CHAPTER 9

ネットワーク デバイスの管理

この章では、ネットワーク内のデバイスを管理する方法について説明します。この章は、次の内容で構成されています。

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、AAA サービス要求はそれらを介して Cisco ISE に送信されます。ネットワーク デバイスとやりとりするには、Cisco ISE に対してネットワーク デバイスを定義する必要があります。RADIUS 認証のネットワーク デバイス、プロファイリング サービスがプロファイリング 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簡易ネットワーク管理プロトコル、および SGA デバイスのセキュリティ グループ アクセス（SGA）属性を設定できます。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 デバイスの定義において、

- RADIUS 認証の 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。共有秘密が一致した場合、ネットワーク アクセスは許可されます。成功した認証レポートが生成されます。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）を定義できます。
- Cisco SGA ソリューションに含めることができる SGA 対応デバイスからの要求を処理するには、Cisco ISE でセキュリティ グループ アクセス（SGA）対応デバイスを定義する必要があります。セキュリティ グループ アクセス ソリューションをサポートするすべてのスイッチは SGA 対応デバイスです。

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

  SGA 対応デバイスは、Cisco ISE との通信にセキュリティ グループ アクセス属性を使用します。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、および Catalyst 3000 シリーズ スイッチなど、SGA 対応デバイスは、SGA のデバイスの追加時に定義する SGA 属性を使用して認証されます。

関連項目

- 「RADIUS 認証設定」（P.A-40）
- 「SNMP 設定」（P.A-42）
- 「SGA デバイス属性の設定」（P.A-43）

Cisco ISE でのデフォルトのネットワーク デバイスの定義

Cisco ISE では、RADIUS 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 共有秘密とアクセス レベルを定義できます。

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 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 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 要求を処理します。

関連項目

- 「RADIUS 認証設定」（P.A-40）

エンドポイントがパスワード認証プロトコル（PAP）を使用して MAB を実行し、デフォルトのネットワーク デバイスが Cisco ISE で設定されている場合、ネットワーク アクセス デバイス（NAD）を使用してエンドポイントをネットワークに接続できるというセキュリティ リスクがあります。このような場合は、保護を強化するために EAP-MD5 を使用する MAB を推奨します。EAP-MD5 は、誤った共有秘密が Cisco ISE に設定されている場合に着信 RADIUS MAB 要求をドロップさせる、Message-Authenticator RADIUS 属性の使用を義務づけます。

Cisco ISE でのネットワーク デバイス定義の作成

Cisco ISE でネットワーク デバイス定義を作成し、Cisco ISE にネットワーク デバイス定義がない場合にそのデフォルトのネットワーク デバイス定義を使用できます。

ネットワーク デバイス定義には、次の設定を含める必要があります。

- デバイス名
- IP アドレスおよびサブネット マスク
- モデル名（任意）
- バージョン名（任意）
- 場所およびデバイス タイプによるネットワーク デバイス グループ
- 認証設定
- SNMP 設定
- セキュリティ グループ アクセス属性の設定

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　追加するネットワーク デバイスの名前と説明を入力します。

ステップ 4　1 つの IP アドレスおよびサブネット マスクを入力します。

ステップ 5　[モデル名（Model Name）] ドロップダウン リストの隣にある矢印をクリックして、ネットワーク デバイス モデルを選択します。

ステップ 6　[ソフトウェア バージョン（Software Version）] ドロップダウン リストの隣にある矢印をクリックして、Cisco Internetwork Operating System（Cisco IOS）バージョンを選択します。

ステップ 7　[場所（Location）] ドロップダウン リストと [デバイス タイプ（Device Type）] ドロップダウン リストからネットワーク デバイス グループを選択します。

ステップ 8　[認証設定（Authentication Settings）] チェックボックスをオンにし、認証のために RADIUS プロトコルを設定します。

ステップ 9　[SNMP 設定（SNMP Settings）] チェックボックスをオンにして、プロファイリング サービスがデバイス情報を収集するため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 10　[高度な Trustsec 設定（Advanced Trustsec Settings）] チェックボックスをオンにし、SGA 対応デバイスを設定します。

ステップ 11　[送信（Submit）] をクリックします。

関連項目

- 「ネットワーク デバイス定義の設定」（P.A-39）
- 「Cisco ISE でのネットワーク デバイスの定義」（P.9-1）
- 「RADIUS 認証設定」（P.A-40）
- 「デフォルトのネットワーク デバイス定義の設定」（P.A-45）

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デバイス定義のリストを Cisco ISE ノードに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、まず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することはできません。たとえば、2 つの異なるインポート ファイルからネットワーク デバイスを同時にインポートできません。

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

デバイスをインポートするときに、新しいレコードを作成したり、既存のレコードを更新したりできます。Cisco ISE では、インポートされたデバイスの数の概要とインポート プロセス中に見つかったエラーが表示されます。デバイスをインポートするときに、Cisco ISE で既存のデバイス定義を新しいデバイス定義で上書きするか、Cisco ISE で最初のエラーが検出されたときにインポート プロセスを中止するかを定義することもできます。

以前の Cisco ISE Release 1.1 および 1.1.x のインポート テンプレートが異なるため、それら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 Cisco ISE Release 1.2 にインポートできません。

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中止（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。

関連項目

- 「Cisco ISE からのネットワーク デバイスのエクスポート」（P.9-4）
- 「ネットワーク デバイスのインポート設定」（P.A-46）
- 「ネットワーク デバイスのインポート テンプレート形式」（P.9-8）

Cisco ISE からのネットワーク デバイスのエクスポート

Cisco ISE に設定されているネットワーク デバイスを CSV ファイルの形式でエクスポートし、そのファイルを使用してそれらのネットワーク デバイスを別の Cisco ISE ノードに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　[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、次のいずれかを実行できます。

- 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。

関連項目

「Cisco ISE へのネットワーク デバイスのインポート」（P.9-4）

Network Device Groups

Cisco ISE では、ネットワーク デバイスを含む階層ネットワーク デバイス グループ（NDG）を作成することができます。NDG は、地理的な場所、デバイス タイプ、およびネットワーク内の相対的な場所（たとえば、「アクセス レイヤ」、「データセンター」など）など、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します。

たとえば、地理的な場所に基づいてネットワーク デバイスを編成するには、大陸、地域、国によっては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

デバイスタイプでネットワーク 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 つ以上の階層的な NDG に割り当てることができます。したがって、Cisco ISE が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ために、設定された NDG の順序付きリストを通過するときに、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 グループに適用します。

ルート ネットワーク デバイス グループ

Cisco ISE には、次の 2 つの事前定義されたルート NDG があります。すべてのデバイス タイプとすべてのロケーション。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。

また、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。新しいルート NDG を作成する場合は、NDG の名前とタイプを指定する必要があります。この情報は、ルート NDG の下に子を作成するときに必要ではありません。

関連項目

「ネットワーク デバイス グループの設定」（P.A-47）

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、ポリシー定義で使用できる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たデバイス ディクショナリに追加されます。Cisco ISE では、デバイス タイプ、場所、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。

関連項目

「システム定義ディクショナリとディクショナリ属性」（P.10-1）

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ネットワーク デバイス グループを Cisco ISE ノードに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することはできません。たとえば、2 つの異なるインポート ファイルからネットワーク デバイス グループを同時にインポートできません。

CSV テンプレートを管理者ポータルからダウンロードし、テンプレートにデバイス グループの詳細を入力して、そのテンプレートを CSV ファイルとして保存できます。そのファイルを Cisco ISE にインポートできます。

デバイス グループをインポートするときに、新しいレコードを作成したり、既存のレコードを更新したりできます。デバイス グループをインポートするときに、Cisco ISE で既存のデバイス グループを新しいデバイス グループで上書きするか、Cisco ISE で最初のエラーが検出されたときにインポート プロセスを中止するかを定義することもできます。

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 Devicee 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中止（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）] をクリックするか、[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て [ネットワーク デバイス グループ（Network Device Groups）] リストページに戻ります。

関連項目

- 「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」（P.9-7）
- 「ネットワーク デバイス グループのインポート設定」（P.A-47）
- 「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」（P.9-10）

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 に設定されているネットワーク デバイス グループを CSV ファイルの形式でエクスポートし、そのファイルを使用してそれらのネットワーク デバイス グループを別の Cisco ISE ノードにインポートできます。

ステップ 1　[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 Devicee 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、次のいずれかを実行できます。

- エクスポートするデバイス グループ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 グループ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 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。

関連項目

「Cisco ISE へのネットワーク デバイス グループのインポート」（P.9-6）

Cisco ISE のインポート テンプレート

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、フィールドの形式を定義するヘッダー行があります。ヘッダー行を編集する必要はなく、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 アプリケーションで 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 ファイルを開いたり、ネットワーク デバイスおよびネットワーク デバイス グループの適切な名前で template.csv ファイルを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。

関連項目

- 「Cisco ISE へのネットワーク デバイスのインポート」（P.9-4）
- 「Cisco ISE からのネットワーク デバイスのエクスポート」（P.9-4）
- 「Cisco ISE へのネットワーク デバイス グループのインポート」（P.9-6）
- 「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」（P.9-7）
- 「ネットワーク デバイスのインポート テンプレート形式」（P.9-8）
- 「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」（P.9-10）

ネットワーク デバイスのインポート テンプレート形式

表 9-1 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 9-1　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:String(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。長さが最大 32 文字の英数字の文字列です。
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。長さが最大 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「|」記号によって区切られている複数の値を含むことができます）。
Model Name:String(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。長さが最大 32 文字の文字列です。
Software Version:String(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。長さが最大 32 文字の文字列です。
Network Device Groups:String(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）これは、長さが最大 128 文字の文字列です。
EnableKeyWrap:Boolean(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 デバイス上でサポートされている場合にのみ有効になります。有効な値は true または false です。
EncryptionKey:String(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。 ASCII：16 文字（バイト）の長さ 16 進数：32 文字（バイト）の長さ。
AuthenticationKey:String(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。 ASCII：20 文字（バイト）の長さ 16 進数：40 文字（バイト）の長さ。
InputFormat:String(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 16 進数です。

表 9-1　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 （続き）

フィールド	説明
SNMP:Version:Enumeration (|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。長さが最大 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。長さが最大 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。長さが最大 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。
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、長さが最大 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、長さが最大 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:Boolean(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:String(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する 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。
SGA:Device Id:String(32)	これはオプションのフィールドです。セキュリティ グループ アクセス デバイス ID で、長さが最大 32 文字の文字列です。
SGA:Device Password:String(256)	（SGA デバイス ID を入力した場合は必須）これはセキュリティ グループ アクセス デバイスのパスワードで、長さが最大 256 文字の文字列です。
SGA:Environment Data Download Interval:Integer:1-2147040000 seconds	これはオプションのフィールドです。セキュリティ グループ アクセス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。

表 9-1　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 （続き）

フィールド	説明
SGA:Peer Authorization Policy Download Interval:Integer:1-2147040000 seconds	これはオプションのフィールドです。セキュリティ グループ アクセス ピアの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。
SGA:Reauthentication Interval:Integer:1-2147040000 seconds	これはオプションのフィールドです。セキュリティ グループ アクセスの再認証間隔です。有効な値は 1 ～ 24850 の整数です。
SGA:SGACL List Download Interval:Integer:1-2147040000 seconds	これはオプションのフィールドです。セキュリティ グループ アクセスの 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。
SGA:Is Other SGA Devices Trusted:Boolean(true|false)	これはオプションのフィールドです。セキュリティ グループ アクセスを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。
SGA:Notify this device about SGA configuration changes:String(ENABLE_ALL|DISABLE_ALL)	これはオプションのフィールドです。SGA デバイスに対する SGA 設定変更を通知します。有効な値は ENABLE_ALL または DISABLE_ALL です
SGA:Include this device when deploying Security Group Tag Mapping Updates:Boolean(true|false)	これはオプションのフィールドです。SGT に含まれているセキュリティ グループ アクセス 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。長さが最大 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、長さが最大 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有効パスワードで、長さが最大 32 文字の文字列です。
SGA:PAC issue date:Date	これは、SGA デバイス用に Cisco ISE によって生成された最後の SGA PAC の発行日を表示するフィールドです。
SGA:PAC expiration date:Date	これは、SGA デバイス用に Cisco ISE によって生成された最後の SGA PAC の有効期限を表示するフィールドです。
SGA:PAC issued by:String	これは、SGA デバイス用に Cisco ISE によって生成された最後の SGA PAC の発行者（SGA 管理者）の名前を表示するフィールドです。それは文字列です。

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

表 9-2 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 ファイルにおけるそれらのフィールドの説明を示します。

表 9-2　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:String(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。長さが最大 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。長さが最大 1024 文字の文字列です。
Type:String(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。長さが最大 64 文字の文字列です。
Is Root:Boolean(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。

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、携帯電話会社、サービス プロバイダー、および企業全体に導入されたモバイル デバイスをセキュリティ保護、モニタ、管理、およびサポートします。MDM サーバは、導入された環境でモバイル デバイスの一部のアプリケーション（たとえば、電子メール アプリケーション）の使用を制御するポリシー サーバで構成されます。ただし、ネットワークは、ACL、SGT などに基づいてエンドポイントに細かなアクセスを提供できる唯一のエンティティです。そのジョブを実行するには、Cisco ISE は、必要なデバイスの属性について MDM サーバにクエリーして、それらのデバイスのネットワーク アクセス制御が可能なことを確認します。

図 9-1　Cisco ISE との MDM の相互運用性

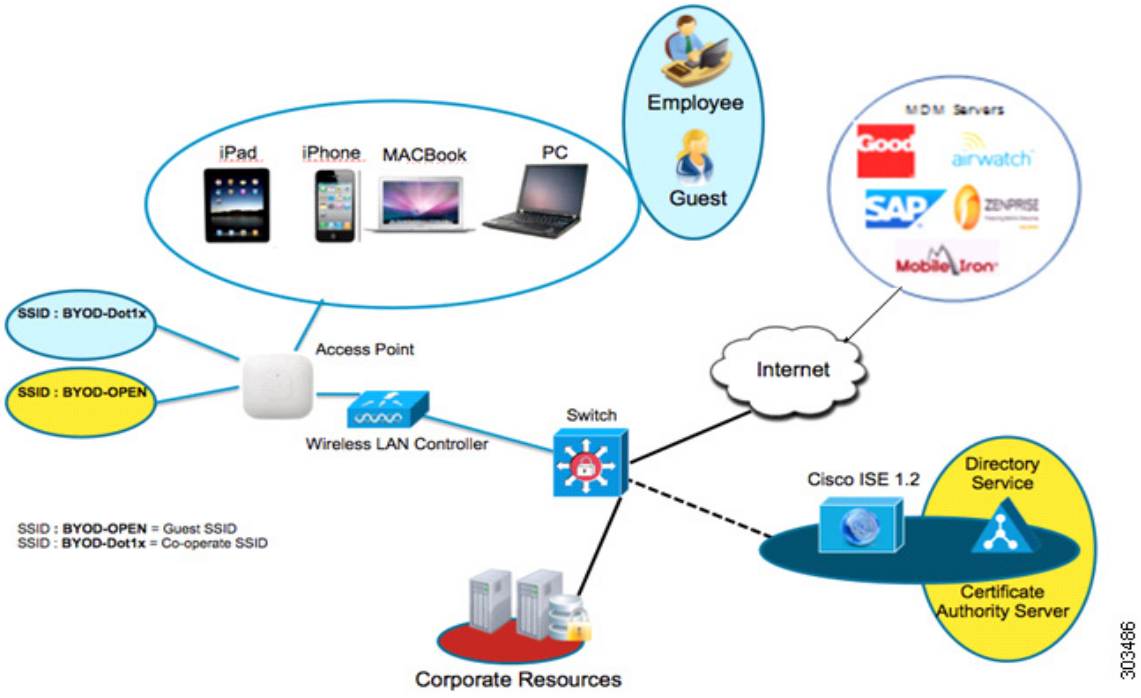


表 9-3 に、MDM セットアップで使用されるコンポーネントが一覧表示されます。

表 9-3　MDM セットアップで使用されるコンポーネント

コンポーネント	仕様
Cisco Identity Services Engine, Release 1.2	次のいずれか：ISE 3315、3355、3395、3415、3495、または VMware
MDM サーバ	—
（*任意*）認証権限サーバ	Microsoft の仕様（Windows 2008 R2 Enterprise SP2）に従う
ワイヤレス LAN コントローラ（WLC）（Wireless LAN Controller (WLC)）	• ハードウェア：5500 シリーズ、2500 シリーズ、WLSM-2 • ソフトウェア：Unified Wireless Network ソフトウェア リリース 7.2
モバイル デバイス	MDM ベンダーでサポートされるデバイス。サポートされる MDM ベンダーの一覧については、「サポート対象の MDM サーバ」（P.9-14）を参照してください。 たとえば、Apple iOS 5.0 以降、Google Android 2.3。

図 9-1 では、Cisco ISE は適用ポイントであるのに対し、MDM ポリシー サーバはポリシー情報ポイントです。Cisco ISE は、完全なソリューションを提供するために MDM サーバからデータを取得します。

外部の 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。このタイプのサードパーティ接続を設定することによって、MDM データベースで使用可能な詳細情報を活用できます。Cisco ISE は、外部の MDM サーバからさまざまな情報を引き出すために REST API コールを使用します。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、および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、Cisco ISE ネットワークへのリモート デバイス アクセスを詳細に制御できるようになります。

これ以降の各項では、MDM 設定についてのみ説明します。ISE および WLC の設定の詳細については、次の場所から入手できる設計ガイドを参照してください。

http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns744/landing_DesignZone_TrustSec.html

サポートされる MDM の使用例

Cisco ISE が外部 MDM サーバと連携して実行する機能は、次のとおりです。

- デバイス登録の促進：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、ユーザ ロール、デバイス タイプなどに基づいて登録されます。
- デバイスの修復の処理：エンドポイントは、非準拠になった後は、制限付きアクセス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 [管理（Administration）] > [ID の管理（Identity Management）] > [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
- 定期的なコンプライアンス チェック：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。
- 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。

Cisco ISE では、次の属性に基づいて MDM ポリシーを設定できます。

- DeviceRegisterStatus
- DeviceCompliantStatus
- DiskEncryptionStatus
- PinLockStatus
- JailBrokenStatus
- Manufacturer
- IMEI
- SerialNumber

- OsVersion
- phoneNumber

サポート対象の 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。

- Airwatch, Inc.
- Good Technology
- MobileIron, Inc.
- Zenprise, Inc.
- SAP Afaria
- Fiberlink MaaS

MDM サーバで使用されるポート

表 9-4 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 Server Documentation*』を参照してください。

表 9-4　MDM サーバで使用されるポート

MDM サーバ	ポート
Mobile Iron	443
Zenprise	443
Good	19005
Airwatch	443
Afaria	443
Fiberlink MaaS	443

MDM ディクショナリ属性

MDM サーバ定義を Cisco ISE に追加したら、認可ポリシーで使用できる MDM ディクショナリ属性が Cisco ISE で使用可能になります。認可ポリシーで使用できるディクショナリ属性を表示できます（[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [ディクショナリ（Dictionaries）] > [MDM] > [ディクショナリ属性（Dictionary Attributes）]）。

ポリシーでこれらの MDM ディクショナリ属性を使用しているときは、Cisco ISE から MDM サーバ コンフィギュレーションを削除できません。MDM サーバ コンフィギュレーションを削除するには、まずポリシーから MDM ディクショナリ属性を排除し、次に Cisco ISE から MDM サーバを削除します。

MDM 統合プロセスのフロー

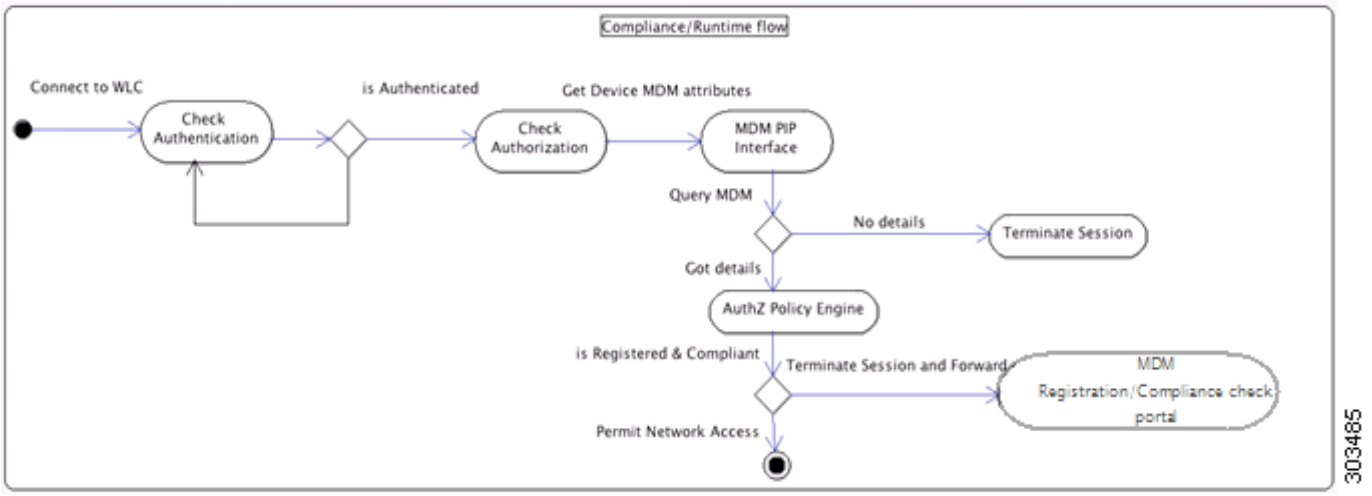
この項では、MDM 統合プロセスについて説明します。

1. ユーザは SSID にデバイスを関連付けます。
2. （任意）デバイスが登録されていない場合、ユーザはデバイス オンボーディング フローを通過します。
3. Cisco ISE は、MDM サーバに API コールを行います。
4. この API コールは、このユーザのデバイスのリストとデバイスのポスチャ ステータスを返します。

（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。

5. 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 にリダイレクトするために NAD に認可要求を送信します。MDM サーバ ページがユーザに表示されます。
6. Cisco ISE は MDM を使用してデバイスをプロビジョニングし、ユーザがデバイスを登録するための適切なページを表示します。
7. 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（自動リダイレクトまたは手動のブラウザの表示更新によって）。
8. Cisco ISE は、再度 MDM サーバにポスチャ ステータスについてクエリーします。
9. ユーザのデバイスが MDM サーバに設定されたポスチャ（コンプライアンス）ポリシーに準拠していない場合は、デバイスが非コンプライアンスであり、準拠する必要があることがユーザに通知されます。
10. ユーザのデバイスが準拠するようになった後に、MDM サーバは内部テーブルのデバイスの状態を更新します。
11. ユーザがブラウザをリフレッシュすると、制御は Cisco ISE に戻されます。
12. 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、認可変更（CoA）を適切に発行します。

次の図に、MDM プロセス フローを示します。



Cisco ISE とともに MDM サーバの設定

Cisco ISE とともに MDM サーバを設定するには、次のタスクを実行します。

1. 「Cisco ISE への MDM サーバ証明書のインポート」（P.9-16）
2. 「Mobile Device Manager 定義の作成」（P.9-16）
3. ワイヤレス LAN コントローラ上で ACL を設定します。詳細については、「MDM の相互運用性のためのワイヤレス LAN コントローラでの ACL の設定」（P.F-10）を参照してください。
4. 「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の設定」（P.9-17）
5. 「MDM 使用例の許可ポリシー ルールの設定」（P.9-18）

Cisco ISE への MDM サーバ証明書のインポート

Cisco ISE が MDM サーバと接続するには、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、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。

ステップ 1　MDM サーバから MDM サーバ証明書をエクスポートして、ローカル マシン上に保存します。

ステップ 2　[管理（Administration）] > [証明書（Certificates）] > [証明書ストア（Certificate Store）] > [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　フレンドリ名を追加します。

ステップ 5　[送信（Submit）] をクリックします。

ステップ 6　[証明書ストア（Certificate Store）] リスト ページに MDM サーバ証明書がリストされていることを確認します。

Mobile Device Manager 定義の作成

Cisco ISE がログインしたユーザのデバイスから最新のデバイス接続ステータスをできるだけオンデマンドで取得できるように、外部 MDM サーバの Mobile Device Manager（MDM）定義を 1 つ以上作成できます。（複数の MDM サーバ定義を設定できますが、Cisco ISE と相互運用する MDM サーバは一度に 1 つしかアクティブにできません）

はじめる前に

Cisco ISE に MDM サーバ証明書をインポートしたことを確認します。詳細については、「Cisco ISE への MDM サーバ証明書のインポート」（P.9-16）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）] > [MDM] 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　追加する MDM サーバの名前と説明を入力します。

ステップ 4　アクティブにする MDM サーバを示すために、[ステータス（Status）] チェックボックスをオン（またはオフ）にします。Cisco ISE は 1 度に 1 つの MDM サーバとしか通信できません。

ステップ 5　[MDM サーバ ホスト（MDM server host）] フィールドに、MDM サーバの IP アドレスまたはホスト名（FQDN）を入力します。

ステップ 6　Cisco ISE が MDM サーバと通信する必要があるネットワークおよびプロキシ ポートを指定します。

ステップ 7　マルチテナント クラウド ベースの MDM サービスを使用している場合、サーバ インスタンスを指定します。

ステップ 8　Cisco ISE が MDM サーバ データベースにログインし、それと相互運用できるように、MDM サーバ管理者のユーザ名とパスワードを指定します。

ステップ 9　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。この値は、MDM サーバのポーリング間隔と同じである必要があります。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。多数のアクティブ クライアントが存在する実稼働環境でこの値を 60 分未満に設定した場合、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。

ステップ 10　Cisco ISE と MDM サーバの接続をアクティブにするには、[有効（Enable）] チェックボックスをオンにします。

ステップ 11　MDM サーバへの Cisco ISE の接続をテストするには、[テスト接続（Test Connection）] をクリックします。

Cisco ISE に接続エラーが表示される場合は、作成した定義を削除し、MDM サーバに到達可能なことを確認し、Cisco ISE で MDM サーバ定義を再作成します。

ステップ 12　[送信（Submit）] をクリックし、MDM サーバ定義を保存します。Cisco ISE を MDM サーバに正常に接続した後にのみ、MDM ディクショナリは Cisco ISE に読み込まれます。

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の設定

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。

はじめる前に

Cisco ISE で MDM サーバ定義を作成したことを確認します。Cisco ISE を MDM サーバに正常に統合した後にのみ、MDM ディクショナリが読み込まれ、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。「Mobile Device Manager 定義の作成」（P.9-16）を参照してください。

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 コントローラ上で ACL を設定します。「MDM の相互運用性のためのワイヤレス LAN コントローラでの ACL の設定」（P.F-10）を参照してください。

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　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（Access Type）] 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　[送信（Submit）] をクリックします。

MDM 使用例の許可ポリシー ルールの設定

Cisco ISE で 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。

はじめる前に

- Cisco ISE 証明書ストアに MDM サーバ証明書を追加します。「Cisco ISE への MDM サーバ証明書のインポート」（P.9-16）を参照してください。
- Cisco ISE で MDM サーバ定義を作成したことを確認します。Cisco ISE を MDM サーバに正常に統合した後にのみ、MDM ディクショナリが読み込まれ、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。「Mobile Device Manager 定義の作成」（P.9-16）を参照してください。
- 未登録または非準拠のデバイスをリダイレクトするために、ワイヤレス LAN コントローラ上で ACL を設定します。「MDM の相互運用性のためのワイヤレス LAN コントローラでの ACL の設定」（P.F-10）

ステップ 1　[ポリシー（Policy）] > [許可（Authorization）] > [新規ルールを下に挿入（Insert New Rule Below）] を選択します。

ステップ 2　次のルールを追加します。

- MDM_Un_Registered_Non_Compliant：MDM サーバにまだ登録されていないか、または MDM ポリシーに準拠していないデバイス用。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 へ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 に登録され、MDM に登録され、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が許可されます。

図 9-2 に、この設定例を示します。

図 9-2　MDM 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。

デバイスの消去またはロック

Cisco ISE では、失われたデバイスを消去するか、そのピン ロックをオンにすることができます。[エンドポイント（Endpoints）] ページからこれを行うことができます。

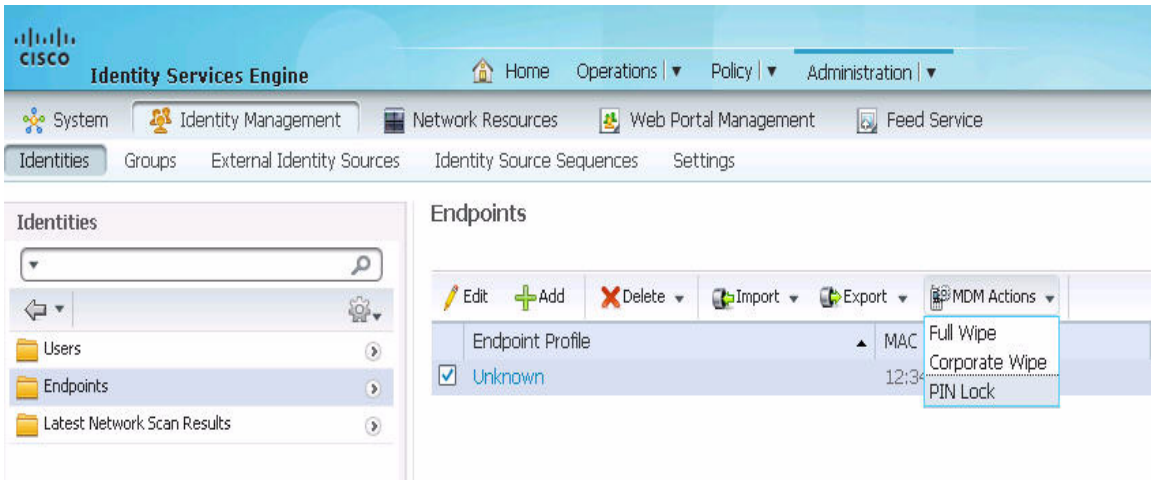
ステップ 1　[管理（Administration）] > [ID の管理（Identity Management）] > [ID（Identities）] > [エンドポイント（Endpoints）] を選択します。

ステップ 2　消去またはロックするデバイスの隣にあるチェックボックスをオンにします。

ステップ 3　図に示すように、[MDM アクセス（MDM Access）] ドロップダウン リストから、次のいずれかのオプションを選択します。

- 完全消去：デバイスからすべての情報を削除します
- 企業消去：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
- ピン ロック：デバイスをロックします

図 9-3　　デバイスのロック



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

Mobile Device Manager 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。

関連項目

- 「Mobile Device Manager と Cisco ISE との相互運用性」（P.9-11）
- 「サポートされる MDM の使用例」（P.9-13）
- 「サポート対象の MDM サーバ」（P.9-14）
- 「Mobile Device Manager 定義の作成」（P.9-16）
- 「Mobile Device Manager ログの表示」（P.9-20）

Mobile Device Manager 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。

関連項目

- 「Mobile Device Manager と Cisco ISE との相互運用性」（P.9-11）
- 「サポートされる MDM の使用例」（P.9-13）
- 「サポート対象の MDM サーバ」（P.9-14）
- 「Mobile Device Manager 定義の作成」（P.9-16）
- 「Mobile Device Manager レポートの表示」（P.9-19）