクセス マネージャは、ネットワーク アクセス マネージャのネットワーク スキャン リストで設定されたネットワークだけに接続を試みます。

  Windows 7 以降では、ネットワーク アクセス マネージャは非表示 SSID をプローブします。最初の非表示 SSID が見つかると、検索を中止します。複数の非表示ネットワークが設定されている場合、ネットワーク アクセス マネージャは次のように SSID を選択します。

  - 管理者が定義した最初の非表示社内ネットワークワークステーションのデフォルト設定は 1 です。サーバのデフォルトは 0 です。
  - 管理者が定義した非表示ネットワーク
  - ユーザが定義した最初の非表示ネットワークネットワーク アクセス マネージャは一度に 1 つの非ブロードキャスト SSID しかプローブできないため、サイトの非表示社内ネットワークは 1 つのみにすることをお勧めします。

- ネットワークの接続性または長い接続時間の瞬時的な喪失：ネットワーク アクセス マネージャをインストールする前に Windows でネットワークが定義済みである場合、Windows の接続マネージャがそのネットワークに接続を試みる場合があります。

  推奨アクション：ネットワークが圏内にある場合、すべての Windows 定義ネットワークに対して [自動的に接続する（Connect Automatically）] をオフにするか、Windows 定義ネットワークをすべて削除します。

- ネットワーク アクセス マネージャ モジュールは、このモジュールがクライアント システムに初めてインストールされたときに、一部の既存の Windows 7 またはそれ以降のワイヤレス プロファイルをネットワーク アクセス マネージャ プロファイル形式に変換するように設定できます。次の条件を満たすインフラストラクチャ ネットワークは変換が可能です。

  - オープン（Open）
  - 静的 WEP
  - WPA/WPA2 Personal
  - 非 GPO ネイティブ Wi-Fi ユーザ ネットワーク プロファイルだけが変換されます。
  - プロファイルの変換中は、WLAN サービスがシステムで実行している必要があります。
  - 変換は、ネットワーク アクセス マネージャ XML コンフィギュレーション ファイルがすでに存在する場合（userConfiguration.xml）は実行されません。

  ネットワーク プロファイルの変換を有効にするには、PROFILE_CONVERSION プロパティの値を 1 に設定する MSI トランスフォームを作成し、それを MSI パッケージに適用します。またはコマンド ラインで PROFILE_CONVERSION プロパティを 1 に変更して、MSI パッケージをインストールします。例：**msiexec /i anyconnect-nam-win-3.1.xxxxx-k9.msi PROFILE_CONVERSION=1**

- ISE ポスチャが開始する前にネットワーク アクセス マネージャをインストールする必要があります。ISE ポスチャは、ネットワーク アクセス マネージャ プラグインを使用して、ネットワーク変更ベントおよび 802.1x WiFi を検出します。

DHCP 接続テストの無効化

ネットワークがダイナミック IP アドレスを使用するように設定されている場合は、Windows OS サービスは DHCP を使用して接続を確立しようとします。ただし、オペレーティング システム プロセスがネットワーク アクセス マネージャに DHCP トランザクションが完了したことを通知するまでに最大で 2 分かかる場合があります。OS の DHCP トランザクションに加えて、ネットワーク アクセス マネージャが DHCP トランザクションをトリガーすることによって、OS 経由の接続が確立するまでの時間を短縮し、ネットワーク接続を確認します。

接続テストで NAM による DHCP トランザクションの使用を無効にする場合は、次のレジストリ キーを DWORD として追加し、指定された値を設定します。

- 64 ビット Windows：HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Cisco\Cisco AnyConnect Network Access Manager\DisableDHCP を 1 に設定
- 32 ビット Windows：HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\Cisco AnyConnect Network Access Manager\DisableDHCP を 1 に設定

（注） ネットワーク アクセス マネージャの DHCP 接続テストを無効にすると、多くの場合、接続時間が長くなるためお勧めできません。

ネットワーク アクセス マネージャ プロファイル

ネットワーク アクセス マネージャ プロファイルは、ネットワーク アクセス マネージャ プロファイル エディタで設定されます。このエディタは ASDM でスタンドアロン Windows アプリケーションとして使用できます。

[クライアント ポリシー（Client Policy）] ウィンドウ

[クライアント ポリシー（Client Policy）] ウィンドウでは、クライアント ポリシー オプションを設定できます。この項では次のトピックについて説明します。

接続の設定

ユーザ ログインの前または後にネットワーク接続しようとするかどうかを定義できます。

- [デフォルト接続タイムアウト（Default Connection Timeout）]：ユーザ作成ネットワークの接続タイムアウトとして使用する秒数。デフォルト値は 40 秒です。
- [ユーザ ログインの前（Before User Logon）]：ユーザがログインする前にネットワークに接続します。サポートされているユーザ ログインの種類として、ユーザ アカウント（Kerberos）認証、ユーザ GPO のロード、GPO ベースのログイン スクリプト実行があります。[ユーザ ログインの前（Before User Logon）] を選択した場合、[ユーザがログインできるまでに待機する時間（Time to Wait Before Allowing a User to Logon）] も設定できます。
- [ユーザがログインできるまでに待機する時間（Time to Wait Before Allowing a User to Logon）]：ネットワーク アクセス マネージャが完全にネットワーク接続するのに待機する最大（最悪のケース）秒数を指定します。この時間内にネットワーク接続が確立できない場合、Windows ログイン プロセスはユーザ ログインにより継続されます。デフォルトは 5 秒です。

（注） ワイヤレス接続を管理するようネットワーク アクセス マネージャが設定されている場合、[ユーザがログインできるまでに待機する時間（Time to Wait Before Allowing a User to Logon）] を 30 秒以上に設定する必要があります。ワイヤレス接続の確立にさらに時間が必要になる可能性があるためです。DHCP 経由で IP アドレスを取得するために必要な時間も考慮する必要があります。2 つ以上のネットワーク プロファイルが設定されている場合、2 回以上の接続試行に対応するように値を大きくする必要があります。

- [ユーザ ログイン後（After User Logon）]：Windows へのユーザ ログイン後にネットワークに接続します。

メディア

ネットワーク アクセス マネージャ クライアントにより制御されるメディアの種類を指定します。

- [Wi-Fi（ワイヤレス）メディアの管理（Manage Wi-Fi (wireless) Media）]：Wi-Fi メディアの管理、また任意で WPA/WPA2 ハンドシェイクの検証ができるようになります。

  IEEE 802.11i ワイヤレス ネットワーキング標準では、サプリカント（この場合はネットワーク アクセス マネージャ）がアクセス ポイントの RSN IE（堅牢でセキュアなネットワーク情報交換）を検証する必要があることを規定しています。IE は、キー導出時に IEEE 801.X プロトコル パケットの EAPOL キー データに送信され、ビーコン/プローブ応答フレームにあるアクセス ポイントの RSN IE に一致する必要があります。

- [WPA/WPA2 ハンドシェイクの検証の有効化（Enable validation of WPA/WPA2 handshake）]：WPA/WPA2 ハンドシェイクを検証します。オフの場合、この任意の検証手順はスキップされます。

（注） 一部のアダプタでは、アクセス ポイントの RSN IE を常に提供するわけではないため、認証試行に失敗し、クライアントが接続されません。

- [デフォルトのアソシエーション タイムアウト（秒）（Default Association Timeout (sec)）]：WPA/WPA2 ハンドシェイクを有効にした場合は、デフォルトのアソシエーション タイムアウトを指定する必要があります。

- [有線（IEEE 802.3）メディアの管理（Manage Wired (IEEE 802.3) Media）]：有線接続の管理を有効にします。

- [モバイルブロードバンド（3G）メディアの管理（Manage Mobile Broadband (3G) Media）]：Windows 7 以降のモバイル ブロードバンド アダプタの管理を有効にします。この機能は、デフォルトではディセーブルになっています。

（注） この機能はベータ版に入っています。Cisco TAC は、ベータ版には対応していません。

- [データ ローミングの有効化（Enable Data Roaming）]：データ ローミングを許可するかどうかを指定します。

エンド ユーザ制御

ユーザに対して次の制御を設定できます。

- [クライアントの無効化（Disable Client）]：ユーザは、AnyConnect UI を使用して、ネットワーク アクセス マネージャによる有線メディアおよびワイヤレス メディアの管理を無効および有効にできます。
- [ユーザ グループの表示（Display User Groups）]：管理者定義のグループに対応しない場合でも、ユーザが作成したグループ（CSSC 5.x から作成）を表示して、接続できるようにします。
- [接続時に実行するスクリプトまたはアプリケーションの指定（Specify a script or application to run when connected）]：ユーザは、ネットワーク接続時に実行するスクリプトまたはアプリケーションを指定できます。

（注） スクリプト設定は 1 つのユーザ設定ネットワークに固有であり、ユーザはローカル ファイル（.exe、.bat、または .cmd）を指定して、そのネットワークが接続状態になったときに実行できます。競合を避けるために、スクリプト機能では、ユーザはユーザ定義のネットワークについてのみスクリプトまたはアプリケーションを設定でき、管理者定義のネットワークについては設定できません。スクリプト機能では、スクリプトの実行に関して管理者ネットワークをユーザが変更できません。このため、ユーザは管理者ネットワークのインターフェイスを使用できません。また、ユーザが実行中のスクリプトを設定できないようにする場合、この機能はネットワーク アクセス マネージャ GUI に表示されません。

- [自動接続（Auto-connect）]：ユーザが選択しなくても自動的にネットワークに接続します。 デフォルトは自動接続です。

管理ステータス

- [サービス オペレーション（Service Operation）]：このサービスをオフにすると、このプロファイルを使用しているクライアントはレイヤ 2 接続を確立するために接続できません。

- [FIPS モード（FIPS Mode）]：FIPS モードを有効にすると、ネットワーク アクセス マネージャは政府の要件を満たす方法で暗号化操作を行います。

  連邦情報処理標準（FIPS 140-2 Level 1）は、暗号化モジュールのセキュリティ要件を指定する米国政府標準規格です。FIPS は、ソフトウェアとハードウェアのタイプに応じて、MACsec または Wi-Fi 用のネットワーク アクセス マネージャでサポートされています。

表 *8*：ネットワーク アクセス マネージャによる *FIPS* サポート

メディア/オペレーティング システム	**Windows 7 以降**
MACsec で有線	Intel HW MACsec 対応 NIC の場合、またはハードウェア以外の MACsec を使用している場合に FIPS に準拠しています。
Wi-Fi	FIPS に準拠していません。

[認証ポリシー（Authentication Policy）] ウィンドウ

[認証ポリシー（Authentication Policy）] ウィンドウでは、すべてのネットワーク接続に適用される、アソシエーションおよび認証ネットワーク フィルタを作成できます。アソシエーション モードまたは認証モードのいずれもオンにしない場合、認証 Wi-Fi ネットワークに接続できません。モードのサブセットを選択すると、それらのタイプのネットワークにのみ接続できます。目的のアソシエーション モードまたは認証モードをそれぞれ選択するか、[すべて選択（Select All）] を選択します。

内部方式も特定の認証プロトコルのみに制限される可能性があります。内部方式は、[許可された認証モード（Allowed Authentication Modes）] ペインの外部方式（トンネリング）下にインデントされて表示されます。

認証プロトコル選択のメカニズムは、現在のクライアント認証データベースと統合されています。セキュアなワイヤレス LAN 展開では、ユーザが新しい認証システムを作成する必要はありません。

内部トンネリングに使用できる EAP 方式は、内部方式のクレデンシャル タイプと外部トンネリング方式に基づいています。次のリストで、外部トンネル方式はそれぞれ、各クレデンシャル タイプに対応した内部方式の種類を一覧表示しています。

- PEAP
  - パスワード クレデンシャル：EAP-MSCHAPv2 または EAP-GTC
  - トークン クレデンシャル：EAP-GTC
  - 証明書クレデンシャル：EAP-TLS
- EAP-FAST
  - パスワード クレデンシャル：EAP-MSCHAPv2 または EAP-GTC

- トークン クレデンシャル：EAP-GTC
- 証明書クレデンシャル：EAP-TLS

- EAP-TTLS
  - パスワードクレデンシャル：EAP-MSCHAPv2、EAP-MD5、PAP（L）、CHAP（L）、MSCHAP（L）、MSCHAP-v2（レガシー）。
  - トークン クレデンシャル：PAP（レガシー）。チャレンジ/レスポンス方式はトークン ベースの認証には適していないため、ネットワーク アクセス マネージャでサポートされるデフォルト トークン オプションは PAP です。
  - 証明書クレデンシャル：該当なし。

[ネットワーク（Networks）] ウィンドウ

[ネットワーク（Networks）] ウィンドウでは、企業ユーザの事前定義ネットワークを設定できます。すべてのグループで使用できるネットワークを設定するか、または特定のネットワークで使用するグループを作成できます。[ネットワーク（Networks）] ウィンドウには、既存のウィンドウにペインを追加できるウィザードが表示され、[次へ（Next）] をクリックしてより多くの設定オプションに進むことができます。

グループとは、基本的に、設定された接続（ネットワーク）の集合です。設定された各接続は、グループに属するか、すべてのグループのメンバーである必要があります。

（注） 下位互換性を確保するため、Cisco Secure Services Client で展開された管理者作成のネットワークは、SSID をブロードキャストしない非表示ネットワークとして扱われます。ユーザ ネットワークは、SSID をブロードキャストするネットワークとして扱われます。

新しいグループを作成できるのは管理者だけです。設定にグループが定義されていない場合、プロファイルエディタによって自動生成グループが作成されます。自動生成グループには、管理者定義のグループに割り当てられていないネットワークが含まれます。クライアントは、アクティブ グループに定義されている接続を使用してネットワーク接続の確立を試みます。[ネットワーク グループ（Network Groups）] ウィンドウの [ネットワークの作成（Create Networks）] オプションの設定に応じて、エンド ユーザは、ユーザ ネットワークをアクティブ グループに追加するか、アクティブ グループからユーザ ネットワークを削除できます。

定義されているネットワークは、リストの先頭にあるすべてのグループで使用できます。グローバル ネットワーク内にどのネットワークがあるかを制御できるため、ユーザ定義のネットワークが存在する場合も、エンドユーザが接続できる企業ネットワークを指定できます。エンド ユーザは管理者が設定したネットワークを変更したり、削除したりできません。

（注） エンドユーザは、globalNetworks セクションのネットワークを除き、グループにネットワークを追加できます。これらのネットワークはすべてのグループ内に存在し、プロファイルエディタを使用してしか作成できないためです。

企業ネットワークの一般的なエンドユーザは、このクライアントを使用するためにグループの知識は必要ありません。アクティブ グループは設定内の最初のグループですが、グループが 1 つしか使用できない場合、アクティブ グループは認識されず、表示されません。一方で、複数のグループが存在する場合、UI にはアクティブ グループが選択されたことを示すグループのリストが表示されます。ユーザはアクティブ グループから選択でき、設定はリブート後も保持されます。[ネットワーク グループ（Network Groups）] ウィンドウの [ネットワークの作成（Create Networks）] オプションの設定に応じて、エンド ユーザは、グループを使用せずに自分のネットワークを追加または削除できます。

（注） グループ選択はリブート後も持続して、ネットワークは修復されます（そのためには、トレイアイコンを右クリックしながら [ネットワーク修復（Network Repair）] を選択します）。ネットワーク アクセス マネージャが修復されるか、またはリスタートされると、以前のアクティブなグループが使用されます。

[ネットワーク（Networks）]、[メディアタイプ（Media Type）]ページ

[ネットワーク（Networks）] ウィンドウの [メディア タイプ（Media Type）] ページにより、有線ネットワークまたはワイヤレス ネットワークを作成または編集できます。設定は、選択内容によって異なります。

最初のダイアログには、次のセクションが含まれています。

- [名前（Name）]：このネットワーク用に表示される名前を入力します。
- [グループ メンバーシップ（Group Membership）]：このプロファイルが使用できるようにするネットワーク グループ（複数の場合もあり）を選択します。
- [ネットワーク メディア（Network Media）]：[有線（Wired）] または [Wi-Fi（ワイヤレス）（Wi-Fi (wireless)）] を選択します。[Wi-Fi] を選択すると、次のパラメータも設定できます。
  - [SSID]：ワイヤレス ネットワークの SSID（サービス セット識別子）を入力します。
  - [非表示ネットワーク（Hidden Network）]：SSID をブロードキャストしない場合でも、ネットワークへの接続を許可します。
  - [社内ネットワーク（Corporate Network）]：[社内（Corporate）] として設定されたネットワークが近接にある場合、まずそのネットワークに強制的に接続します。社内ネットワークが非ブロードキャスト（非表示）SSID を使用し、非表示として設定されて

いる場合、ネットワーク アクセス マネージャは非表示 SSID をアクティブにプローブし、企業 SSID が範囲内にあれば接続を確立します。

- [アソシエーション タイムアウト（Association Timeout）]：ネットワーク アクセス マネージャが、使用できるネットワークを再評価するまでに特定のワイヤレス ネットワークとのアソシエーションを待機する時間を入力します。デフォルトのアソシエーション タイムアウトは 5 秒です。

- 共通設定
  - [スクリプトまたはアプリケーション（Script or application）]：ローカル システムで実行するファイルのパスとファイル名を入力するか、フォルダを参照してファイルを選択します。次のルールは、スクリプトおよびアプリケーションに適用されます。

    .exe、.bat、または .cmd 拡張子のファイルが受け入れられます。

    ユーザは、管理者が作成したネットワークで定義されたスクリプトまたはアプリケーションは変更できません。

    プロファイル エディタを使用してパスおよびスクリプトまたはアプリケーションのファイル名のみを指定できます。スクリプトまたはアプリケーションがユーザのマシンに存在しない場合、エラー メッセージが表示されます。ユーザは、スクリプトまたはアプリケーションがマシンにないこと、およびシステム管理者に問い合わせる必要があると通知されます。

    アプリケーションがユーザのパスに存在する場合を除いて、実行するアプリケーションのフルパスを指定する必要があります。アプリケーションがユーザのパスに存在する場合は、アプリケーション名またはスクリプト名だけを指定できます。

  - [接続タイムアウト（Connection Timeout）]：ネットワーク アクセス マネージャが、（接続モードが自動の場合）別のネットワークに接続しようとするか、または別のアダプタを使用するまでにネットワーク接続の確立を待機する秒数を入力します。

（注） 認証を完了するまでに 60 秒近くかかるスマートカード認証システムもあります。スマートカードを使用している場合、特に、スマートカードが接続に成功するまでにいくつかネットワークに接続しなければならない場合に、[接続タイムアウト（Connection Timeout）] 値を増やす必要があります。

（注） 特定のスマート カード ミドルウェアで見つかった問題を軽減するために、AnyConnect Network Access Manager はテスト データに対して署名操作を実行し、その署名を検証することで、スマートカード PIN を検証します。このテスト署名はスマートカードにある証明書ごとに行われ、証明書の数によってはスマートカード認証が大幅に遅延する場合があります。テスト署名操作を無効にする場合は、HKEY_LOCAL_MACHINE/SOFTWARE/Cisco/Cisco AnyConnect Network Access Manager でレジストリ エントリに **DisableSmartcardPinVerifyBySigning** を追加して DWORD を 1 に設定できます。このキーを有効にする変更を加える場合は、正しく動作するように、すべてのスマートカードおよび関連するハードウェアでその変更を完全にテストしてください。

[ネットワーク（Networks）]、[セキュリティ レベル（Security Level）] ページ

[ネットワーク（Networks）] ウィザードの [セキュリティ レベル（Security Level）] ページで、[オープン ネットワーク（Open Network）]、[認証ネットワーク（Authentication Network）]、または（ワイヤレス ネットワーク メディアにのみ表示される）[共有キー ネットワーク（Shared Key Network）] を選択します。これらのネットワーク タイプの設定フローはそれぞれ異なっており、次の項で説明します。

- 認証ネットワークの設定：企業を安全に保つために推奨されます。
- オープン ネットワークの設定：推奨されません。ただし、キャプティブ ポータル環境を介したゲストアクセスの提供に使用できます。ネットワーク アクセスマネージャは、キャプティブ ポータルの状態にあるときはブラウザの自動起動をサポートしません。
- 共有キー ネットワークの設定：小規模オフィスまたはホーム オフィスなどの無線ネットワークに推奨されます。

認証ネットワークの設定

[セキュリティ レベル（Security Level）] セクションで [認証ネットワーク（Authenticating Network）] を選択した場合、次に説明するペインが追加で表示されます。これらのペインの設定を完了したら、[次へ（Next）] ボタンをクリックするか、[接続タイプ（Connection Type）] タブを選択して [ネットワーク接続タイプ（Network Connection Type）] ダイアログを開きます。

[802.1X 設定（802.1X Settings）] ペイン

ネットワーク設定に応じて IEEE 802.1X 設定を調整します。

（注） AnyConnect ISE ポスチャがネットワーク アクセス マネージャとともにインストールされた場合、ISE ポスチャはネットワーク アクセス マネージャ プラグインを使用してネットワーク変更イベントと 802.1X WiFi を検出します。

- [authPeriod (sec)]：認証が開始された場合、認証メッセージの間隔がこの設定を超えるとサプリカントはタイムアウトします。認証を再度開始するには、サプリカントでオーセンティケータが必要です。
- [heldPeriod (sec)]：認証が失敗した場合、サプリカントはこの設定で定義された時間だけ待機し、この時間を超えると別の認証が試行されます。
- [startPeriod (sec)]：EAPOL-Start メッセージに対する応答をオーセンティケータから受信しない場合に、EAPOL-Start メッセージを再送信する間隔（秒）です。
- [maxStart]：サプリカントが、オーセンティケータが存在しないと見なす前に、IEEE 801.X プロトコル パケット、EAPOL Key データ、または EAPoL-Start を送信することで、サプリカントがオーセンティケータの認証を開始する回数です。これが発生した場合は、サプリカントはデータ トラフィックを許可します。

ヒント 単一の認証有線接続がオープンおよび認証ネットワークの両方と動作するように設定できます。これは、[startPeriod] および [maxStart] を注意深く設定して、認証開始試行に費やす合計時間がネットワーク接続タイマーよりも小さくなるようにします（[startPeriod] x [maxStart] < ネットワーク接続タイマー）。

このシナリオでは、ネットワーク接続タイマーを（[startPeriod] x [maxStart]）秒だけ大きくして、DHCP アドレスを取得してネットワーク接続を完了するために十分な時間をクライアントに与えることに注意してください。

逆に、認証が成功した後にのみデータ トラフィックを許可するには、認証の開始に費やした総時間がネットワーク接続タイマーより長くなるような [startPeriod] および [maxStart] になるようにします（[startPeriod] x [maxStart] > ネットワーク接続タイマー）。

[セキュリティ（Security）] ペイン

有線ネットワークの場合にのみ表示されます。

[セキュリティ（Security）] ペインで、次のパラメータの値を選択します。

- [キー管理（Key Management）]：MACsec 対応有線ネットワークで使用するキー管理プロトコルを決定します。
  - [なし（None）]：キー管理プロトコルを使用しません。また、有線暗号化を実行しません。
  - [MKA]：サプリカントは、MACsec キー承諾プロトコル ポリシーと暗号キーをネゴシエートしようとします。MACsec は MAC レイヤ セキュリティで、有線ネットワーク

で MAC レイヤ暗号化を行います。MACsec プロトコルは、暗号化を使用して MAC レベル フレームを保護する手段であり、MACsec Key Agreement（MKA）エンティティに依存して暗号キーをネゴシエートおよび配布します。

- 暗号化（Encryption）
  - [なし（None）]：データ トラフィックの整合性チェックは行われますが、暗号化はされません。
  - [MACsec: AES-GCM-128]：このオプションは、キー管理に MKA を選択した場合のみ使用できます。AES-GCM-128 を使用して、データ トラフィックが暗号化されます。
  - MACsec: AES GCM 256： このオプションは、エンタープライズ エッジ（eEdge）統合を備えた特定の IOS バージョンでサポートされており、キー管理に MKA を選択した場合にのみ使用できます。スイッチ側の設定が一致する必要があります。MACsec 256 暗号化規格を有効にすることによって、MACsec Key Agreement（MKA）を使用した 802.1AE 暗号化は、MACsec 対応デバイスとホスト デバイス間の暗号化用にダウンリンク ポートでサポートされています。

詳細については、「Identity-Based Networking Services: MAC Security」を参照してください。

[ポート認証例外ポリシー（Port Authentication Exception Policy）] ペイン

このペインは、有線ネットワークでのみ表示されます。

[ポート認証例外ポリシー（Port Authentication Exception Policy）] ペインでは、認証プロセス中の IEEE 802.1X サプリカントの動作を変更できます。ポート例外が有効でない場合、サプリカントはその既存の動作を続け、設定が完全に成功した場合のみ（または、この項で前述したように、オーセンティケータからの応答がない状態で maxStarts 数の認証が開始された後に）ポートを開きます。次のいずれかのオプションを選択します。

- [認証前にデータ トラフィックを許可（Allow data traffic before authentication）]：認証試行の前にデータ トラフィックが許可されます。
- [次の場合でも認証後にデータ トラフィックを許可（Allow data traffic after authentication even if）]：次の場合でもデータ トラフィックが許可されます。
  - [EAP 失敗（EAP Fails）]：選択すると、EAP が失敗した場合でも、サプリカントは認証を試行します。認証に失敗した場合、サプリカントは認証に失敗したにもかかわらず、データ トラフィックを許可します。
  - [EAP は成功したがキー管理に失敗（EAP succeeds but key management fails）]：選択すると、EAP は成功してキー管理が失敗した場合、サプリカントはキー サーバとのキーのネゴシエートを試行しますが、何らかの理由によりキー ネゴシエーションに失敗した場合でもデータ トラフィックを許可します。この設定は、キー管理が設定されている場合のみ有効です。キー管理がなしに設定されている場合、このチェックボックスは淡色表示されます。

制約事項 MACsec には、ACS バージョン 5.1 以降および MACsec 対応スイッチが必要です。ACS またはスイッチの設定については、『*Catalyst 3750-X and 3560-X Switch Software Configuration Guide*』を参照してください。

アソシエーション モード

このペインは、ワイヤレス ネットワークの場合にのみ表示されます。

アソシエーション モードを選択します。

- WEP
- WAP Enterprise（TKIP）
- WPA Enterprise（AES）
- WPA 2 Enterprise（TKIP）
- WPA 2 Enterprise（AES）
- CCKM（TKIP）：（Cisco CB21AG ワイヤレス NIC が必要）
- CCKM（AES）：（Cisco CB21AG ワイヤレス NIC が必要）

オープン ネットワークの設定

オープン ネットワークは、認証や暗号化を使用しません。オープン（非セキュア）ネットワークを作成するには、次の手順を実行します。

手順

ステップ 1 [セキュリティ レベル（Security Level）] ページで [オープン ネットワーク（Open Network）] を選択します。この選択肢では、最もセキュリティ レベルの低いネットワークが提供されます。これは、ゲスト アクセス ワイヤレス ネットワークに推奨されています。

ステップ 2 [Next] をクリックします。

ステップ 3 接続タイプを決定します。

共有キー ネットワークの設定

Wi-Fi ネットワークは、エンドポイントとネットワーク アクセス ポイント間のデータを暗号化する際に使用される暗号キーを導出するために、共有キーを使用することがあります。WPA または WPA2 Personal を備えた共有キーを使用すると、小規模オフィスや自宅オフィスに適した Medium レベルのセキュリティ クラスが実現します。

（注） 共有キーによるセキュリティは、企業ワイヤレス ネットワークには推奨しません。

セキュリティ レベルを共有キー ネットワークにする場合は、次の手順を実行します。

手順

ステップ 1 [共有キー ネットワーク（Shared Key Network）] を選択します。

ステップ 2 [セキュリティ レベル（Security Level）] ウィンドウで [次へ（Next）] をクリックします。

ステップ 3 [ユーザ接続（User Connection）] または [マシン接続（Machine Connection）] を指定します。

ステップ 4 [Next] をクリックします。

ステップ 5 [共有キー タイプ（Shared Key Type）]：共有キーのタイプを決定する共有キー アソシエーション モードを指定します。次の選択肢があります。

- [WEP]：スタティック WEP 暗号化とのレガシー IEEE 802.11 オープン システム アソシエーション。
- [Shared]：スタティック WEP 暗号化とのレガシー IEEE 802.11 共有キー アソシエーション。
- [WPA/WPA2-Personal]：パスフレーズ事前共有キー（PSK）から暗号キーを導出する Wi-Fi セキュリティ プロトコル。

ステップ 6 レガシー IEEE 802.11 WEP または共有キーを選択した場合は、40 ビット、64 ビット、104 ビット、または 128 ビットを選択します。40 または 64 ビットの WEP キーは、5 個の ASCII 文字または 10 桁の 16 進数である必要があります。104 または 128 ビットの WEP キーは、13 個の ASCII 文字または 26 桁の 16 進数である必要があります。

ステップ 7 WPA または WPA2 Personal を選択した場合は、（TKIP/AES）を使用する暗号化のタイプを選択し、共有キーを入力します。入力するキーは、8 ～ 63 個の ASCII 文字またはちょうど 64 桁の 16 進数である必要があります。共有キーが ASCII 文字で構成されている場合は、[ASCII] を選択します。共有キーに 64 桁の 16 進数が含まれている場合は、[Hexadecimal] を選択します。

ステップ 8 [完了（Done）] をクリックします。[OK] をクリックします。

[ネットワーク（Networks）]、[ネットワーク接続タイプ（Network Connection Type）] ペイン

ここでは、ネットワーク アクセス マネージャ プロファイル エディタの [セキュリティ レベル（Security Level）] に続く、[ネットワーク（Networks）] ウィンドウの [ネットワーク接続タイプ（network connection type）] ペインについて説明します。次のいずれかの接続タイプを選択します。

- [マシン接続（Machine Connection）]：Windows Active Directory に保存されているデバイス名が認証に使用されます。マシン接続は通常、接続時にユーザ クレデンシャルが必要ない場合に使用します。ユーザがログオフし、ユーザ クレデンシャルが使用できない場合でも、エンドステーションがネットワークにログインする必要がある場合にこのオプションを選択します。このオプションは通常、ユーザがアクセスする前に、ドメインに接続し、ネットワークから GPO および他のアップデートを取得する場合に使用します。

  （注） 既知のネットワークが使用できない場合、VPN Start Before Login（SBL）は失敗します。SBL モードで許可されるネットワーク プロファイルには、非 802-1X 認証モードを採用するすべてのメディア タイプ（オープン WEP、WPA/WPA2 パーソナル、および静的キー（WEP）ネットワークなど）が含まれます。ネットワーク アクセス マネージャを [ユーザがログインする前（Before User Logon）] に、およびマシン接続認証用に設定している場合、ネットワーク アクセス マネージャはユーザにネットワーク情報を要求し、VPN SBL は正常に行われます。

- [ユーザ接続（User Connection）]：ユーザ クレデンシャルを認証に使用します。

  [クライアント ポリシー（Client Policy）] ペインで [ユーザがログインする前（Before User Logon）] が選択されている場合、Windows スタート画面でユーザがログイン クレデンシャルを入力した後、ネットワーク アクセス マネージャはユーザのクレデンシャルを収集します。Windows がユーザの Windows セッションを開始している間に、ネットワーク接続が確立されます。

  [クライアント ポリシー（Client Policy）] ペインで [ユーザがログインした後（After User Logon）] が選択されている場合、ユーザが Windows にログインしてから、接続が開始されます。

  ユーザがログオフすると、現在のユーザのネットワーク接続は終了します。マシン ネットワーク プロファイルが使用可能な場合、NAM はマシン ネットワークに再接続します。

- [マシンおよびユーザ接続（Machine and User Connection）]：[セキュリティ レベル（Security Level）] ペインで選択したように、[認証ネットワーク（Authenticating Network）] を設定している場合にのみ指定できます。マシン ID とユーザ クレデンシャルの両方を使用しますが、マシン部分はユーザがデバイスにログインしていない場合のみ有効です。2 つの部分の設定は同じですが、マシン接続の認証タイプとクレデンシャルは、ユーザ接続の認証タイプとクレデンシャルと異なる場合があります。

  マシン接続を使用していてユーザがログインしていないとき、およびユーザ接続を使用していてユーザがログインしているときにネットワークに PC を常時接続するには、このオプションを選択します。

  EAP-FAST が（次のペインで）EAP 方式として設定されている場合、EAP チェーンがサポートされています。つまり、ネットワーク アクセス マネージャによって、マシンおよびユーザが既知のエンティティであり、企業によって管理されていることが検証されます。

このネットワーク接続タイプを選択すると、[ネットワーク（Networks）] ダイアログに追加のタブが表示されます。これらのタブでは、選択されたネットワーク接続タイプのEAP方式とクレデンシャルを設定できます。

[ネットワーク（Networks）]、[ユーザまたはマシンの認証（User or Machine Authentication）] ページ

ネットワーク接続タイプを選択した後、それらの接続タイプの認証方式を選択します。認証方式を選択した後、選択した方式に対応するように表示が更新され、追加情報を提供するように要求されます。

（注） MACsec を有効にした場合は、PEAP、EAP-TLS、または EAP-FAST などの MSK キー派生をサポートするEAP方式を必ず選択します。また、MACsecが有効でない場合にも、ネットワークアクセス マネージャを使用すると、MACsec を考慮して MTU が 1500 から 1468 に削減されます。

EAP の概要

EAP は、認証プロトコルを伝送するトランスポート プロトコルから認証プロトコルをデカップリングするための要件を示したIETF RFCです。このデカップリングによって、トランスポート プロトコル（IEEE 802.1X、UDP、またはRADIUS など）は、認証プロトコルを変更せずにEAP プロトコルを伝送できます。

基本的な EAP プロトコルは、次の 4 つのパケット タイプから構成されます。

- EAP要求：オーセンティケータは、要求パケットをサプリカントに送信します。各要求にはtypeフィールドがあり、要求されている内容を示します。これには、使用するサプリカント アイデンティティやEAP タイプなどが含まれます。シーケンス番号により、オーセンティケータおよびピアは、各 EAP 要求に対応する EAP 応答を一致できます。
- EAP応答：サプリカントは応答パケットをオーセンティケータに送信し、シーケンス番号を使用して元の EAP 要求と照合します。EAP 応答のタイプは、通常 EAP 要求と一致しますが、応答が負（NAK）の場合は除きます。
- EAP成功：オーセンティケータは認証に成功した場合にサプリカントに成功パケットを送信します。
- EAP失敗：オーセンティケータは、認証が失敗した場合、サプリカントに失敗パケットを送信します。

EAP が IEEE 802.11X システムで使用中の場合、アクセス ポイントは EAP パススルー モードで動作します。このモードでは、アクセス ポイントはコード、識別子、および長さのフィールドを確認して、サプリカントから受信した EAP パケットを AAA サーバに転送します。AAA サーバ オーセンティケータから受信したパケットは、サプリカントに転送されます。

EAP-GTC

EAP-GTCは、単純なユーザ名とパスワード認証に基づくEAP認証方式です。チャレンジ/レスポンス方式を使用せずに、ユーザ名とパスワードの両方がクリアテキストで渡されます。この方式は、トンネリング EAP 方式の内部で使用（次のトンネリング EAP 方式を参照）、またはワンタイム パスワード（OTP）を使用する場合に推奨されます。

EAP-GTCは、相互認証を提供しません。クライアントのみ認証するため、不正なサーバがユーザのクレデンシャルを取得するおそれがあります。相互認証が必要な場合、EAP-GTC はトンネリング EAP 方式の内部で使用され、サーバ認証を提供します。

EAP-GTCによりキー関連情報は提供されないため、MACsecではこの方式は使用できません。さらなるトラフィック暗号化のためにキー関連情報が必要な場合、EAP-GTC はトンネリング EAP 方式の内部で使用され、キー関連情報（および必要に応じて内部および外部の EAP 方式の暗号化バインド）を提供します。

パスワード ソース オプションには、次の 2 つがあります。

- [パスワードを使った認証（Authenticate using a Password）]：十分に保護された有線環境にのみ適しています。
- [トークンを使った認証（Authenticate using a Token）]：トークン コードまたは OTP のライフタイムが短い（通常約 10 秒）ため、より高いセキュリティを備えています

（注） ネットワーク アクセス マネージャ、オーセンティケータ、またはEAP-GTC プロトコルのいずれもパスワードとトークン コード間を区別できません。これらのオプションは、ネットワーク アクセス マネージャ内のクレデンシャルのライフタイムにのみ影響を与えます。パスワードは、ログアウトまでかそれ以降も記憶できますが、トークン コードは記憶できません（認証ごとにユーザがトークン コードの入力を求められるため）。

パスワードが認証に使用される場合、ハッシュ化パスワードを使用するデータベースに対しての認証でこのプロトコルを使用できます。これは、パスワードがオーセンティケータにクリアテキストで渡されるためです。この方式は、データベースがリークしている可能性がある場合に推奨されます。

EAP-TLS

EAP-Transport Layer Security（EAP-TLS）は、TLSプロトコル（RFC 2246）に基づくIEEE 802.1X EAP 認証アルゴリズムです。TLS は、X.509デジタル証明書に基づく相互認証を使用します。EAP-TLS メッセージ交換は、相互認証、暗号スイート ネゴシエーション、キー交換、クライアントと認証サーバ間の検証、およびトラフィック暗号化に使用できるキー関連情報を提供します。

次のリストに、EAP-TLSクライアント証明書が有線およびワイヤレス接続に強固な認証を提供できる主な理由を示します。

- 通常、ユーザが介入することなく認証が自動で実行される。
- ユーザ パスワードへの依存がない。
- デジタル証明書が強固な認証保護を提供する。
- メッセージ交換が公開キー暗号化により保護される。
- 証明書がディクショナリ攻撃の被害を受けにくい。
- 認証プロセスにより、データ暗号化および署名のための相互決定されたキーが生成される。

EAP-TLS には、次の 2 つのオプションが含まれています。

- [サーバ証明書の確認（Validate Server Certificate）]：サーバ証明書の検証を有効にします。
- [高速再接続を有効にする（Enable Fast Reconnect）]：TLS セッション再開を有効にします。これにより、TLS セッション データがクライアントとサーバの両方で保持されている限り、短縮化した TLS ハンドシェイクを使用することによってはるかに高速な再認証ができます。

（注） [スマート カードを使用するときは無効にする（Disable When Using a Smart Card）] オプションは、マシン接続認証では使用できません。

EAP-TTLS

EAP-Tunneled Transport Layer Security（EAP-TTLS）は、EAP-TLS 機能を拡張する 2 フェーズのプロトコルです。フェーズ 1 では、完全な TLS セッションを実行して、フェーズ 2 で使用するセッション キーを導出し、サーバとクライアント間で属性を安全にトンネリングします。フェーズ2 中では、トンネリングされた属性を使用して、多数のさまざまなメカニズムを使用する追加認証を実行できます。

ネットワーク アクセス マネージャは、EAP-TTLS 認証中に使用する内部および外部方式の暗号化バインドをサポートしません。暗号化バインドが必要な場合は、EAP-FAST を使用する必要があります。暗号化バインドは、クレデンシャルを知らなくても攻撃者がユーザの接続をハイジャックできる中間者攻撃の特殊クラスからの保護を提供します。

フェーズ 2 で使用できる認証メカニズムには、次のプロトコルが含まれます。

- PAP（パスワード認証プロトコル）：ピアが 2 ウェイ ハンドシェイクを使用してそのアイデンティティを証明する単純な方式を提供します。ID/パスワード ペアは、認証が認められるか失敗するまで、ピアからオーセンティケータに繰り返し送信されます。相互認証が必要な場合は、EAP-TTLS を設定して、フェーズ 1 でサーバの証明書を検証する必要があります。

パスワードがオーセンティケータに渡されるため、ハッシュ化パスワードを使用するデータベースに対しての認証でこのプロトコルを使用できます。データベースがリークしている可能性がある場合は、この方式をお勧めします。

（注） EAP-TTLS PAP は、トークンおよびOTP ベースの認証で使用できます。

- CHAP（チャレンジ ハンドシェイク認証プロトコル）：3 ウェイ ハンドシェイクを使用してピアのアイデンティティを検証します。相互認証が必要な場合は、EAP-TTLS を設定して、フェーズ 1 でサーバの証明書を検証する必要があります。このチャレンジ/レスポンス方式を使用する場合、オーセンティケータのデータベースにクリア テキスト パスワードを保存する必要があります。
- MS-CHAP（Microsoft CHAP）：3 ウェイ ハンドシェイクを使用してピアのアイデンティティを検証します。相互認証が必要な場合は、EAP-TTLS を設定して、フェーズ 1 でサーバの証明書を検証する必要があります。パスワードのNT-hash に基づいてこのチャレンジ/レスポンス方式を使用する場合は、オーセンティケータのデータベースにクリアテキストパスワード、または最低でもパスワードのNT-hash のいずれかを保存しておく必要があります。
- MS-CHAPv2：応答パケット内にピア チャレンジおよび成功パケット内にオーセンティケータ応答を含めることによって、ピア間の相互認証を提供します。サーバの前に、クライアントが認証されます。（ディクショナリ攻撃を防ぐために）サーバをクライアントの前に認証する必要がある場合、EAP-TTLS を設定してフェーズ 1 でサーバの証明書を検証する必要があります。パスワードのNT-hash に基づいてこのチャレンジ/レスポンス方式を使用する場合は、オーセンティケータのデータベースにクリア テキスト パスワード、または最低でもパスワードの NT-hash のいずれかを保存しておく必要があります。

EAP-TTLS の設定

- EAP：次の EAP 方法の使用を許可します。
  - EAP-MD5（EAP Message Digest 5）：3 ウェイ ハンドシェイクを使用してピアのアイデンティティを検証します（CHAP と類似）。このチャレンジ/レスポンス方式を使用する場合、オーセンティケータのデータベースにクリア テキスト パスワードを保存する必要があります。
  - EAP-MSCHAPv2：3 ウェイ ハンドシェイクを使用してピアのアイデンティティを確認します。サーバの前に、クライアントが認証されます。（ディクショナリ攻撃の防止のためなどで）サーバをクライアントの前に認証する必要がある場合、EAP-TTLS を設定してフェーズ 1 でサーバの証明書を検証する必要があります。パスワードのNT-hash に基づいてこのチャレンジ/レスポンス方式を使用して、オーセンティケータのデータベースにクリアテキストパスワード、または最低でもパスワードのNT-hash のいずれかを保存しておく必要があります。
- EAP-TTLS 設定

- [サーバ ID の検証（Validate Server Identity）]：サーバ証明書の検証を有効にします。

（注） これを有効にする場合は、RADIUS サーバにインストールされたサーバ証明書にサーバ認証の拡張キーの使用状況（EKU）が含まれていることを確認します。RADIUS サーバでは、認証時にクライアントにその設定済みの証明書を送信するとき、ネットワークアクセスおよび認証のためにこのサーバ認証設定が必要です。

- [高速再接続を有効にする（Enable Fast Reconnect）]：内部認証が省略されるかどうか、またはオーセンティケータによって制御されているかどうかに関係なく、外部 TLS セッション再開のみを有効にします。

（注） [スマート カードを使用するときは無効にする（Disable When Using a Smart Card）] は、マシン接続認証では使用できません。

- [内部方式（Inner Methods）]：TLS トンネルが作成された後で内部方式の使用を指定します。Wi-Fi メディア タイプにのみ使用できます。

PEAP オプション

Protected EAP（PEAP）は、トンネリング TLS ベースの EAP 方式です。PEAP は、内部認証方式の暗号化に対するクライアント認証の前に、サーバ認証に TLS を使用します。内部認証は、信頼される暗号保護されたトンネル内部で実行され、証明書、トークン、およびパスワードを含む、さまざまな内部認証方式をサポートします。ネットワーク アクセス マネージャは、PEAP 認証中に使用する内部および外部方式の暗号化バインドをサポートしません。暗号化バインドが必要な場合は、EAP-FAST を使用する必要があります。暗号化バインドは、クレデンシャルを知らなくても攻撃者がユーザの接続をハイジャックできる中間者攻撃の特殊クラスからの保護を提供します。

PEAP は、次のサービスを提供することによって EAP 方式を保護します。

- EAP パケットに対する TLS トンネル作成
- メッセージ認証
- メッセージの暗号化
- クライアントに対するサーバの認証

次の認証方式を使用できます。

- パスワードを使った認証
  - EAP-MSCHAPv2：3 ウェイ ハンドシェイクを使用してピアのアイデンティティを確認します。サーバの前に、クライアントが認証されます。（ディクショナリ攻撃の防

止のためなどで）サーバをクライアントの前に認証する必要がある場合、PEAP を設定してサーバの証明書を検証する必要があります。パスワードの NT-hash に基づいてチャレンジ/レスポンス方式を使用して、オーセンティケータのデータベースにクリアテキストパスワード、または最低でもパスワードの NT-hash のいずれかを保存しておく必要があります。

- EAP-GTC（EAP Generic Token Card）：ユーザ名とパスワードを伝送するために EAP エンベロープを定義します。相互認証が必要な場合は、PEAP を設定してサーバの証明書を検証する必要があります。パスワードがクリアテキストでオーセンティケータに渡されるため、ハッシュ化パスワードを使用するデータベースに対しての認証でこのプロトコルを使用できます。この方式は、データベースがリークしている可能性がある場合に推奨されます。

- 証明書を使った EAP-TLS
  - EAP-TLS：ユーザ証明書を伝送するために EAP エンベロープを定義します。中間者攻撃（有効なユーザの接続のハイジャック）を避けるため、同じオーセンティケータに対する認証用に PEAP（EAP-TLS）および EAP-TLS プロファイルを混在させないことをお勧めします。その設定に応じて、オーセンティケータを設定する必要があります（プレーンおよびトンネリングされた EAP-TLS の両方を有効にしない）。

PEAP の設定

- PEAP-EAP 設定
  - [サーバ ID の検証（Validate Server Identity）]：サーバ証明書の検証を有効にします。

（注） これを有効にする場合は、RADIUS サーバにインストールされたサーバ証明書にサーバ認証の拡張キーの使用状況（EKU）が含まれていることを確認します。RADIUS サーバでは、認証時にクライアントにその設定済みの証明書を送信するとき、ネットワークアクセスおよび認証のためにこのサーバ認証設定が必要です。

  - [高速再接続を有効にする（Enable Fast Reconnect）]：外部 TLS セッション再開のみを有効にします。オーセンティケータは、内部認証を省略するかどうかを制御します。
  - [スマート カードを使用するときは無効にする（Disable When Using a Smart Card）]：スマートカードを使用して認証する場合に高速再接続を使用しません。スマートカードは、ユーザ接続にのみ適用されます。
  - [トークンおよび EAP-GTC を使用して認証する（Authenticate using a token and EAP-GTC）]：マシン認証には使用できません。

- クレデンシャル ソースに基づく内部方式

- [パスワードを使用した認証（Authenticate using a password）]：[EAP-MSCHAPv2] または [EAP-GTC]。
- [証明書を使用した認証（Authenticate using a certificate）]：EAP-TLS に対応。
- [トークンおよび EAP-GTC を使用して認証する（Authenticate using a token and EAP-GTC）]：マシン認証には使用できません。

（注） ユーザ ログインの前に、スマート カードのサポートは Windows では使用できません。

EAP-FAST 設定

EAP-FAST は、IEEE 802.1X 認証タイプで、柔軟性があり、展開や管理も容易です。EAP-FAST は、さまざまなユーザおよびパスワード データベース タイプ、サーバ主導のパスワードの失効と変更、およびデジタル証明書（任意）をサポートします。

EAP-FAST は、証明書を使用せず、ディクショナリ攻撃からの保護を提供する IEEE 802.1X EAP タイプを展開するお客様向けに開発されました。

AnyConnect 3.1 の時点では、マシン接続とユーザ接続の両方が設定されている場合、EAP チェーンがサポートされています。これは、ネットワーク アクセス マネージャが、マシンおよびユーザが既知のエンティティであり、企業によって管理されていること検証することを意味し、社内ネットワークに接続しているユーザ所有資産を制御するのに便利です。EAP チェーンの詳細については、RFC 3748 を参照してください。

EAP-FAST は、TLS メッセージを EAP 内にカプセル化します。また、次の 3 つのプロトコル フェーズから構成されます。

1. Authenticated Diffie-Hellman Protocol（ADHP）を使用して Protected Access Credential（PAC）と呼ばれる共有秘密クレデンシャルを持つクライアントをプロビジョニングするプロビジョニング フェーズ。
2. トンネルの確立に PAC を使用するトンネル確立フェーズ。
3. 認証サーバでユーザのクレデンシャル（トークン、ユーザ名/パスワード、またはデジタル証明書）を認証する認証フェーズ。

他のトンネリング EAP 方式とは異なり、EAP-FAST は内部および外部方式間に暗号化バインドを提供して、攻撃者が有効なユーザの接続をハイジャックする特殊な中間者攻撃を防止します。

EAP-FAST の設定

- EAP-FAST 設定
  - [サーバ ID の検証（Validate Server Identity）]：サーバ証明書の検証を有効にします。これを有効にすると、管理ユーティリティに 2 つの追加のダイアログが導入されて、

ネットワーク アクセス マネージャ プロファイル エディタのタスク リストに [証明書（Certificate）] ペインがさらに追加されます。

（注） これを有効にする場合は、RADIUS サーバにインストールされたサーバ証明書にサーバ認証の拡張キーの使用状況（EKU）が含まれていることを確認します。RADIUS サーバでは、認証時にクライアントにその設定済みの証明書を送信するとき、ネットワークアクセスおよび認証のためにこのサーバ認証設定が必要です。

- [高速再接続を有効にする（Enable Fast Reconnect）]：セッション再開を有効にします。EAP-FAST で認証セッションを再開する 2 つのメカニズムには、内部認証を再開するユーザ認可 PAC と、短縮化した外部 TLS ハンドシェイクができる TLS セッション再開があります。この [高速再接続を有効にする（Enable Fast Reconnect）] パラメータは、両方のメカニズムを有効または無効にします。オーセンティケータがいずれを使用するかを決定します。

（注） マシン PAC は、短縮化した TLS ハンドシェイクを提供し、内部認証を省きます。この制御は、PAC パラメータを有効/無効にすることによって処理します。

（注） [スマート カードを使用するときは無効にする（Disable When Using a Smart Card）] オプションは、ユーザ接続認証にのみ使用できます。

- [クレデンシャル ソースに基づく内部方式（Inner methods based on Credentials Source）]：パスワードまたは証明書を使用する認証ができます。
  - [パスワードを使用した認証（Authenticate using a password）]：[EAP-MSCHAPv2] または [EAP-GTC]。EAP-MSCHAPv2 は、相互認証を提供しますが、サーバを認証する前にクライアントを認証します。サーバを最初に認証する相互認証を使用する場合は、EAP-FAST を認証付きプロビジョニングのみに設定して、サーバの証明書を検証します。パスワードの NT-hash に基づいてこのチャレンジ/レスポンス方式を使用して、EAP-MSCHAPv2 を使用する場合は、オーセンティケータのデータベースにクリア テキスト パスワード、または最低でもパスワードの NT-hash のいずれかを保存しておく必要があります。パスワードは EAP-GTC 内でクリア テキストでオーセンティケータに渡されるため、データベースに対する認証でこのプロトコルを使用できます。
  - パスワードベースの内部方式を使用している場合、認証されていない PAC プロビジョニングを許可する追加オプションが使用できます。

- [証明書を使用した認証（Authenticate using a certificate）]：証明書を使用する認証に対しての基準を、要求された場合にクライアント証明書を暗号化しないで送信、トンネル内でのみクライアント証明書を送信、またはトンネル内で EAP-TLS を使用してクライアント証明書を送信から決定します。
- トークンおよび EAP-GTC を使用して認証します。

- [PAC を使用する（Use PACs）]：EAP-FAST 認証での PAC の使用を指定できます。PAC は、ネットワーク認証を最適化するためにクライアントに配布されるクレデンシャルです。

（注） EAP-FAST では大半の認証サーバが PAC を使用するため、通常は PAC オプションを使用します。このオプションを削除する前に、認証サーバが EAP-FAST で PAC を使用しないことを確認します。使用する場合は、クライアントの認証試行が失敗します。認証サーバが認証された PAC プロビジョニングをサポートする場合は、認証されていないプロビジョニングを無効にすることを推奨します。未認証のプロビジョニングは、サーバ証明書を検証しないため、侵入者がディクショナリ ベースの攻撃を仕掛けることができる可能性があります。

LEAP 設定

LEAP（Lightweight EAP）はワイヤレス ネットワークに対応しています。拡張認証プロトコル（EAP）フレームワークに基づき、WEP よりセキュアなプロトコルを作成するためシスコにより開発されました。

（注） 強力なパスワードおよび定期的に失効するパスワードを使用しない限り、LEAP はディクショナリ攻撃を受ける場合があります。認証方式がディクショナリ攻撃の被害を受けにくい EAP-FAST、PEAP、または EAP-TLS を使用することをお勧めします。

ユーザ認証にのみ使用できる LEAP 設定：

- ログオフを越えたユーザ接続の延長：ユーザがログオフしても接続は開いたままです。同じユーザが再度ネットワークにログインしても、接続はアクティブのままです。

詳細については、「Dictionary Attack on Cisco LEAP Vulnerability」を参照してください。

ネットワーク クレデンシャルの定義

[ネットワーク（Networks）]>[クレデンシャル（Credentials）]ペインで、ユーザ クレデンシャルまたはマシン クレデンシャルのいずれを使用するか指定し、信頼サーバ検証ルールを設定します。

ユーザ クレデンシャルの設定

EAP カンバセーションには、複数の EAP 認証方式が含まれ、その各認証で要求されるアイデンティティが異なる場合があります（マシン認証の次にユーザ認証が行われるなど）。たとえば、ピアでは最初に nouser@cisco.com のアイデンティティを要求して認証要求を cisco.com EAP サーバにルーティングする場合があります。しかし、いったん TLS セッションがネゴシエートされると、そのピアは johndoe@cisco.com のアイデンティティを要求する場合があります。そのため、ユーザのアイデンティティにより保護が提供される場合でも、カンバセーションがローカル認証サーバで終端しない限り、宛先領域は必ずしも一致しません。

ユーザ接続で、プレースホルダ [username] および [domain] を使用する場合、次の条件が当てはまります。

- 認証にクライアント証明書を使用する場合：さまざまな X509 証明書プロパティから [username] および [password] のプレースホルダ値を取得します。プロパティは最初の一致に応じて次の順序で解析されます。たとえば、ユーザ認証のアイデンティティが userA@example.com（ユーザ名 =userA、ドメイン =example.com）、マシン認証のアイデンティティが hostA.example.com（ユーザ名 =hostA、ドメイン =example.com）の場合、次のプロパティが解析されます。
- ユーザ証明書ベースの認証の場合：
  - SubjectAlternativeName: UPN = userA@example.com
  - Subject = .../CN=userA@example.com/...
  - Subject = userA@eample.com
  - Subject = .../CN=userA/DC=example/DC=com/...
  - Subject = userA (no domain)
- マシン証明書ベースの認証の場合：
  - SubjectAlternativeName: DNS = hostA.example.com
  - Subject = .../DC=hostA.example.com/...
  - Subject = .../CN=hostA.example.com/...
  - Subject = hostA.example.com
- クレデンシャルのソースがエンドユーザの場合：ユーザが入力する情報からプレースホルダ値を取得します。
- クレデンシャルがオペレーティング システムから取得される場合：ログイン情報からプレースホルダ値を取得します。
- クレデンシャルが静的である場合：プレースホルダを使用しません。

[クレデンシャル（Credentials）] ペインでは、目的のクレデンシャルを関連付けられたネットワークの認証で使用するために指定できます。

手順

ステップ 1 [保護されたアイデンティティ パターン（Protected Identity Pattern）] でユーザ アイデンティティを定義します。ネットワーク アクセス マネージャでは、次のアイデンティティ プレースホルダのパターンがサポートされます。

- [username]：ユーザ名を指定します。ユーザが username@domain または domain\username を入力した場合、ドメインの部分は削除されます。
- [raw]：ユーザの入力のとおりにユーザ名を指定します。
- [domain]：ユーザ デバイスのドメインを指定します。

ステップ 2 一般的な、保護されていないアイデンティティ パターンを指定します。

まだネゴシエートされていないセッションでは、整合性保護または認証なしで、暗号化されていないアイデンティティ要求および応答が発生します。これらのセッションは、スヌーピングおよびパケット変更の対象になります。

- anonymous@[domain]：値がクリア テキストで送信されるときに、ユーザ アイデンティティを隠すために、トンネリングされた方式内でよく使用されます。実際のユーザ アイデンティティは、保護されたアイデンティティとして、内部方式で提供されます。
- [username]@[domain]：トンネリングされていない方式の場合。

（注） 保護されていないアイデンティティ情報はクリア テキストで送信されます。最初のクリア テキスト アイデンティティ要求または応答が改ざんされた場合は、TLS セッションが確立されるとサーバがアイデンティティを検証できないことを検出することがあります。たとえば、ユーザ ID が無効であるか、または EAP サーバが処理する領域内にない場合があります。

ステップ 3 保護されるアイデンティティ パターンを指定します。

ユーザ ID をスヌーピングから保護するために、クリア テキスト アイデンティティは、認証要求の正しい領域へのルーティングを有効にするために必要な情報のみを指定する場合があります。

- [username]@[domain]
- ユーザのアイデンティティとして使用する実際の文字列（プレースホルダなし）

ステップ 4 次のユーザ クレデンシャル情報をさらに提供します。

- [シングル サインオン クレデンシャルを使用（Use Single Sign On Credentials）]：クレデンシャルをオペレーティング システムのログイン情報から取得します。ログイン クレデンシャルが失敗すると、ネットワーク アクセス マネージャは一時的に（次のログインまで）切り替わり、ユーザに GUI でクレデンシャルの入力を求めます。

（注） ネットワークアクセスマネージャおよびSSOで、Windowsログイン クレデンシャルを自動的に使用することはできません。ネットワーク アクセス マネージャでSSOを使用するには、ログオン クレデンシャルを代行受信する必要があります。したがって、インストールまたはログオフの後に再起動を求められます。

- [スタティック クレデンシャルを使用（Use Static Credentials）]：ユーザ クレデンシャルをこのプロファイル エディタが提供するネットワーク プロファイルから取得します。スタティック クレデンシャルが失敗すると、ネットワーク アクセス マネージャは、新しい設定がロードされるまでクレデンシャルを再度使用しません。

  （注） アンパサンドはこのフィールドで無効な文字です。

- [クレデンシャルのプロンプト（Prompt for Credentials）]：クレデンシャルを次に指定されたとおりにAnyConnect GUIを使用してエンドユーザから取得します。
  - [永久に記憶（Remember Forever）]：クレデンシャルは永久に記憶されます。記憶されたクレデンシャルが失敗すると、ユーザはクレデンシャルの入力を再度求められます。クレデンシャルはファイルに保存され、ローカル マシン パスワードを使用して暗号化されます。
  - [ユーザのログイン中記憶（Remember while User is Logged On）]：クレデンシャルはユーザがログオフするまで記憶されます。記憶されたクレデンシャルが失敗すると、ユーザはクレデンシャルの入力を再度求められます。
  - [記憶しない（Never Remember）]：クレデンシャルは一切記憶されません。ネットワーク アクセス マネージャは、認証のためにクレデンシャル情報が必要なたびに、ユーザに入力を求めます。

ステップ5 証明書が要求されたときに、認証のためにいずれの証明書ソースを使用するかを決定します。

- [スマート カードまたはOS証明書（Smart Card or OS certificates）]：ネットワーク アクセス マネージャは、OSの証明書ストアまたはスマート カードで検出される証明書を使用します。
- [スマート カード証明書のみ（Smart Card certificates only）]：ネットワーク アクセス マネージャは、スマート カードで検出される証明書のみを使用します。

ステップ6 [スマート カード PIN を記憶（Remember Smart Card Pin）] パラメータでは、ネットワーク アクセス マネージャがスマート カードから証明書を取得するために使用したPINを記憶する期間を決定します。使用できるオプションについては、ステップ2を参照してください。

（注） PIN は、証明書自体よりも長く保存されることは決してありません。

別名 Cryptographic Service Provider（CSP）および Key Storage Provider（KSP）というスマートカードのチップとドライバによっては、他より接続に時間がかかるスマートカードもあります。接続タイムアウトを長くすると、ネットワークにスマートカードベースの認証を実行するのに十分な時間を与えることができます。

マシン クレデンシャルの設定

EAP カンバセーションには、複数の EAP 認証方式が含まれ、その各認証で要求されるアイデンティティが異なる場合があります（マシン認証の次にユーザ認証が行われるなど）。たとえば、ピアでは最初に nouser@example.com のアイデンティティを要求して認証要求を cisco.com EAP サーバにルーティングする場合があります。しかし、いったん TLS セッションがネゴシエートされると、そのピアは johndoe@example.com のアイデンティティを要求する場合があります。そのため、ユーザのアイデンティティにより保護が提供される場合でも、カンバセーションがローカル認証サーバで終端しない限り、宛先領域は必ずしも一致しません。

マシン接続の場合に、[username] および [domain] プレースホルダが使用されたときは、常に次の条件が適用されます。

- 認証にクライアント証明書を使用する場合：さまざまな X509 証明書プロパティから [username] および [password] のプレースホルダ値を取得します。プロパティは最初の一致に応じて次の順序で解析されます。たとえば、ユーザ認証のアイデンティティが userA@cisco.com（ユーザ名 =userA、ドメイン =cisco.com）、マシン認証のアイデンティティが hostA.cisco.com（ユーザ名 =hostA、ドメイン =cisco.com）の場合、次のプロパティが解析されます。
- ユーザ証明書ベースの認証の場合：
  - SubjectAlternativeName: UPN = userA@example.com
  - Subject = .../CN=userA@example.com/...
  - Subject = userA@example.com
  - Subject = .../CN=userA/DC=example.com/...
  - Subject = userA (no domain)
- マシン証明書ベースの認証の場合：
  - SubjectAlternativeName: DNS = hostA.example.com
  - Subject = .../DC=hostA.example.com/...
  - Subject = .../CN=hostA.example.com/...
  - Subject = hostA.example.com
- クライアント証明書が認証に使用されない場合：クレデンシャルをオペレーティング システムから取得し、[username] プレースホルダは割り当てられたマシン名を表します。

[クレデンシャル（Credentials）] パネルでは、目的のマシン クレデンシャルを指定できます。

手順

ステップ 1 [保護されているアイデンティティ パターン（Protected Identity Pattern）] でマシン アイデンティティを定義します。ネットワーク アクセス マネージャでは、次のアイデンティティ プレースホルダのパターンがサポートされます。

- [username]：ユーザ名を指定します。ユーザが username@domain または domain\username を入力した場合、ドメインの部分は削除されます。
- [raw]：ユーザの入力のとおりにユーザ名を指定します。
- [domain]：ユーザの PC のドメインを指定します。

ステップ 2 典型的な保護されていないマシン アイデンティティのパターンを定義します。

まだネゴシエートされていないセッションでは、整合性保護または認証なしで、暗号化されていないアイデンティティ要求および応答が発生します。これらのセッションは、スヌーピングおよびパケット変更の対象になります。

- host/anonymous@[domain]
- マシンのアイデンティティとして送信する実際の文字列（プレースホルダなし）

ステップ 3 保護されているマシン アイデンティティのパターンを定義します。

ユーザ ID をスヌーピングから保護するために、クリア テキスト アイデンティティは、認証要求の正しい領域へのルーティングを有効にするために必要な情報のみを指定する場合があります。典型的な保護されているマシン アイデンティティのパターンは次のとおりです。

- host/[username]@[domain]
- マシンのアイデンティティとして使用する実際の文字列（プレースホルダなし）

ステップ 4 次のマシン クレデンシャル情報をさらに提供します。

- [マシン クレデンシャルを使用（Use Machine Credentials）]：クレデンシャルをオペレーティング システムから取得します。
- [スタティック クレデンシャルを使用（Use Static Credentials）]：展開ファイルに送信する実際のスタティック パスワードを指定します。スタティック クレデンシャルは、証明書ベースの認証には適用されません。

適切な証明書を選択するためのネットワーク アクセス マネージャの設定

クライアント認証時に 2 つの証明書が存在する場合、ネットワーク アクセス マネージャは証明書の属性に基づいて最適な証明書を自動的に選択します。優先する証明書の条件は顧客に

よって異なるため、次に示す証明書の選択を定義するフィールドを設定し、また証明書選択をオーバーライドするルールを指定する必要があります。

複数の証明書が同一ルールに一致するか、ルールに一致する証明書がない場合は、ACEエンジンが、証明書の優先順位を指定するアルゴリズムを実行し、特定の基準（秘密キーがあるかどうか、マシン ストアからの証明書であるかどうかなど）に基づいて証明書を選択します。複数の証明書の優先順位が同一の場合、ACEエンジンはその優先順位で最初に検出した証明書を選択します。

手順

ステップ 1 AnyConnect プロファイル エディタから [ネットワーク（Networks）] タブを選択します。

ステップ 2 編集するネットワークを選択します。

ステップ 3 [マシンクレデンシャル（Machine Credentials）] タブを選択します。

ステップ 4 ページ下部で [証明書一致ルールを使用する（Use Certificate Matching Rule）] を選択します。

ステップ 5 [証明書フィールド（Certificate Field）] ドロップダウン メニューから、検索条件として使用するフィールドを選択します。

ステップ 6 [一致（Match）] ドロップダウン メニューから、検索にフィールドの完全一致（[等しい（Equals）]）または部分一致（[含む（Includes）]）を含めるかどうかを指定します。

ステップ 7 [値（Value）] フィールドに、証明書の検索条件を入力します。

信頼サーバ検証ルールの設定

[サーバ ID の検証（Validate Server Identity）] オプションが [EAP] 方式に設定されている場合、[証明書（Certificate）] パネルが有効になって証明書サーバまたは認証局に対する検証ルールを設定できます。検証の結果によって、証明書サーバまたは認証局が信頼されるかどうかが決定されます。

証明書サーバの検証ルールを定義するには、次の手順を実行します。

手順

ステップ 1 オプション設定が [証明書フィールド（Certificate Field）] および [一致（Match）] カラムに表示されたときに、ドロップダウン矢印をクリックし、目的の設定を選択します。

ステップ 2 [値（Value）] フィールドに、値を入力します。

ステップ 3 ルールの下で [追加（Add）] をクリックします。

ステップ 4 [証明書信頼済み認証局（Certificate Trusted Authority）] ペインで、次のいずれかのオプションを選択します。

- [OS にインストールされたすべてのルート認証局（CA）を信頼（Trust any Root Certificate Authority (CA) Installed on the OS）]：選択すると、ローカル マシンまたは証明書ストアのみがサーバの証明書チェーン検証の対象になります。

- [ルート認証局（CA）証明書を含める（Include Root Certificate Authority (CA) Certificates）]。

（注） [ルート認証局（CA）証明書を含める（Include Root Certificate Authority (CA) Certificates）] を選択した場合は、[追加（Add）] をクリックして CA 証明書を設定にインポートする必要があります。使用している証明書が Windows 証明書ストアからエクスポートされる場合は、[Base 64 encoded X.509 (.cer)] オプションを使用します。

[ネットワーク グループ（Network Groups）] ウィンドウ

[ネットワーク グループ（Network Groups）] ウィンドウで、ネットワーク接続を特定のグループに割り当てます。接続をグループに分類することにより、次の複数の利点がもたらされます。

- 接続の確立試行時のユーザエクスペリエンスの向上。複数の非表示ネットワークが設定された場合、接続が正常に確立するまで、クライアントは非表示ネットワークのリストを定義された順序で順を追って調べます。このような場合に、接続を確立するために必要な時間を大幅に短縮するためにグループが使用されます。
- 設定された接続の管理の簡略化。企業内で複数の役割を持つ（または同じ領域に頻繁にアクセスする）ユーザがグループ内のネットワークを調整して選択可能なネットワークのリストを管理しやすくする場合に、管理者ネットワークをユーザネットワークから分離できます。

配布パッケージの一部として定義されたネットワークはロックされています。これは、ユーザが設定を編集することや、ネットワーク プロファイルを削除することを防止するためです。

ネットワークをグローバルとして定義できます。グローバルとして定義すると、ネットワークは [グローバル ネットワーク（Global Networks）] セクションに表示されます。このセクションは、有線とワイヤレス ネットワーク タイプの間で分割されます。このタイプのネットワークに対しては、ソート順序の編集のみを実行できます。

すべての非グローバル ネットワークは、グループ内に存在する必要があります。1 つのグループがデフォルトで作成されています。すべてのネットワークがグローバルの場合にそのグループを削除できます。

手順

ステップ 1 ドロップダウン リストからグループを選択します。

ステップ 2 [ネットワークの作成（Create networks）] を選択して、エンドユーザがこのグループ内にネットワークを作成できるようにします。これをオフにした場合、展開されたときにネットワークアクセスマネージャはこのグループからユーザ作成ネットワークをすべて削除します。これにより、ユーザがネットワーク設定を別のグループに再入力する必要が生じることがあります。

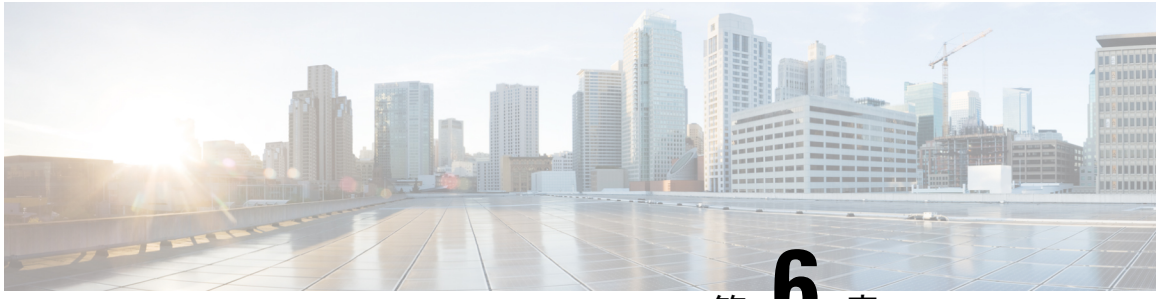
ステップ 3 [スキャン リストの表示（See scan list）] を選択して、AnyConnect GUI を使用してグループがアクティブ グループとして選択されたときに、エンド ユーザがスキャン リストを表示できるようにします。または、このチェックボックスをオフにして、ユーザによるスキャン リストの表示を制限します。たとえば、ユーザが近くのデバイスに誤って接続することを防ぐ必要がある場合に、スキャン リストへのアクセスを制限します。

（注） これらの設定は、グループごとに適用されます。

ステップ 4 右矢印および左矢印を使用して、[グループ（Group）] ドロップダウン リストから選択したグループに対してネットワークを挿入または削除します。ネットワークが現在のグループから移動された場合は、デフォルト グループに配置されます。デフォルト グループを編集する場合、デフォルト グループからネットワークを移動できません（[>] ボタンを使用）。

（注） 指定のネットワーク内で、各ネットワークの表示名は一意である必要があります。このため、1 つのグループには同じ表示名を持つ 2 つ以上のネットワークを含められません。

ステップ 5 上矢印および下矢印を使用してグループ内のネットワークの優先順位を変更します。



第 6 章

ポスチャの設定

AnyConnect Secure Mobility Client は VPN ポスチャ（HostScan）モジュールおよび ISE ポスチャ モジュールを提供します。両方のモジュールにより、Cisco AnyConnect Secure Mobility Client で、ホストにインストールされたアンチウイルス、アンチスパイウェア、ファイアウォール ソフトウェアなどについてエンドポイントのコンプライアンスを評価できます。その後、エンドポイントがコンプライアンスに対応するまでネットワーク アクセスを制限したり、修復方法を確立できるようにローカル ユーザの権限を強化したりできます。

VPN ポスチャは、hostscan_version.pkg にバインドされています。これは、どのようなオペレーティング システム、アンチウイルス、アンチスパイウェア、およびソフトウェアがホストにインストールされているかを収集するアプリケーションです。ISE ポスチャは、ISE 制御ネットワークにアクセスするときに、AnyConnect と NAC Agent の両方を展開するのではなく、1 つのクライアントを展開します。ISE ポスチャは、AnyConnect 製品に（Web セキュリティやネットワーク アクセス マネージャなどと同じように）追加のセキュリティ コンポーネントとしてインストールできるモジュールです。リリース 3.x の AnyConnect バンドルの一部であった HostScan は、別個にインストールされるようになりました。

ISE ポスチャは、クライアント側評価を実行します。クライアントは、ヘッドエンドからポスチャ要件ポリシーを受信し、ポスチャ データ収集を実行し、結果をポリシーと比較し、評価結果をヘッドエンドに返します。エンドポイントがコンプライアンス対応かどうかを実際には ISE が判断する場合でも、ISE はエンドポイント独自のポリシー評価を利用します。

一方、HostScan はサーバ側評価を実行します。ASA がエンドポイント属性（オペレーティング システム、IP アドレス、レジストリ エントリ、ローカル証明書、ファイル名など）のリストのみを要求し、これらが HostScan によって返されます。ポリシーの評価結果に基づいて、どのホストがセキュリティ アプライアンスへのリモート アクセス接続を確立できるかを制御できます。

（注） 2 つの異なるポスチャ エージェントを実行すると予期しない結果が生じる可能性があるため、HostScan と ISE ポスチャ エージェントの組み合わせは推奨されません。

次のポスチャチェックは、HostScan ではサポートされていますが、ISE ポスチャではサポートされていません。ホスト名、IP アドレス、MAC アドレス、ポート番号、OPSWAT バージョン、BIOS シリアル番号、および証明書フィールド属性です。

• ISE ポスチャ モジュールの提供内容 （232 ページ）
• AnyConnect ISE フローを中断する操作 （240 ページ）
• ISE ポスチャのステータス （241 ページ）
• ポスチャとマルチホーミング （243 ページ）
• エンドポイントの同時ユーザ （243 ページ）
• ポスチャ モジュールのロギング （244 ページ）
• ポスチャ モジュールのログ ファイルと場所 （244 ページ）
• ISE ポスチャ プロファイル エディタ （245 ページ）
• [詳細（Advanced）] パネル （247 ページ）
• VPN ポスチャ（HostScan）モジュールの提供内容 （248 ページ）
• OPSWAT サポート （252 ページ）

ISE ポスチャ モジュールの提供内容

ポスチャ チェック

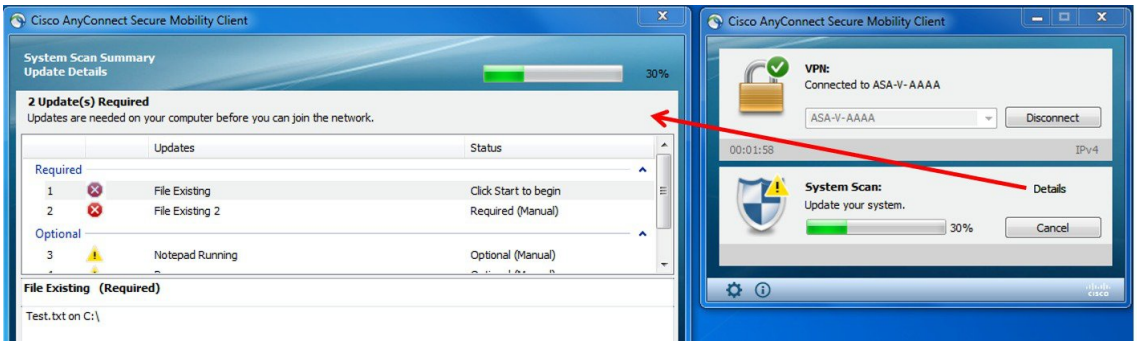
ISE ポスチャ モジュールはポスチャ チェックの実行に OPSWAT v3 または v4 ライブラリを使用します。初回のポスチャ チェックでは、すべての必須要件への一致に失敗したエンドポイントがすべて非準拠と見なされます。その他のエンドポイントの許可ステータスは、ポスチャ不明または準拠（必須要件に合致）です。

（注） macOS 64 ビットの移行では、AnyConnect 4.6 ISE ポスチャ モジュールは古い OPSWAT v3 準拠モジュールと互換性がありません。

ポスチャ チェック フェーズでエラーが発生し、AnyConnect が続行可能な場合、ユーザに通知されますが、可能な場合はポスチャのチェックが続行されます。必須のポスチャ チェック中にエラーが発生した場合、チェックは失敗とマークされます。ネットワーク アクセスは、すべての必須要件が満たされている場合に許可されます。そうでない場合、ユーザはポスチャ プロセスをリスタートできます。

必要な修復

修復ウィンドウはバックグラウンドで実行されるため、ネットワーク アクティビティのアップデートはポップアップ表示されず、干渉や中断は発生しません。AnyConnect UI の ISE ポスチャ タイル部分で [詳細（Details）] をクリックして、検出された内容およびネットワークに参加する前に必要なアップデート内容を確認できます。必須の手動修復が存在する場合、修復ウィンドウが開き、対処が必要な項目が表示されます。このシステム スキャン概要のウィンドウに、アップデートの進捗状況、割り当てられたアップデート時間の残り時間、すべての要件のステータス、およびシステムの準拠状態が表示されます。



管理者は、ISEポスチャプロセスの最後に表示されるネットワーク使用ポリシーを設定できます。ポリシーにアクセスすると、VLANへのアクセス権が付与される前にユーザが同意する必要のある必須の諸条件がすべて表示されます。

オプションのアップデートのみが残っている場合、[スキップ（Skip）] を選択して次の更新に進むことも、[すべてスキップ（Skip All）] を選択して残りの修復をすべて無視することも可能です。時間を節約するためにオプションの修復をスキップしても、ネットワーク アクセスは維持されます。

修復後（または修復が必要でない場合は要件チェック後）、アクセプタブル ユース ポリシーの通知を受け取る場合があります。この場合、ネットワーク アクセスのポリシーに同意する必要があり、同意しなかった場合はアクセスが制限されます。修復のこの部分では、AnyConnect UI のポスチャ タイル部分に、「システム スキャン：ネットワークのアクセプタブル ユース ポリシー（System Scan: Network Acceptable Use Policy）」と表示されます。

修復が完了すると、必須アップデートとしてリストされたチェック項目がすべて[完了（Done）] ステータスとなり、緑色のチェックボックスが表示されます。修復後、エージェントはISEにポスチャ結果を送信します。

（注） Symantec 製品のアーキテクチャの変更に伴い、ISE ポスチャでは Symantec AV 12.1.x 以降の修復がサポートされません。

パッチ管理チェックと修復

AnyConnect 4.x および Microsoft System Center Configuration Manager（SCCM）の統合により、パッチ管理チェックとパッチ管理修復が導入されました。エンドポイントで欠落している重要なパッチのステータスをチェックし、ソフトウェアパッチをトリガーするべきかどうか確認します。重要なパッチが Windows エンドポイントで欠落していない場合は、パッチ管理チェックは合格です。パッチ管理修復は、管理者レベルのユーザのみに対して、1つ以上の重要なパッチが Windows エンドポイントで欠落しているときにのみトリガーされます。

SCCMクライアントで、再起動前にインストールが行われるパッチをインストールすると、マシンが再起動するとすぐに、パッチのインストールステータス（インストール完了または未インストール）がレポートされます。ただし、SCCMクライアントで、再起動後にインストールが開始されるパッチをインストールすると、パッチのステータスはすぐにはレポートされません。

AnyConnect コンプライアンス モジュールは、この時点で SCCM クライアントにステータスの提供を強制できません。ポスチャ モジュール クライアントがネイティブ API 要求を完了するためにかかる時間は、さまざまな動的 OS パラメータ（CPU 負荷、保留中のパッチの量、パッチ インストール後の再起動なしなど）と、ネットワークの要因（ポスチャ モジュール クライアントとサーバ間の接続と遅延）に依存します。SCCM クライアントが応答するまで待機する必要があるかもしれませんが、既知のパッチによる一部のテスト結果は約 10 分でした。

同様の動作は、Windows Server Update Services（WSUS）の検索 API でも見られ、応答時間は長めで、20 ～ 30 分かかることもあります。Windows アップデートは、Windows OS だけでなく、すべてのマイクロソフト製品（Microsoft Office など）についてパッチの不足がないかチェックします。

ISE のポリシー状態の設定方法については「Policy Conditions」を参照してください。またパッチ管理修復の詳細については「Patch Management Remediation」を参照してください。

エンドポイント コンプライアンスの再評価

エンドポイントがコンプライアンス対応と見なされ、ネットワーク アクセスが許可されると、管理者が設定した制御に基づいてエンドポイントを任意で定期的に再評価できます。パッシブ再評価ポスチャ チェックは、初期のポスチャ チェックとは異なります。失敗した場合、ユーザには修復するオプションが与えられます（管理者がそのように設定していた場合）。この構成設定では、1 つ以上の必須要件が満たされていない場合でも、ユーザが信頼ネットワーク アクセスを維持するかどうかを制御します。初期のポスチャ評価では、すべての必須要件が満たされていないと、エンドポイントはコンプライアンス非対応と見なされます。この機能はデフォルトでは無効であり、ユーザ ロールに対して有効になっている場合、ポスチャは 1 ～ 24 時間ごとに再評価されます。

管理者は、結果を [続行（Continue）]、[ログオフ（Logoff）]、または [修復（Remediate）] に設定し、適用や猶予時間など他のオプションを設定できます。

非準拠デバイスの猶予期間

Cisco ISE の UI で猶予期間を設定することができます。これを設定すると、以前のポスチャ ステータスでは準拠していたが準拠しなくなったエンドポイントに、ネットワークへのアクセスを許可できるようになります。Cisco ISE は、以前に認識された良好な状態をキャッシュ内で探し、デバイスに猶予時間を提供します。猶予期間が終了すると、AnyConnect は再度ポスチャ チェックを行いますが、今回は修復を行いません。チェックの結果に基づいてエンドポイントの状態を準拠または非準拠と判断します。

（注） ユーザが猶予期間にいる場合は、定期的な再評価（PRA）は適用されません。

猶予期間は、ISE UI で **[ポリシー（Policy）] > [ポスチャ（Posture）]** または **[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [ポスチャポリシー（Posture Policy）]** の順に移動して、AnyConnect ポスチャ プロファイルに設定します。有効な値は、日、時間、または分単位で指定します。デフォルトでは、この設定は無効です。

AnyConnect UI では、エンドポイントが非準拠の場合に警告が表示され、猶予期間についての説明が表示されます。AnyConnect システム スキャン タイルにはすべてのポスチャ障害が強調表示され、[再度スキャン（Scan Again）] ボタンを押すと、ポスチャ ポリシーの再実行を強制して完全なネットワーク アクセスを維持できます。

（注） ISE ポスチャでは、猶予期間中の AUP ポリシーは許可されません。猶予期間は、一時的なエージェント、ハードウェアのインベントリ、アプリケーションのモニタリングなどのフローには適用されません。

シスコ テンポラル エージェント

シスコ テンポラル エージェントは、ユーザが信頼ネットワークにアクセスしているときにコンプライアンス ステータスを共有できるように、Windows または macOS 環境向けに設計されています。シスコ テンポラル エージェントの設定は、ISE UI で行います。シスコ テンポラル エージェントの実行ファイル .exe（Windows 用）または dmg（macOS 用）は、エンドポイントがインターネットへのアクセスを試行するたび、エンドポイントにダウンロードされます。ユーザは、ダウンロードした実行ファイルまたは dmg を実行し、コンプライアンス チェックを行う必要があります。これには、管理者権限は不要です。

UI が自動的に起動し、エンドポイントのコンプライアンスに問題がないか判断するチェックを開始します。コンプライアンス チェックが完了すると、ISE は、ISE UI でのポリシーの設定方法に基づいて必要なアクションを取れるようになります。

Windows では、実行ファイルは自己解凍されます。この解凍により、コンプライアンス チェックに必要なすべての dll およびその他のファイルが一時フォルダに保存されます。解凍されたファイルおよび実行ファイルは、コンプライアンス チェックの完了後、削除されます。ファイルおよび実行ファイルを完全に削除するには、ユーザが UI を終了する必要があります。

ISE UI での詳細な設定手順については、『*Cisco Identity Services Engine Administrator Guide, Release 2.3*』の「Cisco Temporal Agent Workflows」を参照してください。

シスコ テンポラル エージェントの制限事項

- macOS では、VLAN 制御のポスチャ環境は、ルート権限がないと更新アダプタ（DHCP 更新）プロセスが実行されないため、テンポラル エージェントについてはサポートされていません。テンポラル エージェントはユーザ プロセスとしてのみ実行できます。ACL 制御のポスチャ環境は、エンドポイントの IP を更新する必要がないため、サポートされています。
- 修復中にネットワーク インターフェイスが発生した場合、ユーザは、現在の UI を終了して手順全体をやり直す必要があります。
- macOS では、dmg ファイルは削除されません。
- テンポラル エージェント インストーラは、起動後、エンドポイントでの実行中にブラウザの背後に隠れてしまうことがあります。テンポラル エージェント アプリケーションでのヘルス情報の収集を続行するには、エンドユーザは、ブラウザを最小化する必要があり

ます。この問題は、主に Windows 10 ユーザで発生します。理由は、これらのクライアントでは、高いセキュリティ条件で実行されるサードパーティ アプリケーションを許容するため、UAC モードが「高」に設定されていることです。

- エンドポイントでステルス モードが有効になっている場合は、テンポラル エージェントを使用できません。
- 次の状態は、シスコ テンポラル エージェントではサポートされていません。
  - サービス状態（macOS）：システム デーモンのチェック
  - サービス状態（macOS）：デーモンまたはユーザ エージェントのチェック
  - PM：Up to Date チェック
  - PM：有効化チェック
  - DE：暗号化の場所に基づくチェック

オプション モードのポスチャ ポリシー拡張機能

必須の要件チェックの成否に関係なく、オプションモードで失敗した要件チェックの修復を実行できます。修復に関するメッセージは、AnyConnect ISE ポスチャ UI に表示され、失敗の内容と必要な修復アクションを確認することが可能です。

- オプション モードの手動修復：[システムスキャンのサマリー（System Scan Summary）] 画面には、条件が満たされない場合に修復が必要な可能性がある、オプションモードのステータスが表示されます。[開始（Start）] を手動でクリックして修復するか、[スキップ（Skip）] をクリックします。これらはオプションの要件にすぎないため、修復が失敗しても、エンドポイントはコンプライアンス対応です。[システム サマリー（System Summary）] に、スキップされたのか、失敗したのか、成功したのかが表示されます。
- オプション モードの自動修復：オプションのアップデートの適用時、[システム スキャン（System Scan）] タイルの表示内容を監視できます。修復は自動的に実行されるため、修復を開始するか確認されません。いずれかの自動修復が失敗すると、修復を試行できなかったというメッセージが表示されます。さらに、必要に応じて、修復アクションをスキップできます。

ハードウェア インベントリの可視性

ISE UI の [コンテキストの可視性（Context Visibility）] の下に、[エンドポイント（Endpoints）] > [ハードウェア（Hardware）] タブが追加されました。これは、エンドポイント ハードウェアの情報を短時間で収集、分析、および報告するのに役立ちます。メモリ容量が小さいエンドポイントの検出や、エンドポイントのBIOSモデル/バージョンの検出など、情報を収集することができます。検出結果に基づいて、メモリ容量を増やしたり、BIOS のバージョンをアップグレードしたり、資産の購入を計画する前に要件を評価したりすることができます。[メーカー使用状況（Manufacturers Utilization）] ダッシュレットには、Windows または macOS のエンド

ポイントのハードウェア インベントリの詳細が表示されます。[エンドポイント使用状況（Endpoint Utilizations）] ダッシュレットには、エンドポイントの CPU、メモリ、およびディスクの使用状況が表示されます。詳細については、『Cisco Identity Services Engine Administrator Guide, Release 2.3』の「The Hardware Tab」を参照してください。

ステルス モード

管理者は、AnyConnect UI タイルをエンド ユーザ クライアントに対して非表示にしている間に、ISE ポスチャを設定できます。ポップアップは表示されないので、ユーザによる設定を必要とするどのシナリオでも、デフォルトのアクションが実行されます。この機能は、Windows および Mac オペレーティング システムで使用できます。

『Cisco Identity Services Engine Administrator Guide』の「*Configure Posture Policies*」の項を参照してください。ここでは、クライアントレス状態を無効または有効にしてステルス モードを設定します。

ISE UI では、エンド ユーザにエラー通知が表示されるようにステルス モードで通知を有効にするよう設定できます。

ISE ポスチャ プロファイル エディタ（245 ページ）でプロファイルをマッピングし、AnyConnect 設定を ISE の [クライアント プロビジョニング（Client Provisioning）] ページにマッピングすると、AnyConnect は、ポスチャ プロファイルを読み込んで目的のモードに設定し、最初のポスチャ要求中に選択されたモードに関する情報を ISE に送信できます。モードと、ID グループ、OS、コンプライアンス モジュールなどのその他の要因に基づいて、Cisco ISE は適切なポリシーをマッチングします。

『Cisco Identity Services Engine Administrator Guide』でステルス モードの展開とその影響について参照してください。

ISE ポスチャでは、ステルス モードで次の機能を設定することはできません。

- すべての手動修復
- リンク修復
- ファイル修復
- WSUS 表示 UI 修復
- アクティブ化 GUI 修復
- AUP ポリシー

ポスチャ ポリシーの適用

エンドポイントにインストールされているソフトウェアの全体的な可視性を改善するために、シスコは次のポスチャ拡張機能を提供しました。

- エンドポイントのファイアウォール製品の状態をチェックして、その製品が実行されているかどうか確認できます。必要に応じて、ファイアウォールを有効にし、最初のポスチャ

中や定期的な再評価（PRA）中にポリシーを適用できます。設定するには、『Cisco Identity Services Engine Configuration Guide』の「*Firewall Condition Settings*」の項を参照してください。

- 同様に、エンドポイントにインストールされているアプリケーションのクエリを実行できます。不要なアプリケーションが実行中またはインストールされている場合は、アプリケーションを停止するか、不要なアプリケーションをアンインストールできます。設定するには、ISE UI で、『Cisco Identity Services Engine Configuration Guide』の「*Application Remediation*」の項を参照してください。

UDID 統合

AnyConnect は、デバイスにインストールされていると、AnyConnect のすべてのモジュール間で共有される独自の一意の ID（UDID）を持ちます。この UDID は、エンドポイントの ID であり、エンドポイント属性として保存されるため、MAC アドレスではなく特定のエンドポイントでのポスチャ制御が保証されます。その後は、UDID に基づいてエンドポイントをクエリすることができます。UDID は定数で、エンドポイントの状況（接続、アップグレード、アンインストールなど）に関係なく変化しません。ISE UI の [コンテキスト表示（Context Visibility）] ページ（**[コンテキスト表示（Context Visibility）] > [エンドポイント（Endpoints）] > [コンプライアンス（Compliance）]**）は、複数の NIC を持つエンドポイントについて、複数のエントリではなく 1 つのエントリを表示できます。

アプリケーション監視

ポスチャ クライアントは、動的な変化を監視し、ポリシー サーバに報告できるように、さまざまなエンドポイント属性を継続的に監視できます。ポスチャ ポリシーの設定に応じて、インストールされるアプリケーションや、アプリケーションが実行するアンチスパイウェア、アンチウイルス、アンチマルウェア、ファイアウォールなどのさまざまな属性を監視できます。アプリケーションの条件設定の詳細については、『Cisco Identity Services Engine Administrator Guide』の「*Continuous Endpoint Attribute Monitoring*」の項を参照してください。

USB ストレージ デバイス検出

USB 大容量ストレージ デバイスを Windows エンド ポイントに接続すると、ポスチャ クライアントはそのデバイスを検出し、ポスチャ ポリシー ブロックに応じて、デバイスをブロックしたり許可したりすることができます。エージェントは USB 検出を使用して、同じ ISE 制御ネットワークにある限り、継続的にエンドポイントをモニタします。この期間内に、条件に一致する USB デバイスを接続した場合、指定した修復アクションが実行されます。インシデントは、ポリシー サーバにも報告されます。

USB ストレージ検出は、OPSWAT v4 コンプライアンス モジュールに依存しています。[ワーク センター（Work Centers）] > [ポスチャ（Posture）] > [ポリシー要素（Policy Elements）] > [USB] で、ISE UI の定期再評価ポリシー（PRA）の USB チェックを設定する必要があります。

（注） チェックと修復は順番に実行されるため、その他のチェックの PRA 猶予時間を最小限の値に設定することによって、USB チェックの処理での遅延を防止できます。猶予時間は、[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [設定（Settings）] > [再評価設定（Reassessment Config）] の ISE UI で設定されます。

ISE UI で USB ストレージの検出を設定する手順については、「USB Mass Storage Check Workflow」を参照してください。

自動コンプライアンス

ポスチャ リースにより、ISE サーバは、ポスチャを完全にスキップし、簡単にシステムを準拠状態にすることができます。この機能により、ユーザは、自分のシステムが最近ポスチャされている場合に、ネットワーク間の切り替えによる遅延を感じることがありません。ISE ポスチャエージェントは、単に、ISE サーバが検出されたすぐ後に、システムが準拠しているかどうかを示すステータス メッセージを UI に送信します。ISE の UI（[設定（Settings）] > [ポスチャ（Posture）] > [一般設定（General Settings）]）で、最初のコンプライアンス チェックの後にエンドポイントがポスチャ準拠と見なされる時間を指定できます。ユーザがある通信インターフェイスから別の通信インターフェイスに切り替えた場合でも、コンプライアンス ステータスは維持されることが予期されています。

（注） ポスチャ リースでは、ISE でセッションが有効な場合に、エンドポイントがポスチャ不明状態から準拠状態に移行することが予期されます。

VLAN のモニタリングと遷移

サイトによっては、異なる VLAN またはサブネットを使用して、企業グループおよびアクセス レベル用にネットワークを分割しています。ISE からの認可変更（CoA）では、VLAN の変更を指定します。変更は、セッション終了など管理者のアクションによって発生することもあります。有線接続中の VLAN 変更をサポートするには、ISE ポスチャ プロファイルに次の設定を行います。

- [VLAN 検出間隔（VLAN Detection Interval）]：エージェントが VLAN の遷移を検出する頻度およびモニタリングを無効にするかどうかを決定します。VLAN モニタリングは、この間隔が 0 以外の値に設定されている場合に有効になります。Mac OS X の場合、この値は 5 以上に設定します。

  VLAN モニタリングは Windows と Mac OS X の両方に実装されていますが、Mac では予期しない VLAN 変更を検出するためにのみ必要です。VPN が接続される場合、または acise（メインの AnyConnect ISE プロセス）が実行されていない場合は、自動的に無効になります。有効な値の範囲は 0 ～ 900 秒です。

- [エージェント IP 更新の有効化（Enable Agent IP Refresh）]：オフにすると、ISE はエージェントに [ネットワーク遷移遅延（Network Transition Delay）] 値を送信します。オンにすると、ISE はエージェントに DHCP リリースおよび更新の値を送信し、エージェントは IP 更新を行って最新の IP アドレスを取得します。
- [DHCP リリース遅延（DHCP release delay）] と [DHCP 更新遅延（DHCP renew delay）]：IP 更新および [エージェント IP 更新の有効化（Enable Agent IP Refresh）] 設定との相関で使用されます。[エージェント IP 更新の有効化（Enable Agent IP Refresh）] チェックボックスをオンにし、この値が 0 でない場合、エージェントはリリース遅延秒数を待機し、IP アドレスを更新し、更新遅延秒数を待機します。VPN が接続されている場合、IP 更新は自動的に無効になります。4 連続でプローブがドロップされると、DHCP 更新がトリガーされます。
- [ネットワーク遷移遅延（Network Transition Delay）]：（[エージェント IP 更新の有効化（Enable Agent IP Refresh）] チェックボックスで）VLAN モニタリングがエージェントによって無効または有効にされた場合に使用されます。この遅延により、VLAN が使用されていない場合にはバッファが追加され、サーバからの正確なステータスを待機する十分な時間がエージェントに与えられます。ISE はエージェントにこの値を送信します。また、ISE UI のグローバル設定に [ネットワーク遷移遅延（Network Transition Delay）] 値を設定した場合、ISE ポスチャ プロファイル エディタの値でその値が上書きされます。

（注） ASA は VLAN 変更をサポートしないため、クライアントが ASA を介して ISE に接続されているときには、これらの設定は適用されません。

トラブルシューティング

ポスチャの完了後にエンドポイントデバイスがネットワークにアクセスできない場合は、次の点を確認してください。

- VLAN 変更は ISE UI で設定されていますか。
  - 設定されている場合、DHCP リリース遅延および更新遅延がプロファイルに設定されていますか。
  - どちらの設定も 0 の場合、[ネットワーク遷移遅延（Network Transition Delay）] がプロファイルに設定されていますか。

AnyConnect ISE フローを中断する操作

さまざまな理由から、AnyConnect ISE ポスチャ フローは最初のポスチャ再アセスメントまたはパッシブ再アセスメント中に中断されることがあります。

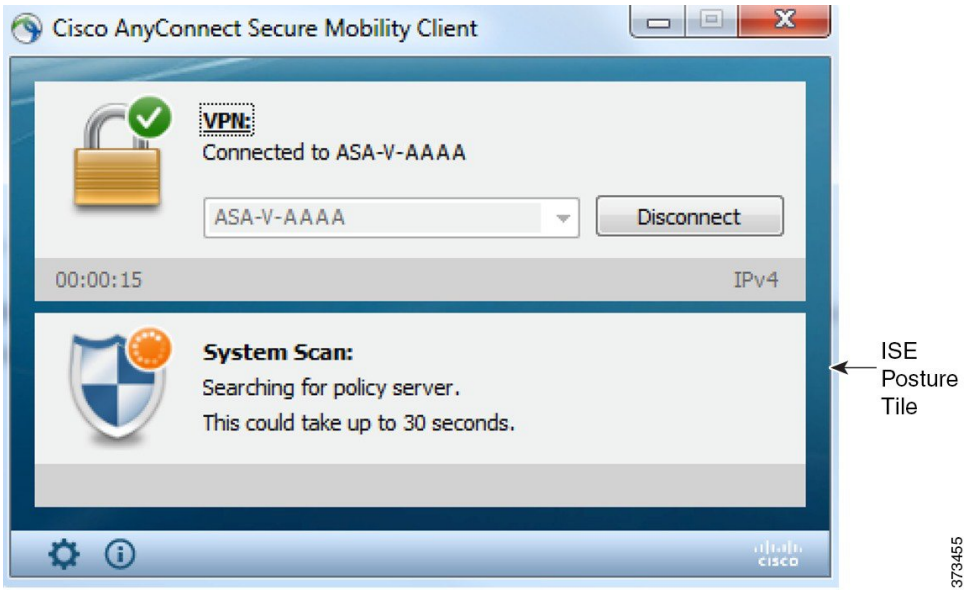
- ユーザが AnyConnect ISE をキャンセルする：ポスチャのチェックと修復の期間に、ユーザは AnyConnect ISE をキャンセルできます。UI にはキャンセルが進行中であることがただちに通知されますが、これはエンドポイントを問題のある状態にすることを回避すると

きにだけ発生します。サードパーティ ソフトウェアを使用している場合、キャンセル操作によってはリブートが必要な場合があります。キャンセル後、AnyConnect UI のポスチャ タイル部分には、準拠状態が示されます。

- 修復タイマーが期限切れになる：ポスチャ要件を満たすための管理者制御時間が終了しました。アセスメント レポートがヘッドエンドに送信されます。パッシブ再アセスメント時には、ユーザはネットワーク アクセスを保持し、ポスチャ アセスメントでは、必須要件すべてが満たされた場合にネットワーク アクセスが許可されます。
- ポスチャ チェック中のエラー：ポスチャ チェック フェーズでエラーが発生し、AnyConnect が続行可能な場合、ユーザに通知されますが、可能な場合はポスチャのチェックが続行されます。必須のポスチャ チェック中にエラーが発生した場合、チェックは失敗とマークされます。ネットワーク アクセスは、すべての必須要件が満たされている場合に許可されます。そうでない場合、ユーザはポスチャ プロセスをリスタートできます。
- 修復中のエラー：修復フェーズでエラーが発生し、AnyConnect ISE ポスチャが続行可能な場合は、ユーザに通知されます。失敗した修復ステップが必須のポスチャ要件と関連付けられている場合、AnyConnect ISE ポスチャは修復プロセスを停止します。失敗した修正ステップがオプションのポスチャの要件に関連付けられている場合は、次のステップに進んで ISE ポスチャ操作を終了しようとします。ネットワーク アクセスは、すべての必須要件が満たされている場合に許可されます。そうでない場合、ユーザはポスチャ プロセスをリスタートできます。
- デフォルト ゲートウェイの変更：デフォルト ゲートウェイに対する変更により、ユーザが信頼ネットワークへのアクセスを失う場合があります。これにより、ISE ポスチャは ISE の再検出を試みます。AnyConnect UI の ISE ポスチャ タイル部分では、再検出モードに入ると ISE ポスチャのステータスが表示されます。
- AnyConnect と ISE 間の接続の喪失：エンドポイントが準拠状態と見なされてネットワーク アクセスが許可された後に、さまざまなネットワーク シナリオが発生する可能性があります。エンドポイントがネットワーク接続を完全に失う場合があります。ISE がダウンする場合があります。ISE ポスチャが失敗する場合があります（セッション タイムアウト、手動リスタートなどによる）。ASA の背後の ISE が VPN トンネルを喪失する場合があります。

ISE ポスチャのステータス

AnyConnect ISE ポスチャが機能し、想定どおりにネットワーク アクセスをブロックしている場合に、AnyConnect UI の [ISE ポスチャ（ISE Posture）] タイルに [システム スキャン：ポリシー サーバを検索しています（System Scan: Searching for policy server）] と表示されます。Windows タスク マネージャまたは Mac OS X システム ログには、プロセスが実行中であると示される場合があります。サービスが実行されていない場合は、AnyConnect UI の [ISE ポスチャ（ISE Posture）] タイルに [システム スキャン：サービスは使用できません（System Scan: Service is unavailable）] と表示されます。



ネットワークを変更すると、検出フェーズが開始されます。AnyConnect ISE ポスチャの場合、プライマリ インターフェイスのデフォルト ルートが変更された場合、エージェントが検出プロセスに戻ります。たとえば、WiFi およびプライマリ LAN が接続された場合、エージェントは検出をリスタートします。同様に、WiFi およびプライマリ LAN が接続されたものの、その後、WiFi の接続が解除された場合、エージェントは検出をリスタートしません。

また、「システム スキャン」後、AnyConnect UI の [ISE ポスチャ（ISE Posture）] タイルに次のステータス メッセージが表示される場合があります。

- [限定的または接続なし（Limited or no connectivity）]：接続がないため検出は発生していません。AnyConnect ISE ポスチャ エージェントは、ネットワーク上の不正なエンドポイントで検出を実行している可能性があります。
- [システム スキャンは現在の WiFi では不要（System scan not required on current WiFi）]：セキュアでない WiFi が検出されたため検出は発生していません。AnyConnect ISE ポスチャ エージェントは、LAN、ワイヤレス（802.1X 認証が使用されている場合）、および VPN でのみ検出を開始します。WiFi がセキュアでないか、またはエージェント プロファイルで OperateOnNonDot1XWireless を 1 に設定してこの機能を無効にしています。
- [不正なポリシー サーバ（Unauthorized policy server）]：ネットワーク アクセスが制限されているか存在しないため、ホストが ISE ネットワークのサーバ名ルールに一致していません。
- [AnyConnect ダウンローダが更新を実行しています…（The AnyConnect Downloader is performing update...）]：ダウンローダが呼び出され、パッケージ バージョンを比較し、AnyConnect 設定をダウンロードし、必要なアップグレードを行います。
- [システムをスキャンしています...（Scanning System...）]：アンチウイルス/アンチスパイウェアのセキュリティ製品のスキャンが開始されました。このプロセス中にネットワークが変更された場合、エージェントはログ ファイルの生成プロセスをリサイクルし、ステータスは [検出されたポリシー サーバなし（No policy server detected）] に戻ります。

- [AnyConnect スキャンのバイパス（Bypassing AnyConnect scan）]：ネットワークは、Cisco NAC Agent を使用するように設定されています。
- [ユーザによってキャンセルされた信頼できないポリシー サーバ（Untrusted Policy Server Cancelled by the user）]：AnyConnect UI の [システム スキャン プリファレンス（System Scan Preferences）] タブで信頼できないサーバへの接続のブロックを解除すると、ポップアップ ウィンドウに AnyConnect ダウンローダのセキュリティ警告が表示されます。この警告ページで [接続のキャンセル（Cancel Connection）] をクリックすると、[ISE ポスチャ（ISE Posture）] タイルがこのステータスに変わります。
- [ネットワークの利用規定（Network Acceptable Use Policy）]：ネットワークへのアクセスには、アクセプタブル ユース ポリシーを確認し、受け入れる必要があります。ポリシーを拒否すると、ネットワーク アクセスが制限される可能性があります。
- [ネットワーク設定の更新（Updating Network Settings）]：ISE UI の [設定（Settings）] > [ポスチャ（Posture）] > [全般設定（General Settings）] では、ネットワーク遷移間で発生させる遅延の秒数を指定できます。
- [コンプライアンス非対応。更新時間の期限が切れました。（Not Compliant. Update time expired.）]：修復のために設定された時間の期限が切れました。
- [コンプライアンス対応。ネットワーク アクセスが許可されています。（Compliant. Network access allowed.）]：修復が完了しました。[システム スキャン（System Scan）] > [スキャン概要（Scan Summary）] にも、ステータスが完了と示されます。
- [検出されたポリシー サーバなし（No policy server detected）]：ISE ネットワークが見つかりません。30 秒後、エージェントによるプローブは低下します。デフォルトのネットワーク アクセスが有効になります。

ポスチャとマルチホーミング

AnyConnect ISE ポスチャ モジュールは、マルチホーミングをサポートしていません。これは、そのようなシナリオの動作が定義されていないためです。たとえば、メディアが有線からワイヤレスに変更された後で有線に戻ると、エンドポイントが実際には有線接続でリダイレクトされている場合でも、ユーザには ISE ポスチャ モジュールに準拠したポスチャ ステータスが表示されることがあります。

エンドポイントの同時ユーザ

AnyConnect ISE は、複数のユーザが同時にエンドポイントにログインしてネットワーク接続を共有した場合、個別のポスチャ評価をサポートしません。最初に AnyConnect ISE を実行したユーザが正常にポスチャされ、エンドポイントに信頼ネットワーク アクセスが許可されると、エンドポイントの他のすべてのユーザがネットワーク アクセスを継承します。これを防ぐため、管理者はエンドポイントに同時ユーザを許可する機能を無効にできます。

ポスチャ モジュールのロギング

ISE ポスチャの場合、イベントはネイティブ オペレーティング システムのイベント ログ（Windows イベント ログ ビューアまたは Mac OS X システム ログ）に記録されます。

VPN ポスチャ（HostScan）の場合、エラーおよび警告は syslog（Windows 以外の場合）とイベント ビューア（Windows の場合）に送信されます。使用可能なすべてのメッセージがログ ファイルに記録されます。

VPN ポスチャ（HostScan）モジュール コンポーネントは、オペレーティング システム、特権レベル、および起動メカニズム（Web 起動または AnyConnect）に基づいて、次の 3 つのログに出力します。

- cstub.log：AnyConnect Web 起動が使用された場合にログを取り込みます。
- libcsd.log：VPN ポスチャ API を使用する AnyConnect スレッドによって作成されます。ログ レベル設定に応じて、このログにデバッグのエントリが入力されます。
- cscan.log：スキャニング実行可能ファイル（cscan.exe）によって作成される、VPN ポスチャのメインのログです。ログ レベル設定に応じて、このログにデバッグのエントリが入力されます。

ポスチャ モジュールのログ ファイルと場所

ISE ポスチャの場合、イベントはインストールされた AnyConnect バージョンの独自のサブフォルダに含まれているため、AnyConnect イベントの他の部分から容易に分離できます。各ビューアでは、キーワードの検索およびフィルタリングが可能です。Web Agent イベントは、標準のアプリケーション ログに書き込まれます。

トラブルシューティングのために、ISE ポスチャ要件ポリシーとアセスメント レポートがイベント ログではなく、エンドポイントの別の難解化されたファイルに記録されます。一部のログ ファイル サイズ（aciseposture など）は、管理者がプロファイルに設定できますが、UI ログ サイズは事前に定義されています。

プロセスが異常終了したときは、他の AnyConnect モジュールと同じように、常にミニ ダンプ ファイルが生成されます。

VPN ポスチャ（HostScan）の場合、ファイルはユーザのホーム フォルダの次のディレクトリにあります。

- （Windows 以外）：.cisco/hostscan/log
- （Windows）：C:\Users\<user_name>\AppData\Local\Cisco HostScan\log\cscan.log

ISE ポスチャ プロファイル エディタ

管理者は、ポスチャ プロファイルを作成し、ISE にアップロードするために、このスタンドアロン エディタを使用することを選択できます。それ以外の場合、組み込みのポスチャ プロファイル エディタが ISE UI の [ポリシー要素（Policy Elements）] に設定されます。AnyConnect コンフィギュレーション エディタが ISE で起動すると、AnyConnect ソフトウェアおよび関連するモジュール、プロファイル、OPSWAT、およびカスタマイズを備えた AnyConnect 設定が作成されます。ASA の ISE ポスチャ用のスタンドアロン プロファイル エディタには、次のパラメータが含まれています。

- **エージェントの動作**
  - [署名チェックの有効化（Enable signature check）]：オンにすると、エージェントによって実行される前に実行可能ファイルの署名チェックが有効になります。
  - [ログ ファイル サイズ（Log file size）]：エージェント ログ ファイルの最大サイズ。有効な値は 5 ～ 200 MB です。
  - [修復タイマー（Remediation timer）]：コンプライアンス非対応とタグ付けされるまでにユーザが修復に割くことができる時間。有効な値は 1 ～ 300 分です。
  - [エージェント ログ トレースの有効化（Enable agent log trace）]：エージェントでのデバッグ ログを有効にします。
  - [非 802.1X ワイヤレス ネットワークでの動作（Operate on non-802.1X wireless networks）]：オンにすると、エージェントは非 802.1X ワイヤレス ネットワークで動作できます。
  - [ステルス モードを有効にする（Enable Stealth Mode）]：ユーザによる設定を行わなくてもポスチャをサービスとして実行できるステルス モードを有効にするかどうかを選択します。
  - [通知によるステルスを有効にする（Enable Stealth With Notification）]：ステルス モードの通知が有効に設定されている場合、エンド ユーザは、AnyConnect ステルス モードが非準拠の状態にある、ネットワーク アクセスが制限されている、到達不能なサーバなどがあるなどの場合でも通知メッセージを受け取ります。
  - [再スキャンボタンを有効にする（Enable Rescan Button）]：障害発生後、手動修復後、ポスチャの動作不能時（など）に、ポスチャ（またはディスカバリ）を再起動する場合は、このボタンを有効にして、[システムスキャン（System Scan）] タイルに **[再度スキャン（Scan Again）]** の選択が表示されるようにします。このオプションは、ISE ポスチャ プロファイルで表示または非表示にできます。**[再度スキャン（Scan Again）]** をクリックすると、ディスカバリが起動し、ポスチャ フロー全体が開始されます。

（注） [再度スキャン（Scan Again）] がタイルに表示されるのは、ポスチャ プロファイルで EnableRescan タグを 1 に設定している場合だけです。0 に設定すると、[再度スキャン（Scan Again）] ボタンが表示されるのは、それが（このオプションよりも先に）表示されていた場合だけです。

（注） ISE 側でプロファイルの変更が発生すると、次回ディスカバリが起動されるときに、その変更が AnyConnect タイルに反映されます。

- [UACポップアップを無効にする（Disable UAC Popup）]：ポリシー検証中に Windows ユーザ アカウント制御（UAC）ポップアップが表示されるかどうかを決定します。デフォルト値（オフ）では、エンドユーザは引き続き接続時に管理者権限を求められます。有効にすると、ポリシーの検証中に Windows ユーザ アカウント制御（UAC）プロンプトが表示されません。UACプロンプトをオフにすることによって、AnyConnect ポスチャは「管理者として実行（Run as administrator）」ではなく、特権昇格のシステム プロセスを使用します。UAC プロンプトを無効にする前に、ユーザにローカル管理者権限があるデバイスでポスチャ ポリシーを検証します。
- [バックオフ タイマーの制限（Backoff Timer Limit）]：AnyConnect が ISE 検出のプローブを送信する最長時間を入力します。プローブによりトラフィックが増えるため、ネットワークの負荷にならない値を選択してください。
- [定期プローブ間隔（Periodic Probe Interval）]：バックオフ タイマーの制限を超えた後の検出プローブの間隔を指定します。AnyConnect は、有効な ISE サーバが見つかるまで、指定された間隔で定期的なプローブを送信します。デフォルトでは 30 分で、プローブは、初回プローブの完了後、30 分間隔で継続的に送信されます。値を 0 に設定すると、定期的なプローブがディセーブルになります。

• IP アドレスの変更

最適なユーザ エクスペリエンスのため、次の値を推奨値に設定してください。

- [VLAN 検出間隔（VLAN detection interval）]：クライアント IP アドレスを更新する前にエージェントが VLAN 変更の検出を試みる間隔。有効な範囲は 0 ～ 900 秒で、推奨値は 5 秒です。
- [ping または ARP（Ping or ARP）]：IP アドレスの変更を検出する方法。推奨設定は ARP です。
- [ping の最大タイムアウト（Maximum timeout for ping）]：1 ～ 10 秒の ping タイムアウト。

- [エージェント IP 更新の有効化（Enable agent IP refresh）]：VLAN 変更の検出を有効にする場合にオンにします。
- [DHCP 更新遅延（DHCP renew delay）]：IP 更新後にエージェントが待機する秒数。[エージェント IP 更新の有効化（Enable Agent IP Refresh）] を有効にしたときに、この値を設定します。この値が 0 ではない場合、エージェントはこの予期される遷移中に IP を更新します。更新中に VPN が検出された場合、更新は無効です。有効な値は 0 ～ 60 秒で、推奨値は 5 秒です。
- [DHCP リリース遅延（DHCP release delay）]：エージェントによる IP 更新を遅延させる秒数。[エージェント IP 更新の有効化（Enable Agent IP Refresh）] を有効にしたときに、この値を設定します。この値が 0 ではない場合、エージェントはこの予期される遷移中に IP を更新します。更新中に VPN が検出された場合、更新は無効です。有効な値は 0 ～ 60 秒で、推奨値は 5 秒です。
- [ネットワーク遷移遅延（Network transition delay）]：計画された IP 変更を待機できるようにエージェントがネットワーク モニタリングを一時停止する期間（秒単位）。推奨値は 5 秒です。

• ポスチャ プロトコル

- [ホストの検索（Discovery host）]：エージェントが接続できるサーバ。スタンドアロン プロファイル エディタでは、1 つのホストのみを入力します。
- [サーバ名ルール（Server name rules）]：エージェントが接続できるサーバを定義する、ワイルドカード対応のカンマで区切られた名前のリスト（.cisco.com など）。
- [Call Home リスト（Call Home List）]：ロード バランシング、ルックアップのモニタリングとトラブルシューティングに使用する FQDN、またはそのノードでデフォルトのポリシー サービス ノード（PSN）にマップする DNS の FQDN（複数シナリオの場合）を入力します。これを設定すると、ルックアップのモニタリングとトラブルシューティングついての最初のプローブは Call Home に送信されます。リダイレクト ネットワークから非リダイレクト ネットワークに移行するときにこれを設定する必要があります。
- [PRA 再送信時間（PRA retransmission time）]：パッシブ再評価の通信障害が発生した場合に、このエージェントが再試行する間隔を指定します。有効な値の範囲は 60 ～ 3600 秒です。

[詳細（Advanced）] パネル

AnyConnect Secure Mobility Client UI の [詳細（Advanced）] パネルは、コンポーネントの統計情報、ユーザプリファレンス、およびコンポーネント固有のその他の情報を表示するための各コンポーネントの領域です。AnyConnect システム トレイで、[すべてのコンポーネントの詳細ウィンドウ（Advanced Window for all components）] アイコンをクリックすると、新しい [システム スキャン（System Scan）] セクションに次のタブが含まれます。

（注） macOS では、これらの統計情報、ユーザ設定、メッセージ履歴などは、[統計情報（Statistics）] ウィンドウの下に表示されます。プリファレンスは、[プリファレンス（Preferences）] ウィンドウに表示され、Windows のようなタブの向きではありません。

- [プリファレンス（Preferences）]：信頼できないサーバへの接続をブロックできます。ダウンローダのプロセス中に、証明書が信頼できず検証されていない ISE サーバに対して、「信頼できないサーバをブロックしました（Untrusted Server Blocked）」というメッセージを受信します。ブロッキングを無効にすると、AnyConnect は悪意がある可能性があるネットワーク デバイスへの接続をブロックしなくなります。
- [統計情報（Statistics）]：現在の ISE ポスチャ ステータス（準拠または未準拠）、OPSWAT のバージョン情報、アクセプタブル ユース ポリシーのステータス、ポスチャの最新の実行タイム スタンプ、不足要件、およびトラブルシューティングの目的で表示するのに十分重要であると考えられるその他の統計情報を提供します。
- [セキュリティ製品（Security Products）]：システムにインストールされているマルウェア対策製品のリストにアクセスします。
- [スキャンの概要（Scan Summary）]：管理者がユーザに対して表示するように設定したポスチャ項目をユーザが確認できるようにします。たとえば、設定されている場合、ユーザはシステム上にポスチャされたすべての項目を表示したり、ポスチャ チェックに失敗して修復が必要な項目のみを表示したりすることができます。
- [メッセージ履歴（Message History）]：コンポーネントについて、システム トレイに送信されたすべてのステータス メッセージの履歴を表示します。この履歴は、トラブルシューティングに役立ちます。

VPN ポスチャ（HostScan）モジュールの提供内容

HostScan

HostScan は、ユーザが ASA に接続した後、かつログインする前に、リモート デバイス上にインストールされるパッケージです。HostScan は、基本モジュール、Endpoint Assessment モジュール、および Advanced Endpoint Assessment モジュールで構成されています。

（注） AnyConnect リリース 3.x では、このパッケージは hostscan_version.pkg ファイルにバンドルされ、HostScan が機能するためには ASA の HostScan イメージ下で更新されて有効化される必要がありました。現在は、独立したインストールです。

基本的機能

HostScan は自動的に Cisco クライアントレス SSL VPN または AnyConnect VPN クライアント セッションを確立しているリモート デバイスのオペレーティング システムとサービス パックを識別します。

特定のプロセス、ファイル、およびレジストリ キーについて、エンドポイントを検査するように HostScan を設定することもできます。HostScan は、トンネルが完全に確立される前にこれらのすべての検査を実行し、この情報を ASA に送信して、会社所有、個人用、および公共のコンピュータを識別します。この情報は、評価にも使用できます。

（注） ログイン前の評価および証明書情報の返送は実行できません。HostScan は認証方式ではありません。HotScan は、接続しようとしているデバイスの内容を検証するチェックを実行するだけです。

また、HostScan は、設定した DAP エンドポイント条件と照合して評価するために、次の追加の値を自動的に返します。

- Microsoft Windows、Mac OS、および Linux オペレーティング システム
- Microsoft サポート技術情報（KB）番号
- デバイス エンドポイント属性タイプ（ホスト名、MAC アドレス、BIOS シリアル番号、ポート番号（レガシー属性）、TCP/UDP ポート番号、プライバシー保護、およびエンドポイント アセスメント（OPSWAT）のバージョンなど）。

（注） HostScan は Windows クライアント システム上の Microsoft のソフトウェア アップデートに関するサービス リリース（GDR）の情報を収集します。サービス リリースには複数のホット フィックスが含まれます。サービス リリース エンドポイント属性は、ホット フィックスではなく、DAP ルールに使用されます。

エンドポイント アセスメント

エンドポイント アセスメントは、HostScan の拡張機能であり、多くの種類のアンチウイルスとアンチスパイウェアのアプリケーション、関連する定義の更新、およびファイアウォールについて、リモート コンピュータを検査します。ASA によって特定のダイナミック アクセス ポリシー（DAP）がセッションに割り当てられる前に、この機能を使用して要件を満たすようにエンドポイント条件を組み合わせることができます。

詳細については、適切なバージョンの『Cisco ASA Series VPN Configuration Guide』の「*Dynamic Access Policies*」の項を参照してください。

Advanced Endpoint Assessment：マルウェア対策およびファイアウォールの修復

Windows、macOS、および Linux のデスクトップでは、マルウェア対策およびパーソナル ファイアウォール保護のソフトウェアで別のアプリケーションが修復を開始することを許可している場合に、Advanced Endpoint Assessment は、それらのソフトウェアに関するさまざまな修復を開始しようとします。

マルウェア対策：Advanced Endpoint Assessment は、マルウェア対策ソフトウェアの以下のコンポーネントを修復しようとします。

- ファイル システム保護の強制：マルウェア対策ソフトウェアが無効の場合に、Advanced Endpoint Assessment はこのコンポーネントを有効にします。
- ウイルス定義更新の強制：Advanced Endpoint Assessment の設定で定義された日数の間、マルウェア対策定義が更新されなかった場合に、Advanced Endpoint Assessment はウイルス定義の更新を開始しようとします。

パーソナル ファイアウォール：Advanced Endpoint Assessment モジュールでは、ファイアウォールを有効または無効にすることができます。

HostScan バージョン 4.4 は、パーソナル ファイアウォールを使用するアプリケーションとポートのブロックまたは許可をサポートしていません。

（注） すべてのパーソナル ファイアウォールがこの有効化の強制/無効化の強制機能をサポートしているわけではありません。

HostScan 用のアンチマルウェア アプリケーションの設定

VPN ポスチャ（HostScan）モジュールをインストールする前に、アンチマルウェア ソフトウェアを「ホワイトリスト」に設定するか、または、次の各アプリケーションについてセキュリティ例外を作成します。アンチマルウェア アプリケーションは、これらのアプリケーションの動作を悪意があるものと誤って認識する場合があります。

- cscan.exe
- ciscod.exe
- cstub.exe

ダイナミック アクセス ポリシーとの統合

ASA では、HostScan の機能がダイナミック アクセス ポリシー（DAP）に統合されます。設定に応じて、ASA では、DAP 割り当ての条件として、オプションの AAA 属性値と組み合わせたエンドポイント属性値が 1 つ以上使用されます。DAP のエンドポイント属性でサポートされる HostScan の機能には、OS 検出、ポリシー、基本結果、およびエンドポイント アセスメントがあります。

セッションに DAP を割り当てるために必要な条件を構成する属性を、単独で、または組み合わせて指定できます。DAP により、エンドポイント AAA 属性値に適したレベルでネットワーク アクセスが提供されます。設定したエンドポイント条件がすべて満たされたときに、ASA によって DAP が適用されます。

『Cisco ASA Series VPN Configuration Guide』の「*Configure Dynamic Access Policies*」の項を参照してください。

DAP の BIOS シリアル番号

VPN ポスチャ（HostScan）は、ホストの BIOS シリアル番号を取得できます。ダイナミック アクセス ポリシー（DAP）を使用し、その BIOS シリアル番号に基づいて ASA への VPN 接続を許可または拒否できます。

DAP エンドポイント属性としての BIOS の指定

手順

ステップ 1 ASDM にログインします。

ステップ 2 **[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）]** または **[クライアントレス SSL VPN アクセス（Clientless SSL VPN Access）] > [ダイナミック アクセス ポリシー（Dynamic Access Policies）]** を選択します。

ステップ 3 [ダイナミック アクセス ポリシーの設定（Configure Dynamic Access Policies）] パネルで、[追加（Add）] または [編集（Edit）] をクリックして、BIOS を DAP エンドポイント属性として設定します。

ステップ 4 エンドポイント ID 表の右にある [追加（Add）] をクリックします。

ステップ 5 [エンドポイント属性タイプ（Endpoint Attribute Type）] フィールドで、[デバイス（Device）] を選択します。

ステップ 6 [BIOS シリアル番号（BIOS Serial Number）] チェックボックスをオンにし、[=]（等しい）または [!=]（等しくない）を選択して、[BIOS シリアル番号（BIOS Serial Number）] フィールドに BIOS 番号を入力します。[OK] をクリックし、[エンドポイント属性（Endpoint Attribute）] ダイアログボックスでの変更を保存します。

ステップ 7 [OK] をクリックして、[ダイナミック アクセス ポリシーの編集（Edit Dynamic Access Policy）] への変更を保存します。

ステップ 8 [適用（Apply）] をクリックして、ダイナミック アクセス ポリシーへの変更を保存します。

ステップ 9 [保存（Save）] をクリックします。

BIOS シリアル番号の取得方法

- Windows：http://support.microsoft.com/kb/558124

- Mac OS X：http://support.apple.com/kb/ht1529
- Linux：このコマンドを使用してください。

```
/usr/bin/hal-get-property --udi /org/freedesktop/Hal/devices/computer --key
system.hardware.serial
```

ASA で有効にされたホスト スキャン イメージの判別

ASDM を開いて [設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ホスト スキャン イメージ（HostScan Image）] を選択します。

HostScan のアップグレード

AnyConnect および HostScan を手動で（msiexec を使用して）アップグレードする場合は、必ず、AnyConnect を最初にアップグレードして、その後に HostScan をアップグレードしてください。

OPSWAT サポート

AnyConnect の VPN（HostScan）ポスチャ モジュールも ISE ポスチャ モジュールも、OPSWAT フレームワークを使用して、エンドポイントを保護します。

クライアントとヘッドエンドの両方を伴うこのフレームワークは、エンドポイント上のサードパーティ アプリケーションを評価するのに役立ちます。クライアントとヘッドエンドで使用されている OPSWAT のバージョンは、一致する必要があります。ポスチャ方式ごとに、サポート表が用意されています。使用される OPSWAT バージョンによって認識されるアプリケーションのリストに、製品およびバージョン情報を記載しています。

ヘッドエンド（ASA または ISE）とエンドポイント（VPN ポスチャまたは ISE ポスチャ）との間にバージョン番号の不一致があるときは、ヘッドエンドのバージョンに合わせて、OPSWAT 準拠モジュールがアップグレードまたはダウングレードされます。これらのアップグレード/ダウングレードは必須であり、ヘッドエンドへの接続が確立されるとすぐにエンドユーザの介入なしで自動的に実行されます。

VPN HostScan ポスチャ OPSWAT サポート

「HostScan サポート表」は、ASA ヘッドエンドで動作する AnyConnect に HostScan ポスチャを提供する HostScan パッケージ バージョンに対応しています。

HostScan は、AnyConnect メジャー リリースおよびメンテナンス リリースと連携するようにバージョン管理されます。ASDM で HostScan パッケージを設定するときに、HostScan バージョンを指定します。[設定（Configuration）] > [リモートアクセスVPN（Remote Access VPN）] > [セキュアデスクトップマネージャ（Secure Desktop Manager）] > [ホストスキャンイメージ（Host Scan Image）] の順に選択してください。

VPN HostScan ポスチャのガイドライン：

- HostScan 4.3.x までの全バージョンが OPSWAT v2 を使用します。HostScan 4.6x 以降は、OPSWAT v4 を使用します。OPSWAT v3 は、HostScan のどのバージョンでもサポートされていません。
- AnyConnect 4.4.x および 4.5.x は、HostScan バージョン 4.3.05017 以降をサポートしています。HostScan には、4.4.x や 4.5.x バージョンはありません。
- AnyConnect 4.6.x は、HostScan 4.3.05050（およびそれ以降の 4.3.x バージョン）と、4.6.x バージョンをサポートしています。
- 基盤となる OPSWAT バージョンの変更に伴い、移行プロセスを完了して HostScan 4.3.x から 4.6.x 以降にアップグレードする必要があります。4.6.x 以降の HostScan イメージをロードして移行を開始するときには、ASDM 7.9.2 以降と HostScan バージョン 4.3.05050（またはそれ以降の 4.3.x バージョン）がヘッドエンドにインストールされている必要があります。

HostScan 4.3.05017 以降で使用される OPSWAT バージョンについては、次の表で詳しく説明します。互換性のある AnyConnect リリース、ASA/ASDM ヘッドエンド要件、および有効なダウングレード/アップグレード操作も記載して、VPN/HostScan ポスチャのために連携する製品の関係を示します。

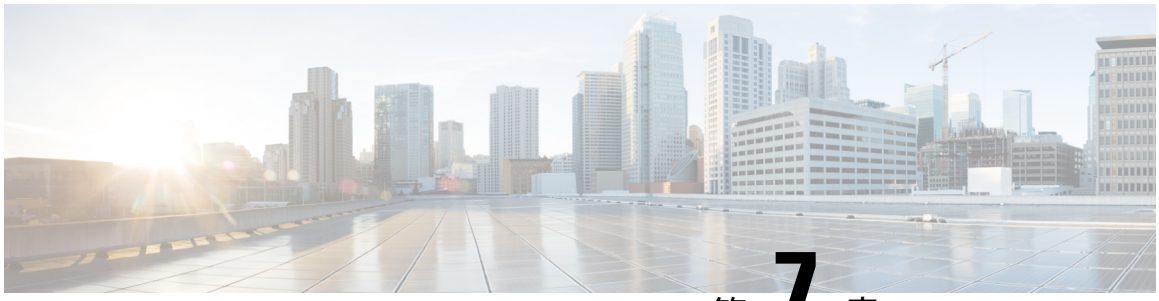
OPSWAT バージョン	サポートされている HostScan バージョン	AnyConnectの互換性のあるバージョン	ASA/ASDM ヘッドエンドの必要なバージョン	ダウングレード/アップグレード操作
v2	4.3.05017 から 4.3.05050 まで	AnyConnect 4.4.x および 4.5x	AnyConnect をサポートするすべてのリリース。	以前の任意の 4.3.x HostScan リリースにダウングレードします。 以降の任意の 4.3.x HostScan リリースにアップグレードします。
	4.3.05050 およびそれ以降のすべての 4.3.x バージョン。	AnyConnect 4.4.x、4.5.x、および 4.6.x	AnyConnect をサポートするすべてのリリース。	以前の任意の 4.3.x HostScan リリースにダウングレードします。 以降の任意の 4.3.x HostScan リリースにアップグレードします。 （注） 任意の 4.6.x HostScan リリースにアップグレードするには、移行プロセスが必要です。 移行プロセスでは、HostScan 4.3.05050（またはそれ以降の 4.3.x バージョン）がヘッドエンドにインストールされている必要があります。
v4	4.6.x	AnyConnect 4.4.x、4.5.x、および 4.6.x	ASDM 7.9.2 以降で AnyConnect をサポートするすべての ASA リリース。	以前の任意の 4.6.x バージョンにダウングレードします。 移行元の 4.3.x HS リリースへのダウングレードに必要なフォールバック プロセス。 以降の任意のリリースにアップグレードします。

ISE ポスチャ OPSWAT サポート

「Cisco AnyConnect エージェント準拠モジュール」は、ISE ポスチャ モジュール用です。

ISE エージェント準拠モジュールのバージョンには、基盤となる OPSWAT バージョンが反映されています。ISE ポスチャでは、OPSWAT バイナリは別個のインストーラにパッケージ化されています。OPSWAT ライブラリをローカル ファイル システムから ISE ヘッドエンドに手動でロードしたり、ISE 更新フィード URL を使用して直接取得するように ISE を設定したりできます。

AnyConnect リリース 4.3 以降を ISE 2.1 以降とともに使用したときは、ISE 準拠モジュールに OPSWAT v3 または v4 のどちらを使用するか選択できます。アンチマルウェアの設定は、[ワーク センター（Work Centers）] > [ポスチャ（Posture）] > [ポスチャ要素（Posture Elements）] > [条件（Conditions）] > [アンチマルウェア（Antimalware）] の ISE UI で行います。



第 7 章

Web セキュリティの設定

- Web セキュリティ モジュールについて （257 ページ）
- 一般的な Web セキュリティの設定 （258 ページ）
- Web セキュリティ ロギング （283 ページ）

Web セキュリティ モジュールについて

AnyConnect Web セキュリティ モジュールは、HTTP トラフィックを Cisco Cloud Web Security スキャニング プロキシにルーティングするエンドポイント コンポーネントです。

同時に各要素を分析できるように、Cisco Cloud Web Security は Web ページの要素を分解します。たとえば、特定の Web ページが HTTP、Flash、および Java 要素の組み合わせである場合、別個の「scanlets」がこれらの各要素を並行して分析します。次に、Cisco Cloud Web Security は、Cisco ScanCenter 管理ポータルに定義されたセキュリティ ポリシーに基づいて、良性または受け入れ可能なコンテンツを許可し、悪意があるか受け入れられないコンテンツをドロップします。これは、少数のコンテンツが許容されないために Web ページ全体が制限される「過剰ブロック」、または許容されないか場合によっては有害なコンテンツがページで提供されているのにページ全体が許可される「不十分なブロック」を防止します。Cisco Cloud Web Security は、社内ネットワークに接続しているかどうかにかかわらずユーザを保護します。

多数の Cisco Cloud Web Security スキャニング プロキシが世界各国に普及することで、AnyConnect Web セキュリティを活用するユーザは、遅延を最小限に抑えるために、応答時間が最も早い Cisco Cloud Web Security スキャニング プロキシにトラフィックをルーティングできます。

社内 LAN 上にあるエンドポイントを識別するように Secure Trusted Network Detection 機能を設定できます。この機能が有効になっている場合、社内 LAN から発信されるすべてのネットワーク トラフィックは、Cisco Cloud Web Security スキャニング プロキシをバイパスします。そのトラフィックのセキュリティは、Cisco Cloud Web Security ではなく、社内 LAN 上のデバイスにより別の方法で管理されます。

AnyConnect Web セキュリティ機能は、AnyConnect プロファイル エディタにより編集する AnyConnect Web セキュリティ クライアント プロファイルを使用して設定されます。

Cisco ScanCenter は、Cisco Cloud Web Security の管理ポータルです。Cisco ScanCenter を使用して作成または設定されたコンポーネントの一部は、AnyConnect Web セキュリティ クライアント プロファイルにも組み込まれています。

（注） ISE サーバは、静的な例外リストに常に記載されている必要があります。このリストは、Web セキュリティ クライアント プロファイルの [例外（Exceptions）] ペインに設定されています。

一般的な Web セキュリティの設定

手順

ステップ 1 クライアント プロファイルでの Cisco Cloud Web Security スキャニング プロキシを設定します。

ステップ 2 （任意）Cisco Cloud Web Security スキャニング プロキシについて、プロファイル エディタ内の既存のリストと、http://www.scansafe.cisco.com/ Web サイトからダウンロードしたスキャニング プロキシのリストを比較して相違がある場合、スキャニング プロキシ リストの更新を実行します。

ステップ 3 （任意）ユーザに対するスキャニング プロキシの表示または非表示を設定します。

ステップ 4 デフォルトのスキャニング プロキシの選択を行います。

ステップ 5 （任意）HTTP(S) トラフィック リスニング ポートの指定を行って、HTTPS Web トラフィックをフィルタリングします。

ステップ 6 Web スキャニング サービスでのエンドポイント トラフィックの除外または包含に対して、ホスト、プロキシ、または静的な例外を設定します。この設定により、指定された IP アドレスからのネットワーク トラフィックの評価が制限されます。

ステップ 7 ユーザ制御の設定および最も早いスキャニング プロキシ応答時間の計算を行います。この設定により、ユーザが接続する Cisco Cloud Web Security スキャニング プロキシが選択されます。

ステップ 8 社内 LAN から発信されるネットワーク トラフィックが Cisco Cloud Web Security スキャニング プロキシをバイパスするようにするには、Secure Trusted Network Detection の使用します。

ステップ 9 認証の設定および Cisco Cloud Web Security プロキシへのグループ メンバーシップの送信を行います。この設定により、企業ドメイン、Cisco ScanCenter または Active Directory グループに基づいてユーザが認証されます。

クライアント プロファイルでの Cisco Cloud Web Security スキャニング プロキシ

Cisco Cloud Web Security は、Web コンテンツを分析して、セキュリティ ポリシーに基づいて良性コンテンツの提供をブラウザに許可し、悪意のあるコンテンツをブロックします。スキャ

ニング プロキシは、Cisco Cloud Web Security が Web コンテンツを分析する Cisco Cloud Web セキュリティ プロキシ サーバです。AnyConnect Web セキュリティ プロファイル エディタ内の [スキャニング プロキシ（Scanning Proxy）] パネルは、AnyConnect Web セキュリティ モジュールによる Web ネットワーク トラフィックの送信先 Cisco Cloud Web Security スキャニング プロキシを定義します。

IPv6 Web トラフィックのガイドライン

IPv6アドレス、ドメイン名、アドレス範囲、またはワイルドカードの例外が指定されている場合を除き、IPv6 Web トラフィックはスキャニング プロキシに送信されます。スキャニング プロキシは、DNS ルックアップを実行して、ユーザが到達しようとしている URL の IPv4 アドレスがあるかどうかを確認します。IPv4 アドレスが見つかると、スキャニング プロキシはこのアドレスを使用して接続します。IPv4 アドレスが見つからない場合、接続はドロップされます。

すべての IPv6 トラフィックがスキャニング プロキシをバイパスできるようにするには、すべての IPv6 トラフィックに静的な例外 ::/0 を追加します。この例外により、すべての IPv6 トラフィックがすべてのスキャニング プロキシをバイパスします。したがって、IPv6 トラフィックは Web セキュリティで保護されません。

（注） Windows が実行されているコンピュータでは、AnyConnect がユーザ ID を判別できない場合、内部 IP アドレスがユーザ ID として使用されます。たとえば、enterprise_domains プロファイル エントリが指定されていない場合、内部 IP アドレスを使用して、Cisco ScanCenter でレポートを生成します。

Mac OS X が実行されているコンピュータでは、Mac がドメインにバインドされている場合、Webセキュリティモジュールは、コンピュータがログインしているドメインを報告できます。ドメインにバインドされていない場合、Web セキュリティ モジュールは、Mac の IP アドレスまたは現在ログインしているユーザ名を報告できます。

ユーザがスキャニング プロキシを選択する方法

プロファイルの設定方法に応じて、ユーザがスキャニング プロキシを選択できるか、または AnyConnect Web セキュリティ モジュールが応答時間が最も早いスキャニング プロキシにユーザを接続します。

- クライアント プロファイルがユーザ制御を許可した場合、ユーザは Cisco AnyConnect Secure Mobility Client Web Security トレイの [設定（Settings）] タブからスキャン プロキシを選択できます。
- クライアント プロファイルで [スキャン プロキシの自動選択（Automatic Scanning Proxy Selection）] 設定が有効になっている場合、AnyConnect Web セキュリティは、スキャニング プロキシを速い順に順序付けし、応答時間が最も速いスキャニング プロキシにユーザを接続します。
- クライアント プロファイルでユーザ制御が許可されなくても、[スキャン プロキシの自動選択（Automatic Scanning Proxy Selection）] が有効になっているときは、AnyConnect Web

セキュリティは、ユーザをデフォルトのスキャニング プロキシから、応答時間が最も速いスキャニング プロキシに切り替えます（応答時間が、最初に接続したデフォルトのスキャニング プロキシよりも大幅に速い場合）。

- ユーザが、現在のスキャニング プロキシからローミングし始めたときに、クライアント プロファイルで [スキャン プロキシの自動選択（Automatic Scanning Proxy Selection）] が設定されていれば、AnyConnect Web セキュリティは、ユーザを新しいスキャニング プロキシに切り替えます（応答時間が現在のスキャニング プロキシよりも大幅に早い場合）。

AnyConnect Web セキュリティでは、Windows の拡張された AnyConnect トレイ アイコン、AnyConnect GUI の [詳細設定（Advanced Settings）] タブ、および [詳細統計情報（Advanced Statistics）] タブに有効になっているスキャニング プロキシ名が表示されるため、ユーザは接続先のスキャニング プロキシを確認できます。

スキャニング プロキシ リストの更新

Web セキュリティ プロファイル エディタのスキャニング プロキシ リストは編集不可能です。Cisco Cloud Web Security スキャニング プロキシを Web セキュリティ プロファイル エディタ内のテーブルで追加したり削除したりすることはできません。

Web セキュリティ プロファイル エディタを起動した後で、スキャニング プロキシの最新のリストが保持されている Cisco Cloud Web Security Web サイトにアクセスすることで、スキャニング プロキシ リストが自動的に更新されます。

AnyConnect Web セキュリティ クライアント プロファイルの追加または編集時に、プロファイル エディタは、Cisco Cloud Web Security スキャニング プロキシの既存のリストを、http://www.scansafe.cisco.com/ からダウンロードされたスキャニング プロキシ リストと比較します。リストが古い場合は、「スキャニング プロキシ リストが古くなっています（Scanning Proxy list is out of date）」というメッセージと [リストの更新（Update List）] と表示されたコマンド ボタンが表示されます。スキャニング プロキシ リストを、Cisco Cloud Web Security スキャニング プロキシの最新のリストで更新するには、[リストの更新（Update List）] をクリックします。

[リストの更新（Update List）] をクリックすると、プロファイル エディタによって、既存の設定が可能な限り保持されます。プロファイル エディタは、デフォルト スキャニング プロキシの設定、および既存の Cisco Cloud Web Security スキャニング プロキシの表示または非表示設定を保持しています。

ユーザに対するスキャニング プロキシの表示または非表示

ユーザが ASA への VPN 接続を確立した後で、ASA は、クライアント プロファイルをエンドポイントにダウンロードします。AnyConnect Web セキュリティ クライアント プロファイルは、ユーザに表示される Cisco Cloud Web Security スキャニング プロキシを判別します。

ローミング ユーザが最大の利点を得るには、すべての Cisco Cloud Web Security スキャニング プロキシをすべてのユーザに表示することをお勧めします。

ユーザは、次の方法で、AnyConnect Web セキュリティ クライアント プロファイルのスキャニング プロキシ リストで「Display」とマークされたスキャニング プロキシと対話します。

- Cisco Cloud Web Security スキャニング プロキシは、Cisco AnyConnect Secure Mobility Client インターフェイスの [Web セキュリティ（Web Security）] パネルの [詳細（Advanced）] 設定のユーザに表示されます。
- AnyConnect Web セキュリティ モジュールは、応答時間でスキャニング プロキシを順序付ける際に、「Display」とマークされた Cisco Cloud Web Security スキャニング プロキシをテストします。
- ユーザは、自分のプロファイルでユーザ制御が許可される場合に接続する Cisco Cloud Web Security スキャニング プロキシを選択できます。
- AnyConnect Web セキュリティ クライアント プロファイルのスキャニング プロキシ テーブルで「Hide」とマークされている Cisco Cloud Web Security スキャニング プロキシは、ユーザに表示されず、応答時間でスキャニング プロキシを順序付ける際に評価されません。ユーザは、「Hide」とマークされたスキャニング プロキシには接続できません。

始める前に

AnyConnect Web セキュリティ クライアント プロファイルを作成します。

手順

ステップ 1 次のいずれかの方法で、Web セキュリティ プロファイル エディタを起動します。

- ASDM で、**[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [AnyConnect クライアント プロファイル（AnyConnect Client Profile）]** を選択します。
- Windows のスタンドアロン モードで、**[スタート（Start）] > [すべてのプログラム] > [Cisco] > [Cisco AnyConnect プロファイル エディタ（Cisco AnyConnect Profile Editor）] > [Web セキュリティ プロファイル エディタ（Web Security Profile Editor）]** を選択します。

ステップ 2 編集する Web セキュリティ クライアント プロファイルを開きます。

ステップ 3 Cisco Cloud Web Security スキャニング プロキシをユーザに非表示または表示するには、次の手順を実行します。

- 非表示にするスキャニング プロキシを選択し、[非表示（Hide）] をクリックします。
- 表示するスキャニング プロキシの名前を選択し、[表示（Display）] をクリックします。すべての Cisco Cloud Web Security スキャニング プロキシを表示するよう設定することをお勧めします。

ステップ 4 AnyConnect Web セキュリティ クライアント プロファイルを保存します。

デフォルトのスキャニング プロキシの選択

ユーザが初めてネットワークに接続すると、デフォルトのスキャニング プロキシにルーティングされます。デフォルトでは、作成するプロファイルには、次の Cisco Cloud Web Security スキャニング プロキシ属性があります。

- スキャニング プロキシ リストには、ユーザがアクセス可能なすべての Cisco Cloud Web Security スキャニング プロキシが入力されています。これらはすべて [表示（Display）] とマークされています。
- デフォルトの Cisco Cloud Web Security スキャニング プロキシは事前選択されています。
- AnyConnect Web セキュリティ モジュールが HTTP トラフィックを受信するポートのリストには、いくつかのポートが設定されています。

手順

ステップ 1 次のいずれかの方法で、Web セキュリティ プロファイル エディタを起動します。

- ASDM で、**[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [AnyConnect クライアント プロファイル（AnyConnect Client Profile）]** を選択します。
- Windows のスタンドアロン モードで、**[スタート（Start）] > [すべてのプログラム] > [Cisco] > [Cisco AnyConnect プロファイル エディタ（Cisco AnyConnect Profile Editor）] > [Web セキュリティ プロファイル エディタ（Web Security Profile Editor）]** を選択します。

ステップ 2 編集する Web セキュリティ クライアント プロファイルを開きます。

ステップ 3 [デフォルトのスキャニング プロキシ（Default Scanning Proxy）] フィールドからデフォルトのスキャニング プロキシを選択します。

ステップ 4 AnyConnect Web セキュリティ クライアント プロファイルを保存します。

HTTP(S) トラフィック リスニング ポートの指定

Scan Safe Web スキャニング サービスは、デフォルトで HTTP Web トラフィックを分析します。設定を通じて、HTTPS Web トラフィックをフィルタリングできます。Web セキュリティ クライアント プロファイルで、Web セキュリティがこれらのタイプのネットワーク トラフィックをリッスンするポートを指定します。

手順

ステップ 1 次のいずれかの方法で、Web セキュリティ プロファイル エディタを起動します。

- ASDM で、**[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [AnyConnect クライアント プロファイル（AnyConnect Client Profile）]** を選択します。
- Windows のスタンドアロン モードで、**[スタート（Start）] > [すべてのプログラム] > [Cisco] > [Cisco AnyConnect プロファイル エディタ（Cisco AnyConnect Profile Editor）] > [Web セキュリティ プロファイル エディタ（Web Security Profile Editor）]** を選択します。

ステップ 2 編集する Web セキュリティ クライアント プロファイルを開きます。

ステップ 3 [トラフィック リスニング ポート（Traffic Listen Port）] フィールドに、Web セキュリティ モジュールが HTTP トラフィック、HTTPS トラフィック、または両方をリッスンする論理ポート番号を入力します。

ステップ 4 Web セキュリティ クライアント プロファイルを保存します。

パブリック プロキシを設定するための Windows インターネット オプションの設定

通常、パブリック プロキシは Web トラフィックの匿名化に使用されます。パブリック プロキシ サーバは認証プロキシ サーバと呼ばれます。このサーバにはユーザ名とパスワードが必要となることがあります。AnyConnect Web セキュリティでは、基本と NTLM という 2 種類の認証がサポートされています。プロキシ サーバが認証必須に設定されている場合、AnyConnect Web セキュリティは実行時にプロキシを検出し、認証プロセスを管理します。プロキシ サーバへの認証に成功すると、AnyConnect Web セキュリティが、Web トラフィックをパブリック プロキシ経由で Cisco クラウド Web セキュリティ スキャン プロキシへルーティングします。AnyConnect Web セキュリティはプロキシのクレデンシャルを暗号化してメモリ内に安全にキャッシュします。ユーザがプロキシ ネットワークから非プロキシ ネットワークに移動し、再びこのプロキシネットワークに戻る場合でも、クレデンシャルが再び必要となることがありません。パブリック プロキシを使用する場合、サービスの再起動は不要です。ユーザが非プロキシ ネットワークに移動すると、AnyConnect Web セキュリティは実行時にこれを自動的に検出し、Cisco クラウド Web セキュリティ スキャン プロキシに Web トラフィックを直接送信開始します。

Windows のインターネット オプションで、クライアント側でパブリック プロキシを使用するように設定されている場合、AnyConnect はその接続を使用します。

（注） Windows では基本および NTLM パブリック プロキシがサポートされています。Mac では基本パブリック プロキシだけがサポートされています。

1. Internet Explorer またはコントロール パネルから [インターネット オプション（Internet Options）] を開きます。
2. [接続（Connections）] タブを選択し、[LANの設定（LAN Settings）] をクリックします。
3. プロキシ サーバを使用するように LAN を設定します。

4. プロキシ サーバの IP アドレスまたはホスト名を入力します。FTP/HTTP/HTTPS に対してそれぞれ個別のプロキシが設定されている場合は、HTTPS プロキシだけが考慮されます。

制限事項

- パブリック プロキシの背後にある IPv6 および TND はサポートされません。
- プロキシ IP は、AnyConnect Web セキュリティの例外リストに含まれていてはなりません。例外リストに含まれている場合、トラフィックが AnyConnect Web セキュリティ に転送されません。
- プロキシ ポートがデフォルトの Web ポートと異なる場合は、AnyConnect Web セキュリティ プロファイルの kdf リスニング ポートの一覧にプロキシ ポートを追加する必要があります。

Web スキャニング サービスでのエンドポイント トラフィックの除外または包含

Cisco Cloud Web Security スキャニングで特定のネットワーク トラフィックを除外または包含するには、Web セキュリティ プロファイル エディタを使用して該当トラフィックに対する例外を設定します。次の複数のカテゴリの例外を設定できます。

- [ホスト例外（Host Exceptions）] または [ホスト包含（Host Inclusions）] : [ホスト例外（Host Exceptions）] が設定されている場合、入力する IP アドレス（パブリックまたはプライベート、ホスト名、またはサブネット）はバイパスされます。[ホスト包含（Host Inclusions）] が設定されている場合、入力する IP アドレス（パブリックまたはプライベート、ホスト名、またはサブネット）は Web セキュリティ プロキシに転送されますが、その他のトラフィックはすべてバイパスされます。

（注） AnyConnect は、[ホスト例外（Host Exceptions）] にリストされているトラフィックも代行受信できます。

- [プロキシ例外（Proxy Exceptions）] : ここにリストされている内部プロキシ サーバは、スキャンから除外されます。
-
- [静的な例外（Static Exceptions）] : ここにリストされている IP アドレスまたはホスト名は、スキャンおよび AnyConnect から除外されます。

ISE サーバ要件

ISE サーバは、静的な例外リストに常に記載されている必要があります。このリストは、Web セキュリティ クライアント プロファイルの [例外（Exceptions）] ペインに設定されています。さらに、ISE ポスチャ クライアントが ISE サーバに到達できるように、Web セキュリティ モ

ジュールはISEポスチャ プローブをバイパスする必要があります。ISEポスチャ プロファイルは、ISE サーバを検出するために次の順序でネットワーク プローブを送信します。

1. デフォルト ゲートウェイ
2. Discovery host
3. enroll.cisco.com
4. 以前に接続した ISE サーバ

ホスト例外の除外と包含

始める前に

- トップレベル ドメインの両側にワイルドカードを使用しないでください（たとえば *.cisco.*）。これによりフィッシング サイトが含まれることがあるためです。
- デフォルトのホスト例外エントリを削除または変更しないでください。

[ホスト例外（Host Exceptions）] と [ホスト包含（Host Inclusions）] のいずれかを設定することを選択できます。[ホスト例外（Host Exceptions）] を選択した場合、指定された IP アドレスは Cisco クラウド Web セキュリティ プロキシによりバイパスされます。[ホスト包含（Host Inclusions）] を選択した場合、指定された IP アドレスは Cisco クラウド Web セキュリティ プロキシに転送され、その他のトラフィックはすべてバイパスされます。AnyConnect は除外されたホスト例外からのインターネット トラフィックを引き続き代行受信する場合があることに注意してください。Web Security と AnyConnect の両方からのトラフィックを除外するには、静的な例外を設定します。

手順

ステップ 1 [ホスト例外（Host Exceptions）] または [ホスト包含（Host Inclusions）] を選択します。

ステップ 2 ステップ 1 の選択に応じてバイパスまたは転送する IP アドレス（パブリックまたはプライベート、ホスト名、またはサブネット）を追加します。

ステップ 3 次の構文を使用してサブネットと IP アドレスを入力します。

構文	例
個々の IPv4 および IPv6 アドレス	10.255.255.255 2001:0000:0234:C1AB:0000:00A0:AABC:003F
Classless Inter-Domain Routing（CIDR）表記	10.0.0.0/8 2001:DB8::/48

完全修飾ドメイン名	windowsupdate.microsoft.com ipv6.google.com （注） 部分的なドメインはサポートされません。たとえば、example.com はサポートされません。
完全修飾ドメイン名または IP アドレスのワイルドカード	127.0.0.* *.cisco.com

（注） ホスト例外リストでドメイン名を使用するように Web セキュリティが設定されている場合、ユーザがホスト HTTP ヘッダー エントリをスプーフィングして Web セキュリティ プロキシをバイパスできます。例外リストでホスト名の代わりに IP アドレスを使用すると、このリスクを緩和できます。

Web セキュリティとローミング セキュリティの互換性に必須のホスト例外

Umbrella ローミング セキュリティ モジュールと Web セキュリティ モジュールを一緒に展開している場合は、ホスト例外として *.opendns.com を設定する必要があります。この設定に失敗すると、Umbrella ローミング セキュリティ DNS 保護は完全にバイパスされます。

また、Web セキュリティと Umbrella ローミング セキュリティ モジュールの互換性に必須の静的な例外 （267 ページ）に記載されている静的な例外の除外を設定する必要があります。

プロキシ例外の除外

[プロキシ例外（Proxy Exceptions）] 領域には、認証された内部プロキシの IP アドレスを入力します（例：`172.31.255.255`）。

このフィールドに IPv4 および IPv6 アドレスを指定できますが、ポート番号を一緒に指定することはできません。CIDR 表記を使用して IP アドレスを指定できません。

IP アドレスを指定すると、Cisco Cloud Web Security が、これらのサーバ宛の Web データを代行受信して SSL を使用してデータをトンネルしないようにします。プロキシ サーバは、サービスを中断させることなく実行できます。プロキシ サーバを追加しなかった場合は、Cisco Cloud Web Security トラフィックが SSL トンネルのように見えます。

プロキシサーバ経由のブラウザのトラフィックを除外する場合は、それらのホスト名をホスト例外でリストし、転送されないようにする必要があります。プロキシを通過するトラフィックの静的な例外を設定できないだけでなく、プロキシ例外リストにリストすることもできません。

このリストに存在しないプロキシの場合、Web セキュリティは SSL を使用してプロキシにトンネルしようとします。したがって、インターネットアクセスのためにプロキシをネットワークから除外する必要がある別の企業サイトにユーザが存在する場合、Cisco Cloud Web Security ではオープンなインターネット接続を利用しているかのような同じレベルのサポートが提供されます。

静的な例外の除外

Cisco Cloud Web Security をバイパスするトラフィックを決定し、Classless Inter-Domain Routing（CIDR）表記での個々の IP アドレスまたは IP アドレス範囲のリストを追加します。リストには、VPN ゲートウェイの入力 IP アドレスを含めます。AnyConnect リリース 4.3.02039 以降を使用すると、スキャンから除外するホスト名を追加できます。Web セキュリティは、インスペクションのためにクラウド Web セキュリティ プロキシに HTTP/HTTPS トラフィックを転送しません。

同じ IP アドレスの複数のホスト名があるが、ホスト名の 1 つが静的な例外リストに設定されている場合は、Web セキュリティはトラフィックを除外します。

http://www.ietf.org/rfc/rfc1918.txt に記載されたプライベート IP アドレスは、デフォルトで静的な例外リストに含まれています。

（注） 静的な例外リストのいずれかの範囲に含まれる IP アドレスを持つプロキシ サーバがある場合は、ホストの例外リストにその例外を移動します。たとえば、静的な例外リストに 10.0.0.0/8 が記載されているとします。10.1.2.3 に設定されているプロキシがある場合、ホストの例外リストに 10.0.0.0/8 を移動します。そうしないと、このプロキシに送信されたトラフィックは Cloud Web Security をバイパスします。

CIDR 表記を使用して、IPv4 および IPv6 アドレスまたはアドレスの範囲を指定できます。完全修飾ドメイン名を指定したり、IP アドレスにワイルドカードを使用したりすることはできません。正しい構文の例は次のとおりです。

```
10.10.10.5
192.0.2.0/24
```

（注） SSL VPN コンセントレータの IP アドレスを静的な除外リストに追加してください。

Web セキュリティと Umbrella ローミング セキュリティ モジュールの互換性に必須の静的な例外

Umbrella ローミング セキュリティと Web セキュリティ モジュール間の相互運用性を確保するためには、AnyConnect にプロビジョニングされる Web セキュリティ プロファイルで次の例外を設定する必要があります。

- 77.67.54.0/27
- 77.67.54.32/27
- 77.67.54.64/27
- 77.67.54.96/27
- 77.67.54.128/27
- 77.67.54.160/27

- 67.215.64.0/19
- 204.194.232.0/21
- 208.67.216.0/21
- 208.69.32.0/21
- 185.60.84.0/22
- 146.112.61.0/22
- 146.112.128.0/18
- 146.112.255.101

また、Web セキュリティとローミング セキュリティの互換性に必須のホスト例外 （266 ページ）に記載されているホスト例外の除外を設定する必要があります。

ユーザ制御の設定および最も早いスキャニングプロキシ応答時間の計算

ユーザが、接続先の Cisco Cloud Web Security スキャニング プロキシを選択できるようにするには、次の手順を実行します。

手順

ステップ 1 次のいずれかの方法で、Web セキュリティ プロファイル エディタを起動します。

- ASDM で、**[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [AnyConnect クライアント プロファイル（AnyConnect Client Profile）]** を選択します。
- Windows のスタンドアロン モードで、**[スタート（Start）] > [すべてのプログラム] > [Cisco] > [Cisco AnyConnect プロファイル エディタ（Cisco AnyConnect Profile Editor）] > [Web セキュリティ プロファイル エディタ（Web Security Profile Editor）]** を選択します。

ステップ 2 編集する Web セキュリティ クライアント プロファイルを開きます。

ステップ 3 [プリファレンス（Preferences）] をクリックします。

ステップ 4 [ユーザ制御可（User Controllable）] をオンにします（これがデフォルト設定です）。[ユーザ制御可（User Controllable）] は、ユーザが AnyConnect インターフェイスで [自動タワー選択（Automatic Tower Selection）] および [応答時間によるスキャニングプロキシの順序付け（Order Scanning Proxies by Response Time）] 設定を変更できるかどうかを決定します。

ステップ 5 Web セキュリティで自動的にスキャン プロキシを選択するには、[スキャンプロキシの自動選択（Automatic Scanning Proxy Selection）] を選択します。これを選択すると、[応答時間によるスキャニング プロキシの順序付け（Order Scanning Proxies by Response Time）] が自動的にオンになります。

- [スキャンプロキシの自動選択（Automatic Scanning Proxy Selection）] を選択すると、Web セキュリティは、応答時間が最も早いスキャニング プロキシを判別して、ユーザをそのスキャニング プロキシに自動的に接続します。
- [スキャンプロキシの自動選択（Automatic Scanning Proxy Selection）] を選択しなくても、まだ [応答時間によるスキャニング プロキシの順序付け（Order Scanning Proxies by Response Time）] が選択されている場合、ユーザには、接続できるスキャニング プロキシのリストが、応答時間が早い順に表示されます。
- [スキャンプロキシの自動選択（Automatic Scanning Proxy Selection）] を選択しない場合でも、ユーザが AnyConnect ユーザ インターフェイスでこの機能を有効にできますが、いったん有効にすると、再度無効に切り替えることができません。

（注） [スキャンプロキシの自動選択（Automatic Scanning Proxy Selection）] を有効にすると、一時的な通信の中断と障害が原因で、アクティブなスキャニング プロキシの選択が自動的に変更される可能性があります。スキャニング プロキシの変更は不適切な場合があり、異なる言語を使用する異なる国のスキャニング プロキシから検索結果が返されるなど、予期しない動作を引き起こすことがあります。

ステップ 6 [応答時間によるスキャニング プロキシの順序付け（Order Scanning Proxies by Response Time）] をオンにした場合は、応答時間が最も早いスキャニング プロキシを計算するための次の設定を行います。

- [テスト間隔の有効化（Enable Test Interval）]：各パフォーマンス テストの実行間の時間（時間および分単位。デフォルトは 2 分間です）。[テスト間隔の有効化（Enable Test Interval）] チェックボックスをオフにすることで、テスト間隔をオフにして、テストが実行されないようにできます。
- [テストの非アクティブ タイムアウト（Test Inactivity Timeout）]：Web セキュリティが、ユーザ非アクティブのために応答時間テストを一時停止するまでの時間（分単位）。Web セキュリティは、スキャニング プロキシで接続試行が行われるとすぐにテストを再開します。この設定は、カスタマーサポートから指示された場合以外は変更しないでください。

（注） [応答時間によるスキャニング プロキシの順序付け（Ordering Scanning Proxies by Response Time）] テストは、次の例外を除き、テスト間隔に基づいて実行し続けます。

- Secure Trusted Network Detection が有効で、マシンが社内 LAN 上にあることが検出された。
- Web セキュリティのライセンス キーがないか、無効である。
- ユーザが、設定済みの時間非アクティブで、その結果 [テストの非アクティブ タイムアウト（Test Inactivity Timeout）] しきい値に達した。

ステップ 7 エンドポイントが社内 LAN 上に物理的に存在するタイミング、または VPN 接続を使用して存在するタイミングを検出する [セキュアな信頼ネットワーク検出（Secure Trusted Network Detection）] をクリックし、有効化します。有効になっている場合、社内 LAN から発信される

すべてのネットワーク トラフィックは、Cisco Cloud Web Security スキャニング プロキシをバイパスします。

ステップ 8 [https] フィールドに各信頼サーバの URL を入力し、[追加（Add）] をクリックします。URL にはポート アドレスを含めることができます。プロファイル エディタは、信頼サーバへの接続を試みます。接続できなくても、サーバ証明書の SHA-256 ハッシュがわかっている場合は、それを [証明書ハッシュ（Certificate hash）] ボックスに入力し、[設定（Set）] をクリックします。

ステップ 9 Web セキュリティ クライアント プロファイルを保存します。

次のタスク

詳細については、『*ScanCenter Administrator Guide, Release 5.2*』を参照してください。

Secure Trusted Network Detection の使用

Secure Trusted Network Detection 機能は、エンドポイントが社内 LAN 上に物理的に存在するタイミング、または VPN 接続を使用して存在するタイミングを検出します。Secure Trusted Network Detection 機能が有効になっている場合、社内 LAN からのネットワーク トラフィックはすべて、送信元の Cisco Cloud Web Security スキャニング プロキシをバイパスします。そのトラフィックのセキュリティは、Cisco Cloud Web Security ではなく、社内 LAN に存在するデバイスにより別の方法で管理されます。

Secure Trusted Network Detection では、既知の URL（アドレス、IP、または FQDN）にあるサーバ上の SSL 証明書の SHA-256 ハッシュ（サムプリント）を使用してクライアントが社内ネットワークに接続されていることを確認します。証明書によって使用される暗号化アルゴリズムは問いませんが、SHA-256 ハッシュのみを使用できます。

ネットワークにプロキシが存在する（Cisco Cloud Web Security コネクタなど）状態で、Secure Trusted Network Detection を使用しない場合は、プロファイル エディタの [例外（Exceptions）] パネルで、プロキシ例外のリストに各プロキシを追加する必要があります。

複数のサーバ：複数のサーバを定義すると、クライアントが最初のサーバに対して 2 回連続試行しても接続できない場合に、2 番目のサーバに対して試行します。クライアントは、リスト内のすべてのサーバに対して試行した後、5 分間待ってから、最初のサーバに再接続を試みます。

（注） 内部ネットワークの外から操作する場合は、Secure Trusted Network Detection が DNS 要求を行い、プロビジョニングした HTTPS サーバに接続を試みます。シスコでは、内部ネットワークの外で使用されているマシンからのこのような要求によって組織内の名前や内部構造が明らかになることを防ぐために、エイリアス設定の使用をお勧めします。

始める前に

- プロキシ例外の除外

- データ損失の防止（DLP）アプライアンスなどの一部のサードパーティ製ソリューションでは、Webセキュリティの影響を受けないトラフィックが必要になるため、Secure Trusted Network Detection を設定することが必要となります。
- プロファイルを編集するときは、SSL 証明書がホストされるサーバへの直接接続があることを確認します。

手順

ステップ 1 次のいずれかの方法で、Web セキュリティ プロファイル エディタを起動します。

- ASDM で、**[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [AnyConnect クライアント プロファイル（AnyConnect Client Profile）]** を選択します。
- Windows のスタンドアロン モードで、**[スタート（Start）] > [すべてのプログラム] > [Cisco] > [Cisco AnyConnect プロファイル エディタ（Cisco AnyConnect Profile Editor）] > [Web セキュリティ プロファイル エディタ（Web Security Profile Editor）]** を選択します。

ステップ 2 編集する Web セキュリティ クライアント プロファイルを開きます。

ステップ 3 [Web セキュリティ（Web Security）] ツリー ペインで、[プリファレンス（Preferences）] をクリックします。

ステップ 4 [Trusted Network Detection の有効化（Enable Trusted Network Detection）] を選択します。

ステップ 5 [https] フィールドに各信頼サーバの URL を入力し、[追加（Add）] をクリックします。URL にはポート アドレスを含めることができます。プロファイル エディタは、信頼サーバへの接続を試みます。接続できなくても、サーバ証明書の SHA-256 ハッシュがわかっている場合は、それを [証明書ハッシュ（Certificate hash）] ボックスに入力し、[設定（Set）] をクリックします。

（注） プロキシの背後にある信頼サーバはサポートされません。

ステップ 6 Web セキュリティ クライアント プロファイルを保存します。

Secure Trusted Network Detection の不使用

ネットワークにプロキシが存在する（Cisco Cloud Web Security コネクタなど）状態で、Secure Trusted Network Detection を使用しない場合は、プロファイル エディタの [例外（Exceptions）] パネルで、プロキシ例外のリストに各プロキシを追加する必要があります。

認証の設定および Cisco Cloud Web Security プロキシへのグループ メンバーシップの送信

始める前に

Windows を使用したフィルタの無効化と有効化 （282 ページ）

手順

ステップ 1 次のいずれかの方法で、Web セキュリティ プロファイル エディタを起動します。

- ASDM で、**[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [AnyConnect クライアント プロファイル（AnyConnect Client Profile）]** を選択します。
- Windows のスタンドアロン モードで、**[スタート（Start）] > [すべてのプログラム] > [Cisco] > [Cisco AnyConnect プロファイル エディタ（Cisco AnyConnect Profile Editor）] > [Web セキュリティ プロファイル エディタ（Web Security Profile Editor）]** を選択します。

ステップ 2 編集する Web セキュリティ クライアント プロファイルを開きます。

ステップ 3 [認証（Authentication）] をクリックします。

ステップ 4 [プロキシ認証ライセンス キー（Proxy Authentication License Key）] フィールドに、Cisco ScanCenter で作成した企業キー、グループ キー、またはユーザ キーに対応するライセンス キーを入力します。これらの企業ドメインに基づいてユーザを認証するには、作成した企業キーを入力します。Cisco ScanCenter または Active Directory グループに基づいてユーザを認証するには、作成したグループ キーを入力します。デフォルトでは、このタグは空です。空のままにした場合、Web セキュリティはパススルー モードで動作します。

ステップ 5 [サービス パスワード（Service Password）] に入力します。Web セキュリティのデフォルト パスワードは websecurity です。プロファイルのカスタマイズ時にこのパスワードを変更してください。パスワードには英数字（a ～ z、A ～ Z、0 ～ 9）のみを使用する必要があります。次のような特殊文字は、Windows コマンド シェルによって制御文字と間違われる可能性があるか、XML で特殊な意味を持つことがあります。

```
~ @ # $ % * - _ + = { } [ ] : , . ? /
```

このパスワードを使用して、管理者の権限を持っているユーザは、Web セキュリティ サービスを停止できます。管理者権限を持つユーザまたは持たないユーザは、このパスワードなしで Web セキュリティ サービスを開始できます。

ステップ 6 すべての HTTP 要求とともに企業ドメイン情報および Cisco Cloud Web Security または Active Directory グループ情報をスキャニング プロキシ サーバに送信します。スキャニング プロキシは、ユーザのドメインおよびグループ メンバーシップについて認識している内容に基づいてトラフィック フィルタリング ルールを適用します。

（注） ユーザのカスタム ユーザ名およびカスタム グループ情報をスキャニング サーバ プロキシに送信するには、このステップをスキップし、ステップ 7 に進みます。Active Directory を使用しない企業の場合は、ステップ 7 もスキップしてください。

a) [企業ドメインの有効化（Enable Enterprise Domains）] をクリックします。リストから [すべてのドメイン（All Domains）] をクリックします。[すべてのドメイン（All Domains）] オプションが選択され、マシンがドメイン内にある場合、ユーザが属するドメインが照合され、ユーザ名とグループ メンバーシップ情報が Cisco Cloud Web Security スキャニング プロキシに送信されます。このオプションは、社内に複数のドメインがある場合に役立ちます。

b) または、[個々のドメインの指定（Specify Individual Domains）] をクリックします。

NetBIOS 形式で各ドメイン名を入力し、[追加（Add）] をクリックします。たとえば、`example.cisco.com` の NetBIOS 形式は cisco です。DNS 形式を使用したドメイン名（abc.def.com）を入力しないでください。

[企業ドメイン名（Enterprise Domain name）] フィールドにドメイン名を指定すると、Cisco Cloud Web Security は、現在ログインしている Active Directory ユーザを識別し、そのユーザの Active Directory グループを列挙し、その情報をすべての要求とともにスキャニング プロキシに送信します。

c) [使用（Use）] リストで、[グループ包含リスト（Group Include List）] または [グループ除外リスト（Group Exclude List）] をクリックし、Cisco Cloud Web Security スキャニング プロキシに対する HTTP 要求でグループ情報を含めるか除外します。値には、照合する文字列の任意の部分文字列を指定できます。

[グループ包含リスト（Group Include List）]。[グループ包含リスト（Group Include List）] を選択した後、Cisco Cloud Web Security グループ名または Active Directory グループ名を [グループ包含リスト（Group Include List）] に追加します。これらのグループ名は、HTTP 要求とともに Cisco Cloud Web Security スキャニング プロキシ サーバに送信されます。要求が、指定された企業ドメイン内のユーザから出された場合、HTTP 要求は、ユーザのグループ メンバーシップに従ってフィルタリングされます。ユーザにグループ メンバーシップがない場合、HTTP 要求は、デフォルトのフィルタリング ルール セットを使用してフィルタリングされます。

[グループ除外リスト（Group Exclude List）]。[グループ除外リスト（Group Exclude List）] に、Cisco Cloud Web Security グループ名または Active Directory グループ名を追加します。これらのグループ名は、HTTP 要求とともに Cisco Cloud Web Security スキャニング プロキシ サーバに送信されません。ユーザが、[グループ除外リスト（Group Exclude List）] のいずれかのグループに属している場合、そのグループ名はスキャニング プロキシ サーバに送信されず、ユーザの HTTP 要求は、その他のグループ メンバーシップ、または最低でも Active Directory または Cisco Cloud Web Security グループ所属を持たないユーザに対して定義されたデフォルトのフィルタリング ルール セットのいずれかによってフィルタリングされます。

ステップ 7 スキャニング プロキシ サーバのカスタム名を送信するには、[ドメインに参加していないマシンのカスタム照合およびレポート（Custom matching and reporting for machines not joined to domains）] をクリックします。

a) コンピュータの名前を使用するには、リストの [コンピュータ名（Computer Name）] をクリックします。または、ローカル ユーザ名を使用するには、[ローカル ユーザ（Local User）] をクリックします。または、カスタム ユーザ名を入力するには、[カスタム名（Custom Name）] をクリックします。これは、任意の文字列で定義できます。文字列を入力しない場合、代わりにコンピュータの IP アドレスが、スキャニング プロキシ サーバに送信されます。このユーザ名または IP アドレスは、カスタム ユーザから HTTP トラフィックを識別する Cisco ScanCenter レポートで使用されます。

b) [認証グループ（Authentication Group）] フィールドに、最大 256 文字の英数字のカスタム グループ名を入力し、[追加（Add）] をクリックします。

HTTP 要求がスキャニング プロキシ サーバに送信されると、カスタム グループ名が送信された場合に、スキャニング プロキシ サーバに対応するグループ名があれば、HTTP トラフィックは、カスタム グループ名に関連付けられたルールによってフィルタリングされます。スキャニング プロキシ サーバで定義された対応するカスタム グループがない場合、HTTP 要求はデフォルト ルールによってフィルタリングされます。

カスタム ユーザ名のみを設定し、カスタム グループを設定していない場合、HTTP 要求は、スキャニング プロキシ サーバのデフォルト ルールによってフィルタリングされます。

ステップ 8 Web セキュリティ クライアント プロファイルを保存します。

Web セキュリティの詳細設定

Web セキュリティ クライアント プロファイルの [詳細（Advanced）] パネルには、シスコ カスタマー サポート エンジニアによる問題のトラブルシューティングに役立ついくつかの設定が表示されます。このパネルの設定は、カスタマー サポートから指示された場合以外は変更しないでください。

プロファイル エディタの [詳細（Advanced）] パネルから、次のタスクを実行します。

- KDF リスニング ポートの設定 （274 ページ）
- ポートが着信接続を受信する方法の設定 （275 ページ）
- タイムアウトと再試行が発生するタイミングの設定 （276 ページ）
- DNS ルックアップ （276 ページ）
- デバッグの設定 （277 ページ）
- トラフィックのブロックと許可 （277 ページ）

KDF リスニング ポートの設定

Kernel Driver Framework（KDF）は、トラフィック リスニング ポートの 1 つを宛先ポートとして使用する接続をすべて代行受信して、トラフィックを KDF リスニング ポートに転送します。Web スキャニング サービスは、KDF リスニング ポートに転送されるトラフィックをすべて分析します。

始める前に

この設定は、カスタマー サポートから指示された場合以外は変更しないでください。

手順

ステップ 1 次のいずれかの方法で、Web セキュリティ プロファイル エディタを起動します。

- ASDM で、**[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [AnyConnect クライアント プロファイル（AnyConnect Client Profile）]** を選択します。
- Windows のスタンドアロン モードで、**[スタート（Start）] > [すべてのプログラム] > [Cisco] > [Cisco AnyConnect プロファイル エディタ（Cisco AnyConnect Profile Editor）] > [Web セキュリティ プロファイル エディタ（Web Security Profile Editor）]** を選択します。

ステップ 2 編集する Web セキュリティ クライアント プロファイルを開きます。

ステップ 3 [Web セキュリティ（Web Security）] ツリー ペインで、[詳細（Advanced）] をクリックします。

ステップ 4 [KDF リスニング ポート（KDF Listen Port）] フィールドに KDF リスニング ポートを指定します。

ステップ 5 Web セキュリティ クライアント プロファイルを保存します。

ポートが着信接続を受信する方法の設定

サービス通信ポートは、Web スキャニング サービスが、AnyConnect GUI コンポーネントおよびその他のユーティリティ コンポーネントからの着信接続を受信するポートです。

始める前に

この設定は、カスタマー サポートから指示された場合以外は変更しないでください。

手順

ステップ 1 次のいずれかの方法で、Web セキュリティ プロファイル エディタを起動します。

- ASDM で、**[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [AnyConnect クライアント プロファイル（AnyConnect Client Profile）]** を選択します。
- Windows のスタンドアロン モードで、**[スタート（Start）] > [すべてのプログラム] > [Cisco] > [Cisco AnyConnect プロファイル エディタ（Cisco AnyConnect Profile Editor）] > [Web セキュリティ プロファイル エディタ（Web Security Profile Editor）]** を選択します。

ステップ 2 編集する Web セキュリティ クライアント プロファイルを選択して [編集（Edit）] をクリックします。[Web セキュリティ（Web Security）] ツリー ペインで、[詳細（Advanced）] をクリックします。

ステップ 3 [サービス通信ポート（Service Communication Port）] フィールドを編集します。

ステップ 4 Web セキュリティ クライアント プロファイルを保存します。

（注） デフォルト値の 5300 からポートを変更した場合は、Web セキュリティ サービスと AnyConnect GUI コンポーネントをリスタートする必要があります。

タイムアウトと再試行が発生するタイミングの設定

接続タイムアウト設定によって、Web セキュリティがスキャニング プロキシを使用せずにインターネットにアクセスしようとするまでのタイムアウトを設定できます。空白のままにすると、デフォルト値の 4 秒が使用されます。この設定により、ユーザは再試行までのタイムアウトを待つことなく、有料ネットワーク サービスに迅速にアクセスできます。

手順

ステップ 1 次のいずれかの方法で、Web セキュリティ プロファイル エディタを起動します。

- ASDM で、**[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [AnyConnect クライアント プロファイル（AnyConnect Client Profile）]** を選択します。
- Windows のスタンドアロン モードで、**[スタート（Start）] > [すべてのプログラム] > [Cisco] > [Cisco AnyConnect プロファイル エディタ（Cisco AnyConnect Profile Editor）] > [Web セキュリティ プロファイル エディタ（Web Security Profile Editor）]** を選択します。

ステップ 2 編集する Web セキュリティ クライアント プロファイルを開きます。

ステップ 3 [Web セキュリティ（Web Security）] ツリー ペインで、[詳細（Advanced）] をクリックします。

ステップ 4 [接続タイムアウト（Connection Timeout）] フィールドを変更します。

ステップ 5 Web セキュリティ クライアント プロファイルを保存します。

DNS ルックアップ

プロファイル エディタの [詳細（Advanced）] パネルには、ドメイン ネーム サーバ ルックアップを管理するためのフィールドがいくつか含まれています。これらは、DNS ルックアップに最適な値で設定されています。

ガイドライン

この設定は、カスタマー サポートから指示された場合以外は変更しないでください。

デバッグの設定

[デバッグ レベル（Debug Level）] は設定可能なフィールドです。

ガイドライン

この設定は、カスタマー サポートから指示された場合以外は変更しないでください。

トラフィックのブロックと許可

Cisco Cloud Web Security プロキシ サーバへの接続が確立できない場合、トラフィックをブロックするように [接続障害ポリシー（Connection Failure Policy）] リストで [フェール クローズ（Fail Close）] を選択します。または、[フェール オープン（Fail Open）] を選択し、トラフィックを許可します。

Cisco Cloud Web Security プロキシ サーバへの接続が確立できないけれども、Wi-Fi ホット スポットなどのキャプティブ ポータルが検出された場合に、トラフィックを許可するには、[キャプティブ ポータルが検出された場合（When a captive portal is detected）] リストで [フェール オープン（Fail Open）] を選択します。または、[フェール クローズ（Fail Close）] を選択し、トラフィックをブロックします。

（注） キャプティブ ポータルのアドレスを含めるようにホスト、プロキシ、または静的な例外が設定されている場合、[フェール クローズ（Fail Close）] はトラフィックをブロックしません。

他のカスタマイズ可能な Web セキュリティ オプション

エクスポート オプション

プレーン テキストの Web セキュリティ クライアント プロファイル ファイルのエクスポート

難解化 Web セキュリティ クライアント プロファイルを ASA からエクスポートして、エンドポイント デバイスに配布します。

手順

ステップ 1 ASDM で、**[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [AnyConnect クライアント プロファイル（AnyConnect Client Profile）]** の順に選択します。

ステップ 2 編集する Web セキュリティ クライアント プロファイルを選択して [エクスポート（Export）] をクリックします。

ステップ 3 ファイルを保存するローカル フォルダを参照します。[ローカル パス（Local Path）] フィールドのファイル名を編集すると、その新しいファイル名で Web セキュリティ クライアント プロファイルが保存されます。

ステップ 4 [エクスポート（Export）] をクリックします。

ASDM は、Web セキュリティ クライアント プロファイルのプレーン テキスト バージョンである `filename.wsp` をエクスポートします。

DART バンドルのプレーン テキストの Web セキュリティ クライアント プロファイル ファイルのエクスポート

Diagnostic AnyConnect Reporting Tool（DART）バンドルをシスコのカスタマー サービスに送信する必要がある場合、プレーン テキスト バージョンの Web セキュリティ クライアント プロファイル ファイル（`filename.wsp` または `filename.xml`）を DART バンドルとともに送信する必要があります。シスコ カスタマー サービスは難読化されたバージョンを読み取ることはできません。

プロファイル エディタのスタンドアロン バージョンは、Web セキュリティ プロファイル ファイルの 2 つのバージョンを作成します。1 つはファイル名が `filename.wso` の難解化ファイル、もう 1 つはファイル名が `filename.xml` のプレーン テキスト ファイルです。

DART バンドルをシスコのカスタマー サービスに送信する前に、プレーン テキスト バージョンの Web セキュリティ クライアント プロファイルを DART バンドルに追加します。

プレーン テキストの Web セキュリティ クライアント プロファイル ファイルの編集および ASDM からのインポート

プレーン テキストの Web セキュリティ クライアント プロファイル ファイルをエクスポートした場合は、ローカル コンピュータで、AnyConnect Web セキュリティ プロファイル エディタでサポートされていない編集が可能ないずれかのプレーン テキストまたは XML エディタを使用して編集します。プレーン テキスト バージョンの Web セキュリティ クライアント プロファイルは、カスタマーサポートから指示された場合以外は変更しないでください。エディタをインポートするには、次の手順を実行します。

始める前に

ファイルをインポートすると、選択した Web セキュリティ クライアント プロファイルの内容は上書きされます。

手順

ステップ 1 ASDM で、**[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [AnyConnect クライアント プロファイル（AnyConnect Client Profile）]** の順に選択します。

ステップ 2 編集する Web セキュリティ クライアント プロファイルを選択して [エクスポート（Export）] をクリックします。

ステップ 3 `filename.wsp` を変更した後で、[AnyConnect クライアント プロファイル（AnyConnect Client Profile）] ページに戻って、編集したファイルのプロファイル名を選択します。

ステップ 4 [インポート（Import）] をクリックします。

ステップ 5 編集したバージョンの Web セキュリティ クライアント プロファイルを参照して、[インポート（Import）] をクリックします。

難解化 Web セキュリティ クライアント プロファイル ファイルのエクスポート

手順

ステップ 1 ASDM を開き、**[ツール（Tools）] > [ファイル管理（File Management）]** を選択します。

ステップ 2 [ファイル管理（File Management）] 画面で、**[ファイル転送（File Transfer）] > [ローカル PC とフラッシュ間（Between Local PC and Flash）]** をクリックして、[ファイル転送（File Transfer）] ダイアログを使用して難解化 `filename.wso` クライアント プロファイル ファイルをローカル コンピュータに転送します。

Web セキュリティのためのスプリット トンネル除外の設定

ユーザが VPN セッションを確立した場合は、すべてのネットワーク トラフィックが VPN トンネル経由で送信されます。ただし、AnyConnect ユーザが Web セキュリティを使用している場合、エンドポイントで発信された HTTP トラフィックはトンネルから除外され、クラウド Web セキュリティ スキャニング プロキシに直接送信される必要があります。

クラウド Web セキュリティ スキャニング プロキシ用のトラフィックのスプリット トンネル除外を設定するには、グループ ポリシーで [Web セキュリティのためのスプリット除外の設定（Set up split exclusion for Web Security）] ボタンを使用します。

始める前に

- AnyConnect クライアントで使用するように Web セキュリティを設定します。
- グループ ポリシーを作成して、Web セキュリティが設定された AnyConnect クライアントの接続プロファイルを割り当てます。

Secure Trusted Network Detection 機能を使用する場合に、Web セキュリティと VPN が同時にアクティブになるようにするには、HTTPS サーバが VPN トンネル経由で到達可能にならないようにネットワークを設定します。この方法では、ユーザが社内 LAN 上にいるときに限り、Web セキュリティ機能はバイパス モードになります。

手順

ステップ 1 ASDM で、**[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [グループ ポリシー（Group Policies）]** に移動します。

ステップ 2 グループ ポリシーを選択し、新しいグループ ポリシーの **[編集（Edit）]** または **[追加（Add）]** をクリックします。

ステップ 3 **[詳細（Advanced）]** > **[スプリット トンネリング（Split Tunneling）]** を選択します。

ステップ 4 [Web セキュリティのためのスプリット除外の設定（Set up split exclusion for Web Security）] をクリックします。

ステップ 5 Web セキュリティのスプリット除外に使用される新しいアクセス リストを入力するか、既存のアクセス リストを選択します。ASDM は、ネットワーク リストで使用するアクセス リストを設定します。

ステップ 6 新しいリストの場合は [アクセス リストの作成（Create Access List）] をクリックし、既存のリストの場合は [アクセス リストの更新（Update Access List）] をクリックします。

ステップ 7 [OK] をクリックします。

次のタスク

追加スキャニング プロキシを追加した場合は、この手順で作成した統合アクセス リストを新しい情報で更新します。

Cisco Cloud Web Security ホステッド プロファイルの使用

AnyConnect リリース 3.0.4 から、Web セキュリティ ホステッド クライアント プロファイルの Cisco ScanCenter ホステッド コンフィギュレーションにより、Web セキュリティ クライアントに新しい設定を提供できます。Web セキュリティを備えたデバイスは、クラウドから新しい Web セキュリティ ホステッド クライアント プロファイルをダウンロードできます（ホステッド コンフィギュレーション ファイルは Cisco ScanCenter サーバに格納されています）。

AnyConnect クライアントは、リソース サービスから AnyConnect バイナリにハードコード化されているホスト名を使用してコンフィギュレーション ファイルをダウンロードする必要があります。要求は hostedconfig.scansafe.net/（IP：46.155.41.2）に対して行われ、通信は TCP ポート 443 で暗号化されます。

ホスト設定で、AnyConnect Web セキュリティに TCP ポート 443（およびプレーン モードで展開している場合はポート 8080）からの CWS タワー/プロキシの入力 IP へのアクセスを許可します。AnyConnect Web セキュリティのタワー/プロキシの完全なリストは、『Cisco ScanCenter Administration Guide』の「**Prepare**」セクションに記載されています。クライアントは TCP ポート 80 で 80.254.145.118 にアクセスできる必要があります。このアクセスにより、プロキシ タワーのリストを取得し、最新に保ちます。Web セキュリティ モジュールは TCP ポート 80 で Verisign に接続するように設定する必要があります。この範囲では、クライアントは証明書失効を **TJ.symcb.com** 、**T1.symcb.com**、および **T2.symcb.com** でチェックします。

Web セキュリティ プロファイル エディタを使用してクライアント プロファイルを作成してから、クリア テキスト XML ファイルを Cisco ScanCenter サーバにアップロードします。この XML ファイルには、同じ会社、グループ、またはユーザ ライセンス キーが Cisco Cloud Web Security で定義されホストされたホスト設定と関連付けられている、有効なライセンス キーを

含める必要があります。クライアントは、ホステッド コンフィギュレーション サーバに適用されてから 8 時間以内に、新しいコンフィギュレーション ファイルを取得します。

ホステッド コンフィギュレーション機能では、ホステッド コンフィギュレーション（Cisco ScanCenter）サーバから新しいクライアント プロファイル ファイルを取得する際にライセンス キーが使用されます。新しいクライアント プロファイル ファイルがサーバ上に置かれたら、Web セキュリティを実装したデバイスは自動的にサーバをポーリングし、新しいクライアント プロファイルをダウンロードします。これには、既存の Web セキュリティ クライアント プロファイルにあるライセンスがホステッド サーバ上のクライアント プロファイルに関連付けられたライセンスと同じであることが条件となります。新しいクライアント プロファイルをダウンロードした場合、新しいクライアント プロファイル ファイルを使用可能にするまで Web セキュリティは同じファイルを再度ダウンロードしません。

ライセンス キーの詳細については、『*Cisco ScanCenter Administration Guide, Release 5.2*』を参照してください。

始める前に

- Web セキュリティ クライアント デバイスを、Cisco Cloud Web Security ライセンス キーを含む有効なクライアント プロファイルを使用してインストールします。
- Web セキュリティ エージェント サービスのリスタート オプションは、サービスを再開するために必要な権限を持つユーザのみが使用可能です。
- ACWS エージェントを実行するクライアント コンピュータは、信頼されたルート証明機関ストアの Thawte プライマリ ルート CA および Thawte SSL CA - G2 が必要です。

手順

ステップ 1 Web セキュリティ プロファイル エディタを使用して、Web セキュリティ デバイス用の新しいクライアント プロファイルを作成します。このクライアント プロファイルは、Cisco Cloud Web Security ライセンス キーを含んでいる必要があります。

ステップ 2 クライアント プロファイル ファイルをクリア テキストの XML ファイルとして保存します。このファイルを Cisco ScanCenter サーバにアップロードします。このファイルをアップロードしたら、新しいクライアント プロファイルを Web セキュリティ クライアントに対して使用可能にします。

ステップ 3 新しいクライアント プロファイルをアップロードし、会社の Cisco ScanCenter を介して適用します。ただし、ホステッド コンフィギュレーション機能が会社で有効になっている必要があります。ホステッド クライアント プロファイルはライセンスに関連付けられています。異なるライセンス（たとえば、異なるグループのライセンス キー）を使用している場合、各ライセンスに独自のクライアント プロファイルを関連付けることができます。ユーザに設定されているライセンスに応じて、異なるユーザに異なるクライアント プロファイルを適用できます。ライセンスごとにさまざまな設定を格納して、クライアントがダウンロードするデフォルト クライアント プロファイルを設定します。その後、クライアントは、Cisco ScanCenter のホステッド コンフィギュレーション エリアに格納されている他のリビジョンの設定の 1 つをデフォルトとして選択することで、そのクライアント プロファイルに切り替えることができます。1 つのラ

イセンスは、1つのクライアントプロファイルのみに関連付けられます。したがって、複数のリビジョンがライセンスに関連付けられている場合、デフォルトにできるのは1つだけです。

Cisco AnyConnect Web セキュリティ エージェントの無効化および有効化

次の手順を実行することで、Web トラフィックを代行受信する Cisco AnyConnect Web セキュリティ エージェントの機能を無効化および有効化できます。

Windows を使用したフィルタの無効化と有効化

手順

ステップ 1 コマンド プロンプト ウィンドウを開きます。

ステップ 2 **%PROGRAMFILES%\Cisco\Cisco AnyConnect Secure Mobility Client** フォルダに移動します。

ステップ 3 フィルタリングを有効または無効にします。

- フィルタリングを有効にするには、**acwebsecagent.exe -enablesvc** と入力します。
- フィルタリングを無効にするには、**acwebsecagent.exe -disablesvc -servicepassword** と入力します。

Mac OS X を使用したフィルタの無効化と有効化

サービス パスワードは、Web セキュリティ プロファイル エディタの [認証（Authentication）] パネルで設定します。

手順

ステップ 1 ターミナル アプリケーションを起動します。

ステップ 2 /opt/cisco/anyconnect/bin フォルダに移動します。

ステップ 3 フィルタリングを有効または無効にします。

- フィルタリングをオンにするには、**./acwebsecagent -enablesvc** と入力します。
- フィルタリングを無効にするには、**./acwebsecagent -disablesvc -servicepassword** と入力します。

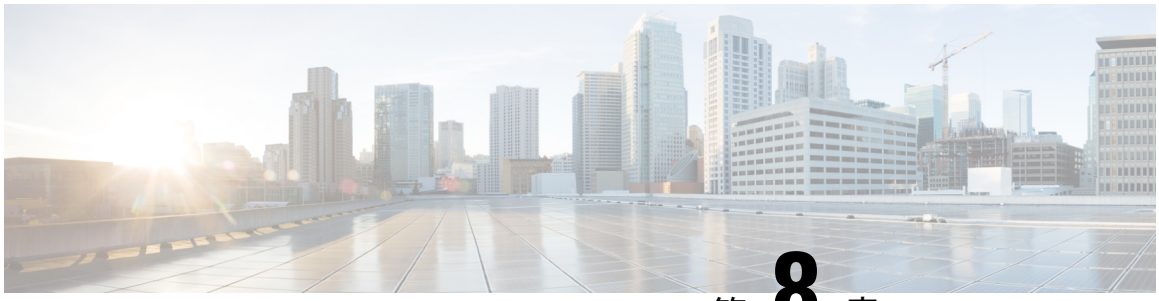
Web セキュリティ ロギング

Windows

すべての Web セキュリティ メッセージは、Windows イベント ビューアの `Event Viewer (Local)\Cisco AnyConect Web Security Module` フォルダに記録されます。Web セキュリティがイベント ビューアに記録するイベントは、Cisco Technical Assistance Center のエンジニアが分析します。

Mac OS X

Web セキュリティ メッセージは、syslog またはコンソールから表示します。



第 8 章

AMP イネーブラの設定

- AMP イネーブラについて （285 ページ）
- AMP イネーブラの導入 （285 ページ）
- AMP イネーブラ プロファイル エディタ （286 ページ）
- AMP イネーブラのステータス （287 ページ）

AMP イネーブラについて

AnyConnect AMP イネーブラは、エンドポイント向けの高度なマルウェア防御（AMP）を導入する手段として使用されます。社内でローカルにホストされているサーバからエンドポイントのサブセットにエンドポイント向け AMP ソフトウェアをプッシュし、既存のユーザ ベースに AMP サービスをインストールします。このアプローチでは、AnyConnect ユーザ ベース管理者が、追加のセキュリティ エージェントを使用できます。このエージェントは、ネットワークで発生する潜在的なマルウェア脅威を検出して排除し、企業を侵害から保護します。ダウンロードにかかる時間と帯域幅を節約し、ポータル側では変更を行う必要がなく、認証クレデンシャルをエンドポイントに送信せずに実行できます。

AMP イネーブラの導入

エンドポイント向け AMP ソフトウェアを適切に配布するには、次のワークフローに従う必要があります。

1. エンドポイント向け AMP ポータルにログインします。
2. エンドポイント向け AMP ポータルで適切なポリシーを設定します。設定したポリシーに応じて、適切なエンドポイント向け AMP ソフトウェア パッケージが作成されます。このソフトウェア パッケージは .exe ファイル（Windows 用）または .pkg ファイル（Mac 用）です。Windows では、再配布可能な .exe を選択できます。
3. 生成されたキット（Windows または Mac）をローカル サーバにダウンロードします。
4. AMP イネーブラ プロファイルを作成して保存するため、ASA または ISE ヘッドエンドにログインします。

（注） 特に ISE ポスチャを使用する場合は、1 つのヘッドエンド（ASA または ISE のいずれか）に対してのみプロファイルを設定することをお勧めします。

5. ASA または ISE ヘッドエンドで、オプション モジュールのリストから AMP Enable モジュールを選択し、AMP イネーブラ プロファイルを指定します。

   作成したプロファイルは、AnyConnect AMP イネーブラに使用されます。AMP イネーブラとこのプロファイルが ASA または ISE ヘッドエンドからエンドポイントにプッシュされます。

AMP イネーブラ プロファイル エディタ

管理者は、AMP イネーブラ プロファイルを作成して ASA にアップロードするために、このスタンドアロン エディタを使用することができます。それ以外の場合は、組み込みの AMP イネーブラ プロファイル エディタが[ポリシー要素（Policy Elements）] 下の ISE UI 内で、または ASDM 内で設定されます。信頼されているローカル Web サーバが AMP プロファイル エディタと連携できるようにするには、keytool コマンドを使用してルート CA 証明書を Java 証明書ストアにインポートする必要があります。

Windows：keytool -import -keystore [JAVA-HOME]/lib/security/cacerts -storepass changeit -trustcacerts -alias root -file [PATH_TO_THE_CERTIFICATE]/certnew.cer

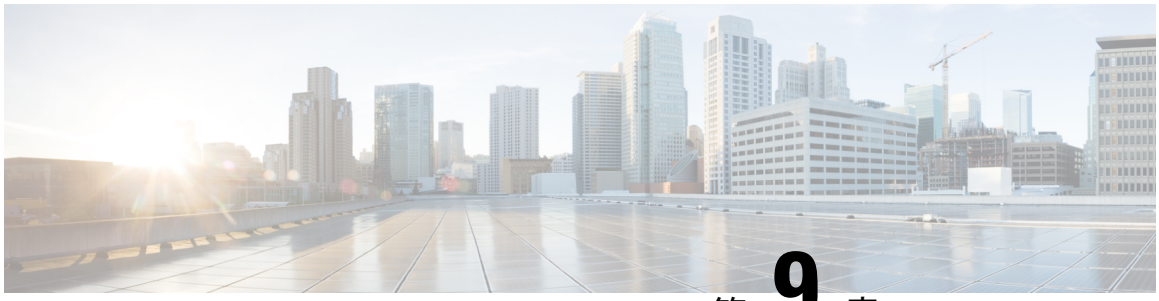
Mac：sudo keytool-import-keystore [JAVA-HOME]/lib/security/cacerts -storepass changeit -trustcacerts -alias root -file [PATH_TO_THE_CERTIFICATE]/certnew.cer

- Name
- Description
- [エンドポイント向けAMPのインストール（Install AMP for Endpoints）]：エンドポイント向け AMP をインストールするためにこのプロファイルを設定する場合に選択します。
- [エンドポイント向けAMPのアンインストール（Uninstall AMP for Endpoints）]：エンドポイント向け AMP をアンインストールするためにこのプロファイルを設定する場合に選択します。アンインストールを選択した場合、その他のフィールドに入力する必要はありません。
- [Windowsインストーラ（Windows Installer）]：.exe ファイルが存在するローカル ホスティング サーバのアドレスまたは URL を入力します。
- [Macインストーラ（Mac Installer）]：.pkg ファイルが存在するローカル ホスティング サーバのアドレスまたは URL を入力します。
- [チェック（Check）]：URL をチェックしてこの URL が有効であることを確認する場合にクリックします。有効な URL とは、到達可能であり信頼できる証明書が含まれている URL です。サーバが到達可能であり、この URL で接続が確立されたら、プロファイルを保存できます。
- [スタートメニューに追加（Add to Start Menu）]：[スタート（Start）] メニューにショートカットを作成します。

- [デスクトップに追加（Add to Desktop）]：デスクトップ アイコンを作成します。
- [コンテキストメニューに追加（Add to Context Menu）]：このオプションを選択すると、ファイルやフォルダを右クリックし、[今すぐスキャン（Scan Now）]を選択してスキャンを実行できるようになります。

AMP イネーブラのステータス

AMP の実際のダウンロードとインストールに関連するメッセージはすべて、AnyConnect UI の [AMP イネーブラ（AMP Enabler）] タイルに部分的なタイルとして表示されます。インストール完了後、すべての AMP 関連メッセージは エンドポイント向け AMP UI に表示されます。たとえば、マルウェア対策防御のインストール時またはアンインストール時にメッセージがユーザに対して表示され、失敗が示されるか、または再起動が必要なことが示されます。



第 9 章

ネットワーク可視性モジュール

- ネットワーク可視性モジュールについて （289 ページ）
- NVM の使用方法 （291 ページ）
- NVM プロファイル エディタ （292 ページ）
- NVM のコレクション パラメータ （295 ページ）
- カスタマー フィードバック モジュールによる NVM ステータスの提供 （298 ページ）

ネットワーク可視性モジュールについて

ユーザが管理対象外デバイスを使用する状況が増加しているため、企業内管理者はネットワーク内外の状況を把握しにくくなっています。ネットワークの可視性モジュール（NVM）は、オンプレミスまたはオフプレミスのエンドポイントから豊富なフローコンテキストを収集するもので、Stealthwatch などのシスコ ソリューションまたは Splunk などのサードパーティ ソリューションと併用すると、ネットワークに接続されたデバイスおよびユーザの動作に対する可視性を提供します。これにより、企業内管理者は、キャパシティとサービスの計画、監査、コンプライアンス、およびセキュリティ分析を実行することができます。NVM は次のサービスを提供します。

- ネットワーク設計を情報に基づいてより適切に改善する（VzFlow プロトコル仕様の IPFIX コレクタ要素の拡張）ために、アプリケーションの使用状況をモニタする。
- アプリケーション、ユーザ、またはエンドポイントを論理グループに分類する。
- 企業の資産を追跡し、移行アクティビティを計画するため、潜在的な異常を洗い出す。

この機能により、インフラストラクチャ導入環境全体ではなく、テレメトリを対象とするかどうかを選択できます。NVM は、次の情報に対するより正確な可視性を得るため、エンドポイント テレメトリを収集します。

- デバイス：エンドポイント（場所に関係なく）
- ユーザ：エンドポイントにログインしているユーザ
- アプリケーション：トラフィックを生成するアプリケーション
- 場所：トラフィックが生成されるネットワークの場所

• 宛先：このトラフィックの宛先の実際の FQDN

信頼ネットワークでは、AnyConnect NVM はフロー レコードをコレクタ（Cisco Stealthwatch、または LiveAction などのサードパーティ ベンダー）にエクスポートし、このコレクタがファイル分析を実行し、UI インターフェイスを提供します。フロー レコードはユーザの機能に関する情報を提供するもので、値は ID（たとえば、LoggedInUserAccountType は 12361、ProcessUserAccountType は 12362、ParentProcessUserAccountType は 12363）とともにエクスポートされます。Splunk などのサードパーティ ベンダーも、レポートを表示するための UI インターフェイスを提供します。ほとんどの企業内 IT 管理者は、データを使用して独自の可視化テンプレートを作成することを望むため、シスコは Splunk アプリケーション プラグインを介していくつかのサンプル ベース テンプレートを提供しています。

デスクトップ AnyConnect での NVM

従来、フロー コレクタにはスイッチまたはルータのインターフェイスに入る時点またはインターフェイスから出る時点で IP ネットワーク トラフィックを収集できる機能がありました。ネットワーク内の輻輳の原因とフローパスを特定できましたが、それ以外は特定できませんでした。エンドポイントで NVM を使用すると、デバイスのタイプ、ユーザ、アプリケーションなどの豊富なエンドポイント コンテキストによってフローが拡張されます。これにより、収集プラットフォームの機能に応じてフロー レコードがより実用的になります。IPFIX 経由で NVM によって提供されるエクスポート データは、Cisco NetFlow コレクタだけでなく、Splunk、IBM Qradar、LiveAction などの他のサードパーティ フロー収集プラットフォームと互換性があります。追加情報については、各プラットフォームの統合ドキュメントを参照してください。たとえば、Splunk 統合については、https://www.cisco.com/c/en/us/support/docs/security/anyconnect-secure-mobility-client/200600-Install-and-Configure-Cisco-Network-Visi.html で確認できます。

ネットワーク可視性モジュールのインストールを選択すると、AnyConnect Secure Mobility Client UI の [バージョン情報（About）] 画面に、このモジュールがインストール済みとしてリストされます。NVM の実行中、AnyConnect UI に他の表示はありません。

NVM の AnyConnect プロファイルは、ISE または ASA ヘッドエンドからプッシュされます（この機能が有効な場合）。ISE ヘッドエンドでは、スタンドアロン プロファイル エディタを使用し、NVM サービス プロファイル XML を生成して ISE にアップロードし、新しい NVM モジュールに対してマップできます。これは、Web セキュリティ、ネットワーク アクセス マネージャなどでの操作と同様です。ASA ヘッドエンドでは、スタンドアロン プロファイル エディタまたは ASDM プロファイル エディタのいずれかを使用できます。

VPN の状態が接続済みに変更した時点と、エンドポイントが信頼ネットワーク内にある場合に、NVM に通知が送信されます。

（注） NVM を Linux で使用する場合は、必ず、Linux 上での NVM の使用 （8 ページ）に記載されている準備手順を事前に完了してください。

モバイル AnyConnect での NVM

ネットワーク可視性モジュール（NVM）は、Google Play ストアで入手可能な Android 用の Cisco AnyConnect セキュア モビリティ クライアントの最新バージョン（リリース 4.0.09xxx）に含まれています。NVM は、Samsung Knox バージョン 2.8 以降を実行している Samsung のデバイスでサポートされています。その他のモバイル デバイスは、現在サポートされていません。モバイル NVM の詳細については、『*Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 4.0*』の「*AnyConnect on Mobile Devices*」の章に記載の手順、「*Configure NVM for Mobile*」を参照してください。

Android のネットワーク可視性は、サービス プロファイル設定の一部です。Android 上で NVM を設定するためには、AnyConnect NVM プロファイル エディタによって AnyConnect NVM プロファイルが生成され、モバイル デバイス マネジメント（MDM）を使用して Samsung のモバイル デバイスにプッシュされます。NVM をモバイル デバイス用に設定するには、AnyConnect リリース 4.4.3 以降の AnyConnect NVM プロファイル エディタが必要です。

ガイドライン

- NVM は、Samsung Knox バージョン 3.0 以降を実行している Samsung のデバイスでサポートされています。その他のモバイル デバイスは、現在サポートされていません。
- モバイル デバイスでは、コレクタへの接続は、IPv4 または IPv6 でサポートされています。
- Java ベースのアプリケーションでのデータ収集トラフィックはサポートされています。

NVM の使用方法

NVM は、次のシナリオで使用できます。

- セキュリティ インシデントの発生後、漏洩がなかったか確認するため、ユーザのネットワーク履歴を監査する。
- システムまたは管理者権限が、ユーザのマシンで実行されているネットワーク接続プロセスにどのように影響しているか確認する。
- レガシー OS を実行しているすべてのデバイスの一覧を取得する。
- ネットワーク内のどのアプリケーションが最も多くのネットワーク帯域幅を使用しているか確認する。
- ネットワーク内で何種類のバージョンの Firefox が使用されているか確認する。
- ネットワーク内で Chrome.exe 接続の何パーセントを IPv6 が占めているか確認する。

NVM プロファイル エディタ

プロファイル エディタで、コレクション サーバの IP アドレスまたは FQDN を設定します。送信するデータのタイプや、データ匿名化の有効/無効を選択することで、データ収集ポリシーをカスタマイズすることもできます。

ネットワーク可視性モジュールは、OS で優先される IP アドレスに対して、IPv4 アドレスのシングル スタック IPv4、IPv6 アドレスのシングル スタック IPv6、またはデュアル スタック IPv4/IPv6 で接続を確立できます。

モバイル ネットワーク可視性モジュールは、IPv4 を使用してのみ接続を確立できます。IPv6 接続はサポートされていません。

（注） ネットワーク可視性モジュールがフロー情報を送信するのは、信頼できるネットワーク上に限られます。デフォルトでは、データは収集されません。データが収集されるのは、プロファイルでそのように設定されている場合のみです。エンドポイントが接続されている間は、データが継続して収集されます。非信頼ネットワーク上で収集が行われた場合、データはキャッシュされ、エンドポイントが信頼ネットワーク上に接続された際に送信されます。

TND が NVM プロファイルに設定されている場合、信頼ネットワーク検出は NVM によって実行され、エンドポイントが信頼ネットワーク内にあるかどうかの判断は VPN に依存しません。ただし、TND が NVM プロファイルに明示的に設定されていない場合、NVM は VPN の TND 機能を使用してエンドポイントが信頼ネットワーク内にあるかどうかを判断します。また、VPN 接続状態にある場合、エンドポイントは信頼ネットワークにあると見なされ、フロー情報が送信されます。NVM に固有のシステム ログに TND の使用状況が表示されます。TND パラメータの設定については、AnyConnect プロファイル エディタ、プリファレンス（Part 2）（101 ページ）を参照してください。

- [デスクトップ（Desktop）] または [モバイル（Mobile）]：NVM をデスクトップとモバイル デバイスのどちらにセットアップするかを決定します。[デスクトップ（Desktop）] がデフォルトです。 モバイルは、将来的にサポートされます。
- **コレクタの設定**
  - [IP アドレス/FQDN（IP Address/FQDN）]：コレクタの IPv4 または IPv6 の IP アドレス/FQDN を指定します。
  - [IP アドレス/FQDN（IP Address/FQDN）]：コレクタの IPv4 の IP アドレス/FQDN を指定します。
  - [ポート（Port）]：コレクタがリッスンするポート番号を指定します。
- **キャッシュの設定**
  - [最大サイズ（Max Size）]：データベースが到達できる最大サイズを指定します。以前はキャッシュ サイズに事前設定の制限がありましたが、プロファイル内で設定でき

るようになりました。キャッシュのデータは暗号化された形式で保存され、ルート権限のプロセスのみがデータを復号化できます。

サイズ制限に到達すると、最新データの代わりに最も古いデータがスペースからドロップされます。

- [最高期間（Max Duration）]：データを保存する日数を入力します。最大サイズも設定している場合は、最初に到達した制限が優先されます。

  日数制限に到達すると、最新の日付のデータの代わりに最も古い日付のデータがスペースからドロップされます。[最高期間（Max Duration）] のみを設定している場合は、サイズ制限がありません。どちらも無効にしている場合は、サイズが 50 MB に制限されます。

- [定期的なフロー レポート（Periodic Flow Reporting）]（任意、デスクトップのみに該当）：クリックすると、フロー レポートが定期送信されます。デフォルトで、NVM は接続終了時にフローに関する情報を送信します（このオプションが無効のとき）。フローを閉じる前にフローに関する情報が定期的に必要な場合は、間隔を秒単位で設定します。値 0 は各フローの開始時と終了時にフロー情報が送信されることを意味します。値が *n* の場合、フロー情報は各フローの開始時、 *n* 秒ごと、および終了時に送信されます。長時間の接続を、フローが閉じられるまで待つことなく追跡するためには、この設定を使用します。

- [スロットル レート（Throttle Rate）]：スロットリングは、エンド ユーザへの影響が最小限になるように、キャッシュからコレクタにデータが送信されるレートを制御します。キャッシュされたデータがある限り、リアルタイム データとキャッシュされたデータの両方にスロットリングを適用できます。スロットル レートを Kbps 単位で入力します。デフォルト値は 500 Kbps です。

  キャッシュ データはこの一定期間後にエクスポートされます。この機能を無効にするには 0 を入力します。

- [収集モード（Collection Mode）]：エンドポイントのデータを収集する時点を指定するには、[収集モードがオフ（collection mode is off）]、[信頼ネットワークのみ（trusted network only）]、[信頼できないネットワークのみ（untrusted network only）]、または [すべてのネットワーク（all networks）] を選択します。

- [収集基準（Collection Criteria）]：データ収集期間に不要なブロードキャストを減らすことによって、関連データだけを分析できるようになります。次のオプションを使用して、データ収集を制御します。

  - [ブロードキャスト パケット（Broadcast packets）] および [マルチキャスト パケット（Multicast packets）]：デフォルトでは、効率性のため、バックエンド リソースにかかる時間が削減されるよう、ブロードキャスト パケットおよびマルチキャスト パケットの収集はオフになっています。ブロードキャスト パケットとマルチキャスト パケットの収集を有効にし、データをフィルタリングするには、チェックボックスをオンにします。

  - [KNOX のみ（KNOX only）]（任意、モバイルのみ）：オンにすると、KNOX ワークプレイスからのみデータが収集されます。デフォルトではこのフィールドはオフで、ワークプレイス外からもデータが収集されます。

- [データ収集ポリシー（Data Collection Policy）]：データ収集ポリシーを追加して、ネットワーク タイプまたは接続シナリオに関連付けできます。複数のインターフェイスを同時にアクティブにすることができるため、あるプロファイルを VPN トラフィックに適用し、別のプロファイルを非 VPN トラフィックに適用できます。

  [追加（Add）] をクリックすると、[データ収集ポリシー（Data Collection Policy）] ウィンドウが表示されます。ポリシーを作成するときに、次の点に留意してください。

  - ポリシーを作成していない場合、またはポリシーをネットワーク タイプに関連付けていない場合は、デフォルトでは、すべてのフィールドがレポートおよび収集されます。
  - それぞれのデータ コレクション ポリシーを少なくとも 1 つのネットワーク タイプに関連付ける必要がありますが、2 つのポリシーを同じネットワーク タイプに関連付けることはできません。
  - より具体的なネットワーク タイプを含むポリシーが優先されます。たとえば、VPN は信頼ネットワークに属しているため、VPN をネットワーク タイプとして含むポリシーはネットワーク タイプとして信頼が指定されたポリシーより優先されます。
  - 選択したコレクションモードに基づいて適用されるネットワークに対してのみデータ コレクション ポリシーを作成できます。たとえば、[収集モード（Collection Mode）] が[信頼ネットワークのみ（Trusted Network Only）] に設定されている場合、[非信頼（Untrusted）] の[ネットワーク タイプ（Network Type）] には、[データ収集ポリシー（Data Collection Policy）] を作成できません。
  - 以前の AnyConnect リリースのプロファイルがそれより後の AnyConnect リリース のプロファイルエディタで開かれた場合、プロファイルは、新しい方のリリースに自動的に変換されます。変換により、以前匿名化されていたフィールドを除外するデータ収集ポリシーが追加されます。
  - [名前（Name）]：作成するポリシーの名前を指定します。
  - [ネットワーク タイプ（Network Type）]：収集モードを指定するか、[VPN]、[信頼（trusted）]、または [非信頼（untrusted）] を選択してデータ収集ポリシーを適用するネットワークを指定します。信頼を選択した場合は、ポリシーが VPN ケースにも適用されます。
  - **[包含（Include）]/[除外（Exclude）]**
    - [タイプ（Type）]：データ収集ポリシーで [包含（Include）] または [除外（Exclude）] するフィールドを決定します。デフォルトは [除外（Exclude）] です。オンになっていないフィールドがすべて収集され、すべてのフィールドがオフにされます。
    - [フィールド（Fields）]：データ収集ポリシーの一部とするフィールドを決定します。 ネットワーク タイプと包含または除外するフィールドに基づいて、NVM はエンドポイント上で該当するデータを収集します。

      詳細については、NVM のコレクション パラメータ （295 ページ）を参照してください。

AnyConnect リリース 4.4（およびそれ以降）では、インターフェイスの状態と SSID を選択できるようになりました。これによりインターフェイスのネットワーク状態を信頼する/信頼しないを指定します。

- [任意の匿名化フィールド（Optional Anonymization Fields）]：同一のエンドポイントからのレコードをプライバシーを維持しつつ関連付ける場合は、該当するフィールドを匿名化対象に選択します。これにより、フィールド情報は実際の値ではなく値のハッシュとして送信されます。匿名化ではフィールドのサブセットが利用できます。

  包含/除外指定のフィールドは匿名化できません。同様に、匿名化と指定したフィールドは包含/除外できません。

- [利用規定（Acceptable Use Policy）]（任意、モバイルのみ）：[編集（Edit）] をクリックして、ダイアログ ボックス上でモバイル デバイス用の利用規定を定義します。終了したら、[OK] をクリックします。最大 4000 文字を使用できます。

  このメッセージは、NVM が設定されると、ユーザに対して表示されるようになります。リモート ユーザは、NVM アクティビティの拒否を選択できません。ネットワーク管理者は、MDM 機能を使用して NVM を制御します。

プロファイルを `NVM_ServiceProfile.xml` として保存します。この名前でプロファイルを保存する必要があります。そうしないと、NVM はデータの収集と送信に失敗します。

NVM のコレクション パラメータ

エンドポイントで収集され、コレクタにエクスポートされるパラメータを次に示します。

表 *9*: エンドポイント アイデンティティ

パラメータ	説明/注意事項
[仮想ステーション名（Virtual Station Name）]	Android の場合、Samsung による提供がないため、空。
[UDID]	汎用一意識別子。各フローに対応するエンドポイントを一意に識別します。この UDID 値は、デスクトップの HostScan およびモバイルの ACIDex でも報告されます。
[OS 名（OS Name）]	
[OS のバージョン（OS Version）]	
[SystemManufacturer]	

パラメータ	説明/注意事項
[システム タイプ（System Type）]	Android の場合、arm に設定。 それ以外のプラットフォームの場合、x86 または x64。
[OS のエディション（OS Edition）]	

表 *10 :* インターフェイス情報

パラメータ	説明/注意事項
[エンドポイント UDID（Endpoint UDID）]	UDID と同じ。
[インターフェイス UID（Interface UID）]	
[インターフェイス インデックス（Interface Index）]	
[インターフェイス タイプ（Interface Type）]	
[インターフェイス名（Interface Name）]	
[インターフェイス詳細リスト（Interface Details List）]	状態および SSID、InterfaceDetailsList の属性。インターフェイスのネットワークの状態（信頼または非信頼）と、当該の接続の SSID を示す。
[インターフェイス MAC アドレス（Interface MAC address）]	Windows および Mac OS のみ Android の場合、サポートされていないため、空。

表 *11 :* フロー情報

プロトコル識別子	説明/注意事項
[送信元 IPv4 アドレス（Source IPv4 Add）]	
[宛先 IPv4 アドレス（Destination IPv4 Addr）]	
[送信元転送ポート（Source Transport Port）]	
[宛先転送ポート（Source Transport Port）]	

プロトコル識別子	説明/注意事項
[送信元 IPv6 アドレス（Source IPv6 Addr）]	Android の場合、サポートされていないため、空。
[宛先 IPv6 アドレス（Destination IPv6 Addr）]	Android の場合、サポートされていないため、空。
[開始時刻（秒）（Start Sec）] [終了時刻（秒）（End Sec）]	フローの開始または終了を示す絶対的なタイムスタンプ。
[フロー UDID（Flow UDID）]	UDID と同じ。
[ログイン ユーザ（Logged In User）]	Android の場合、サポートされていないため、空。
[ログイン ユーザのアカウント タイプ（Logged In User Account Type）]	Windows および Mac OS のみ。 Android の場合、サポートされていないため、空。
[プロセス アカウント（Process Account）]	Android の場合、サポートされていないため、空。
[プロセス アカウントのタイプ（Process Account type）]	Windows および Mac OS のみ。 Android の場合、サポートされていないため、空。
[プロセス名（Process Name）]	
[プロセス ハッシュ（Process Hash）]	
[親プロセスのアカウント（Parent Process Account）]	Android の場合、サポートされていないため、空。
[親プロセスのアカウント タイプ（Parent Process Account Type）]	Windows および Mac OS のみ。 Android の場合、サポートされていないため、空。
[親プロセス名（Parent Process Name）]	
[親プロセス ハッシュ（Parent Process Hash）]	Android の場合、0 に設定。
[DNS サフィックス（DNS suffix）]	エンドポイント上のフローに関連付けられたインターフェイス上で設定。
[L4ByteCountIn]	
[L4ByteCountOut]	
[宛先ホスト名（Destination Hostname）]	エンドポイントの宛先 IP に解決される実際の FQDN

プロトコル識別子	説明/注意事項
[インターフェイス UID（Interface UID）]	
[モジュール名リスト（Module Name List）]	Android の場合、サポートされていないため、空。
[モジュールのハッシュ リスト（Module Hash List）]	Android の場合、サポートされていないため、空。

（注） また NVM は、エンドポイントのアイデンティティに関する情報を定期的に送信します。

カスタマーフィードバックモジュールによるNVMステータスの提供

カスタマー フィードバック モジュールのコレクションの一部は、NVM がインストールされているかどうか、1 日のフロー数、および DB サイズについてのデータを提供します。

第 10 章

Umbrella ローミング セキュリティ

Umbrella ローミング セキュリティ モジュールには、Professional、Insights、Platform、MSP のいずれかのパッケージでの Cisco Umbrella ローミング サービスのサブスクリプションが必要です。Cisco Umbrella ローミングはアクティブな VPN がないときに DNS レイヤ セキュリティを提供し、Cisco Umbrella サブスクリプションはネットワークがオンのときとオフのときの両方でインテリジェント プロキシと IP レイヤの適用機能を追加します。さらに、Cisco Umbrella サブスクリプションはコンテンツ フィルタリング、複数ポリシー、強力なレポート、Active Directory の統合などの機能を提供します。サブスクリプションに関係なく、同じ Umbrella ローミング セキュリティ モジュールが使用されます。

Umbrella ローミング モジュールのプロファイル（OrgInfo.json）は、各展開を対応するサービスに関連付け、対応する保護機能は自動的に有効化されます。

Umbrella ダッシュボードは、ローミング セキュリティ モジュールから発信されるすべてのインターネット アクティビティについてリアルタイムの可視性を提供します。ポリシーおよびレポートの精度のレベルは Umbrella サブスクリプションによって異なります。

サービス レベル サブスクリプションごとに含まれる機能の詳細な比較については、https://umbrella.cisco.com/products/packages を参照してください。

- Umbrella ローミング クライアントと Umbrella ローミング セキュリティ モジュールの非互換性 （300 ページ）
- Cisco Umbrella アカウントの取得 （300 ページ）
- ダッシュボードからの OrgInfo ファイルのダウンロード （300 ページ）
- Umbrella ローミング セキュリティの起動と実行 （301 ページ）
- OrgInfo.json ファイルの設定 （301 ページ）
- クラウド最新情報 （302 ページ）
- セキュリティ ポリシーの設定とレポートの確認 （303 ページ）
- エンドポイントに表示される UI の変更内容解説 （303 ページ）
- 診断の解釈 （309 ページ）

Umbrella ローミング クライアントと Umbrella ローミング セキュリティ モジュールの非互換性

Umbrella ローミング セキュリティ モジュールと Umbrella ローミング クライアントは互換性がありません。Umbrella ローミング セキュリティ モジュールを展開している場合は、ローミング セキュリティ モジュールのインストール中に Umbrella ローミング クライアントのすべての既存のインストールが検出され、競合を防ぐために自動的に削除されます。Umbrella ローミング クライアントの既存インストールを Umbrella サービス サブスクリプションに関連付けている場合は、OrgInfo.json ファイルを AnyConnect インストーラと同じ場所に配置して Umbrella モジュールのディレクトリで Web 展開または事前展開を設定していない限り、Umbrella ローミング セキュリティ モジュールに自動的に移行されます。Umbrella ローミング セキュリティ モジュールを展開する前に、手動で Umbrella ローミング クライアントをアンインストールすることもできます。

Cisco Umbrella アカウントの取得

Umbrella ダッシュボード（http://dashboard.umbrella.com/）は、展開に含める AnyConnect Umbrella ローミング セキュリティ モジュールのプロファイル（OrgInfo.json）を取得できるログイン ページです。このページでは、ローミング クライアントのアクティビティのポリシーとレポートを制御することもできます。

ダッシュボードからの OrgInfo ファイルのダウンロード

OrgInfo.json ファイルは、ローミング セキュリティ モジュールにレポートの送信先と適用するポリシーを知らせる、Umbrella ダッシュボード インスタンスについての詳細情報です。

Umbrella ローミング セキュリティ モジュールの導入準備を行うには、Umbrella ダッシュボード（https://dashboard.umbrella.com）から、OrgInfo.json ファイルを取得する必要があります。

[ID（Identities）] メニュー ストラクチャで [ローミング コンピュータ（Roaming Computers）] をクリックし、続いて、ページ左上隅の [+] 記号をクリックします。AnyConnect Umbrella ローミング セキュリティ モジュールまでスクロールし、[モジュール プロファイル（Module Profile）] をクリックします。特定のインストール/展開手順と特定のパッケージおよびファイルについては、AnyConnect 展開の概要 （2 ページ）を参照してください。

（注） OrgInfo.json ファイルを初めて展開すると、データ サブディレクトリ（/umbrella/data）にコピーされて、他のいくつかの登録ファイルも作成されます。したがって、OrgInfo.json 置換ファイルを展開する必要がある場合は、このデータ サブディレクトリを削除する必要があります。または、Umbrella ローミング セキュリティ モジュールをアンインストールし（データ サブディレクトリが削除されます）、新しい OrgInfo.json ファイルを再インストールすることもできます。

Umbrella ローミング セキュリティの起動と実行

AnyConnect を展開するとき、Umbrella ローミング セキュリティ モジュールは、追加機能を有効にするために含めることができるオプション モジュールの 1 つです。

（注） Umbrella ローミング セキュリティ モジュールと Web セキュリティ モジュールを展開している場合は、Web セキュリティとローミング セキュリティの互換性に必須のホスト例外（266 ページ）とWeb セキュリティと Umbrella ローミング セキュリティ モジュールの互換性に必須の静的な例外（267 ページ）を参照して静的な例外の除外とホスト例外を設定する必要があります。

Windows 7 SP1 ユーザは、インストールまたは初回使用前に、Microsoft .NET Framework 4.0 をインストールすることを推奨します。起動時に、Umbrella サービスは .NET Framework 4.0（または以上）がインストールされているかどうかを確認します。検出されない場合は、Umbrella ローミング セキュリティ モジュールはアクティブにならず、メッセージが表示されます。.NET Framework にアクセスし、これをインストールするには、再起動して Umbrella ローミング セキュリティ モジュールを有効にする必要があります。

OrgInfo.json ファイルの設定

OrgInfo.json ファイルには、Umbrella サービスのサブスクリプションについての固有の情報が格納されており、レポート先や適用するポリシーに関する情報をセキュリティ ローミング モジュールに通知します。OrgInfo.json ファイルを展開し、CLI または GUI を使用して ASA または ISE から Umbrella ローミング セキュリティ モジュールを有効にすることができます。次の手順では、最初に ASA から有効にする方法、次に ISE から有効にする方法を示します。

ASA CLI

1. Umbrella ダッシュボード（https://dashboard.umbrella.com）から ASA ファイル システムに取得した OrgInfo.json をアップロードします。
2. 設定に応じてグループ ポリシー名を適切に調整して、次のコマンドを実行します。

```
webvpn
 anyconnect profiles OrgInfo disk0:/OrgInfo.json
```

```
group-policy DfltGrpPolicy attribute
 webvpn
  anyconnect profiles value OrgInfo type umbrella
```

ASDM GUI

1. **[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [AnyConnect クライアント プロファイル（AnyConnect Client Profile）]** の順に移動します。
2. [追加（Add）] を選択します。
3. プロファイルの名前を入力します。
4. [プロファイルの使用（Profile Usage）] ドロップダウン メニューから Umbrella セキュリティ ローミング クライアント タイプを選択します。OrgInfo.json ファイルが、[プロファイルの場所（Profile Location）] フィールドに入力されます。
5. [アップロード（Upload）] をクリックして、ダッシュボードからダウンロードした OrgInfo.json ファイルの場所を参照します。
6. [グループ ポリシー（Group Policy）] ドロップダウン メニューで DfltGrpPolicy に関連付けます。グループ ポリシーで新しいモジュール名を指定するには、追加の AnyConnect モジュールの有効化 （31 ページ）を参照してください。

ISE

ISE からイネーブルにするには、以下の手順に従います。

1. Umbrella ダッシュボード（https://dashboard.umbrella.com）から OrgInfo.json をアップロードします。
2. ファイル OrgInfo.xml の名前を変更します。
3. AnyConnect を展開するための ISE の設定 （34 ページ）の手順に従います。

クラウド最新情報

Umbrella ローミング セキュリティ モジュールは、Umbrella クラウド インフラストラクチャからインストールされたすべての AnyConnect モジュールの自動更新を提供できます。クラウド更新では、ソフトウェア アップグレードは Umbrella クラウド インフラストラクチャから自動的に得られます。更新トラックは管理者のアクションではなくこれによって決まります。

デフォルトでは、クラウド更新からの自動更新は無効です。Umbrella ローミング セキュリティとその他の AnyConnect のクラウド更新を有効にするには、Umbrella ダッシュボードにログインします。**[ID（Identities）] > [ローミング コンピュータ（Roaming Computers）]** > 設定アイコン（歯車アイコン）の下で、[新しいバージョンがリリースされたら常に、VPN モジュールを含む AnyConnect を自動的に更新する（Automatically update AnyConnect, including VPN module, whenever new versions are released）] をオンにします。更新は VPN が有効である間は実行されません。デフォルトでは、このオプションは選択されていません。

クラウド更新に関して以下を検討してください。

- 現在インストールされているソフトウェア モジュールのみが更新されます。
- カスタマイズ、ローカリゼーション、およびその他の展開タイプはサポートされません。
- 更新は、デスクトップにログインしたときにのみ実行され、VPNが確立されているときは実行されません。
- 更新を無効にすると、最新のソフトウェア機能と更新を利用できません。
- クラウド更新を無効にしても、他の更新メカニズムや設定（Web展開、遅延更新など）には影響しません。
- クラウド更新は、AnyConnectのより新しいバージョンや未公開バージョン（暫定リリース、修繕公開されたバージョンなど）を持つデバイスを無視します。

セキュリティ ポリシーの設定とレポートの確認

保護を受信し、レポート情報を表示し、ポリシーを設定するには、Cisco Umbrella ローミング アカウントが必要です。詳細な説明については、https://docs.umbrella.com/product/umbrella/ または https://support.umbrella.com にアクセスして追加情報を参照してください。

インストール後 90 分から 2 時間以内に、ローミング コンピュータが Umbrella ダッシュボードに表示されます。https://dashboard.umbrella.com に移動して認証し、**[ID（Identities）] > [ローミング コンピュータ（Roaming Computers）]** の順にアクセスすると、ローミング クライアントのリスト（アクティブクライアントと非アクティブクライアントの両方）とインストールされている各クライアントの詳細が表示されます。

最初は、セキュリティ フィルタリングが基本レベルのデフォルトのポリシーがローミング コンピュータに適用されています。このデフォルトのポリシーは、ダッシュボードの [ポリシー（Policies）] セクション（または [設定（Configuration）] > [Cisco Umbrella アカウントのポリシー（Policy for Cisco Umbrella accounts）]）にあります。

ローミングクライアントのレポートは、[レポート（Reports）]セクションにあります。Umbrella ローミング セキュリティ モジュールがインストールされVPNがオフにされているコンピュータからのDNSトラフィックを確認するには、アクティビティ検索レポートをチェックします。

エンドポイントに表示されるUIの変更内容解説

AnyConnect UIでは、Umbrella ローミング セキュリティ モジュールのタイルに現在のステータスが表示されます。

状態	アイコンの色	説明	条件
予約済（Reserved）	オレンジ（Orange）	接続状況をチェック中です。Umbrella モジュールは保護状態をまだ確認していません。	この動作ステータスは次の条件で発生します。 • モジュールが最初にアクティブにされたとき。 • ネットワーク インターフェイスの変更（新しいネットワーク アダプタの検出、既存アダプタの IP の変更、新しい VPN トンネルの確立または中断）が発生したとき。
オープン（Open）	黄	現在、*Umbrella* によって保護されていません。Umbrella リゾルバとの接続の問題が原因で、ローカル Umbrella モジュールの DNS 保護がアクティブになっていません。少なくとも 1 つのアクティブなネットワーク接続が存在します。ただし、ローミング クライアントは、アクティブな接続の Umbrella サービスに接続できません。 システムの DNS 設定は元の設定（DHCP または固定）に戻ります。	この動作ステータスは次の条件で発生します。 • Umbrella リゾルバ（208.67.222.222）に UDP ポート 443 または UDP ポート 53 で接続していない。 • Umbrella DNS VA がローカル ネットワークで設定されていない。 • VPN トンネルが一時的に中断または確立状態になっている可能性がある。
保護済み（Protected）	グリーン	*Umbrella* によって保護されています。DNS クエリーが暗号化されていません。ローカル Umbrella モジュールの DNS 保護がアクティブで、DNS 要求は暗号化されずに Umbrella リゾルバに送信されます。	このステータスは、モジュールが最初にアクティブ化されたときか、ネットワーク インターフェイスの変更があるときに発生する可能性があります。

状態	アイコンの色	説明	条件
暗号化	グリーン	*Umbrella* によって保護されています。DNSクエリーが暗号化されています。ローカル Umbrella モジュールの DNS 保護がアクティブで、DNS 要求は暗号化されて Umbrella リゾルバに送信されます。	この動作ステータスは次の条件で発生します。 • Umbrella リゾルバ（209.67.222.222）に UDP ポート 443 で接続している。 • Umbrella リゾルバ（208.67.222.222）に TCP ポート 443 および TCP ポート 53 で接続している。
保護されたネットワーク（Protected Network）	グリーン	*Umbrella* によってネットワークが保護されています。現在のエンドポイント ネットワークが Umbrella リゾルバを使用して保護されているため、ローカル Umbrella モジュール DNS 保護はアクティブではありません。ローミング クライアントにより、DNS 設定が DHCP 経由または固定設定で設定されていた内容に戻されました。接続は暗号化されていません。	この動作ステータスは次の条件で発生します。 • 現在のエンドポイント ネットワーク出力 IP アドレスが、エンドポイントと同じ Umbrella アカウントに登録されている。 • 使用されるリゾルバが Umbrella クラウド リゾルバ（208.67.222.222、208.67.220.220）である。 • Umbrella ダッシュボード（[保護されたネットワークでは無効にする（Disable Behind Protected Networks）]）で設定されたポリシーで、保護されたネットワークでは Umbrella モジュールを無効にすることが指定されている。 （注） ネットワーク レベルの保護がないため、すべての Cisco Umbrella ローミング パッケージのお客様がこのステータスになることはありません。

状態	アイコンの色	説明	条件
仮想アプライアンスの背後（Behind Virtual Appliance）	グリーン	*Umbrella*仮想アプライアンスによって保護されています。Umbrella 仮想アプライアンスはオンプレミスの DNS リゾルバとして設定されているため、ローカル Umbrella モジュールの DNS 保護はアクティブではありません。ローミング クライアントは無効になり、DNS 設定が DHCP 経由または固定設定で設定されていた内容に戻されました。接続は暗号化されていません。	この動作ステータスは、エンドポイントで設定された DNS アドレス（DHCP 経由または固定）が Umbrella VA アドレスであるときに発生します。
Umbrella 信頼ネットワーク ステータス（Umbrella Trusted Network State）	グレー	信頼済みのネットワーク上では無効。現在のエンドポイント ネットワークが Umbrella 信頼ネットワークとして設定されているため、ローカル Umbrella モジュールの DNS 保護はアクティブではありません。	この動作ステータスは次の条件で発生します。 • Umbrella ダッシュボードがマジック ドメイン名で設定されている。 • 対応するマジック ドメイン名またはレコードがローカル DNS リゾルバで設定されている。

状態	アイコンの色	説明	条件
VPN 信頼ネットワーク ステータス（VPN Trusted Network State）	グレー	信頼済みのネットワーク上では無効。現在のエンドポイントネットワークが AnyConnect VPN 信頼ネットワークとして設定されているため、ローカル Umbrella モジュールの DNS 保護はアクティブではありません。	この動作ステータスは次の条件で発生します。 • AnyConnect VPN モジュールが信頼ネットワーク検出の状態を信頼できると報告している。 • AnyConnect VPN トンネルが接続されていないか、完全トンネルモードで確立されていない。 • Umbrella ダッシュボードで設定されたポリシーで、AnyConnect VPN 信頼ネットワークにあるときは Umbrella モジュールを無効にすると指定されている。 （注） この設定は、すべてのローミング パッケージのお客様に対して適用され、管理者が変更することはできません。

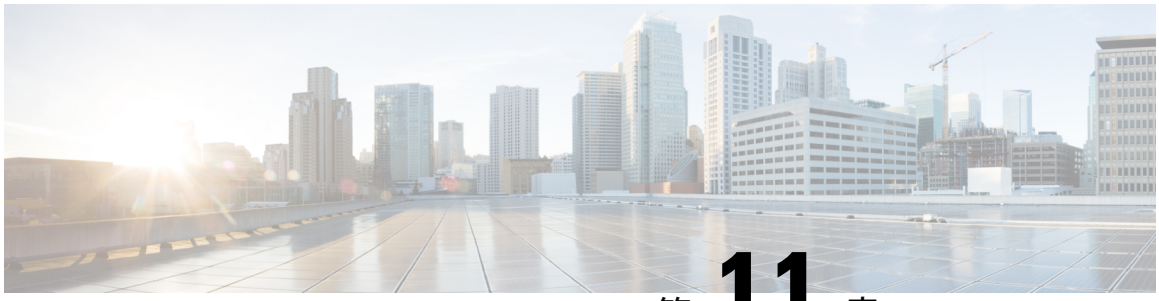
状態	アイコンの色	説明	条件
VPN 状態が原因で無効（Disabled Due to VPN State）	グレー	*VPN* がアクティブな間は無効。現在エンドポイントでアクティブな AnyConnect VPN トンネルが確立されているため、ローカル Umbrella モジュールの DNS 保護はアクティブではありません。	この動作ステータスは次の条件で発生します。 • AnyConnect VPN モジュールが信頼ネットワーク検出の状態を信頼できないと報告している。 • AnyConnect VPN トンネルが完全トンネル モードで確立されている。 • Umbrella ダッシュボードで設定されたポリシーで、AnyConnect VPN トンネルが確立されているときは Umbrella モジュールを無効にすると指定されている。 （注） この設定は、すべてのローミング パッケージのお客様に対して適用され、管理者が変更することはできません。
OrgInfo.json ステートなし（No OrgInfo.json State）	レッド	現在、*Umbrella* によって保護されていません。プロファイルが見つかりません。現在エンドポイントでアクティブな AnyConnect VPN トンネルが確立されているため、ローカル Umbrella モジュールの DNS 保護はアクティブではありません。	この動作ステータスは、OrgInfo.json ファイルが次の適切なディレクトリに配置されていない場合に発生します。 Windows：%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Umbrella macOS：opt/cisco/anyconnect/umbrella
エージェント利用不可ステート（Agent Unavailable State）	レッド	現在、*Umbrella* によって保護されていません。サービスは利用できません。Umbrella エージェントが実行されていないため、ローカル Umbrella モジュールの DNS 保護はアクティブではありません。	この動作ステータスは、Umbrella エージェント サービスが現在実行していないとき（クラッシュまたは手動によるサービス停止のため）に発生します。

状態	アイコンの色	説明	条件
.NET 依存ステータスが見つからない（Missing .NET Dependency State）（Windows のみ）	レッド	現在、*Umbrella* によって保護されていません。Microsoft 4.0 NET Framework がインストールされていません。ローカルの Umbrella モジュールの DNS 保護がアクティブではありません。Umbrella エージェントが実行されていないためです。.NET ランタイム フレームワークが見つかりません。	この動作ステータスは、.NET 4.0 ランタイムが見つからないために Umbrella エージェント サービスが実行していないときに発生します。

AnyConnect UI は、Umbrella ローミング セキュリティ モジュールの統計とメッセージ履歴を表示します。

診断の解釈

Cisco Umbrella ローミング セキュリティ モジュールの問題を診断するには、DART レポートを実行する必要があります。Umbrella の問題とトラブルシューティングの詳細については、docs.umbrella.com を参照してください。



第 11 章

ローカル ポリシーでの FIPS の有効化

- FIPS、NGE、および AnyConnect について （311 ページ）
- AnyConnect コア VPN クライアントのための FIPS の設定 （315 ページ）
- ネットワーク アクセス マネージャのための FIPS の設定 （316 ページ）

FIPS、NGE、および AnyConnect について

AnyConnect には、Cisco Common Cryptographic Module（C3M）が組み込まれています。この Cisco SSL の実装には、新世代の暗号化（NGE）アルゴリズムの一部として、連邦情報処理標準（FIPS）140-2 に準拠した暗号化モジュールや国家安全保障局（NSA）Suite B 暗号化が含まれます。

NGEには、増え続けるセキュリティおよびパフォーマンス要件のための新しい暗号化、認証、デジタル署名、キー交換アルゴリズムが導入されています。RFC 6279 では、Suite B 暗号化アルゴリズムが定義されています。これは、米国の FIPS 140-2 標準を満たします。

AnyConnect コンポーネントは、ヘッドエンド（ASA または IOS ルータ）の設定に基づいて FIPS 標準暗号化をネゴシエートして使用します。次の AnyConnect クライアント モジュールは FIPS をサポートしています。

- AnyConnect コア VPN：VPN クライアントの FIPS 準拠は、ユーザ コンピュータ上のローカル ポリシー ファイルの FIPS モード パラメータを使用して有効化されます。Suite B 暗号化は、TLS/DTLS および IKEv2/IPsec VPN 接続で使用可能です。詳細および手順については、「AnyConnect コア VPN クライアントのための FIPS の設定」を参照してください。

  AnyConnect ローカル ポリシー ファイル AnyConnectLocalPolicy.xml には、ローカル クライアントに適用される FIPS モードの他に追加のセキュリティ設定が含まれています。これは ASA によって展開されないため、手動でインストールするか、社内のソフトウェア展開システムを使用して展開する必要があります。このプロファイルの使用方法については、「AnyConnect ローカル ポリシー」を参照してください。

- AnyConnect ネットワーク アクセス マネージャ：ネットワーク アクセス マネージャの FIPS 準拠は、AnyConnectLocalPolicy.xml ファイルの FIPS モード パラメータ、およびネットワーク アクセス マネージャ プロファイルの FIPS モード パラメータを使用して有効にします。ネットワーク アクセス マネージャのための FIPS は Windows でサポートされています。

詳細および手順については、「ネットワーク アクセス マネージャのための FIPS の設定」を参照してください。

AnyConnect の FIPS 機能

機能	コア VPN モジュール	ネットワーク アクセス マネージャ モジュール
対称暗号化や完全性のための AES-GCM サポート。	IKEv2 ペイロード暗号化と認証用の 128、192、256 ビットの各キー。 ESP パケット暗号化および認証。	ソフトウェア（Windows）で有線トラフィック暗号化を実現する 802.1AE（MACsec）用 128 ビット キー。
ハッシュ用 SHA-2 サポート、256/384/512 ビットの SHA。	IKEv2 ペイロード認証および ESP パケット認証。（Windows 7 以降および macOS 10.7 以降）。	TLS ベースの EAP 方式で SHA-2 を使用して証明書を使用できる機能。
キー交換向けの ECDH サポート。	グループ 19、20、および 21 の IKEv2 キー交換および IKEv2 PFS。	TLS ベースの EAP 方式で ECDH を使用できる機能（Windows）。
デジタル署名、非対称暗号化、および認証の ECDSA サポート、256、384、521 ビット楕円曲線。	IKEv2 ユーザ認証およびサーバ証明書の確認。	TLS ベースの EAP 方式で ECDSA を使用して証明書を使用できる機能。
その他のサポート。	IPsecV3 に必須のすべての暗号アルゴリズムがヌル暗号化を想定しています。 IKEv2 用の Diffie-Hellman Groups 14 および 24。 TLS/DTLS および IKEv2 用の 4096 ビット キーを使用する RSA 証明書。	該当なし

[1] Linux では、AnyConnect ファイル ストアのみが ECDSA でサポートされます。ファイル ストアに証明書を追加するには、「Mac および Linux での PEM 証明書ストアの作成」を参照してください。

[2] IPsecV3 は、ESN（Extended Sequence Numbers）がサポートされなければならないことも明記していますが、AnyConnect は ESN をサポートしません。

AnyConnect FIPS の要件

- Suite B 暗号化は、TLS/DTLS および IKEv2/IPsec VPN 接続で使用可能です。
- FIPS または Suite B のサポートは、セキュア ゲートウェイで必要です。シスコは、ASA バージョン 9.0 以降では Suite B 機能、ASA バージョン 8.4.1 以降では FIPS 機能を提供します。
- ECDSA 証明書の要件は次のとおりです。
  - カーブ強度以上のダイジェスト強度がなければなりません。たとえば、EC-384 キーは SHA2-384 以上を使用しなければなりません。
  - Windows 7 以降、macOS 10.7 以降、Red Hat Enterprise Linux 6.x または 6.4（64 ビット）、Ubuntu 12.4 および 12.10（64 ビット）でサポートされています。ECDSA スマート カードは、Windows 7 （およびそれ以降のバージョン）でのみサポートされています。

AnyConnect FIPS の制限事項

SHA-2 を使用して署名された証明書を検証する際、EAP 方式は、TLS ベースの EAP を除き SHA-2 をサポートしません。

AnyConnect FIPS のガイドライン

- AnyConnect クライアントの [統計情報（Statistics）] パネル（[トランスポート情報（Transport Information）] ヘッダーの下）には、使用中の暗号名が表示されます。
- AES-GCM は、計算集約型のアルゴリズムであるため、これらのアルゴリズムを使用するときは、全体的なデータ レートが低くなる可能性があります。新しい Intel プロセッサの一部は、特に AES-GCM の性能を向上させるために採用された特別な命令を含むものもあります。AnyConnect は、それが実行されるプロセッサ上でそれらの新しい命令がサポートされているかどうかを自動的に検出します。サポートされている場合は、AnyConnect は新しい命令を使用し、特別な命令を持たないプロセッサと比較して VPN データ レートを大幅に向上させます。新しい命令をサポートするプロセッサのリストについては、http://ark.intel.com/Search/FeatureFilter?productType=processors&AESTech=true を参照してください。詳細については、http://software.intel.com/en-us/articles/intel-carry-less-multiplication-instruction-and-its-usage-for-computing-the-gcm-mode/ を参照してください。
- 暗号化と整合性の検証の両方が 1 回の操作で実行される複合モードの暗号化アルゴリズムは、ハードウェア クリプト アクセラレーションを使用する SMP ASA ゲートウェイ（5585 および 5515-X など）でのみサポートされます。AES-GCM は、シスコがサポートする複合モードの暗号化アルゴリズムです。

（注） IKEv2 ポリシーは、通常モードまたは複合モードの暗号化アルゴリズムのうちの 1 つを含めることができますが、両方は不可能です。複合モードのアルゴリズムが IKEv2 ポリシーで設定されると、通常モードのアルゴリズムすべてが無効になるので、唯一有効な整合性アルゴリズムは NULL です。

IKEv2 IPsec プロポーザルは別のモデルを使用し、同じプロポーザル内で標準モードと複合モードの両方の暗号化アルゴリズムを指定できます。この使用方法では、両方に整合性アルゴリズムを設定する必要があります。その結果、非NULL整合性アルゴリズムが AES-GCM 暗号化で設定されます。

- ASA が SSL および IPsec 用の異なるサーバ証明書で設定されている場合は、信頼できる証明書を使用してください。異なる IPsec および SSL 証明書を持つ Suite B（ECDSA）の信用されていない証明書を使用する場合、ポスチャ評価、WebLaunch、またはダウンローダの障害が発生する可能性があります。

AnyConnect FIPS のレジストリ変更によるエンドポイントに関する問題の回避

コア AnyConnect クライアントの FIPS を有効にすると、エンドポイントで Windows レジストリの設定が変更されます。エンドポイントの他のコンポーネントでは、AnyConnect が FIPS を有効にしたこと、および暗号化の使用を開始したことを検出できます。たとえば、Remote Desktop Protocol（RDP）では、サーバで FIPS 準拠の暗号化を使用している必要があるため、Microsoft Terminal Services クライアントの RDP は機能しません。

これらの問題を回避するために、パラメータ
[Use FIPS compliant algorithms for encryption, hashing, and signing] を Disabled に変更することにより、[Windows Local System Cryptography] 設定で FIPS 暗号化を一時的に無効にできます。エンドポイントデバイスをリブートすると、この設定が変更されて有効に戻ることに注意してください。

次の表に、認識の必要がある、AnyConnect によって実行される Windows レジストリ変更を示します。

レジストリ キー	変更内容
HKLM\System\CurrentControlSet\ Control\Lsa	FIPSAlgorithmPolicy が 0 から 1 に変更されます。
HKCU\Software\Microsoft\Windows\ CurrentVersion\Internet Settings	元の設定にビット単位で 0x080 の「or」を実行することにより、[SecureProtocols] 設定が TLSV1 に変更されます。

レジストリ キー	変更内容
HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet	元の設定にビット単位で 0x080 の「or」を実行することにより、[SecureProtocols] 設定が TLSV1 に変更されます。 これにより、1 つのグループ ポリシーに対する TLSv1 が設定されます。

AnyConnect コア VPN クライアントのための FIPS の設定

AnyConnect コア VPN のための FIPS の有効化

手順

ステップ 1 AnyConnect プロファイル エディタで、VPN ローカル ポリシー プロファイルを開くか、作成します。

ステップ 2 [FIPS モード（FIPS Mode）] を選択します。

ステップ 3 VPN ローカル ポリシー プロファイルを保存します。

FIPS が有効であることを示す名前をプロファイルに付けることをお勧めします。

Windows インストール時の FIPS の有効化

Windows インストールでは、Cisco MST ファイルを標準 MSI インストール ファイルに適用して、AnyConnect ローカル ポリシーで FIPS を有効にできます。この MST のダウンロード元の詳細については、FIPS 用に受け取ったライセンシング情報を参照してください。インストール時に、FIPS が有効にされた AnyConnect ローカル ポリシー ファイルが生成されます。このユーティリティを実行した後、ユーザのシステムを更新します。

（注） この MST は FIPS だけを有効にします。その他のパラメータは変更しません。Windows インストール中に他のローカル ポリシーの設定を変更するには、「MST ファイルでのローカル ポリシー パラメータの有効化」を参照してください。

ネットワーク アクセス マネージャのための FIPS の設定

ネットワーク アクセス マネージャは、FIPS ネットワークと非 FIPS ネットワークの両方に同時に接続したり、FIPS ネットワークだけに接続したりするように設定できます。

手順

ステップ 1 ネットワーク アクセス マネージャのための FIPS の有効化。

FIPS を有効にすると、ネットワーク アクセス マネージャは FIPS ネットワークと非 FIPS ネットワークの両方に接続できます。

ステップ 2 必要に応じて、ネットワーク アクセス マネージャに対する FIPS モードの適用。

FIPS モードを適用すると、ネットワーク アクセス マネージャの接続が FIPS ネットワークだけに制限されます。

ネットワーク アクセス マネージャのための FIPS の有効化

手順

ステップ 1 AnyConnect ローカル ポリシーで FIPS モードを有効にします。

a) AnyConnect プロファイル エディタで、VPN ローカル ポリシー プロファイルを開くか、作成します。
b) [FIPS モード（FIPS Mode）] を選択します。
c) VPN ローカル ポリシー プロファイルを保存します。

FIPS が有効であることを示す名前をプロファイルに付けることをお勧めします。

ステップ 2 AnyConnect ネットワーク アクセス マネージャ クライアント プロファイルで FIPS モードを有効にします。

a) AnyConnect プロファイル エディタで、ネットワーク アクセス マネージャ プロファイルを開くか、作成します。
b) [クライアント ポリシー（Client Policy）] 設定ウィンドウを選択します。
c) [管理ステータス（Administrative Status）] セクションで、[FIPS モード（FIPS Mode）] に [有効（Enable）] を選択します。
d) ネットワーク アクセス マネージャ プロファイルを保存します。

FIPS が有効であることを示す名前をプロファイルに付けることをお勧めします。

ネットワーク アクセス マネージャに対する FIPS モードの適用

ネットワーク アクセス マネージャ プロファイルで、許可する関連付け、暗号化モード、認証方式を制限することにより、企業の従業員に対して FIPS 準拠のネットワークのみへの接続を強制します。

まず、ネットワーク アクセス マネージャのための FIPS の有効化を行い、FIPS モードを適用します。

手順

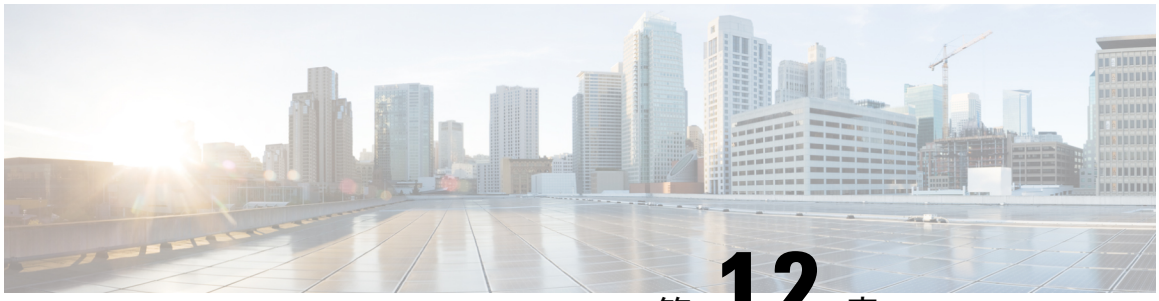
ステップ 1 AnyConnect プロファイル エディタでネットワーク アクセス マネージャ プロファイルを開きます。

ステップ 2 ネットワーク アクセス マネージャの FIPS 準拠では、WPA2 パーソナル（WPA2-PSK）、WPA2 エンタープライズ（802.1X）などの FIPS 認定の AES 暗号化モードをサポートしています。

ステップ 3 ネットワーク アクセス マネージャの FIPS サポートには、EAP 方式 EAP-TLS、EAP-TTLS、PEAP、EAP-FAST、および LEAP が含まれています。

ステップ 4 ネットワーク アクセス マネージャ プロファイルを保存します。

FIPS 接続だけが可能であることを示す名前をプロファイルに付けることをお勧めします。



第 12 章

Cisco AnyConnect カスタマー エクスペリエンス フィードバック モジュール

（注） デフォルトでは、プライベート データおよび企業データが収集されます。

カスタマー エクスペリエンス フィードバック（CEF）モジュールにより、カスタマーが使用し、有効にしたモジュールおよび機能の情報を取得できます。この情報によりユーザエクスペリエンスを把握できるため、シスコは AnyConnect の品質、信頼性、パフォーマンス、ユーザエクスペリエンスを継続して改善できます。

情報の収集および使用の詳細については、「Cisco Online Privacy Statement Highlights」ページからアクセスできる、「AnyConnect Secure Mobility Client Supplement」を参照してください。 すべてのデータは匿名で収集され、個人を特定できるデータは含まれません。また、データは安全に送信されます。

シスコは、次のタイプのデータを収集します。

- ユーザビリティ データ：詳細については、プライバシー ポリシーを参照してください。このデータは、毎月一度収集され送信されます。
- Web 脅威データ：脅威が報告されるたびに送信されます。
- クラッシュ レポート：AnyConnect が生成したクラッシュ ダンプ ファイルが 24 時間おきにチェックされ、収集され、カスタマー エクスペリエンス フィードバック サーバに送信されます。

カスタマー エクスペリエンス フィードバック モジュールの主なコンポーネントは次のとおりです。

- フィードバック モジュール：AnyConnect のソフトウェア コンポーネントで、情報を収集し定期的にサーバに送信します。
- Cisco フィードバック サーバ：カスタマー エクスペリエンス フィードバック データを収集し、未処理形式で一時的なストレージに保存する、シスコが所有するクラウドインフラストラクチャです。

• カスタマー エクスペリエンス フィードバックの設定 （320 ページ）

カスタマー エクスペリエンス フィードバックの設定

AnyConnect カスタマー エクスペリエンス フィードバック モジュールは AnyConnect とともに展開され、デフォルトで有効になっています。カスタマー エクスペリエンス フィードバック プロファイルを作成することで、エクスペリエンスフィードバックから完全に除外するなど、送信されるフィードバックの内容を変更できます。この方法は、フィードバック モジュールを無効にする場合に適した方法ですが、AnyConnect の展開中にフィードバック モジュールを完全に排除することもできます。

始める前に

カスタマー エクスペリエンス フィードバック モジュールは自動的に有効になります。

手順

ステップ 1 スタンドアロンのカスタマー エクスペリエンス フィードバック プロファイル エディタまたは ASDM を開きます。**[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [AnyConnect クライアント プロファイル（AnyConnect Client Profile）]** に移動します。

ステップ 2 [フィードバック サービス プロファイル（Feedback Service Profile）] のプロファイルの用途で AnyConnect クライアント プロファイルを作成します。

ステップ 3 フィードバックを提供しない場合は、[カスタマー エクスペリエンス フィードバック サービスの有効化（Enable customer Experience Feedback Service）] をオフにします。

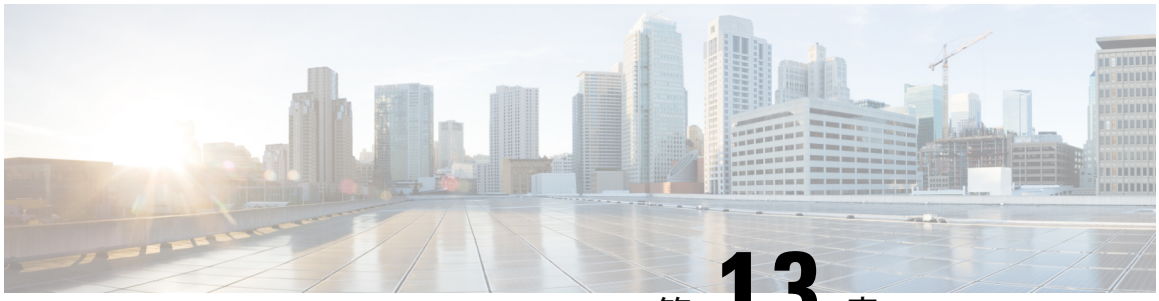
フィードバックは、インストール後にいつでも無効にできます。

ステップ 4 AnyConnect によって生成されたクラッシュ レポートを送信しない場合は、[クラッシュ レポートを含める（Include Crash Report）] をオフにします。

デフォルトでは、クラッシュ レポートが含まれます。

ステップ 5 任意のカスタマー キーまたはカスタマー ID を入力します。

この ID により、シスコはどの組織からの情報であるかを識別できます。



第 13 章

AnyConnect のトラブルシューティング

- トラブルシューティングに必要な情報の収集 （321 ページ）
- AnyConnect 接続または接続解除の問題 （325 ページ）
- VPN サービスの障害 （328 ページ）
- ドライバのクラッシュ （330 ページ）
- その他のクラッシュ （331 ページ）
- セキュリティの警告 （333 ページ）
- 接続のドロップ （334 ページ）
- インストールの失敗 （336 ページ）
- 非互換性の問題 （336 ページ）
- 既知のサードパーティ製アプリケーション競合 （338 ページ）

トラブルシューティングに必要な情報の収集

統計詳細情報の表示

管理者またはエンド ユーザは、現在の AnyConnect セッションの統計情報を表示できます。

手順

ステップ 1 Windows では、**[詳細ウィンドウ（Advanced Window）] > [統計情報（Statistics）] > [VPN ドロワ（VPN drawer）]** に移動します。Linux では、ユーザ GUI 上の [詳細（Details）] ボタンをクリックします。

ステップ 2 クライアント コンピュータにロードされたパッケージに応じて、次のオプションから選択します。

- [統計情報のエクスポート（Export Stats）]：後で分析およびデバッグできるようにテキスト ファイルに接続統計情報を保存します。
- [リセット（Reset）]：接続情報を 0 にリセットします。 AnyConnect による新しいデータの収集がすぐに開始されます。

- [診断（Diagnostics）]：AnyConnect Diagnostics and Reporting Tool（DART）ウィザードを起動します。ウィザードは、クライアント接続を分析およびデバッグできるように、指定されたログ ファイルと診断情報をバンドルします。

トラブルシューティング用にデータを収集するための DART の実行

DART は AnyConnect Diagnostics and Reporting Tool の略で、AnyConnect のインストールと接続に関する問題のトラブルシューティング用データの収集に使用できます。DART によってログ、ステータス、および診断情報が収集され、それを Cisco Technical Assistance Center（TAC）での分析に使用できます。

DART ウィザードは、AnyConnect を実行するデバイス上で実行されます。DART は AnyConnect から起動できます。または AnyConnect を使用せずにそれ自体を起動できます。

次のオペレーティング システムがサポートされています。

- Windows
- macOS
- Linux

手順

ステップ 1 DART を起動します。

- Windows デバイスの場合は、Cisco AnyConnect Secure Mobility Client を起動します。
- Linux デバイスの場合は、**[アプリケーション（Applications）] > [インターネット（Internet）] > [Cisco DART]** を選択します。

  または /opt/cisco/anyconnect/dart/dartui を選択します。
- Mac デバイスの場合、**[アプリケーション（Applications）] > [Cisco] > [Cisco DART]** を選択します。

ステップ 2 [統計情報（Statistics）] タブをクリックし、次に [診断（Diagnostics）] をクリックします。

ステップ 3 [デフォルト（Default）] または [カスタム（Custom）] のバンドル作成を選択します。

- [デフォルト（Default）]：AnyConnect ログ ファイル、コンピュータに関する一般情報、および DART ツールが実行した内容と実行しなかった内容の概要などの一般的なログ ファイルと診断情報を含みます。バンドルのデフォルト名は `DARTBundle.zip` であり、このバンドルはローカル デスクトップに保存されます。
- [カスタム（Custom）]：バンドルに含めるファイル（またはデフォルト ファイル）、およびバンドルの保存場所を指定できます。

Linux および macOS での成功したルートおよびフィルタリングの変更がログから除外されるようになり、重要なイベントに注意しやすくなります。そうでない場合、syslog のイベント レートの制限により、重要なイベントがドロップして見落とされる可能性があります。また、キャプチャ フィルタリング設定を使用すると、AnyConnect のフィルタリング設定ファイルだけでなく、Mac のシステム PF 設定ファイルも表示できるようになります。Linux の場合、これらの設定のほとんどは DART ツールが sudo を介して実行されている場合以外アクセスが制限されているにもかかわらず、iptables および ip6tables の出力が DART に表示されます。

（注） macOS のオプションは、[デフォルト（Default）] のみです。バンドルに含めるファイルは、カスタマイズできません。

（注） [カスタム（Custom）] を選択すると、バンドルに含めるファイルを指定でき、また、ファイルに対して異なる保存場所を指定できます。

ステップ 4 DART がデフォルト リストのファイル収集に時間がかかっていると思われる場合は、[キャンセル（Cancel）] をクリックし、DART を再実行して、[カスタム（Custom）] を選択して含めるファイルを減らします。

ステップ 5 [デフォルト（Default）] を選択すると、DART はバンドルの作成を開始します。[カスタム（Custom）] を選択した場合、ウィザードのプロンプトに従って、ログ、プリファレンス ファイル、診断情報、およびその他のカスタマイズを指定します。

インストールまたはアンインストールの問題についてデータを収集するためのログの収集（Windows）

AnyConnect のインストールまたはアンインストールに失敗した場合は、DART コレクションはこの状況を診断しないため、ログを収集する必要があります。

AnyConnect ファイルを解凍したのと同じディレクトリで、msiexec コマンドを実行します。

- インストールに失敗した場合は、次のように入力します。

```
C:/temp>msiexec /i anyconnect-win-version-pre-deploy-k9.msi /lvx
c:/Temp/ac-install.log?
```

ここで *c:/temp/ac-install.log?* は、任意のファイル名にすることができます。

- アンインストールに失敗した場合は、次のように入力します。

```
c:/temp/msiexec /x anyconnect-win-version-pre-deploy-k9.msi /lvx
c:/Temp/ac-install.log?
```

ここで *c:/temp/ac-uninstall.log?* は、選択したファイル名にすることができます。

（注） アンインストールに失敗した場合は、現在インストールされているバージョン固有の MSI を使用する必要があります。

上記と同じコマンドを変更して、正しくインストールまたはアンインストールされなかった Windows のすべてのモジュールに関する情報をキャプチャすることもできます。

コンピュータ システム情報の取得

Windows の場合は、**msinfo32 /nfo c:\msinfo.nfo** と入力します。

systeminfo ファイル ダンプの取得

Windows の場合は、sysinfo コマンド プロンプトで **c:\sysinfo.txt** と入力します。

レジストリ ファイルの確認

次の SetupAPI ログ ファイル内のエントリは、ファイルが見つからないことを示しています。

```
E122 Device install failed. Error 2: The system cannot find the file specified.
E154 Class installer failed. Error 2: The system cannot fine the file specified.
```

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce レジストリ キーが存在することを確認してください。このレジストリ キーが存在しない場合、すべての inf インストール パッケージが禁止されます。

AnyConnect ログ ファイルの場所

ログは、次のファイル内に保持されます。

Windows：`\Windows\Inf\setupapi.app.log` または `\Windows\Inf\setupapi.dev.log`

- Windows：`\Windows\Inf\setupapi.app.log` または `\Windows\Inf\setupapi.dev.log`

（注） Windows では、隠しファイルを表示する必要があります。

これが新規の Web 展開インストールの場合、このログ ファイルは次のユーザ別の temp ディレクトリに格納されます。

`%TEMP%\anyconnect-win-4.X.xxxxx-k9-install-yyyyyyyyyyyyyy.log`。

アップグレードが最適ゲートウェイからプッシュされた場合、ログ ファイルは次の場所にあります。

`%WINDIR%\TEMP\anyconnect-win-3.X.xxxxx-k9-install-yyyyyyyyyyyyyy.log`。

インストールするクライアントのバージョンの最新ファイルを取得します。*xxx* はバージョンによって異なり、*yyyyyyyyyyyyy* はインストールの日時を示します。

AnyConnect 接続または接続解除の問題

AnyConnect が初期接続を確立しないか、接続解除しない

問題：AnyConnect が初期接続を確立しないか、または [Cisco AnyConnect Secure Mobility Client] ウィンドウで [接続解除（Disconnect）] をクリックすると予期しない結果が得られます。

解決策： 次の点をチェックします。

- Citrix Advanced Gateway Client Version 2.2.1 を使用している場合は、CtxLsp.dll の問題が Citrix によって解決されるまで Citrix Advanced Gateway Client を削除してください。
- AT&T Sierra Wireless 875 カードと AT&T Communication Manager Version 6.2 または 6.7 を使用している場合は、次の手順に従って問題を修正してください。
  1. Aircard でアクセラレーションを無効にします。
  2. [ツール（Tools）] > [設定（Settings）] > [アクセラレーション（Acceleration）] > [スタートアップ（Startup）] から AT&T Communications Manager を起動します。
  3. **manual** と入力します。
  4. [停止（Stop）] をクリックします。
- ASA からコンフィギュレーション ファイルを取得し、次のようにして接続失敗の兆候を探します。
  - ASA コンソールから **write net x.x.x.x:ASA-Config.txt** と入力します。この *x.x.x.x* はネットワーク上の TFTP サーバの IP アドレスです。
  - ASA コンソールから、**show running-config** と入力します。設定を切り取ってテキスト エディタに貼り付け、これを保存します。
- ASA イベント ログを表示します。
  1. ASA コンソールで、次の行を追加し、ssl、webvpn、anyconnect、および auth のイベントを調べます。

```
config terminal
logging enable
logging timestamp
logging class auth console debugging
logging class webvpn console debugging
logging class ssl console debugging
logging class anyconnect console debugging
```

  2. AnyConnect クライアントの接続を試行し、接続エラーが発生した場合は、そのコンソールのログ情報を切り取ってテキスト エディタに貼り付け、保存します。
  3. **no logging enable** と入力し、ロギングを無効にします。

- Windows イベント ビューアを使用してクライアント コンピュータから Cisco AnyConnect VPN クライアント ログを取得します。
  1. [スタート（Start）] > [ファイル名を指定して実行（Run）] の順に選択し、**eventvwr.msc /s** と入力します。
  2. [アプリケーションとサービス ログ（Applications and Services Logs ）]（Windows 7）で、`Cisco AnyConnect VPN Client` を見つけ、[**ログ ファイルの名前を付けて保存...**（Save Log File As...）] を選択します。.
  3. ファイル名（たとえば、`AnyConnectClientLog.evt`）を割り当てます。`.evt` ファイル形式を使用する必要があります。
- Windows 診断デバッグ ユーティリティを変更します。
  1. WinDbg のマニュアルに記載されているとおりに vpnagent.exe プロセスを接続します。
  2. IPv6/IPv4 IP アドレス割り当てで競合が存在するかどうかを確認します。特定済みの競合がないか、イベント ログで確認します。
  3. 競合が特定されていた場合は、使用するクライアント コンピュータのレジストリにルーティングのデバッグを追加します。このような競合は、AnyConnect イベント ログで次のように表示されます。

```
Function: CRouteMgr:modifyRoutingTable Return code: 0xFE06000E File: .\VpnMgr.cpp
 Line:1122
Description: ROUTEMGR_ERROR_ROUTE_TABLE_VERIFICATION_FAILED.
Termination reason code 27: Unable to successfully verify all routing table
modifications are correct.

Function: CChangeRouteTable::VerifyRouteTable Return code: 0xFE070007
File: .\RouteMgr.cpp Line: 615 Description: ROUTETABLE_ERROR_NOT_INITIALIZED
gr.cpp Line: 615 Description: ROUTETABLE_ERROR_NOT_INITIALIZED
```

  4. 特定のレジストリ エントリ（Windows）またはファイル（Linux および macOS）を追加して、接続用にワンタイム単位でルートのデバッグを有効にします。
     - 32 ビット Windows の場合、DWORD レジストリ値は `HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\Cisco AnyConnect Secure Mobility Client\DebugRoutesEnabled` である必要があります。
     - 64 ビット Windows の場合、DWORD レジストリ値は `HKEY_LOCAL_MACHINE\Software\WOW6432node\Cisco\Cisco AnyConnect Secure Mobility Client\DebugRoutesEnabled` である必要があります。
     - Linux または macOS の場合、sudo touch コマンドを使用してパス `/opt/cisco/anyconnect/debugroutes` にファイルを作成します。

（注） トンネル接続が開始されると、キーまたはファイルは削除されます。デバッグを有効にするには、ファイルまたはキーが存在するだけで十分であり、キーの値またはファイルの内容は重要ではありません。

VPN 接続を開始します。このキーまたはファイルが検出されると、2 つのルート デバッグ テキスト ファイルがシステムの一時ディレクトリ（通常 Windows では C:\Windows\Temp、Mac または Linux では /tmp）に作成されます。2 つのファイル（debug_routechangesv4.txt4 と debug_routechangesv6.txt）がすでに存在する場合、これらのファイルは上書きされます。

AnyConnect がトラフィックを通過させない

問題：AnyConnect クライアントは、接続後、プライベート ネットワークにデータを送信できません。

解決策： 次の点をチェックします。

- AT&T Sierra Wireless 875 カードと AT&T Communication Manager Version 6.2 または 6.7 を使用している場合は、次の手順に従って問題を修正してください。
  1. Aircard でアクセラレーションを無効にします。
  2. [ツール（Tools）] > [設定（Settings）] > [アクセラレーション（Acceleration）] > [スタートアップ（Startup）] から AT&T Communications Manager を起動します。
  3. **manual** と入力します。
  4. [停止（Stop）] をクリックします。
- show vpn-sessiondb detail anyconnect filter name <username> コマンドの出力を取得します。出力にフィルタ名 XXXXX が指定されている場合は、show access-list XXXXX コマンドの出力も取得してください。ACL によってトラフィック フローがブロックされていないか確認してください。
- [AnyConnect VPN クライアント（AnyConnect VPN Client）] > [統計情報（Statistics）] > [詳細（Details）] > [エクスポート（Export）] の順に選択し、DART のファイルまたは出力（AnyConnect-ExportedStats.txt）を取得します。統計情報、インターフェイス、およびルーティング テーブルを調べます。
- ASA コンフィギュレーション ファイルの NAT 文を確認します。NAT が有効になっている場合は、クライアントに返されるデータをネットワーク アドレス変換から除外する必要があります。たとえば、AnyConnect プールから IP アドレスを NAT 除外するには、次のコードが使用されます。

```
access-list in_nat0_out extended permit ip any 10.136.246.0 255.255.255.0
```

```
ip local pool IPPool1 10.136.246.1-10.136.246.254 mask 255.252.0.0
nat (inside) 0 access-list in_nat0_out
```

- トンネリングされたデフォルト ゲートウェイがその設定に対して有効になっているかどうかを確認してください。従来型のデフォルト ゲートウェイは、次のように非復号化トラフィックのラスト リゾート ゲートウェイです。

```
route outside 0.0.209.165.200.225
route inside 0 0 10.0.4.2 tunneled
```

  VPN クライアントが、VPN ゲートウェイのルーティング テーブルに存在しないリソースにアクセスする必要がある場合、パケットは標準デフォルト ゲートウェイによってルーティングされます。VPN ゲートウェイは、完全な内部ルーティング テーブルを必要としません。トンネリングされたキーワードを使用する場合、IPsec/SSL VPN 接続から受信した復号化トラフィックはルーティングによって処理されます。VPN ルートから受信したトラフィックは 10.0.4.2 にルーティングされて復号化されますが、標準トラフィックは最終的に 209.165.200.225 にルーティングされます。

- AnyConnect でトンネルを確立する前後の、ipconfig /all のテキスト ダンプおよび route print の出力を収集します。
- クライアントでネットワーク パケット キャプチャを実行するか、ASA のキャプチャを有効にします。

（注） 一部のアプリケーション（Microsoft Outlook など）がトンネルで動作しない場合、受け入れられるサイズを確認するために、一定の基準に従って大きくした ping（たとえば、ping -| 500, ping -| 1000, ping -| 1500, and ping -| 2000）を使用して、ネットワーク内の既知のデバイスに ping します。ping の結果から、ネットワークにフラグメンテーションの問題が発生しているかがわかります。その後、フラグメンテーションが発生していると思われるユーザの特別なグループを設定して、このグループの anyconnect mtu を 1200 に設定できます。また、古い IPsec クライアントから Set MTU.exe ユーティリティをコピーして、物理アダプタの MTU を強制的に 1300 に設定できます。リブート時に、違いがあるかどうか確認してください。

VPN サービスの障害

VPN サービス接続に失敗

問題：「処理を進めることができません。VPN サービスに接続できません（Unable to Proceed, Cannot Connect to the VPN Service）」というメッセージが表示されます。AnyConnect の VPN サービスが実行されていません。

解決策：別のアプリケーションがサービスと競合していないか確認してください。11-7ページの「何がサービスと競合しているかの特定」を参照してください。

何がサービスと競合しているかの特定

次の手順では、サーバが起動されないため、競合が起動時にサーバの初期化との間で生じたか、または他の実行中のサービスとの間で生じたかを判別します。

手順

ステップ 1 Windows 管理ツールでサービスを確認して、Cisco AnyConnect VPN エージェントが動作していないか確認します。このエージェントが動作している場合にエラー メッセージが引き続き表示される場合は、ワークステーション上の別の VPN アプリケーションを無効にするか、アンインストールすることが必要になる可能性があります。その操作を実行した後、リブートし、この手順を繰り返します。

ステップ 2 Cisco AnyConnect VPN エージェントを起動してみます。

ステップ 3 イベント ビューアの AnyConnect ログに、サービスを起動できなかったことを示すメッセージがないか確認します。ステップ 2 での手動によるリスタートのタイム スタンプおよびワークステーションが起動した時間に注目します。

ステップ 4 イベント ビューアのシステム ログおよびアプリケーション ログに、競合メッセージの同一の一般的なタイム スタンプがないかを確認します。

ステップ 5 サービスの起動に失敗したことをログが示している場合、同一のタイム スタンプの前後にある、次のいずれかを示すその他の情報メッセージを探します。

- 欠落したファイル：欠落したファイルを除外するには、AnyConnect クライアントをスタンドアロン MSI インストールから再インストールします。
- 別の依存するサービスでの遅延：起動アクティビティを無効にして、ワークステーションのブート時間を短縮します。
- 別のアプリケーションまたはサービスとの競合：別のサービスが、vpnagent が使用するポートと同じポート上で受信していないか、または一部の HIDS ソフトウェアによって、シスコのソフトウェアがポート上で受信できなくなっているかどうかを判別します。

ステップ 6 ログに原因が直接示されていない場合は、試行錯誤的な方法で競合を識別してください。最も可能性の高い候補を識別したら、[サービス（Services）] パネルから該当するサービス（VPN 製品、HIDS ソフトウェア、spybot クリーナ、スニファ、アンチウイルス ソフトウェアなど）を無効にします。

ステップ 7 リブートします。VPN エージェント サービスが依然として起動に失敗する場合は、オペレーティング システムのデフォルト インストールでインストールされなかったサービスをオフにします。

VPNクライアントドライバで（MicrosoftWindowsアップデート後に）エラーが発生する

問題：最近Microsoft certclass.infファイルを更新し、その後、VPN接続を確立しようとすると、次のメッセージが表示されます。

```
The VPN client driver has encountered an error.
```

C:\WINDOWS\setupapi.log を確認すると、次のエラーが表示される場合があります。

```
#W239 The driver signing class list "C:\WINDOWS\INF\certclass.inf" was missing or invalid.
 Error 0xfffffbf8: Unknown Error. Assuming all device classes are subject to driver
signing policy.
```

解決策：コマンドプロンプトで**C:\>systeminfo**と入力するか、C:\WINDOWS\WindowsUpdate.logを確認して、最近インストールされた更新プログラムを確認してください。VPNドライバを修正する手順に従ってください。

VPN クライアント ドライバ エラーの修復

上記の手順を実行すると、カタログが破損していないことが示される場合がありますが、キーファイルが無署名のもので上書きされた可能性があります。障害が解消されない場合は、ドライバ署名のデータベースの破損原因を特定するためにMicrosoftに依頼してケースをオープンしてください。

手順

ステップ 1 コマンド プロンプトを管理者として開きます。

ステップ 2 **net stop CryptSvc** と入力します。

ステップ 3 **esentutl /g %systemroot%\System32\catroot2\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\catdb** と入力してデータベースを分析し、そのデータベースの妥当性を検証するか、%/WINDIR%\system32\catroot2 ディレクトリの名前を catroot2_old に変更します。

ステップ 4 プロンプトが表示されたら、[OK] を選択して修復を試行します。コマンド プロンプトを終了し、リブートします。

ドライバのクラッシュ

VPNVA.sys でのドライバ クラッシュの修復

問題：VPNVA.sys ドライバがクラッシュします。

解決策：Cisco AnyConnect 仮想アダプタにバインドされている中間ドライバを検索し、オフにしてください。

vpnagent.exe でのドライバ クラッシュの修復

手順

ステップ 1 c:\vpnagent という名前のディレクトリを作成します。

ステップ 2 タスク マネージャの [プロセス（process ）] タブを調べ、vpnagent.exe のプロセスの PID を判別します。

ステップ 3 コマンドプロンプトを開き、デバッグ ツールをインストールしたディレクトリに移動します。デフォルトでは、Windows のデバッグ ツールは `C:\Program Files\Debugging Tools` にあります。

ステップ 4 **cscript vpnagent4.vbs -crash -p PID -o c:\vpnagent -nodumponfirst** と入力します。ここで、*PID* は **vpnagent.exe** の PID です。

ステップ 5 オープン ウィンドウを最小化した状態で実行します。モニタリングしている間は、システムをログオフできません。

ステップ 6 クラッシュが発生すると、c:\vpnagent の中身を zip ファイルに収集します。

ステップ 7 **!analyze -v** を使用して、crashdmp ファイルをさらに診断します。

ネットワーク アクセス マネージャに関するリンク/ドライバの問題

ネットワーク アクセス マネージャが有線接続のアダプタの認識に失敗した場合は、ネットワーク ケーブルのプラグを抜き、もう一度差し込んでみてください。これでうまくいかない場合は、リンクに問題がある可能性があります。ネットワーク アクセス マネージャがアダプタの適切なリンク ステートを判別できない可能性があります。NIC ドライバの接続プロパティを確認してください。[詳細（Advanced）] パネルに [リンクを待機（Wait for Link）] オプションが表示される場合があります。この設定がオンになっている場合、有線接続の NIC ドライバの初期化コードは、自動ネゴシエーションが完了するまで待機してから、リンクが存在するかどうかを判別します。

その他のクラッシュ

AnyConnect のクラッシュ

問題：リブート後に「システムは重大なエラーから回復しました（the system has recovered from a serious error）」というメッセージを受け取りました。

解決策：%temp% ディレクトリ（C:\DOCUME~1\jsmith\LOCALS~1\Temp など）から .log および .dmp の生成済みファイルを収集します。ファイルをコピーするか、またはバックアップします。「.log ファイルまたは .dmp ファイルのバックアップ方法」を参照してください。

.log ファイルまたは .dmp ファイルのバックアップ方法

手順

ステップ 1 [スタート（Start）] > [ファイル名を指定して実行（Run）] メニューからワトソン博士（Drwtsn32.exe）という Microsoft ユーティリティを実行します。

ステップ 2 次のように設定し、[OK] をクリックします。

```
Number of Instructions     : 25
Number of Errors to Save : 25
Crash Dump Type   : Mini
Dump Symbol Table : Checked
Dump All Thread Contexts : Checked
Append to Existing Log File : Checked
Visual Notification : Checked
Create Crash Dump File : Checked
```

ステップ 3 クライアント コンピュータで [スタート（Start）] > [ファイル名を指定して実行（Run）] メニューの順に選択し、**eventvwr.msc /s** と入力して、Windows イベント ビューアから Cisco AnyConnect VPN クライアント ログを取得します。

ステップ 4 [アプリケーションとサービス ログ（Applications and Services Logs ）]（Windows 7）で、**Cisco AnyConnect VPN Client** を見つけ、[**ログ ファイルの名前を付けて保存...**（Save Log File As...）] を選択します。. .evt ファイル形式のファイル名（例：AnyConnectClientLog.evt）を割り当てます。

AnyConnectがvpndownloaderでクラッシュする（LayeredServiceProvider（LSP）モジュールおよび NOD32 AV）

問題：LSP または NOD32 AV を使用している場合、AnyConnect は、接続を確立しようとした際、認証に成功し、SSL セッションを構築するものの、その後 AnyConnect クライアントが vpndownloader でクラッシュします。

解決策：ESET NOD32 AV のバージョン 2.7 で Internet Monitor コンポーネントを削除し、バージョン 3.0 にアップグレードしてください。

ブルー スクリーン（AT & T Dialer）

問題：AT&T Dialer を使用している場合に、クライアント オペレーティング システムでブルースクリーンが発生して、ミニ ダンプ ファイルが作成されることがあります。

解決策：AT&T Global Network Client を最新の 7.6.2 にアップグレードしてください。

セキュリティの警告

Microsoft Internet Explorer のセキュリティの警告

問題：Microsoft Internet Explorer で、[セキュリティの警告（security alert）] ウィンドウが表示され、次のテキストが示されます。

```
Information you exchange with this site cannot be viewed or changed by others. However,
 there is a problem with the site's security certificate. The security certificate was
issued by a company you have not chosen to trust. View the certificate to determine
whether you want to trust the certifying authority.
```

解決策：このアラートは、信頼済みサイトとして認識されていない ASA に接続すると表示されることがあります。このアラートを回避するには、クライアントに信頼できるルート証明書をインストールします。「クライアントでの信頼できるルート証明書のインストール」を参照してください。

「不明な機関による認証」アラート

問題：「不明な機関による Web サイト認証」アラート ウィンドウがブラウザに表示されることがあります。[セキュリティの警告（Security Alert）] ウィンドウの上半分に、次のテキストが表示されます。

```
Unable to verify the identity of <Hostname_or_IP_address> as a trusted site.
```

解決策：このセキュリティ アラートは、信頼済みサイトとして認識されていない ASA に接続すると表示されることがあります。このアラートを回避するには、クライアントに信頼できるルート証明書をインストールします。「クライアントでの信頼できるルート証明書のインストール」を参照してください。

クライアントでの信頼できるルート証明書のインストール

始める前に

信頼できるルート証明書として使用する証明書を生成または取得します。

（注） クライアントで信頼できるルート証明書として自己署名証明書をインストールすることによって、短期的にセキュリティ証明書の警告を回避できます。ただし、これはお勧めしません。理由は、ユーザが誤って不正なサーバ上の証明書を信頼するようにブラウザを設定する可能性があるため、また、ユーザがセキュア ゲートウェイに接続する際に、セキュリティ警告に応答する手間がかかるためです。

手順

ステップ 1 [セキュリティの警告（Security Alert）] ウィンドウの [証明書の表示（View Certificate）] をクリックします。
ステップ 2 [証明書のインストール（Install Certificate）] をクリックします。
ステップ 3 [Next] をクリックします。
ステップ 4 [証明書をすべて次のストアに配置する（Place all certificates in the following store）] を選択します。
ステップ 5 [参照（Browse）] をクリックします。
ステップ 6 ドロップダウンリストで、[信頼されたルート証明機関（Trusted Root Certification Authorities）] を選択します。
ステップ 7 [証明書のインポート（Certificate Import）] ウィザードのプロンプトに従って続行します。

接続のドロップ

有線接続が導入された場合のワイヤレス接続のドロップ（Juniper Odyssey クライアント）

問題：Odyssey クライアントでワイヤレス サプレッションが有効である場合、有線接続が導入されると、ワイヤレス接続がドロップします。ワイヤレス サプレッションが無効である場合、ワイヤレス機能は期待どおりに動作する。

解決策：11-11 ページで、Odyssey クライアントの設定。

Odyssey クライアントの設定

手順

ステップ 1 [ネットワーク接続（Network Connections）] で、アダプタの名前を接続プロパティの表示どおりにコピーします。レジストリを編集する場合、誤って変更すると重大な問題が発生する可能性があるため、バックアップを実行してから、細心の注意を払って変更してください。
ステップ 2 レジストリを開き、HKEY_LOCAL_MACHINE\SOFTWARE\Funk Software, Inc.\odyssey\client\configuration\options\adapterType\virtual に移動します。
ステップ 3 virtual の下に新しい文字列値を作成します。アダプタの名前をネットワーク プロパティからレジストリ部分にコピーします。追加のレジストリ設定を保存すると、MSI が作成されて他のクライアントにプッシュされたときに、この設定が移植されます。

ASA への接続に失敗（Kaspersky AV Workstation 6.x）

問題：Kaspersky 6.0.3 がインストールされると（無効であっても）、CSTP state＝CONNECTED の直後に ASA への AnyConnect 接続が失敗します。次のメッセージが表示されます。

```
SVC message: t/s=3/16: Failed to fully establish a connection to the secure gateway
(proxy authentication, handshake, bad cert, etc.).
```

解決策：Kaspersky をアンインストールし、Kaspersky のフォーラムを参照して追加のアップデートがないか確認してください。

UDP DTLS 接続なし（McAfee Firewall 5）

問題：McAfee Firewall 5 を使用しているときに、UDP DTLS 接続を確立できません。

解決策：McAfee Firewall のセンター コンソールで、[高度なタスク（Advanced Tasks）] > [高度なオプションとロギング（Advanced options and Logging）] を選択し、McAfee Firewall の [Block incoming fragments automatically] チェックボックスをオフにします。

ホスト デバイスへの接続に失敗（Microsoft ルーティングとリモート アクセス サーバ）

問題：RRAS を使用している場合に、AnyConnect がホスト デバイスへの接続を確立しようとすると、イベント ログに次の終了エラーが返されます。

```
Termination reason code 29 [Routing and Remote Access service is running]
The Windows service “Routing and Remote Access” is incompatible with the Cisco AnyConnect
 VPN Client.
```

解決策：RRAS サービスを無効にします。

接続障害/クレデンシャル不足（ロード バランサ）

問題：クレデンシャルがないために、接続が失敗します。

解決策：サードパーティ製ロード バランサでは、ASA デバイスにかかる負荷を把握できません。一方、ASA のロード バランス機能は非常にインテリジェントで、VPN の負荷をデバイス全体で均等に分散できるため、ASA 内蔵のロード バランシングを使用することをお勧めします。

インストールの失敗

AnyConnect がダウンロードに失敗する（Wave EMBASSY Trust Suite）

問題：AnyConnect クライアントがダウンロードに失敗し、次のエラー メッセージが表示されます。

```
"Cisco AnyConnect VPN Client Downloader has encountered a problem and needs to close."
```

ソリューションdllの問題をすべて解決するために、パッチアップデートをバージョン1.2.1.38に更新してください。

非互換性の問題

ルーティング テーブルの更新に失敗（Bonjour Printing Service）

問題：Bonjour Print Service を使用している場合に、AnyConnect イベント ログに IP 転送テーブルの識別に失敗したことが示されます。

解決策：コマンド プロンプトで **net stop "bonjour service"** と入力し、Bonjour Print Service を無効にします。mDNSResponder の新しいバージョン（1.0.5.11）が Apple から提供されています。この問題を解決するために、Bonjour の新しいバージョンが iTunes にバンドルされ、個別のダウンロードとして Apple の Web サイトで配布されています。

TUN のバージョンに互換性がない（OpenVPN クライアント）

問題：このバージョンの TUN がこのシステムにすでにインストールされていて、AnyConnect クライアントと互換性がないことを示すエラーが表示されます。

解決策：Viscosity OpenVPN Client をアンインストールします。

Winsock カタログの競合（LSP 症状 2 競合）

問題：クライアント上にLSPモジュールが存在する場合、Winsockカタログが競合することがあります。

解決策：LSP モジュールをアンインストールしてください。

データ スループット低下（LSP 症状 3 競合）

問題：Windows 7 で NOD32 Antivirus V4.0.468 x64 を使用すると、データ スループットが低下する場合があります。

解決策：SSL プロトコル スキャンを無効にします。「SSL プロトコル スキャンの無効化」を参照してください。

SSL プロトコル スキャンの無効化

手順

ステップ 1 [詳細設定（Advanced Setup）] の **[プロトコル フィルタリング（Protocol Filtering）]** > **[SSL]** を選択し、SSL プロトコル スキャンを有効にします。

ステップ 2 **[Web アクセス保護（Web access protection）]** > **[HTTP, HTTPS]** の順に選択し、[HTTPS プロトコル チェックを使用しない（Do not use HTTPS protocol checking）] をオンにします。

ステップ 3 **[プロトコル フィルタリング（Protocol Filtering）]** > **[SSL]** に戻り、SSL プロトコル スキャンを無効にします。

DPD 障害（EVDO ワイヤレス カードおよび Venturi ドライバ）

問題：クライアントの接続解除中に、EVDO ワイヤレス カードおよび Venturi ドライバを使用すると、イベント ログに次のことが報告されます。

```
%ASA-5-722037: Group <Group-Name> User <User-Name> IP <IP-Address> SVC closing connection:
 DPD failure.
```

ソリューション

- アプリケーション、システム、および AnyConnect の各イベント ログに関係する接続解除イベントがないか確認すると同時に、NIC カードのリセットが適用されたかどうか判別してください。
- Venturi ドライバが最新のものであるか確認してください。AT&T Communications Manager バージョン 6.7 の [ルール エンジンの使用（Use Rules Engine）] を無効にします。

DTLS トラフィック障害（DSL ルータ）

問題：DSL ルータに接続している場合、正常にネゴシエーションされても、DTLS トラフィックが失敗することがあります。

解決策： 工場出荷時の設定を使用して Linksys ルータに接続してください。この設定により、DTLS セッションが安定し、ping で中断が発生しません。DTLS リターン トラフィックを許可するルールを追加してください。

NETINTERFACE_ERROR（CheckPoint と、Kaspersky などの他のサードパーティ製ソフトウェア）

問題：SSL 接続に使用されるコンピュータ ネットワークのオペレーティング システム情報を取得しようとしたときに、セキュア ゲートウェイへの接続を完全には確立できなかったことが AnyConnect ログに示されることがあります。

ソリューション

- 整合性エージェントをアンインストールしてから AnyConnect をインストールする場合は、TCP/IP を有効にしてください。
- 整合性エージェントのインストール時に SmartDefense を無効にすると、TCP/IP がチェックされます。
- サードパーティ製のソフトウェアがネットワーク インターフェイス情報の取得中に、オペレーティング システムの API コールを代行受信またはブロックしている場合は、疑わしい AV、FW、AS などがないか確認してください。
- デバイス マネージャに AnyConnect アダプタのインスタンスが 1 つだけ表示されていることを確認してください。インスタンスが 1 つだけの場合は、AnyConnect で認証し、5 秒後にデバイス マネージャからアダプタを手動で有効にしてください。
- 疑わしいドライバが AnyConnect アダプタ内で有効にされている場合は、これらのドライバを [Cisco AnyConnect VPN Client 接続（Cisco AnyConnect VPN Client Connection）] ウィンドウでオフにして無効にしてください。

パフォーマンスの問題（Virtual Machine Network Service ドライバ）

問題：一部の Virtual Machine Network Service デバイスで AnyConnect を使用しているときに、パフォーマンスの問題が発生しました。

解決策：AnyConnect 仮想アダプタ内のすべての IM デバイスに対するバインドをオフにしてください。アプリケーション dsagent.exe は、C:\Windows\System\dgagent にあります。これはプロセス リストに表示されませんが、TCPview（sysinternals）でソケットを開くと表示できます。このプロセスを終了すると、AnyConnect が正常の動作に戻ります。

既知のサードパーティ製アプリケーション競合

次のサードパーティ アプリケーションは、Cisco AnyConnect Secure Mobility Client との間に既知の複雑な問題があります。

- Adobe および Apple：Bonjour Print Service
  - Adobe Creative Suite 3
  - BonJour Print Service

    - iTunes
- AT&T Communications Manager バージョン 6.2 および 6.7
    - AT&T Sierra Wireless 875 カード
- AT&T Global Dialer
- Citrix Advanced Gateway Client バージョン 2.2.1
- ファイアウォールとの競合
    - サードパーティ製のファイアウォールが、ASA グループ ポリシーで設定されたファイアウォール機能と干渉する可能性があります。
- Juniper Odyssey Client
- Kaspersky AV Workstation 6.x
- McAfee Firewall 5
- Microsoft Internet Explorer 8
- Microsoft Routing and Remote Access Server
- Microsoft Windows アップデート
- OpenVPN クライアント
- ロード バランサ
- Wave EMBASSY Trust Suite
- Layered Service Provider（LSP）モジュールおよび NOD32 AV
- EVDO ワイヤレスカードおよび Venturi ドライバ
- DSL ルータ
- CheckPoint と、Kaspersky など他のサードパーティ製ソフトウェア
- Virtual Machine Network Service ドライバ