# 安全な有線アクセス



## 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、アカウンティング（AAA）クライアントであり、これを使用して、AAA サービス要求が Cisco ISE に送信されます。Cisco ISE がネットワーク デバイスとやり取りするように、ネットワーク デバイスを定義する必要があります。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 属性を収集するための Simple Network Management Protocol（SNMP）を設定したり、TrustSec デバイスの TrustSec 属性を設定することができます。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。

ネットワーク デバイスの定義：

- 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できます。プロファイルには、URL ダイレクトや許可変更の設定などの、デバイスに事前定義された設定が含まれています。
- RADIUS 認証用の RADIUS プロトコルを設定できます。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。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、RADIUS サーバは、さらにポリシーと設定に基づいて要求を処理します。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。

- TACACS+ 認証用の TACACS+ プロトコルを設定できます。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+ サーバは、さらにポリシーと設定に基づいて要求を処理します。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 に TrustSec 対応デバイスを定義する必要があります。TrustSec ソリューションをサポートするスイッチはすべて TrustSec 対応デバイスです。

  TrustSec デバイスでは IP アドレスは使用されません。代わりに、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。

  TrustSec 対応デバイスは Cisco ISE との通信に TrustSec 属性を使用します。Nexus 7000 シリーズ スイッチ、Catalyst 6000 シリーズ スイッチ、Catalyst 4000 シリーズ スイッチ、Catalyst 3000 シリーズ スイッチなどの TrustSec 対応デバイスは、TrustSec デバイスの追加時に定義した 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、共有秘密にバックスラッシュ（\）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。

# 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。

また、**[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）]** ページで、ネットワークデバイスを作成することもできます。

### 始める前に

ネットワークデバイスで AAA 機能が有効になっていることを確認します。詳細については、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** **[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）]** を選択します。

**ステップ 2** [追加（Add）] をクリックします。

**ステップ 3** ネットワークデバイスの [名前（Name）] を入力します。

**ステップ 4** **IP アドレス**を入力します。

**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** （任意）[SNMP の設定（SNMP Settings）] チェックボックスをオンにして、デバイス情報を収集するプロファイリング サービスの簡易ネットワーク管理プロトコルを設定します。

**ステップ 8** （任意）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

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できます。Cisco ISE にネットワーク デバイスをインポートする前に、インポートしたテンプレートを更新する必要があります。同じリソース タイプ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。

管理者ポータルから CSV テンプレートをダウンロードし、テンプレートにデバイス定義の詳細を入力し、Cisco ISE にインポート可能な CSV ファイルとしてテンプレートを保存できます。

デバイスのインポート中に、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。インポートされたデバイスの数の概要が表示され、インポート プロセス中に見つかったエラーが報告されます。デバイス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、既存のデバイス定義を新しい定義で上書きするか、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。

リリース間でインポート テンプレートが異なるため、Cisco ISE の以前のリリースでエクスポートされたネットワーク デバイスをインポートすることはできません。

（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** **[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）]** を選択します。

**ステップ 2** [インポート（Import）] をクリックします。

**ステップ 3** [参照（Browse）] 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 4** [新しいデータで既存のデータを上書き（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** [インポート（Import）] をクリックします。

# Cisco ISE からのネットワーク デバイスのエクスポート

Cisco ISE で設定されたネットワーク デバイスを CSV ファイル形式でエクスポートし、これを使用して別の Cisco ISE ノードにそれらのネットワーク デバイスをインポートできます。

（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** **[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）]** を選択します。

**ステップ 2** [エクスポート（Export）] をクリックします。

**ステップ 3** ネットワーク デバイス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の隣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。
- 定義されているすべてのネットワーク デバイスをエクスポートするには、**[エクスポート（Export）]> [すべてエクスポート（Export All）]** を選択します。

**ステップ 4** ローカル ハード ディスクに export.csv ファイルを保存します。

# 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** **[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）]** を選択します。

**ステップ 2** 設定を評価するデバイスのネットワーク デバイス IP アドレスを入力し、必要に応じて他のフィールドを指定します。

**ステップ 3** 推奨テンプレートと比較する設定オプションを選択します。

**ステップ 4** [実行（Run）] をクリックします。

**ステップ 5** [ユーザ入力必須（User Input Required）] をクリックし、必要に応じてフィールドを変更します。

**ステップ 6** 分析するインターフェイスの隣のチェックボックスをオンにして、[送信（Submit）] をクリックします。

**ステップ 7** [結果概要の表示（Show Results Summary）] をクリックします。

# Execute Network Device Command 診断ツール

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。結果は、コンソールに表示される場合とまったく同じ形式であり、デバイスの設定における問題を特定するために使用できます。設定が間違っていると思われる場合や、設定を検証したい場合、または単にどのように設定されているか関心がある場合に、使用することができます。

# 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設定でサードパーティ 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+、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。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 などのさまざまなフローに使用する属性および値。これを使用して、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。
- デバイスが持つ認可変更（CoA）機能。RFC 5176 では CoA 要求のタイプが定義されますが、要求に必要な属性はデバイスによって異なります。RFC 5176 サポート付き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」機能もサポートします。RADIUS CoA タイプをサポートしていないデバイスについては、ISE も SNMP CoA をサポートします。CoA タイプの詳細については、以降に説明します。
- デバイスが MAB 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許可プロファイルを自動的に生成します。
- URL リダイレクションは、BYOD、ゲスト、ポスチャなどの高度なフローに必要です。デバイス内で見つかる URL リダイレクションには、スタティックとダイナミックの 2 つのタイプがあります。スタティック URL リダイレクションの場合は、ISE ポータル URL をコピーして設定に貼り付けることができます。ダイナミック URL リダイレクションの場合、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。また、デバイスがダイナミック URL もスタティック URL もサポートしていない場合には、ISE が URL リダイレクトをシミュレートする認証 VLAN を提供します。認証 VLAN は、ISE ボックスで実行されている DHCP/DNS サービスに基づいています。認証 VLAN を作成するには、DHCP/DNS サービス設定を定義します。詳細については、『』の「DHCP および DNS サービス」のセクション「DHCP および DNS サービス」を参照してください。URL リダイレクト フローの詳細については、以降に説明します。

ISE で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、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

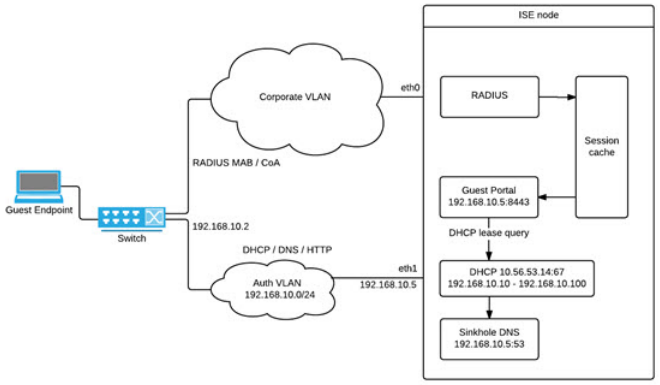
ネットワークでサードパーティデバイスが使用されていて、デバイスがダイナミックまたはスタティック URL リダイレクトをサポートしていない場合、ISE が URL リダイレクト フローをシミュレートします。このようなデバイスの URL リダイレクト シミュレーション フローは、ISE ボックスで DHCP/DNS サービスを実行することで動作します（詳細については、『』の「DHCP および DNS サービス」のセクション「DHCP および DNS サービス」を参照してください）。認証 VLAN フローは次のとおりです。

1. ゲスト エンドポイントが NAD に接続します。
2. デバイスが ISE に RADIUS/MAB 要求を送信します。
3. ISE が認証/承認ポリシーを実行し、ユーザ アカウンティング情報を保存します。
4. 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、ISE DHCP サービスからクライアント IP アドレスと ISE シンクホール DNS IP アドレスを取得します。
7. ゲストエンドポイントがブラウザを開きます。ブラウザが DNS クエリを送信し、ISE IP アドレスを受け取ります。
8. エンドポイント HTTP または HTTPS 要求が ISE ボックスに送られます。
9. ISE は HTTP 301/Moved で応答し、ゲスト ポータル URL を提供します。エンドポイント ブラウザがゲスト ポータル ページにリダイレクトされます。
10. ゲスト エンドポイント ユーザが認証のためにログインします。
11. コンプライアンスの検証が完了すると、ISE は NAD に応答し、CoA の送信、エンドポイントの認証、シンクホールのバイパスを行います。
12. CoA に基づいて適切なアクセスがユーザに提供され、エンドポイントが企業 DHCP から IP アドレスを受信し、ユーザがネットワークを使用できるようになります。

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 は社内ネットワークから分離する必要があります。認証 VLAN IP ヘルパーを設定して ISE マシンを示すか、いずれかの 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。VLAN（DHCP/DNS サーバ）設定の詳細については、『』の「DHCP および DNS サービス」のセクション「DHCP および DNS サービス」を参照してください。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、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。さらに、ゲスト フローについて、通常のゲスト フローと同様にゲスト ポータルを定義して、MAB 認証にバインドされる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、『』の「Cisco ISE ゲスト サービス」のセクションCisco ISE ゲスト サービスを参照してください。

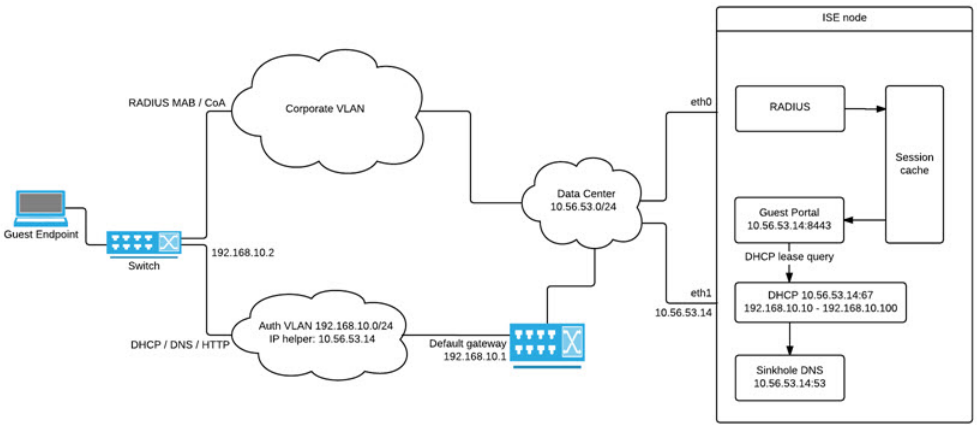
次の図に、認証 VLAN が定義されているときの基本的なネットワーク設定を示します（認証 VLAN が Cisco ISE ノードに直接接続されています）。

**図 *1 : Cisco ISE* ノードに接続する認証 *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***




## CoA タイプ

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。ISE から NAD を設定するときにデバイスによってサポートされる RADIUS および SNMP の設定を定義し、NAD プロファイルを設定するときに特定のフローのために使用される CoA タイプを示します。NAD のプロトコルの定義の詳細については、『』の「ネットワーク デバイス」のセクション「ネットワーク デバイス」を参照してください。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、一部の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。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 は、次の表に記載されているベンダー デバイスでテストされています。

**表 *1 : Cisco ISE 2.1* でテスト済みのベンダー デバイス**

| **Device Type** | **Vendor** | **CoA タイプ** | **URL リダイレクト タイプ** | サポートされる/検証済みの使用例 | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | **802.1X/ MAB** | **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/BYOD** |
| ワイヤレス | Aruba 7000、InstantAP | RADIUS | スタティック URL | √ | √ | √ | √ | √ |
| | Motorola RFS 4000 | RADIUS | ダイナミック URL | √ | √ | √ | √ | √ |
| | HP 830 | RADIUS | スタティック URL | √ | √ | √ | √ | √ |
| | Ruckus ZD 1200 | RADIUS | — | √ | √ | √ | √ | √ |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 有線 | HP A5500 | RADIUS | ISE が提供する認証 VLAN | √ | √ | √ | √ | √ |
| | HP 3800 および 2920 (ProCurve) | RADIUS | ISE が提供する認証 VLAN | √ | √ | √ | √ | √ |
| | Alcatel 6850 | SNMP | ダイナミック URL | √ | √ | √ | √ | √ |
| | Brocade ICX 6610 | RADIUS | ISE が提供する認証 VLAN | √ | √ | √ | √ | √ |
| | Juniper EX3300-24p | RADIUS | ISE が提供する認証 VLAN | √ | √ | √ | √ | √ |
| 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。 | | | | √ | √ | CoA サポートが必要 | CoA サポートが必要です。URL リダイレクトについて、有線デバイスに URL リダイレクトがない場合は、ISE 認証 VLAN を利用します。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できます。ゲスト、BYOD、ポスチャなどの高度なフローについては、デバイスは、RFC 5176、「許可変更（CoA）」をサポートしている必要があります。これらのフローに対するサポートは、NAD の機能によって異なります。ネットワーク デバイス プロファイルに必要な多くの属性については、デバイスの管理ガイドを参照する必要があります。

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

ISE Community Resource

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、サードパーティ製ネットワーク アクセス デバイス（NAD）をサポートします。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

『Cisco Identity Services Engine 管理者ガイド』のネットワーク デバイス プロファイル （9 ページ）の定義を確認してください。

**ステップ 1** デバイスが ISE で設定されていることを確認します。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、認可変更（CoA）が定義され、NAD の URL リダイレクト機能が、関連する 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 リダイレクトの場合は、ポータルのランディング ページから ISE ポータルの URL をコピーできます。ISE の NAD の CoA タイプおよび URL リダイレクトの設定に関する詳細については、『』の「ネットワークデバイス」のセクションネットワークデバイス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 デバイスの管理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 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 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 （12 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。**[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）]** を選択します。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 リストから適切な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 プロファイルに明示的に設定する必要があります。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、[いずれか（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。関連する認可プロファイルを開き、[ネットワーク デバイス プロファイル（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、『』の「Cisco ISE ゲスト サービス」のセクションCisco ISE ゲスト サービスを参照してください。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

- カスタム プロファイルの作成方法の詳細については、『Network Access Device Profiles with Cisco Identity Services Engine』ドキュメントを確認してください。
- ほとんどの NAD には、標準の IETF RADIUS 属性に加えて多数のベンダー固有の属性を提供する、ベンダー固有の RADIUS ディクショナリがあります。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。ISE から、**[ポリシー要素（Policy Elements）]** > **[ディクショナリ（Dictionaries）]** > **[システム（System）]** > **[RADIUS]** > **[RADIUS ベンダー（RADIUS Vendors）]** を選択します。RADIUS ディクショナリのインポートの詳細については、『』の「RADIUS ベンダー ディクショナリの作成」のセクション 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、デバイスは RFC 5176、許可変更（CoA）を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値の詳細については、『』の「ネットワーク デバイス プロファイルの設定」のセクション「ネットワーク デバイス プロファイルの設定」を参照してください。

---

**ステップ 1** **[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。

**ステップ 2** [追加（Add）] をクリックします。

**ステップ 3** ネットワーク デバイスの名前と説明を入力します。

**ステップ 4** 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** 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。デバイスが RADIUS、TACACS+、TrustSec をサポートする場合には、各ボックスにマークを付けます。実際に使用するプロトコルにのみマークを付ける必要があります。デバイスが RADIUS をサポートしている場合は、[RADIUS ディクショナリ（RADIUS Dictionaries）] フィールドのダイナミック 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 RADIUS ディクショナリを選択します。

**ステップ 6** [テンプレート（Templates）] セクションから次のように関連情報を入力します。

a) [認証/許可（Authentication/Authorization）] から、フローのタイプ、属性エイリアシングおよびホスト ルックアップに対するデバイスのデフォルト設定を設定します。[フロータイプの条件（Flow Type Conditions）] には、デバイスが有線 MAB または 802.1x などのさまざまなフローに使用する、属性と値を入力してください。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 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 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）] から、デバイス固有の属性名を共通名にマップして、ポリシー ルールを簡素化することができます。現在は、SSID のみが定義されています。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。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 つのルールの 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）] から、[ホストルックアップの処理（Process Host Lookup）] オプションを有効にして、サードパーティの指示に基づいて、デバイスに関連する MAB プロトコルと属性を選択します。

b) [権限（Permissions）] から、VLAN および 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。これらは自動的に、ISE で作成した認可プロファイルに基づいてマッピングされます。

c) [許可変更（CoA）（Change of Authorization（CoA））] から、デバイスの CoA 機能を設定します。

d) [リダイレクト（Redirect）] セクションを展開し、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 およびポスチャに必要です。

**ステップ 7** [送信（Submit）] をクリックします。

# 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

XML ファイルを編集してから、そのファイルを新しいネットワーク プロファイルとしてインポートするために、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 形式でエクスポートします。

### 始める前に

『Network Access Device Profiles with Cisco Identity Services Engine』のドキュメントを参照してください。

**ステップ 1** **[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。

**ステップ 2** [エクスポート（Export）] をクリックします。

**ステップ 3** エクスポートするデバイスの隣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。

**ステップ 4** DeviceProfiles.xml 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、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できます。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します。必要に応じて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てから、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一緒にインポートして、ISE で複数のファイルを作成します。

デバイスプロファイルのインポート中は、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。既存のプロファイルを編集してから上書きするには、既存のプロファイルをエクスポートし、ISE からそのプロファイルを削除してから、適切に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

『Network Access Device Profiles with Cisco Identity Services Engine』のドキュメントを参照してください。

**ステップ 1** **[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。

**ステップ 2** [インポート（Import）] をクリックします。

**ステップ 3** [参照（Browse）] 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** [インポート（Import）] をクリックします。

# ネットワークデバイスグループ（NetworkDeviceGroups）

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。NDG は、地理的な場所、デバイス タイプ、ネットワーク内での相対的な位置（アクセス レイヤ、データ センターなど）のようなさまざまな基準に基づいて、ネットワーク デバイスを論理的にグループ化するために使用できます。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できます。

- アフリカ -> 南部 -> ナミビア
- アフリカ -> 南部 -> 南アフリカ
- アフリカ -> 南部 -> ボツワナ

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することもできます。

- アフリカ -> 南部 -> ボツワナ -> ファイアウォール
- アフリカ -> 南部 -> ボツワナ -> ルータ
- アフリカ -> 南部 -> ボツワナ -> スイッチ

ネットワーク デバイスは、1 つ以上の階層型 NDG に割り当てることができます。したがって、Cisco ISE が、設定された NDG の順序リスト全体を参照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とき、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ている場合、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 NDG の最大数に制限はありません。NDG 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。

ツリー ビューやフラット テーブル ビューでデバイス グループ階層を表示できます。ツリー ビューで、ルート ノードはツリーの最上位に表示され、子グループが階層順序で次に続きます。各ルート グループに属する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 グループだけを表示するには、[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 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。

また、各子グループに割り当てられたネットワーク デバイスの数を確認できます。そのデバイス グループに割り当てられているすべてのネットワーク デバイスを一覧表示する、[ネットワーク デバイス（Network Devices）] ウィンドウを起動するには、この番号付きリンクをクリックしてください。デバイス グループに追加デバイスを追加したり、別のデバイス グループに既存のデバイスを移動できます。

デバイス グループを追加するときに、新しいグループをルート グループとして追加するか、親グループとして既存のグループを選択する必要があるかどうかを指定できます。

（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 タイプとすべてのロケーションという 2 つの定義済みルート NDG が含まれます。これらの事前定義された NDG 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 グループを追加できます。

ルート ネットワーク デバイス グループ（NDG）を作成し、[ネットワーク デバイス グループ（Network Device Groups）] ページでそのルート グループの下に子 NDG 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に定義されているデバイス ディクショナリに追加され、ポリシー定義に使用できるようになります。Cisco ISE では、デバイス タイプ、ロケーション、モデル名、およびネットワーク 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に基づい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。同じリソース タイプ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 グループをインポートできません。

管理者ポータルから CSV テンプレートをダウンロードし、テンプレートにデバイス グループの詳細を入力し、Cisco ISE にインポート可能な CSV ファイルとしてテンプレートを保存できます。

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** **[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）] > [グループ（Groups）]** を選択します。

**ステップ 2** [インポート（Import）] をクリックします。

**ステップ 3** [参照（Browse）] 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 4** [新しいデータで既存のデータを上書き（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** [ネットワーク デバイス グループ（Network Device Groups）] リスト ページに戻るには、[インポート（Import）] または [ネットワーク デバイス グループ リスト（Network Device Groups List）] リンクをクリックします。

# 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 に設定されたネットワーク デバイス グループを CSV ファイル形式でエクスポートし、これを使用して別の Cisco ISE ノードにそれらのネットワーク デバイス グループをインポートできます。

**ステップ 1** **[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）] > [グループ（Groups）]** を選択します。

**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。

**ステップ 3** ローカル ハード ディスクに export.csv ファイルを保存します。

# ネットワーク デバイス グループ（Network Device Groups）

これらのページを使用すると、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できる [ネットワーク デバイス グループ（Network Device Groups）]ページのフィールドについて説明します。このページへのナビゲーション パスは、**[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 グループ（Network Device Groups）]** > **[グループ（Groups）]** です。

**[ワークセンター（Work Centers）]** > **[デバイス管理（Device Administration）]** > **[ネットワークデバイスグループ（Network Device Groups）]** > **[グループ（Groups）]** ページでネットワーク デバイス グループを作成することもできます。

**表 *2:* ネットワーク デバイス グループの設定**

| フィールド | 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（NDG）の名前を入力します。ルート NDG の下の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、新しいネットワーク デバイス グループの名前を入力します。<br><br>ルート ノードを含み、最大で 6 つのノードを NDG 階層に含めることができます。各 NDG 名は最大 32 文字です。 |
| 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。 |
| 親グループ（Parent Group） | 親グループとして既存のグループを選択するか、ルートグループとして、この新しいグループを追加できます。 |

**関連トピック**

ネットワーク デバイス グループ（Network Device Groups） （14 ページ）
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 （15 ページ）
Cisco ISE でのネットワークデバイスの追加

# 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、Cisco ISE にネットワーク デバイス グループを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 グループ インポート（Network Device Group Import）] ページのフィールドについて説明します。このページへのナビゲーション パスは、**[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 グループ（Network Device Groups）]** > **[グループ（Groups）]** です。

**表 *3:* ネットワーク デバイス グループのインポート設定**

| フィールド | 使用上のガイドライン |
|---|---|
| テンプレートの生成（Generate a Template） | カンマ区切り形式（.csv）テンプレート ファイルを作成するには、このリンクをクリックします。<br><br>同じ形式のネットワーク デバイス グループ情報でテンプレートを更新し、それらのネットワーク デバイス グループを Cisco ISE 展開にインポートするためにローカルで保存します。 |
| ファイル（File） | 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カンマ区切り形式ファイルの場所を参照するには、[参照（Browse）] をクリックします。<br><br>インポートを使用して、新しい、更新されたネットワーク デバイス グループ情報を含むネットワーク デバイス グループを別の Cisco ISE 展開に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） | Cisco ISE で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。<br><br>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。 |

| フィールド | 使用上のガイドライン |
|---|---|
| 最初のエラーでインポートを停止（Stop Import on First Error） | インポート中にエラーが発生すると、Cisco ISE にインポートを中止させる場合、このチェックボックスをオンにしますが、Cisco ISE はエラーのその時点までネットワーク デバイス グループをインポートします。<br><br>このチェックボックスがオフで、エラーが発生した場合は、エラーが報告され、Cisco ISE はデバイス グループを引き続きインポートします。 |

**関連トピック**

ネットワーク デバイス グループ（Network Device Groups） （14 ページ）
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 （15 ページ）
Cisco ISE へのネットワーク デバイス グループのインポート （16 ページ）

# Cisco ISE でのテンプレートのインポート

Cisco ISE では、カンマ区切り形式（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。ヘッダー行は編集しないでそのまま使用してください。

デフォルトで、[テンプレートの生成（Generate a Template）] リンクを使用して、Microsoft Office Excel アプリケーションに CSV ファイルをダウンロードし、このファイル形式をシステム上にローカルに保存できます。[テンプレートの生成（Generate a Template）] リンクをクリックすると、Cisco ISE サーバは、[template.csv を開く（Opening template.csv）] ダイアログを表示します。このダイアログを使用すると、template.csv ファイルを開いて、その template.csv ファイルにネットワーク デバイスおよびネットワーク デバイス グループに適切な名前を付けて、システム上にローカルに保存できます。このダイアログで template.csv ファイルを開くことを選択した場合、このファイルはデフォルトで Microsoft Office Excel アプリケーションで開かれます。

## ネットワーク デバイスのインポート テンプレート形式

次の表では、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 *4:* 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 | 説明 |
|---|---|
| Name：文字列（32） | （必須）このフィールドはネットワーク デバイスの名前です。これは、最大32文字の英数字文字列です。 |
| Description:String(256) | このフィールドは、ネットワーク デバイスの任意の説明です。最大 256 文字の文字列。 |
| IP Address:Subnets（a.b.c.d/m\|...） | （必須）このフィールドは、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です。（パイプ記号「\|」で区切って複数の値を指定できます）。<br>IPv4 および IPv6、ネットワーク デバイス（TACACS および RADIUS）設定および外部 RADIUS サーバ設定でサポートされるようになりました。<br>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。 |
| Model Name：文字列（32） | （必須）このフィールドはネットワーク デバイスのモデル名です。これは、最大32文字の文字列です。 |
| Software Version：文字列（32） | （必須）このフィールドはネットワーク デバイスのソフトウェアバージョンです。これは、最大 32 文字の文字列です。 |
| Network Device Groups：文字列（100） | （必須）このフィールドは、既存のネットワーク デバイス グループにする必要があります。サブグループを指定できますが、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) | これはオプションのフィールドです。認証に使用するプロトコルです。唯一の有効な値は RADIUS です（大文字と小文字は区別されません）。 |
| Authentication:Shared Secret:String(128) | （認証プロトコルのフィールドの値を入力した場合は必須）このフィールドは、最大 128 文字の文字列です。 |

| フィールド | 説明 |
|---|---|
| EnableKeyWrap：ブール（true\|false） | これはオプションのフィールドです。これはネットワーク デバイスでサポートされている場合に限り有効です。有効な値は true または false です。 |
| 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示します。<br>ASCII：16 文字（バイト）の長さ<br>16 進数：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 Hashed Message Authentication Code（HMAC）の計算を示します。<br>ASCII：20 文字（バイト）の長さ<br>16 進数：40 文字（バイト）の長さ。 |
| InputFormat：文字列（32） | 暗号化と認証キーの入力形式を示します。有効な値は、ASCII または Hexadecimal です。 |
| SNMP:Version：列挙（\|2c\|3） | これはオプションのフィールドで、プロファイラ サービスによって使用されます。SNMP プロトコルのバージョンです。有効な値は1、2c、または 3 です。 |
| SNMP:RO Community:String(32) | （SNMP バージョンのフィールドの値を入力した場合は必須）SNMP読み取り専用のコミュニティ。これは、最大32 文字の文字列です。 |
| SNMP:RW Community:String(32) | （SNMP バージョンのフィールドの値を入力した場合は必須）SNMP 読み取り書き込みコミュニティ。これは、最大32 文字の文字列です。 |
| SNMP:Username:String(32) | これはオプションのフィールドです。これは、最大 32 文字の文字列です。 |
| SNMP:Security Level:Enumeration(Auth\|No Auth\|Priv) | （SNMPバージョン3を選択した場合は必須）有効な値は、Auth、No Auth、または Priv です。 |
| 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）有効な値は、MD5 または SHA です。 |

| フィールド | 説明 |
|---|---|
| SNMP:Authentication Password:String(32) | （SNMP セキュリティ レベルで Auth を入力した場合は必須）これは、最大 32 文字の文字列です。 |
| SNMP:Privacy Protocol:Enumeration(DES\|AES128\|AES192\|AES256\|3DES) | （SNMP セキュリティ レベルで Priv を入力した場合は必須）有効な値は、DES、AES128、AES192、AES256、または 3DES です。 |
| SNMP:Privacy Password:String(32) | （SNMP セキュリティ レベルで Priv を入力した場合は必須）これは、最大 32 文字の文字列です。 |
| SNMP:Polling Interval:Integer:600-86400 seconds | これはオプションのフィールドで、SNMP ポーリング間隔を設定します。有効な値は 600 ～ 86400 の整数です。 |
| SNMP:Is Link Trap Query:Boolean(true\|false) | これはオプションのフィールドで、SNMP リンク トラップを有効または無効にします。有効な値は true または false です。 |
| SNMP:Is MAC Trap Query：ブール（true\|false） | これはオプションのフィールドで、SNMP MAC トラップを有効または無効にします。有効な値は true または false です。 |
| SNMP:Originating Policy Services Node：文字列（32） | これはオプションのフィールドです。SNMP データのポーリングに使用される ISE サーバを示します。デフォルトでは自動ですが、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） | これはオプションのフィールドです。これは、TrustSec デバイス ID で、最大 32 文字の文字列です。 |
| Trustsec:Device Password：文字列（256） | （TrustSec デバイス ID を入力した場合は必須）これは TrustSec デバイスのパスワードで、最大 256 文字の文字列です。 |
| Trustsec:Environment Data Download Interval：整数：1-2147040000 秒 | これはオプションのフィールドです。これは TrustSec 環境データのダウンロード間隔です。有効な値は 1 ～ 24850 の整数です。 |
| Trustsec:Peer Authorization Policy Download Interval：整数：1-2147040000 秒 | これはオプションのフィールドです。これは TrustSec のピア許可ポリシーのダウンロード間隔です。有効な値は 1 ～ 24850 の整数です。 |

| フィールド | 説明 |
|---|---|
| Trustsec:Reauthentication Interval：整数：1-2147040000 秒 | これはオプションのフィールドです。これは TrustSec の再認証間隔です。有効な値は 1 ～ 24850 の整数です。 |
| Trustsec:SGACL List Download Interval：整数：1-2147040000 秒 | これはオプションのフィールドです。また、TrustSec SGACL リストのダウンロード間隔です。有効な値は 1 ～ 24850 の整数です。 |
| Trustsec:Is Other Trustsec Devices Trusted：ブール（true\|false） | これはオプションのフィールドです。TrustSec が信頼できるかどうかを示します。有効な値は true または false です。 |
| Trustsec:Notify this device about Trustsec configuration changes：文字列（ENABLE_ALL\|DISABLE_ALL） | これはオプションのフィールドです。TrustSec デバイスに対する TrustSec 設定変更を通知します。有効な値は ENABLE_ALL または DISABLE_ALL です |
| Trustsec:Include this device when deploying Security Group Tag Mapping Updates：ブール（true\|false） | これはオプションのフィールドです。これは、SGT に含まれる TrustSec デバイスです。有効な値は true または false です。 |
| Deployment:Execution Mode Username:String(32) | これはオプションのフィールドです。デバイス設定を編集する権限を持っているユーザ名です。これは、最大 32 文字の文字列です。 |
| Deployment:Execution Mode Password:String(32) | これはオプションのフィールドです。デバイス パスワードで、最大 32 文字の文字列です。 |
| Deployment:Enable Mode Password:String(32) | これはオプションのフィールドです。設定を編集するためのデバイスのイネーブルパスワードで、最大 32 文字の文字列です。 |
| Trustsec:PAC issue date：日付 | これは、TrustSec デバイス用に Cisco ISE によって生成された最後の TrustSec PAC の発行日を表示するフィールドです。 |
| Trustsec:PAC expiration date：日付 | これは、TrustSec デバイス用に Cisco ISE によって生成された最後の TrustSec PAC の有効期限を表示するフィールドです。 |
| Trustsec:PAC issued by：文字列 | これは、TrustSec 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（TrustSec 管理者）の名前を表示するフィールドです。文字列です。 |

# 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 *5:* 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、親グループ Global > Asia の下にサブグループ India を作成している場合、作成する NDG の完全な名前は Global#Asia#India になり、この完全な名前の長さは 100 文字を超えることはできません。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、オプションのネットワーク デバイス グループの説明です。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-NAD 通信を保護する IPsec セキュリティ

インターネット プロトコル セキュリテ（IPsec）は、インターネット プロトコルにセキュリティを提供するプロトコルのセットです。AAA プロトコル、RADIUS および TACACS+ 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、送信者を認証し、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。

IPSec は、スマート ライセンスがデフォルトで有効になっているため（e0/2—> eth2）、ギガビット イーサネット 2 で有効にすることはできません。ただし、IPSec を有効にする必要がある場合は、スマート ライセンスに別のインターフェイスを選択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 およびギガビット 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。ギガビット イーサネット 0 およびボンド 0 では IPsec はサポートされていません。

必要なコンポーネントには次のものがあります。

- Cisco ISE、リリース 2.2 以降
- Cisco IOS ソフトウェア、C5921 ESR（埋め込み型サービス ルータ）ソフトウェア（C5921_I86-UNIVERSALK9-M）：ESR 5921 設定では、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。

# 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でのみ設定できます。

**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) [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）] の順に選択します。
b) [ネットワーク デバイス（Network Devices）] ページで [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、サブネットを入力します。
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) [送信（Submit）] をクリックします。

**ステップ 3** （オプション。スマート ライセンスでのみ必要）。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。また、ESR にはスマート ソフトウェア マネージャ サテライトも使用できます。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（またはボンド 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 サーバにアクセスできる必要があります。

**ステップ 4** Cisco ISE 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** IPsec に対し Cisco ISE ノードを有効にします。

a) [管理（Administration）] > [システム（System）] > [設定（Settings）] > [プロトコル（Protocols）] > [IPSec] を選択します。

展開内のすべての Cisco ISE ノードがこのページにリストされます。

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 通信に使用するインターフェイスを選択します。
d) 次のオプションから、選択されている ISE ノードの認証タイプを選択します。

- [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 での事前共有キー設定の出力 （35 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 （29 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、異なる設定で 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 ポートを受け入れます。

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

**ステップ 7** （オプション：ステップ 3 でスマート ライセンスを有効にしていない場合にのみ必要）。Classic ライセンスまたは Evaluation ライセンス（有効期間 90 日）を Cisco ISE アプライアンスに追加します。

- Cisco ISE CLI から次のコマンドを実行してライセンス ファイルをダウンロードします。

```
ise/admin# license esr classic import esr.lic repository esrrepo
```

Classic ライセンスの詳細については、『Cisco 5921 Embedded Services Router Integration Guide』の「Licensing the Software with Classic Licensing」を参照してください。

**ステップ 8** 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 にユーザを追加し、ユーザ グループに割り当てます（[管理（Administration）] > [ID 管理（Identity Management）] > [ID（Identities）] > [ユーザ（Users）]）。

b) Cisco ISE と NAD の間で IPsec トンネルが確立されていることを確認します。手順は次のとおりです。

1. **ping** コマンドを使用して、Cisco ISE と NAD の間の接続が確立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 CLI から次のコマンドを実行して、接続がアクティブ状態であるかどうかを確認します。 **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）] ページで詳細を確認します。
- 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）] ページで詳細を確認します。

# ESR-5921 での X.509 証明書の設定とインストール

ESR-5921 で X.509 証明書を設定およびインストールするには、次の手順を実行します。

**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 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** CSR 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、署名された証明書と 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 CA 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。

以下に、Cisco 5921 ESR で X.509 証明書を設定してインストールするときの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
```

以下に、Cisco Catalyst 3850 で X.509 証明書を設定してインストールするときの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 での事前共有キー設定の出力

Cisco Catalyst 3850 で事前共有キーを設定する場合の出力の例を次に示します。

```
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
```

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

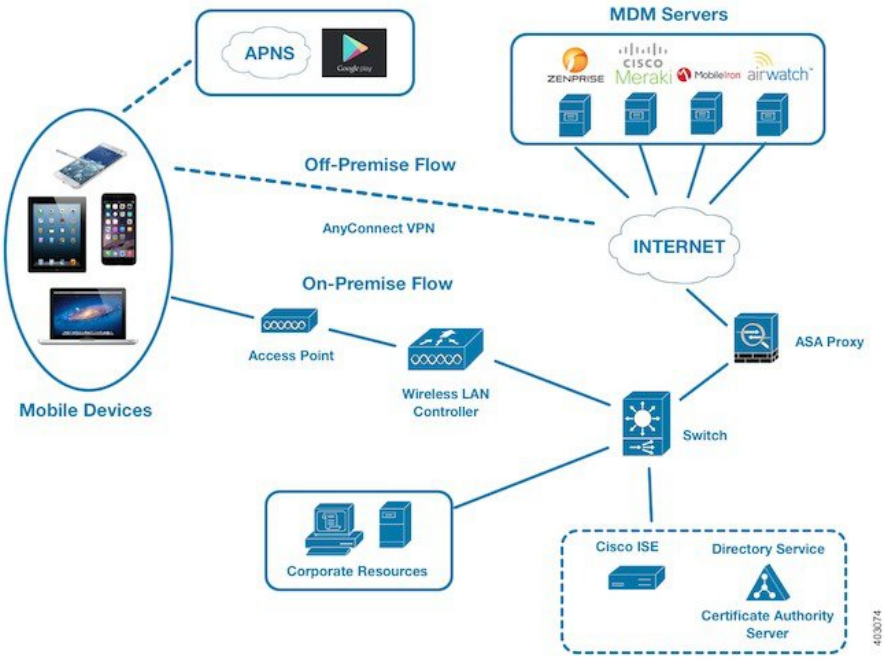
モバイルデバイス管理（MDM）サーバはモバイル事業者、サービスプロバイダー、企業にわたって展開されたモバイルデバイスの保護、モニタ、管理、およびサポートを行います。MDM サーバはポリシー サーバとして機能し、ポリシー サーバは展開環境のモバイル デバイスにある一部のアプリケーション（電子メール アプリケーションなど）の使用を制御します。ただし、ネットワークは、ACL に基づいてエンドポイントへのきめ細かいアクセス権を提供できる唯一のエンティティです。Cisco ISE は必要なデバイス属性について MDM サーバにクエリを行い、それらのデバイスに対してネットワーク アクセス コントロールを提供する ACL を作成します。

さまざまなベンダーからのサーバなど、複数のアクティブな MDM サーバ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、シスコの MDM API バージョン 2 を使用して MDM サーバと統合し、デバイスが AnyConnect 4.1 および Cisco ASA 9.3.2 以降を介して VPN 経由でネットワークにアクセスできるようにします。

この図では、Cisco ISE が適用ポイントで、MDM ポリシー サーバがポリシー情報ポイントです。Cisco ISE は、MDM サーバ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 つ以上の外部 Mobile Device Manager（MDM）サーバと相互運用するように Cisco ISE を設定できます。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活用できます。Cisco ISE は REST API コールを使用して、外部 MDM サーバ

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、Cisco ISE ネットワークへのリモート デバイス アクセスをより適切に制御します。

サポートされる MDM ベンダーは次のとおりです。サポートされる MDM サーバ（38 ページ）

# サポートされる MDM の使用例

Cisco ISE が外部 MDM サーバを使用して実行する機能は、次のとおりです。

- 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 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だけが付与されます。
- エンドポイント データの増加：Cisco ISE プロファイラを使用して収集できない、MDM サーバの情報でエンドポイント データベースを更新します。エンドポイントが MDM のモニタ対象デバイスの場合、Cisco ISE は **[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）]** ページを使用して表示できる 6 つのデバイス属性を使用します。次に例を示します。
  - MDMImei: 99 000100 160803 3
  - MDMManufacturer: Apple
  - MDMModel: iPhone
  - MDMOSVersion: iOS 6.0.0
  - MDMPhoneNumber: 9783148806
  - MDMSerialNumber: DNPGQZGUDTF9
- Cisco ISE は、4 時間ごとに MDM サーバをポーリングし、デバイス コンプライアンス データを確認します。これは管理者が設定できます。
- MDM サーバを介したデバイス手順の発行：MDM サーバを介してユーザのデバイスに対するリモート アクションを発行します。管理者は、ISE コンソールからリモート操作を開始します。

### ベンダー MDM 属性

ISE で MDM サーバを設定すると、このベンダーの属性は ISE システム ディクショナリに **mdm** という名前で新しいエントリに追加されます。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。

- DeviceRegisterStatus
- DeviceCompliantStatus
- DiskEncryptionStatus

- PinLockStatus
- JailBrokenStatus
- Manufacturer
- IMEI
- SerialNumber
- OsVersion
- PhoneNumber
- MDMServerName
- MDMServerReachable
- MEID
- モデル
- UDID

ベンダー固有の属性はサポートされませんが、ベンダーがその属性をサポートする場合は、ERS API を使用してベンダー固有の属性を変換できる場合があります。

新しい MDM ディクショナリ属性は許可ポリシーで使用可能です。

# サポートされる MDM サーバ

サポートされる MDM サーバは、次のベンダーの製品です。

- 絶対値（Absolute）
- AirWatch
- Citrix XenMobile
- Globo
- Good Technology
- IBM MaaS360
- JAMF ソフトウェア
- Meraki SM/EMM
- MobileIron
- SAP Afaria
- SOTI
- Symantec
- Tangoe

- Microsoft Intune - モバイル デバイス用
- Microsoft SCCM -デスクトップ デバイス用

**ISE コミュニティ リソース**

How To: Meraki EMM / MDM Integration with ISE

# MDM サーバにより使用されるポート

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

**表 *6 : MDM* サーバにより使用されるポート**

| MDM サーバ | ポート |
|---|---|
| MobileIron | 443 |
| Zenprise | 443 |
| Good | 19005 |
| Airwatch | 443 |
| Afaria | 443 |
| Fiberlink MaaS | 443 |
| Meraki | 443 |
| Microsoft Intune | 80 および 443 |
| Microsoft SCCM | 80 および 443 |

# MDM 統合プロセス フロー

ここでは、MDM 統合プロセスについて説明します。

1. ユーザはデバイスを SSID に関連付けます。
2. Cisco ISE は、MDM サーバに対して API コールを実行します。
3. この API コールは、このユーザ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。

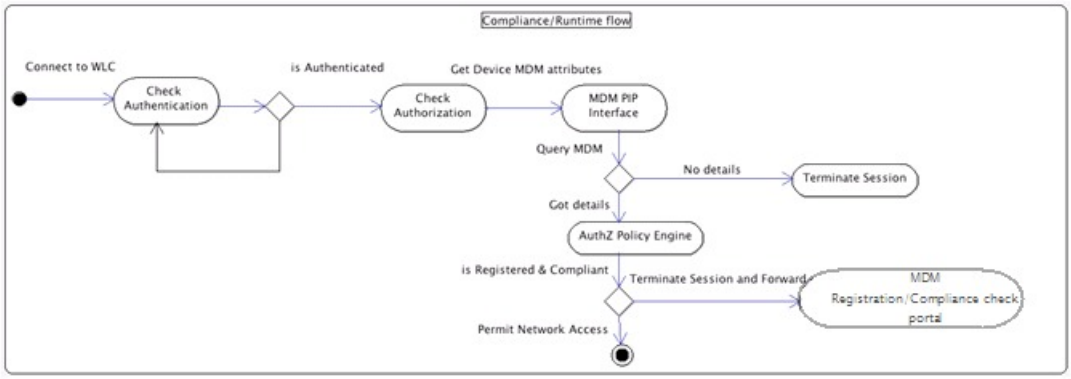
（注） 入力パラメータは、エンドポイント デバイスの MAC アドレスです。構外の Apple iOS デバイスの場合は UDID です。

4. ユーザ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。ユーザが MDM サーバ ページに表示されます。

（注） MDM ポータルを介して Cisco ISE ネットワークの外の MDM サーバに登録済みのデバイスを登録する必要があります。これは Cisco ISE、リリース 1.4 以降に適用されます。ISE の以前のバージョンでは、Cisco ISE ネットワークの外に登録済みのデバイスはポスチャ ポリシーに準拠している場合に自動的に登録されます。

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ページをユーザに表示します。
6. ユーザは MDM サーバにデバイスを登録し、MDM サーバは Cisco ISE に要求をリダイレクトします（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）。
7. Cisco ISE は MDM サーバ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. ユーザのデバイスが MDM サーバ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おらず、準拠する必要があることがユーザに通知されます。
9. ユーザのデバイスがポリシーに準拠するようになった後、MDM のサーバ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 サーバを 4 時間ごとにポーリングし、必要に応じて許可変更（CoA）を発行します。これは管理者が設定できます。また、Cisco ISE は 5 分ごとに MDM サーバをチェックして使用できるかどうかを確認します。

次の図は、MDM プロセス フローを示しています。




（注） 一度に 1 つの MDM サーバ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、[設定（Settings）] > [全般（General）] > [デバイス管理（Device management）] の順に移動し、削除の管理をクリックすることができます。または、ISE の MyDevices ポータルに移動し、企業ワイプをクリックすることができます。

# Cisco ISE による MDM サーバの設定

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

**ステップ 1** Azure に 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** ワイヤレス LAN コントローラの ACL を設定します。

**ステップ 4** MDM サーバに未登録のデバイスをリダイレクトするための許可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 サーバがある場合は、各ベンダーに個別の許可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 MDM サーバ証明書のインポート

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

（注） Microsoft Azure の場合は、ISE 証明書を Azure にインポートします。詳細については、MDM サーバとしての Microsoft Intune の設定 （46 ページ）を参照してください。

**ステップ 1** MDM サーバ証明書を MDM サーバ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** **[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificate）] > [インポート（Import）]** を選択します。

**ステップ 3** [参照（Browse）] をクリックして、MDM サーバから取得した MDM サーバ証明書を選択します。

**ステップ 4** わかりやすい名前を追加します。

**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）] リスト ページに MDM サーバ証明書が一覧表示されることを確認します。

### 次のタスク

ISE でのモバイル デバイス管理サーバの定義 （42 ページ）

。

## ISE でのモバイル デバイス管理サーバの定義

外部 MDM サーバ用のモバイル デバイス管理（MDM）定義とデスクトップ デバイス マネージャ（SCCM）定義を 1 つ以上作成できます。

1. **[管理（Administration）] > [ネットワーク リソース（Network Resources）] > [外部 MDM（External MDM）]** の順に選択します。
2. [追加（Add）] をクリックします。
3. 追加する MDM サーバの名前と説明を入力します。
4. [サーバ タイプ（Server Type）] で、[モバイル デバイス マネージャ（Mobile Device Manager）] または [デスクトップ デバイス マネージャ（Desktop Device Manager）] を選択します。どちらを選択するかで、どのフィールドが次に表示されるかが決定します。[デスクトップ デバイス マネージャ（Desktop Device Manager）] を選択した場合は、「デスクトップ デバイス管理 （44 ページ）」に進みます。[モバイルデバイス マネージャ（Mobile Device Manager）] を選択した場合は、次の手順を続行します。
5. [認証タイプ（Authentication Type）] で、[ベーシック（Basic）] または [OAuth - クライアント クレデンシャル（OAuth - Client Credentials）] を選択します。Microsoft Intune サーバを設定する [OAuth -クライアント クレデンシャル（OAuth - Client Credentials）] を選択した場合は、「モバイル デバイス管理 - OAuth - クライアント クレデンシャル（Mobile Device

Management - OAuth - Client Credentials）（43 ページ）」に進みます。[ベーシック（Basic）] を選択した場合は、次の手順を続行します。

6. すべての画面で、MDM サーバ定義の名前と説明が求められます。ここでは、サーバと認証タイプに基づいて、その他のフィールドと手順について説明しています。

### モバイル デバイス管理：ベーシック

- ホスト名/IPアドレス（Host Name / IP Address）：MDM サーバのホスト名または IP アドレスを入力します。
- ポート（Port）：MDM サーバとの接続に使用するポートを入力します。通常は 443。
- インスタンス名（Instance Name）：この MDM サーバ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。
- ポーリング間隔（Polling Interval）：Cisco ISE が MDM サーバをポーリングしてコンプライアンス チェック情報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。ネットワーク上の少数のアクティブ クライアントをテストする場合のみポーリング間隔を 60 分未満に設定することを推奨します。多くのアクティブ クライアントを持つ実稼働環境でこの値を 60 分未満に設定すると、システムの負荷が大幅に増加し、パフォーマンスに悪影響を与える場合があります。

  ポーリング間隔を 0 に設定すると、ISE は MDM サーバとの通信をディセーブルにします。
- 準拠デバイス再認証クエリの間隔（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、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が [準拠デバイス再認証クエリの間隔（Time Interval For Compliance Device ReAuth Query）] の値よりも古い場合、ISE は新しい値を取得するために、MDM サーバへのデバイス クエリを作成します。準拠ステータスが変更されると、ISE は CoA をトリガーします。

  有効な範囲は 1 ～ 1440 分です。デフォルト値は 1 分です。

### モバイル デバイス管理 - OAuth - クライアント クレデンシャル（Mobile Device Management - OAuth - Client Credentials）

OAuth を使用するには、OAuth サーバの設定が必要です。これについては、次で説明します。MDM サーバとしての Microsoft Intune の設定 （46 ページ）

- 自動検出URL（Auto Discovery URL）：Microsoft Azure 管理ポータルの [Microsoft Azure AD Graph APIエンドポイント（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 Azure AD ディレクトリのデータに直接アクセスできるエンドポイントです。URL の形式は `https://<hostname>/<tenant id>`、たとえば、`https://graph.ppe.windows.net/47f09275-5bc0-4807-8aae-f35cb0341329` です。この URL の拡大バージョンもプロパティ ファイルに含まれます。形式は、`https://<Graph_API_Endpoint>/<TenantId_Or_Domain>/servicePrincipalsByAppId/<Microsoft`

Intune AppId>/serviceEndpoints?api-version=1.6&client-request-id=<Guid.NewGuid()> です。

- 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）：前のステップの [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、アプリケーションが OAuth2.0 を使用してアクセス トークンを取得できるエンドポイントです。アプリケーションが認証されると、Microsoft Azure AD はアプリケーション（ISE）にアクセス トークンを発行します。このトークンを使用するとアプリケーションから Graph API/Intune API を呼び出すことができます。
- 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。パブリックの既知の Microsoft Intune API の APP ID URL。
- ポーリング間隔（Polling Interval）：Cisco ISE が MDM サーバをポーリングしてコンプライアンス チェック情報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。ネットワーク上の少数のアクティブ クライアントをテストする場合のみポーリング間隔を 60 分未満に設定することを推奨します。多くのアクティブ クライアントを持つ実稼働環境でこの値を 60 分未満に設定すると、システムの負荷が大幅に増加し、パフォーマンスに悪影響を与える場合があります。

  ポーリング間隔を0に設定すると、ISEはMDMサーバとの通信をディセーブルにします。
- 準拠デバイス再認証クエリの間隔（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、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が [準拠デバイス再認証クエリの間隔（Time Interval For Compliance Device ReAuth Query）] の値よりも古い場合、ISE は新しい値を取得するために、MDM サーバへのデバイス クエリを作成します。準拠ステータスが変更されると、ISE は CoA をトリガーします。

  有効な範囲は 1 ～ 1440 分です。デフォルト値は 1 分です。

### デスクトップ デバイス管理

次の設定では、ISE と通信できるように SCCM サーバの WMI を設定する必要があります。詳細については、ISE 用の Microsoft SCCM サーバの設定 （50 ページ）を参照してください。

- ホスト名/IPアドレス（Host Name / IP Address）：MDM サーバのホスト名または IP アドレスを入力します。
- サイトまたはインスタンス名（Site or Instance Name）：サイト名または、MDM サーバに複数のインスタンスがある場合はインスタンス名を入力します。

# Microsoft Intune および SCCM のための ISE MDM サポート

- **Microsoft Intune**：MDM-ISE はパートナー MDM サーバ管理モバイル デバイスとして、Microsoft の Intune デバイス管理をサポートします。

  Intune サーバ管理モバイル 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 ISE を設定します。ISE は、Azure からトークンを取得し、ISE Intune アプリケーションとのセッションを確立します。

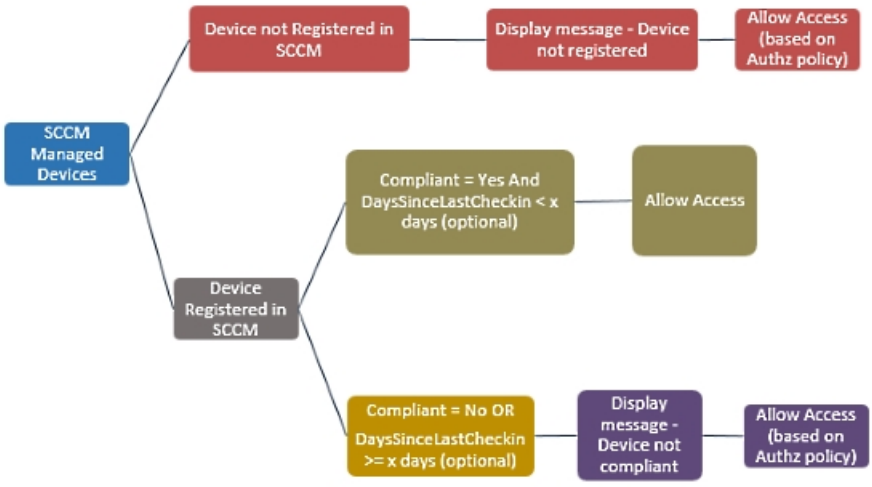
  Intune がクライアント アプリケーションとどのように通信するかについての詳細は、https://msdn.microsoft.com/en-us/library/azure/dn645543.aspx を参照してください。

- **デスクトップ デバイス マネージャ（Microsoft SCCM）**：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 サーバとしてサポートします。ISE は、WMI を使用してコンプライアンス情報を SCCM サーバから取得し、その情報を使用してユーザの Windows デバイスへのネットワーク アクセスを許可または拒否します。

### SCCM のワークフロー

ISE はデバイスが登録されているかについて、また登録済みの場合は準拠しているかどうかについて SCCM サーバから情報を取得できます。次の図に、SCCM により管理されるデバイス用のワークフローを示します。

**図 *4 : SCCM* のワークフロー**




デバイスを接続し、SCCM ポリシーが一致すると、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、許可ポリシーで指定されている SCCM サーバを照会します。この情報を使用して、ISE はエンドポイント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 SCCM に登録されていない、およびリダイレクト プロファイルが許可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 SCCM に登録されていないというメッセージがユーザに表示されます。ユーザがメッセージを受け取った後、ISE は

SCCM 登録サイトへ CoA を発行できます。承認ポリシーおよびプロファイルに基づいてユーザにアクセスを許可できます。

#### Microsoft SCCM サーバ接続の監視

ポーリングは SCCM 用に設定できません。

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

## MDM サーバとしての Microsoft Intune の設定

ISE の MDM サーバとして Microsoft Intune を設定することは、他の MDM サーバの設定とは少し異なります。Azure への ISE の接続および ISE への Azure の接続を設定するには、次の手順を使用します。

1. パブリック証明書を Intune/Azure Active Directory テナントから取得し、ISE にインポートして SSL ハンドシェイクをサポートします。
    1. 1. サイトがテナントを持つ Intune 管理コンソールまたは Azure 管理コンソールにログオンします。
    2. ブラウザを使用して証明書の詳細を取得します。たとえば、Internet Explorer の場合は次のように操作します。
        1. ブラウザのツールバーのロック シンボルをクリックしてから、[証明書の表示（View Certficates）] をクリックします。
        2. [証明書（Certificate）] ウィンドウで、[認証パス（Certification Path）] タブを選択します。
        3. Baltimore Cyber Trust ルートを見つけて、そのルート証明書をエクスポートします。
    3. ISE で、**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）]** の順に選択し、保存したルート証明書をインポートします。証明書に Azure MDM などのわかりやすい名前を付けます。
2. ISE 自己署名証明書をエクスポートし、InTune/Azure 用に準備をします。
    1. PAN で、**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [システム証明書（System Certificates）]** の順に移動し、デフォルトの自己署名サーバ証明書を選択して、[エクスポート（Export）] をクリックします。
    2. [証明書のみエクスポート（Export Certificate Only）]（デフォルト）を選択し、保存する場所を選択します。

    エクスポートされた証明書ファイルに次の PowerShell スクリプトを実行します。

```
$cer = New-Object System.Security.Cryptography.X509Certificates.X509Certificate2
$cer.Import("mycer.cer")
```

```
$bin = $cer.GetRawCertData()
$base64Value = [System.Convert]::ToBase64String($bin)

$bin = $cer.GetCertHash()
$base64Thumbprint = [System.Convert]::ToBase64String($bin)

$keyid = [System.Guid]::NewGuid().ToString()
```

次の手順で使用するため、**$base64Thumbprint**、**$base64Value**、**$keyid** の値をメモしておきます。

3. Intune で ISE アプリケーションを作成します。
   1. Microsoft Azure 管理ポータルで顧客ドメインにサインインし、**[ディレクトリ（Directory）]**>**[アプリケーション（Applications）]**>**[アプリケーションの追加（Add an Application）]** に移動して、[自分の組織が開発中のアプリケーションの追加（Add an application my organization is developing）] を選択します。
   2. 次のパラメータを使用して、Azure で ISE アプリケーションを設定します。
      - アプリケーション名（Application Name）：**ISE** と入力します。
      - [Web アプリケーションまたは Web アプリ（WEB APPLICATION AND/OR WEB APP）] を選択します。
      - サインオン URL およびアプリ ID URL（SIGN-ON URL and APP ID URL）：任意の有効な URL を追加します。この値は ISE では使用されません。
4. Azure からマニフェスト ファイルを取得し、ISE 証明書情報を追加して、更新されたマニフェストを Azure にアップロードします。
   1. Microsoft Azure 管理ポータル（https://manage.windowsazure.com）で、AAD スナップインを開き、ISE アプリケーションに移動します。

   [マニフェストの管理（Manage Manifest）] メニューからアプリケーション マニフェスト ファイルをダウンロードします。
5. *Base64 Encoded String of ISE PAN cert* を、PowerShell スクリプトの $base64Value である、エクスポートされ編集された ISE からの証明書ファイルと置き換えて、次の例のようにマニフェスト json ファイルの [keyCredentials] フィールドを更新します。

```
"keyCredentials": [
                                {
                               "customKeyIdentifier": "$base64Thumbprint_from_above",

                                  "keyId": "$keyid_from_above",
                                  "type": "AsymmetricX509Cert",
                                  "usage": "Verify",
                                  "value": "Base64 Encoded String of ISE PAN cert"
                                }
                            ]
```

（注） マニフェスト ファイルの名前は変更しないようにします。

KeyCredentials の複雑なタイプは、http://msdn.microsoft.com/en-us/library/azure/dn151681.aspx でドキュメント化されています。

6. Azure に更新されたマニフェスト ファイルをアップロードします。
7. Microsoft Azure 管理ポータルで、アプリ エンドポイントのリストに移動します。次のエンドポイント属性の値を使用して ISE を設定します。
   - MICROSOFT AZURE AD GRAPH API ENDPOINT
   - OAUTH 2.0 TOKEN ENDPOINT
8. ISE で、ISE の Intune サーバを設定します。設定と外部 MDM サーバの詳細については、ISE でのモバイル デバイス管理サーバの定義 （42 ページ）を参照してください。Intune にとって重要なフィールドは次のとおりです。
   - 自動検出URL（Auto Discovery URL）：Microsoft Azure 管理ポータルの [Microsoft Azure AD Graph APIエンドポイント（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 Azure AD ディレクトリのデータに直接アクセスできるエンドポイントです。URL の形式は `https://<hostname>/<tenant id>`、たとえば、`https://graph.ppe.windows.net/47f09275-5bc0-4807-8aae-f35cb0341329` です。この URL の拡大バージョンもプロパティ ファイルに含まれます。形式は、`https://<Graph_API_Endpoint>/<TenantId_Or_Domain>/servicePrincipalsByAppId/<Microsoft Intune AppId>/serviceEndpoints?api-version=1.6&client-request-id=<Guid.NewGuid()>` です。
   - 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）：前のステップの [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、アプリケーションが OAuth2.0 を使用してアクセス トークンを取得できるエンドポイントです。アプリケーションが認証されると、Microsoft Azure AD はアプリケーション（ISE）にアクセス トークンを発行します。このトークンを使用するとアプリケーションから Graph API/Intune API を呼び出すことができます。
   - 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。パブリックの既知の Microsoft Intune API の APP ID URL。

Intune アプリケーションの詳細については、次のリンクを参照してください。

- https://msdn.microsoft.com/en-us/library/azure/dn645543.aspx
- http://blogs.msdn.com/b/exchangedev/archive/2015/01/22/building-daemon-or-service-apps-with-office-365-mail-calendar-and-contacts-apis-oauth2-client-credential-flow.aspx
- https://azure.microsoft.com/en-us/documentation/articles/active-directory-authentication-scenarios
- https://azure.microsoft.com/en-us/documentation/articles/active-directory-integrating-applications
- https://azure.microsoft.com/en-us/documentation/articles/active-directory-application-manifest

# Microsoft SCCM のポリシー設定の例

ポリシーでは次の新しいディクショナリ エントリが使用され、SCCM をサポートすることができます。

- MDM.DaysSinceLastCheckin：ユーザが最後に確認してからの日数、または SCCM のデバイスと同期してからの日数で、1 ～ 365 日です。
- MDM.UserNotified：値は Y または N です。ユーザが登録されていないことをユーザに通知したかどうかを示します。さらに、登録ポータルへの制限付きアクセスやリダイレクトを許可し、またはアクセスを拒否できます。
- MDM.ServerType：値はモバイル デバイス マネージャの場合 MDM またはデスクトップ デバイス マネージャの場合 DM です。

次のサンプル ポリシー セットで SCCM をサポートする一連のポリシーを示します。

| ポリシー名 | 条件（IF） | 実行されるアクション（Then） |
|---|---|---|
| SCCM_Comp | Wireless_802.1X AND<br>MDM:MDMServerName EQUALS SccmServer1 AND<br>MDM:DeviceRegisterStatus EQUALS Registered | PermitAccess |
| SCCM_NonComp_Notify | Wireless_802.1X AND<br>MDM:MDMServerName EQUALS SccmServer1 AND<br>MDM:DeviceCompliantStatus EQUALS NonCompliant AND<br>MDM:UserNotified EQUALS 28 | PermitAccess |
| SCCM_NonComp_Days | Wireless_802.1X AND<br>MDM:MDMServerName EQUALS SccmServer1 AND<br>MDM:MDMDeviceCompliantStatus EQUALS Registered AND<br>MDM:DaysSinceLastCheckin EQUALS 28 | SCCMRedirect |

| ポリシー名 | 条件（IF） | 実行されるアクション（Then） |
|---|---|---|
| SCCM_NonComp | Wireless_802.1X AND<br>MDM:MDMServerName EQUALS SccmServer1 AND<br>MDM:DeviceCompliantStatus EQUALS NonCompliant AND<br>MDM:DeviceRegisterStatus EQUALS Registered | SCCMRedirect |
| SCCM_UnReg_Notify | Wireless_802.1X AND<br>MDM:DeviceRegisterStatus EQUALS Registered AND<br>MDM:UserNotified EQUALS Yes | PermitAccess |

## ISE 用の Microsoft SCCM サーバの設定

ISE は、WMI を使用して SCCM サーバと通信します。WMI は、SCCM を実行している Windows サーバで設定する必要があります。

（注） ISE 統合に使用するユーザ 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 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 SCCM サイトです。

### AD ユーザ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 2012 および Windows 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ができません。Active Directory の管理者は、Active Directory ユーザに次のレジストリ 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 Active Directory のバージョンでは、レジストリ変更は必要ありません。

- Windows 2003

- Windows 2003R2
- Windows 2008

完全な制御を許可するには、次に示すように、まず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** キーを右クリックして [オーナー（Owner）] タブに移動します。

**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。

## AD ユーザがドメイン管理グループの一部ではない場合に必要な権限

Windows 2012 R2 の場合は、Active Directory ユーザに次のレジストリ 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}`

Active Directory ユーザがドメイン管理グループの一部ではなく、ドメイン ユーザ グループの一部である場合は、次の権限も必要です。

- ISE がドメイン コントローラに接続できるようにするレジストリ キーを追加します（下記を参照）
- 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

これらの権限は、次の Active Directory のバージョンでのみ必要となります。

- Windows 2003
- Windows 2003R2
- Windows 2008
- Windows 2008 R2
- Windows 2012
- Windows 2012 R2
- Windows 2016

### ISE がドメイン コントローラに接続できるようにするレジストリ キーを追加する

ISE がドメインユーザとして接続し、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 コントローラに一部のレジストリ 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では必要ありません。

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"="  "
```

キー **DllSurrogate** 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。

上記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む、空の行を保持してください。

## ドメイン コントローラで DCOM を使用するための権限

ISE パッシブ ID サービスに使用される Active Directory ユーザは、ドメイン コントローラで DCOM（リモート COM）を使用する権限がなければなりません。**dcomcnfg** コマンド ライン ツールを使用して権限を設定できます。

**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）] を選択して、[プロパティ（properties）] をクリックし、[COMセキュリティ（COM Security）] をクリックします。

**ステップ 5** アクセスおよび起動の両方に対して ISE が使用するアカウントに許可権限があることを確認します。Active Directory ユーザは、4 つのオプション（[アクセス権限（Access Permissions）] および [起動およびアクティベーションの権限（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）]）のすべてに追加される必要があります。

**ステップ 6** [アクセス権限（Access Permissions）] および [起動およびアクティベーションの権限（Launch and Activation Permissions）] の両方に対してローカルおよびリモート アクセスをすべて許可します。

図 *5 : [*アクセス権限（***Access Permissions***）*]*のローカルおよびリモート アクセス

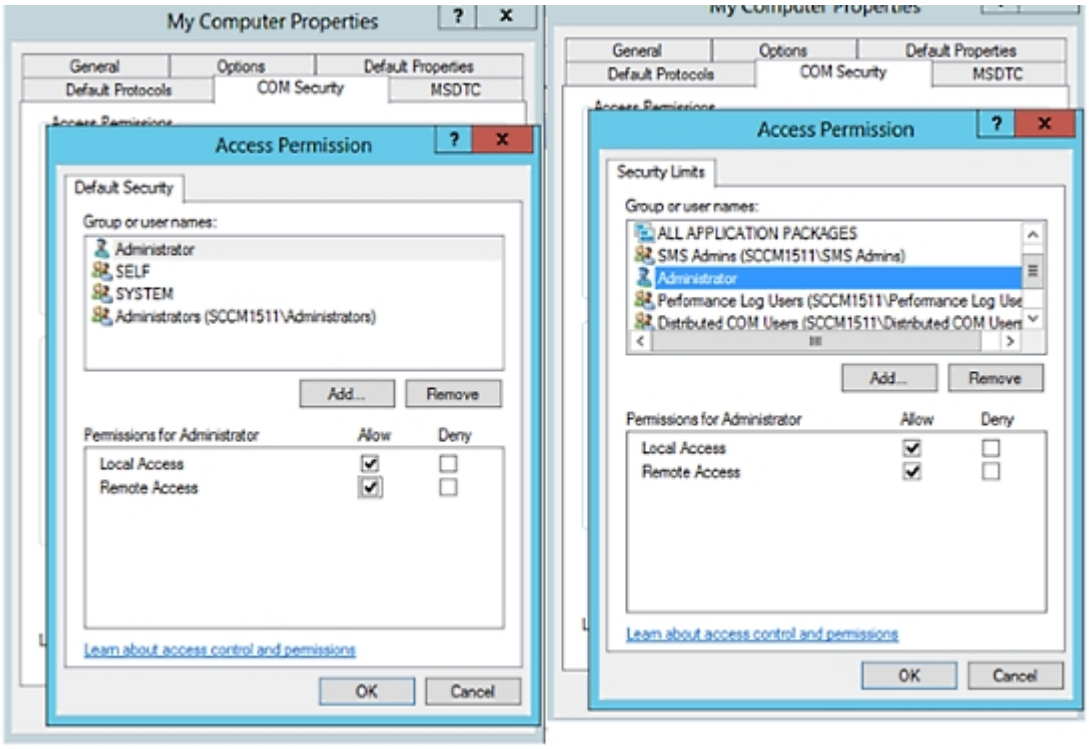
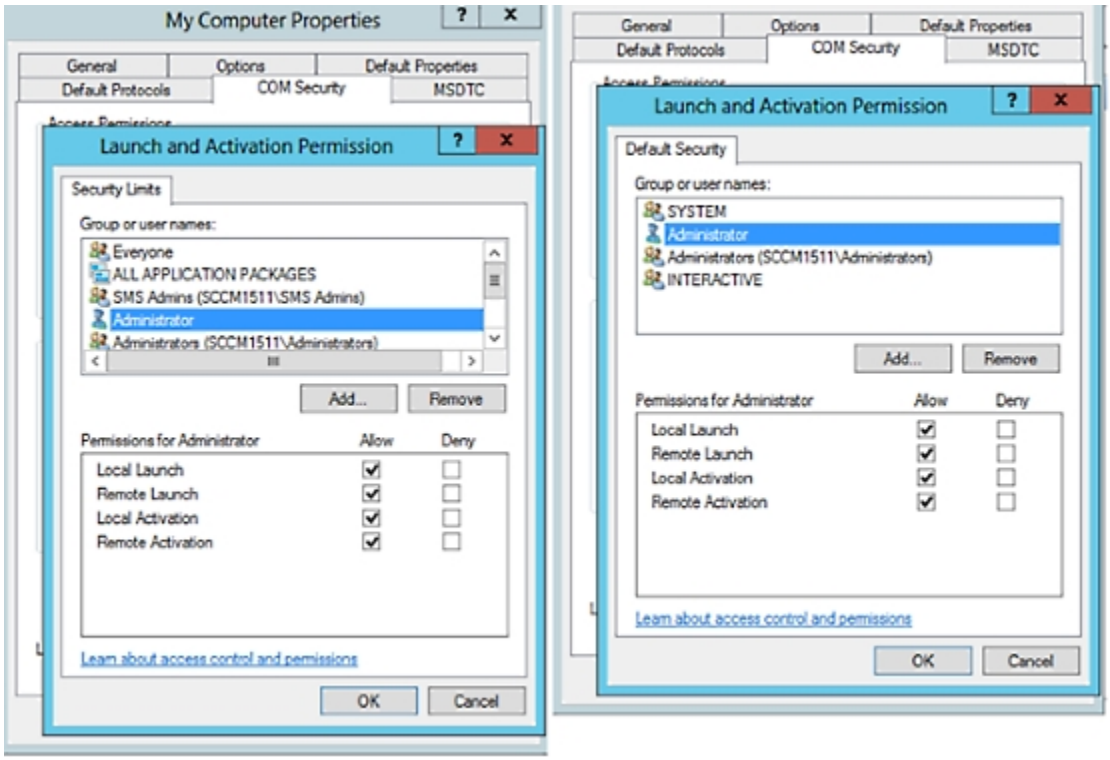


図 *6 :* [起動およびアクティベーションの権限（***Launch and Activation Permissions***）] のローカルおよびリモート アクセス




## 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、Active Directory ユーザには実行メソッドおよびリモートイネーブル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] > [Run] をクリックし、`wmimgmt.msc` と入力します。

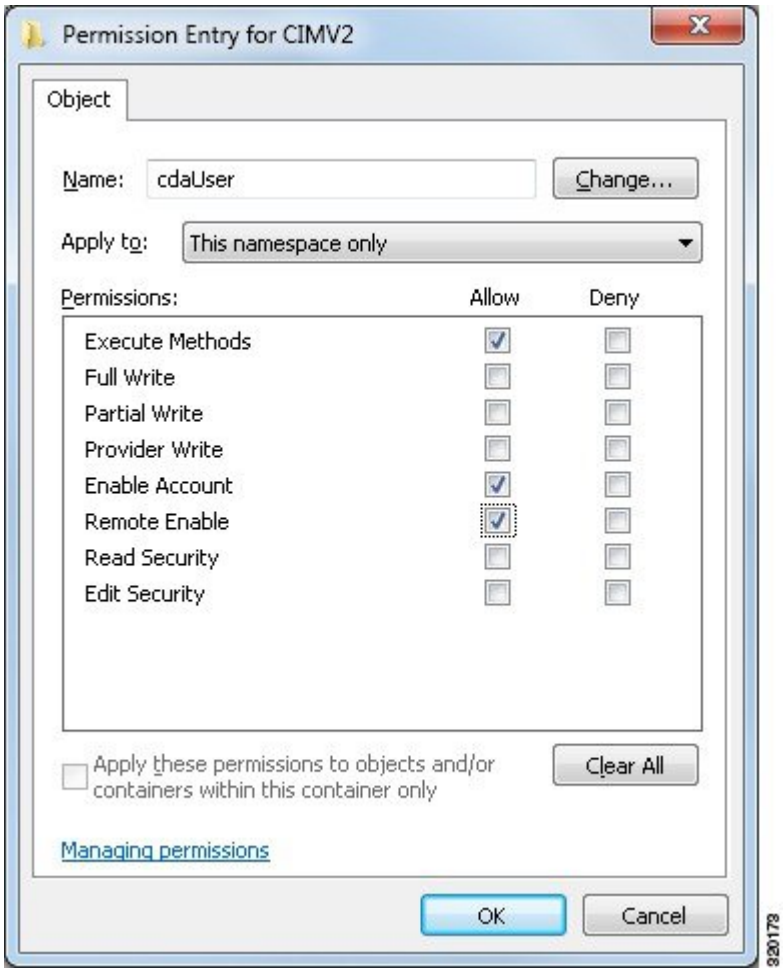
**ステップ 2** [WMI Control] を右クリックし、[プロパティ] をクリックします。

**ステップ 3** [セキュリティ] タブで [ルート] 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** 下に示すように、Active Directory ユーザを追加し、必要な権限を設定します。

図 *7 : WMI Root\CIMv2* 名前空間に必要な権限




## WMI アクセス用にファイアウォール ポートを開く

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（ISE 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 発信をすると、このポートでリスニングしているサービスが、クライアントに、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：SMB

（注） Cisco ISE 1.3 以降は SMB 2.0 をサポートします。

数値の大きいポートは動的に割り当てられ、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（ISE IP）に割り当てることができます。

## 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 サーバ定義を作成したことを確認します。正常に MDM サーバと ISE を統合した後に限り、MDM ディクショナリにデータが入力され、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、ワイヤレス LAN コントローラの 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 サーバ名または IP アドレスを追加する必要があります。**[管理（Administration）]** > **[設定（Settings）]** > **[プロキシ設定（Proxy Settings）]**の順に選択して、このアクションを実行します。

**ステップ 1** **[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[許可（Authorization）]** > **[許可プロファイル（Authorization Profiles）]** > **[追加（Add）]** を選択します。

**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 サーバ名と一致する許可プロファイルの名前を入力します。

**ステップ 4** アクセス タイプとして ACCESS_ACCEPT を選択します。

**ステップ 5** [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] フィールドに入力します。

**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** ドロップダウン リストから、使用する MDM サーバを選択します。

**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

MDM 設定を完了するには、Cisco ISE で許可ポリシー ルールを設定する必要があります。

### 始める前に

- Cisco ISE 証明書ストアに MDM サーバ証明書を追加します。
- Cisco ISE で MDM サーバ定義を作成したことを確認します。正常に MDM サーバと ISE を統合した後に限り、MDM ディクショナリにデータが入力され、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。
- 未登録のデバイスまたは非準拠のデバイスをリダイレクトするために、ワイヤレス LAN コントローラの ACL を設定します。

**ステップ 1** **[ポリシー（Policy）]** > **[ポリシー セット（Policy Sets）]** を選択し、許可ポリシー 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、ISE MDM ページが表示され、MDM でのデバイスの登録に関する情報が示されます。
- [PERMIT]：デバイスが Cisco ISE および MDM に登録されており、Cisco ISE および MDM 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。

次の図は、この設定の例を示します。

**図 *8 : MDM* の使用例の許可ポリシー ルール**


**ステップ 3** [保存（Save）] をクリックします。

## デバイスのワイプまたはロック

Cisco ISE では、失われたデバイスをワイプしたり、PIN ロックをオンにしたりできます。これは [エンドポイント（Endpoints）] ページから行うことができます。

**ステップ 1** **[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）]** を選択します。

**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）] : MDM サーバ ポリシーで設定したアプリケーションを削除します
- [PIN ロック（PIN Lock）] : デバイスをロックします

**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。

## Mobile Device Manager のレポートの表示

Cisco ISE では、MDM サーバ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報告する「変更設定監査」レポートで表示できます。

**[操作（Operations）] > [レポート（Reports）] > [変更設定監査（Change Configuration Audit）] > [MDM]** を選択し、結果のレポートで表示する期間を指定します。

## Mobile Device Manager のログの表示

[メッセージ カタログ（Message Catalog）] ページを使用して、Mobile Device Manager のログ メッセージを表示できます。**[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [メッセージカタログ（Message Catalog）]** を選択します。MDM ログ エントリのデフォルトのレポーティング レベルは「INFO」です。レポーティング レベルを「DEBUG」または「TRACE」に変更できます。

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

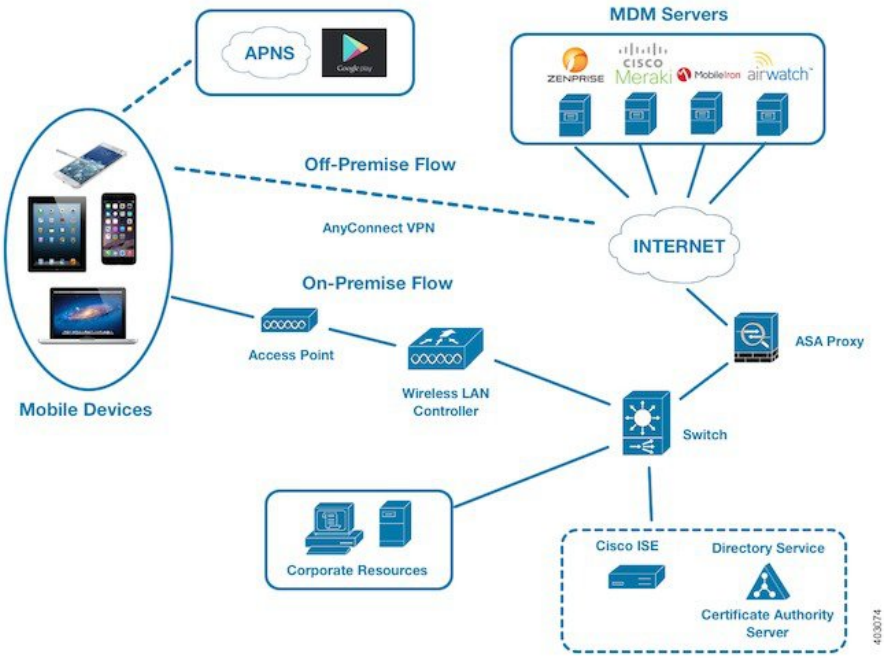
モバイルデバイス管理（MDM）サーバはモバイル事業者、サービス プロバイダー、企業にわたって展開されたモバイルデバイスの保護、モニタ、管理、およびサポートを行います。MDM サーバはポリシー サーバとして機能し、ポリシー サーバは展開環境のモバイル デバイスにある一部のアプリケーション（電子メール アプリケーションなど）の使用を制御します。ただし、ネットワークは、ACL に基づいてエンドポイントへのきめ細かいアクセス権を提供できる唯一のエンティティです。Cisco ISE は必要なデバイス属性について MDM サーバにクエリを行い、それらのデバイスに対してネットワーク アクセス コントロールを提供する ACL を作成します。

さまざまなベンダーからのサーバなど、複数のアクティブなMDMサーバ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、シスコの MDM API バージョン 2 を使用して MDM サーバと統合し、デバイスが AnyConnect 4.1 および Cisco ASA 9.3.2 以降を介して VPN 経由でネットワークにアクセスできるようにします。

この図では、Cisco ISE が適用ポイントで、MDM ポリシー サーバがポリシー情報ポイントです。Cisco ISE は、MDM サーバ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 *9 : MDM* の *Cisco ISE* との相互運用性**




1 つ以上の外部 Mobile Device Manager（MDM）サーバと相互運用するように Cisco ISE を設定できます。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活用できます。Cisco ISE は REST API コールを使用して、外部 MDM サーバ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、Cisco ISE ネットワークへのリモート デバイス アクセスをより適切に制御します。

サポートされるMDMベンダーは次のとおりです。サポートされるMDMサーバ（38ページ）

# サポートされる MDM の使用例

Cisco ISE が外部 MDM サーバを使用して実行する機能は、次のとおりです。

- 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だけが付与されます。
- エンドポイント データの増加：Cisco ISE プロファイラを使用して収集できない、MDM サーバの情報でエンドポイントデータベースを更新します。エンドポイントがMDMのモニタ対象デバイスの場合、Cisco ISE は **[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）]** ページを使用して表示できる 6 つのデバイス属性を使用します。次に例を示します。
  - MDMImei: 99 000100 160803 3
  - MDMManufacturer: Apple
  - MDMModel: iPhone
  - MDMOSVersion: iOS 6.0.0
  - MDMPhoneNumber: 9783148806
  - MDMSerialNumber: DNPGQZGUDTF9
- Cisco ISE は、4 時間ごとに MDM サーバをポーリングし、デバイス コンプライアンス データを確認します。これは管理者が設定できます。
- MDM サーバを介したデバイス手順の発行：MDM サーバを介してユーザのデバイスに対するリモート アクションを発行します。管理者は、ISE コンソールからリモート操作を開始します。

### ベンダー MDM 属性

ISE で MDM サーバを設定すると、このベンダーの属性は ISE システム ディクショナリに **mdm** という名前で新しいエントリに追加されます。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。

- DeviceRegisterStatus
- DeviceCompliantStatus
- DiskEncryptionStatus
- PinLockStatus
- JailBrokenStatus
- Manufacturer
- IMEI
- SerialNumber
- OsVersion
- PhoneNumber
- MDMServerName
- MDMServerReachable

- MEID
- モデル
- UDID

ベンダー固有の属性はサポートされませんが、ベンダーがその属性をサポートする場合は、ERS API を使用してベンダー固有の属性を変換できる場合があります。

新しい MDM ディクショナリ属性は許可ポリシーで使用可能です。

# サポートされる MDM サーバ

サポートされる MDM サーバは、次のベンダーの製品です。

- 絶対値（Absolute）
- AirWatch
- Citrix XenMobile
- Globo
- Good Technology
- IBM MaaS360
- JAMF ソフトウェア
- Meraki SM/EMM
- MobileIron
- SAP Afaria
- SOTI
- Symantec
- Tangoe
- Microsoft Intune - モバイル デバイス用
- Microsoft SCCM -デスクトップ デバイス用

**ISE コミュニティ リソース**

How To: Meraki EMM / MDM Integration with ISE

# MDM サーバにより使用されるポート

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

表 *7: MDM* サーバにより使用されるポート

| MDM サーバ | ポート |
|---|---|
| MobileIron | 443 |
| Zenprise | 443 |
| Good | 19005 |
| Airwatch | 443 |
| Afaria | 443 |
| Fiberlink MaaS | 443 |
| Meraki | 443 |
| Microsoft Intune | 80 および 443 |
| Microsoft SCCM | 80 および 443 |

# MDM 統合プロセス フロー

ここでは、MDM 統合プロセスについて説明します。

1. ユーザはデバイスを SSID に関連付けます。
2. Cisco ISE は、MDM サーバに対して API コールを実行します。
3. この API コールは、このユーザ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。構外の Apple iOS デバイスの場合は UDID です。

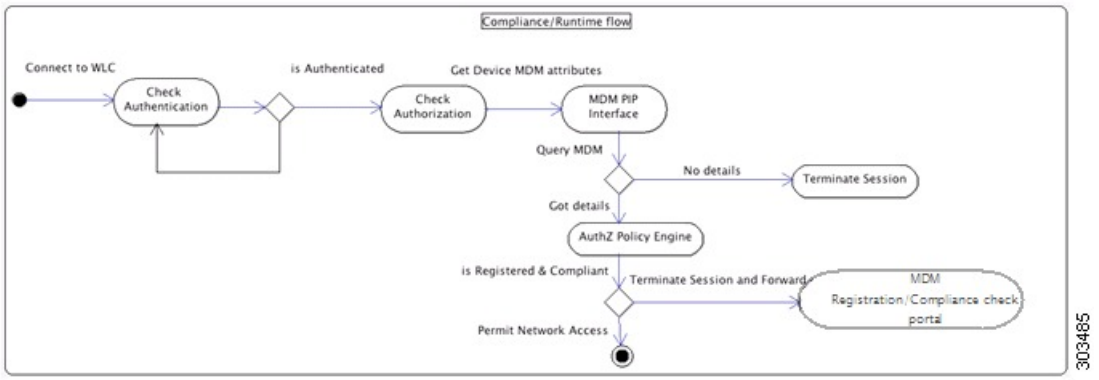
4. ユーザのデバイスがこのリストにない場合、デバイスが登録されていないことを意味します。Cisco ISE は、Cisco ISE にリダイレクトされる許可要求を NAD に送信します。ユーザが MDM サーバ ページに表示されます。

（注） MDM ポータルを介して Cisco ISE ネットワークの外の MDM サーバに登録済みのデバイスを登録する必要があります。これは Cisco ISE、リリース 1.4 以降に適用されます。ISE の以前のバージョンでは、Cisco ISE ネットワークの外に登録済みのデバイスはポスチャ ポリシーに準拠している場合に自動的に登録されます。

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ページをユーザに表示します。

6. ユーザは MDM サーバにデバイスを登録し、MDM サーバは Cisco ISE に要求をリダイレクトします（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）。
7. Cisco ISE は MDM サーバ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. ユーザのデバイスが MDM サーバ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おらず、準拠する必要があることがユーザに通知されます。
9. ユーザのデバイスがポリシーに準拠するようになった後、MDM のサーバ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 サーバを 4 時間ごとにポーリングし、必要に応じて許可変更（CoA）を発行します。これは管理者が設定できます。また、Cisco ISE は 5 分ごとに MDM サーバをチェックして使用できるかどうかを確認します。

次の図は、MDM プロセス フローを示しています。




（注） 一度に 1 つの MDM サーバ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、[設定（Settings）] > [全般（General）] > [デバイス管理（Device management）] の順に移動し、削除の管理をクリックすることができます。または、ISE の MyDevices ポータルに移動し、企業ワイプをクリックすることができます。

# Cisco ISE による MDM サーバの設定

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

**ステップ 1** Azure に 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** ワイヤレス LAN コントローラの ACL を設定します。

**ステップ 4** MDM サーバに未登録のデバイスをリダイレクトするための許可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 サーバがある場合は、各ベンダーに個別の許可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 MDM サーバ証明書のインポート

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

（注） Microsoft Azure の場合は、ISE 証明書を Azure にインポートします。詳細については、MDM サーバとしての Microsoft Intune の設定 （46 ページ）を参照してください。

**ステップ 1** MDM サーバ証明書を MDM サーバ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** **[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificate）] > [インポート（Import）]** を選択します。

**ステップ 3** [参照（Browse）] をクリックして、MDM サーバから取得した MDM サーバ証明書を選択します。

**ステップ 4** わかりやすい名前を追加します。

**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）] リスト ページに MDM サーバ証明書が一覧表示されることを確認します。

### 次のタスク

ISE でのモバイル デバイス管理サーバの定義 （42 ページ）

。

# ISE でのモバイル デバイス管理サーバの定義

外部 MDM サーバ用のモバイル デバイス管理（MDM）定義とデスクトップ デバイス マネージャ（SCCM）定義を 1 つ以上作成できます。

1. **[管理（Administration）] > [ネットワーク リソース（Network Resources）] > [外部 MDM（External MDM）]** の順に選択します。
2. [追加（Add）] をクリックします。
3. 追加する MDM サーバの名前と説明を入力します。
4. [サーバ タイプ（Server Type）] で、[モバイル デバイス マネージャ（Mobile Device Manager）] または [デスクトップ デバイス マネージャ（Desktop Device Manager）] を選択します。どちらを選択するかで、どのフィールドが次に表示されるかが決定します。[デスクトップ デバイス マネージャ（Desktop Device Manager）] を選択した場合は、「デスクトップ デバイス管理 （67 ページ）」に進みます。[モバイル デバイス マネージャ（Mobile Device Manager）] を選択した場合は、次の手順を続行します。
5. [認証タイプ（Authentication Type）] で、[ベーシック（Basic）] または [OAuth - クライアント クレデンシャル（OAuth - Client Credentials）] を選択します。Microsoft Intune サーバを設定する [OAuth - クライアント クレデンシャル（OAuth - Client Credentials）] を選択した場合は、「モバイル デバイス管理 - OAuth - クライアント クレデンシャル（Mobile Device Management - OAuth - Client Credentials） （66 ページ）」に進みます。[ベーシック（Basic）] を選択した場合は、次の手順を続行します。
6. すべての画面で、MDM サーバ定義の名前と説明が求められます。ここでは、サーバと認証タイプに基づいて、その他のフィールドと手順について説明しています。

### モバイル デバイス管理：ベーシック

- ホスト名/IPアドレス（Host Name / IP Address）：MDM サーバのホスト名または IP アドレスを入力します。
- ポート（Port）：MDM サーバとの接続に使用するポートを入力します。通常は 443。
- インスタンス名（Instance Name）：この MDM サーバ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。
- ポーリング間隔（Polling Interval）：Cisco ISE が MDM サーバをポーリングしてコンプライアンス チェック情報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。ネットワーク上の少数のアクティブ クライアントをテストする場合のみポーリング間隔を 60 分未満に設定することを推奨します。多くのアクティブ クライアントを持つ実稼働環境でこの値を 60 分未満に設定すると、システムの負荷が大幅に増加し、パフォーマンスに悪影響を与える場合があります。

  ポーリング間隔を 0 に設定すると、ISE は MDM サーバとの通信をディセーブルにします。

- 準拠デバイス再認証クエリの間隔（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、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が [準拠デバイス再認証クエリの間隔（Time Interval For Compliance Device ReAuth Query）] の値よりも古い場合、ISE は新しい値を取得するために、MDM サーバへのデバイス クエリを作成します。準拠ステータスが変更されると、ISE は CoA をトリガーします。

  有効な範囲は 1 ～ 1440 分です。デフォルト値は 1 分です。

### モバイル デバイス管理 - OAuth - クライアント クレデンシャル（Mobile Device Management - OAuth - Client Credentials）

OAuth を使用するには、OAuth サーバの設定が必要です。これについては、次で説明します。MDM サーバとしての Microsoft Intune の設定 （46 ページ）

- 自動検出URL（Auto Discovery URL）：Microsoft Azure 管理ポータルの [Microsoft Azure AD Graph APIエンドポイント（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 Azure AD ディレクトリのデータに直接アクセスできるエンドポイントです。URL の形式は `https://<hostname>/<tenant id>`、たとえば、`https://graph.ppe.windows.net/47f09275-5bc0-4807-8aae-f35cb0341329` です。この URL の拡大バージョンもプロパティ ファイルに含まれます。形式は、`https://<Graph_API_Endpoint>/<TenantId_Or_Domain>/servicePrincipalsByAppId/<Microsoft Intune AppId>/serviceEndpoints?api-version=1.6&client-request-id=<Guid.NewGuid()>` です。

- 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）：前のステップの [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、アプリケーションが OAuth2.0 を使用してアクセス トークンを取得できるエンドポイントです。アプリケーションが認証されると、Microsoft Azure AD はアプリケーション（ISE）にアクセス トークンを発行します。このトークンを使用するとアプリケーションから Graph API/Intune API を呼び出すことができます。

- 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。パブリックの既知の Microsoft Intune API の APP ID URL。

- ポーリング間隔（Polling Interval）：Cisco ISE が MDM サーバをポーリングしてコンプライアンス チェック情報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。ネットワーク上の少数のアクティブクライアントをテストする場合のみポーリング間隔を 60 分未満に設定することを推奨します。多くのアクティブ クライアントを持つ実稼働環境でこの値を 60 分未満に設定すると、システムの負荷が大幅に増加し、パフォーマンスに悪影響を与える場合があります。

  ポーリング間隔を0に設定すると、ISEはMDMサーバとの通信をディセーブルにします。

- 準拠デバイス再認証クエリの間隔（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、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が [準拠デバイス再認証クエリの間隔（Time Interval For Compliance Device ReAuth Query）] の値よりも古い場合、ISE は新しい値を取得するために、MDM サーバへのデバイス クエリを作成します。準拠ステータスが変更されると、ISE は CoA をトリガーします。

  有効な範囲は 1 ～ 1440 分です。デフォルト値は 1 分です。

### デスクトップ デバイス管理

次の設定では、ISE と通信できるように SCCM サーバの WMI を設定する必要があります。詳細については、ISE 用の Microsoft SCCM サーバの設定 （50 ページ）を参照してください。

- ホスト名/IPアドレス（Host Name / IP Address）：MDM サーバのホスト名または IP アドレスを入力します。
- サイトまたはインスタンス名（Site or Instance Name）：サイト名または、MDM サーバに複数のインスタンスがある場合はインスタンス名を入力します。

# Microsoft Intune および SCCM のための ISE MDM サポート

- **Microsoft Intune**：MDM-ISE はパートナー MDM サーバ管理モバイル デバイスとして、Microsoft の Intune デバイス管理をサポートします。

  Intune サーバ管理モバイル 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 ISE を設定します。ISE は、Azure からトークンを取得し、ISE Intune アプリケーションとのセッションを確立します。

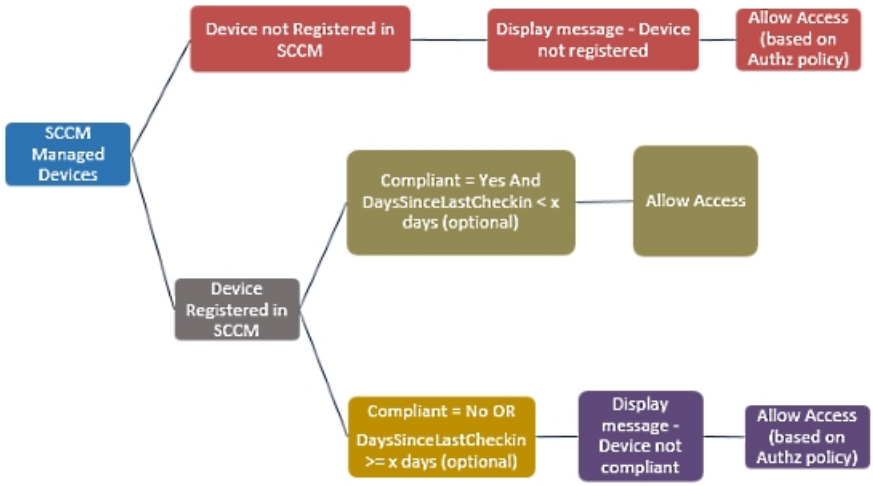
  Intune がクライアント アプリケーションとどのように通信するかについての詳細は、https://msdn.microsoft.com/en-us/library/azure/dn645543.aspx を参照してください。

- **デスクトップ デバイス マネージャ（Microsoft SCCM）**：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 サーバとしてサポートします。ISE は、WMI を使用してコンプライアンス情報を SCCM サーバから取得し、その情報を使用してユーザの Windows デバイスへのネットワーク アクセスを許可または拒否します。

### SCCM のワークフロー

ISE はデバイスが登録されているかについて、また登録済みの場合は準拠しているかどうかについて SCCM サーバから情報を取得できます。次の図に、SCCM により管理されるデバイス用のワークフローを示します。

図 *10 : SCCM* のワークフロー




デバイスを接続し、SCCM ポリシーが一致すると、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、許可ポリシーで指定されている SCCM サーバを照会します。この情報を使用して、ISE はエンドポイント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 SCCM に登録されていない、およびリダイレクト プロファイルが許可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 SCCM に登録されていないというメッセージがユーザに表示されます。ユーザがメッセージを受け取った後、ISE は SCCM 登録サイトへ CoA を発行できます。承認ポリシーおよびプロファイルに基づいてユーザにアクセスを許可できます。

### Microsoft SCCM サーバ接続の監視

ポーリングは SCCM 用に設定できません。

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

# MDM サーバとしての Microsoft Intune の設定

ISE の MDM サーバとして Microsoft Intune を設定することは、他の MDM サーバの設定とは少し異なります。Azure への ISE の接続および ISE への Azure の接続を設定するには、次の手順を使用します。

1. パブリック証明書を Intune/Azure Active Directory テナントから取得し、ISE にインポートして SSL ハンドシェイクをサポートします。
    1. 1. サイトがテナントを持つ Intune 管理コンソールまたは Azure 管理コンソールにログオンします。

2. ブラウザを使用して証明書の詳細を取得します。たとえば、Internet Explorer の場合は次のように操作します。
   1. ブラウザのツールバーのロックシンボルをクリックしてから、[証明書の表示（View Certficates）] をクリックします。
   2. [証明書（Certificate）] ウィンドウで、[認証パス（Certification Path）] タブを選択します。
   3. Baltimore Cyber Trust ルートを見つけて、そのルート証明書をエクスポートします。
3. ISE で、**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）]** の順に選択し、保存したルート証明書をインポートします。証明書に Azure MDM などのわかりやすい名前を付けます。

2. ISE 自己署名証明書をエクスポートし、InTune/Azure 用に準備をします。
   1. PAN で、**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [システム証明書（System Certificates）]** の順に移動し、デフォルトの自己署名サーバ証明書を選択して、[エクスポート（Export）] をクリックします。
   2. [証明書のみエクスポート（Export Certificate Only）]（デフォルト）を選択し、保存する場所を選択します。

   エクスポートされた証明書ファイルに次の PowerShell スクリプトを実行します。

```
$cer = New-Object System.Security.Cryptography.X509Certificates.X509Certificate2
$cer.Import("mycer.cer")
$bin = $cer.GetRawCertData()
$base64Value = [System.Convert]::ToBase64String($bin)

$bin = $cer.GetCertHash()
$base64Thumbprint = [System.Convert]::ToBase64String($bin)

$keyid = [System.Guid]::NewGuid().ToString()
```

   次の手順で使用するため、**$base64Thumbprint、$base64Value、$keyid** の値をメモしておきます。

3. Intune で ISE アプリケーションを作成します。
   1. Microsoft Azure 管理ポータルで顧客ドメインにサインインし、**[ディレクトリ（Directory）] > [アプリケーション（Applications）] > [アプリケーションの追加（Add an Application）]** に移動して、[自分の組織が開発中のアプリケーションの追加（Add an application my organization is developing）] を選択します。
   2. 次のパラメータを使用して、Azure で ISE アプリケーションを設定します。
      - アプリケーション名（Application Name）：**ISE** と入力します。
      - [Web アプリケーションまたは Web アプリ（WEB APPLICATION AND/OR WEB APP）] を選択します。

- サインオン URL およびアプリ ID URL（SIGN-ON URL and APP ID URL）：任意の有効な URL を追加します。この値は ISE では使用されません。

4. Azure からマニフェスト ファイルを取得し、ISE 証明書情報を追加して、更新されたマニフェストを Azure にアップロードします。

   1. Microsoft Azure 管理ポータル（https://manage.windowsazure.com）で、AAD スナップインを開き、ISE アプリケーションに移動します。

   [マニフェストの管理（Manage Manifest）] メニューからアプリケーション マニフェスト ファイルをダウンロードします。

5. *Base64 Encoded String of ISE PAN cert* を、PowerShell スクリプトの $base64Value である、エクスポートされ編集された ISE からの証明書ファイルと置き換えて、次の例のようにマニフェスト json ファイルの [keyCredentials] フィールドを更新します。

```
"keyCredentials": [
                                {
                               "customKeyIdentifier": "$base64Thumbprint_from_above",

                                  "keyId": "$keyid_from_above",
                                  "type": "AsymmetricX509Cert",
                                  "usage": "Verify",
                                  "value": "Base64 Encoded String of ISE PAN cert"
                                }
                            ]
```

（注） マニフェスト ファイルの名前は変更しないようにします。

KeyCredentials の複雑なタイプは、http://msdn.microsoft.com/en-us/library/azure/dn151681.aspx でドキュメント化されています。

6. Azure に更新されたマニフェスト ファイルをアップロードします。

7. Microsoft Azure 管理ポータルで、アプリ エンドポイントのリストに移動します。次のエンドポイント属性の値を使用して ISE を設定します。

   - MICROSOFT AZURE AD GRAPH API ENDPOINT
   - OAUTH 2.0 TOKEN ENDPOINT

8. ISE で、ISE の Intune サーバを設定します。設定と外部 MDM サーバの詳細については、ISE でのモバイル デバイス管理サーバの定義 （42 ページ）を参照してください。Intune にとって重要なフィールドは次のとおりです。

   - 自動検出URL（Auto Discovery URL）：Microsoft Azure 管理ポータルの [Microsoft Azure AD Graph APIエンドポイント（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 Azure AD ディレクトリのデータに直接アクセスできるエンドポイントです。URL の形式は `https://<hostname>/<tenant id>`、たとえば、`https://graph.ppe.windows.net/47f09275-5bc0-4807-8aae-f35cb0341329` です。この

URL の拡大バージョンもプロパティ ファイルに含まれます。形式は、`https://<Graph_API_Endpoint>/<TenantId_Or_Domain>/servicePrincipalsByAppId/<Microsoft Intune AppId>/serviceEndpoints?api-version=1.6&client-request-id=<Guid.NewGuid()>` です。

- 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）：前のステップの [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、アプリケーションが OAuth2.0 を使用してアクセス トークンを取得できるエンドポイントです。アプリケーションが認証されると、Microsoft Azure AD はアプリケーション（ISE）にアクセス トークンを発行します。このトークンを使用するとアプリケーションから Graph API/Intune API を呼び出すことができます。
- 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。パブリックの既知の Microsoft Intune API の APP ID URL。

Intune アプリケーションの詳細については、次のリンクを参照してください。

- https://msdn.microsoft.com/en-us/library/azure/dn645543.aspx
- http://blogs.msdn.com/b/exchangedev/archive/2015/01/22/building-a-daemon-or-service-app-with-office-365-mail-calendar-and-contacts-apis-oauth2-client-credentials-flow.aspx
- https://azure.microsoft.com/en-us/documentation/articles/active-directory-authentication-scenarios
- https://azure.microsoft.com/en-us/documentation/articles/active-directory-integrating-applications
- https://azure.microsoft.com/en-us/documentation/articles/active-directory-application-manifest

# Microsoft SCCM のポリシー設定の例

ポリシーでは次の新しいディクショナリ エントリが使用され、SCCM をサポートすることができます。

- MDM.DaysSinceLastCheckin：ユーザが最後に確認してからの日数、または SCCM のデバイスと同期してからの日数で、1 ～ 365 日です。
- MDM.UserNotified：値は Y または N です。ユーザが登録されていないことをユーザに通知したかどうかを示します。さらに、登録ポータルへの制限付きアクセスやリダイレクトを許可し、またはアクセスを拒否できます。
- MDM.ServerType：値はモバイル デバイス マネージャの場合 MDM またはデスクトップ デバイス マネージャの場合 DM です。

次のサンプル ポリシー セットで SCCM をサポートする一連のポリシーを示します。

| ポリシー名 | 条件（IF） | 実行されるアクション（Then） |
|---|---|---|
| SCCM_Comp | Wireless_802.1X AND<br>MDM:MDMServerName EQUALS SccmServer1 AND<br>MDM:DeviceRegisterStatus EQUALS Registered | PermitAccess |
| SCCM_NonComp_Notify | Wireless_802.1X AND<br>MDM:MDMServerName EQUALS SccmServer1 AND<br>MDM:DeviceCompliantStatus EQUALS NonCompliant AND<br>MDM:UserNotified EQUALS 28 | PermitAccess |
| SCCM_NonComp_Days | Wireless_802.1X AND<br>MDM:MDMServerName EQUALS SccmServer1 AND<br>MDM:MDMDeviceCompliantStatus EQUALS Registered AND<br>MDM:DaysSinceLastCheckin EQUALS 28 | SCCMRedirect |
| SCCM_NonComp | Wireless_802.1X AND<br>MDM:MDMServerName EQUALS SccmServer1 AND<br>MDM:DeviceCompliantStatus EQUALS NonCompliant AND<br>MDM:DeviceRegisterStatus EQUALS Registered | SCCMRedirect |
| SCCM_UnReg_Notify | Wireless_802.1X AND<br>MDM:DeviceRegisterStatus EQUALS Registered AND<br>MDM:UserNotified EQUALS Yes | PermitAccess |

# ISE 用の Microsoft SCCM サーバの設定

ISE は、WMI を使用して SCCM サーバと通信します。WMI は、SCCM を実行している Windows サーバで設定する必要があります。

（注） ISE 統合に使用するユーザ 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 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 SCCM サイトです。

## AD ユーザ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 2012 および Windows 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ができません。Active Directory の管理者は、Active Directory ユーザに次のレジストリ 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 Active Directory のバージョンでは、レジストリ変更は必要ありません。

- Windows 2003
- Windows 2003R2
- Windows 2008

完全な制御を許可するには、次に示すように、まず 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** キーを右クリックして [オーナー（Owner）] タブに移動します。
**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。

## AD ユーザがドメイン管理グループの一部ではない場合に必要な権限

Windows 2012 R2 の場合は、Active Directory ユーザに次のレジストリ 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}`

Active Directory ユーザがドメイン管理グループの一部ではなく、ドメイン ユーザ グループの一部である場合は、次の権限も必要です。

- ISE がドメイン コントローラに接続できるようにするレジストリ キーを追加します（下記を参照）
- 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

これらの権限は、次の Active Directory のバージョンでのみ必要となります。

- Windows 2003
- Windows 2003R2
- Windows 2008
- Windows 2008 R2
- Windows 2012
- Windows 2012 R2
- Windows 2016

### ISE がドメイン コントローラに接続できるようにするレジストリ キーを追加する

ISE がドメイン ユーザとして接続し、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 コントローラに一部のレジストリ 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では必要ありません。

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"="  "
```

キー **DllSurrogate** 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。

上記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む、空の行を保持してください。

# ドメイン コントローラで DCOM を使用するための権限

ISE パッシブ ID サービスに使用される Active Directory ユーザは、ドメイン コントローラで DCOM（リモート COM）を使用する権限がなければなりません。**dcomcnfg** コマンド ライン ツールを使用して権限を設定できます。

**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）] を選択して、[プロパティ（properties）] をクリックし、[COMセキュリティ（COM Security）] をクリックします。

**ステップ 5** アクセスおよび起動の両方に対して ISE が使用するアカウントに許可権限があることを確認します。Active Directory ユーザは、4 つのオプション（[アクセス権限（Access Permissions）] および [起動およびアクティベーションの権限（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）]）のすべてに追加される必要があります。

**ステップ 6** [アクセス権限（Access Permissions）] および [起動およびアクティベーションの権限（Launch and Activation Permissions）] の両方に対してローカルおよびリモート アクセスをすべて許可します。

**図 *11 : [アクセス権限（Access Permissions）] のローカルおよびリモート アクセス***

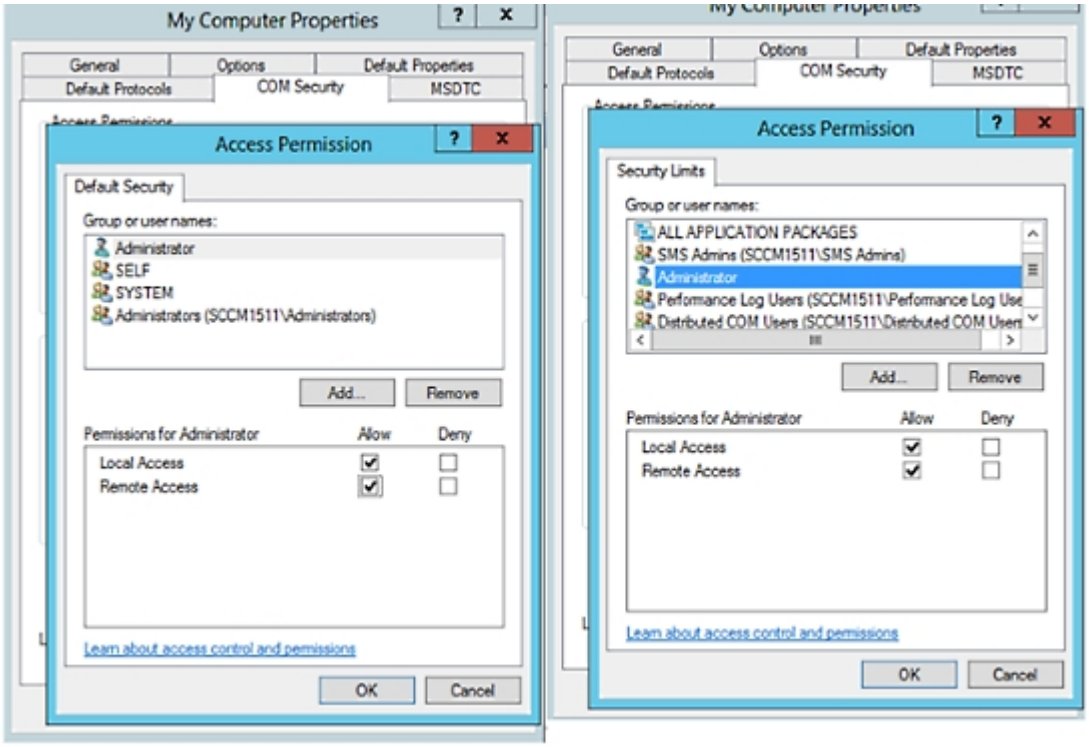
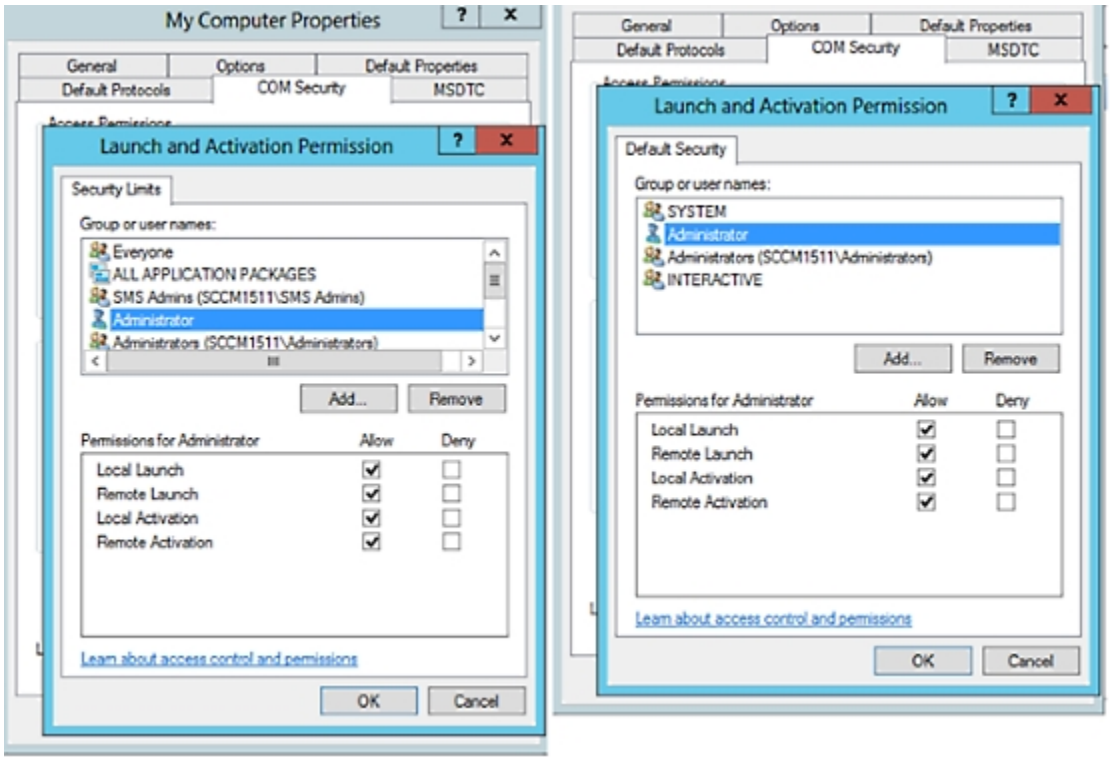


図 *12 : [*起動およびアクティベーションの権限（***Launch and Activation Permissions***）*]* のローカルおよびリモート アクセス




## 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、Active Directory ユーザには実行メソッドおよびリモートイネーブル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] > [Run] をクリックし、`wmimgmt.msc` と入力します。

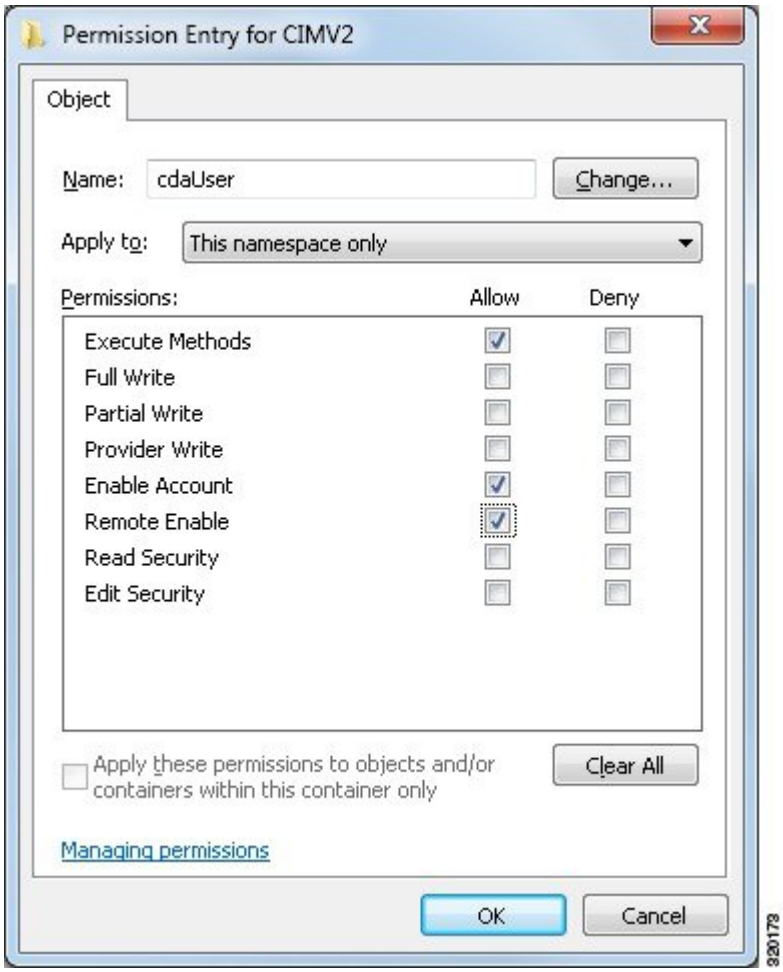
**ステップ 2** [WMI Control] を右クリックし、[プロパティ] をクリックします。

**ステップ 3** [セキュリティ] タブで [ルート] 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** 下に示すように、Active Directory ユーザを追加し、必要な権限を設定します。

図 *13 : WMI Root\CIMv2* 名前空間に必要な権限




# WMI アクセス用にファイアウォール ポートを開く

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（ISE 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 発信をすると、このポートでリスニングしているサービスが、クライアントに、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：SMB

（注） Cisco ISE 1.3 以降は SMB 2.0 をサポートします。

数値の大きいポートは動的に割り当てられ、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（ISE IP）に割り当てることができます。

# 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 サーバ定義を作成したことを確認します。正常に MDM サーバと ISE を統合した後に限り、MDM ディクショナリにデータが入力され、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、ワイヤレス LAN コントローラの 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 サーバ名または IP アドレスを追加する必要があります。**[管理（Administration）]** > **[設定（Settings）]** > **[プロキシ設定（Proxy Settings）]**の順に選択して、このアクションを実行します。

**ステップ 1** **[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[許可（Authorization）]** > **[許可プロファイル（Authorization Profiles）]** > **[追加（Add）]** を選択します。

**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 サーバ名と一致する許可プロファイルの名前を入力します。

**ステップ 4** アクセス タイプとして ACCESS_ACCEPT を選択します。

**ステップ 5** [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] フィールドに入力します。

**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** ドロップダウン リストから、使用する MDM サーバを選択します。

**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

MDM 設定を完了するには、Cisco ISE で許可ポリシー ルールを設定する必要があります。

### 始める前に

- Cisco ISE 証明書ストアに MDM サーバ証明書を追加します。
- Cisco ISE で MDM サーバ定義を作成したことを確認します。正常に MDM サーバと ISE を統合した後に限り、MDM ディクショナリにデータが入力され、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。
- 未登録のデバイスまたは非準拠のデバイスをリダイレクトするために、ワイヤレス LAN コントローラの ACL を設定します。

**ステップ 1** **[ポリシー（Policy）] > [ポリシー セット（Policy Sets）]** を選択し、許可ポリシー 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、ISE MDM ページが表示され、MDM でのデバイスの登録に関する情報が示されます。
- [PERMIT]：デバイスが Cisco ISE および MDM に登録されており、Cisco ISE および MDM 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。

  次の図は、この設定の例を示します。

  **図 *14 : MDM* の使用例の許可ポリシー ルール**


**ステップ 3** [保存（Save）] をクリックします。

# MDM Interoperability のためのワイヤレス LAN 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許可ポリシーで使用する ACL をワイヤレス LAN 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 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への着信 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への着信 DHCP トラフィックを許可します。

**ステップ 7** 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、社内ネットワークの 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 サブネットは 204.8.168.0 です。

図 *15 :* 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、失われたデバイスをワイプしたり、PIN ロックをオンにしたりできます。これは [エンドポイント（Endpoints）] ページから行うことができます。

**ステップ 1** **[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）]** を選択します。

**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）] : MDM サーバ ポリシーで設定したアプリケーションを削除します
- [PIN ロック（PIN Lock）] : デバイスをロックします

**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。

# Mobile Device Manager のレポートの表示

Cisco ISE では、MDM サーバ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報告する「変更設定監査」レポートで表示できます。

**[操作（Operations）] > [レポート（Reports）] > [変更設定監査（Change Configuration Audit）] > [MDM]** を選択し、結果のレポートで表示する期間を指定します。

# Mobile Device Manager のログの表示

[メッセージ カタログ（Message Catalog）] ページを使用して、Mobile Device Manager のログ メッセージを表示できます。**[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [メッセージカタログ（Message Catalog）]** を選択します。MDM ログ エントリのデフォルトのレポーティング レベルは「INFO」です。レポーティング レベルを「DEBUG」または「TRACE」に変更できます。