セキュアなアクセス

Cisco ISE でのネットワークデバイスの定義

スイッチやルータなどのネットワークデバイスは、認証、許可、およびアカウンティング（AAA）クライアントであり、Cisco ISE に AAA サービス要求を送信します。Cisco ISE でネットワークデバイスを定義すると、Cisco ISE とネットワークデバイス間の連携動作が有効になります。

ネットワークデバイスを RADIUS または TACACS AAA に設定したり、プロファイリングサービスでプロファイリング エンドポイントの Cisco Discovery Protocol 属性および Link Layer Discovery Protocol（LLDP）属性を収集するための Simple Network Management Protocol（SNMP）を設定したり、Cisco TrustSec デバイスの TrustSec 属性を設定したりします。Cisco ISE に定義されていないネットワーク デバイスは、Cisco ISE から AAA サービスを受信できません。

Cisco ISE のメインメニューで、**[管理（Administration）] > [ネットワークリソース（Network Resources）] > [ネットワークデバイス（Network Devices）]** を選択し、[追加（Add）] をクリックします。表示される [新しいネットワークデバイス（New Network Device）] ウィンドウで、次の詳細を入力してネットワークデバイスを定義します。

- ネットワークデバイスに応じたベンダープロファイルを選択します。プロファイルには、URL リダイレクトや許可変更の設定などの、デバイスに事前に定義された設定が含まれています。

- RADIUS 認証用の RADIUS プロトコルを設定します。Cisco ISE はネットワークデバイスから RADIUS 要求を受信すると、対応するデバイス定義を探して設定されている共有秘密を取得します。Cisco ISE はデバイス定義を検出すると、デバイスに設定されている共有秘密を取得し、それを要求内の共有秘密と照合してアクセスを認証します。共有秘密が一致すると、RADIUS サーバーは、ポリシーと設定に基づいて要求をさらに処理します。共有秘密が一致しない場合は、拒否応答がネットワークデバイスに送信されます。失敗した認証レポートが生成され、失敗の理由が示されます。
- TACACS+ 認証用の TACACS+ プロトコルを設定します。Cisco ISE はネットワーク デバイスから TACACS+ 要求を受信すると、対応するデバイス定義を探して設定されている共有秘密を取得します。デバイス定義が見つかった場合、デバイスに設定されている共有秘密を取得し、それを要求内の共有秘密と照合してアクセスを認証します。共有秘密が一致すると、TACACS+ サーバーは、ポリシーと設定に基づいて要求をさらに処理します。一致しない場合は、拒否応答がネットワーク デバイスに送信されます。失敗した認証レポートが生成され、失敗の理由が示されます。
- プロファイリング サービスがネットワーク デバイスと通信し、ネットワーク デバイスに接続されているエンドポイントをプロファイリングするように、ネットワーク デバイス定義で簡易ネットワーク管理プロトコル（SNMP）を設定できます。
- Cisco TrustSec ソリューションの一部となる可能性がある TrustSec 対応デバイスからの要求を処理するには、Cisco ISE 内に Cisco TrustSec 対応デバイスを定義する必要があります。Cisco TrustSec ソリューションをサポートするスイッチはすべて Cisco TrustSec 対応デバイスです。

  Cisco TrustSec デバイスでは IP アドレスは使用されません。代わりに、Cisco TrustSec デバイスが Cisco ISE と通信できるように、その他の設定を定義する必要があります。

  Cisco TrustSec 対応デバイスは Cisco ISE との通信に TrustSec 属性を使用します。Cisco Nexus 7000 シリーズ スイッチ、Cisco Catalyst 6000 シリーズ スイッチ、Cisco Catalyst 4000 シリーズ スイッチ、Cisco Catalyst 3000 シリーズ スイッチなどの Cisco TrustSec 対応デバイスは、Cisco TrustSec デバイスの追加時に定義した Cisco TrustSec 属性を使用して認証されます。

（注） Cisco ISE でネットワークデバイスを設定する際には、共有秘密の一部としてバックスラッシュ（\）を含めないことをお勧めします。これは、Cisco ISE をアップグレードすると、共有秘密にバックスラッシュが表示されなくなるためです。ただし、Cisco ISE をアップグレードせずに再イメージ化すると、共有秘密にバックスラッシュが表示されます。

Cisco ISE でのデフォルト ネットワーク デバイスの定義

Cisco ISE では、RADIUS および TACACS 認証のデフォルトのデバイス定義がサポートされています。特定の IP アドレスのデバイス定義が見つからない場合、Cisco ISE で使用できるデフォルトのネットワーク デバイスを定義することができます。この機能を使用すると、新しくプロビジョニングされたデバイスのデフォルトの RADIUS または TACACS 共有秘密とアクセス レベルを定義できます。

（注） 基本的な RADIUS および TACACS 認証のみにデフォルトのデバイス定義を追加することを推奨します。高度なフローについては、ネットワークデバイスごとに個別のデバイス定義を追加する必要があります。

Cisco ISE は、ネットワーク デバイスから RADIUS または TACACS 要求を受信すると、対応するデバイス定義を検索して、ネットワーク デバイス定義に設定されている共有秘密を取得します。

RADIUS または TACACS 要求が受信されると、Cisco ISE は次の手順を実行します。

1. 要求内の IP アドレスに一致する特定の IP アドレスを探します。
2. 範囲を調べて、要求内の IP アドレスが指定された範囲内にあるかどうかを確認します。
3. ステップ 1 と 2 の両方が失敗すると、要求の処理にデフォルトのデバイス定義（定義されている場合）が使用されます。

Cisco ISE は、そのデバイスのデバイス定義に設定されている共有秘密を取得し、それを RADIUS または TACACS 要求内の共有秘密と照合してアクセスを認証します。デバイス定義が見つからない場合、Cisco ISE はデフォルトのネットワーク デバイス定義から共有秘密を取得し、RADIUS または TACACS 要求を処理します。

ネットワーク デバイス

後続の項で説明されているウィンドウを使用して、Cisco ISE でネットワークデバイスを追加および管理できます。

ネットワーク デバイス定義の設定

次の表では、Cisco ISE のネットワーク アクセス デバイスを設定するために使用できる [ネットワークデバイス（Network Devices）] ウィンドウのフィールドについて説明します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして選択します**[管理（Administration）] > [ネットワークリソース（Network Resources）] > [ネットワークデバイス（Network Devices）]** で、**[追加（Add）]** をクリックします。

ネットワーク デバイスの設定

次の表では、[ネットワークデバイスの設定（Network Device Settings）][新しいネットワークデバイス（New Network Devices）] ウィンドウのフィールドについて説明します。

表 *1:* ネットワーク デバイスの設定

フィールド名	説明
名前（Name）	ネットワークデバイスの名前を入力します。 ネットワークデバイスに、デバイスのホスト名とは異なるわかりやすい名前を指定できます。デバイス名は論理識別子です。 （注）　必要に応じて、設定後にデバイスの名前を変更できます。
説明	このデバイスの説明を入力します。
IP アドレスまたは **IP 範囲**	ドロップダウンリストから次のいずれかを選択し、表示されるフィールドに必要な値を入力します。 • [IP アドレス（IP Address）]：単一の IP アドレス（IPv4 または IPv6 アドレス）とサブネットマスクを入力します。 • [IP 範囲（IP Ranges）]：必要な IPv4 アドレスの範囲を入力します。認証時に IP アドレスを除外するには、[除外（Exclude）] フィールドに IP アドレスまたは IP アドレスの範囲を入力します。 IP アドレスとサブネットマスクまたは IP アドレスの範囲を定義するためのガイドラインを次に示します。 • 特定の IP アドレスを定義するか、サブネットマスクを使用して IP 範囲を定義できます。デバイス A の IP アドレス範囲が定義されている場合、デバイス A に定義されている範囲の個別のアドレスを別のデバイス B に設定できます。 • すべてのオクテットの IP アドレス範囲を定義できます。IP アドレスの範囲を指定するときに、ハイフン（-）またはアスタリスク（*）をワイルドカードとして使用できます。たとえば、*.*.*.*、1-10.1-10.1-10.1-10 または 10-11.*.5.10-15 などです。 • サブセットがすでに追加されている場合は、設定された範囲からその IP アドレス範囲のサブセットを除外できます。例：10.197.65.*/10.197.65.1 または 10.197.65.* exclude 10.197.65.1。 • ネットワークデバイスごとに最大 40 の IP アドレス、または IP 範囲を設定できます。 • 同じ IP アドレスを持つ 2 台のデバイスを定義することはできません。 • 同じ IP 範囲を持つ 2 台のデバイスを定義することはできません。IP 範囲は、一部または全部が重複することはできません。

フィールド名	説明
[デバイスプロファイル（Device Profile）]	ドロップダウンリストから、ネットワークデバイスのベンダーを選択します。 選択したベンダーのネットワークデバイスがサポートしているフローおよびサービスを表示するには、ドロップダウンリストの横にあるツールのヒントを使用します。ツールのヒントには、デバイスが使用する URL リダイレクトの RADIUS 認可変更（CoA）ポートとタイプも表示されます。これらの属性は、デバイス タイプのネットワーク デバイス プロファイルで定義されます。
モデル名（Model Name）	ドロップダウンリストからデバイスのモデルを選択します。 モデル名は、ルールベースのポリシーの条件をチェックするときに、パラメータの1つとして使用します。この属性は、デバイスディクショナリにあります。
ソフトウェア バージョン（Software Version）	ドロップダウンリストから、ネットワークデバイスで実行するソフトウェアのバージョンを選択します。 ソフトウェアバージョンは、ルールベースのポリシーの条件をチェックするときに、パラメータの 1 つとして使用できます。この属性は、デバイスディクショナリにあります。
ネットワーク デバイス グループ（Network Device Group）	[ネットワークデバイスグループ（Network Device Group）] エリアで、[ロケーション（Location）]、[IPSEC]、および[デバイスタイプ（Device Type）] ドロップダウンリストから必要な値を選択します。 グループに明確にデバイスを割り当てないと、そのグループはデフォルトのデバイスグループ（ルート ネットワーク デバイス グループ）に含まれます。これにより、ロケーションは[すべてのロケーション（All Locations）]、デバイスタイプは[すべてのデバイスタイプ（All Device Types）] となります。

（注） フィルタを使用して Cisco ISE 展開からネットワーク アクセス デバイス（NAD）を選択して削除する場合は、ブラウザのキャッシュをクリアして、選択した NAD のみが削除されるようにします。

RADIUS 認証設定

次の表では、[RADIUS 認証設定（RADIUS Authentication Settings）] エリアのフィールドについて説明します。

表 *2 : [RADIUS* 認証設定（*RADIUS Authentication Settings*）*]* エリア

フィールド名	使用上のガイドライン
RADIUS UDP の設定	
Protocol	選択したプロトコルとして **RADIUS** を表示します。
共有秘密鍵（Shared Secret）	ネットワーク デバイスの共有秘密鍵を入力します。 共有秘密鍵は、**pac** オプションを指定した **radius-host** コマンドを使用してネットワークデバイスに設定したキーです。 （注） 共有秘密鍵の長さは、[デバイスのセキュリティ設定（Device Security Settings）] ウィンドウ（[管理（Administration）] > [ネットワークリソース（Network Resources）] > [ネットワークデバイス（Network Devices）] > [デバイスセキュリティ設定（Device Security Settings）]）の [RADIUS 共有秘密鍵の最小長（Minimum RADIUS Shared Secret Length）] フィールドで設定された値と同等以上である必要があります。 RADIUS サーバーでのベストプラクティスは、22 文字にすることです。新規インストールおよびアップグレードされた展開の場合、共有秘密鍵の長さはデフォルトで 4 文字です。この値は [デバイスセキュリティ設定（Device Security Settings）] ウィンドウで変更できます。
2 番目の共有秘密の使用	ネットワークデバイスと Cisco ISE で使用される 2 番目の共有秘密鍵を指定します。 （注） Cisco TrustSec デバイスには、デュアル共有秘密（鍵）の利点がありますが、Cisco ISE により送信される Cisco TrustSec CoA パケットは常に最初の共有秘密（鍵）を使用します。2 番目の共有秘密鍵の使用を有効にするには、Cisco TrustSec CoA パケットを Cisco TrustSec デバイスに送信する Cisco ISE ノードを選択します。**[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [ネットワークリソース（Network Resources }] > [ネットワークデバイス（Network Devices）] > [追加（Add）] > [高度な TrustSec 設定（Advanced Trustsec Settings）]** ウィンドウの [送信元（Send From）] ドロップダウンリストで、このタスクに使用する Cisco ISE ノードを設定します。プライマリ管理ノード（PAN）またはポリシーサービスノード（PSN）を選択できます。選択した PSN ノードがダウンしている場合、PAN は Cisco TrustSec デバイスに Cisco TrustSec CoA パケットを送信します。 （注） RADIUS アクセス要求の 2 番目の共有秘密機能は、**[Message-Authenticator]** フィールドを含むパケットに対してのみ機能します。

フィールド名	使用上のガイドライン
CoA ポート（CoA Port）	RADIUS CoA に使用するポートを指定します。 デバイスのデフォルトの CoA ポートは、ネットワークデバイス用に設定されたネットワーク デバイス プロファイルで定義されます（**[管理（Administration）] > [ネットワークリソース（Network Resources）] > [ネットワークデバイスプロファイル（Network Device Profiles）] > [ネットワークリソース（Network Resources）] > [ネットワークデバイスプロファイル（Network Device Profiles）]**）。デフォルト CoA ポートを使用するには、[デフォルトに設定（Set To Default）] をクリックします。 （注） [RADIUS 認証設定（RADIUS Authentication Settings）] の **[ネットワークデバイス（Network Devices）]** ウィンドウ（**[管理（Administration）] > [ネットワークリソース（Network Resources）] > [ネットワークデバイス（Network Devices）]**）で指定した CoA ポートを変更する場合は、**[ネットワークデバイスプロファイル（Network Device Profile）]** ウィンドウ（**[管理（Administration）] > [ネットワークリソース（Network Resources）] > [ネットワークデバイスプロファイル（Network Device Profiles）]**）で対応するプロファイルに同じ CoA ポートを指定します。
RADIUS DTLS の設定	
必要な DTLS	[必要な DTLS（DTLS Required）] チェックボックスをオンにすると、Cisco ISE ではこのデバイスからの DTLS 要求のみが処理されます。このオプションを無効にすると、Cisco ISE ではこのデバイスからの UDP 要求と DTLS 要求の両方が処理されます。 RADIUS DTLS はセキュアソケットレイヤ（SSL）トンネルの確立および RADIUS の通信用に強化されたセキュリティを提供します。
共有秘密鍵（Shared Secret）	RADIUS DTLS に使用される共有秘密鍵が表示されます。この値は固定されており、Message Digest 5（MD5）完全性チェックを計算するために使用されます。
CoA ポート（CoA Port）	RADIUS DTLS CoA に使用するポートを指定します。
CoA の ISE 証明書の発行元 CA	ドロップダウンリストから RADIUS DTLS CoA に使用する認証局を選択します。

フィールド名	使用上のガイドライン
DNS 名	ネットワーク デバイスの DNS 名を入力します。[RADIUS/DTLS クライアント ID 検証の有効化（Enable RADIUS/DTLS Client Identity Verification）] オプションが [RADIUS 設定（RADIUS Settings）] ウィンドウ（**[管理（Administration）]** > **[システム（System）]** > **[設定（Settings）]** > **[プロトコル（Protocols）]** > **[RADIUS]**）で有効になっている場合、Cisco ISE はこの DNS 名とクライアント証明書で指定されている DNS 名を比較して、ネットワークデバイスの ID を確認します。
全般設定	
KeyWrap の有効化（Enable KeyWrap）	KeyWrap アルゴリズムがネットワークデバイスでサポートされている場合にのみ、[KeyWrap の有効化（Enable KeyWrap）] チェックボックスをオンにします。ネットワークデバイスは、AES KeyWrap RFC（RFC 3394）と互換性がある必要があります。 このオプションは、AES KeyWrap アルゴリズムを介して RADIUS セキュリティを強化するために使用されます。
キー暗号キー（Key Encryption Key）	セッションの暗号化（秘密）に使用される暗号キーを入力します。
メッセージ オーセンティケータ コード キー（Message Authenticator Code Key）	RADIUS メッセージに対するキー付きハッシュメッセージ認証コード（HMAC）の計算に使用されるキーを入力します。
キー入力形式（Key Input Format）	次のいずれかのオプション ボタンをクリックします。 • [ASCII] : [キー暗号キー（Key Encryption Key）] フィールドに入力する値の長さは16 文字（バイト）、[メッセージ認証コードキー（Message Authenticator Code Key）] フィールドに入力する値の長さは 20 文字（バイト）にする必要があります。 • [16 進数（Hexadecimal）] : [キー暗号キー（Key Encryption Key）] フィールドに入力する値の長さは 32 文字（バイト）、[メッセージ認証コードキー（Message Authenticator Code Key）] フィールドに入力する値の長さは 40 文字（バイト）にする必要があります。 ネットワークデバイスの設定と一致するように、キー暗号キーおよびメッセージ認証コードキーの入力に使用するキー入力形式を指定できます。指定する値はキーの正しい（全体の）長さにする必要があり、それよりも短い値は許可されません。

TACACS 認証設定

表 *3 : [TACACS* 認証設定（*TACACS Authentication Settings*）*]* エリアのフィールド

フィールド名	使用上のガイドライン
共有秘密鍵（**Shared Secret**）	TACACS+ プロトコルが有効のときにネットワークデバイスに割り当てられたテキストの文字列。ユーザーは、ネットワークデバイスによってユーザー名およびパスワードが認証される前にテキストを入力する必要があります。ユーザーが共有秘密情報を提示するまで、接続は拒否されます。
廃止された共有秘密がアクティブです（**Retired Shared Secret is Active**）	リタイアメント期間がアクティブな場合に表示されます。
廃止（**Retire**）	既存の共有秘密を終了する代わりに廃止します。[廃止（Retire）] をクリックすると、ダイアログボックスが表示されます。[はい（Yes）] または [いいえ（No）] をクリックできます。
残りの廃止期間（**Remaining Retired Period**）	（[Retire] ダイアログボックスで [Yes] を選択した場合にのみ利用可能）**[Work Centers]** > **[Device Administration]** > **[Settings]** > **[Connection Settings]** > **[Default Shared Secret Retirement Period]** で指定されたデフォルト値が表示されます。必要に応じて、デフォルト値を変更できます。 古い共有秘密は、指定された日数の間はアクティブなままになります。
終了（**End**）	（[廃止（Retire）] ダイアログボックスで [はい（Yes）] をクリックした場合にのみ利用可能）リタイアメント期間が終了し、古い共有秘密が終了します。
シングル接続モードを有効にする（**Enable Single Connect Mode**）	[シングル接続モードを有効にする（Enable Single Connect Mode）] チェックボックスは、ネットワークデバイスとのすべての TACACS+ 通信に単一の TCP 接続を使用する場合にオンにします。次のいずれかのオプションボタンをクリックします。 • **[レガシーシスコデバイス（Legacy Cisco Devices）]** • **TACACS ドラフト コンプライアンス シングル接続のサポート** （注） **[シングル接続モード（Single Connect Mode）]** を無効にすると、Cisco ISE はすべての TACACS 要求に対して新しい TCP 接続を使用します。

SNMP 設定

次の表では、[SNMP 設定（SNMP Settings）] セクションのフィールドについて説明します。

表 *4 : [SNMP*設定（***SNMP Settings***）*]* エリアのフィールド

フィールド名	使用上のガイドライン
SNMP バージョン（SNMP Version）	**[SNMP バージョン（SNMP Version）]** ドロップダウンリストから、次のいずれかのオプションを選択します。 • **1**：SNMPv1 は informs をサポートしていません。 • **2c** • 3：SNMPv3 は、[セキュリティレベル（Security Level）] フィールドで [Priv] を選択した場合にパケットの暗号化が可能であるため、最もセキュアなモデルです。 （注） ネットワークデバイスに SNMPv3 パラメータを設定した場合、モニタリングサービス（**[操作（Operations）]** > （**[レポート（Reports）]** > **[診断（Diagnostics）]** > **[ネットワークデバイスセッションステータス（Network Device Session Status）]**）によって提供される **[ネットワーク デバイス セッション ステータス（Network Device Session Status）]** 概要レポートを生成できません。ネットワークデバイスが SNMPv1 または SNMPv2c パラメータを使用して設定されている場合は、このレポートを正常に生成できます。
SNMP RO コミュニティ（SNMP RO Community）	（SNMP バージョン 1 および 2c にのみ適用可能）Cisco ISE にデバイスへの特定タイプのアクセスを提供する読み取り専用コミュニティ文字列を入力します。 （注） キャレット記号（曲折アクセント付き^）は使用できません。
SNMP ユーザー名（SNMP Username）	（SNMP バージョン 3 の場合のみ）SNMP ユーザー名を入力します。
セキュリティ レベル（Security Level）	（SNMP バージョン 3 の場合のみ）**[セキュリティレベル（Security Level）]** ドロップダウンリストから次のオプションのいずれかを選択します。 • **[Auth]**：MD5 またはセキュア ハッシュ アルゴリズム（SHA）パケットの認証を有効にします。 • **[No Auth]**：認証なし、プライバシーなしのセキュリティレベル。 • **[Priv]**：Data Encryption Standard（DES; データ暗号規格）パケットの暗号化を有効にします。

フィールド名	使用上のガイドライン
認証プロトコル（**Auth Protocol**）	（SNMP バージョン 3 でセキュリティレベル **[Auth]** または **[Priv]** を選択した場合のみ）**[認証プロトコル（Auth Protocol）]** ドロップダウンリストから、ネットワークデバイスで使用する認証プロトコルを選択します。 • **[MD5]** • **[SHA]**
認証パスワード（**Auth Password**）	（SNMP バージョン 3 で **[Auth]** および **[Priv]** セキュリティレベルを選択した場合のみ）認証キーを入力します。8 文字以上の長さにする必要があります。 デバイスにすでに設定されている認証パスワードを表示するには、[表示（Show）] をクリックします。 （注） キャレット記号（曲折アクセント付き^）を使用することはできません。
プライバシー プロトコル（**Privacy Protocol**）	（SNMP バージョン 3 で **[Priv]** セキュリティレベルを選択した場合のみ）**[プライバシープロトコル（Privacy Protocol）]** ドロップダウンリストから次のいずれかのオプションを選択します。 • **[DES]** • **AES128** • **AES192** • **AES256** • **3DES**
プライバシー パスワード（**Privacy Password**）	（SNMP バージョン 3 で **[Priv]** セキュリティレベルを選択した場合のみ）プライバシーキーを入力します。 デバイスにすでに設定されているプライバシーパスワードを表示するには、[表示（Show）] をクリックします。 （注） キャレット記号（曲折アクセント付き^）を使用することはできません。
ポーリング間隔（**Polling Interval**）	ポーリング間隔を秒単位で入力します。デフォルト値は 3600 です。
リンク トラップ クエリー（**Link Trap Query**）	SNMP トラップを介して受信する linkup 通知と linkdown 通知を受信して解釈するには、[Link Trap Query] チェックボックスをオンにします。

フィールド名	使用上のガイドライン
MAC トラップ クエリ（MAC Trap Query）	SNMP トラップを介して受信する MAC 通知を受信して解釈するには、[MAC トラップクエリ（MAC Trap Query）] チェックボックスをオンにします。
送信元ポリシー サービス ノード（Originating Policy Services Node）	[送信元ポリシーサービスノード（Originating Policy Services Node）] ドロップダウンリストから、SNMP データのポーリングに使用する Cisco ISE サーバーを選択します。このフィールドのデフォルト値は **[自動（Auto）]** です。ドロップダウンリストから特定の値を選択して、設定を上書きします。

高度な TrustSec 設定

次の表は、[高度なTrustSec設定（Advanced TrustSec Settings）] セクションのフィールドについて説明しています。

表 *5 : [*高度な *TrustSec* 設定（*Advanced TrustSec Settings*）*]* エリアのフィールド

フィールド名	使用上のガイドライン
デバイスの認証設定	
TrustSec ID にデバイス ID を使用（Use Device ID for TrustSec Identification）	[デバイスID（Device ID）] フィールドにデバイス ID としてデバイス名をリストするには、[TrustSec ID にデバイス ID を使用（Use Device ID for TrustSec Identification）] チェックボックスをオンにします。
デバイスID（Device ID）	このフィールドは、[TrustSec ID にデバイス ID を使用（Use Device ID for TrustSec Identification）] チェックボックスがオフになっている場合にのみ使用できます。
パスワード（Password）	Cisco TrustSec デバイスを認証するために Cisco TrustSec デバイスの CLI で設定したパスワードを入力します。 パスワードを表示するには、[表示（Show）] をクリックします。
HTTP REST API の設定	
HTTP REST API の有効化	HTTP REST API を使用して、ネットワークデバイスに必要な Cisco TrustSec 情報を提供するには、[HTTP REST API の有効化（Enable HTTP REST API）]チェックボックスをオンにします。これにより、効率性と能力が向上し、RADIUS プロトコルと比較して、短時間で大規模な設定をダウンロードできます。また、UDP を介した TCP を使用することで、信頼性が向上します。

フィールド名	使用上のガイドライン
Username	Cisco TrustSec デバイスを認証するために Cisco TrustSec デバイスの CLI で設定したユーザー名を入力します。ユーザー名にスペース、!%^:;、[{|}] ' "= <>? を含めることはできません
パスワード（**Password**）	Cisco TrustSec デバイスを認証するために Cisco TrustSec デバイスの CLI で設定したパスワードを入力します。
TrustSec デバイスの通知および更新	
デバイス**ID**（**Device ID**）	このフィールドは、[TrustSec ID にデバイス ID を使用（Use Device ID for TrustSec Identification）] チェックボックスがオフになっている場合にのみ使用できます。
パスワード（**Password**）	Cisco TrustSec デバイスを認証するために Cisco TrustSec デバイスの CLI で設定したパスワードを入力します。 パスワードを表示するには、[表示（Show）] をクリックします。
環境データのダウンロード間隔 <...>（**Download Environment Data Every <...>**）	このエリアのドロップダウンリストから必要な値を選択して、デバイスが Cisco ISE から環境データをダウンロードする必要がある時間間隔を指定します。時間を秒、分、時、日、または週で選択できます。デフォルト値は 1 日です。
ピア許可ポリシーのダウンロード間隔 <...>（**Download Peer Authorization Policy Every <...>**）	デバイスが Cisco ISE からピア認証ポリシーをダウンロードする必要がある時間間隔を、このエリアのドロップダウンリストから必要な値を選択して指定します。時間間隔を秒、分、時、日数、または週数で指定できます。デフォルト値は 1 日です。
再認証間隔 <...>（**Reauthentication Every <...>**）	このエリアのドロップダウンリストから必要な値を選択して、最初の認証後、デバイスが Cisco ISE に対して自身を再認証する時間間隔を指定します。時間間隔は秒、分、時、日、または週で設定できます。たとえば 1000 秒と入力すると、デバイスは 1000 秒ごとに Cisco ISE に対して自身を認証します。デフォルト値は 1 日です。
SGACL リストのダウンロード間隔 <...>（**Download SGACL Lists Every <...>**）	このエリアのドロップダウンリストから必要な値を選択して、デバイスが Cisco ISE から SGACL リストをダウンロードする時間間隔を指定します。時間間隔は秒、分、時、日、または週で設定できます。デフォルト値は 1 日です。

フィールド名	使用上のガイドライン
その他の TrustSec デバイスでこのデバイスを信頼する（信頼できる TrustSec）（Other TrustSec Devices to Trust This Device (TrustSec Trusted)）	すべてのピアデバイスがこの Cisco TrustSec デバイスを信頼できるようにするには、[このデバイスを信頼する他の TrustSec デバイス（Other TrustSec Devices to Trust This Device）] チェックボックスをオンにします。このチェックボックスをオフにした場合、ピアデバイスはこのデバイスを信頼せず、このデバイスから到着したすべてのパケットが適宜色付けまたはタグ付けされます。
設定変更のデバイスへの送信（Send Configuration Changes to Device）	Cisco ISE で CoA または CLI（SSH）を使用して Cisco TrustSec 構成変更を Cisco TrustSec デバイスに送信する場合は、[構成変更のデバイスへの送信（Send Configuration Changes to Device）] チェックボックスをオンにします。必要に応じて、[CoA] または [CLI（SSH）（CLI (SSH)）] オプションボタンをクリックします。 Cisco ISE で CoA を使用して設定変更を Cisco TrustSec デバイスに送信する場合は、[CoA] オプションボタンをクリックします。 Cisco ISE で CLI を使用（SSH 接続を使用）して設定変更を Cisco TrustSec デバイスに送信するには、[CLI（SSH）（CLI (SSH)）] オプションボタンをクリックします。詳細については、非 CoA サポート デバイスへの設定変更のプッシュを参照してください。
送信元（Send From）	ドロップダウンリストから、設定変更を Cisco TrustSec デバイスに送信する必要がある送信元 Cisco ISE ノードを選択します。PAN または PSN を選択できます。選択した PSN がダウンした場合、PSN を使用して Cisco TrustSec デバイスに設定変更が送信されます。
Test Connection	Cisco TrustSec デバイスと選択した Cisco ISE ノード（PAN または PSN ノード）の間の接続をテストするには、このオプションを使用できます。
SSH キー（SSH Key）	この機能を使用するには、Cisco ISE からネットワーク デバイスへの SSHv2 トンネルを開き、デバイスの CLI を使用して SSH キーを取得します。確認のために、このキーをコピーして [SSHキー（SSH Key）] フィールドに貼り付ける必要があります。詳細については、SSH キーの検証を参照してください。
デバイス構成の展開	

フィールド名	使用上のガイドライン
セキュリティ グループ タグ マッピングの展開時にこのデバイスを含める（**Include this device when deploying Security Group Tag Mapping Updates**）	Cisco TrustSec デバイスがデバイスインターフェイスのログイン情報を使用して IP-SGT マッピングを取得するには、[セキュリティ グループ タグ マッピングの更新の展開時にこのデバイスを含める（Include this device when deploying Security Group Tag Mapping Updates）] チェックボックスをオンにします。
EXEC モード ユーザー名（EXEC Mode Username）	Cisco TrustSec デバイスへのログインに使用するユーザー名を入力します。
EXEC モード パスワード（EXEC Mode Password）	デバイス パスワードを入力します。 パスワードを表示するには、**[表示（Show）]** をクリックします。 （注） セキュリティの脆弱性を回避するために、パスワード（EXEC モードやイネーブルモードのパスワードを含む）の文字に % を使用しないことを推奨します。
有効モード パスワード（Enable Mode Password）	（任意）特権 EXEC モードで Cisco TrustSec デバイスの設定を編集するために使用する有効なパスワードを入力します。 パスワードを表示するには、**[表示（Show）]** をクリックします。
アウトオブバンドTrustSec PAC	
発行日（Issue Date）	この Cisco TrustSec デバイス用に Cisco ISE によって生成された最後の Cisco TrustSec PAC の発行日を表示します。
期限日（Expiration Date）	この Cisco TrustSec デバイス用に Cisco ISE によって生成された最後の Cisco TrustSec PAC の期限日を表示します。
発行元（Issued By）	このデバイス用に Cisco ISE によって生成された最後の TrustSec PAC の発行者（Cisco TrustSec 管理者）の名前を表示します。
PAC の生成（Generate PAC）	Cisco TrustSec デバイスのアウトオブバンド Cisco TrustSec PAC を生成するには、[PACの生成（Generate PAC）] ボタンをクリックします。

デフォルトのネットワーク デバイス定義の設定

次の表では、Cisco ISE が RADIUS または TACACS+ 認証に使用できる、デフォルトのネットワークデバイスを設定できるようにする [デフォルトのネットワークデバイス（Default Network device）] ウィンドウのフィールドについて説明します。次のナビゲーションパスのいずれかを選択します。

- **[管理（Administration）] > [ネットワークリソース（Network Resources）] > [ネットワークデバイス（Network Devices）] > [デフォルトのデバイス（Default Devices）]**
- **[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [ネットワーク ソース（Network Resources）] > [デフォルトのデバイス（Default Devices）]**

表 *6 : [*デフォルトのネットワークデバイス（***Default Network Device***）*]* ウィンドウのフィールド

フィールド名	使用上のガイドライン
デフォルトのネットワーク デバイスのステータス（Default Network Device Status）	デフォルトのネットワークデバイスの定義を有効にするには、[デフォルトのネットワークデバイスのステータス（Default Network Device Status）] ドロップダウンリストから [有効化（Enable）] を選択します。 （注） デフォルトのデバイスが有効になっている場合は、ウィンドウ内の関連するチェックボックスをオンにすることで、RADIUS または TACACS+ の認証設定を有効にする必要があります。
デバイス プロファイル	デフォルトのデバイスベンダーとして [シスコ（Cisco）] が表示されます。
RADIUS 認証設定	
RADIUS の有効化	デバイスの RADIUS 認証を有効にするには、[RADIUS の有効化（Enable RADIUS）] チェックボックスをオンにします。
RADIUS UDP の設定	
共有秘密鍵（Shared Secret）	共有秘密を入力します。共有秘密情報の長さは、最大 127 文字です。 共有秘密鍵は、pac キーワードを指定した radius-host コマンドを使用してネットワークデバイスに設定したキーです。 （注） 共有秘密の長さは、[デバイスのセキュリティ設定（Device Security Settings）] ウィンドウ（**[管理（Administration）] > [ネットワークリソース（Network Resources）] > [ネットワークデバイス（Network Devices）] > [デバイスのセキュリティ設定（Device Security Settings）]**）の [RADIUS 共有秘密の最小長（Minimum RADIUS Shared Secret Length）] フィールドで設定された値と同等以上である必要があります。デフォルトでは、この値は新規インストールとアップグレードされた展開の場合は 4 文字です。RADIUS サーバーでのベストプラクティスは、22 文字にすることです。

フィールド名	使用上のガイドライン
RADIUS DTLS の設定	
必要な DTLS	[必要な DTLS（DTLS Required）] チェックボックスをオンにすると、Cisco ISE ではこのデバイスからの DTLS 要求のみが処理されます。このオプションを無効にすると、Cisco ISE ではこのデバイスからの UDP 要求と DTLS 要求の両方が処理されます。 RADIUS DTLS は SSL トンネルの確立および RADIUS の通信用に強化されたセキュリティを提供します。
共有秘密鍵（Shared Secret）	RADIUS DTLS に使用される共有秘密鍵が表示されます。この値は固定されており、MD5 整合性チェックを計算するために使用されます。
CoA の ISE 証明書の発行元 CA	RADIUS DTLS CoA に使用する認証局を [CoA の ISE 証明書の発行元 CA（Issuer CA of ISE Certificates for CoA）] ドロップダウンリストから選択します。
全般設定	
KeyWrap の有効化（Enable KeyWrap）	（任意）KeyWrap アルゴリズムがネットワークデバイスでサポートされている場合にのみ [KeyWrap の有効化（Enable KeyWrap）] チェックボックスをオンにします。これにより AES KeyWrap アルゴリズムを介した RADIUS のセキュリティが強化されます。
キー暗号キー（Key Encryption Key）	KeyWrap を有効にした場合は、セッションの暗号化（秘密）に使用する暗号キーを入力します。
メッセージ オーセンティケータ コード キー（Message Authenticator Code Key）	KeyWrap を有効にしているときに、RADIUS メッセージに対するキー付き Hashed Message Authentication Code（HMAC）の計算に使用されるキーを入力します。

フィールド名	使用上のガイドライン
キー入力形式（Key Input Format）	対応するオプションボタンをクリックして次のいずれかの形式を選択し、[キー暗号化キー（Key Encryption Key）] フィールドと [メッセージ認証コードキー（Message Authenticator Code Key）] フィールドに値を入力します。 • [ASCII]：**キー暗号化キー**の長さは 16 文字（バイト）、**メッセージ オーセンティケータ コード キー**の長さは 20 文字（バイト）である必要があります。 • [16 進数（Hexadecimal）]：キー暗号化キーの長さは 32 バイト、メッセージ オーセンティケータ コード キーの長さは 40 バイトである必要があります。 ネットワークデバイスの設定と一致するように、キー暗号キーおよびメッセージ認証コードキーの入力に使用するキー入力形式を指定します。指定する値はキーの正しい（全体の）長さにする必要があります。それよりも短い値は許可されません。
TACACS 認証設定	
共有秘密鍵（Shared Secret）	TACACS+ プロトコルが有効のときにネットワークデバイスに割り当てるテキスト文字列を入力します。ユーザーはネットワークデバイスによってユーザー名およびパスワードが認証される前にテキストを入力する必要があることに注意してください。ユーザーが共有秘密情報を提示するまで、接続は拒否されます。
廃止された共有秘密がアクティブです（Retired Shared Secret is Active）	リタイアメント期間がアクティブな場合に表示されます。
廃止（Retire）	既存の共有秘密を終了する代わりに廃止します。[廃止（Retire）] をクリックすると、ダイアログボックスが表示されます。[はい（Yes）] または [いいえ（No）] をクリックします。
残りの廃止期間（Remaining Retired Period）	（任意）[廃止（Retire）] ダイアログボックスで [はい（Yes）] をクリックした場合にのみ使用できます。**[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [設定（Settings）] > [接続設定（Connection Settings）] > [デフォルトの共有秘密リタイアメント期間（Default Shared Secret Retirement Period）]** ウィンドウで指定されたデフォルト値が表示されます。デフォルト値は変更することができます。 これにより、新しい共有秘密を入力できます。古い共有秘密は、指定された日数の間はアクティブなままになります。

フィールド名	使用上のガイドライン
終了（End）	（任意）[残りの廃止期間（Remaining Retired Period）] ダイアログボックスで [はい（Yes）] を選択した場合にのみ使用できます。廃止期間が終了し、古い共有秘密の設定は解除されます。
シングル接続モードを有効にする（Enable Single Connect Mode）	[シングル接続モードを有効にする（Enable Single Connect Mode）] チェックボックスは、ネットワークデバイスとのすべての TACACS+ 通信に単一の TCP 接続を使用する場合にオンにします。次のいずれかのオプションボタンをクリックします。 • **[レガシーシスコデバイス（Legacy Cisco Devices）]** • [TACACS ドラフト コンプライアンス シングル接続のサポート（TACACS Draft Compliance Single Connect Support）] （注） このフィールドを無効にすると、Cisco ISE はすべての TACACS+ 要求に新しい TCP 接続を使用します。

ネットワーク デバイスのインポート設定

次の表では、ネットワークデバイスの詳細を Cisco ISE にインポートするために使用できる [ネットワークデバイスのインポート（Import Network Devices）] ウィンドウのフィールドについて説明します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして選択します**[管理（Administration）]** > **[ネットワークリソース（Network Resources）]** > **[ネットワークデバイス（Network Devices）]**。[ネットワークデバイス（Network Devices）] ウィンドウで、[インポート（Import）] をクリックします。

表 *7:* ネットワークデバイスのインポート設定

フィールド名	使用上のガイドライン
テンプレートの生成（Generate a Template）	カンマ区切りの値（CSV）テンプレートファイルを作成するには、[テンプレートの生成（Generate a Template）] をクリックします。 CSV形式のネットワークデバイス情報でテンプレートを更新し、ローカルに保存します。次に、編集したテンプレートを使用して、Cisco ISE展開にネットワークデバイスをインポートします。
ファイル	最近作成したか、または Cisco ISE 展開から以前にエクスポートした CSV ファイルを選択するには、**[ファイルの選択（Choose File）]** をクリックします。 [インポート（Import）]オプションを使用して、新規および更新されたネットワークデバイスの情報を含む別の Cisco ISE 展開にネットワークデバイスをインポートできます。

フィールド名	使用上のガイドライン
新しいデータで既存のデータを上書き（Overwrite existing data with new data）	既存のネットワークデバイスをインポートファイル内のデバイスに置き換えるには、[既存のデータを新しいデータで上書き（Overwrite Existing Data with New Data）] チェックボックスをオンにします。 このチェックボックスをオンにしない場合、インポートファイル内の新しいネットワーク デバイス定義がネットワーク デバイス リポジトリに追加されます。重複エントリは無視されます。
最初のエラーでインポートを停止（Stop Import on First Error）	インポート時にエラーが発生したときに Cisco ISE にインポートを中止する場合は、[最初のエラー時にインポートを停止（Stop Import on First Error）] チェックボックスをオンにします。Cisco ISE は、エラーが発生するまでネットワークデバイスをインポートします。 このチェックボックスがオンになっておらず、エラーが発生した場合は、エラーが報告され、Cisco ISE は残りのデバイスを引き続きインポートします。

Cisco ISE でのネットワークデバイスの追加

Cisco ISE でネットワークデバイスを追加したり、デフォルトのネットワークデバイスを使用したりできます。

[ネットワークデバイス（Network Devices）]（**[ワークセンター（Work Centers）]** > **[デバイス管理（Device Administration）]** > **[ネットワークリソース（Network Resources）]** > **[ネットワークデバイス（Network Devices）]**）ウィンドウでもネットワークデバイスを追加できます。

始める前に

追加するネットワークデバイスで AAA 機能を有効にする必要があります。AAA 機能を有効にするコマンドを参照してください。

ステップ 1 Cisco ISE の GUI で、[メニュー（Menu）] アイコン（☰）をクリックし、次を選択します。**[管理（Administration）]** > **[ネットワークリソース（Network Resources）]** > **[ネットワークデバイス（Network Device）]**

ステップ 2 [Add] をクリックします。

ステップ 3 [名前（Name）]、[説明（Description）]、および [IP アドレス（IP Address）] の各フィールドに対応する値を入力します。

ステップ 4 [デバイスプロファイル（Device Profile）]、[モデル名（Model Name）]、[ソフトウェアバージョン（Software Version）]、および [ネットワーク デバイス グループ（Network Device Group）] ドロップダウンリストから必要な値を選択します。

ステップ 5 （任意）[RADIUS 認証設定（RADIUS Authentication Settings）] チェックボックスをオンにして、RADIUS プロトコル認証を設定します。

ステップ 6 （任意）[TACACS 認証設定（TACACS Authentication Settings）] チェックボックスをオンにして、TACACS プロトコル認証を設定します。

ステップ 7 （オプション）[SNMP の設定（SNMP Settings）] チェックボックスをオンにして、ネットワークデバイスから情報を収集するように Cisco ISE プロファイリングサービスに SNMP を設定します。

ステップ 8 （オプション）TrustSec 対応デバイスを設定するには [高度なTrustSec 設定（Advanced Trustsec Settings）] チェックボックスをオンにします。

ステップ 9 [送信（Submit）] をクリックします。

Cisco ISE へのネットワーク デバイスのインポート

Cisco ISE がネットワークデバイスと通信できるようにするには、Cisco ISE でネットワークデバイスのデバイス定義を追加する必要があります。[ネットワークデバイス（Network Devices）] ウィンドウ（メインメニューから、**[管理（Administration）]**>**[ネットワークリソース（Network Resources）]** > **[ネットワークデバイス（Network Devices）]**）で、ネットワークデバイスのデバイス定義を Cisco ISE にインポートします。

カンマ区切り形式（CSV）ファイルを使用して、Cisco ISE ノードにデバイス定義のリストをインポートします。**[ネットワークデバイス（Network Devices）]** ウィンドウで **[インポート（Import）]** をクリックすると、CSV テンプレートファイルを使用できます。このファイルをダウンロードし、必要なデバイス定義を入力してから、**[インポート（Import）]** ウィンドウで編集したファイルをアップロードします。

同じリソースタイプの複数のインポートを同時に実行できません。たとえば、2 つの異なるインポート ファイルから同時にネットワーク デバイスをインポートできません。

デバイス定義の CSV ファイルをインポートする場合、新しいレコードを作成するか、[既存のデータを新しいデータで上書きする（Overwrite Existing Data with New Data）] オプションをクリックして既存のレコードを更新できます。

インポートテンプレートは、Cisco ISE ごとに異なる場合があります。異なる Cisco ISE リリースからエクスポートしたネットワークデバイスの CSV ファイルをインポートしないでください。リリースの CSV テンプレートファイルにネットワークデバイスの詳細を入力し、このファイルを Cisco ISE にインポートします。

（注） すべてのオクテットで IP 範囲を持つネットワーク デバイスをインポートできます。

ステップ 1 Cisco ISE GUI で、[メニュー（Menu）] アイコン（☰）をクリックし、**[管理（Administration）]** > **[ネットワークリソース（Network Resources）]** > **[ネットワークデバイス（Network Device）]**。

ステップ 2 [Import] をクリックします。

ステップ 3 表示された **[ネットワークデバイスのインポート（Import Network Devices）]** ウィンドウで、**[テンプレートの生成（Generate A Template）]** をクリックして、編集可能な CSV ファイルをダウンロードし、必要な詳細情報とともに Cisco ISE にインポートします。

ステップ 4 [ファイルの選択（Choose Files）] をクリックして、クライアントブラウザを実行しているシステムから CSV ファイルを選択します。

ステップ 5 （オプション）必要に応じて、**[新しいデータで既存のデータを上書き（Overwrite Existing Data with New Data）]** および **[最初のエラーでインポートを停止（Stop Import on First Error）]** チェックボックスをオンにします。

ステップ 6 [インポート（Import）] をクリックします。

ファイルのインポートが完了すると、Cisco ISE には概要メッセージが表示されます。このメッセージには、インポートのステータス（成功または失敗）、発生したエラーの数（ある場合）、およびファイルインポートプロセスにかかった合計処理時間が含まれます。

Cisco ISE からのネットワーク デバイスのエクスポート

Cisco ISE ノードで使用可能なネットワークデバイスのデバイス定義を CSV ファイル形式でエクスポートします。その後、この CSV ファイルを別の Cisco ISE ノードにインポートして必要な Cisco ISE ノードでデバイス定義を使用できるようにします。

（注） すべてのオクテットで IP 範囲を持つネットワーク デバイスをエクスポートできます。

ステップ 1 Cisco ISE GUI で、[メニュー（Menu）] アイコン（☰）をクリックし、**[管理（Administration）]** > **[ネットワークリソース（Network Resources）]** > **[ネットワークデバイス（Network Device）]**。

ステップ 2 [Export] をクリックします。

ステップ 3 次のいずれかのアクションを実行して、Cisco ISE ノードに追加されたネットワークデバイスのデバイス定義をエクスポートします。

- エクスポートするデバイスの横にあるチェックボックスをオンにし、**[エクスポート（Export）]** ドロップダウンリストから **[選択済みをエクスポート（Export Selected）]** を選択します。
- **[エクスポート（Export）]** ドロップダウンリストから **[すべてエクスポート（Export All）]** を選択して、Cisco ISE ノードに追加されたすべてのネットワークデバイスをエクスポートします。

ステップ 4 どちらの場合も、デバイス定義の CSV ファイルがシステムにダウンロードされます。

ネットワーク デバイス設定の問題のトラブルシューティング

ステップ 1 Cisco ISE の GUI で、[メニュー（Menu）] アイコン（☰）をクリックし、**[操作（Operations）]** > **[トラブルシューティング（Troubleshoot）]** > **[診断ツール（Diagnostic Tools）]** > **[一般ツール（General Tools）]** > **[設定バリデータの評価（Evaluate Configuration Validator）]** 選択します。

ステップ 2 評価するネットワークデバイスの IP アドレスを、[Network Device IP] フィールドに入力します。

ステップ 3 チェックボックスをオンにして、推奨テンプレートと比較する設定オプションの横にあるオプションボタンをクリックします。

ステップ 4 [Run] をクリックします。

ステップ 5 [進行状況の詳細…（Progress Details ...）] 領域で、[ここをクリックしてログイン情報を入力（Click Here to Enter Credentials）] をクリックします。

ステップ 6 [Credentials Window] ダイアログボックスで、ネットワークデバイスとの接続を確立するために必要な接続パラメータとログイン情報を入力します。

ステップ 7 [Submit] をクリックします。`

ステップ 8 （オプション）ワークフローをキャンセルするには、[Progress Details ...] ウィンドウで [Click Here to Cancel the Running Workflow] をクリックします。

ステップ 9 （オプション）分析するインターフェイスの隣にあるチェックボックスをオンにして、[Submit] をクリックします。

ステップ 10 （オプション）設定の評価の詳細については、[Show Results Summary] をクリックします。

Network Device コマンド診断ツールの実行

Execute Network Device Command 診断ツールを使用すると、ネットワーク デバイスに対して **show** コマンドを実行することができます。

表示される結果は、コンソールに表示されるものと同じです。ツールにより、デバイス構成の問題（ある場合）を特定できます。

このツールは、ネットワークデバイスの構成を検証するか、またはネットワークデバイスの設定方法を確認する場合に使用します。

Execute Network Device Command 診断ツールにアクセスするには、次のナビゲーションパスのいずれかを選択します。

1. Cisco ISE GUI で、[メニュー（Menu）] アイコン（☰）をクリックし、**[操作（Operations）] > [トラブルシュート（Troubleshoot）] > [診断ツール（Diagnostic Tools）] > [ネットワークデバイスコマンドの実行（Execute Network Device Command）]** を選択します。Cisco ISE GUI で、[メニュー（Menu）] アイコン（☰）をクリックし、**[ワークセンター（Work Centers）] > [プロファイラ（Profiler）] > [トラブルシュート（Troubleshoot）] > [ネットワークデバイスコマンドの実行（Execute Network Device Command）]** を選択します。
2. 表示される **[ネットワークデバイスコマンドの実行（Execute Network Device Command）]** ウィンドウで、ネットワークデバイスの IP アドレスと実行する **show** コマンドを対応するフィールドに入力します。
3. [Run] をクリックします。

Cisco ISE でのサードパーティ ネットワーク デバイスのサポート

Cisco ISE は、ネットワーク デバイス プロファイルを使用して、サードパーティ製ネットワーク アクセスデバイス（NAD）をサポートします。NAD プロファイルは、ベンダー側の導入に関係なく、シンプルなポリシー構成でサードパーティデバイスの機能を定義します。ネットワーク デバイス プロファイルには、次のものが含まれています。

- RADIUS、TACACS+、Cisco TrustSec などの、ネットワークデバイスがサポートするプロトコル。ネットワークデバイスに存在するベンダー固有の RADIUS ディクショナリを Cisco ISE にインポートできます。
- デバイスが有線 MAB、802.1X などのさまざまな認証フローに使用する属性および値。これらの属性と値により、Cisco ISE は、ネットワークデバイスが使用する属性に従って、デバイスに適した認証フローを検出できます。
- ネットワークデバイスの認可変更（CoA）機能。RADIUS プロトコル RFC 5176 では CoA 要求が定義されていますが、CoA 要求で使用される属性はネットワークデバイスによって異なります。RFC 5176 対応のほとんどのシスコ以外のデバイスは、「プッシュ」および「切断」機能をサポートします。RADIUS CoA タイプをサポートしていないデバイスについては、Cisco ISE も SNMP CoA をサポートします。
- ネットワークデバイスが MAB フローに使用する属性およびプロトコル。さまざまなベンダーからのネットワーク デバイスは、MAB 認証を異なる方法で実行します。
- デバイスで使用される VLAN および ACL の権限。プロファイルを保存すると、Cisco ISE は設定された各権限に対し認証プロファイルを自動的に生成します。
- URL リダイレクション技術情報。URL リダイレクションは、個人所有デバイスの持ち込み（BYOD）、ゲストアクセス、ポスチャサービスなどの高度なフローに必要です。ネットワークデバイス内で見つかる URL リダイレクションには、静的と動的の 2 つのタイプがあります。静的 URL リダイレクションの場合は、Cisco ISE ポータル URL をコピーして構成に貼り付けることができます。動的 URL リダイレクションの場合、Cisco ISE は RADIUS 属性を使用して、リダイレクト先をネットワークデバイスに伝えます。

  ネットワークデバイスが動的および静的 URL リダイレクトのいずれもサポートしない場合、Cisco ISE は URL リダイレクトをシミュレートすることにより認証 VLAN 構成を提供します。認証 VLAN 構成は、Cisco ISE で実行されている DHCP および DNS サービスに基づいています。

Cisco ISE でネットワークデバイスを定義したら、これらのデバイスプロファイルを設定するか、Cisco ISE によって提供された事前設定済みデバイスプロファイルを使用して、Cisco ISE が基本認証フローや、プロファイラ、ゲスト、BYOD、MAB、ポスチャなどの高度なフローを有効にするために使用する機能を定義します。

URL リダイレクト メカニズムと認証 VLAN

ネットワークでサードパーティデバイスが使用されていて、デバイスがダイナミックまたはスタティック URL リダイレクトをサポートしていない場合、Cisco ISE が URL リダイレクトフローをシミュレートします。このようなデバイスの URL リダイレクト シミュレーション フローは、Cisco ISE で DHCP または DNS サービスを実行することによって動作します。

次に、認証 VLAN フローの例を示します。

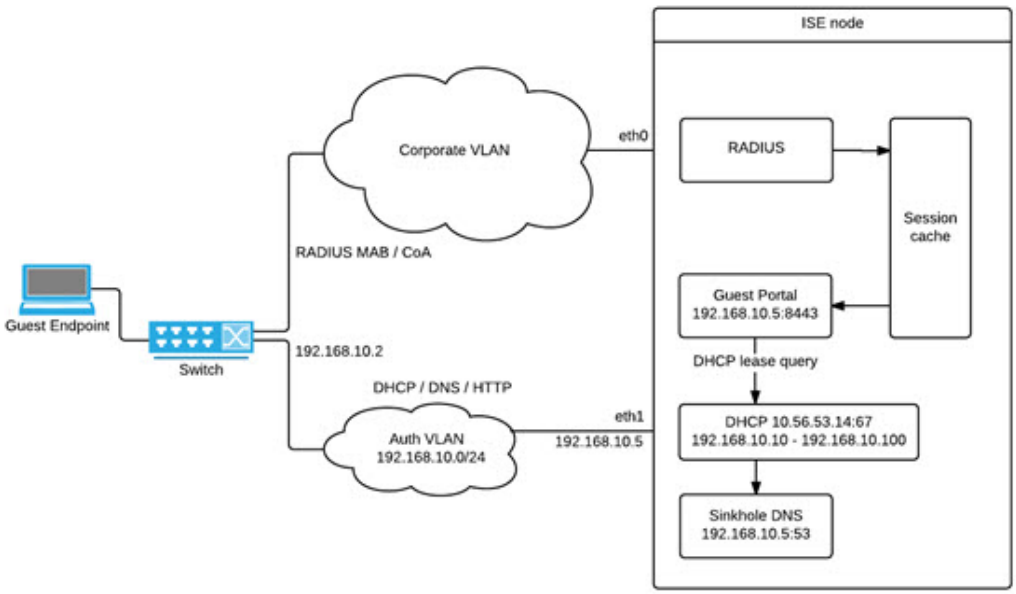
1. ゲスト エンドポイントが NAD に接続します。
2. ネットワークデバイスは、RADIUS 要求または MAB 要求を Cisco ISE に送信します。
3. ISE が認証ポリシーと許可ポリシーを実行し、ユーザーアカウンティング情報を保存します。
4. Cisco ISE が認証 VLAN ID を含む RADIUS アクセス承認メッセージを送信します。
5. ゲスト エンドポイントがネットワーク アクセスを受け取ります。
6. エンドポイントが DHCP 要求を送信し、Cisco ISE DHCP サービスからクライアント IP アドレスと Cisco ISE DNS シンクホール IP アドレスを取得します。
7. ゲストエンドポイントは、DNS クエリを送信して Cisco ISE IP アドレスを受け取るブラウザを開きます。
8. エンドポイントの HTTP 要求と HTTPS 要求は Cisco ISE に転送されます。
9. Cisco ISE は、ゲストポータル URL を含む **HTTP 301 Moved** メッセージで応答します。エンドポイントブラウザがゲストポータルウィンドウにリダイレクトされます。
10. ゲスト エンドポイント ユーザーが認証のためにログインします。
11. Cisco ISE はエンドポイントコンプライアンスを検証してから、NAD に応答します。Cisco ISE は CoA を送信し、エンドポイントを許可して、シンクホールをバイパスします。
12. ゲストユーザーは CoA に基づいて適切なアクセスを受け、エンドポイントが企業 DHCP から IP アドレスを受信します。これで、ゲストユーザーはネットワークを使用できます。

エンドポイントが認証を通過する前にゲストエンドポイントによって不正なネットワークアクセスが行われないように、認証 VLAN を企業のネットワークから分離することができます。認証 VLAN IP ヘルパーを設定して Cisco ISE マシンを示すか、いずれかの Cisco ISE ネットワーク インターフェイスを認証 VLAN に接続します。

NAD 設定から VLAN IP ヘルパーを設定することで、複数の VLAN を 1 つのネットワーク インターフェイス カードに接続することができます。IP ヘルパーの設定の詳細については、ネットワークデバイス用のアドミニストレーションガイドの指示を参照してください。IP ヘルパーを持つ VLAN を含むゲストアクセスフローの場合、ゲストポータルを定義し、MAB 許可にバインドされた認証プロファイルでそのポータルを選択します。ゲスト ポータルの詳細については、Cisco ISE ゲスト サービスを参照してください。

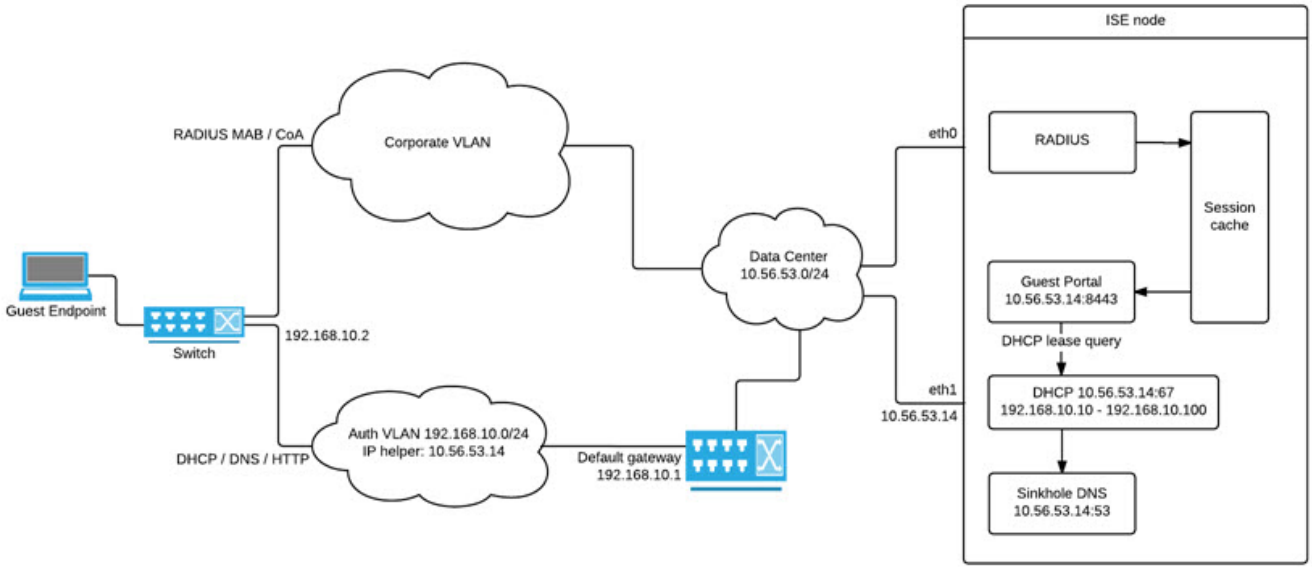
次の図に、認証 VLAN が定義されているときの基本的なネットワーク設定を示します（認証 VLAN が Cisco ISE ノードに直接接続されています）。

図 *1 : Cisco ISE* ノードに接続された認証 *VLAN*



次の図に、認証 VLAN と IP ヘルパーを備えたネットワークを示します。

図 *2 : IP* ヘルパーを備えた認証 *VLAN* 構成



CoA タイプ

Cisco ISE は、RADIUS と SNMP の両方の CoA タイプをサポートします。RADIUS または SNMP CoA タイプのサポートは、基本的なフローでは必須ではありませんが、NAD が複雑なフローで機能するために必要です。

Cisco ISE で NAD を設定するときに、ネットワークデバイスがサポートする RADIUS および SNMP 設定を定義します。NAD プロファイルを設定するときに、特定のフローに使用する CoA タイプを指定します。NAD のプロトコルの定義の詳細については、ネットワーク デバイス定義の設定 （3 ページ）を参照してください。Cisco ISE でデバイスと NAD のプロファイルを作成する前に、NAD でどの CoA タイプがサポートされているかをサードパーティサプライヤに確認してください。

ネットワーク デバイス プロファイル

Cisco ISE は、ネットワーク デバイス プロファイルを使用してサードパーティ製の NAD をサポートしています。これらのプロファイルによって、基本フローと、ゲスト、BYOD、MAB、ポスチャなどの高度なフローを有効にするために Cisco ISE が使用する機能が定義されます。

Cisco ISE には、いくつかのベンダーからのネットワーク デバイスの定義済みプロファイルが含まれています。Cisco ISE 2.1 以降のリリースは、次の表に記載されているネットワークデバイスでテストされています。

表 *8 : Cisco ISE 2.1* 以降のリリースでテスト済みのベンダーデバイス

デバイスタイプ	ベンダー	CoA タイプ	URL リダイレクト タイプ	サポートされる使用例または検証済みの使用例				
				802.1X フローと MAB フロー	CoA のないプロファイラ	CoA があるプロファイラ	ポスチャ（Posture）	ゲストと BYOD
ワイヤレス	Aruba 7000、InstantAP	RADIUS	スタティック URL	対応	対応	対応	対応	対応
	Motorola RFS 4000	RADIUS	ダイナミック URL	対応	対応	対応	対応	対応
	HP 830	RADIUS	スタティック URL	対応	対応	対応	対応	対応
	Ruckus ZD 1200	RADIUS	—	対応	対応	対応	対応	対応

有線	HP A5500	RADIUS	ISE が提供する認証 VLAN	対応	対応	対応	対応	対応
	HP 3800 および 2920 (ProCurve)	RADIUS	ISE が提供する認証 VLAN	対応	対応	対応	対応	対応
	Alcatel 6850	SNMP	ダイナミック URL	対応	対応	対応	対応	対応
	Brocade ICX 6610	RADIUS	ISE が提供する認証 VLAN	対応	対応	対応	対応	対応
	Juniper EX3300-24p	RADIUS	ISE が提供する認証 VLAN	対応	対応	対応	対応	対応
その他のサードパーティ製 NAD の場合は、デバイスのプロパティおよび機能を識別し、Cisco ISE でカスタム NAD プロファイルを作成する必要があります。				対応	対応	CoA サポートが必要	CoA サポートが必要です。 有線デバイスが URL リダイレクトをサポートしていない場合、Cisco ISE は認証 VLAN を使用します。ワイヤレス デバイスは認証 VLAN でテストされていません。	

定義済みプロファイルがないその他のサードパーティ製ネットワークデバイス用のカスタム NADプロファイルを作成する必要があります。ゲスト、BYOD、ポスチャなどの高度なワークフローについては、ネットワークデバイスは、これらのフローの CoA サポートに関連する RADIUS プロトコル RFC 5176をサポートしている必要があります。Cisco ISE でネットワークデバイスプロファイルを作成するために必要な属性については、デバイスのアドミニストレーション ガイドを参照してください。

ISE コミュニティ リソース

サードパーティ製NADプロファイルについては、「ISE Third-Party NAD Profiles and Configs」を参照してください。

Cisco ISE でのサードパーティ製ネットワークデバイスの設定

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

始める前に

ネットワーク デバイス プロファイル （27 ページ）を参照してください。

ステップ 1 Cisco ISE へサードパーティ製ネットワークデバイスを追加します（Cisco ISE へのネットワーク デバイスのインポート （21 ページ）を参照）。ゲスト、BYOD またはポスチャのワークフローを設定している場合、CoA が定義され、NAD の URL リダイレクトメカニズムが、関連する Cisco ISE ポータルをポイントするように設定されていることを確認します。URL リダイレクトを設定するには、ポータルのランディングページから Cisco ISE ポータルの URL をコピーします。Cisco ISE の NAD の CoA タイプと URL リダイレクトの設定に関する詳細については、ネットワーク デバイス定義の設定 （3 ページ）を参照してください。さらに、手順については、サードパーティデバイスのアドミニストレーション ガイドを参照してください。

ステップ 2 デバイスに適切な NAD プロファイルが Cisco ISE で利用できることを確認します。既存のプロファイルを表示するには、**[管理（Administration）]** > **[ネットワークリソース（Network Resources）]** > **[ネットワークデバイスプロファイル（Network Device Profiles）]** を選択します。適切なプロファイルが Cisco ISE に存在しない場合は、カスタムプロファイルを作成します。カスタム プロファイルの作成方法の詳細については、ネットワーク デバイス プロファイルの作成 （30 ページ）を参照してください。

ステップ 3 設定する NAD に NAD プロファイルを割り当てます。Cisco ISE の GUI で、[メニュー（Menu）] アイコン（☰）をクリックし、次を選択します。**[管理（Administration）]** > **[ネットワークリソース（Network Resources）]** > **[ネットワークデバイス（Network Device）]** プロファイルを割り当てるデバイスを開き、**[デバイスプロファイル（Device Profile）]** ドロップダウンリストから割り当てるプロファイルを選択します。

ステップ 4 ポリシールールを設定する場合は、許可プロファイルをステップ 1 で NAD プロファイルに設定します。または、VLAN または ACL を使用するだけの場合、あるいはネットワークに異なるベンダーからのさまざまなデバイスがある場合は、[Any] に設定します。許可プロファイルの NAD プロファイルを設定するには、**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[認証（Authorization）]** > **[許可プロファイル（Authorization Profiles）]** を選択します。関連する許可プロファイルを開き、[Network Device Profiles] ドロップダウンリストから関連する NAD プロファイルを選択します。ゲストフロー用に認証 VLAN を使用する場合、通常のゲストフローと同様に、ゲストポータルを定義し、MAB 認証にバインドされた認証プロファイルでそのポータルを選択する必要があります。ゲストポータルの詳細については、「Cisco ISE ゲストサービス」のセクションを参照してくださいCisco ISE ゲスト サービス を参照してください。

ネットワーク デバイス プロファイルの作成

始める前に

- ほとんどのNADには、標準のIETF RADIUS属性に加えてベンダー固有のいくつかの属性を提供する、ベンダー固有のRADIUSディクショナリが備わっています。ネットワークデバイスにベンダー固有のRADIUSディクショナリがある場合は、それをCisco ISEにインポートします。RADIUSディクショナリが必要な手順については、サードパーティ製デバイスの管理ガイドを参照してください。Cisco ISEのGUIで、[Menu]アイコン（☰）をクリックし、次を選択します。**[Policy]** > **[Policy Elements]** > **[Dictionaries]** > **[System]** > **[Radius]** > **[RADIUS Vendors]**。RADIUSディクショナリをインポートするには、RADIUSベンダー ディクショナリの作成を参照してください。
- ゲストやポスチャなどの複雑なフローの場合、ネットワークデバイスはRFC 5176で定義されているCoAタイプサポートしている必要があります
- ネットワークデバイスのプロファイルを作成するためのフィールドと可能な値の詳細については、ネットワーク デバイス プロファイル設定を参照してください。

ステップ1 Cisco ISE GUIで、[Menu]アイコン（☰）をクリックし、次を選択します。**[Administration]** > **[Network Resources]** > **[Network Device Profiles]**。

ステップ2 [追加（Add）]をクリックします。

ステップ3 表示される **[新しいネットワークデバイスのプロファイル（New Network Device Profile）]** ウィンドウで、ネットワークデバイスの **[名前（Name）]** フィールドと **[説明（Description）]** フィールドに対応する値を入力します。

ステップ4 **[ベンダー（Vendor）]** ドロップダウンリストから、ネットワークデバイスのベンダーを選択します。

ステップ5 **[アイコン（Icon）]** 領域で、**[アイコンの変更...（Change Icon ...）]** をクリックして、システムからネットワークデバイスのアイコンをアップロードします。

または、**[アイコン（Icon）]** 領域で **[デフォルトに設定（Set To Default）]** をクリックして、Cisco ISEが提供するデフォルトのアイコンを使用します。

ステップ6 **[サポートされているプロトコル（Supported Protocols）]** 領域で、デバイスがサポートするプロトコルのチェックボックスをオンにします。実際に使用するプロトコルのチェックボックスのみをオンにします。ネットワークデバイスがRADIUSプロトコルをサポートしている場合は、デバイスで使用するRADIUSディクショナリを **[RADIUSディクショナリ（RADIUS Dictionaries）]** ドロップダウンリストから選択します。

ステップ7 **[テンプレート（Templates）]** 領域で、関連する詳細情報を入力します。

a) **[認証/許可（Authentication/Authorization）]** をクリックし、フロータイプ、属性エイリアシング、およびホストルックアップに関するネットワークデバイスのデフォルト設定を行います。表示される新しい **[フロータイプ条件（Flow Type Conditions）]** 領域で、デバイスがさまざまな認証と許可フロー（有線MABや802.1Xなど）に使用する属性と値を入力します。これにより、Cisco ISEは使用される属性に従ってデバイスに適切なフロータイプを検出できます。MAB用のIETF標準がないため、ベンダーごとに異なる値が[サービスタイプ（Service Type）]に使用されています。正しい設定を判断する

には、デバイスのユーザーガイドを参照するか、またはMAB認証のスニファトレースを使用してください。[属性エイリアシング（Attribute Aliasing）] 領域で、デバイス固有の属性名を共通名にマップして、ポリシールールを簡素化します。現在、サービスセット識別子（SSID）のみが定義されています。ネットワークデバイスにワイヤレスSSIDの概念がある場合には、使用される属性に対してこれを設定します。Cisco ISE は、これを正規化された RADIUS ディクショナリの SSID という属性にマッピングします。これは、1 つのルール内で SSID を参照でき、基盤となる属性が異なっていても複数のデバイスで動作するので、ポリシールールの設定を簡素化します。**[ホストルックアップ（Host Lookup）]** 領域で、**[ホストルックアップの処理（Process Host Lookup）]** チェックボックスをオンにし、サードパーティ デバイス ベンダーが提供する指示に基づき、関連する MAB プロトコルと属性を選択します。

b) **[権限（Permissions）]** から、VLAN と ACL に関するネットワークデバイスのデフォルト設定を行います。これらは、Cisco ISE で作成した認証プロファイルに基づいて自動的にマッピングされます。

c) [Change of Authorization (CoA)] をクリックし、ネットワークデバイスの CoA 機能。

[CoA By] ドロップダウンリストから [RADIUS] を選択した場合は、表示される設定エリアで、スタティック属性のみを選択する必要があります。ダイナミック属性はサポートされていません。

d) **[リダイレクト（Redirect）]** をクリックし、ネットワークデバイスの URL リダイレクト機能を設定します。URL リダイレクションは、ゲスト、BYOD およびポスチャサービスに必要です。

ステップ 8 [Submit] をクリックします。

関連トピック

Cisco ISE ネットワーク アクセス デバイス プロファイルの作成方法

Cisco ISE からのネットワーク デバイス プロファイルのエクスポート

Cisco ISE で設定された単一または複数のネットワーク デバイス プロファイルを XML ファイルの形式でエクスポートします。XML ファイルを編集し、新しいネットワークプロファイルとして Cisco ISE ファイルにインポートできます。

始める前に

「How to Create ISE Network Access Device Profiles」を参照してください。

ステップ 1 Cisco ISE GUI で、[メニュー（Menu）] アイコン（☰）をクリックし、**[管理（Administration）]** > **[ネットワークリソース（Network Resources）]** > **[ネットワークデバイス（Network Device）]** を選択します。

ステップ 2 エクスポートするデバイスの横にあるチェックボックスをオンにし、[選択済みをエクスポート（Export Selected）] をクリックします。

ステップ 3 **DeviceProfiles.xml** という名前のファイルがローカルハードディスクにダウンロードされます。

Cisco ISE へのネットワーク デバイス プロファイルのインポート

Cisco ISE XML 構造を備えた単一の XML ファイルを使用して、Cisco ISE に単一または複数のネットワーク デバイス プロファイルをインポートします。複数のインポート ファイルから同時にネットワーク デバイス プロファイルをインポートすることはできません。

通常は、まずテンプレートとして使用するために Cisco ISE 管理者ポータルから既存のプロファイルをエクスポートする必要があります。デバイスプロファイルの詳細をファイルに入力し、XML ファイルとして保存します。次に、編集したファイルを Cisco ISE に再度インポートします。複数のネットワーク デバイス プロファイルを扱うには、単一の XML ファイルとして一緒に構造化された複数のプロファイルをエクスポートし、ファイルを編集してからプロファイルを一緒にインポートして、Cisco ISE で複数のプロファイルを作成します。

ネットワーク デバイス プロファイルのインポート時は、新しいレコードの作成のみができます。既存のプロファイルは上書きできません。既存のネットワーク デバイス プロファイルを更新するには、Cisco ISE から既存のプロファイルをエクスポートし、Cisco ISE からプロファイルを削除してから、必要に応じてプロファイルを編集した後にそのプロファイルをインポートします。

始める前に

「How to Create ISE Network Access Device Profiles」を参照してください。

ステップ 1 Cisco ISE GUI で、**[メニュー（Menu）]** アイコン（☰）をクリックし、**[管理（Administration）]** > **[ネットワークリソース（Network Resources）]** > **[ネットワークデバイスプロファイル（Network Device Profiles）]**。

ステップ 2 [Import] をクリックします。

ステップ 3 **[ファイルの選択（Choose Files）]** をクリックして、クライアントブラウザを実行しているシステムから XML ファイルを選択します。

ステップ 4 [Import] をクリックします。

ネットワーク デバイス グループの管理

次のウィンドウを使用すると、ネットワークデバイスグループを設定し、管理することができます。

ネットワーク デバイス グループの設定

次の表では、ネットワーク デバイス グループを作成するために使用する **[ネットワークデバイスグループ（Network Device Groups）]** ウィンドウのフィールドについて説明します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして選択します **[管理（Administration）]** > **[ネットワーク リソース（Network Resources）]** > **[ネットワーク デバイス グループ（Network Device Groups）]** > **[すべてのグループ（All Groups）]**。

ネットワーク デバイス グループは、**[ワークセンター（Work Centers）]**>**[デバイス管理（Device Administration）]** > **[ネットワークリソース（Network Resources）]** > **[ネットワーク デバイス グループ（Network Device Groups）]** > **[すべてのグループ（All Groups）]** ウィンドウでも作成できます。

表 *9 : [*ネットワーク デバイス グループ（***Network Device Group***）*]*ウィンドウのフィールド

フィールド名	使用上のガイドライン
名前（Name）	ルート ネットワーク デバイス グループの名前を入力します。このルート ネットワーク デバイス グループに追加される後続のすべての子ネットワーク デバイス グループに対して、新たに作成したこのネットワーク デバイス グループの名前を入力します。 ネットワーク デバイス グループ階層内には、ルートノードを含めて、最大で 6 つのノードを含めることができます。各ネットワーク デバイス グループの名前には最大で 32 文字を使用できます。
説明	ルートまたは子のネットワーク デバイス グループの説明を入力します。
ネットワークデバイスの数（No. of Network Devices）	ネットワークグループ内のネットワークデバイスの数がこの列に表示されます。

ネットワーク デバイス グループのインポート設定

次の表では、**[ネットワークデバイスグループ（Network Device Group）]** ウィンドウの **[インポート（Import）]** ダイアログボックスのフィールドについて説明します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして選択します**[管理（Administration）]** > **[ネットワークリソース（Network Resources）]** > **[ネットワーク デバイス グループ（Network Device Groups）]**。

表 *10 : [*ネットワーク デバイス グループのインポート（***Network Device Groups Import***）*]*ウィンドウのフィールド

フィールド名	使用上のガイドライン
テンプレートの生成（Generate a Template）	CSV テンプレートファイルをダウンロードするには、このリンクをクリックします。 同じ形式のネットワーク デバイス グループの情報でテンプレートを更新します。そのテンプレートをローカルに保存し、ネットワーク デバイス グループを Cisco ISE 展開にインポートします。

フィールド名	使用上のガイドライン
ファイル	**[ファイルの選択（Choose File）]** をクリックして、アップロードする CSV ファイルの場所に移動します。そのファイルは、新規ファイル、または別の Cisco ISE 展開からエクスポートされたファイルである可能性があります。 更新されたネットワーク デバイス グループ情報を使用して、ある Cisco ISE 展開から別の展開にネットワーク デバイス グループをインポートできます。
新しいデータで既存のデータを上書き（Overwrite existing data with new data）	既存のネットワーク デバイス グループをインポートファイル内のデバイスグループに置き換える場合は、このチェックボックスをオンにします。 このチェックボックスをオンにしない場合、インポートファイル内の新しいネットワーク デバイス グループのみがネットワーク デバイス グループ リポジトリに追加されます。重複エントリは無視されます。
最初のエラーでインポートを停止（Stop Import on First Error）	インポート時にエラーが発生した最初のインスタンスでインポートを中止するには、このチェックボックスをオンにします。 このチェックボックスをオンにしていないためにエラーが発生した場合は、Cisco ISE はエラーを報告し、残りのデバイスグループを引き続きインポートします。

ネットワーク デバイス グループ

Cisco ISE では、階層型ネットワーク デバイス グループ（NDG）を作成できます。ネットワーク デバイス グループを使用し、地理的な場所、デバイスタイプ、またはネットワーク内の相対的な位置（アクセスレイヤやデータセンターなど）に基づいて、ネットワークデバイスを論理的にグループ化します。

[ネットワーク デバイス グループ（Network Device Groups）] ウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックし、**[管理（Administration）]** > **[ネットワーク リソース（Network Resources）]** > **[ネットワーク デバイス グループ（Network Device Groups）]** を選択します。

たとえば、地理的な場所に基づいてネットワークデバイスを編成するには、大陸、地域、または国でグループ化します。

- **[アフリカ（Africa）]** > **[南部（Southern）]** > **[ナミビア（Namibia）]**
- **[アフリカ（Africa）]** > **[南部（Southern）]** > **[南アフリカ（South Africa）]**
- **[アフリカ（Africa）]** > **[南部（Southern）]** > **[ボツワナ（Botswana）]**

デバイスタイプに基づいてネットワークデバイスをグループ化します。

- **[アフリカ（Africa）] > [南部（Southern）] > [ボツワナ（Botswana）] > [ファイアウォール（Firewalls）]**
- **[アフリカ（Africa）] > [南部（Southern）] > [ボツワナ（Botswana）] > [ルータ（Routers）]**
- **[アフリカ（Africa）] > [南部（Southern）] > [ボツワナ（Botswana）] > [スイッチ（Switches）]**

ネットワークデバイスを 1 つ以上の階層型ネットワーク デバイス グループに割り当てます。Cisco ISE が、設定されたネットワーク デバイス グループの順序リストを処理して特定のデバイスに割り当てる適切なグループを決定する場合、同じデバイスプロファイルが複数のデバイスグループに適用されることがわかることがあります。この場合、Cisco ISE は最初に一致したデバイスグループを適用します。

作成できるネットワーク デバイス グループの最大数に制限はありません。ネットワーク デバイス グループの階層レベル（親グループを含む）は最大 6 レベルまで作成できます。

デバイスグループ階層は、[ツリーテーブル（Tree Table）] と [フラットテーブル（Flat Table）] の 2 つのビューに表示されます。ネットワーク デバイス グループのリストの上にある **[ツリーテーブル（Tree Table）]** または **[フラットテーブル（Flat Table）]** をクリックして、リストを対応するビューに編成します。

[ツリーテーブル（Tree Table）] ビューで、ルートノードはツリーの最上位に表示され、その後に子グループが階層順で続きます。各ルートグループのすべてのデバイスを表示するには、[すべて展開（Expand All）] をクリックします。ルートグループのみのリストを表示するには、[すべて折りたたむ（Collapse All）] をクリックします。

[フラットテーブル（Flat Table）] ビューでは、各デバイスグループの階層が [グループ階層（Group Hierarchy）] 列に表示されます。

両方のビューで、各子グループに割り当てられているネットワークデバイスの数が、対応する [ネットワークデバイスの数（No. of Network Devices）] 列に表示されます。デバイスグループに割り当てられているすべてのネットワークデバイスのリストを表示するダイアログボックスをクリックするには、この数字をクリックします。表示されるダイアログボックスには、ネットワークデバイスをあるグループから別のグループに移動するための 2 つのボタンも含まれています。現在のグループから別のグループにネットワークデバイスを移動するには、**[デバイスを別のグループに移動（Move Devices to Another Group）]** をクリックします。選択したネットワーク デバイス グループにネットワークデバイスを移動するには、**[デバイスをグループに追加（Add Devices to Group）]** をクリックします。

[ネットワークデバイスグループ（Network Device Groups）] ウィンドウでネットワーク デバイス グループを追加するには、**[追加（Add）]** をクリックします。**[親グループ（Parent Group）]** ドロップダウンリストで、ネットワーク デバイス グループを追加する必要がある親グループを選択するか、または **[ルートグループとして追加（Add As Root Group）]** オプションを選択して、新しいネットワーク デバイス グループを親グループとして追加します。

（注） デバイスが割り当てられているデバイス グループは削除できません。デバイスグループを削除する前に、すべての既存のデバイスを別のデバイスグループに移動する必要があります。

ルート ネットワーク デバイス グループ

Cisco ISE には、[すべてのデバイスタイプ（All Device Types）] と [すべてのロケーション（All Locations）] という 2 つの事前に定義されたルート ネットワーク デバイス グループが含まれています。これらの事前に定義されたネットワーク デバイス グループを編集、複製、または削除することはできませんが、それらの下に新しいデバイスグループを追加することはできます。

ルート ネットワーク デバイス グループ（ネットワーク デバイス グループ）を作成した後に、すでに説明したように、**[ネットワークデバイスグループ（Network Device Groups）]** ウィンドウでルートグループの下に子ネットワーク デバイス グループを作成できます。

ポリシー評価で Cisco ISE が使用するネットワークデバイスの属性

新しいネットワーク デバイス グループを作成すると、新しいネットワークデバイス属性が**システムディクショナリ（[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [ディクショナリ（Dictionaries）]**）内の**デバイス**ディクショナリに追加されます。追加されたデバイス属性は、ポリシー定義で使用されます。

Cisco ISE では、デバイスタイプ、ロケーション、モデル名、またはネットワークデバイス上で実行しているソフトウェアバージョンなどの**デバイス**ディクショナリ属性を使用して、認証ポリシーと許可ポリシーを設定できます。

Cisco ISE へのネットワーク デバイス グループのインポート

カンマ区切り形式（CSV）ファイルを使用して Cisco ISE ノードにネットワーク デバイス グループをインポートできます。2 つの異なるインポートファイルから同時にネットワーク デバイス グループをインポートできません。

Cisco ISE 管理者ポータルから CSV テンプレートをダウンロードします。そのテンプレートにネットワーク デバイス グループの詳細を入力して CSV ファイルとして保存した後、編集したファイルを Cisco ISE にインポートします。

デバイスグループのインポート中に、新しいレコードを作成するか、または既存のレコードを更新できます。デバイス グループをインポートする場合、Cisco ISE で最初のエラーが発生した場合、既存のデバイス グループを新しいグループで上書きするか、またはインポート プロセスを停止するかを定義できます。

ステップ 1 Cisco ISE の GUI で、[メニュー（Menu）] アイコン（☰）をクリックし、次を選択します**[管理（Administration）] > [ネットワークリソース（Network Resources）] > [ネットワーク デバイス グループ（Network Device Groups）]**。

ステップ 2 [Import] をクリックします。

ステップ 3 ダイアログボックスで、**[Choose Files]** をクリックし、クライアントブラウザを実行しているシステムから CSV ファイルを選択します。

ネットワーク デバイス グループを追加するための CSV テンプレートファイルをダウンロードするには、[テンプレートの生成（Generate a Template）] をクリックします。

ステップ 4 既存のネットワークデバイスグループを上書きするには、**[既存のデータを新しいデータで上書き（Overwrite Existing Data with New Data）]** チェックボックスをオンにします。

ステップ 5 [最初のエラーでインポートを停止（Stop Import on First Error）] チェックボックスをオンにします。

ステップ 6 [Import] をクリックします。

Cisco ISE からのネットワーク デバイス グループのエクスポート

Cisco ISE で設定されたネットワーク デバイス グループは、CSV ファイルの形式でエクスポートできます。その後で、これらのネットワーク デバイス グループを別の Cisco ISE ノードにインポートできます。

ステップ 1 Cisco ISE GUI で、[メニュー（Menu）] アイコン（☰）をクリックし、次を選択します。**[管理（Administration）]** > **[ネットワークリソース（Network Resources）]** > **[ネットワーク デバイス グループ（Network Device Groups）]** > **[すべてのグループ（All Groups）]**

ステップ 2 ネットワーク デバイス グループをエクスポートするには、次のいずれかを行うことができます。

- エクスポートするデバイスグループの横にあるチェックボックスをオンにし、**[エクスポート（Export）]** > **[選択済みをエクスポート（Export Selected）]** を選択します。
- **[エクスポート（Export）]** > **[すべてエクスポート（Export All）]** を選択して、定義されたネットワーク デバイス グループをすべてエクスポートします。

CSV ファイルがローカルハードディスクにダウンロードされます。

ネットワーク デバイス グループの管理

次のウィンドウを使用すると、ネットワークデバイスグループを設定し、管理することができます。

ネットワーク デバイス グループの設定

次の表では、ネットワーク デバイス グループを作成するために使用する **[ネットワークデバイスグループ（Network Device Groups）]** ウィンドウのフィールドについて説明します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして選択します **[管理（Administration）]** > **[ネットワーク リソース（Network Resources）]** > **[ネットワーク デバイス グループ（Network Device Groups）]** > **[すべてのグループ（All Groups）]**。

ネットワーク デバイス グループは、**[ワークセンター（Work Centers）]** > **[デバイス管理（Device Administration）]** > **[ネットワークリソース（Network Resources）]** > **[ネットワーク デバイス グループ（Network Device Groups）]** > **[すべてのグループ（All Groups）]** ウィンドウでも作成できます。

表 *11 : [*ネットワーク デバイス グループ（***Network Device Group***）*]*ウィンドウのフィールド

フィールド名	使用上のガイドライン
名前（**Name**）	ルート ネットワーク デバイス グループの名前を入力します。このルート ネットワーク デバイス グループに追加される後続のすべての子ネットワーク デバイス グループに対して、新たに作成したこのネットワーク デバイス グループの名前を入力します。 ネットワーク デバイス グループ階層内には、ルートノードを含めて、最大で 6 つのノードを含めることができます。各ネットワーク デバイス グループの名前には最大で 32 文字を使用できます。
説明	ルートまたは子のネットワーク デバイス グループの説明を入力します。
ネットワークデバイスの数（**No. of Network Devices**）	ネットワークグループ内のネットワークデバイスの数がこの列に表示されます。

ネットワーク デバイス グループのインポート設定

次の表では、**[ネットワークデバイスグループ（Network Device Group）]** ウィンドウの **[インポート（Import）]** ダイアログボックスのフィールドについて説明します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして選択します**[管理（Administration）]** > **[ネットワークリソース（Network Resources）]** > **[ネットワーク デバイス グループ（Network Device Groups）]**。

表 *12 : [*ネットワーク デバイス グループのインポート（***Network Device Groups Import***）*]*ウィンドウのフィールド

フィールド名	使用上のガイドライン
テンプレートの生成（**Generate a Template**）	CSVテンプレートファイルをダウンロードするには、このリンクをクリックします。 同じ形式のネットワーク デバイス グループの情報でテンプレートを更新します。そのテンプレートをローカルに保存し、ネットワーク デバイス グループを Cisco ISE 展開にインポートします。
ファイル	**[ファイルの選択（Choose File）]** をクリックして、アップロードする CSV ファイルの場所に移動します。そのファイルは、新規ファイル、または別の Cisco ISE 展開からエクスポートされたファイルである可能性があります。 更新されたネットワーク デバイス グループ情報を使用して、ある Cisco ISE展開から別の展開にネットワーク デバイス グループをインポートできます。

フィールド名	使用上のガイドライン
新しいデータで既存のデータを上書き（Overwrite existing data with new data）	既存のネットワーク デバイス グループをインポートファイル内のデバイスグループに置き換える場合は、このチェックボックスをオンにします。 このチェックボックスをオンにしない場合、インポートファイル内の新しいネットワーク デバイス グループのみがネットワーク デバイス グループ リポジトリに追加されます。重複エントリは無視されます。
最初のエラーでインポートを停止（Stop Import on First Error）	インポート時にエラーが発生した最初のインスタンスでインポートを中止するには、このチェックボックスをオンにします。 このチェックボックスをオンにしていないためにエラーが発生した場合は、Cisco ISE はエラーを報告し、残りのデバイスグループを引き続きインポートします。

Cisco ISE でのテンプレートのインポート

Cisco ISE では、CSV ファイルを使用して大量のネットワークデバイスやネットワーク デバイス グループをインポートできます。テンプレートには、フィールドのフォーマットを定義するヘッダー行が含まれます。次の表に記載されている列を追加する場合を除き、このヘッダー行は編集しないでください。

ネットワークデバイスやネットワーク デバイス グループに関連するインポートフロー内で [テンプレートの生成（Generate a Template）] リンクを使用して CSV ファイルをローカルシステムにダウンロードします。

ネットワーク デバイスのインポート テンプレート形式

次の表は、インポート ネットワーク デバイスの CSV テンプレートファイルのフィールドのリストと説明です。

表 *13 :* ネットワークデバイスの *CSV* テンプレートのフィールドと説明

フィールド	使用上のガイドライン
[名前（Name）]：文字列（32）	ネットワークデバイスの名前を入力します。name には、最大 32 字の英数字を指定できます。
Description:String(256)	（オプション）最大 256 文字でネットワークデバイスの説明を入力します。

フィールド	使用上のガイドライン
IP Address:Subnets（a.b.c.d/m|...）	ネットワークデバイスのIPアドレスおよびサブネットマスクを入力します。パイプ記号（|）で区切って複数の値を指定できます。 IPv4 および IPv6 アドレスは、ネットワークデバイス（TACACS および RADIUS）構成および外部 RADIUS サーバー構成でサポートされています。 IPv4 アドレスを入力する場合は、範囲とサブネットマスクを使用できます。
[モデル名（Model Name）]：**文字列（32）**	ネットワークデバイスの機種名を最大32文字で入力します。
[ソフトウェアバージョン（Software Version）]：**文字列（32）**	ネットワークデバイスのソフトウェアバージョンを最大32 文字で入力します。
[ネットワークデバイスグループ（Network Device Groups）]：**文字列（100）**	既存のネットワークデバイスグループの名前を入力します。サブグループの場合は、親グループとサブグループの両方をスペースで区切って含める必要があります。最大 100 文字の文字列（たとえば、*Location>All Location>US*）です。
Authentication:Protocol:String(6)	使用する認証プロトコルを入力します。有効な値は **RADIUS** のみです（大文字と小文字は区別されません）。
Authentication:Shared Secret:String(128)	（**[認証：プロトコル（Authentication:Protocol）]**：**文字列（6）**のフィールドの値を入力した場合に限り必須）最大 128 文字の文字列を入力します。
EnableKeyWrap：**ブール（true|false）**	このフィールドは、KeyWrap がネットワークデバイスでサポートされている場合に限り有効です。**true** または **false** を入力します。
EncryptionKey：**文字列（ascii:16|hexa:32）**	（KeyWrap を有効にした場合は必須）セッションの暗号化に使用される暗号キーを入力します。 ASCII 値：16 文字（バイト）の長さ。 16 進数値：32 文字（バイト）の長さ。
AuthenticationKey：**文字列（ascii:20|hexa:40）**	（KeyWrap を有効にした場合は必須）RADIUS メッセージに対するキー付きハッシュメッセージ認証コード（HMAC）の計算を入力します。 ASCII 値：20 文字（バイト）の長さ。 16 進数値：40 文字（バイト）の長さ。

フィールド	使用上のガイドライン
InputFormat：文字列（32）	暗号化キーと認証キーの入力形式を入力します。ASCII 値および 16 進数値を使用できます。
SNMP:Version：列挙（|2c|3）	プロファイラサービスが使用する必要のある SNMP プロトコルのバージョンを入力します（1、2c、または 3）。
SNMP:RO Community:String(32)	（**[SNMP**：**バージョン（SNMP:Version）]**：**列挙（|2c|3）**のフィールドに値を入力する場合は必須）。読み取り専用コミュニティの文字列を最大 32 文字で入力します
SNMP:RW Community:String(32)	（**[SNMP**：**バージョン（SNMP:Version）]**：**列挙（|2c|3）**のフィールドに値を入力する場合は必須）。読み取り書き込みコミュニティの文字列を最大 32 文字で入力します。
SNMP:Username:String(32)	最大 32 文字の文字列を入力します。
	（**[SNMP**：**バージョン（SNMP:Version）]**：**列挙（|2c|3）**のフィールドに SNMP バージョン 3 を入力した場合は必須）**[Auth]**、**[No Auth]**、または **[Priv]** を入力します。
SNMP:Authentication Protocol:Enumeration(MD5|SHA)	（SNMP セキュリティレベルで **[Auth]** または **[Priv]** を入力した場合は必須）**[MD5]** または **[SHA]** を入力します。
SNMP:Authentication Password:String(32)	（**[SNMP**：**セキュリティレベル（SNMP:Security Level）]**：**列挙（Auth|No Auth|Priv）**のフィールドに **[Auth]** を入力した場合は必須）最大 32 文字の文字列を入力します。
SNMP:Privacy Protocol:Enumeration(DES|AES128|AES192|AES256|3DES)	（**[SNMP**：**セキュリティレベル（SNMP:Security Level）]**：**列挙（Auth|No Auth|Priv）**のフィールドに **[Priv]** を入力した場合は必須）**[DES]**、**[AES128]**、**[AES192]**、**[AES256]**、または **[3DES]** を入力します。
SNMP:Privacy Password:String(32)	（**[SNMP**：**セキュリティレベル（SNMP:Security Level）]**：**列挙（Auth|No Auth|Priv）**のフィールドに **[Priv]** を入力した場合は必須）最大 32 文字の文字列を入力します。
SNMP:Polling Interval:Integer:600-86400 seconds	SNMP ポーリング間隔を秒単位で入力します。有効な値は 600 ー 86400 の整数です。
SNMP:Is Link Trap Query:Boolean(true|false)	**true** または **false** を入力して、SNMP リンクトラップを有効または無効にします。
SNMP:Is MAC Trap Query：ブール（**true|false**）	**true** または **false** を入力して、SNMP MAC トラップを有効または無効にします。

フィールド	使用上のガイドライン
SNMP:Originating Policy Services Node：文字列（**32**）	SNMP データのポーリングに使用される Cisco ISE サーバーを示します。デフォルトでは自動ですが、このフィールドに別の値を割り当てて設定を上書きできます。
Trustsec:Device Id：文字列（**32**）	Cisco Trustsec デバイス ID を、最大 32 文字の文字列で入力します。
Trustsec:Device Password：文字列（**256**）	（Cisco TrustSec デバイス ID を入力した場合は必須）Cisco TrustSec デバイスのパスワードを、最大 256 文字の文字列で入力します。
Trustsec:Environment Data Download Interval：整数：**1-2147040000 秒**	TrustSec 環境データのダウンロード間隔を入力します。有効な値は 1 ー 2147040000 の整数です。
Trustsec:Peer Authorization Policy Download Interval：整数：**1-2147040000 秒**	TrustSec のピア許可ポリシーのダウンロード間隔を入力します。有効な値は 1 ー 2147040000 の整数です。
Trustsec:Reauthentication Interval：整数：**1-2147040000 秒**	TrustSec の再認証間隔を入力します。有効な値は 1 ー 2147040000 の整数です。
Trustsec:SGACL List Download Interval：整数：**1-2147040000 秒**	Cisco TrustSec セキュリティグループ ACL リストのダウンロード間隔を入力します。有効な値は 1 ー 2147040000 の整数です。
Trustsec:Is Other Trustsec Devices Trusted：ブール（**true|false**）	**true** または **false** を入力して、Cisco TrustSec デバイスが信頼できるかどうかを示します。
Trustsec:Notify this device about Trustsec configuration changes：文字列（**ENABLE_ALL|DISABLE_ALL**）	**ENABLE_ALL** または **DISABLE_ALL** を入力して、Cisco TrustSec の構成変更を Cisco TrustSec デバイスに通知します。
Trustsec:Include this device when deploying Security Group Tag Mapping Updates：ブール（**true|false**）	**true** または **false** を入力して、Cisco TrustSec デバイスがセキュリティグループタグに含まれているかどうかを示します。
Deployment:Execution Mode Username:String(32)	ネットワークデバイス設定を編集する権限を持っているユーザー名を入力します。これは、最大32文字の文字列です。
Deployment:Execution Mode Password:String(32)	デバイスのパスワードを、最大32文字の文字列で入力します。

フィールド	使用上のガイドライン
Deployment:Enable Mode Password:String(32)	デバイスの構成を編集するためのデバイスのパスワードを入力します。これは、最大 32 文字の文字列です。
Trustsec:PAC issue date：日付	Cisco TrustSec デバイス用に Cisco ISE によって生成された最後の Cisco TrustSec PAC の発行日を入力します。
Trustsec:PAC expiration date：日付	Cisco TrustSec デバイス用に Cisco ISE によって生成された最後の Cisco TrustSec PAC の期限日を入力します。
Trustsec:PAC issued by：文字列	Cisco TrustSec デバイス用に Cisco ISE によって生成された最後の Cisco TrustSec PAC の発行者（Cisco TrustSec 管理者）の名前を入力します。文字列値である必要があります。

ネットワーク デバイス グループのインポート テンプレート形式

次の表に、テンプレート ヘッダーのフィールドとネットワーク デバイス グループの CSV ファイルにおけるこれらのフィールドの説明を示します。

表 *14*：ネットワーク デバイス グループの *CSV* テンプレートのフィールドと説明

フィールド	説明
Name：文字列（100）	（必須）このフィールドはネットワーク デバイス グループの名前です。最大 100 文字の文字列です。NDG の完全な名前の長さは、最大 100 文字です。たとえば、Global > Asia という親グループの下に India というサブグループを作成する場合、作成する NDG の完全な名前は Global#Asia#India になります。完全な名前の長さは、100 文字以内でなければなりません。NDG の完全な名前の長さが 100 文字を超えた場合、NDG の作成は失敗します。
Description:String(1024)	これはオプションのフィールドです。これは、最大 1024 文字の文字列です。
Type：文字列（64）	（必須）このフィールドはネットワーク デバイス グループのタイプです。これは、最大 64 文字の文字列です。
Is Root：ブール（true|false）	（必須）これは、特定のネットワーク デバイス グループがルート グループかどうかを示すフィールドです。有効な値は true または false です。

Cisco ISE と NAD 間の通信を保護する IPSec セキュリティ

IPSec は、IP にセキュリティを実装するプロトコルのセットです。AAA、RADIUS および TACACS+ のプロトコルは MD5 ハッシュアルゴリズムを使用します。セキュリティを強化するため、Cisco ISE には IPSec 機能があります。IPSec は、送信元を認証し、送信中のデータ変更を検出し、送信されたデータを暗号化することで通信を保護します。

Cisco ISE は、トンネルモードとトランスポートモードで IPSec をサポートしています。Cisco ISE インターフェイスで IPSec を有効にし、ピアを設定すると、通信を保護するため Cisco ISE と NAD の間に IPSec トンネルが作成されます。

事前共有キーを定義するか、または IPSec 認証に X.509 証明書を使用できます。IPSec は、ギガビット イーサネット 1 ~ 5 のインターフェイスで有効にできます。IPSec は PSN あたり 1 つの Cisco ISE インターフェイスでのみ設定できます。

スマートライセンスは、ギガビットイーサネット 2（e0/2—> eth2）インターフェイスではデフォルトで有効になっています。したがって、このインターフェイスで IP セキュリティを有効にする場合は、スマートライセンス用に別のインターフェイスを設定する必要があります。

（注） ギガビットイーサネット 0 とボンド 0（ギガビットイーサネット 0 と ギガビットイーサネット 1 インターフェイスがボンディングされている場合）は、Cisco ISE CLI の管理インターフェイスです。IPSec はギガビットイーサネット 0 と ボンド 0 ではサポートされていません。

IPSec は Cisco ISE リリース 2.2 以降でサポートされています。

Cisco ISE で IPSec を設定する際には、次の点に注意してください。

- IPSec は Cisco ISE リリース 2.2 以降でサポートされています。
- Cisco IOS ソフトウェア、C5921 ESR ソフトウェア（C5921_I86-UNIVERSALK9-M）：ESR 5921 構成では、デフォルトでトンネルモードとトランスポートモードで IPSec がサポートされています。Diffie-Hellman Group 14 および Group 16 がサポートされています。

（注） C5921 ESR ソフトウェアは Cisco ISE リリース 2.2 以降に付属しています。このソフトウェアを使用可能にするには ESR ライセンスが必要です。ESR ライセンスの情報については、『Cisco 5921 Embedded Services Router Integration Guide』を参照してください。

IPSec の設定、制限、およびサポートの詳細については、『Security Configuration Guide, Cisco IOS XE Cupertino 17.7.x (Catalyst 9300 Switches)』を参照してください。

Cisco ISE リリース 3.3 では、次の 2 つの方法を使って Cisco ISE PSN ノードで IPSec を設定できます。

- Cisco ISE でのネイティブ IPSec の設定

• Cisco ISE での RADIUS IPSec の設定

Cisco ISE でのネイティブ IPSec の設定

ネイティブ IPSec 設定を使用すると、IKEv1 および IKEv2 プロトコルを使用して、IPSec トンネルを介した Cisco ISE PSN と NAD 間のセキュリティ アソシエーションを確立できます。

（注）
- Cisco ISE の PSN 上の IPSec 設定と NAD の IPSec 設定が同じであることを確認します。

始める前に

Cisco ISE でネイティブ IPSec を設定するには、次の準備が必要です。

Cisco ISE で、次の手順を実行します。

- Cisco ISE Essentials ライセンスがあることを確認します。
- （オプション）[X.509 Certificates] オプションを使用している場合は、ネイティブ IPSec 接続を確立するすべての PSN の IPSec のシステム証明書をアップロードします。[System Certificates] ウィンドウの [IPSEC: Use certificate for Native IPSec] チェックボックスをオンにします。また、Cisco ISE IPSec システム証明書および NAD 証明書用の CA 証明書を信頼ストアにアップロードする必要があります。[Trusted Certificates] ウィンドウで、[CA IPSec Trusted Certificate] の [Trust for authentication within ISE] チェックボックスをオンにします。
- [Network Devices] ウィンドウで、特定の IP アドレスを持つ NAD を追加します。
- NAD で IPSec を設定します。Cisco ISE PSN と NAD の IPSec 設定は同じである必要があります。

ステップ 1 Cisco ISE GUI で、**[Administration]** にカーソルを合わせ、**[System]** > **[Settings]** > **[Protocols]** > **[IPSec]** > **[Native IPSec]**に移動します。

ステップ 2 [Add] をクリックして、Cisco ISE PSN と NAD 間のセキュリティ アソシエーションを設定します。

ステップ 3 [Node-Specific Settings] セクションで、次の詳細情報を入力します。

a) [Select Node] ドロップダウンリストから、必要な Cisco ISE PSN を選択します。
b) **[NAD IP Address with Mask]** フィールドに、対応する値を入力します。
c) [Default Gateway] フィールドに、対応する値を入力します。
d) **[Native IPSec Traffic Interface]** ドロップダウンリストから、必要なネイティブ IPSec トラフィック インターフェイスを選択します。

ステップ 4 [Authentication Settings] セクションでオプションボタンをクリックして、選択した Cisco ISE PSN ノードに対し、次の認証タイプのいずれかを選択します。

a) [Pre-shared Key]：このオプションを選択した場合は、事前共有キーを入力し、ネットワークデバイスで同じキーを設定する必要があります。事前共有キーには英数字を使用してください。特殊文字はサポートされていません。ネットワークデバイスで事前共有キーを設定する方法については、ネットワークデバイスのマニュアルを参照してください。事前共有キー設定の出力例については、例：Cisco Catalyst 3850 シリーズ スイッチでの事前共有キー設定の出力 （57 ページ）を参照してください。

b) [X.509 Certificates]：[X.509 Certificates] ドロップダウンリストから、IPSec トンネルに必要な X.509 証明書を選択します。

（注） [X.509 Certificates] オプションを選択する前に、必要な証明書（IPSec システム証明書および CA IPSec 信頼証明書）を設定してください。証明書には、SAN（サブジェクト代替名）拡張と DNS が含まれている必要があります。

相関するネイティブ IPSec 設定が行われた後に証明書が追加または変更された場合は、ネイティブ IPSec 設定を再度保存する必要があります。

ステップ 5 [General Settings] セクションで、以下の詳細を入力します。

a) [IKE Version] ドロップダウンリストから、必要な IKE バージョンを選択します。

b) [Mode] ドロップダウンリストから、必要なモードを選択します。

c) [ESP/AH Protocol] ドロップダウンリストから、必要なプロトコルを選択します。

d) （オプション）[IKE Reauth Time] フィールドに、対応する値を入力します。

[IKE Reauth Time] の値の範囲は 0 ～ 86,400 です。このフィールドに値 0 を入力すると、[IKE Reauth Time] フィールドを無効にできます。

ステップ 6 [Phase One Settings] セクションで、IKE セキュリティアソシエーション構成のセキュリティ設定を行うと、2つの IKE デーモン間の通信を保護できます。

a) [Encryption Algorithm] ドロップダウンリストから、必要な暗号化アルゴリズムを選択します。

b) [Hash Algorithm] ドロップダウンリストから、必要なハッシュアルゴリズムを選択します。

c) [DH Group] ドロップダウンリストから、必要な DH グループを選択します。

d) （オプション）[Re-key Time] フィールドに、対応する値を入力します。

[Re-key Time] の値の範囲は 0 ～ 86,400 です。このフィールドに値 0 を入力すると、[Re-key Time] フィールドを無効にできます。

ステップ 7 [Phase Two Settings] セクションでは、2 つのエンドポイント間の IP トラフィックを保護するために、ネイティブ IPSec セキュリティアソシエーション構成のセキュリティ設定を行えます。次の詳細を入力します。

a) [Encryption Algorithm] ドロップダウンリストから、必要な暗号化アルゴリズムを選択します。

b) [Hash Algorithm] ドロップダウンリストから、必要なハッシュアルゴリズムを選択します。

c) （オプション）[DH Group] ドロップダウンリストから、必要な DH グループを選択します。

d) （オプション）[Re-key Time] フィールドに、対応する値を入力します。

[Re-key Time] の値の範囲は 0 ～ 2,592,000 です。このフィールドに値 0 を入力すると、[Re-key Time] フィールドを無効にできます。

ステップ 8 [Save] をクリックして、選択した Cisco ISE PSN ノードでネイティブ IPSec をアクティブにします。

（注）
- ネイティブ IPSec の設定中に、複数の Cisco ISE インターフェイスを同じ IP サブネットに設定しないでください。
- 既存の IPSec トンネルインターフェイスで IP アドレスが変更された場合は、既存のトンネル設定を再度有効にして、IP アドレスの変更を反映する必要があります。
- IPSec トンネルの既存のインターフェイスがシャットダウンされた場合、そのトンネルの IPSec ステータスは、次のキー再生成または再認証が行われるまで、[Established] と表示されます。

Cisco ISE でのネイティブ IPSec 設定の表示と変更

[Native IPSec Configuration] ウィンドウのネイティブ IPSec 設定を使用して、Cisco ISE PSN と NAD の間に確立されたセキュリティ アソシエーションを追加、表示、編集、複製、無効化、および削除できます。

クイックフィルタを使用して、ネイティブ IPSec 設定をフィルタリングできます。

[Native IPSec Configuration] テーブルには、さらに列を追加できます。[Native IPSec Configuration] テーブルの右上にある歯車アイコンをクリックし、[Phase-one Encryption Algorithm]、[Phase-two Encryption Algorithm]、[Phase-one Hash Algorithm] などの列から希望する列を選択し、[Go] をクリックして、選択した列を [Native IPSec Configuration] テーブルに追加します。

（注） Cisco ISE 3.3 は、ネイティブ IPSec 設定で VTI をサポートしていません。

Cisco ISE での RADIUS IPSec の設定

Cisco ISE で RADIUS IPSec を設定するには、次の操作を行う必要があります。

ステップ 1 Cisco ISE CLI からインターフェイスで IP アドレスを設定します。

ギガビット イーサネット 1 からギガビット イーサネット 5 インターフェイス（ボンド 1 およびボンド 2）では、IPSec がサポートされています。ただし、IPsec は Cisco ISE ノードの 1 つのインターフェイスのみで設定できます。

ステップ 2 直接接続ネットワークデバイスを IPsec ネットワーク デバイス グループに追加します。

（注） RADIUS IPSec では、スタティック ルート ゲートウェイがデバイスのインターフェイスに直接接続している必要があります。

a) Cisco ISE の GUI で、[メニュー（Menu）] アイコン（☰）をクリックし、**[管理（Administration）]** > **[ネットワークリソース（Network Resources）]** > **[ネットワークデバイス（Network Device）]** を選択します。

b) [ネットワークデバイス（Network Devices）] ウィンドウで、[追加（Add）] をクリックします。
c) 追加するネットワークデバイスの名前、IP アドレス、およびサブネットを対応するフィールドに入力します。
d) [IPSEC] ドロップダウンリストから、[はい（Yes）] を選択します。
e) [RADIUS 認証設定（RADIUS Authentication Settings）] チェックボックスをオンにします。
f) [共有秘密（Shared Secret）] フィールドに、ネットワークデバイスに設定した共有秘密キーを入力します。
g) [Submit]> [Save] をクリックします。

ステップ 3 Cisco Smart Software Manager（CSSM）とのやりとりのために個別の管理インターフェイスを追加します。埋め込み型サービスルータ（ESR）の詳細については、Smart Software Manager サテライトを参照してください。このためには、Cisco ISE CLI から次のコマンドを実行し、対応する管理インターフェイス（ギガビット イーサネット 1 ～ 5（あるいはボンド 1 または 2）を選択します。

ise/admin# **license esr smart** {*interface*}

このインターフェイスは、Cisco.com に到達してシスコのオンライン ライセンス サーバーにアクセスできる必要があります。

既存のインターフェイスで ise/admin# **license esr smart** を無効にするには、次の手順を実行します。

- 新しい管理インターフェイスを追加します。
- Cisco ISE GUI で、[Administration] にカーソルを合わせ、**[System]** > **[Settings]** > **[Protocols]** > **[IPSec]** > **[Legacy IPSec (ESR)]** に移動します。 新しいインターフェイスで IPSec を有効または無効にします。

ステップ 4 Cisco ISE の CLI から、直接接続ゲートウェイにネットワークデバイスを追加します。

ip route [*destination network*] [*network mask*] **gateway** [*next-hop address*]

ステップ 5 Cisco ISE ノードで IPSec をアクティブにします。

a) Cisco ISE GUI で、[Administration] にカーソルを合わせ、**[System]** > **[Settings]** > **[Protocols]** > **[IPSec]** > **[Legacy IPSec (ESR)]** に移動します。

このウィンドウに展開内のすべての Cisco ISE ノードが表示されます。

b) IPSec を有効にする Cisco ISE ノードの横のチェックボックスをオンにして、[有効化（Enable）] オプション ボタンをクリックします。
c) [IPSec Interface for selected nodes] ドロップダウンリストから、IPSec 通信に使用するインターフェイスを選択します。
d) 選択した Cisco ISE ノードの次のいずれかの認証タイプのオプションボタンをクリックします。

- [事前共有キー（Pre-shared Key）]：このオプションを選択した場合は、事前共有キーを入力し、ネットワークデバイスで同じキーを設定する必要があります。事前共有キーには英数字を使用してください。特殊文字はサポートされていません。ネットワーク デバイスで事前共有キーを設定する方法については、ネットワーク デバイスのマニュアルを参照してください。事前共有キー設定の出力例については、例：Cisco Catalyst 3850 シリーズ スイッチでの事前共有キー設定の出力（57 ページ）を参照してください。

- [X.509 証明書（X.509 Certificates）]：このオプションを選択した場合は、Cisco ISE CLI から ESR シェルに進み、ESR 5921 の X.509 証明書を設定してインストールします。次に、ネットワーク デバイスで IPSec を設定します。この説明については、ESR-5921 での X.509 証明書の設定とインストール （51 ページ） を参照してください。

e) [保存（Save）] をクリックします。

（注） IPsec 設定を直接変更することはできません。IPSec が有効な場合に IPSec トンネルまたは認証を変更するには、現在の IPSec トンネルを無効にし、IPSec 設定を変更し、別の設定で IPSec トンネルを再度有効にします。

（注） IPsec が有効になると、Cisco ISE インターフェイスから IP アドレスが削除され、インターフェイスがシャットダウンします。ユーザーが Cisco ISE CLI からログインすると、インターフェイスが表示されますが IP アドレスは表示されず、シャットダウン状態になります。この IP アドレスは ESR-5921 インターフェイスで設定されます。

ステップ 6 **esr** と入力して ESR シェルを開始します。

```
ise/admin# esr
% Entering ESR 5921 shell
% Cisco IOS Software, C5921 Software (C5921_I86-UNIVERSALK9-M), Version 15.5(2)T2, RELEASE SOFTWARE
 (fc3)
% Technical Support: http://www.cisco.com/techsupport
% Copyright (c) 1986-2015 Cisco Systems, Inc.

Press RETURN to get started, CTRL-C to exit

ise-esr5921>
ise-esr5921>
```

（注） FIPS に準拠するため、8 文字以上のシークレットパスワードを設定する必要があります。**Enable secret level 1** コマンドを入力してパスワードを指定します。

```
ise-esr5921(config)#enable secret level 1 ?
0 Specifies an UNENCRYPTED password will follow
5 Specifies a MD5 HASHED secret will follow
8 Specifies a PBKDF2 HASHED secret will follow
9 Specifies a SCRYPT HASHED secret will follow
LINE The UNENCRYPTED (cleartext) 'enable' secret
```

（注） カスタム RADIUS ポートを GUI から設定する場合（1645、1646、1812、および 1813 以外）、ESR シェルで次の CLI コマンドを入力し、設定した RADIUS ポートを受け入れる必要があります。

```
ip nat inside source static udp 10.1.1.2 [port_number] interface Ethernet0/0 [port_number]
```

ステップ 7 IPSec トンネルと、IPSec トンネル経由での RADIUS 認証を検証します。

a) Cisco ISE にユーザーを追加し、そのユーザーをユーザーグループに割り当てます（Cisco ISE の GUI で、[メニュー（Menu）] アイコン（☰）をクリックし、次を選択します。**[管理（Administration）]** > **[ID 管理（Identity Management）]** > **[ID（Identities）]** > **[ユーザー（Users）]**）。

b) 次の手順を実行して、IPSec トンネルが Cisco ISE と NAD 間で確立されていることを確認します。

1. **ping**コマンドを使用して、Cisco ISE が NAD に接続されているかどうかをテストします。

2. ESR シェルまたは NAD の CLI から次のコマンドを実行して、接続がアクティブな状態であることを確認します。

show crypto isakmp sa

```
ise-esr5921#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
192.168.30.1    192.168.30.3    QM_IDLE           1001 ACTIVE
```

3. ESR シェルまたは NAD CLI から次のコマンドを実行して、トンネルが確立されているかどうかを確認します。

show crypto ipsec sa

```
ise-esr5921#show crypto ipsec sa

interface: Ethernet0/0
    Crypto map tag: radius, local addr 192.168.30.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.30.1/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (192.168.30.2/255.255.255.255/0/0)
   current_peer 192.168.30.2 port 500
     PERMIT, flags={}
    #pkts encaps: 52, #pkts encrypt: 52, #pkts digest: 52
    #pkts decaps: 57, #pkts decrypt: 57, #pkts verify: 57
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 192.168.30.1, remote crypto endpt.: 192.168.30.2
     plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
     current outbound spi: 0x393783B6(959939510)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0x8EA0F6EE(2392913646)
        transform: esp-aes esp-sha256-hmac ,
        in use settings ={Tunnel, }
        conn id: 99, flow_id: SW:99, sibling_flags 80000040, crypto map: radius
        sa timing: remaining key lifetime (k/sec): (4237963/2229)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x393783B6(959939510)
        transform: esp-aes esp-sha256-hmac ,
        in use settings ={Tunnel, }
        conn id: 100, flow_id: SW:100, sibling_flags 80000040, crypto map: radius
        sa timing: remaining key lifetime (k/sec): (4237970/2229)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     outbound ah sas:
```

```
outbound pcp sas:
```

c) 次のいずれかの方法で RADIUS 認証を検証します。

- ステップ 8（a）で作成したユーザーのクレデンシャルを使用してネットワーク デバイスにログインします。RADIUS 認証要求が Cisco ISE ノードに送信されます。[ライブ認証（Live Authentications）] ウィンドウに詳細を表示します。
- エンド ホストをネットワーク デバイスに接続し、802.1X 認証を設定します。ステップ 8（a）で作成したユーザーのクレデンシャルを使用してエンド ホストにログインします。RADIUS 認証要求が Cisco ISE ノードに送信されます。[ライブ認証（Live Authentications）] ウィンドウに詳細を表示します。

ESR-5921 での X.509 証明書の設定とインストール

ステップ 1 **esr** と入力して ESR シェルを開始します。

```
ise/admin# esr
% Entering ESR 5921 shell
% Cisco IOS Software, C5921 Software (C5921_I86-UNIVERSALK9-M), Version 15.5(2)T2, RELEASE SOFTWARE
 (fc3)
% Technical Support: http://www.cisco.com/techsupport
% Copyright (c) 1986-2015 Cisco Systems, Inc.

Press RETURN to get started, CTRL-C to exit

ise-esr5921>
ise-esr5921>
```

（注） FIPS に準拠するため、8 文字以上のシークレットパスワードを設定する必要があります。**Enable secret level 1** コマンドを入力してパスワードを指定します。

```
ise-esr5921(config)#enable secret level 1 ?
0 Specifies an UNENCRYPTED password will follow
5 Specifies a MD5 HASHED secret will follow
8 Specifies a PBKDF2 HASHED secret will follow
9 Specifies a SCRYPT HASHED secret will follow
LINE The UNENCRYPTED (cleartext) 'enable' secret
```

（注） カスタム RADIUS ポートを GUI から設定する場合（1645、1646、1812、および 1813 以外）、ESR シェルで次の CLI コマンドを入力し、設定した RADIUS ポートを受け入れます。

```
ip nat inside source static udp 10.1.1.2 [port_number] interface Ethernet0/0 [port_number]
```

ステップ 2 次のコマンドを使用して RSA キー ペアを生成します。

例：

```
crypto key generate rsa label rsa2048 exportable modulus 2048
```

ステップ 3 次のコマンドを使用して、トラストポイントを作成します。

例：

```
crypto pki trustpoint trustpoint-name

enrollment terminal
serial-number none
fqdn none
ip-address none
subject-name cn=networkdevicename.cisco.com
revocation-check none
rsakeypair rsa2048
```

ステップ 4 次のコマンドを使用して、証明書署名要求（CSR）を生成します。

例：

```
crypto pki enroll rsaca-mytrustpoint

Display Certificate Request to terminal? [yes/no]: yes
```

ステップ 5 証明書署名要求の出力をテキストファイルにコピーし、署名のために外部 CA に送信し、署名付き証明書と CA 証明書を取得します。

ステップ 6 次のコマンドを使用して、認証局（CA）証明書をインポートします。

例：

```
crypto pki authenticate rsaca-mytrustpoint
```

CA 証明書の内容（「**—BEGIN—**」行と「**—-End—**」行を含む）をコピーして貼り付けます。

ステップ 7 次のコマンドを使用して、署名付き証明書をインポートします。

例：

```
crypto pki import rsaca-mytrustpoint
```

署名付き証明書の内容（「**—BEGIN—**」行と「**—-End—**」行を含む）をコピーして貼り付けます。

次に、Cisco 5921 ESR で X.509 証明書を設定してインストールするときに表示される出力の例を示します。

```
ise-esr5921#show running-config
!
hostname ise-esr5921
!
boot-start-marker
boot host unix:default-config
boot-end-marker
!
no aaa new-model
bsd-client server url https://cloudsso.cisco.com/as/token.oauth2
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
call-home
! If contact email address in call-home is configured as sch-smart-licensing@cisco.com
! the email address configured in Cisco Smart License Portal will be used as contact email address
 to send SCH notifications.
contact-email-addr sch-smart-licensing@cisco.com
profile "CiscoTAC-1"
  active
  destination transport-method http
  no destination transport-method email
```

```
!
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
crypto pki trustpoint SLA-TrustPoint
enrollment pkcs12
revocation-check crl
!
crypto pki trustpoint rsaca-mytrustpoint
enrollment terminal
serial-number none
fqdn none
ip-address none
subject-name cn=ise-5921.cisco.com
revocation-check none
rsakeypair rsa2048
!
crypto pki certificate chain SLA-TrustPoint
certificate ca 01
  30820321 30820209 A0030201 02020101 300D0609 2A864886 F70D0101 0B050030
  32310E30 0C060355 040A1305 43697363 6F312030 1E060355 04031317 43697363
  6F204C69 63656E73 696E6720 526F6F74 20434130 1E170D31 33303533 30313934
  3834375A 170D3338 30353330 31393438 34375A30 32310E30 0C060355 040A1305
  43697363 6F312030 1E060355 04031317 43697363 6F204C69 63656E73 696E6720
  526F6F74 20434130 82012230 0D06092A 864886F7 0D010101 05000382 010F0030
  82010A02 82010100 A6BCBD96 131E05F7 145EA72C 2CD686E6 17222EA1 F1EFF64D
  CBB4C798 212AA147 C655D8D7 9471380D 8711441E 1AAF071A 9CAE6388 8A38E520
  1C394D78 462EF239 C659F715 B98C0A59 5BBB5CBD 0CFEBEA3 700A8BF7 D8F256EE
  4AA4E80D DB6FD1C9 60B1FD18 FFC69C96 6FA68957 A2617DE7 104FDC5F EA2956AC
  7390A3EB 2B5436AD C847A2C5 DAB553EB 69A9A535 58E9F3E3 C0BD23CF 58BD7188
  68E69491 20F320E7 948E71D7 AE3BCC84 F10684C7 4BC8E00F 539BA42B 42C68BB7
  C7479096 B4CB2D62 EA2F505D C7B062A4 6811D95B E8250FC4 5D5D5FB8 8F27D191
  C55F0D76 61F9A4CD 3D992327 A8BB03BD 4E6D7069 7CBADF8B DF5F4368 95135E44
  DFC7C6CF 04DD7FD1 02030100 01A34230 40300E06 03551D0F 0101FF04 04030201
  06300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604 1449DC85
  4B3D31E5 1B3E6A17 606AF333 3D3B4C73 E8300D06 092A8648 86F70D01 010B0500
  03820101 00507F24 D3932A66 86025D9F E838AE5C 6D4DF6B0 49631C78 240DA905
  604EDCDE FF4FED2B 77FC460E CD636FDB DD44681E 3A5673AB 9093D3B1 6C9E3D8B
  D98987BF E40CBD9E 1AECA0C2 2189BB5C 8FA85686 CD98B646 5575B146 8DFC66A8
  467A3DF4 4D565700 6ADF0F0D CF835015 3C04FF7C 21E878AC 11BA9CD2 55A9232C
  7CA7B7E6 C1AF74F6 152E99B7 B1FCF9BB E973DE7F 5BDDEB86 C71E3B49 1765308B
  5FB0DA06 B92AFE7F 494E8A9E 07B85737 F3A58BE1 1A48A229 C37C1E69 39F08678
  80DDCD16 D6BACECA EEBC7CF9 8428787B 35202CDC 60E4616A B623CDBD 230E3AFB
  418616A9 4093E049 4D10AB75 27E86F73 932E35B5 8862FDAE 0275156F 719BB2F0
  D697DF7F 28
        quit
crypto pki certificate chain rsaca-mytrustpoint
certificate 39
  30820386 3082026E A0030201 02020139 300D0609 2A864886 F70D0101 0B050030
  61310B30 09060355 04061302 5553310B 30090603 5504080C 024E4331 0C300A06
  03550407 0C035254 50310E30 0C060355 040A0C05 43495343 4F310C30 0A060355
  040B0C03 53544F31 19301706 03550403 0C107273 6163612E 65726368 616F2E63
  6F6D301E 170D3136 30393031 32313037 34335A17 0D313730 39303132 31303734
  335A301D 311B3019 06035504 03131269 73652D35 3932312E 63697363 6F2E636F
  6D308201 22300D06 092A8648 86F70D01 01010500 0382010F 00308201 0A028201
  0100EE87 CABFBA18 7E0405A8 ACAAAB23 E7CB6109 2CF98BAE 8EE93536 BF1EBBD3
  73E60BE7 F430B5AF EBF8B0C5 969B2828 A6783BB4 64E333E4 29C8744E 6E783617
  194AF1B0 7F04B4EA B89FD6EB F9C4F2DD 196DC6E0 CAA49B8B 665B6E0D 2FBC1D2F
  8E8181B9 60FAE126 D1B2E4E4 1F321A97 10C1B76A C2BB3174 361B13FA 2CB7BDFE
  22C0C33F 2792D714 C41E2237 00B1AE49 6593DCC3 A799D526 D81F9706 A71DA14E
  5ED76038 7A2C84B4 C668E35C 337BA1DC 9CA56AC2 C8E0059F 660CE39C 925310A0
  F9A21FFB 3C3C507A 20B924F7 E0125D60 6552321C 35736079 42449401 15E68DA6
```

```
  B4776DAA FB5AFDF8 59E31373 263175E3 1F14416A 24C21D69 A46173B6 96CC84FB
  5B9D0203 010001A3 818C3081 89300906 03551D13 04023000 302C0609 60864801
  86F84201 0D041F16 1D4F7065 6E53534C 2047656E 65726174 65642043 65727469
  66696361 7465301D 0603551D 0E041604 146DD31C 03690B98 330B67FA 6EDC7B20
  F99FB924 60301F06 03551D23 04183016 8014966A 0C21AF96 3E827690 423599CC
  EE8087A1 2909300E 0603551D 0F0101FF 04040302 05A0300D 06092A86 4886F70D
  01010B05 00038201 0100C0B9 D2845D97 6FFC16DB 01559659 BC1DECA6 E1A01965
  1F6CD459 E03D7ABE 91179FEB 08BF5B9B 84B62C36 236F528E E30C921C 81DA29E1
  EA3DFDC1 B0B0EEBA 14EADAEC 078576E4 D643A0EF 7D8E0880 C5FC3965 811B08C0
  5696DBF5 FADA4092 ACF549B8 2257F508 636D52AA 6CDC9596 AB43313F 6C33C9C1
  2CFDDBE3 EA9D407C 8D1B0F49 BBACD0CD 2832AC12 CD3FEFC8 501E1639 A4EFDC27
  69CA0147 971A1B2D DB2758E6 A84AFC86 4F9A4942 3D7EDBCC 7BDCC1BB 61F69B31
  BF13E39B 10AAC31C 55E73C8B C30BE516 7C506FF4 AC367D94 814A6880 EF201A6D
  CD2E1A95 7BBEC982 01CE867D 931F56E1 1EF1C457 9DC9A0BE 9DB2DC9B 19873585
  89AE82F6 A37E51D6 EECD
        quit
certificate ca 008DD3A81106B14664
  308203A2 3082028A A0030201 02020900 8DD3A811 06B14664 300D0609 2A864886
  F70D0101 05050030 61310B30 09060355 04061302 5553310B 30090603 5504080C
  024E4331 0C300A06 03550407 0C035254 50310E30 0C060355 040A0C05 43495343
  4F310C30 0A060355 040B0C03 53544F31 19301706 03550403 0C107273 6163612E
  65726368 616F2E63 6F6D301E 170D3135 31303231 32313135 34335A17 0D323531
  30313832 31313534 335A3061 310B3009 06035504 06130255 53310B30 09060355
  04080C02 4E43310C 300A0603 5504070C 03525450 310E300C 06035504 0A0C0543
  4953434F 310C300A 06035504 0B0C0353 544F3119 30170603 5504030C 10727361
  63612E65 72636861 6F2E636F 6D308201 22300D06 092A8648 86F70D01 01010500
  0382010F 00308201 0A028201 0100CB82 2AECEE38 1BCB27B9 FA5F2FBD 8609B190
  16A6F741 5BEC18B8 8B260CAF 190EA1CE 063BC558 556DC085 6FAC5425 14AFE225
  0E9E3A12 05F3DA7E D17E03F2 7FFE92FB 38D67027 DBC5C175 EB53E96B 66C20D11
  B4C32D38 AE04385C 8FD4CB74 31A97824 CA1CAFD5 091806C3 6F9CBF8D DC42DD5B
  D985703D F3BB9ED1 7DE99614 422D765C 86AB25CD E80008C5 22049BE8 66D1CA27
  E1EB6D4F 4FD3CC18 E091BBF0 6FE0EB52 B33F231A 6D6B7190 4196C929 D22E2C42
  B9CD2BBD 24550E82 8CD8838F C41B4DAD 2FA1636A 5787BBB2 F21E4718 335B005B
  DFBE6EA7 56EBE30B D52DE85F FFAF0189 E372CBFC 44BFF235 4DA7C9EF DAAC6D0A
  A196DA5A 1B525175 C26B3581 EA4B0203 010001A3 5D305B30 1D060355 1D0E0416
  0414966A 0C21AF96 3E827690 423599CC EE8087A1 2909301F 0603551D 23041830
  16801496 6A0C21AF 963E8276 90423599 CCEE8087 A1290930 0C060355 1D130405
  30030101 FF300B06 03551D0F 04040302 02A4300D 06092A86 4886F70D 01010505
  00038201 01002334 A3F0E5D3 4D229985 67A07754 73EC52E3 05B7D05F 926CC863
  220F849B 861C36B2 EF7C3485 474D4EF0 73895879 CAE08BBB 183B7CFA A20C4354
  86C6D9DF D445DACE C252C608 236F6673 F3F3C329 474B22E8 660BF91E 41054B8D
  43B80E44 AE69C164 2C9F41A2 8284F577 21FFAB8E A6771A5E DD34EBE4 A0DC2EAD
  95702010 02964566 478DA90F 5E134643 81A5F5EA 362D0394 1F9F23D1 DEE50B07
  12938299 1AF11A36 82DAFC6A 164B2F66 8B0AB7CC 9A723EBC B50E740B 0A9270E3
  60E2ED42 7F10D1A6 F6735144 AE93BF86 3D5A0502 6811D2BD 6E694693 28DE84C5
  3747CF0A D2B8D6C9 6CBEBA0A D1137CF8 E31CBF6B 437D82DD D74A4A9F 3557B3D9
  D0BD055F 65A8
        quit
license udi pid CISCO5921-K9 sn 9XG4481W768
username lab password 0 lab
!
redundancy
!
crypto keyring MVPN-spokes
rsa-pubkey address 0.0.0.0
  address 0.0.0.0
  key-string
  quit
!
crypto isakmp policy 10
encr aes
hash sha256
group 16
!
```

```
crypto isakmp policy 20
encr aes
hash sha256
group 14
crypto isakmp profile MVPN-profile
   description LAN-to-LAN for spoke router(s) connection
   keyring MVPN-spokes
   match identity address 0.0.0.0
!
crypto ipsec transform-set radius esp-aes esp-sha256-hmac
mode tunnel
crypto ipsec transform-set radius-2 esp-aes esp-sha256-hmac
mode transport
!
crypto dynamic-map MVPN-dynmap 10
set transform-set radius radius-2
!
crypto map radius 10 ipsec-isakmp dynamic MVPN-dynmap
!
interface Ethernet0/0
description e0/0->connection to external NAD
ip address 192.168.20.1 255.255.255.0
ip nat outside
ip virtual-reassembly in
no ip route-cache
crypto map radius
!
interface Ethernet0/1
description e0/1->tap0 internal connection to ISE
ip address 10.1.1.1 255.255.255.252
ip nat inside
ip virtual-reassembly in
no ip route-cache
!
interface Ethernet0/2
no ip address
shutdown
!
interface Ethernet0/3
no ip address
shutdown
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
ip nat inside source list 1 interface Ethernet0/0 overload
ip nat inside source static udp 10.1.1.2 1645 interface Ethernet0/0 1645
ip nat inside source static udp 10.1.1.2 1646 interface Ethernet0/0 1646
ip nat inside source static udp 10.1.1.2 1812 interface Ethernet0/0 1812
ip nat inside source static udp 10.1.1.2 1813 interface Ethernet0/0 1813
!
access-list 1 permit 10.1.1.0 0.0.0.3
!
control-plane
!
line con 0
logging synchronous
line aux 0
line vty 0 4
login
transport input none
!
end
```

次に、Cisco 3850 シリーズ スイッチで X.509 証明書を設定してインストールするときに表示される出力の例を示します。

```
cat3850#show running-config

enable password lab
!
username lab password 0 lab
aaa new-model

!

aaa group server radius ise
server name ise-vm
deadtime 60
!
aaa authentication login default group radius local

aaa authentication enable default group radius enable

!

crypto isakmp policy 10

encr aes

hash sha256
authentication rsa-sig
group 16
!
crypto ipsec security-association lifetime seconds 86400
!
crypto ipsec transform-set radius esp-aes esp-sha256-hmac
mode tunnel

!

crypto ipsec profile radius-profile

!

crypto map radius 10 ipsec-isakmp
set peer 192.168.20.1
set transform-set radius

match address 100

!

interface GigabitEthernet1/0/1
no switchport
ip address 192.168.20.2 255.255.255.0

crypto map radius

!
access-list 100 permit ip host 192.168.20.2 host 192.168.20.1
!
snmp-server community public RO
snmp-server community private RW
!
radius server rad-ise
address ipv4 192.168.20.1 auth-port 1645 acct-port 1646
```

```
key secret
```

例：Cisco Catalyst 3850 シリーズ スイッチでの事前共有キー設定の出力

次に、Cisco Catalyst 3850 シリーズ スイッチで事前共有キーを設定する場合に表示される出力の例を示します。

```
cat3850#show running-config

enable password lab
 !
 username lab password 0 lab
 aaa new-model
 !
 aaa group server radius ise
 server name ise-vm
 deadtime 60
 !
 aaa authentication login default group radius local

 aaa authentication enable default group radius enable

!

crypto isakmp policy 10

 encr aes

 hash sha256
 authentication pre-share
 group 16
 crypto isakmp key 123456789 address 0.0.0.0
 !
 crypto ipsec security-association lifetime seconds 86400
 !
 crypto ipsec transform-set radius esp-aes esp-sha256-hmac
 mode tunnel
 !
 crypto ipsec profile radius-profile
 !
 crypto map radius 10 ipsec-isakmp
 set peer 192.168.20.1
 set transform-set radius
 match address 100
!
interface GigabitEthernet1/0/1
 no switchport
 ip address 192.168.20.2 255.255.255.0

 crypto map radius
!
 access-list 100 permit ip host 192.168.20.2 host 192.168.20.1
 !
 snmp-server community public RO
 snmp-server community private RW
 !
 radius server rad-ise
 address ipv4 192.168.20.1 auth-port 1645 acct-port 1646

 key secret
```

Cisco ISE でのレガシー IPSec からネイティブ IPSec への移行

始める前に

Cisco ISE でレガシー IPSec からネイティブ IPSec に移行するには、次のものが必要です。

- レガシー IPSec（ESR）設定のバックアップ
- レガシー IPSec（ESR）のキーと証明書

ステップ 1 レガシー IPSec（ESR）の設定をバックアップします。

a) Cisco ISE CLI ESR シェルにログインし、実行中の設定をブートフラッシュのファイルに保存します。

b) SCP または FTP を使用して、その実行中の設定ファイルをコンピュータにエクスポートします。この保存した ESR 設定ファイルを ESR 設定のバックアップとして使用できます。

ステップ 2 IPSec の設定をエクスポートします。

a) レガシー IPSec（ESR）からキーと証明書をエクスポートします。Cisco ISE でのキーと証明書のエクスポートの詳細については、「Backup and Restoration of Cisco ISE CA Certificates and Keys」[英語] を参照してください。

b) Cisco ISE CLI ESR シェルから、**show runnning config** コマンドを実行し、実行中の設定と暗号化設定を表示します。

c) レガシー IPSec（ESR）で設定された暗号化設定を、表 15 : レガシー IPSec 設定とネイティブ IPSec 設定の比較：フェーズ 1 の設定 および 表 16 : レガシー IPSec 設定とネイティブ IPSec 設定の比較：フェーズ 2 の設定 に記載されている参照情報と比較します。

表 15 : レガシー IPSec 設定とネイティブ IPSec 設定の比較：フェーズ 1 の設定 および 表 16 : レガシー IPSec 設定とネイティブ IPSec 設定の比較：フェーズ 2 の設定 は、レガシー IPSec（ESR）の CLI コマンドと、Cisco ISE GUI のネイティブ IPSec 設定でのそれらに対応する内容との直接比較を示しています。レガシー IPSec（ESR）の設定情報を使用して、Cisco ISE でネイティブ IPSec を設定できます。

表 *15 :* レガシー *IPSec* 設定とネイティブ *IPSec* 設定の比較：フェーズ *1* の設定

レガシー IPSec（ESR）での show running config コマンド	Cisco ISE GUI でのネイティブ IPSec 設定

• **crypto isakmp policy 10**
• **encr aes**
• **hash sha256**
• **authentication pre-share**
• **group 14**
• **crypto isakmp key cisco123 address 0.0.0.0**
	• **Authentication Settings**: Pre-share
	• **Pre-share Key**: cisco123
	• **IKE Version**: IKEv1
	• **Phase-One Settings**
	  • **Encryption Algorithm**: AES-128
	  • **Hash Algorithm**: SHA-256
	  • **DH Group**: Group-14

表 *16 :* レガシー *IPSec* 設定とネイティブ *IPSec* 設定の比較：フェーズ *2* の設定

レガシー IPSec（ESR）での show running config コマンド	Cisco ISE GUI でのネイティブ IPSec 設定

• **crypto ipsec transform-set ipsec-ts esp-aes esp-sha256-hmac mode tunnel**
• **crypto map ipsec-crypto-map 10 ipsec-isakmp**
• **set peer 192.168.10.1**
• **set transform-set ipsec-ts**
• **set pfs group14**
• **match address 100**
	• **ESP/AH Protocol**: ESP
	• **Mode**: Tunnel
	• **Phase-Two Settings**
	  • **Encryption Algorithm**: AES-128
	  • **Hash Algorithm**: SHA-256
	  • **DH Group**: Group-14

ステップ 3 レガシー IPSec（ESR）を無効にします。

a) Cisco ISE GUI で、[Administration] にカーソルを合わせ、**[System]** > **[Settings]** > **[Protocols]** > **[IPSec]** > **[Legacy IPSec (ESR)]** に移動します。

b) チェックボックスをオンにして、レガシー IPSec（ESR）を無効にする必要がある Cisco ISE ノードを選択します。

c) [Enable/Disable IPSec for Selected Nodes] フィールドの [Disable] オプションボタンをクリックします。

これにより、選択したノードの IPSec が無効になり、Cisco ISE が再起動します。

d) Cisco ISE 管理 CLI から **ISE/admin#show esr status** コマンドを実行して、選択した Cisco ISE ノードの ESR ステータスが無効になっていることを確認します。次の出力が表示されます。

% ESR 5921 is disabled.

e) （オプション）Cisco ISE 管理 CLI から **ISE/admin#esr** コマンドを実行して、ESR シェルが無効になっているかどうかを確認します。

f) Cisco ISE 管理 CLI から **ISE/admin#show interface** コマンドを実行して、Cisco ISE インターフェイスで IP アドレスが復元されているかどうかを確認します。次の出力が表示されます。

GigabitEthernet 1 flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500 inet 192.168.10.11 netmask 255.255.255.0 broadcast 192.168.10.255 inet6 fe80::250:56ff:fe92:5f13 prefixlen 64 scopeid 0x20<link>.

ステップ 4 ネイティブ IPSec を有効化します。

a) Cisco ISE GUI で、**[Administration]** にカーソルを合わせ、**[Network Resources]** > **[Network Devices]**に移動します。

b) レガシー IPSec（ESR）の設定で以前に選択された NAD を、ネイティブ IPSec 設定でも選択します。

c) [Edit] をクリックして、NAD の IPSec の詳細を編集します。

d) [Network Device Group] セクションの [Legacy IPSEC (ESR)] ドロップダウンリストから、[No] を選択します。

e) [Save] をクリックします。

f) IKEv1 および IKEv2 プロトコルを使用して、IPSec トンネルを介して Cisco ISE PSN と選択した NAD 間のセキュリティ アソシエーションを確立するように、ネイティブ IPSec を設定します。ネイティブ

IPSec の設定方法の詳細については、Cisco ISE でのネイティブ IPSec の設定 （45 ページ）を参照してください。

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

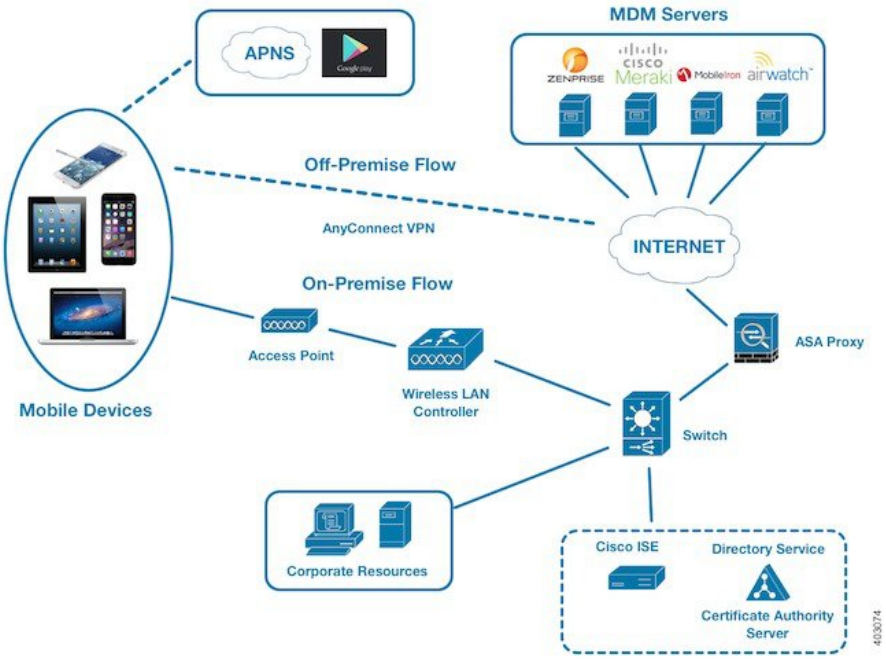
モバイルデバイス管理（MDM）サーバーはモバイル事業者、サービスプロバイダ、および企業に展開されたモバイルデバイスの保護、モニター、管理、およびサポートを行います。従来、MDM サーバーはモバイルデバイスのみをサポートしていました。一部の MDM サーバーは、ネットワーク内のすべてのタイプのデバイス（携帯電話、タブレット、ラップトップ、デスクトップ）を管理するようになり、統合エンドポイント管理（UEM）サーバーと呼ばれています。MDM サーバーはポリシーサーバーとして機能し、ポリシーサーバーは展開環境のモバイルデバイスにある一部のアプリケーション（電子メールアプリケーションなど）の使用を制御します。Cisco ISE は、ネットワーク認証ポリシーの作成に使用できるさまざまな属性に関する情報について、接続された MDM サーバーにクエリします。

さまざまなベンダーの複数のアクティブな MDM サーバーをネットワークで実行できます。これにより、ロケーションやデバイス タイプなどのデバイスの要因に基づいて、異なる MDM サーバーに異なるエンドポイントをルーティングすることができます。

また、Cisco ISE は、Cisco MDM Server Info API バージョン 2 以降を使用して MDM サーバーと統合し、Cisco AnyConnect 4.1 およびシスコの適応型セキュリティアプライアンス 9.3.2 以降を介して VPN 経由でデバイスがネットワークにアクセスできるようにします。

次の図では、Cisco ISE が適用ポイントで、MDM ポリシーサーバーがポリシー情報ポイントです。Cisco ISE は、MDM サーバーからデータを取得して、完全なソリューションを提供します。

図 *3 : MDM* の *Cisco ISE* との相互運用性



1 台以上の外部 MDM サーバーと相互運用するように Cisco ISE を設定します。サードパーティのこのタイプの接続を設定することによって、MDM データベースにある詳細情報を使用できます。Cisco ISE は REST API コールを使用して、外部 MDM サーバーから情報を取得します。Cisco ISE はスイッチ、アクセスルータ、ワイヤレスアクセスポイント、その他のネットワークアクセスポイントに適切なアクセス コントロール ポリシーを適用しています。ポリシーにより、Cisco ISE 対応ネットワークにアクセスしているリモートデバイスが強化されます。

Cisco ISE でサポートされる MDM ベンダーのリストについては、サポートされている統合エンドポイント管理およびモバイルデバイス管理サーバー （66 ページ）を参照してください。

サポートされているモバイルデバイス管理の使用例

Cisco ISE は外部 MDM サーバーを使用して次の機能を実行します。

- デバイス登録の管理：ネットワークにアクセスする未登録のエンドポイントは、MDM サーバー上でホストされている登録ページにリダイレクトされます。デバイス登録には、ユーザーロール、デバイスタイプなどが含まれます。
- デバイスの修復の処理：修復中のエンドポイントには制限付きアクセス権が付与されます。
- エンドポイントデータの増加：Cisco ISE プロファイリングサービスを使用して収集できない MDM サーバーの情報でエンドポイントデータベースを更新します。Cisco ISE では、[Endpoints] ページに表示できる複数のデバイス属性が使用されます。Cisco ISE の GUI で [メニュー（Menu）] アイコン（☰）をクリックし、次を選択します**[ワークセンター（Work**

Centers）] > **[ネットワークアクセス（Network Access）] > [ID（Identities）] > [エンドポイント（Endpoints）]**。

次に、使用可能なデバイス属性の例を示します。

- MDMImei: xx xxxxxx xxxxxx x
- MDMManufacturer: Apple
- MDMModel: iPhone
- MDMOSVersion: iOS 6.0.0
- MDMPhoneNumber: 5550100
- MDMSerialNumber: DNPGQZGUDTFx

- 4 時間に 1 回 MDM サーバーをポーリングし、デバイス コンプライアンス データを確認します。[External MDM Servers] ページでポーリング間隔を設定します。（このページを表示するには、[Menu] アイコン（☰）をクリックし、**[Work Centers]** > **[Network Access]** > **[Network Resources]** > **[External MDM Servers]** を選択します。）
- MDM サーバーを介したデバイス手順の発行：Cisco ISE は、MDM サーバーを介してユーザーのデバイスに対するリモートアクションを発行します。[Endpoints] ページを使用して、Cisco ISE 管理ポータルからリモートアクションを開始します。このページを表示するには、[Menu] アイコン（☰）をクリックし、**[Context Visibility]** > **[Endpoints]** を選択します。MDM サーバーの横にあるチェックボックスをオンにし、[MDM アクション（MDM Actions）] をクリックします。表示されるドロップダウンリストから必要なアクションを選択します。

ベンダー MDM 属性

Cisco ISE で MDM サーバーを設定すると、Cisco ISE は MDM サーバーにデバイス属性情報をクエリし、その情報を MDM システムディクショナリに追加します。次の属性は登録ステータスで使用され、MDM ベンダーで一般的にサポートされています。

Cisco ISE は API を使用して、MDM サーバーに必要なデバイス属性をクエリします。Cisco ISE リリース 3.1 以降のリリースでは、MDM API バージョン 3 がサポートされています。バージョン 3 の API には、MAC アドレスのランダム化を使用するエンドポイントを識別するのに役立つデバイス属性について、Cisco ISE が MDM サーバーにクエリを送信できる API が含まれています。Cisco ISE は MDM サーバーに次の属性をクエリします。

- GUID：MAC アドレスを使用してデバイスを識別する固有のデバイス識別子。
- MAC アドレス：UEM または MDM サーバーが特定のデバイス用に記録した MAC アドレスのリスト。1 つのデバイスで最大 5 つの MAC アドレスが共有されます。

MDM サーバーから必須属性の値が提供されない場合、Cisco ISE により次の表に示すデフォルト値が属性フィールドに入力されます。

表 *17 : MDM* 属性と値

属性名	属性ディクショナリ	デフォルト値	UEM または MDM サーバーから予期されるデータ	Microsoft SCCM サーバーから予期されるデータ
DaysSinceLastCheckin MDM API バージョン3以降でサポート	MDM	なし	ユーザーが UEM または MDM サーバーとデバイスを最後にチェックインまたは同期してからの日数。有効な範囲は 1 ～ 365 日です。	ユーザーが SCCM サーバーとデバイスを最後にチェックインまたは同期してからの日数。有効な範囲は 1 ～ 365 日です。
DeviceCompliantStatus	MDM	非準拠（NonCompliant）	[準拠（Compliant）] または [非準拠（NonCompliant）]。	[準拠（Compliant）] または [非準拠（NonCompliant）]。
DeviceRegisterStatus	MDM	UnRegistered	[登録済み（Registered）] または [未登録（UnRegistered）]。	[登録済み（Registered）] または [未登録（UnRegistered）]。
DiskEncryptionStatus	MDM	オフ	[オン（On）] または [オフ（Off）]。	[オン（On）] または [オフ（Off）]。
IMEI	MDM	なし	デバイスの IMEI 番号。	適用なし
JailBrokenStatus	MDM	完全（Unbroken）	[到達可能（Reachable）] または [到達不能（UnReachable）]。	[到達可能（Reachable）] または [到達不能（UnReachable）]。
MDMFailureReason	MDM	なし	デバイス障害の理由。	デバイス障害の理由。
MDMServerName	MDM	なし	サーバの名前。	サーバの名前。
MDMServerReachable	MDM	到達可能	[到達可能（Reachable）] または [到達不能（UnReachable）]。	[到達可能（Reachable）] または [到達不能（UnReachable）]。

属性名	属性ディクショナリ	デフォルト値	UEM または MDM サーバーから予期されるデータ	Microsoft SCCM サーバーから予期されるデータ
MEID	MDM	なし	デバイスの MEID 値。	適用なし
製造元	MDM	なし	デバイスの製造元の名前。	適用なし
モデル	MDM	なし	デバイスモデルの名前。	適用なし
OsVersion	MDM	なし	デバイスのオペレーティングシステムのバージョン。	適用なし
PhoneNumber	MDM	なし	デバイスの電話番号。	適用なし
PinLockStatus	MDM	オフ	[オン（On）] または [オフ（Off）]。	適用なし
SerialNumber	MDM	なし	デバイスのシリアル番号。	適用なし
server-type	MDM	なし	Mobile Device Manager サーバーの MDM。 デスクトップ デバイス マネージャ サーバーの DM。	デスクトップ デバイス マネージャ サーバーの DM。
[UDID]	MDM	なし	デバイスの UDID 番号。	適用なし
UserNotified	MDM	なし	[あり（Yes）] または [なし（No）]	適用なし

属性名	属性ディクショナリ	デフォルト値	UEM または MDM サーバーから予期されるデータ	Microsoft SCCM サーバーから予期されるデータ
GUID MDM API バージョン3以降でサポート	ディクショナリ属性ではない	なし	GUID は、デバイスの MAC アドレス、UDID、MEID、または IMEI 値の代わりにデバイスを識別するために使用される固有のデバイス識別子です。GUID テンプレートは GUIDMDMMDNameValue です。 GUID 値は、Cisco ISE ではなく MDM サーバーによって生成されて提供されます。	適用なし
Macaddresses MDM API バージョン3以降でサポート	ディクショナリ属性ではない	なし	UEM または MDM サーバーが特定のデバイス用に記録した MAC アドレスのリスト。1 つのデバイスで最大 5 つの MAC アドレスを共有できます。 Macaddresses 値は、Cisco ISE ではなく、MDM サーバーによって生成されて提供されます。	適用なし

ベンダー固有の属性はサポートされていませんが、ERS API を使用してベンダー固有の属性を交換できる場合があります。サポートされている ERS API については、ベンダーのマニュアルを参照してください。

新しい MDM ディクショナリ属性は認証ポリシーで使用可能です。

サポートされている統合エンドポイント管理およびモバイルデバイス管理サーバー

サポートされる MDM サーバーは、次のベンダーの製品です。

- Absolute
- Blackberry：BES
- Blackberry：Good Secure EMM
- Cisco Meraki Systems Manager
- Citrix XenMobile 10.x（オンプレミス）
- Globo
- IBM MaaS360
- Ivanti（旧 MobileIron UEM）、コアおよびクラウド UEM サービス

  Cisco ISE 3.1 におけるランダムおよび変更 MAC アドレスの処理に関するユースケースでは、MobileIron Core 11.3.0.0 ビルド 24 以降のリリースを統合し、GUID 値を受け取る必要があります。

（注） 一部のバージョンの MobileIron は Cisco ISE では動作しません。MobileIron はこの問題を認識しており、修正があります。詳細については、MobileIron 社までお問い合わせください。

- JAMF Casper Suite
- Microsoft Endpoint Configuration Manager
- Microsoft Endpoint Manager Intune
- Mosyle
- SAP Afaria
- Sophos
- SOTI MobiControl
- Symantec
- Tangoe
- VMware Workspace ONE（以前の AirWatch）
- 42Gears

サーバーを Cisco ISE と統合するためにエンドポイント管理サーバーで実行する必要がある設定については、「Integrate UEM and MDM Servers With Cisco ISE」を参照してください。

ISE コミュニティ リソース

How To: Meraki EMM / MDM Integration with ISE

モバイルデバイス管理サーバーで使用されるポート

次の表に、相互に通信ができるように Cisco ISE と MDM サーバー間で開く必要のあるポートを示します。MDM エージェントとサーバーで開く必要があるポートのリストについては、MDM ベンダーのドキュメントを参照してください。

表 *18 : MDM* サーバーにより使用されるポート

MDM サーバー	ポート
MobileIron	443
Citrix XenMobile 10.x（オンプレミス）	443
Blackberry：Good Secure EMM	19005
VMware Workspace ONE（以前の AirWatch）	443
SAP Afaria	443
IBM MaaS360	443
Cisco Meraki	443
Microsoft Intune	80 および 443
Microsoft SCCM	80 および 443

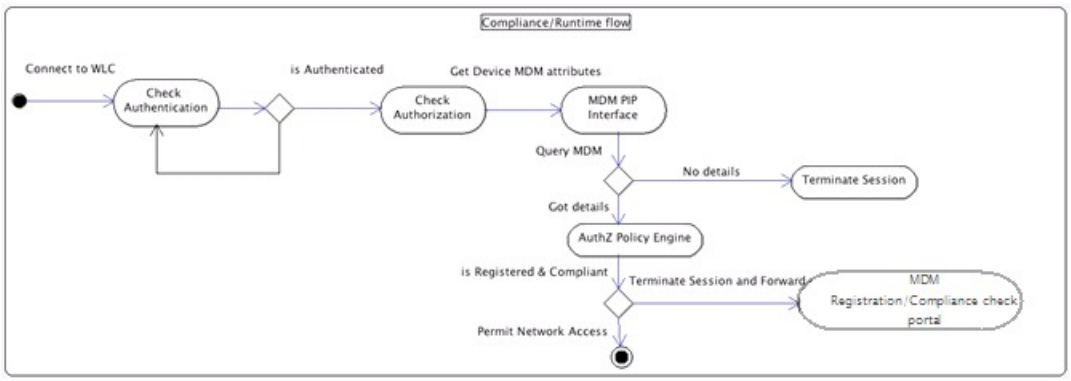
モバイルデバイス管理の統合プロセスフロー

1. ユーザーはデバイスを SSID に関連付けます。
2. Cisco ISE は、MDM サーバーに対して API コールを実行します。
3. この API コールは、ユーザーのデバイスとデバイスのポスチャステータスのリストを戻します。

（注） 入力パラメータは、エンドポイントデバイスのMACアドレスです。オフプレミスのAppleiOSデバイス（VPN 経由で Cisco ISE に接続するデバイス）の場合、入力パラメータは UDID です。

4. ユーザーのデバイスがこのリストにない場合、デバイスが登録されていないことを意味します。Cisco ISE は、Cisco ISE にリダイレクトされる許可要求を NAD に送信します。ユーザーが MDM サーバーページに表示されます。
5. Cisco ISE は、MDM を使用してデバイスをプロビジョニングし、デバイスを登録するための適切なウィンドウをユーザーに表示します。
6. ユーザーは MDM サーバーにデバイスを登録し、MDM サーバーは自動リダイレクションまたは手動のブラウザリフレッシュによってCisco ISEに要求をリダイレクトします。
7. Cisco ISE はMDM サーバーに対して再度ポスチャ ステータスのクエリーを実行します。
8. ユーザーのデバイスが MDM サーバーで設定されているポスチャ（コンプライアンス）ポリシーに準拠していない場合、デバイスがポリシーに準拠していないことがユーザーに通知されます。ユーザーは、デバイスがポリシーに準拠していることを確認するために必要なアクションを実行する必要があります。
9. ユーザーのデバイスがポリシーに準拠すると、MDM のサーバーは内部テーブルのデバイスのステータスを更新します。
10. ここでユーザーがブラウザをリフレッシュすると、制御が Cisco ISE に返されます。
11. Cisco ISE はコンプライアンス情報を取得するために MDM サーバーを 4 時間ごとにポーリングし、適切な認可変更（CoA）を発行します。ポーリング間隔を設定できます。また、Cisco ISE は 5 分ごとに MDM サーバーをチェックして使用できるかどうかを確認します。

図 *4 : Cisco ISE* での *MDM* プロセスフロー



（注） 一度に 1 つの MDM サーバーに登録できるデバイスは 1 台のみです。別のベンダーから MDM サービスに同じデバイスを登録する場合、デバイスから前のベンダーのプロファイルを削除する必要があります。MDM サービスは通常、「企業ワイプ」を提供し、これはデバイスからベンダーの設定のみを削除します（デバイス全体ではありません）。ユーザーはこのファイルを削除することもできます。たとえば、iOS デバイスで、**[Settings]** > **[General]** > **[Device management]** ウィンドウの順に移動し、[Remove Management] をクリックすることができます。または、Cisco ISE の MyDevices ポータルに移動し、[企業ワイプ（Corporate Wipe）] をクリックすることができます。

モバイルデバイス管理サーバーを使用した、ランダムで変化するMAC アドレスの処理

ランダムで変化する MAC アドレスの使用に起因する問題を回避するために、MAC アドレスではなく一意のデバイス識別子を使用して MDM サーバーに接続されているエンドポイントを識別するように Cisco ISE を設定します。プライバシー対策として、モバイルデバイスでは接続先の SSID ごとにランダムおよび変更 MAC アドレスを使用することが増えています。一部のデスクトップ オペレーティング システムは、ユーザーが定期的に MAC アドレスをランダム化する機能も提供しています。これは、エンドポイントから MDM サーバーと Cisco ISE に異なる MAC アドレスが提示されることを意味します。その結果、MDM サーバーと Cisco ISE が統合され、エンドポイントに対してアクションが開始されると、2 つのシステムでエンドポイント ID が異なるために問題が発生します。

この問題を回避するために、MAC アドレスではなく固有のデバイス識別子を使用するように Cisco ISE を設定できます。エンドポイントが MDM サーバーに登録されると、GUID 値を含む証明書が MDM サーバーからエンドポイントに送信されます。エンドポイントでは、Cisco ISE での認証にこの証明書が使用されます。Cisco ISE は、証明書からエンドポイントの GUID を受信します。Cisco ISE と MDM サーバー間のすべての通信で、GUID を使用してエンドポイントが識別され、2 つのシステム間の精度と一貫性が確保されます。

GUID は、証明書ベースの認証方式でのみ使用できることに注意してください。SAN URI または CN フィールドに GUID を含めるには、MDM または UEM サーバーによって発行された証明書を設定する必要があります。GUID の SAN URI フィールドを設定することを推奨します。Active Directory に接続されたエンドポイントの認証に同じ証明書が使用される場合、CN フィールドに GUID が存在すると問題が発生する可能性があります。

ユーザー名とパスワードのみを使用する基本認証方式では、GUID ベースのソリューションを利用できません。

EAP-TLS プロトコルを介した MAC アドレスと GUID によるエンドポイントの再認証の場合、コンテキスト可視性サービスを更新するための 1 秒あたりのトランザクション（TPS）は、1 秒あたり 12 ～ 15 エンドポイントです。

GUID データの収集と管理を容易にするために、Cisco ISE MDM API（Cisco ISE MDM API バージョン3）が更新されました。

接続された MDM サーバーの GUID の設定

Cisco ISE にすでに接続している MDM サーバーが最新の Cisco ISE MDM API をサポートし、GUID 情報を送信できるかどうかを確認するには、次の手順を実行します。

1. Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして選択します **[管理（Administration）]>[ネットワークリソース（Network Resources）]>[外部 MDM（External MDM）]** を選択します。
2. [MDM サーバー（MDM Servers）] ウィンドウで、更新する MDM サーバーのチェックボックスをオンにし、[編集（Edit）] をクリックします。
3. [Test Connection] をクリックします。
4. MDM サーバーが Cisco ISE MDM API バージョン 3 をサポートしている場合は、[デバイス識別子（Device Identifiers）] という新しいセクションが表示されます。

   次のオプションのうち有効にする 1 つ以上のチェックボックスをオンにします。

   - **[証明書：SAN URI、GUID（Cert - SAN URI, GUID）]**
   - **[証明書：CN、GUID（Cert - CN, GUID）]**
   - **[レガシー MAC アドレス（Legacy MAC Address）]**

   オプションをドラッグアンドドロップして、優先順に並べ替えることができます。たとえば、[Cert - SAN URI, GUID] を最初に配置し、次に [Cert - CN, GUID] を配置すると、Cisco ISE は最初にエンドポイントの SAN URI 属性と GUID 属性について MDM サーバーにクエリします。要求された属性が使用できない場合、Cisco ISE はエンドポイントの共通名と GUID 属性をクエリします。
5. [Save] をクリックします。

pxGrid による GUID の共有

Cisco ISE は、pxGrid を介してこの GUID 情報を他のシスコのソリューションと共有できます。たとえば、MDM サーバーから受信した GUID は、pxGrid トピックを使用して展開内の Catalyst Center と共有できます。

Cisco ISE によるモバイルデバイス管理サーバーのセットアップ

Cisco ISE で MDM サーバーを設定するには、次の高レベル タスクを実行します。

ステップ 1 Azure にポリシー管理ノード（PAN）の証明書をインポートする Intune を除き、Cisco ISE に MDM のサーバー証明書をインポートします。

ステップ 2 Mobile Device Manager の定義を作成します。

ステップ 3 Cisco WLC で ACL を設定します。

ステップ 4 MDM サーバーに未登録のデバイスをリダイレクトする認証プロファイルを設定します。

ステップ 5 ネットワークに複数の MDM サーバーがある場合は、ベンダーごとに個別の認証プロファイルを設定します。

ステップ 6 MDM 使用例の許可ポリシー ルールを設定します。

Cisco ISE へのモバイルデバイス管理サーバー証明書のインポート

Cisco ISE を MDM サーバーに接続するには、Cisco ISE 信頼できる証明書ストアに MDM サーバー証明書をインポートする必要があります。MDM サーバーに CA 署名付き証明書がある場合は、Cisco ISE 信頼できる証明書ストアにルート証明書をインポートする必要があります。

（注） Microsoft Azure の場合は、Cisco ISE 証明書を Azure にインポートします。「Cisco ISE へのモバイルデバイス管理サーバーとしての Microsoft Intune の接続」を参照してください。

ステップ 1 MDM サーバー証明書を MDM サーバーからエクスポートして、ローカル マシンに保存します。

ステップ 2 Cisco ISE GUI で、[メニュー（Menu）] アイコン（☰）をクリックし、**[管理（Administration）]** > **[システム（System）]** > **[証明書（Certificates）]** > **[信頼できる証明書（Trusted Certificates）]** > **[インポート（Import）]** を選択します。

ステップ 3 [証明書ストアへの新しい証明書のインポート（Import a new Certificate into the Certificate Store）] ウィンドウで、**[ファイルの選択（Choose File）]** をクリックして、MDM サーバーから取得した MDM サーバー証明書を選択します。

ステップ 4 [フレンドリ名（Friendly Name）] フィールドに証明書の名前を入力します。

ステップ 5 [ISE 内の認証用に信頼する（Trust for authentication within ISE）] チェックボックスをオンにします。

ステップ 6 [送信（Submit）] をクリックします。

ステップ 7 [証明書ストア（Certificate Store）] ウィンドウに新たに追加した MDM サーバー証明書のリストが表示されることを確認します。

Cisco ISE でのデバイス管理サーバーの定義

Cisco ISE が必要なサーバーと通信できるように、Cisco ISE でモバイルデバイス管理サーバーとデスクトップデバイス管理サーバーを定義します。サーバーとの通信に使用される認証タイプ、Cisco ISE がデバイス管理サーバーのデバイス情報を要求する頻度などを設定できます。

モバイル管理サーバーを定義するには、Cisco ISE でのモバイルデバイス管理サーバーの設定（72 ページ）を参照してください。

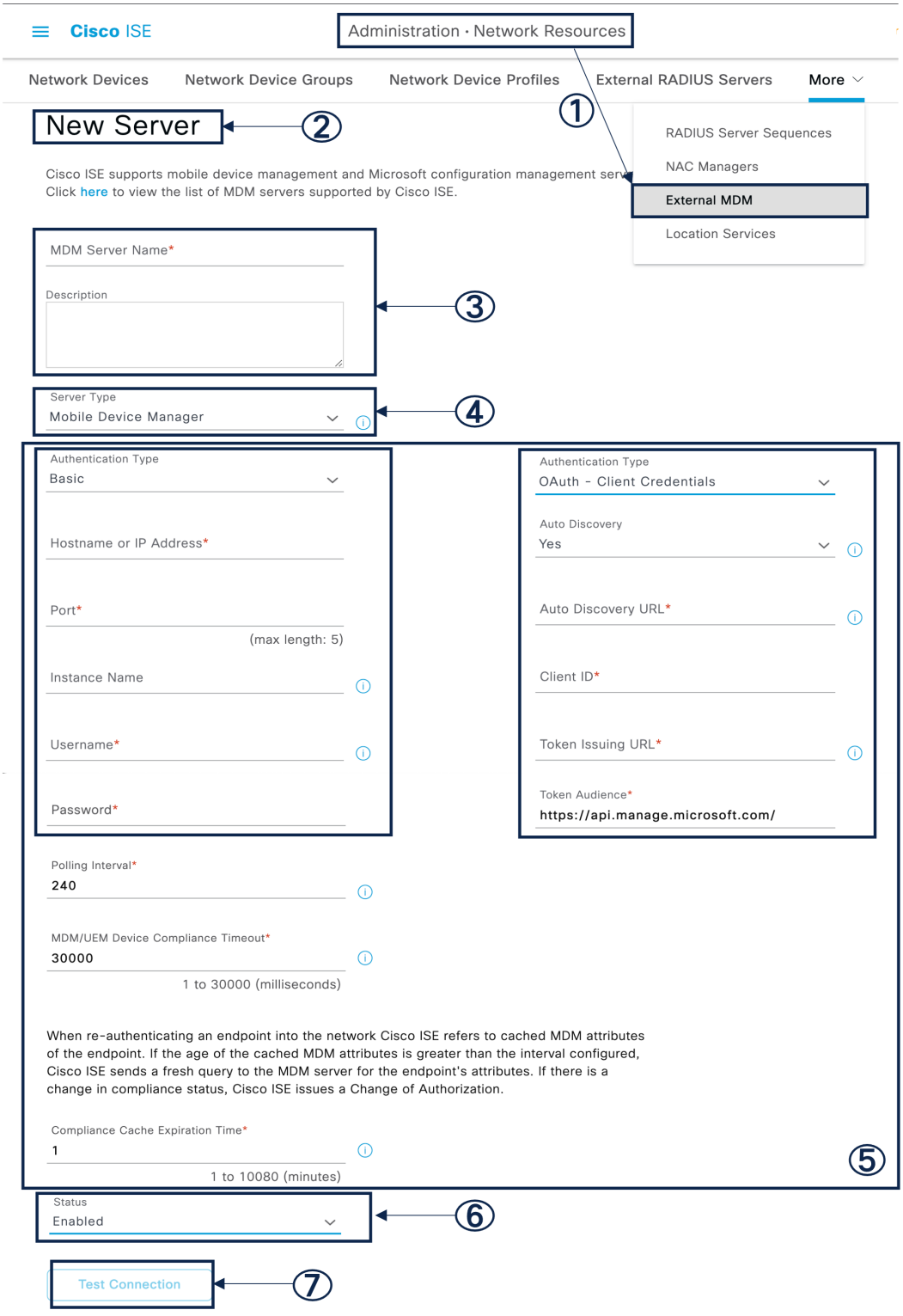
Microsoft System Center Configuration Manager（SCCM）サーバーを定義するには、「デスクトップ デバイス マネージャ サーバーでのエンドポイント コンプライアンスの設定基準ポリシーの選択」を参照してください。

Cisco ISE でのモバイルデバイス管理サーバーの設定

Cisco ISE にエンドポイントの情報を提供する最初の MDM サーバーは、[コンテキストの可視性（Context Visibility）] > [エンドポイント（Endpoints）] ウィンドウのエンドポイント情報に表示されます。エンドポイントが別の MDM サーバーに接続しても、MDM サーバー情報は自動的に更新されません。[コンテキストの可視性（Context Visibility）] ウィンドウからエンドポイントを削除してから、[コンテキストの可視性（Context Visibility）] ウィンドウに更新された情報を表示するためには、エンドポイントを MDM サーバーに再接続する必要があります。

次の画像は、このタスク中に操作する必要がある Cisco ISE GUI フィールドを示しています。画像中の番号は、次のタスクに含まれる手順の番号に対応しています。

図 *5 : Cisco ISE* での *MDM* サーバーの追加



ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして選択します **[管理（Administration）]** > **[ネットワークリソース（Network Resources）]** > **[外部 MDM（External MDM）]**。

ステップ 2 **[MDM/UEM統合（MDM / UEM Integrations）]** ウィンドウで、[追加（Add）] をクリックします。

ステップ 3 追加する MDM サーバーの名前と説明を対応するフィールドに入力します。

ステップ 4 [サーバータイプ（Server Type）] ドロップダウンリストから [Mobile Device Manager] を選択します。

ステップ 5 [認証タイプ（Authentication Type）] ドロップダウンリストから、[基本（Basic）] または [OAuth：クライアントのクレデンシャル（OAuth - Client Credentials）] のいずれかを選択します。

[基本（Basic）] 認証タイプを選択すると、次のフィールドが表示されます。

- [ホスト名/IPアドレス（Host Name/IP Address）]：MDM サーバーのホスト名または IP アドレスを入力します。
- [ポート（Port）]：MDM サーバーとの接続に使用するポートを指定します。通常は 443 です。
- [インスタンス名（Instance Name）]：この MDM サーバーに複数のインスタンスがある場合に、接続するインスタンスを入力します。
- [ユーザー名（Username）]：MDM サーバーへの接続に使用する必要があるユーザー名を入力します。
- [パスワード（Password）]：MDM サーバーへの接続に使用するパスワードを入力します。

[OAuth：クライアントクレデンシャル（OAuth - Client Credentials）] 認証タイプを選択すると、次のフィールドが表示されます。

- [自動検出（Auto Discovery）] ドロップダウンリストから、[はい（Yes）] または [いいえ（No）] を選択します。
- [Auto Discovery URL]：Microsoft Azure 管理ポータルの [Microsoft Azure AD Graph API Endpoint] の値を入力します。この URL は、アプリケーションが Graph API を使用して Microsoft Entra ID のデータに直接アクセスできるエンドポイントです。詳細については、『MDM および UEM サーバーと Cisco ISE の統合』を参照してください。
- [クライアント ID（Client ID）]：アプリケーションの固有識別子。アプリケーションが Microsoft Azure AD Graph API、Microsoft Intune API などの他のアプリケーションのデータにアクセスする場合に、この属性を使用します。
- [トークン発行URL（Token Issuing URL）]：[OAuth2.0認証エンドポイント（Oauth2.0 Authorization Endpoint）] の値を入力します。これは、Cisco ISE が OAuth2.0 を使用してアクセストークンを取得するエンドポイントです。
- [トークン対象者（Token Audience）]：トークンが対象とする受信者リソースであり、公開されている既知の Microsoft Intune API の **APP ID URL** です。

[ポーリング間隔（Polling Interval）]：Cisco ISE が MDM サーバーをポーリングして非準拠エンドポイントを確認するためのポーリング間隔（分単位）を入力します。MDM サーバー上のポーリング間隔に一致するようにこの値を設定します。有効な範囲は 15 ～ 1440 分です。デフォルト値は 240 分です。多数の非準

拠エンドポイントが原因で発生する可能性のあるパフォーマンスへの影響を最小限に抑えるために、運用環境ではポーリング間隔を 60 分より長く設定することをお勧めします。

ポーリング間隔を 0 に設定すると、Cisco ISE は MDM サーバーへのポーリングを無効にします。

（注） 外部 MDM サーバーが 20000 を超える非準拠エンドポイントから要求を受信した場合、外部 MDM サーバーのポーリング間隔は自動的に 0 に設定されます。また、Cisco ISE に次のアラームが表示されます。

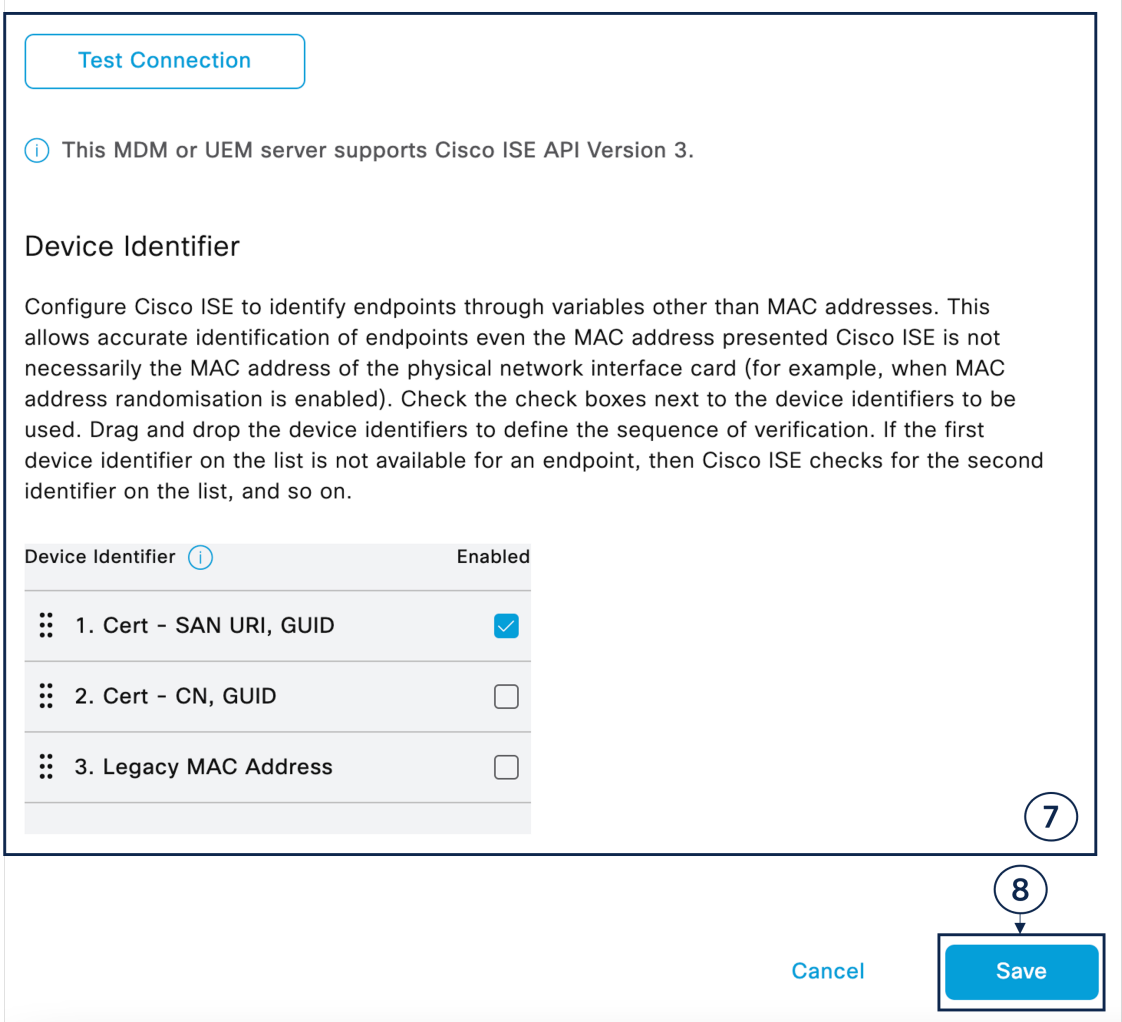
MDM コンプライアンスポーリングが無効：定期的なコンプライアンスポーリングで、膨大な非準拠デバイス情報を受信しました（MDM Compliance Polling Disabled: Reason is Periodic Compliance Polling received huge non-compliance device information）。

[MDM/UEMデバイス コンプライアンス タイムアウト（MDM / UEM Device Compliance Timeout）]：Cisco ISE が MDM または UEM サーバーへのクエリ後に MDM または UEM サーバーからの応答を待機するタイムアウト期間をミリ秒単位で入力します。デフォルト値は 30000 ミリ秒です。1 台の MDM サーバーまたは UEM サーバーのみにクエリを実行する場合は、1 ～ 30000 ミリ秒の値を設定できます。デバイスのコンプライアンス API を使用して複数の MDM サーバーまたは UEM サーバーにクエリを実行する場合は、300 ミリ秒未満の値を設定して、システムパフォーマンスへの影響を回避する必要があります。

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

ステップ 7 MDM サーバーが Cisco ISE に接続されているかどうかを確認するには、[接続のテスト（Test Connection）] をクリックします。[接続のテスト（Test Connection）] は、すべての使用例（ベースラインの取得、デバイス情報の取得など）の権限を確認するためのものではないことに注意してください。これらは、サーバーが Cisco ISE に追加されるときに検証されます。

図 *6 : Cisco ISE* での *MDM* サーバーの追加



設定する MDM サーバーが Cisco ISE MDM API バージョン 3 をサポートしており、属性 GUID を Cisco ISE と共有できる場合は、[デバイス識別子（Device Identifiers）] 領域が表示されます。詳細については、モバイルデバイス管理サーバーを使用した、ランダムで変化する MAC アドレスの処理 （69 ページ）を参照してください。

有効にする次のオプションの 1 つ以上のチェックボックスをオンにし、各オプションを適切な場所にドラッグアンドドロップして、優先順に配置します。

- **[証明書：SAN URI、GUID（Cert - SAN URI, GUID）]**
- **[証明書：CN、GUID（Cert - CN, GUID）]**
- **[レガシー MAC アドレス（Legacy MAC Address）]**

ステップ 8 [Save] をクリックします。

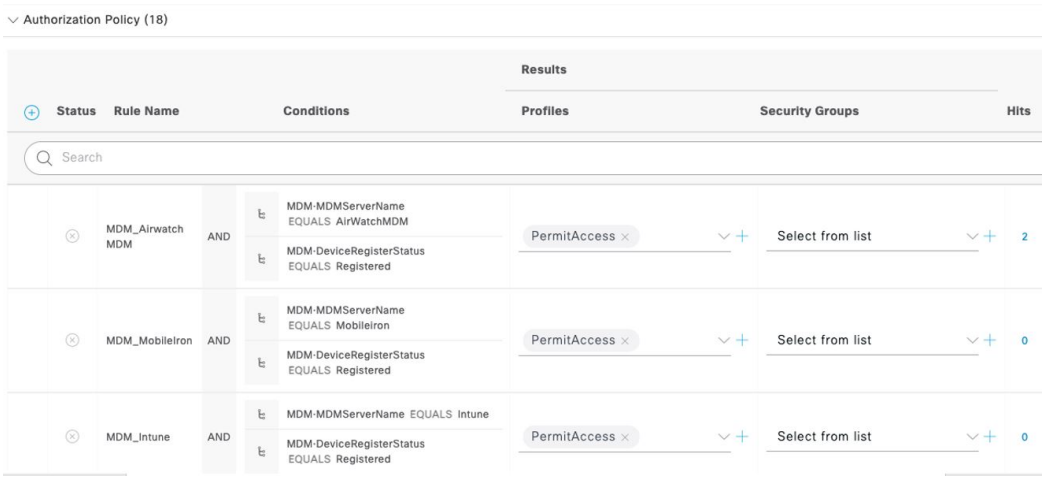
全般的な MDM 設定または UEM 設定の構成

Cisco ISE が複数の MDM サーバーまたは UEM サーバーを照会し、エンドポイントが接続されている MDM サーバーまたは UEM サーバーを識別できるように MDM 設定または UEM 設定を構成します。

たとえば、新しいエンドポイントが Intune に登録されている場合、Cisco ISE でエンドポイントの Intune を評価するには、認証ポリシーにデバイスタイプやユーザータイプといったいくつかの条件が必要になります。

[複数のMDM/UEM統合のクエリ（Query Multiple MDM / UEM Integrations）] オプションを有効にすると、Cisco ISE は認証ポリシーにリストされているすべての MDM サーバーにクエリを実行し、エンドポイントが登録されているサーバーを識別します。

図 *7*: 複数の *MDM* サーバーを含む認証ポリシーの例



ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして選択します **[管理（Administration）]** > **[システム（System）]** > **[設定（Settings）]** > **[全般的なMDM/UEM設定（General MDM / UEM Settings）]** を選択します。

ステップ 2 [全般的な MDM/UEM 設定（General MDM / UEM Settings）] ウィンドウで、[複数の MDM/UEM 統合のクエリ（Query Multiple MDM / UEM Integrations）] をクリックします。

（注） デフォルトでは、[複数の MDM/UEM 統合のクエリ（Query Multiple MDM / UEM Integrations）] オプションは無効になっています。

ステップ 3 次のいずれかのオプションを選択します。

- [エンドポイントが構成済みのプライマリMDM/UEMサーバーに登録されていない（Endpoint is not Registered with the Configured Primary MDM/UEM Server）]：次のシナリオで、Cisco ISE が認証ポリシーで指定されたすべての MDM または UEM サーバーからコンプライアンス情報を取得するようにする場合は、このオプションを選択します。
  - エンドポイントの登録情報がプライマリ MDM または UEM サーバーに存在しない。

- エンドポイントが初めてネットワークにアクセスしている。
- エンドポイントが Cisco ISE に保存されていない。
- エンドポイントが登録されている MDM または UEM サーバーがわからない。

MDM サーバーとのエンドポイントの関連付けは、認証ポリシーの MDM サーバー名の条件に基づいてチェックされます。

- [Primary MDM/UEM Server Sends Error/exception Response]：プライマリ MDM または UEM サーバーがエラーメッセージを送信した場合、または到達不能な場合に、Cisco ISE が認証ポリシーで指定された他の MDM または UEM サーバーにクエリを実行するようにする場合は、このオプションを選択します。

ステップ 4 [Save] をクリックします。

MDM または UEM サーバーのタイムアウトの設定

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして選択します **[管理（Administration）]** > **[ネットワークリソース（Network Resources）]** > **[外部 MDM（External MDM）]** を選択します。

ステップ 2 [MDM/UEM統合（MDM / UEM Integrations）] ウィンドウで、タイムアウト値を変更する MDM サーバーまたは UEM サーバーの横のチェックボックスをオンにします。

ステップ 3 [タイムアウトの変更（Change Timeout）] をクリックします。

ステップ 4 [接続タイムアウト（ミリ秒）（Connection Timeout (milliseconds)）] フィールドにタイムアウト値を入力します。

（注） MDM サーバーまたは UEM サーバーのデフォルトのタイムアウトは、30000 ミリ秒です。

ステップ 5 [変更（Change）] をクリックします。

Microsoft Intune と Microsoft SCCM 用の Cisco ISE MDM サポート

- **Microsoft Intune**：Cisco ISE は、モバイルデバイスを管理するパートナー MDM サーバーとして Microsoft Intune のデバイス管理をサポートしています。

  Microsoft Intune サーバーの管理モバイルデバイスの OAuth 2.0 クライアント アプリケーションとして Cisco ISE を設定します。Cisco ISE は、Azure からトークンを取得し、Cisco ISE Intune アプリケーションとのセッションを確立します。

  Microsoft Intune がクライアント アプリケーションとどのように通信するかの詳細については、https://msdn.microsoft.com/en-us/library/azure/dn645543.aspx を参照してください。

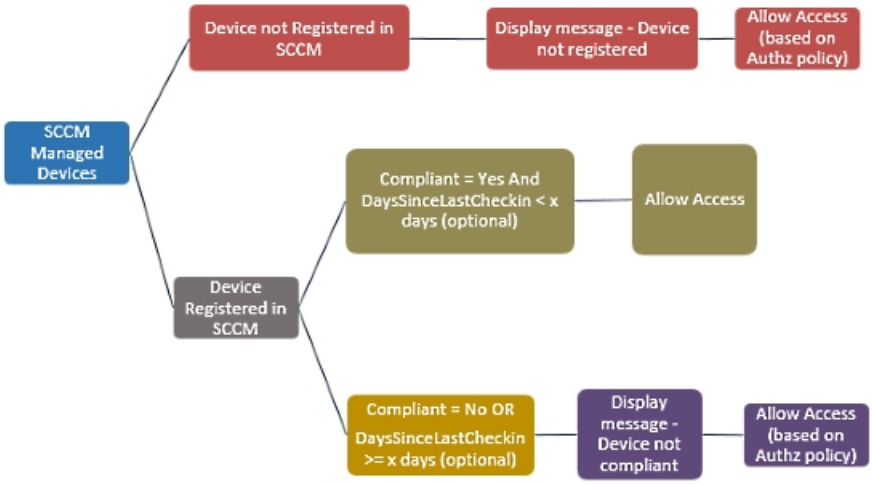
- **デスクトップ デバイス マネージャ（Microsoft SCCM）**：Cisco ISE は Microsoft System Center Configuration Manager（SCCM）を Windows コンピュータの管理用パートナー MDM サーバーとしてサポートしています。

  Microsoft SCCM 統合のパフォーマンスとスケーラビリティの情報については、「Size and Scale Numbers for Configuration Manager」を参照してください。Microsoft は、コンポーネント オブジェクト モデル（COM）に基づく Windows Management Instrumentation（WMI）インターフェイスを使用しているため、スケーラビリティに制限があります。

Microsoft SCCM のワークフロー

Cisco ISE はデバイスが登録されているかどうかについて、Microsoft SCCM サーバーから情報を取得します。エンドポイントが登録されている場合、Cisco ISE はその準拠のステータスをチェックします。次の図に、Microsoft SCCM により管理されるデバイスのワークフローを示します。

図 *8 : SCCM* のワークフロー



デバイスをネットワークに接続し、Microsoft SCCM ポリシーが一致すると、Cisco ISE はコンプライアンスと最終ログイン（チェックイン）時間を取得するために、関連する SCCM サーバーを照会します。この情報を使用して、Cisco ISE は [エンドポイント（Endpoints）] のリストのデバイスのコンプライアンス ステータスと lastCheckinTimeStamp を更新します。

デバイスが準拠していないか、または Microsoft SCCM サーバーに登録されていない場合にリダイレクトプロファイルが認証ポリシーで使用されている場合、デバイスが準拠していないか、または Microsoft SCCM に登録されていないというメッセージがユーザーに表示されます。ユーザーがメッセージを受け取った後、Cisco ISE は Microsoft SCCM 登録サイトへ CoA を発行できます。認証ポリシーとプロファイルに基づいてユーザーにアクセスを許可します。

Microsoft SCCM サーバー接続の監視

Microsoft SCCM のポーリング間隔は設定できません。

Cisco ISE は、Microsoft SCCM サーバーとの接続を検証し、Cisco ISE が Microsoft SCCM サーバーへの接続を失うと MDM ハートビートジョブを実行し、アラームを発生させます。ハートビートジョブの間隔は設定できません。

Microsoft System Center Configuration Manager のポリシー設定例

Microsoft SCCM をサポートするために次の新しいディクショナリエントリを使用します。

- **MDM.DaysSinceLastCheckin**：ユーザーが最後に確認するか、または Microsoft SCCM とデバイスを同期してからの日数。値は 1 ～ 365 日の範囲になります。
- **MDM.UserNotified**：有効な値は **Y** または **N** です。この値は、デバイスが登録されていないことをユーザーに通知したかどうかを示します。その後で、ユーザーにネットワークへの制限付きアクセスを許可してから、登録ポータルにリダイレクトしたり、ユーザーによるネットワークへのアクセスを拒否したりできます。
- **MDM.ServerType**：有効な値は、MDM サーバーの場合は **MDM**、デスクトップデバイス管理の場合は **DM** です。

次に、Microsoft SCCM をサポートするポリシーセットの例を示します。

ポリシー名	条件（IF）	解決策
SCCM_Comp	Wireless_802.1X AND MDM:MDMServerName EQUALS SccmServer1 AND MDM:DeviceRegisterStatus EQUALS Registered	PermitAccess
SCCM_NonComp_Notify	Wireless_802.1X AND MDM:MDMServerName EQUALS SccmServer1 AND MDM:DeviceCompliantStatus EQUALS NonCompliant AND MDM:UserNotified EQUALS 28	PermitAccess
SCCM_NonComp_Days	Wireless_802.1X AND MDM:MDMServerName EQUALS SccmServer1 AND MDM:MDMDeviceCompliantStatus EQUALS Registered AND MDM:DaysSinceLastCheckin EQUALS 28	SCCMRedirect

ポリシー名	条件（IF）	解決策
SCCM_NonComp	Wireless_802.1X AND MDM:MDMServerName EQUALS SccmServer1 AND MDM:DeviceCompliantStatus EQUALS NonCompliant AND MDM:DeviceRegisterStatus EQUALS Registered	SCCMRedirect
SCCM_UnReg_Notify	Wireless_802.1X AND MDM:DeviceRegisterStatus EQUALS Registered AND MDM:UserNotified EQUALS Yes	PermitAccess

Cisco ISE 用の Microsoft System Center Configuration Manager サーバーの設定

Cisco ISE は、Windows Management Instrumentation（WMI）を使用して Microsoft SCCM サーバーと通信します。Microsoft SCCM を実行している Windows サーバーで WMI を設定します。

（注） Cisco ISE 統合に使用するユーザーアカウントは、次のいずれかの条件を満たしている必要があります。

- SMS 管理ユーザーグループのメンバーである。
- WMI 名前空間で SMS オブジェクトと同じアクセス許可がある。

  `root\sms\site_<sitecode>`

  サイトコードは Microsoft SCCM サイトです。

Microsoft Active Directory ユーザーがドメイン管理グループに属しているときの権限の設定

Windows 2008 R2、Windows Server 2012 および Windows Server 2012 R2 の場合、ドメイン管理グループは、デフォルトで Windows オペレーティングシステムの特定のレジストリ キーを完全に制御することはできません。Microsoft Active Directory の管理者は、Microsoft Active Directory ユーザーに次のレジストリキーに対する完全制御権限を提供する必要があります。

- **HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}**
- **HKLM\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}**

次の Microsoft Active Directory バージョンでは、レジストリを変更する必要はありません。

- Windows 2003
- Windows 2003 R2
- Windows 2008。

完全な制御を許可するには、まず Microsoft Active Directory 管理者がキーの所有権を取得する必要があります。

ステップ 1 キーアイコンを右クリックし、[所有者（Owner）] タブを選択します。
ステップ 2 [アクセス許可（Permissions）] をクリックします。
ステップ 3 [詳細設定（Advanced）] をクリックします。

ドメイン管理グループに属していない Microsoft Active Directory ユーザー の権限

Windows 2012 R2 の場合は、Microsoft AD ユーザーに次のレジストリキーに対する完全制御権限を提供します。

- `HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}`
- `HKLM\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}`

Windows PowerShell で次のコマンドを使用して、レジストリキーに完全な権限が付与されているかどうかを確認します。

- `get-acl -path "Microsoft.PowerShell.Core\Registry::HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}" | format-list`
- `get-acl -path "hklm:\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}" | format-list`

Microsoft AD ユーザーがドメイン管理者グループではなく、ドメインユーザーグループに所属している場合は、次の権限が必要です。

- Cisco ISE がドメインコントローラに接続できるようにするには、レジストリキーを追加します。
- ドメイン コントローラで DCOM を使用するための権限
- WMI ルート/CIMv2 名前空間にアクセスするための権限の設定 （85 ページ）

これらの権限は、次のバージョンの Microsoft AD でのみ必要となります。

- Windows 2003
- Windows 2003 R2

- Windows 2008。
- Windows 2008 R2
- Windows 2012
- Windows 2012 R2
- Windows 2016

ドメインコントローラへの Cisco ISE の接続を許可するためにレジストリキーを追加

Cisco ISE がドメインユーザーとして接続し、ログイン認証イベントを取得できるようにするには、ドメインコントローラにいくつかのレジストリ キーを手動で追加する必要があります。エージェントはドメインコントローラまたはドメイン内のマシンには必要ありません。

次のレジストリのスクリプトは追加するキーを示しています。これをコピーしてテキストファイルに貼り付け、.reg の拡張子でファイルを保存し、ファイルをダブルクリックすることでレジストリの変更を行うことができます。レジストリ キーを追加するには、ルート キーのオーナーである必要があります。

```
Windows Registry Editor Version 5.00

[HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"AppID"="{76A64158-CB41-11D1-8B02-00600806D9B6}"

[HKEY_CLASSES_ROOT\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"DllSurrogate"="  "

[HKEY_CLASSES_ROOT\Wow6432Node\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"DllSurrogate"="  "
```

DllSurrogate キーの値には、2 つのスペースが含まれていることを確認します。レジストリを手動で更新する場合は、2つのスペースのみを含める必要があり、引用符は含めないでください。レジストリを手動で更新する際は、AppID、DllSurrogate、およびその値に引用符が含まれていないことを確認してください。

前述のスクリプトに示すように、ファイルの末尾の空の行を含めて、空の行は保持します。

Windows コマンドプロンプトで次のコマンドを使用して、レジストリキーが作成され、正しい値が設定されているかどうかを確認します。

- `reg query "HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}" /f "{76A64158-CB41-11D1-8B02-00600806D9B6}" /e`
- `reg query HKEY_CLASSES_ROOT\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6} /f "  " /e`
- `reg query HKEY_CLASSES_ROOT\Wow6432Node\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6} /f "  " /e`

ドメイン コントローラで DCOM を使用するための権限

Cisco ISE パッシブ ID サービスに使用される Microsoft Active Directory ユーザーには、ドメイン コントローラ サーバーで DCOM を使用する権限が必要です。**dcomcnfg** コマンドラインツールを使用して権限を設定します。

ステップ 1 コマンド ラインから **dcomcnfg** ツールを実行します。

ステップ 2 [コンポーネントサービス（Component Services）] を展開します。

ステップ 3 **[コンピュータ（Computers）] > [マイコンピュータ（My Computer）]** を展開します。

ステップ 4 メニューバーで [アクション（Action）] を選択し、[プロパティ（Properties）] をクリックして [COM セキュリティ（COM Security）] をクリックします。

ステップ 5 Cisco ISE がアクセスと起動の両方に使用するアカウントには許可権限が必要です。4 つのオプション（[アクセス権限Access Permissions）] と [起動およびアクティブ化の権限（Launch and Activation Permissions）] の両方に対する [制限の編集（Edit Limits）] と [デフォルトの編集（Edit Default）]）のすべてに Microsoft Active Directory ユーザーを追加します。

ステップ 6 [アクセス権限（Access Permissions）] と [起動およびアクティブ化の権限（Launch and Activation Permissions）] の両方に対してローカルアクセスとリモートアクセスをすべて許可します。

図 *9 : [アクセス権限（Access Permissions）]* に対するローカルアクアセスとリモートアクセス

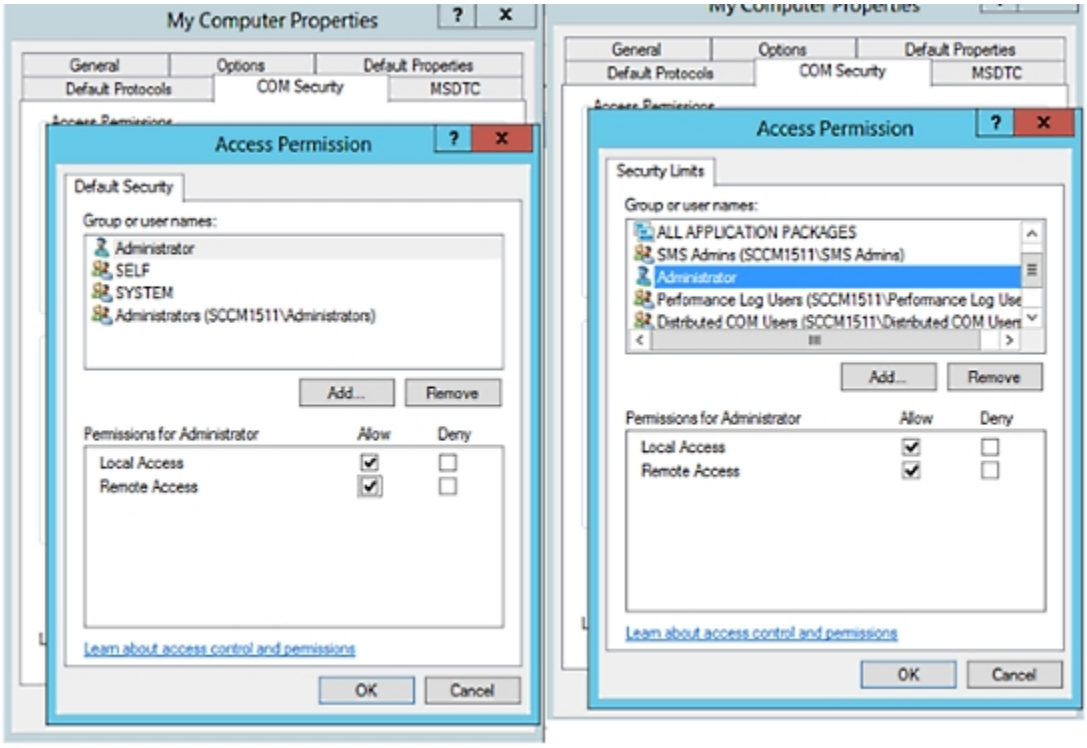
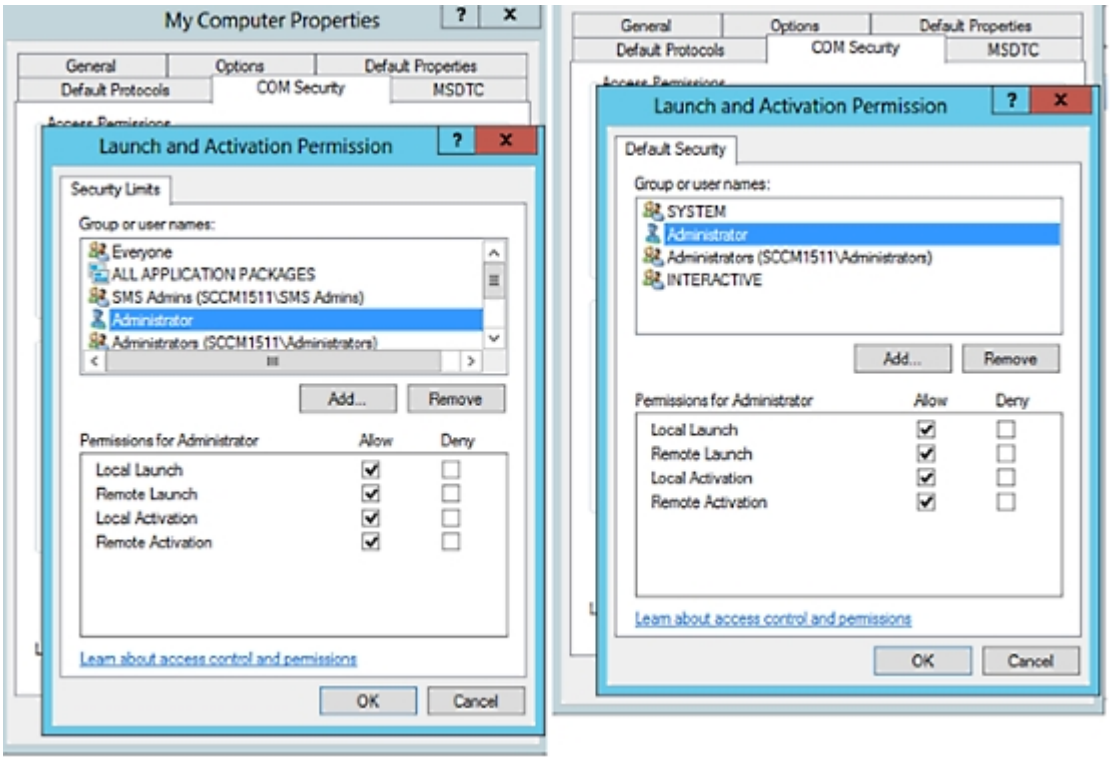


図 *10 : [*起動およびアクティブ化の権限（***Launch and Activation Permissions***）*]* のローカルアクセスとリモートアクセス



WMI ルート/CIMv2 名前空間にアクセスするための権限の設定

デフォルトでは、Microsoft Active Directory ユーザーには実行メソッドおよびリモートの有効化のための権限がありません。wmimgmt.msc MMC コンソールを使用してアクセス権を付与できます。

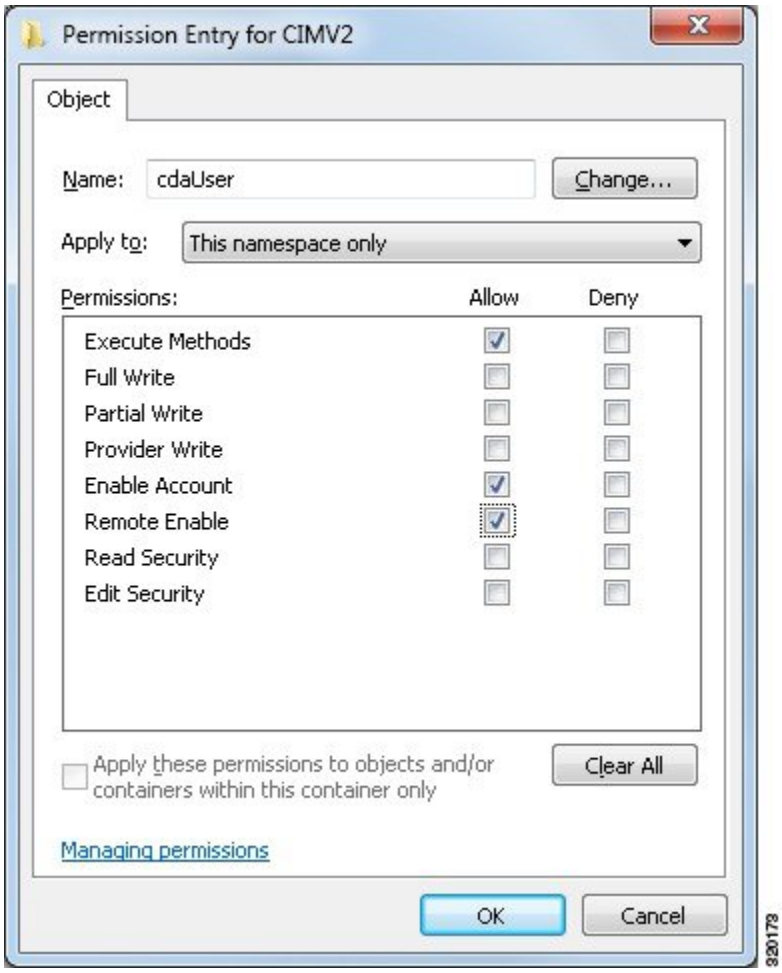
ステップ 1 **[スタート（Start）]** > **[実行（Run）]** を選択し、`wmimgmt.msc` と入力します。

ステップ 2 **[WMI Control]** を右クリックし、**[プロパティ]** をクリックします。

ステップ 3 **[セキュリティ（Security）]** タブで、**[ルート（Root）]** を展開し、**[CIMV2]** を選択します。

ステップ 4 [セキュリティ（Security）] をクリックします。

ステップ 5 次のイメージに示すように、Microsoft Active Directory ユーザーを追加し、必要な権限を設定します。



WMI アクセス用にファイアウォール ポートを開く

Microsoft Active Directory ドメインコントローラのファイアウォール ソフトウェアは、WMI へのアクセスをブロックすることがあります。ファイアウォールをオフにするか、または次のポートへの特定の IP アドレス（Cisco ISE の IP アドレス）のアクセスを許可することができます。

- TCP 135：一般的な RPC ポート。非同期 RPC コールを実行すると、このポートでリスニングしているサービスが、この要求を処理できるコンポーネントが使用しているポートをクライアントに通知します。
- UDP 138：NetBIOS データグラムサービス
- TCP 139：NetBIOS セッションサービス
- TCP 445：サーバーメッセージブロック（SMB）

（注） Cisco ISE は SMB 2.0 をサポートしています。

数値の大きいポートは動的に割り当てられるか、または手動で設定できます。ターゲットとして *%SystemRoot%\System32\dllhost.exe* を追加することを推奨します。このプログラムは、ポートを動的に管理します。

すべてのファイアウォールルールを、特定の IP アドレス（Cisco ISE の IP）に割り当てることができます。

デスクトップ デバイス マネージャ サーバーでのエンドポイント コンプライアンスの設定基準ポリシーの選択

Cisco ISE に追加されたデスクトップ デバイス マネージャ サーバー（Microsoft SCCM サーバーなど）で使用可能な基準ポリシーを表示し、ネットワークアクセスのエンドポイントコンプライアンスを確認するための特定の基準ポリシーを選択できます。デスクトップデバイスマネージャ サーバーで有効化および展開された構成基準ポリシーは、Cisco ISE 管理ポータルで確認できます。

（注） デスクトップデバイス管理サーバーで自分のユーザー権限を確認し、基準ポリシーとコンプライアンス情報を Cisco ISE に送信するために必要なセキュリティ権限があることを確認します。デスクトップデバイスマネージャの [セキュリティ（Security）]>[管理者ユーザー（Administrator Users）] フォルダに管理者を追加する必要があります。

Cisco ISE GUI でデスクトップ デバイス マネージャ サーバーの基準ポリシーを表示するには、**[メニュー（Menu）]** アイコン（☰）をクリックし、**[管理（Administration）]** > **[ネットワーク リソース（Network Resources）]** > **[外部 MDM（External MDM）]** > **[MDM サーバー（MDM Servers）]** を選択します。

新しいデスクトップ デバイス マネージャ サーバーを Cisco ISE に追加し、構成基準ポリシーを選択します。

1. [MDM サーバー（MDM Servers）] ウィンドウで、[追加（Add）] をクリックします。
2. [サーバータイプ（Server Type）] ドロップダウンリストから、[デスクトップデバイスマネージャ（Desktop Device Manager）] を選択します。
3. 次のフィールドに必要な詳細情報を入力します。
   - **[ホスト名/IP アドレス（Host Name / IP Address）]**：Microsoft SCCM サーバーのホスト名または IP アドレスを入力します。
   - **[インスタンス名（Instance Name）]**：Microsoft SCCM サーバーに複数のインスタンスがある場合、接続するインスタンスを入力します。

- **[ユーザー名（Username）]**：Microsoft SCCM サーバーへの接続に使用する必要があるユーザー名を入力します。
- **[パスワード（Password）]**：Microsoft SCCM サーバーへの接続に使用する必要があるパスワードを入力します。
- [準拠デバイス再認証クエリの時間間隔（Time Interval For Compliance Device ReAuth Query）]：エンドポイントが認証または再認証されるときに、Cisco ISE はそのエンドポイントの MDM 変数を取得するのにキャッシュを使用します。キャッシュされた値の経過時間がこのフィールドで設定された値よりも大きい場合、Cisco ISE は新しい値を取得するために MDM サーバーに新しいデバイスクエリを送信します。準拠ステータスが変更されると、Cisco ISE は適切な CoA をトリガーします。

  有効な範囲は 1 ～ 10080 分です。デフォルト値は 1 分です。

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

サーバーが Cisco ISE に接続されていることを確認するには、[テスト接続（Test Connection）] ボタンをクリックします。このサーバーで使用可能な構成基準ポリシーを表示するには、[保存して続行（Save & Continue）] をクリックします。新しいウィンドウが開き、基準ポリシーの名前と ID のリストが表示されます。

既存のデスクトップ デバイス マネージャ サーバーから構成基準ポリシーを選択する

[MDM サーバー（MDM Servers）] ウィンドウで、目的のサーバーのチェックボックスをオンにし、**[編集（Edit）]** をクリックします。このサーバーで使用可能な基準ポリシーのリストを表示するには、**[構成基準（Configuration Baselines）]** タブをクリックします。

デフォルトでは、すべての基準ポリシーが選択されています。[名前（Name）] の横にあるチェックボックスをオフにして、すべての基準ポリシーの選択を解除します。ポリシーの名前の横にあるチェックボックスをオンにして、必要な基準ポリシーを選択します。[Save] をクリックします。

エンドポイントのコンプライアンスは、選択した構成基準ポリシーに基づいてチェックされます。

デスクトップ デバイス マネージャ サーバーの構成基準ポリシーに変更がある場合は、Cisco ISE で更新する変更に対して [構成基準（Configuration Baselines）] タブの [今すぐ更新（Update Now）] ボタンをクリックします。

Windows エンドポイントのデバイス識別子の設定

デスクトップ デバイス マネージャ サーバーは、特定の属性を識別子として使用して、ネットワークに接続するエンドポイントを確認します。エンドポイントの MAC アドレスは、最も一般的に使用される識別子です。ただし、ドングル、ドッキングステーション、または MAC アドレスのランダム化技術が使用されている場合、MAC アドレスは最も信頼性の高い識別子ではありません。

ホスト名を識別子として使用するように選択できるようになりました。ホスト名は、証明書で使用可能な共通名（CN）または SAN-DNS 属性から取得されます。エンドポイントの証明書

ベースの認証は、ホスト名を使用して基準ポリシーのコンプライアンスをチェックするために必須です。

デスクトップデバイスマネージャサーバーのデバイス識別子を設定するには、[サーバー構成（Server Configuration）]タブに移動します。メインメニューから、**[管理（Administration）]**>**[ネットワークリソース（Network Resources）]**>**[外部 MDM（External MDM）]**>**[MDM サーバー（MDM Servers）]**>**[編集（Edit）]**を選択します。

[デバイス識別子の構成（Device Identifier Configurations）]セクションでは、次の順序で識別子がデフォルトで有効になっています。

1. **レガシー MAC アドレス**
2. **Cert**：**CN、ホスト名**
3. **Cert**：**SAN-DNS、ホスト名**

識別子の選択を解除するには、その識別子のチェックボックスをオフにします。属性をドラッグして、検証のためにサーバーで使用される順序を並べ替えることができます。

デバイス識別子の構成の確認

ホスト名が検証に使用される場合、GUID は Cisco ISE によってエンドポイントに割り当てられます。[ライブログ（Live Logs）]ウィンドウを表示し（Cisco ISE GUI で、[メニュー（Menu）]アイコン（☰）をクリックし、**[操作（Operations）]**>**[RADIUS]**>**[ライブログ（Live Logs）]**を選択して、GUID エントリの詳細を確認します。

未登録のデバイスのリダイレクトのための許可プロファイルの設定

各外部 MDM サーバーの未登録のデバイスをリダイレクトするには、Cisco ISE で許可プロファイルを設定する必要があります。

始める前に

- Cisco ISE で MDM サーバー定義を作成したことを確認します。Cisco ISE を MDM サーバーと正常に統合できてはじめて、MDM ディクショナリは読み込まれます。その後、MDM ディクショナリ属性を使用して許可ポリシーを作成できます。
- 未登録のデバイスをリダイレクトするために、Cisco WLC の ACL を設定します。
- インターネット接続にプロキシを使用していて、MDM サーバーが内部ネットワークの一部である場合は、プロキシバイパスリストに MDM サーバー名または IP アドレスを追加する必要があります。Cisco ISE の GUI で、[メニュー（Menu）]アイコン（☰）をクリックし、**[管理（Administration）]**>**[システム（System）]**>**[設定（Settings）]**>**[プロキシ（Proxy）]**このアクションを実行します。

ステップ 1 Cisco ISE の GUI で、[メニュー（Menu）] アイコン（☰）をクリックし、**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [認証（Authorization）] > [認証プロファイル（Authorization Profiles）] > [追加（Add）]**。

ステップ 2 準拠していないまたは登録されていない未登録デバイスをリダイレクトするための許可プロファイル作成します。

ステップ 3 MDM サーバー名と一致する認証プロファイルの名前を [名前（Name）] フィールドに入力します。

ステップ 4 [アクセスタイプ（Access Type）] ドロップダウンリストから [ACCESS_ACCEPT] を選択します。

ステップ 5 [共通タスク（Common Tasks）] セクションで、[Web リダイレクション（Web Redirection）] チェックボックスをオンにし、ドロップダウンリストから [MDM リダイレクト（MDM Redirect）] を選択します。

ステップ 6 ワイヤレス LAN コントローラ上で設定した ACL の名前を [ACL] ドロップダウンリストから選択します。

ステップ 7 [値（Value）] ドロップダウンリストから MDM ポータルを選択します。

ステップ 8 使用する MDM サーバーを [MDM サーバー（MDM Server）] ドロップダウンリストから選択します。

ステップ 9 [送信（Submit）] をクリックします。

次のタスク

MDM 使用例の許可ポリシー ルールの設定。

MDM 使用例の許可ポリシー ルールの設定

Cisco ISE で認証ポリシールールを設定して、MDM 設定を完了します。

始める前に

- Cisco ISE 証明書ストアに MDM サーバー証明書を追加します。
- Cisco ISE で MDM サーバー定義を作成したことを確認します。正常に MDM サーバーと Cisco ISE を統合した後にのみ、MDM ディクショナリが入力され、MDM ディクショナリ属性を使用して認証ポリシーを作成できます。
- 未登録または非準拠のデバイスをリダイレクトするための ACL を Cisco WLC で設定します。

ステップ 1 Cisco ISE の GUI で [メニュー（Menu）] アイコン（☰）をクリックし、次を選択し**[ポリシー（Policy）] > [ポリシーセット（Policy Sets）]**、認証ポリシールールを表示するポリシーセットを展開します。

ステップ 2 次のルールを追加します。

- [MDM_Un_Registered_Non_Compliant]：MDM サーバーに登録されていないか、MDM ポリシーに準拠していないデバイスの場合。要求がこのルールに一致すると、ユーザーに Cisco ISE MDM ウィンドウが表示され、MDM サーバーでのデバイスの登録に関する情報が示されます。

（注） このポリシーでは、**MDM.MDMServerName** 条件を使用しないでください。この条件を使用すると、エンドポイントが MDM サーバーに登録されている場合にのみ、エンドポイントはポリシーに一致します。

- [PERMIT]：デバイスが Cisco ISE と MDM に登録されており、Cisco ISE と MDM のポリシーに準拠している場合、Cisco ISE で設定されたアクセス コントロール ポリシーに基づいてネットワークへのアクセス権が付与されます。

ステップ 3 [Save] をクリックします。

MDM との相互運用性を確保するためのワイヤレスコントローラでの ACL の設定

未登録のデバイスおよび証明書プロビジョニングをリダイレクトするために認証ポリシーで使用する ACL をワイヤレスコントローラで設定します。ACL は次の順序にする必要があります。

ステップ 1 サーバーからクライアントへのすべての発信トラフィックを許可します。

ステップ 2 （任意）トラブルシューティングのためにクライアントからサーバーへの ICMP 着信トラフィックを許可します。

ステップ 3 未登録および非準拠のデバイスが MDM エージェントをダウンロードし、コンプライアンスチェックに進むように MDM サーバーへのアクセスを許可します。

ステップ 4 Web ポータルおよびサプリカント用 Cisco ISE、および証明書プロビジョニングフローに対するクライアントからサーバーへのすべての着信トラフィックを許可します。

ステップ 5 名前解決のためにクライアントからサーバーへの着信ドメインネームシステム（DNS）トラフィックを許可します。

ステップ 6 IP アドレスのためにクライアントからサーバーへの着信 DHCP トラフィックを許可します。

ステップ 7 Cisco ISE へのリダイレクションのための、クライアントからサーバーへの企業リソースに対するすべての着信トラフィックを（会社のポリシーに応じて）拒否します。

ステップ 8 （任意）残りのトラフィックを許可します。

例

次の例では、未登録のデバイスを BYOD フローにリダイレクトするための ACL を示しています。この例では、Cisco ISE IP アドレスは 10.35.50.165 で、企業のネットワークの IP アドレスは 192.168.0.0 および 172.16.0.0（リダイレクト用）で、MDM サーバーサブネットは 204.8.168.0 です。

図 *11* : 登録されていないデバイスをリダイレクトするための *ACL*

General

Access List Name NSP-ACL

Deny Counters 0

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Outbound	150720
2	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	ICMP	Any	Any	Any	Inbound	7227
3	Permit	0.0.0.0 / 0.0.0.0	204.8.168.0 / 255.255.255.0	Any	Any	Any	Any	Any	17626
4	Permit	0.0.0.0 / 0.0.0.0	10.35.50.165 / 255.255.255.255	Any	Any	Any	Any	Inbound	7505
5	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Inbound	2864
6	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DHCP Server	Any	Inbound	0
7	Deny	0.0.0.0 / 0.0.0.0	192.168.0.0 / 255.255.0.0	Any	Any	Any	Any	Inbound	0
8	Deny	0.0.0.0 / 0.0.0.0	172.16.0.0 / 255.240.0.0	Any	Any	Any	Any	Inbound	4
9	Deny	0.0.0.0 / 0.0.0.0	10.0.0.0 / 255.0.0.0	Any	Any	Any	Any	Inbound	457
10	Deny	0.0.0.0 / 0.0.0.0	173.194.0.0 / 255.255.0.0	Any	Any	Any	Any	Inbound	1256
11	Deny	0.0.0.0 / 0.0.0.0	171.68.0.0 / 255.252.0.0	Any	Any	Any	Any	Inbound	11310
12	Deny	0.0.0.0 / 0.0.0.0	171.71.181.0 / 255.255.255.0	Any	Any	Any	Any	Any	0
13	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	71819

デバイスのワイプまたはロック

Cisco ISE では、紛失したデバイスのワイプや PIN ロックの有効化が可能です。この操作は、[エンドポイント（Endpoints）] ウィンドウで設定できます。

ステップ 1 Cisco ISE の GUI で [メニュー（Menu）] アイコン（☰）をクリックし、次を選択します**[ワークセンター（Work Centers）] > [ネットワークアクセス（Network Access）] > [ID（Identities）] > [エンドポイント（Endpoints）]**。

ステップ 2 ワイプまたはロックするデバイスの横にあるチェックボックスをオンにします。

ステップ 3 [MDM アクセス（MDM Access）] ドロップダウンリストから、次のオプションのいずれかを選択します。

- [完全ワイプ（Full Wipe）] : このオプションを使用すると、MDM ベンダーに応じて、企業アプリケーションが削除されるか、またはデバイスが工場出荷時の設定にリセットされます。
- [企業ワイプ（Corporate Wipe）] : このオプションを使用すると、MDM サーバーポリシーで設定したアプリケーションが削除されます。
- [PIN ロック（PIN Lock）] : このオプションを使用すると、デバイスがロックされます。

ステップ 4 [はい（Yes）] をクリックして、デバイスをワイプまたはロックします。

モバイルデバイス管理レポートの表示

Cisco ISE では、MDM サーバー定義のすべての追加、更新、および削除を記録します。これらのイベントは、選択された期間での任意のシステム管理者によるすべての設定変更を表示する [変更設定監査（Change Configuration Audit）] レポートに表示できます。

Cisco ISE の GUIで、[メニュー（Menu）] アイコン（☰）をクリックし、**[操作（Operations）]** > **[レポート（Reports）]** > **[レポート（Reports）]** > **[監査]** > **[変更設定監査（）]** を選択します。確認する MDM サーバーの **[Object Type]** 列と **[Object Name]** 列のエントリを確認し、対応する **[Event]** の値をクリックして設定イベントの詳細を表示します。

モバイルデバイス管理ログの表示

[デバッグウィザード（Debug Wizard）] ウィンドウを使用して、モバイルデバイス管理のログメッセージを表示できます。Cisco ISE GUI で、[メニュー（Menu）] アイコン（☰）をクリックし、**[操作（Operations）]** > **[トラブルシュート（Troubleshoot）]** > **[デバッグウィザード（Degug Wizard）]** > **[デバッグログの構成（Debug Log Configuration）]** を選択します。Cisco ISE ノードの横にあるオプションボタンをクリックし、[編集（Edit）] をクリックします。表示された新しいウィンドウで、コンポーネント名 **external-mdm** の横にあるオプションボタンをクリックし、[編集（Edit）] をクリックします。デフォルトのレベルは [情報（INFO）] です。対応する [ログレベル（Log Level）] ドロップダウンリストから [デバッグ（DEBUG）] または [トレース（TRACE）] を選択し、[保存（Save）] をクリックします。

Cisco Private 5G をサービスとして構成する

Cisco ISE リリース 3.2 以降、Cisco ISE は Cisco Private 5G およびセッション管理機能（SMF）ソフトウェアをサポートします。Cisco ISE は、RADIUS 認証のみおよびアカウンティングフローで実装される 5G 認証のポリシー設定を提供します。SMF との通信は、RADIUS プロトコルを使用して行われます。Cisco ISE と Cisco Private 5G 間の通信は、OpenAPI および ERS API を使用して行われます。

始める前に

Cisco ISE でサービスとして有効化する前に、ネットワークで Cisco Private 5G を展開しておく必要があります。

ステップ 1 Cisco Private 5G オンプレミス Cisco ISE プロキシで Cisco ISE を RADIUS サーバーとして設定します。

ステップ 2 ERS と Open API を有効にします。

ERS と Open API を有効にすると、API を使用するか、Cisco ISE GUI から、後続の手順を実行できます。

ステップ 3 Cisco ISE で 5G を有効にします。

a) Cisco ISE GUI で、[メニュー（Menu）] アイコン（☰）をクリックし、**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[認証（Authentication）]** > **[許可されるプロトコル（Allowed Protocols）]** を選択します。

b) 新しい**許可されるプロトコル**サービスを追加するか、既存のサービスを変更します。

（注） 新しいサービスを作成することは必須ではありません。5G エンドポイントにも既存の**デフォルト ネットワーク アクセス** サービスを使用できます。

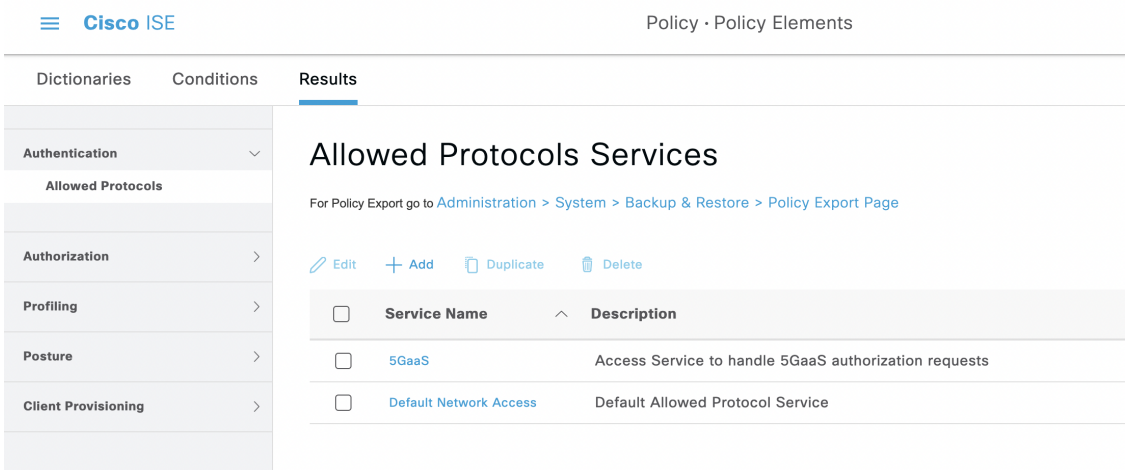
c) ネットワーク要件に従って設定を変更します。

d) [5G] チェックボックスをオンにします。

e) [保存（Save）] をクリックします。

たとえば、次の図に示す**許可されるプロトコルサービス**を作成して、5G トラフィックに一致させることができます。

図 *12 : 5G* の許可されるプロトコルサービス



ステップ 4 Cisco ISE で SMF をネットワークデバイスとして設定します。

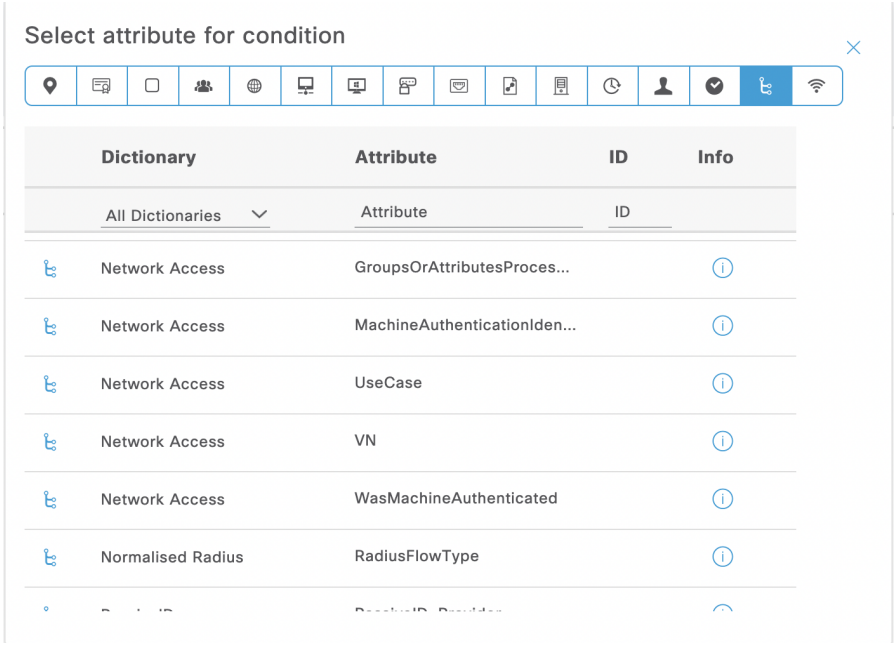
ステップ 5 新しい ID グループを作成するか、既存の ID グループを使用します。5G ユーザーは、Cisco ISE 内部データベースにサブスクライバとして保存されます。

ステップ 6 ユーザー ID グループを作成するか、Cisco ISE のデフォルトのユーザー ID グループから選択します。

ステップ 7 新しいポリシーセットを作成するか、既存のポリシーを使用します。

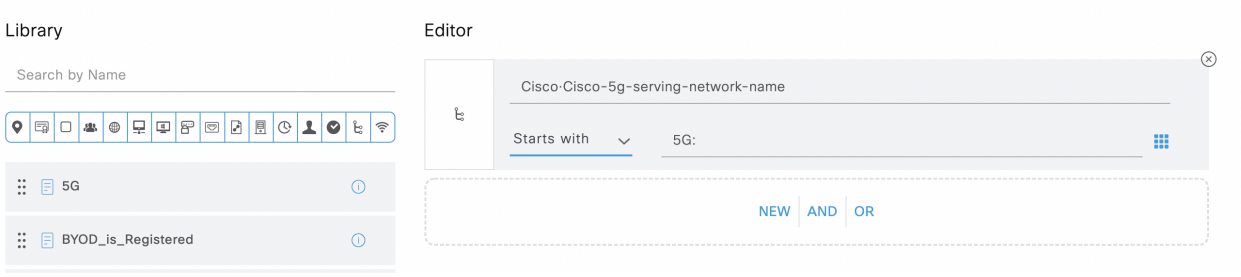
Conditions Studio の **Network Access.UseCase** 属性に、新しい値 **FiveG** が入力されます。**UseCase** 属性にも基づいてポリシーを作成できるようになりました。

図 *13* : 条件ライブラリの *UseCase* 属性の場所



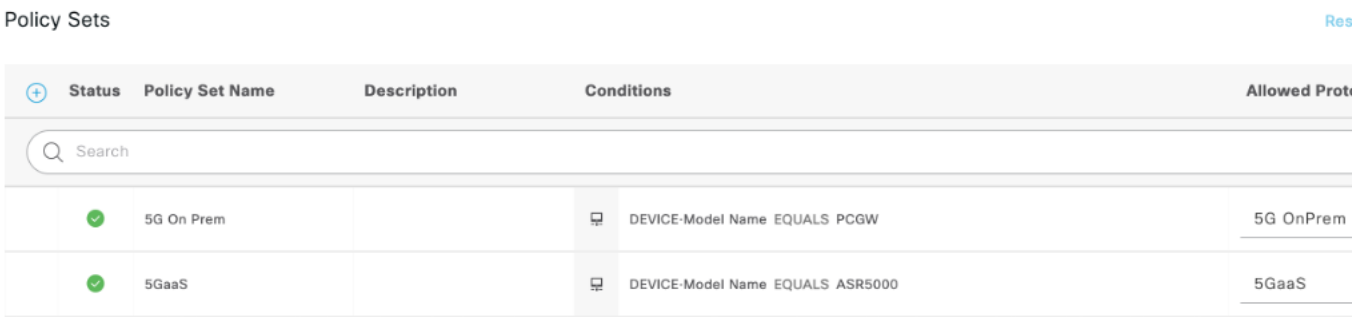
新しい組み込み条件である **5G** は、**Conditions Studio** の**ライブラリ**でも利用できます。この条件では、5G エンドポイントの照合に使用できる **Cisco·Cisco-5g-serving-network-name** 属性を使用します。

図 *14* : *5G* の条件



このポリシーには、以前に作成した、許可されるプロトコルサービスプロファイルをプッシュできます。

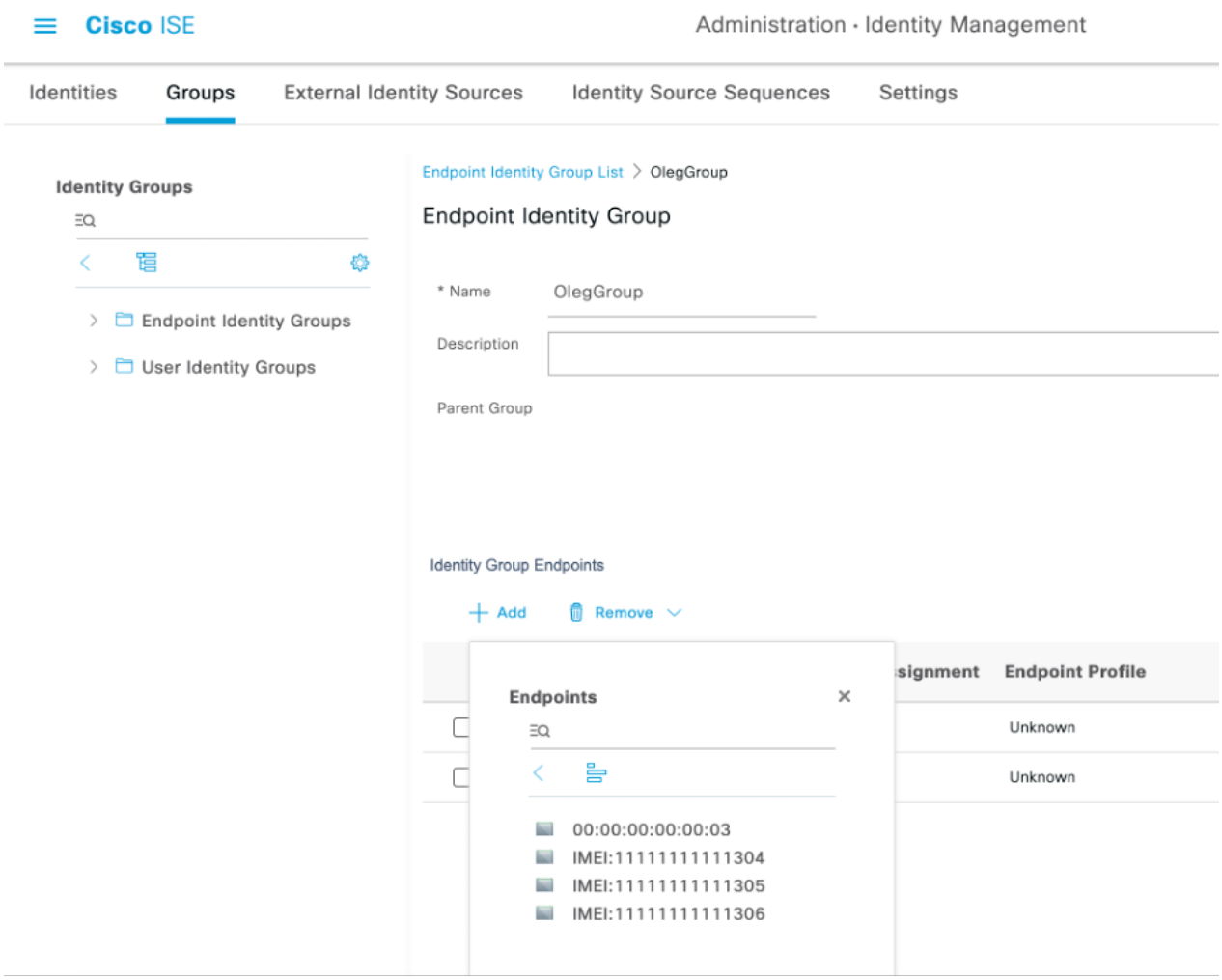
図 *15* : *5G* のポリシーセット



ステップ 8 Cisco Private 5G は、5GaaS API を使用して、サブスクライバ（セルラーユーザー）とユーザー機器（モバイルデバイス）を Cisco ISE に追加します。

たとえば、次の図に示すように、エンドポイント ID グループには追加されたサブスクライバが表示されます。

図 *16 : 5G* サブスクライバのエンドポイント *ID* グループ



ライブログと**ライブセッション**をチェックして、5G セッションログを表示し、必要に応じてトラブルシューティングを行うことができます。**ライブセッション**には、**ユースケース**（デフォルトでは無効）という新しい列があり、**5G** フィルタを使用して 5G エンドポイントをフィルタ処理できます。**エンドポイント**列でプレフィックス **IMEI:** を使用して、5G エンドポイントをフィルタ処理することもできます。

図 *17 : 5G* ライブログ

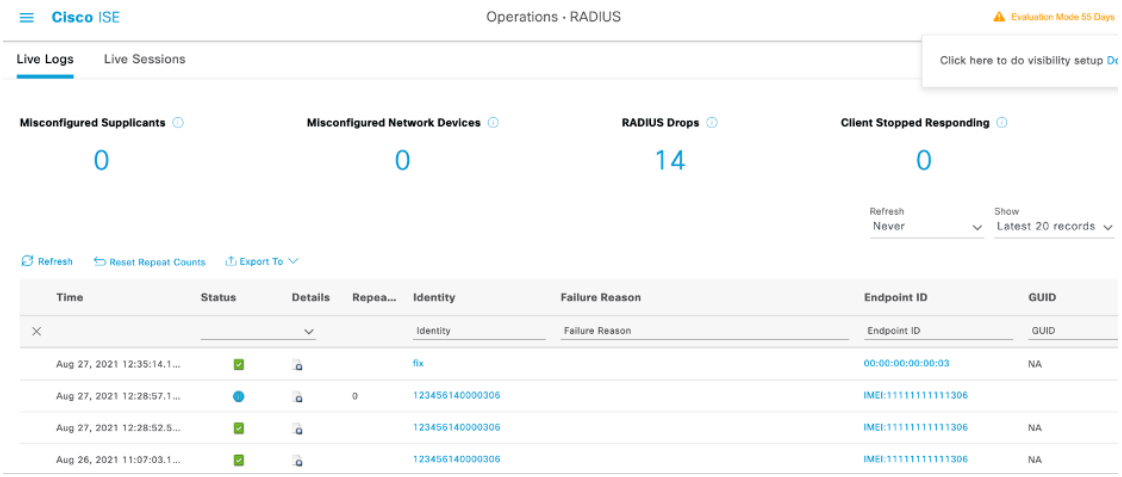
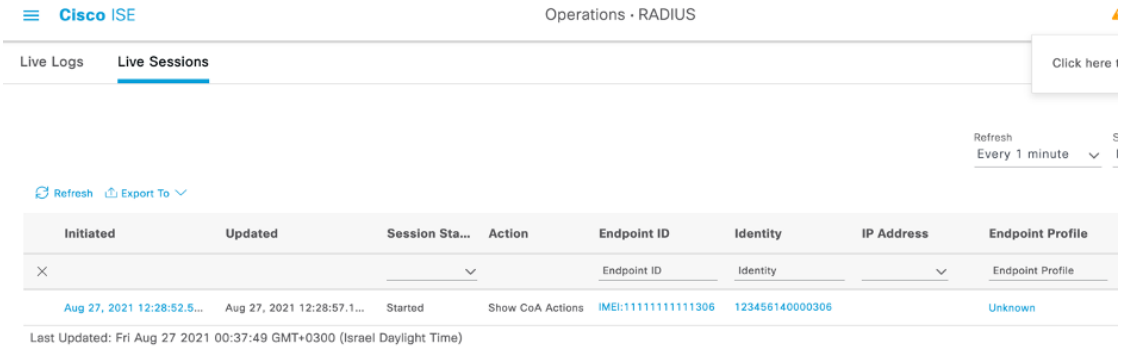


図 *18 : 5G* ライブセッション



Cisco Private 5G をサービスとして構成する

Cisco ISE リリース 3.2 以降、Cisco ISE は Cisco Private 5G およびセッション管理機能（SMF）ソフトウェアをサポートします。Cisco ISE は、RADIUS 認証のみおよびアカウンティングフローで実装される 5G 認証のポリシー設定を提供します。SMF との通信は、RADIUS プロトコルを使用して行われます。Cisco ISE と Cisco Private 5G 間の通信は、OpenAPI および ERS API を使用して行われます。

始める前に

Cisco ISE でサービスとして有効化する前に、ネットワークで Cisco Private 5G を展開しておく必要があります。

ステップ 1 Cisco Private 5G オンプレミス Cisco ISE プロキシで Cisco ISE を RADIUS サーバーとして設定します。

ステップ 2 ERS と Open API を有効にします。

ERS と Open API を有効にすると、API を使用するか、Cisco ISE GUI から、後続の手順を実行できます。

ステップ 3 Cisco ISE で 5G を有効にします。

a) Cisco ISE GUI で、[メニュー（Menu）] アイコン（☰）をクリックし、**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[認証（Authentication）]** > **[許可されるプロトコル（Allowed Protocols）]** を選択します。

b) 新しい**許可されるプロトコル**サービスを追加するか、既存のサービスを変更します。

（注） 新しいサービスを作成することは必須ではありません。5G エンドポイントにも既存の**デフォルト ネットワーク アクセス** サービスを使用できます。

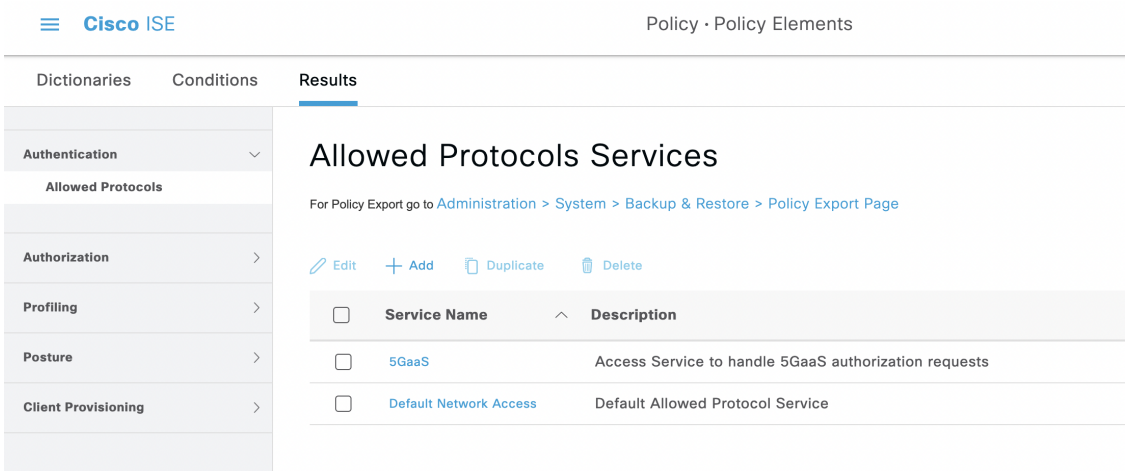
c) ネットワーク要件に従って設定を変更します。

d) [5G] チェックボックスをオンにします。

e) [保存（Save）] をクリックします。

たとえば、次の図に示す**許可されるプロトコルサービス**を作成して、5G トラフィックに一致させることができます。

図 *19 : 5G* の許可されるプロトコルサービス



ステップ 4 Cisco ISE で SMF をネットワークデバイスとして設定します。

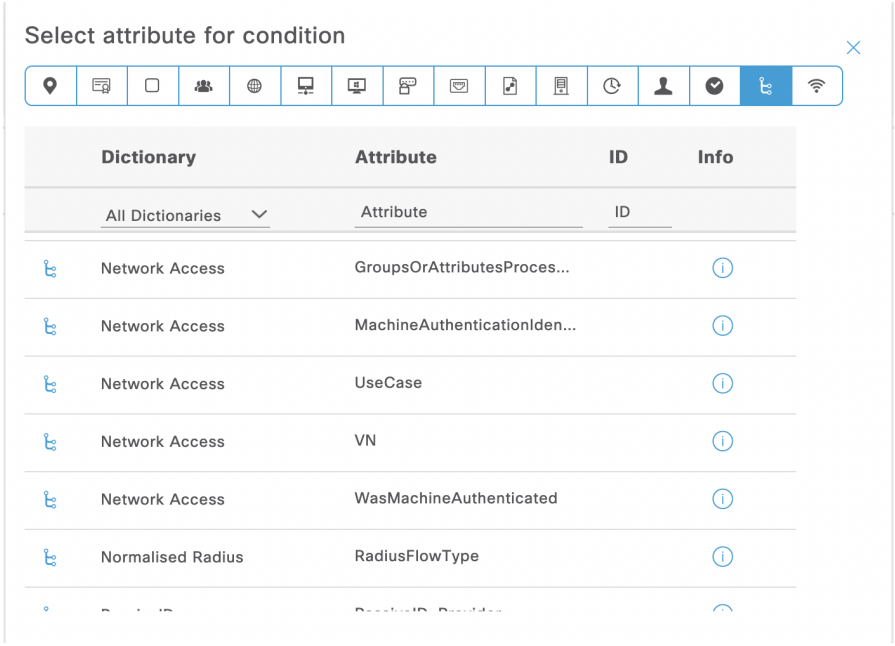
ステップ 5 新しい ID グループを作成するか、既存の ID グループを使用します。5G ユーザーは、Cisco ISE 内部データベースにサブスクライバとして保存されます。

ステップ 6 ユーザー ID グループを作成するか、Cisco ISE のデフォルトのユーザー ID グループから選択します。

ステップ 7 新しいポリシーセットを作成するか、既存のポリシーを使用します。

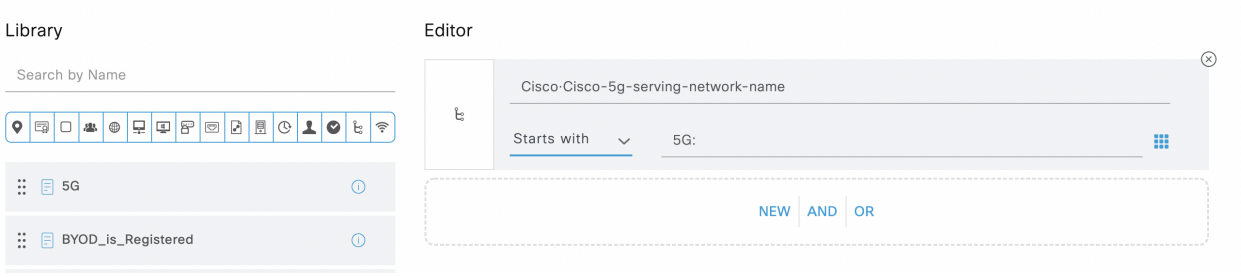
Conditions Studio の **Network Access.UseCase** 属性に、新しい値 **FiveG** が入力されます。**UseCase** 属性にも基づいてポリシーを作成できるようになりました。

図 *20* : 条件ライブラリの *UseCase* 属性の場所



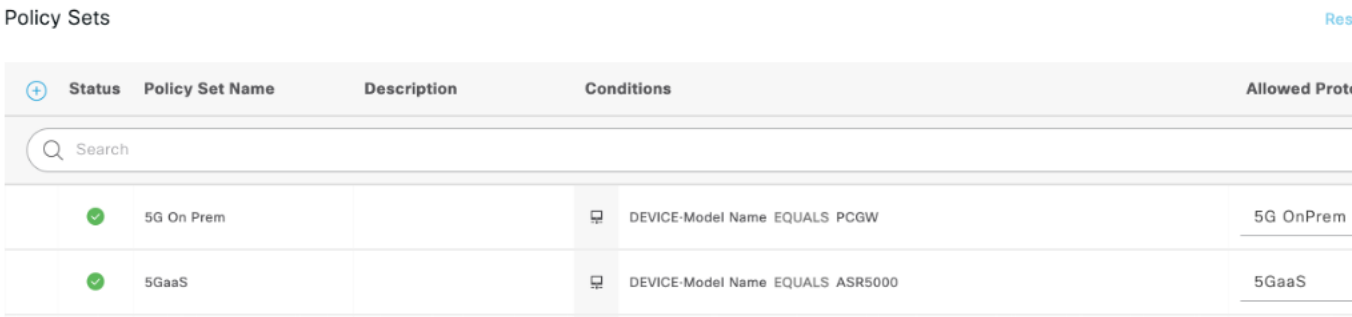
新しい組み込み条件である **5G** は、**Conditions Studio** の**ライブラリ**でも利用できます。この条件では、5G エンドポイントの照合に使用できる **Cisco·Cisco-5g-serving-network-name** 属性を使用します。

図 *21* : *5G* の条件



このポリシーには、以前に作成した、許可されるプロトコルサービスプロファイルをプッシュできます。

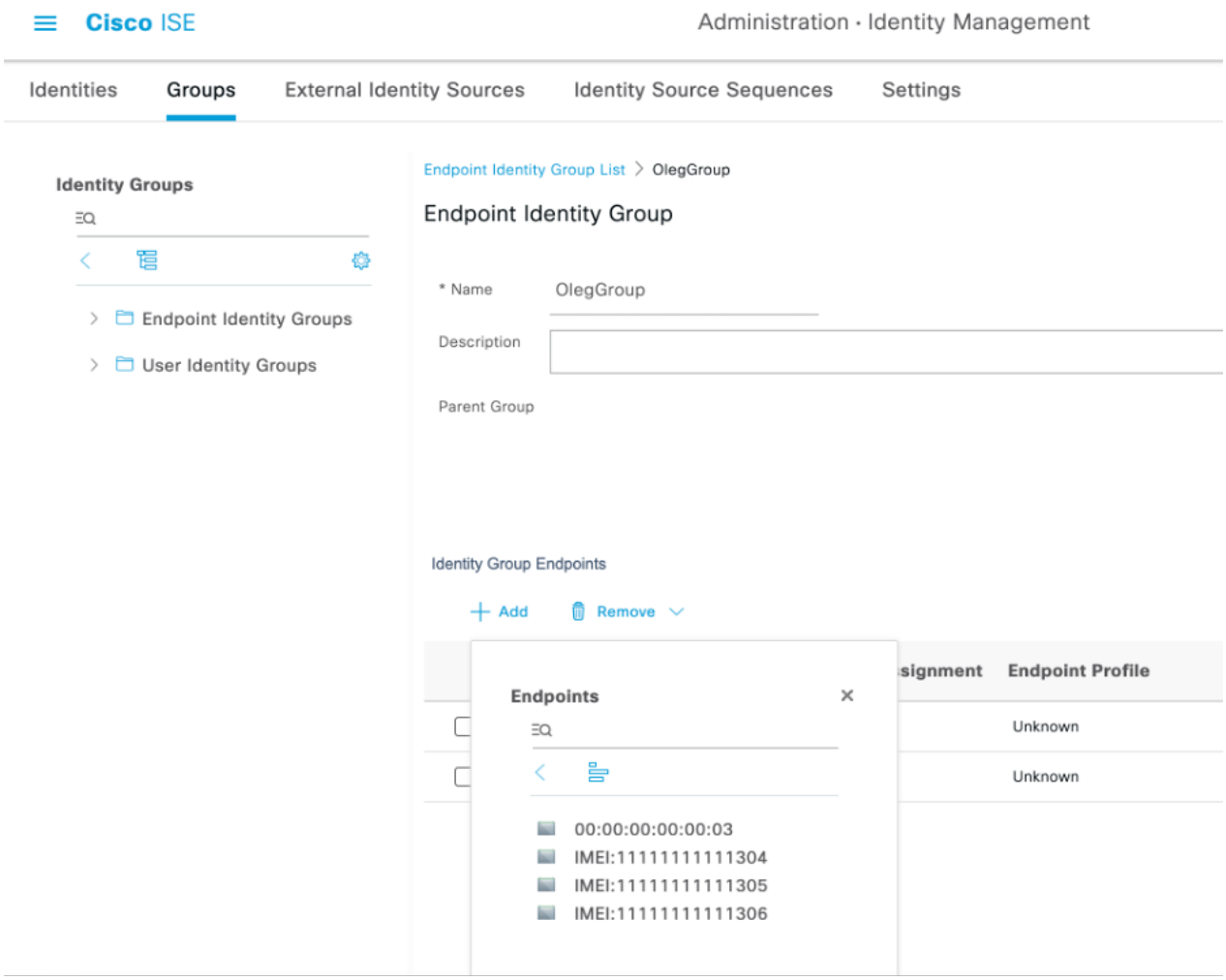
図 *22* : *5G* のポリシーセット



ステップ 8 Cisco Private 5G は、5GaaS API を使用して、サブスクライバ（セルラーユーザー）とユーザー機器（モバイルデバイス）を Cisco ISE に追加します。

たとえば、次の図に示すように、エンドポイント ID グループには追加されたサブスクライバが表示されます。

図 *23 : 5G* サブスクライバのエンドポイント *ID* グループ



ライブログと**ライブセッション**をチェックして、5G セッションログを表示し、必要に応じてトラブルシューティングを行うことができます。**ライブセッション**には、**ユースケース**（デフォルトでは無効）という新しい列があり、**5G** フィルタを使用して 5G エンドポイントをフィルタ処理できます。**エンドポイント**列でプレフィックス **IMEI:** を使用して、5G エンドポイントをフィルタ処理することもできます。

図 *24 : 5G* ライブログ

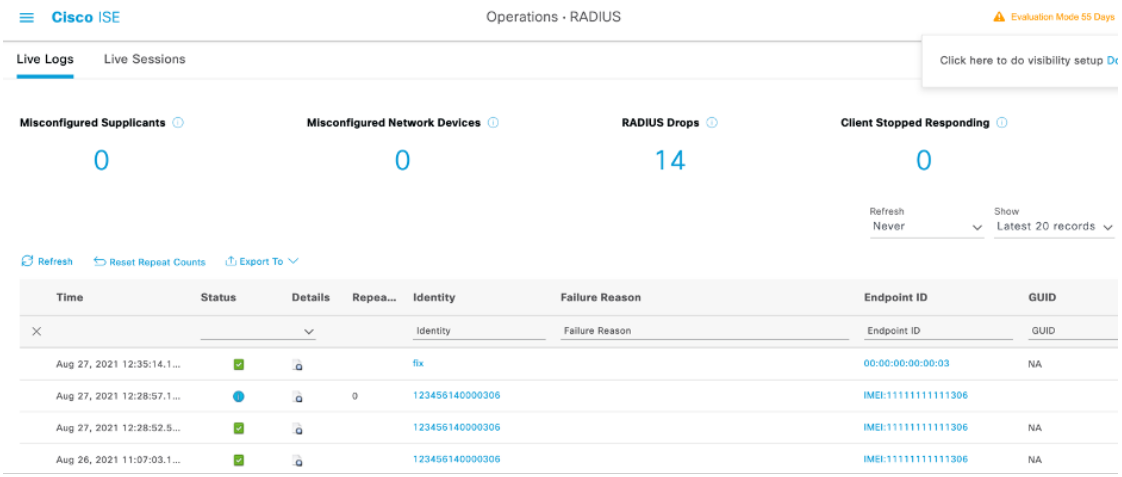
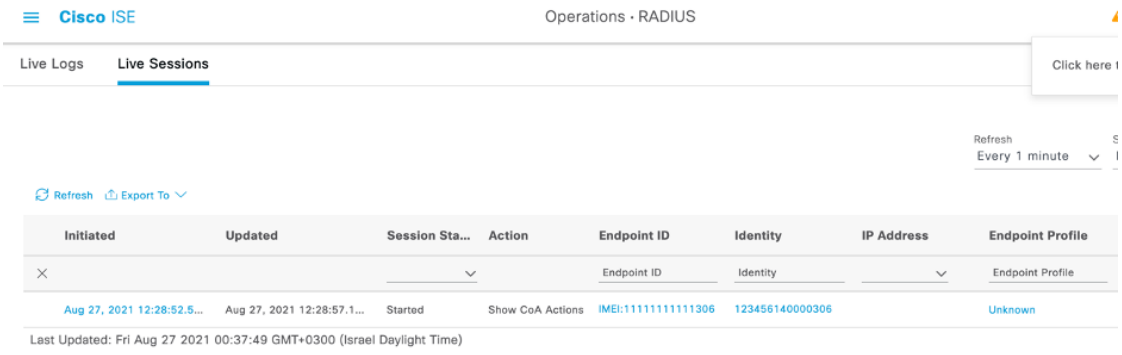


図 *25 : 5G* ライブセッション



翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。