基本的なセットアップ

管理ポータル

図 *1 : Cisco ISE* 管理ポータル

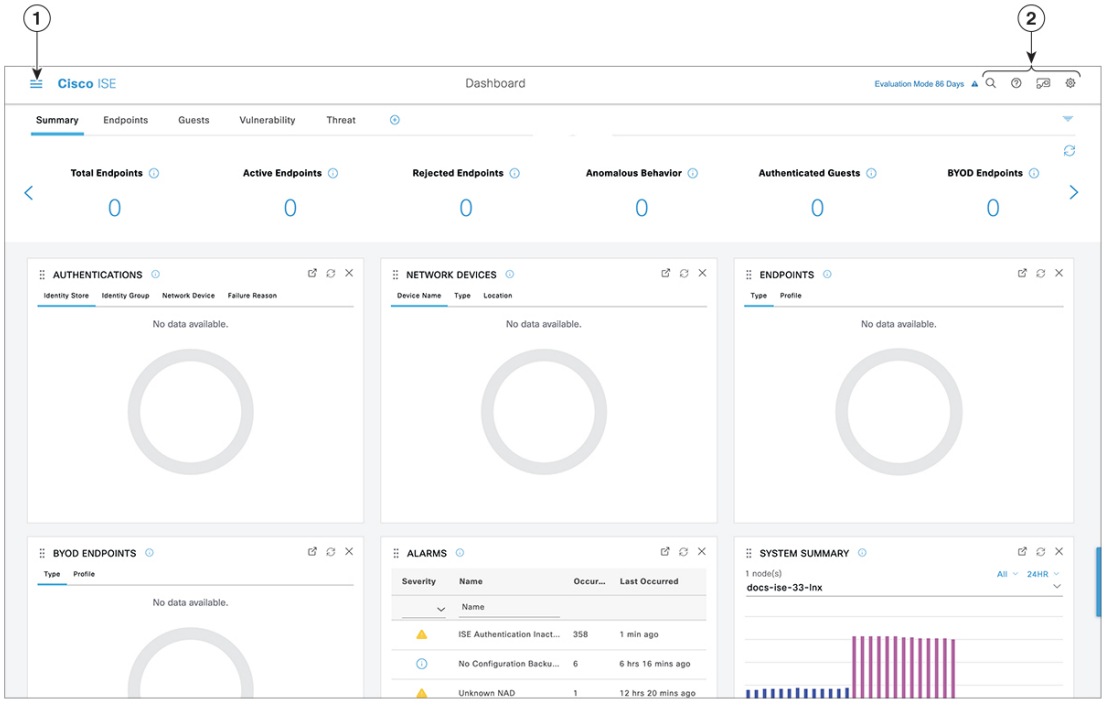
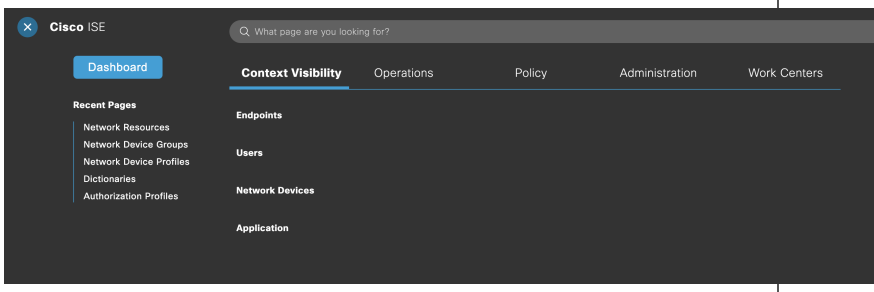


表 *1 : Cisco ISE* 管理ポータルのコンポーネント

1	メニューアイコン	[メニュー（Menu）] アイコン（☰）をクリックすると、次のメニューを含むスライドインウィンドウが表示されます。スライドインメニューウィンドウには、必要なウィンドウを見つけるための検索バーもあります。ホームページで [ダッシュボード（Dashboard）] をクリックします。 図 *2 : Cisco ISE* メインメニュー  • [コンテキストの可視性（Context Visibility）] : コンテキストの可視性ウィンドウには、エンドポイント、ユーザー、およびネットワーク アクセス デバイス（NAD）に関する情報が表示されます。コンテキスト可視性情報は、登録したライセンスに応じて、機能、アプリケーション、個人所有デバイスの持ち込み（BYOD）、およびその他のカテゴリでセグメント化されます。コンテキスト可視性ウィンドウは、中央データベースを使用し、データベーステーブル、キャッシュ、バッファから情報を収集します。その結果、コンテキスト可視性ダッシュレットとリストのコンテンツがすぐに更新されます。コンテキスト可視性ウィンドウは上部のダッシュレットおよび下部の情報のリストから構成されます。リストのカラム属性を変更することによってデータをフィルタすると、変更したコンテンツを表示するためにダッシュレットが更新されます。 • [ポリシー（Policy）] : ポリシーウィンドウには、認証、許可、プロファイリング、ポスチャ、クライアントプロビジョニングの領域でネットワークセキュリティを管理するためのツールが含まれています。 • [管理（Administration）] : 管理ウィンドウには、Cisco ISE ノード、ライセンス、証明書、ネットワークデバイス、ユーザー、エンドポイント、およびゲストサービスを管理するためのツールが含まれています。

2	右上のメニューアイコン	

- 

  このアイコンを使用してエンドポイントを検索し、プロファイル、障害、ID ストア、ロケーション、デバイスタイプ別にそれらの分布を表示します。

- 

  アイコンをクリックすると、複数のリソースへのアクセスを提供するインタラクティブヘルプメニューが表示されます。

- 

  このアイコンをクリックすると、次のオプションにアクセスできます。

  - [PassiveIDセットアップ（PassiveID Setup）]：[PassiveIDセットアップ（PassiveID Setup）]オプションでは、Active Directory を使用してパッシブ ID をセットアップする [PassiveIDセットアップ（PassiveID Setup）] ウィザードが起動されます。外部認証サーバーからユーザー ID と IP アドレスを収集し、認証済み IP アドレスを対応するサブスクライバに配信するように、サーバーを設定します。

  - [可視性セットアップ（Visibility Setup）]：[可視性セットアップ（Visibility Setup）] は、アプリケーション、ハードウェアインベントリ、USB ステータス、ファイアウォールステータス、Windows エンドポイントの全般的なコンプライアンスステータスなどのエンドポイントデータを収集する、価値の実証（PoV）サービスです。収集されたデータは、Cisco ISE に送信されます。[ISE 可視性セットアップ（ISE Visibility Setup）] ウィザードを起動すると、IP アドレスの範囲を指定して、ネットワークの特定セグメントまたはエンドポイントグループに対してエンドポイント検出を実行できます。

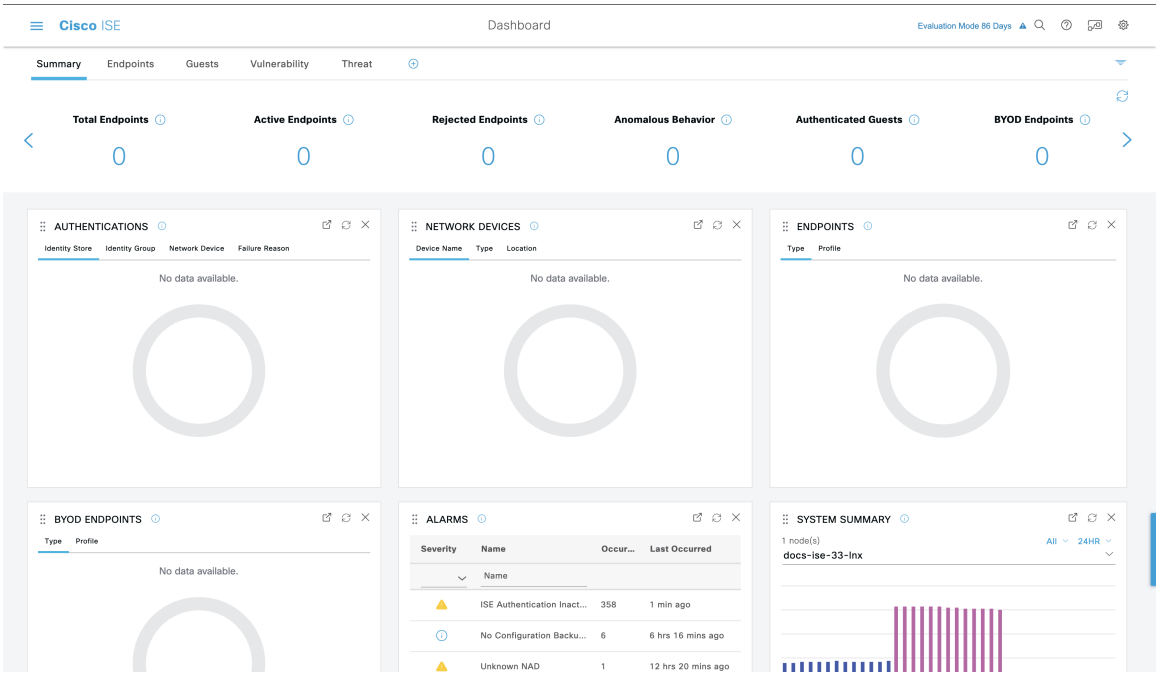
    PoV サービスは Cisco Stealth Temporal エージェントを使用して、エンドポイントポスチャデータを収集します。Cisco ISE は、管理者アカウントタイプで Windows を実行しているコンピュータに Cisco Stealth Temporal エージェントをプッシュし、一時的な実行ファイルを自動実行してコンテキストを収集します。その後、エージェントは自動的に削除されます。Cisco Stealth Temporal エージェントのオプションデバッグ機能を使用するには、[エンドポイントロギング（Endpoint Logging）] チェックボックス（[メニュー（Menu）]アイコン（）をクリックして、**[可視性セットアップ（Visibility Setup）]** > **[ポスチャ（Posture）]** を選択）をチェックして、1 つまた

		は複数のエンドポイントにデバッグログを保存します。ログは、次のいずれかの場所で参照できます。 • C:\WINDOWS\syswow64\config\systemprofile\（64 ビット オペレーティング システム） • C:\WINDOWS\system32\config\systemprofile\（32 ビット オペレーティング システム） • [エンドポイントスクリプトの実行（Run Endpoint Scripts）]：接続されたエンドポイントでスクリプトを実行して、組織の要件に準拠する管理タスクを実行するには、このオプションを選択します。これには、使用されていないソフトウェアのアンインストール、プロセスやアプリケーションの開始または終了、特定のサービスの有効化または無効化などのタスクが含まれます。 •  このアイコンをクリックすると、オンラインヘルプの起動やアカウント設定の構成など、システムアクティビティのメニューが表示されます。

Cisco ISE ホームのダッシュボード

Cisco ISE ホームダッシュボードには、効果的なモニターリングおよびトラブルシューティングに必要不可欠な、統合された相関性のあるライブ統計データが表示されます。ダッシュボード要素には通常、24時間のアクティビティが表示されます。次の図に、Cisco ISE ダッシュボードで使用できる情報を例示します。Cisco ISE ダッシュボードデータはプライマリポリシー管理ノード（PAN）のポータルでのみ表示されます。

図 *3 : Cisco ISE* ホームダッシュボード



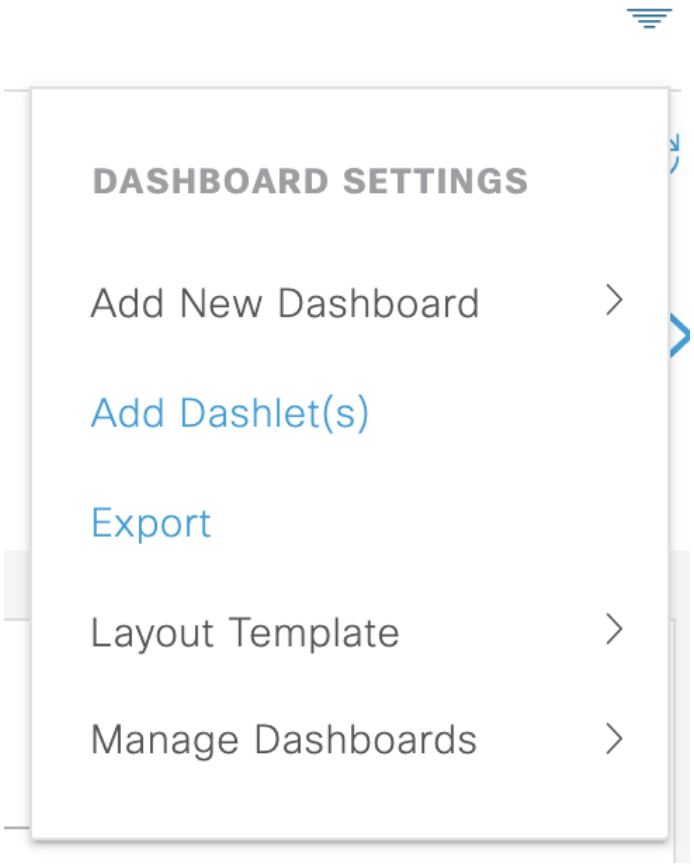
[ホーム（Home）] ページには、Cisco ISE データを表示する 5 つのデフォルトのダッシュボードがあります。これらの各ダッシュボードには、複数の事前定義ダッシュレットがあります。

- **[概要（Summary）]**：このダッシュボードには、線形の [メトリック（Metrics）] ダッシュレット、円グラフダッシュレット、およびリストダッシュレットがあります。[メトリック（Metrics）] ダッシュレットは設定できません。このダッシュボードにはデフォルトでは、**[ステータス（Status）]**、**[エンドポイント（Endpoints）]**、**[エンドポイントカテゴリ（Endpoint Categories）]**、**[ネットワークデバイス（Network Devices）]** があります。
- **[エンドポイント（Endpoints）]**：このダッシュボードにはデフォルトでは、**[ステータス（Status）]**、**[エンドポイント（Endpoints）]**、**[エンドポイントカテゴリ（Endpoint Categories）]**、**[ネットワークデバイス（Network Devices）]** があります。
- **[ゲスト（Guests）]**：このダッシュボードには、ゲストユーザータイプ、ログイン失敗、およびアクティビティのロケーションに関する情報を提供するダッシュレットがあります。
- **[脆弱性（Vulnerability）]**：このダッシュボードには、脆弱性サーバーが Cisco ISE にレポートする情報が表示されます。
- **[脅威（Threat）]**：このダッシュボードには、Cisco ISE に送信された脅威サーバーのレポートの情報が表示されます。

ホーム ダッシュボードの設定

ホームページダッシュボードをカスタマイズするには、ページの右上隅にある [逆ピラミッド（Inverted Pyramid）] アイコンをクリックします。

図 *4:* ダッシュボードのカスタマイズ



ドロップダウンリストには、次のオプションが表示されます。

- [新しいダッシュボードの追加（Add New Dashboard）] では、新しいダッシュボードを追加できます。表示されたフィールドに値を入力し、[適用（Apply）] をクリックします。
- [ダッシュレットの追加（Add Dashlet(s)）] は、使用可能なダッシュレットのリストを含むダイアログボックスを表示します。ダッシュレットをダッシュボードに追加または削除するには、ダッシュレット名の横にある [追加（Add）] または [削除（Remove）] をクリックします。
- [エクスポート（Export）] を選択すると、選択されているホームビューを PDF に保存します。
- [レイアウトテンプレート（Layout Template）] を選択すると、このビューに表示されるカラムの数を設定します。

- [ダッシュボード管理（Manage Dashboards）] には、次の 2 つのオプションがあります。
  - [デフォルトダッシュボードとしてマーク（Mark As Default Dashboard）]：このオプションを選択すると、[ホーム（Home）] を選択したときに現在のダッシュボードがデフォルトビューになります。
  - [すべてのダッシュボードをリセット（Reset All Dashboards）]：このオプションを使用すると、すべてのダッシュボードもリセットし、すべてのホームダッシュボードの設定を削除します。

[コンテキストの可視性（Context Visibility）] のビュー

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

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

プライマリ PAN からのコンテキストの可視性データのみを表示できます。

[コンテキストの可視性（Context Visibility）] ウィンドウのダッシュレットには、エンドポイントと、エンドポイントから NAD への接続に関する情報が表示されます。現在表示されている情報は、各ウィンドウのダッシュレットの下にあるデータのリストの内容に基づいています。各ウィンドウには、タブの名前に基づいてエンドポイントデータが表示されます。データをフィルタリングすると、リストとダッシュレットの両方が更新されます。データをフィルタリングするには、1 つ以上の円グラフの特定部分をクリックするか、表で行をフィルタリングするか、またはこれらの操作を組み合わせて実行します。複数のフィルタを選択した場合、フィルタ結果は加算的になります。これはカスケードフィルタと呼ばれます。これにより、ドリルダウンして特定のデータを見つけることができます。また、リストでエンドポイントをクリックして、そのエンドポイントの詳細ビューを表示することもできます。

[コンテキストの可視性（Context Visibility）] の下には、4 つのメインメニューオプションがあります。

- [エンドポイント（Endpoints）]：デバイスのタイプ、コンプライアンス ステータス、認証タイプ、ハードウェア インベントリなどに基づいて表示するエンドポイントをフィルタ処理できます。詳細については、ハードウェア ダッシュボード （15 ページ）を参照してください。

（注） アカウンティングの開始と更新の情報が Cisco ISE に確実に送信されるように、ネットワーク アクセス デバイス（NAD）でアカウンティングの設定を有効にすることを推奨します。

Cisco ISE では、アカウンティングが有効になっている場合にのみ、最新の IP アドレス、セッションのステータス（ [接続（Connected）]、 [切断（Disconnected）]、または [拒否（Rejected）]）、エンドポイントの非アクティブな日数などのアカウンティング情報を収集できます。この情報は、Cisco ISE 管理ポータルの [ライブログ（Live Logs）]、[ライブセッション（Live Sessions）]、および [コンテキストの可視性（Context Visibility）] の各ウィンドウに表示されます。NAD でアカウンティングが無効になっている場合、[ライブセッション（Live Sessions）]、[ライブログ（Live Logs）]、および [コンテキストの可視性（Context Visibility）] の各ウィンドウ間でアカウンティング情報が欠落しているか、間違っているか、または一致していない可能性があります。

（注） Cisco ISE 管理ポータルのホームページで使用可能な [可視性の設定（Visibility Setup）] ワークフローでは、エンドポイント検出用の IP アドレス範囲のリストを追加できます。このワークフローの設定後に Cisco ISE はエンドポイントを認証しますが、設定した IP アドレス範囲内に含まれていないエンドポイントは、**[コンテキストの可視性（Context Visibility）] > [エンドポイント（Endpoints）]** ウィンドウと [エンドポイント（Endpoints）] のリストページ（**[ワークセンター（Work Centers）] > [ネットワークアクセス（Endpoints）] > [ID（Identities）] > [エンドポイント（Endpoints）]**）に表示されません。

- [ユーザー（Users）]：ユーザー ID ソースからのユーザーベースの情報を表示します。

  ユーザー名またはパスワード属性が変更されると、認証ステータスが変更された時点で [ユーザー（Users）] ウィンドウに反映されます。

  Microsoft Active Directory でユーザー名が変更されると、再認証後すぐに [ユーザー（Users）] ウィンドウに更新された変更が表示されます。

  Microsoft Active Directory で電子メール、電話番号、部門など、その他の属性が変更されると、再認証から 24 時間後に [ユーザー（Users）] ウィンドウに更新された属性が表示されます。

（注） AD からのユーザー属性の更新は、Active Directory プローブで設定されている間隔によって異なります。詳細については、「Active Directory プローブ」を参照してください。

- [ネットワークデバイス（Network Devices）]：このウィンドウには、接続しているエンドポイントがある NAD のリストが表示されます。任意の NAD について、対応する [エンドポイント数（Number of endpoints）] 列に表示されるエンドポイントの数をクリックします。その NAD によってフィルタ処理されたすべてのデバイスをリストしたウィンドウが表示されます。

（注） ネットワークデバイスに SNMPv3 パラメータを設定した場合、Cisco ISE モニターリングサービス（**[操作（Operations）]** > **[レポート（Reports）]** > **[カタログ（Catalog）]** > **[ネットワークデバイス（Network Device）]** > **[セッションステータス概要（Session Status Summary）]**）によって提供される [ネットワークデバイスセッションステータス概要（Network Device Session Status Summary）] レポートを生成できません。ネットワーク デバイスが SNMPv1 または SNMPv2c パラメータを使用して設定されている場合は、このレポートを正常に生成できます。

- [アプリケーション（Application）]：このウィンドウを使用して、インストールされている特定のアプリケーションがあるエンドポイントの数を識別します。結果は、グラフ形式と表形式で表示されます。グラフ表示は、比較分析に役立ちます。たとえば、Google Chrome ソフトウェアを使用してエンドポイントの数をバージョン、ベンダー、カテゴリ（フィッシング詐欺対策、ブラウザなど）と共に、表や棒グラフで確認することができます。詳細については、「アプリケーション ダッシュボード」を参照してください。

[コンテキストの可視性（Context Visibility）] ウィンドウの新しいタブを作成し、カスタムリストを作成して、さらにフィルタリングを行います。カスタムビューではダッシュレットはサポートされていません。

ダッシュレット内の円形グラフのセクションをクリックすると、そのダッシュレットからフィルタ処理されたデータを含む新しいウィンドウが表示されます。この新しいウィンドウから、ビューに表示するデータのフィルタリング （18 ページ）の説明に従って、表示されたデータを引き続きフィルタ処理できます。

エンドポイントデータを検出するための [コンテキストの可視性（Context Visibility）] ウィンドウの使用に関する詳細については、Cisco YouTube ビデオ（https://www.youtube.com/watch?v=HvonGhrydfg）を参照してください。このビデオでは ISE 2.1 を使用しています。

関連トピック

ハードウェア ダッシュボード （15 ページ）

コンテキストの可視性の属性

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

オペレーティング システム

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

（注） CiscoISEでエンドポイントに複数のプローブを有効にした場合、[コンテキストの可視性（Context Visibility）] ページに表示されるエンドポイントのオペレーティングシステムのデータにいくつかの不一致が生じることがあります。

ポータル名

- *Portal.Name*：デバイス登録が有効になっている場合のゲストポータル名。
- *PortalName*：デバイス登録が無効になっている場合の名。

ポータルユーザー

- *User-Name*：RADIUS 認証のユーザー名
- *GuestUserName*：ゲストユーザー名。
- *PortalUser*：ポータルユーザー名。

アプリケーション ダッシュボード

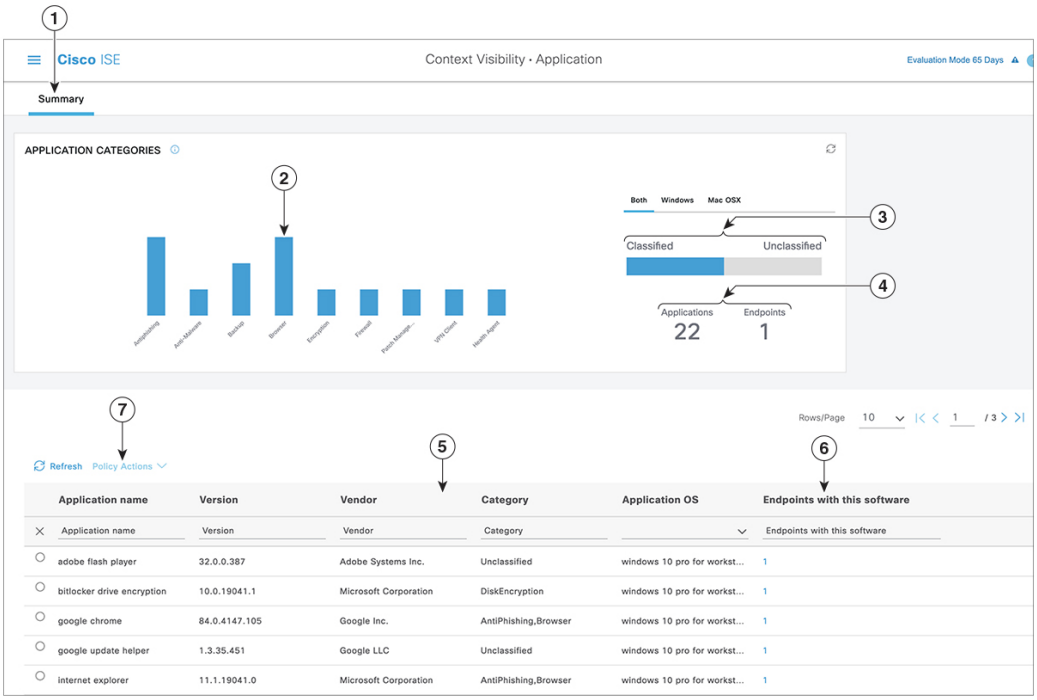
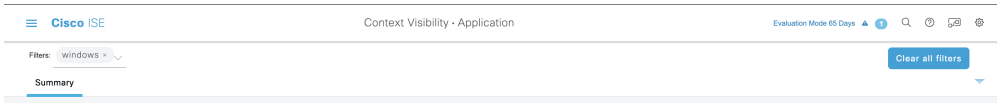


表 *2:* アプリケーション ダッシュボードの説明

ラベル	説明
1	**[要約（Summary）]** タブは、デフォルトでホームページに表示されます。棒グラフを含む[アプリケーション カテゴリ（Application Categories）] ダッシュレットが表示されます。アプリケーションは13のカテゴリに分類されます。これらのカテゴリに属さないアプリケーションは、**[未分類（Unclassified）]** としてグループ化されます。 利用可能なカテゴリは、[マルウェア対策（Anti-Malware）]、[フィッシング対策（Antiphishing）]、[バックアップ（Backup）]、[ブラウザ（Browser）]、[データ漏洩防止（Data Loss Prevention）]、[データ ストレージ（Data Storage）]、[暗号化（Encryption）]、[ファイアウォール（Firewall）]、[メッセンジャ（Messenger）]、[パッチ管理（Patch Management）]、[パブリック ファイル共有（Public File Sharing）]、[仮想マシン（Virtual Machine）]、[VPN クライアント（VPN Client）] です。
2	各バーは、分類されたカテゴリに対応します。各バーの上にマウスを置くと、選択したアプリケーションカテゴリに対応するアプリケーションとエンドポイントの合計数が表示されます。

<table>
<tr><th>ラベル</th><th>説明</th></tr>
<tr><td>3</td><td>分類されたカテゴリに該当するアプリケーションとエンドポイントは青色で表示されます。未分類のアプリケーションとエンドポイントはグレーで表示されます。分類されたカテゴリバーまたは分類されていないカテゴリバーの上にマウスを置くと、そのカテゴリに属するアプリケーションとエンドポイントの合計数が表示されます。[分類済み（Classified）] をクリックして、ウィンドウ内の棒グラフと表で結果を表示できます。[未分類（Unclassified）] をクリックすると、ウィンドウ内の棒グラフが無効になり（グレー表示）、表に結果が表示されます。</td></tr>
<tr><td>4</td><td>アプリケーションとエンドポイントは、選択されたフィルタに基づいて表示されます。異なるフィルタをクリックすると、パンくずリストを表示できます。[すべてのフィルタをクリア（Clear All Filters）] の順にクリックして、すべてのフィルタを削除できます。
 
</td></tr>
<tr><td>5</td><td>複数のバーをクリックすると、対応する分類されたアプリケーションとエンドポイントが表に表示されます。たとえば、[マルウェア対策（Antimalware）]および[パッチ管理（Patch Management）] カテゴリを選択すると、次の結果が表示されます。
<table>
<tr><th>アプリケーション</th><th>バージョン</th><th>Vendor</th><th>カテゴリ</th><th>アプリケーション OS</th><th>このソフトウェアで使用するエンドポイント</th></tr>
<tr><td>Gatekeeper</td><td>9.9.5</td><td>Apple Inc.</td><td>マルウェア対策</td><td>Windows 7 64 ビット、mac osx 10.10、mac osx 8、mac osx 9</td><td>5</td></tr>
<tr><td>Gatekeeper</td><td>10.9.5</td><td>Apple Inc.</td><td>マルウェア対策</td><td>Windows 8 64 ビット、mac osx 10.10</td><td>3</td></tr>
<tr><td>ソフトウェア更新</td><td>2.3</td><td>Apple Inc.</td><td>パッチ管理</td><td>Windows 7 64 ビット、mac osx 10.10、mac osx 8、mac osx 9</td><td>5</td></tr>
</table></td></tr>
<tr><td>6</td><td>表の [このソフトウェアで使用するエンドポイント（Endpoints With This Software）] 列のエンドポイントをクリックして、Mac アドレス、NAD IP アドレス、NAD ポート ID/SSID、IPv4 アドレスなどのエンドポイントの詳細を表示します。</td></tr>
</table>

ラベル	説明
7	アプリケーションのコンプライアンス条件と修復を作成するには、アプリケーション名を選択し、[ポリシー アクション（Policy Actions）] ドロップダウンリストから [アプリケーション コンプライアンスの作成（Create App Compliance）] オプションを選択します。

ハードウェア ダッシュボード

[コンテキストの可視性（context visibility）] の下の [エンドポイント ハードウェア（endpoint hardware）] タブは、短期間にエンドポイント ハードウェア インベントリ情報を収集、分析、およびレポートするのに役立ちます。メモリ容量が小さいエンドポイントの検出や、エンドポイントのBIOSモデル/バージョンの検出など、情報を収集することができます。これらの結果に基づいて、メモリ容量を増やしたり、BIOS バージョンをアップグレードすることができます。アセットの購入を計画する前に、要件を評価することができます。リソースを適時に交換することができます。モジュールをインストールしたりエンドポイントとやりとりすることなく、この情報を収集できます。要約すると、アセットのライフサイクルを効果的に管理できます。

[コンテキストの可視性（Context Visibility）] > [エンドポイント（Endpoints）] > [ハードウェア（Hardware）] ページには、[製造者（Manufacturers）] および [エンドポイント使用率（Endpoint Utilizations）] ダッシュレットが表示されます。これらのダッシュレットは、選択されたフィルタに基づく変更を反映します。[製造者（Manufacturers）] ダッシュレットには、Windows および Mac OS が搭載されたエンドポイントのハードウェア インベントリの詳細が表示されます。[エンドポイント使用率（Endpoint Utilizations）] ダッシュレットには、エンドポイントのCPU、メモリ、およびディスク使用率が表示されます。3 つのオプションのいずれかを選択すると、利用率をパーセンテージで表示できます。

- [CPU 使用率が n% を超えるデバイス（Devices With Over n% CPU Usage）]
- [メモリ使用率が n% を超えるデバイス（Devices With Over n% Memory Usage）]
- [ディスク使用率が n% を超えるデバイス（Devices With Over n% Disk Usage）]

（注） ハードウェア インベントリ データは、ISE GUI に表示されるまでに 120 秒かかります。ハードウェア インベントリ データは、ポスチャ準拠および非準拠の状態について収集されます。

（注）

- [ハードウェアの可視性（Hardware Visibility）] ページのクイック フィルタには、3 文字以上入力する必要があります。クイック フィルタを効率的に機能させるには、文字の入力後に他のカラム属性のフィルタをクリックする方法もあります。
- 次の表はハードウェアに関連した属性に基づいたフィルタリングにのみ使用されるため、一部のカラム属性はグレー表示されています。
- オペレーティング システムのフィルタは、[製造元（Manufacturers）] チャートにのみ適用されます。これは、次の表には関連しません。

エンドポイントとその接続された外部デバイスのハードウェア属性は表形式で表示されます。次のハードウェア属性が表示されます。

- MAC アドレス
- BIOS 製造元
- BIOS シリアル番号
- BIOS モデル
- 接続デバイス
- CPU 名
- CPU 速度（GHz）
- CPU 使用率（%）
- コア数
- プロセッサ数
- メモリ サイズ（GB）
- メモリ使用率（%）
- 内部ディスクの合計サイズ（GB）
- 内部ディスクの合計フリー サイズ（GB）
- 内部ディスクの合計使用率（%）
- 内部ディスク数
- NAD ポート ID
- ステータス
- ネットワークデバイス名
- 参照先

- UDID
- IPv4 アドレス
- ユーザー名
- ホストネーム
- OS タイプ
- 異常な動作
- エンドポイント プロファイル
- 説明
- エンドポイント タイプ
- ID グループ
- 登録日
- ID ストア
- 許可プロファイル

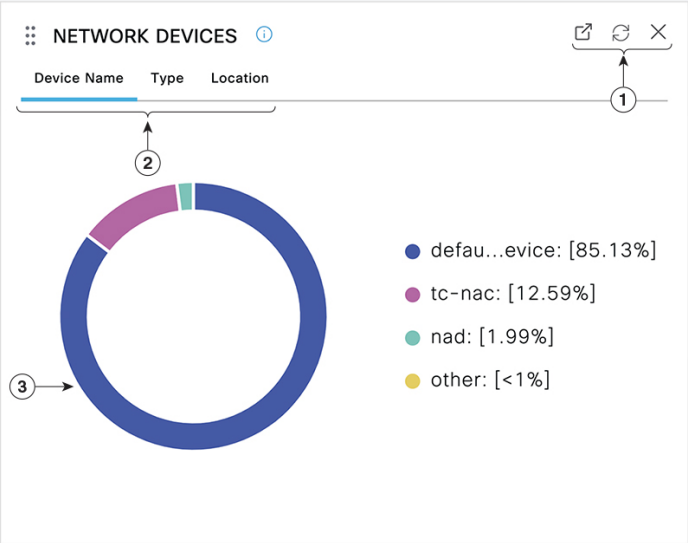
エンドポイントに対応する [接続デバイス（Attached Devices）] 列の番号をクリックすると、現在エンドポイントに接続されている USB デバイスの名前、カテゴリ、製造元、タイプ、製品 ID、およびベンダー ID を表示できます。

（注） Cisco ISE はクライアントのシステムのハードウェア属性をプロファイリングしますが、Cisco ISE がプロファイリングしないハードウェア属性がいくつか存在することがあります。これらのハードウェア属性は、[ハードウェア コンテキストの可視性（Hardware Context Visibility）] ページに表示されないことがあります。

ハードウェア インベントリ データの収集間隔は、**[管理（Administration）]** > **[システム（System）]** > **[設定（Settings）]** > **[ポスチャ（Posture）]** > **[全般設定（General Settings）]** ページで制御できます。デフォルトの間隔は 5 分です。

ダッシュレット

次のイメージは、ダッシュレットの例です。



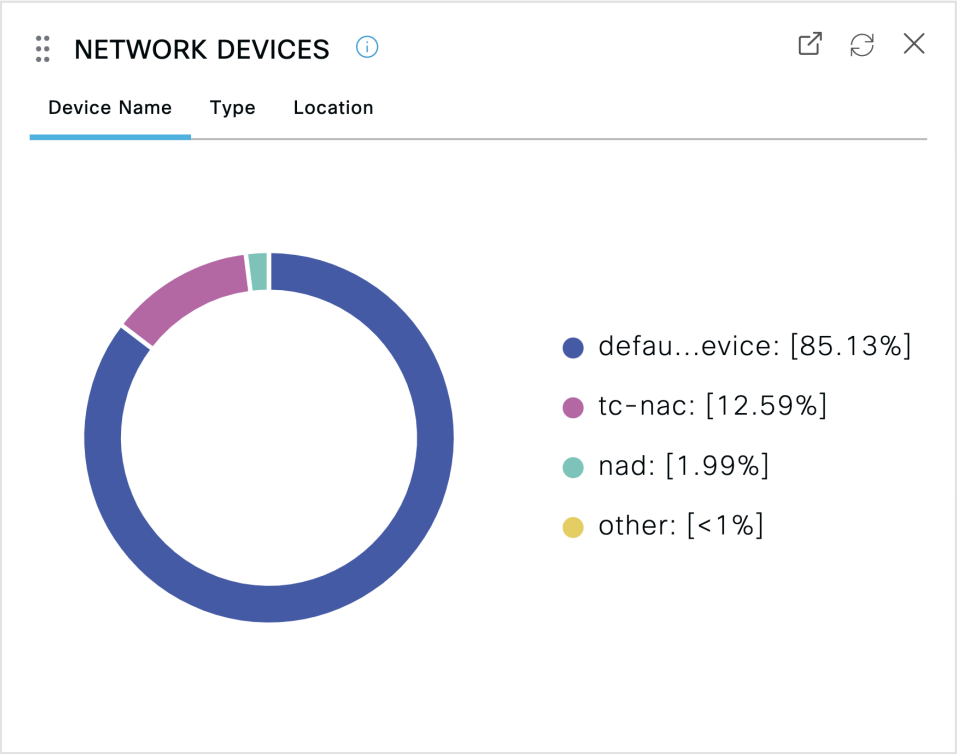
1. つまり、[新しいウィンドウを開く（Open New Window）] アイコンにより、新しいブラウザウィンドウでこのダッシュレットを開きます。円グラフが更新されます。このダッシュレットを削除するには、[X] をクリックします。このオプションは、ホームページでのみ使用できます。[コンテキストの可視性（Context Visibility）] ウィンドウでダッシュレットを削除するには、画面右上隅にある歯車のシンボルを使用します。
2. 一部のダッシュレットには異なるカテゴリのデータが表示されます。カテゴリをクリックすると、そのデータセットの円グラフが表示されます。
3. 円グラフには、選択したデータが表示されます。円グラフの 1 つのセグメントをクリックすると、新しいタブが開き、その円グラフセグメントに基づいてフィルタリングされたデータが表示されます。

ホームページダッシュボードの円グラフのセクションをクリックすると、新しいブラウザウィンドウでグラフを開きます。新しいウィンドウには、クリックした円グラフのセクションでフィルタリングされたデータが表示されます。

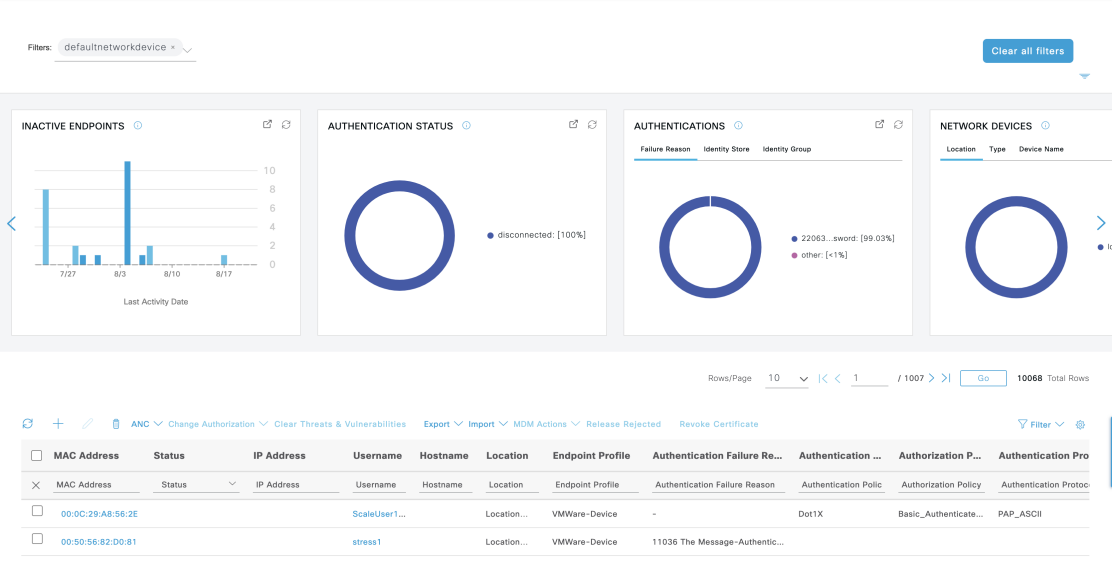
[コンテキストの可視性（Context Visibility）] ウィンドウで円グラフのセクションをクリックすると、表示されるデータはフィルタリングされますが、コンテキストは変更されません。フィルタリングされたデータは、同じブラウザウィンドウで表示されます。

ビューに表示するデータのフィルタリング

[コンテキストの可視性（Context Visibility）] ウィンドウでダッシュレットをクリックすると、対応するデータがクリックした項目でフィルタ処理されて表示されます。たとえば、円グラフのセクションをクリックすると、選択したセクションのデータがフィルタ処理されて表示されます。



[ネットワークデバイス（Network Devices）] ダッシュレットで **defau...evice** をクリックすると、次のイメージに示すように、新しいウィンドウにデータが表示されます。



円グラフのその他のセクションをクリックして、データをさらにフィルタ処理します。[フィルタ（Filter）] ドロップダウンリストまたはデータのリストの右上隅にある歯車アイコンを使用して、表示されるデータを管理することもできます。

カスタムフィルタを保存します。

カスタム フィルタの作成

自分だけがアクセスできるユーザー固有のカスタムフィルタを作成して保存します。Cisco ISE にログインしている他のユーザーは、作成したカスタムフィルタを表示できません。これらのカスタムフィルタは Cisco ISE データベースに保存されます。Cisco ISE にログインしているコンピュータやブラウザからアクセスできます。

ステップ 1 **[フィルタ（Filter）]**をクリックし、ドロップダウンリストから [拡張フィルタ（Advanced Filter）] を選択します。

ステップ 2 [フィルタ（Filter）] メニューからフィールド、演算子、値などの検索属性を指定します。

ステップ 3 [+] をクリックして、その他の条件を追加します。

ステップ 4 [実行（Go）] をクリックして、指定された属性に一致するエントリを表示します。

ステップ 5 **[保存 (Save)]** をクリックしてフィルタを保存します。

ステップ 6 名前を入力し、[Save（保存）] をクリックします。[フィルタ（Filter）] ドロップダウンリストにフィルタが表示されるようになりました。

拡張フィルタを使用した条件によるデータのフィルタリング

拡張フィルタを使用して、指定した条件（名 = Mike、ユーザー グループ = 従業員など）に基づいて情報をフィルタリングできます。複数の条件を指定できます。

ステップ 1 **[フィルタ（Filter）]**をクリックし、[拡張フィルタ（Advanced Filter）] を選択します。

ステップ 2 [フィルタ（Filter）] メニューから検索属性（フィールド、演算子、値など）を指定します。

ステップ 3 [+] をクリックして、その他の条件を追加します。

ステップ 4 [実行（Go）] をクリックして、指定した属性に一致するエントリを表示します。

クイックフィルタを使用したフィールド属性によるデータのフィルタリング

クイック フィルタを使用して、リストページに表示されるフィールド属性の値を入力し、ページをリフレッシュすることで、フィルタ基準に一致するレコードのみを一覧表示できます。

ステップ 1 **[フィルタ（Filter）]**をクリックし、ドロップダウンリストから [クィックフィルタ（Quick Filter）] を選択します。

ステップ 2 属性フィールドの 1 つ以上に検索条件を入力すると、指定した属性に一致するエントリが自動的に表示されます。

ダッシュレットビューでのエンドポイントアクション

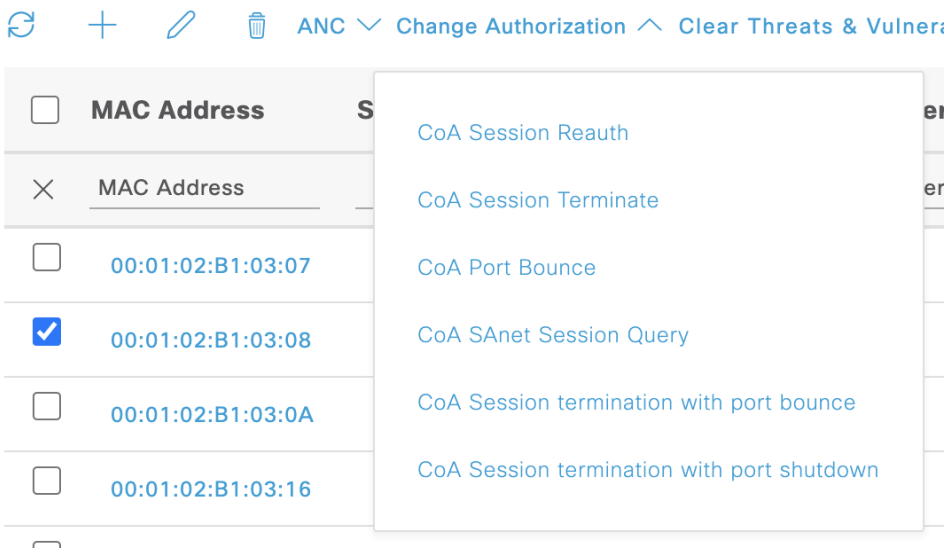
リストの上部にあるツールバーでは、選択したリスト内のエンドポイント上でアクションを実行できます。すべてのリストですべてのアクションが有効になっているわけではありません。使用可能になっている機能によってアクションは異なります。使用する前に Cisco ISE で有効にする必要がある 2 つのエンドポイントアクションを次のリストに示します。

- **適応型ネットワーク制御アクション**

  適応型ネットワーク制御を有効にした場合、リストでエンドポイントを選択して、ネットワークアクセスを割り当てたり、取り消したりできます。また、認可変更も発行できます。

  ホームページダッシュレットで円グラフをクリックすると、表示される新しいウィンドウに [ANC] オプション と[認可変更（Change Authorization）] オプションが表示されます。アクションを実行するエンドポイントのチェックボックスをオンにし、[ANC] ドロップダウンリストと [認可変更（Change Authorization）] ドロップダウンリストから必要なアクションを選択します。

  図 5: ダッシュレットビューでのエンドポイントアクション



- **MDM アクション**

  MDM サーバーを Cisco ISE に接続すると、選択したエンドポイントで MDM アクションを実行できます。[MDM アクション（MDM Actions）] ドロップダウンリストから必要なアクションを選択します。

Cisco ISE ダッシュボード

Cisco ISE のダッシュボードまたはホームページ（[メニュー（Menu）]アイコン（☰）をクリックし [ダッシュボード（Dashboard）] を選択）は、Cisco ISE 管理ポータルへのログイン後に表示されるランディングページです。ダッシュボードは、ウィンドウの上部に沿って表示されるメトリック メーターと下にあるダッシュレットで構成された、集中化された管理コンソールです。デフォルトのダッシュボードは、[概要（Summary）]、[エンドポイント（Endpoints）]、[ゲスト（Guests）]、[脆弱性（Vulnerability）]、[脅威（Threat）] です。Cisco ISE ホームのダッシュボード （6 ページ）を参照してください。

（注） Cisco ISE プライマリ PAN ポータルでのみ、このダッシュボードを表示できます。

ダッシュボードのリアルタイムデータによって、ネットワークにアクセスしているデバイスとユーザーを一目で確認できるステータスと、システムの正常性の概要が表示されます。

2 番目のレベルのメニューバーにある歯車アイコンをクリックして、ダッシュボード設定のドロップダウンリストを表示します。次の表では、ドロップダウンリストで使用可能なダッシュボード設定オプションについて説明します。

ドロップダウンリスト オプション	説明
新しいダッシュボードの追加（Add New Dashboard）	5つのデフォルトのダッシュボードを含めて、最大で 20 個のダッシュボードを設定できます。
ダッシュボードの名前の変更（Rename Dashboard）	（このオプションはカスタムダッシュボードでのみ使用可能）ダッシュボードの名前を変更するには、次の手順を実行します。 **1.** [ダッシュボードの名前の変更（Rename Dashboard）] をクリックします。 **2.** 新しい名前を指定します。 **3.** [適用（Apply）] をクリックします。

ドロップダウンリスト オプション	説明
ダッシュレットの追加（**Add Dashlet**）	ホームページダッシュボードにダッシュレットを追加するには、次の手順を実行します。 **1.** [ダッシュレットの追加（Add Dashlets）] をクリックします。 **2.** [ダッシュレットの追加（Add Dashlets）] ウィンドウで、追加するダッシュレットの横にある [追加（Add）] をクリックします。 **3.** [保存（Save）] をクリックします。 （注） ダッシュボードごとに最大で 9 個のダッシュレットを追加できます。

ドロップダウンリスト オプション	説明
エクスポート（**Export**）	ダッシュボードのデータは PDF または CSV ファイルとしてエクスポートできます。 **1.** [エクスポート（Export）] をクリックします。 **2.** [エクスポート（Export）] ダイアログボックスで、次のいずれかのファイル形式の横にあるオプションボタンをクリックします。 • [PDF]：選択したダッシュレットのスナップショットビューを表示するには、 PDF 形式を選択します。 • [CSV]：選択したダッシュボードのデータを zip ファイルとしてダウンロードするには、CSV 形式を選択します。 **3.** [エクスポート（Export）] ダイアログボックスで、エクスポートするダッシュレットの横にあるチェックボックスをオンにします。 **4.** [エクスポート（Export）] をクリックします。 zip ファイルには、選択したダッシュボードの個々のダッシュレット CSV ファイルが含まれています。ダッシュレットの各タブに関連するデータは、対応するダッシュレット CSV ファイルで個別のセクションとして示されます。 カスタムダッシュボードをエクスポートする場合、zip ファイルは同じ名前でエクスポートされます。たとえば、MyDashboard という名前のカスタムダッシュボードをエクスポートすると、エクスポートされたファイルの名前は MyDashboard.zip となります。

ドロップダウンリスト オプション	説明
レイアウト テンプレート（**Layout Template**）	ダッシュレットが表示されるテンプレートのレイアウトを変更できます。 レイアウトを変更するには、次の手順を実行します。 **1.** [レイアウトテンプレート（Layout Template）] をクリックします。 **2.** 使用可能なオプションから必要なレイアウトを選択します。
ダッシュボードの管理（**Manage Dashboards**）	[ダッシュボードの管理（Manage Dashboards）] をクリックし、次のいずれかのオプションを選択します。 • [デフォルトのダッシュボードにする（Mark as Default Dashboard）]：ダッシュボードをデフォルトのダッシュボード（ホームページ）として設定するには、このオプションを使用します。 • [すべてのダッシュボードのリセット（Reset all Dashboards）]：すべてのダッシュボードを元の設定にリセットするには、このオプションを使用します。

対応するカスタムダッシュボードの横にある閉じる（**x**）アイコンをクリックすることで、作成したダッシュボードを削除できます。

（注） デフォルト ダッシュボードの名前を変更したり、削除することはできません。

各ダッシュレットの右上隅には、次の操作を実行できるツールバーがあります。

- [分離（Detach）]：別のウィンドウにダッシュレットを表示します。
- [更新（Refresh）]：ダッシュレットを更新します。
- [削除（Remove）]：ダッシュボードからダッシュレットを削除します。

ダッシュレットの左上隅にあるグリッパ アイコンを使用して、ダッシュレットをドラッグ アンド ドロップできます。

[アラーム（Alarms）] ダッシュレットには、[重大度（Severity）] 列のクイックフィルタが含まれています。[重大度（Severity）] ドロップダウンリストから [クリティカル（Critical）]、[警

告（Warning）]、または [情報（Info）] を選択して、アラームを重大度でフィルタ処理できます。

Cisco ISE 国際化およびローカリゼーション

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

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

サポートされる言語

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

表 *3:* サポートされる言語とロケール

言語	ブラウザ ロケール
中国語（繁体字）	zh-tw
中国語（簡体字）	zh-cn
チェコ語	cs-cz
オランダ語	nl-nl
英語	en
フランス語	fr-fr
ドイツ語	de-de
ハンガリー語	hu-hu
イタリア語	it-it
日本語	ja-jp
韓国語	ko-kr
ポーランド語	pl-pl
ポルトガル語（ブラジル）	pt-br

言語	ブラウザ ロケール
ロシア語	ru-ru
スペイン語	es-es

エンドユーザー Web ポータルのローカリゼーション

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

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

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

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

UTF-8 文字データ エントリのサポート

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

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

UTF-8 クレデンシャル認証

ネットワーク アクセス認証では、UTF-8 ユーザー名およびパスワードのクレデンシャルがサポートされます。これには、RADIUS、Extensible Authentication Protocol（EAP）、RADIUS プロキシ、RADIUS トークン、ゲストおよび管理ポータルのログイン認証からの Web 認証が含

まれます。ユーザー名とパスワードの UTF-8 サポートは、ローカル ID ストアと外部 ID ストアを照合する認証に適用されます。

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

（注） RSA は UTF-8 ユーザーをサポートしていないため、RSA での UTF-8 認証はサポートされていません。Cisco ISE と互換性がある RSA サーバーも UTF-8 をサポートしていません。

UTF-8 ポリシーおよびポスチャ アセスメント

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

ポスチャ要件を、UTF-8 文字セットに基づくファイル、アプリケーション、およびサービス条件として変更します。

サプリカントに送信されるメッセージの UTF-8 サポート

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

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

レポートおよびアラートの UTF-8 サポート

モニターリングとトラブルシューティングのレポートおよびアラートでは、Cisco ISE でサポートされている言語について、次のように関連属性の UTF-8 の値がサポートされています。次のアクティビティがサポートされています。

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

ポータルでの UTF-8 文字のサポート

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

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

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

表 *4 :* 管理ポータルの *UTF-8* 文字フィールド

管理ポータルの要素	UTF-8 フィールド
ネットワーク アクセスのユーザー設定	• **[ユーザー名（Username）]** ユーザー名には、大文字と小文字、数字、スペース、特殊文字（`、%、^、;、:、[、{、|、}、]、\、‘、“、=、<、>、?、!、制御文字を除く）を組み合わせて使用できます。スペースのみのユーザー名は送信できません。 • **[名（First Name）]** • **[姓（Last Name）]** • E メール（Email）
ユーザー リスト	• すべてのフィルタフィールド。 • [ユーザーリスト（User List）] ウィンドウに表示される値。 • 左側のナビゲーション クイック ビューに表示される値

管理ポータルの要素	UTF-8 フィールド
ユーザー パスワード ポリシー	パスワードには、大文字と小文字、数字、特殊文字（「!」、@、#、$、^、&、*、（、および）の組み合わせを使用できます。[パスワード（Password）] フィールドでは、UTF-8 文字を含むあらゆる文字を使用できますが、制御文字は使用できません。 言語の中には大文字または小文字のアルファベットがないものがあります。ユーザーパスワード ポリシーでユーザーに大文字または小文字でパスワードを入力することを求め、ユーザーの言語がこれらの文字をサポートしていない場合、ユーザーはパスワードを設定できません。ユーザーパスワードフィールドで UTF-8 文字に対応するには、[ユーザーパスワードポリシー（User Password Policy）] ページ（[メニュー（Menu）] アイコンをクリックし、**[管理（Administration）] > [ID 管理（Identity Management）] > [設定（Settings）] > [ユーザー管理設定（User Authentication Settings）] > [パスワードポリシー（Password Policy）]**を選択）で次のチェックボックスをオフにします。 • **英文字の小文字** • **英文字の大文字** 辞書に載っている単語とその順序を逆にした文字列、またはその文字を他の文字に置き換えた文字列は使用できません。
管理者リスト	• すべてのフィルタフィールド。 • 管理者リストウィンドウに表示される値。 • 左側のナビゲーションクイックビューに表示される値。
管理者ログイン ページ	• **[ユーザー名（Username）]**
RSA	• メッセージ • プロンプト

管理ポータルの要素	UTF-8 フィールド
RADIUS トークン	• [認証（Authentication）] タブ > [プロンプト（Prompt）]
ポスチャ要件	• [名前（Name）] • [修復アクション（Remediation action）] > エージェント ユーザーに表示されるメッセージ • 要件リスト表示
ポスチャ条件	**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[条件（Conditions）]** > **[ポスチャ（Posture）]** ウィンドウの次のフィールドは次のとおりです。 • **[ファイル条件（File condition）]** > **[追加（Add）]** > **[ファイルパス（File path）]**の順に選択します。 • **[アプリケーション条件（Application Condition）]** > **[追加（Add）]** > **[プロセス名（Process Name）]**の順に選択します。 • **[サービス条件（Service condition）]** > **[追加（Add）]** > **[サービス名（Service name）]**の順に選択します。 • 条件リストが表示されます。
ゲストおよびデバイスの設定	• [スポンサー（Sponsor）] > [言語テンプレート（Language Template）]：サポートされているすべての言語、すべてのフィールド • [ゲスト（Guest）] > [言語テンプレート（Language Template）]：サポートされているすべての言語、すべてのフィールド • [デバイス（My Devices）] > [言語テンプレート（Language Template）]：サポートされているすべての言語、すべてのフィールド
システム設定	• [SMTP サーバー（SMTP Server）] > [デフォルトの電子メールアドレス（Default e-mail address）]

管理ポータルの要素	UTF-8 フィールド
[操作（Operations）]>[アラーム（Alarms）]>[ルール（Rule）]	• [基準（Criteria）] > [ユーザー（User）] • [通知（Notification）] > [電子メール通知ユーザー リスト（e-mail Notification user list）]
[操作（Operations）] > [レポート（Reports）]	• [操作（Operations）] > [ライブ認証（Live Authentications）] > [フィルタ（Filter）] フィールド • [操作（Operations）] > [レポート（Reports）]>[カタログ（Catalog）]>[レポートフィルタ（Report filter）] フィールド
[操作（Operations）]>[トラブルシューティング（Troubleshoot）]	• [一般ツール（General Tools）] > [RADIUS 認証トラブルシューティング（RADIUS Authentication Troubleshooting）] > [ユーザー名（Username）]
ポリシー	• [認証（Authentication）]>ポリシー条件内でのウィルス対策式の値 • [許可（Authorization）] または [ポスチャ（Posture）]、あるいは [クライアント プロビジョニング（Client Provisioning）]>[その他の条件（Other Conditions）]>ポリシー条件内でのウィルス対策式の値

管理ポータルの要素	UTF-8 フィールド
ポリシー ライブラリ条件の属性値	• [認証（Authentication）] > [単純条件/複合条件（Simple Condition/Compound Condition）] > ウィルス対策式の値 • [認証（Authentication）]> 単純条件リスト表示 • [認証（Authentication）]> 単純条件リスト > 左のナビゲーション クイック ビュー表示 • [許可（Authorization）] > [単純条件/複合条件（Simple Condition/Compound Condition）] > ウィルス対策式の値 • [許可（Authorization）] > 単純条件リスト > 左のナビゲーション クイック ビュー表示 • [ポスチャ（Posture）] > [ディクショナリ単純条件/ディクショナリ複合条件（Dictionary Simple Condition/Dictionary Compound Condition）] > ウィルス対策式の値 • [ゲスト（Guest）] > [単純条件/複合条件（Simple Condition/Compound Condition）] > ウィルス対策式の値

Cisco ISE ユーザーインターフェイス以外での UTF-8 サポート

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

デバッグ ログおよび CLI 関連の UTF-8 サポート

一部のデバッグ ログには、属性値とポスチャ条件の詳細が表示されます。すべてのデバッグログが UTF-8 値を受け入れます。raw UTF-8 データを含むデバッグログをダウンロードして、UTF-8 対応ビューアで表示できます。

Cisco Secure ACS 移行での UTF-8 サポート

Cisco ISE では、Cisco Secure Access Control Server（ACS）の UTF-8 設定のオブジェクトと値を移行できます。一部の UTF-8 オブジェクトの移行は、Cisco ISE UTF-8 言語でサポートされない場合があります。そのため、移行中に提供されるUTF-8データの一部は、管理ポータルまたはレポート方式を使用して読み取れない表示になる場合があります。（Cisco Secure ACS から

移行された）読み取り不能な UTF-8 値を ASCII テキストに変換します。Cisco Secure ACS から Cisco ISE への移行の詳細については、お使いの ISE バージョンの『Cisco Secure ACS to Cisco ISE Migration Tool』を参照してください。

UTF-8 の値のインポートおよびエクスポートのサポート

管理ポータルとスポンサー ポータルは、ユーザー アカウントの詳細をインポートするときに使用される UTF-8 値のプレーンテキストファイルと CSV ファイルをサポートしています。エクスポートされたファイルは CSV ファイルとして提供されます。

REST での UTF-8 サポート

External Representational State Transfer（REST）通信は、UTF-8 値をサポートします。これは、管理者認証を除き、Cisco ISE ユーザーインターフェイスの UTF-8 がサポートされる設定可能項目に適用されます。REST での管理者認証には、ログインのために ASCII テキストクレデンシャルが必要です。

ID ストアの許可データの UTF-8 サポート

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

MAC アドレスの正規化

Cisco ISE は次のいずれかの形式で入力した MAC アドレスの正規化をサポートしています。

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

Cisco ISE の次のウィンドウには、MAC アドレスが完全な状態で、または部分的に表示されます。

- **[ポリシー（Policy）]** > **[ポリシーセット（Policy Sets）]**の順に選択します。
- **[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[条件（Conditions）]** > [許可（Authorization）]
- [認証（Authentications）] > [フィルタ（Filters）]（エンドポイント カラムおよび ID カラム）
- グローバル検索
- **[操作（Operations）]** > **[レポート（Reports）]** > [レポートフィルタ（Reports Filters）]

- **[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）] > [エンドポイントデバッグ（Endpoint Debug）]**

次の Cisco ISE API ウィンドウには、完全な MAC アドレス（「:」または「-」、あるいは「.」で区切られた 6 オクテット）が表示されます。

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

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

オクテットの有効な範囲は、0 ー 9、a ー f、または A ー Fです。

Cisco ISE 展開のアップグレード

Cisco ISE では、管理ポータルから GUI ベースの一元化されたアップグレードが提供されます。アップグレードの進行状況とノードのステータスが Cisco ISE の GUI に表示されます。実行する必要があるアップグレード前およびアップグレード後のタスクについては、アップグレード先の Cisco ISE リリースの『*Cisco Identity Services Engine Upgrade Guide*』を参照してください。

アップグレードの [概要（Overview）] ウィンドウ（**[管理（Administration）] > [システム（System）] > [アップグレード（Upgrade）] > [概要（Overview）]**）には展開内のすべてのノード、それらのノードで有効になっているペルソナ、現在使用されている Cisco ISE のバージョン、および各ノードのステータス（そのノードがアクティブか非アクティブか）がリストされます。ノードが [アクティブ（Active）] な状態である場合にのみアップグレードを開始できます。

管理者アクセス コンソール

次の手順では、管理ポータルにログインする方法について説明します。

ステップ 1 Cisco ISE URL をブラウザのアドレス バーに入力します（たとえば https://<ise hostname or ip address>/admin/）。

ステップ 2 ユーザー名と、Cisco ISE の初期セットアップで指定して設定した大文字と小文字が区別されるパスワードを入力します。

ステップ 3 [ログイン（Login）] をクリックするか、Enter を押します。

ログインに失敗した場合は、[ログイン（Login）] ウィンドウの [ログインで問題が発生する場合（Problem logging in?）] リンクをクリックして、表示される手順に従ってください。

管理者ログイン ブラウザのサポート

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

- Mozilla Firefox 102 以前のバージョン（バージョン 82 以降）
- Mozilla Firefox ESR 91.3 以前のバージョン
- Google Chrome 103 以前のバージョン（バージョン 86 以降）
- Microsoft Edge の最新バージョンと最新バージョンより 1 つ前のバージョン

ISE コミュニティ リソース

ISE Pages Fail to Fully Load When Adblock Plus is Used

ログインの試行による管理者のロックアウト

管理者ユーザー ID に対して誤ったパスワードを何度も入力すると、アカウントは指定された時間一時停止されるか、またはロックアウトされます（設定による）。ユーザーをロックアウトするように Cisco ISE が設定されている場合、管理ポータルによってシステムからロックアウトされます。Cisco ISE は、サーバー管理者ログインレポートにログエントリを追加し、その管理者 ID のログイン情報を一時停止します。その管理者 ID のパスワードをリセットするには、『Cisco Identity Services Engine Installation Guide』の「Reset a Disabled Password Due to Administrator Lockout」のセクションでの説明に従います。管理者アカウントが無効になるまでに失敗できるログイン試行の回数は、『*Cisco Identity Services Engine Administrator Guide*』の「Cisco ISE への管理アクセス」のセクションに記載されているとおりに設定されます。管理者ユーザーアカウントがロックアウトされると、関連付けられたユーザーに Cisco ISE から電子メールが送信されます（この情報が設定されている場合）。

ネットワーク管理者の役割を持つ管理者（Microsoft Active Directory ユーザーを含む）のみが、管理者アクセスを無効にするオプションを設定できます。

Cisco ISE でのプロキシの設定

既存のネットワークトポロジで、Cisco ISE が外部リソース（クライアント プロビジョニングやポスチャ関連のリソースがあるリモートのダウンロードサイトなど）にアクセスできるよう

にするためにプロキシサーバーを使用する必要がある場合は、管理ポータルを使用してプロキシ設定を行います。

プロキシ設定は次の Cisco ISE 機能に影響します。

- パートナー モバイル管理
- エンドポイント プロファイラ フィード サービスの更新
- エンドポイント ポスチャの更新
- エンドポイント ポスチャ エージェント リソースのダウンロード
- 証明書失効リスト（CRL）のダウンロード
- ゲスト通知
- SMS メッセージの送信
- ソーシャル ログイン
- Microsoft Azure Active Directory
- pxGrid クラウド

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

ステップ 1 Cisco ISE の GUI で、[メニュー（Menu）] アイコン（☰）をクリックし、**[管理（Administration）] > [システム（System）] > [設定（Settings）] > [プロキシ（Proxy）]** を選択します。

ステップ 2 プロキシの IP アドレスまたは DNS 解決可能ホスト名を入力し、Cisco ISE との間のプロキシトラフィックを通過させるポートを [プロキシホストサーバー：ポート（Proxy host server : port）] フィールドに指定します。

ステップ 3 必要に応じて、[パスワード必須（Password required）] チェックボックスをオンにします。

ステップ 4 [ユーザー名（User Name）] フィールドと [パスワード（Password）] フィールドにプロキシサーバーへの認証に使用するユーザー名とパスワードを入力します。[パスワードの確認（Confirm Password）] フィールドにパスワードを再入力します。

ステップ 5 [次のホストとドメインに対するプロキシをバイパス（Bypass proxy for these hosts and domain）] テキストボックスに、バイパスする必要があるホストまたはドメインの IP アドレスまたはアドレス範囲を入力します。

ステップ 6 [保存（Save）] をクリックします。

管理ポータルで使用されるポート

管理ポータルは、HTTP ポート 80 と HTTPS ポート 443 を使用します。ユーザーはこれらの設定を変更できません。管理ポータルのリスクを軽減するために、これらのポートを使用するようにエンドユーザーポータルを設定することはできません。

Cisco ISE アプリケーション プログラミング インターフェイス ゲートウェイの設定

Cisco ISE の API ゲートウェイは、複数の Cisco ISE サービス API への単一のエントリポイントとして機能する API 管理ソリューションであり、セキュリティとトラフィック管理を向上させます。外部クライアントからの API 要求は、Cisco ISE の API ゲートウェイにルーティングされます。内部アルゴリズムに基づいて、サービス API が実行されている Cisco ISE ノードに要求が転送されます。

Cisco ISE リリース 3.1 以降、MnT（モニターリング）API、ERS API、およびオープン API はすべて API ゲートウェイを介してルーティングされます。API ゲートウェイノードと、それぞれの API の展開内の他のすべてのノード間で、次のポートを開く必要があります。

- MnT API：9443
- オープン API：9070
- ERS API：9060

API ゲートウェイを有効にする Cisco ISE ノードを選択できます。Cisco ISE 展開では、2 つ以上のノードで API ゲートウェイを実行することを推奨します。

ERS およびオープン API サービスが該当ノードで無効になっている場合でも、API ゲートウェイは常にスタンドアロンノードで有効になります。分散展開の場合、API ゲートウェイが展開内の他のノードで有効になっていない場合に API ゲートウェイはデフォルトでプライマリ PAN で有効になります。

ステップ 1 プライマリ PAN にログインします。

ステップ 2 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[管理（Administration）] > [システム（System）] > [設定（Settings）] > [API 設定（API Settings）] > [AIP ゲートウェイ設定（API Gateway Settings）]**の順に選択します。

ステップ 3 [ISE API ゲートウェイノードリスト（ISE API Gateway Nodes List）] 領域で、API ゲートウェイを有効にするノードの横にあるチェックボックスをオンにします。

ステップ 4 [有効（Enable）] をクリックします。

トラブルシューティング

APIゲートウェイ関連の問題をトラブルシューティングするには、[デバッグログの設定（Debug Log Configuration）] ウィンドウで、次のコンポーネントの [ログレベル（Log Level）] を [デバッグ（DEBUG）] に設定します。（このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして、**[操作（Operations）] > [トラブルシューティング（Troubleshoot）] > [デバッグウィザード（Debug Wizard）] > [デバッグログの設定（Debug Log Configuration）]**の順に選択）。

- **ise-kong**
- **kong**

ログは、[ログのダウンロード（Download Logs）] ウィンドウからダウンロードできます（このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして、**[操作（Operations）]>[トラブルシューティング（Troubleshoot）]>[ログのダウンロード（Download Logs）]**の順に選択）。[サポートバンドル（Support Bundle）] タブからサポートバンドルをダウンロード（タブの [ダウンロード（Download）] ボタンをクリック）するか、または [デバッグログ（Debug Logs）] タブから kong デバッグログをダウンロードします（**kong** デバッグログの [ログファイル（Log File）] の値をクリック）。

確認

Cisco ISE プライマリ PAN に毎回正常にログインできる場合は、API ゲートウェイの設定は想定どおりに機能しています。

（注） GUI にログインしている同じ Web ブラウザの別のタブにある API ゲートウェイを介して REST API にアクセスすると、GUI からログアウトします。

これは、API が API ゲートウェイノード以外のリモートノードによって提供されている場合にのみ発生します。

Cisco ISE 3.0 以降、ポート 443 の UI サービスは Docker サービスを介して提供されるため、複数のネットワークインターフェイスコントローラ（NIC）シナリオを含む場合に動作が変更される可能性があります。管理シェルから **ip route** コマンドを使用して、特定のニーズに基づいて目的のインターフェイスまたはゲートウェイを介してパケットがルーティングされるように、ルートを調整する必要がある場合があります。**ip route** コマンドの詳細については、『Cisco ISE CLI Reference Guide』の「*Cisco ISE CLI Commands in Configuration Mode*」の章を参照してください。

API サービスの有効化

Cisco ISE API サービスは、Cisco ISE 環境で Web アプリケーションを開発および展開するためのフレームワークを提供します。この機能は REST API をドキュメント化します。REST API を使用すると、さまざまな言語でコードを生成したり、API を理解するためにユーザー間でコードを共有したりできます。Cisco ISE API サービスは、REST API を記述するために業界で広く受け入れられている OpenAPI 仕様に基づいています。

API サービスにアクセスするには、API ゲートウェイを有効にする必要があります。すべての API サービス要求は、Cisco ISE のスタンドアロンと分散型の両方の展開で API ゲートウェイを介して Cisco ISE に入ります。API ゲートウェイは、ポート 443 を介して API サービス要求を受信します。

スタンドアロンの Cisco ISE ノードでは、API 要求を受信した後、API ゲートウェイは API サービスに要求を転送します。

分散環境では、読み取り要求は PSN またはプライマリ PAN のいずれかに転送されますが、書き込み要求はプライマリ PAN にのみ転送されます。プライマリ PAN は、展開環境で書き込み権限を持つ唯一のノードです。

Cisco ISE では、次の 2 種類の API 形式を使用して Cisco ISE ノードを管理するための API アクセスが可能です。

- **外部 RESTful サービス API**

  外部 RESTful サービス（ERS）API は、標準 HTTPS ポート 443（ポート 9060 も使用できます）で動作する HTTPS プロトコルに基づく REST API です。ERS API は基本認証をサポートしています。認証クレデンシャルは、暗号化され、要求ヘッダーの一部となっています。JAVA、cURL Linux コマンド、Python などの REST クライアントやその他のクライアントを使用して、外部 RESTful サービス API コールを呼び出すことができます。

（注）

- ERS API は TLS 1.1 および TLS 1.2 をサポートしていますが、[セキュリティ設定（Security Settings）] ウィンドウ（**[管理（Administration）] > [システム（System）] > [設定（Settings）] > [セキュリティ設定（Security Settings）]**）で TLS 1.0 を有効にした場合でも、TLS 1.0 をサポートしません。[セキュリティ設定（Security Settings）] ウィンドウで TLS 1.0 を有効にしても、EAP プロトコルのみに関係し、ERS API には影響しません。
- ERS セッションのアイドルタイムアウトは 60 秒です。この期間中に複数の要求が送信された場合、同じクロスサイトリクエスト フォージェリ（CSRF）トークンで同じセッションが使用されます。セッションがアイドル状態になっている時間が 60 秒を超えると、そのセッションはリセットされ、新しい CSRF トークンが使用されます。

ERS API の SDK 定義については、https://<*ise-ip*>:9060/ers/sdk または https://<ise-ip>/ers/sdk にアクセスしてください。この情報は、**[API設定（API Settings）]** ウィンドウ（**[管理（Administration）] > [システム（System）] > [設定（Settings）] > [API設定（API Settings）] > [概要（Overview）]**）の **[概要（Overview）]** セクションにもあります。

Cisco ISE の Amazon マシンイメージ（AMI）バージョンが VMware クラウド環境に展開されている場合、ERS サービスはデフォルトで有効になっています。これにより、Cisco ISE

GUI から ERS サービスを有効にすることなく、Cisco ISE と他のシスコ製品およびサードパーティ製アプリケーションを簡単に統合できます。

（注） ユーザーデータの取得は、メタデータバージョン V1（IMDSv1）でのみ機能し、V2 では機能しません。

ERS の Open API 仕様

ERS API の Open API 仕様（JSON ファイル）は、Cisco ISE の **[API設定（API Settings）]** ウィンドウの **[概要（Overview）]** セクションでダウンロードできます（**[管理（Administration）]** > **[システム（System）]** > **[設定（Settings）]** > **[API設定（API Settings）]** > **[概要（Overview）]**）。この Open API JSON ファイルは、Python、JAVA などのプログラミング言語を使用した API クライアントコードの自動生成に使用できます。Open API の仕様とツールの詳細については、https://openapi.tools/ を参照してください。

- **オープン API**

  オープン API は、ポート 443 で動作する HTTPS に基づく REST API です。Cisco ISE リリース 3.1 では、新しい API をオープン API 形式で使用できます。Cisco ISE オープン API の詳細については、https://<*ise-ip*>/api/swagger-ui/index.html または Cisco ISE Open API にアクセスしてください。

  Cisco ISE リリース 3.1 では、次の Open API が導入されています。

  - リポジトリ：これらの API は、リポジトリを管理する機能を提供します。リポジトリ設定を作成、取得、更新、および削除し、設定されたリポジトリからファイルを一覧表示できます。
  - **バックアップと復元**：これらの API は、バックアップと復元の操作を管理する機能を提供します。設定のバックアップを作成、キャンセル、更新、および復元できます。また最後のバックアップのステータスを一覧表示できます。ユーザーはバックアップスケジュールを作成および編集することもできます。
  - **証明書**：これらの API は、証明書を管理する機能を提供します。システム証明書と信頼できる証明書の作成、取得、更新、削除、証明書署名要求（CSR）の作成、および証明書のエクスポートとインポートが可能です。自己署名証明書 API の生成は、Cisco ISE リリース 3.1 パッチ 1 以降で使用できます。
  - ポリシー：これらの API は、ポリシーを管理する機能を提供します。次の 2 つのタイプがあります。
    - RADIUS ポリシー：これらの API は、RADIUS ポリシーを管理する機能を提供します。必要なすべての境界（認証プロファイル、SecurityGroup、IdentityStore、プロファイル）とディスカバリ ディクショナリ フィルタ ヘルパーのリストを取得できます。これらの API により、ディクショナリと属性の管理、条件管理（ライブラリ、ネットワーク、時刻と日付の条件）、および AuthN ルール、Authz ルール、例外ルール、グローバル例外ルールを含むポリシーセットの管理が可能です。

- **TACACS+ ポリシー**：これらの API は、TACACS+ ポリシーを管理する機能を提供します。必要なすべての境界（コマンドセット、TACACS プロファイル、IdentityStore、ServiceName）のリストと、TACACS ヘルパーに関連するディクショナリのディスカバリを取得できます。これらの API により、条件管理（ライブラリ、ネットワーク、時刻と日付の条件）、および AuthN ルール、Authz ルール、例外ルール、グローバル例外ルールを含むポリシーセットの管理が可能です。

- TrustSec：これらの API は、仮想ネットワーク（VN）、セキュリティグループ - 仮想ネットワークマッピング（SG-VN マッピング）、VN-VLAN マッピングなどの TrustSec 関連の操作を管理します。
- タスクサービス：これらの API は、Cisco ISE で実行されるさまざまなタスクのステータスをモニターする機能を提供します。
- 展開：これらの API は、Cisco ISE ノードを設定し、展開を設定する機能を提供します。
- パッチおよびホットパッチ：これらの API は、パッチのインストール、パッチの削除、インストールされているすべてのパッチの一覧表示など、パッチ関連の操作を実行する機能を提供します。

（注） この API は、プライマリ PAN サービスが稼働している場合にのみ機能します。プライマリ PAN サービスがダウンしている場合、セカンダリ PAN の API コールは失敗します。

- ライセンス：これらの API は、スマートライセンスを登録、有効化、および管理する機能を提供します。
- **システム設定**：これらの API は、Cisco ISE でプロキシ設定とトランスポートゲートウェイ設定を構成および更新する機能を提供します。

（注） Cisco ISE クラウドの設定で、AWS クラウド内の API ドキュメントページにアクセスするには、iptables を使用してファイアウォールルールを開く必要があります。

（注） サブネットからの OpenAPI 要求に存在する IP アドレスは、そのネットワークからのリモート IP アドレスとして表示されることが予想されます。

API サービスで操作するユーザーに特別な権限を割り当てる必要があります。API サービスユーザーは、内部ユーザーか、または外部の Microsoft Active Directory グループに所属することができます。内部ユーザーまたは外部ユーザーが所属する Active Directory グループは [ERS 管理

者（ERS Admin）] または [ERS オペレータ（ERS Operator）] のグループのいずれかにマッピングする必要があります。

- [ERS 管理者（ERS Admin）]：これらのユーザーは外部 RESTful サービス API 要求を作成、読み取り、および削除できます。すべての外部 RESTful サービス API（GET、POST、DELETE、および PUT）へのフルアクセスを備えています。
- [ERS オペレータ（ERS Operator）]：これらのユーザーには読み取り専用アクセス（GET 要求のみ）があります。

（注） スーパー管理者ロールを持つユーザーは、すべての API サービスにアクセスできます。

デフォルトでは、API サービスは無効になっています。Cisco ISE で API サービスを有効にする前に API コールを呼び出すと、エラーメッセージが表示されます。Cisco ISE REST API 用に開発されたアプリケーションを Cisco ISE にアクセスできるようにするには、Cisco ISE REST API 機能を有効にします。ERS API は標準 HTTPS ポート 443（ポート 9060 も使用できます）を使用し、Open API は HTTPS ポート 9070 を使用します。これらのポートはどちらも、デフォルトで無効になっています。Cisco ISE 管理サーバーで API サービスが有効になっていない場合、クライアントアプリケーションはゲスト REST API 要求に対してサーバーからタイムアウトエラーを受信します。

ステップ 1 Cisco ISE の GUI で、[メニュー（Menu）] アイコン（☰）をクリックし、**[管理（Administration）] > [システム（System）] > [設定（Settings）] > [API設定（API Settings）] > [API サービス設定（API Service Settings）]** を選択します。

ステップ 2 [プライマリ管理ノードの API サービス設定（API Service Settings for Primary Administration Node）] 領域で、[ERS（読み取り/書き込み）（ERS (Read/Write)）] トグルボタンをクリックしてプライマリ管理ノード（PAN）の外部 RESTful サービスを有効にします。あるいは、[オープン API（Open API）] トグルボタンをクリックして PAN でオープン API サービスを有効にします。

ステップ 3 [他のすべてのノードの API サービス設定（API Service Settings for All Other Nodes）] 領域で、[ERS（読み取り）（ERS (Read)）] トグルボタンをクリックして他のすべてのノードで外部 RESTful サービスを有効します。あるいは、[OpenAPI（読み取り/書き込み）（OpenAPI (Read/Write)）] トグルボタンをクリックして他のすべてのノードでオープン API サービスを有効にします。

ステップ 4 [CSRF チェック（CSRF Check）] 領域で次のオプションのいずれかのオプションボタンをクリックします。

- [セキュリティの強化に CSRF チェックを使用する（Use CSRF Check for Enhanced Security）]：このオプションを有効にした場合、外部 RESTful サービスクライアントは GET 要求を送信して Cisco ISE から CSRF トークンを取得し、Cisco ISE に送信する要求内にその CSRF トークンを含める必要があります。その後、Cisco ISE は、外部 RESTful サービスクライアントから要求を受信したときに CSRF トークンを検証します。Cisco ISE は、トークンが有効な場合にのみ要求を処理します。このオプションは、Cisco ISE リリース 2.3 より前のリリースの外部 RESTful サービスクライアントには適用されません。

- [ERS 要求に対して CSRF を無効にする（Disable CSRF for ERS Request）]：このオプションを有効にすると、CSRF 検証は実行されません。このオプションは、Cisco ISE リリース 2.3 より前のリリースの外部 RESTful サービスクライアントに使用できます。

ステップ 5 [保存（Save）] をクリックします。

（注） Cisco ISE ノードが PAN に登録されると、OpenAPI はデフォルトで以前の有効な状態から無効になります。上記の手順に従って、Cisco ISE GUI で OpenAPI を再度有効にして、ゼロタッチ OpenAPI 展開を維持します。

Cisco ISE は、GET 操作と UPDATE 操作に異なる API を提供します。

[GET]：

- URL：https://<ise-node>/admin/API/apiService/get
- **応答**：{"id": "1234","papIsEnabled":false,"psnsIsEnabled":true}

UPDATE：

- URL：https://<ise-node>/admin/API/apiService/update
- **要求の本文**：{"papIsEnabled":false,"psnsIsEnabled":false}
- **応答**：{"id": "1234","papIsEnabled":false,"psnsIsEnabled":false}

トラブルシューティング

すべての REST 操作が監査され、ログがシステム ログに記録されます。オープン API に関連する問題をトラブルシューティングするには、[デバッグログの設定（Debug Log Configuration）] ウィンドウで **apiservice** コンポーネントの [ログレベル（Log Level）] を [デバッグ（DEBUG）] に設定します。ERS API 関連の問題をトラブルシューティングするには、[デバッグログの設定（Debug Log Configuration）] ウィンドウ（このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして、**[操作（Operations）] > [トラブルシューティング（Troubleshoot）] > [デバッグウィザード（Debug Wizard）] > [デバッグログの設定（Debug Log Configuration）]**）で ers コンポーネントの [ログレベル（Log Level）] を [デバッグ（DEBUG）] に設定します。

[ログのダウンロード（Download Logs）] ウィンドウ（このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして、**[操作（Operations）] > [トラブルシューティング（Troubleshoot）] > [ログのダウンロード（Download Logs）]**）からログをダウンロードできます。[サポートバンドル（Support Bundle）] タブからサポートバンドルをダウンロード（タブの [ダウンロード（Download）] ボタンをクリック）するか、または [デバッグログ（Debug Logs）] タブから **API サービス**のデバッグログをダウンロード（api-service デバッグログの [ログファイル（Log File）] の値をクリック）します。

確認

API サービス GUI ページ（https://<*iseip*>:<*port*>/api/swagger-ui/index.html または https://<*iseip*>/ers/sdk など）にアクセスできる場合、API サービスは期待どおりに動作しています。

関連トピック

外部 RESTful サービスソフトウェア開発キット （46 ページ）

API サービスの外部 Active Directory アクセスの有効化

ステップ 1 Cisco ISE の GUI で、[メニュー（Menu）] アイコン（☰）をクリックし、**[管理（Administration）] > [ID 管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [Active Directory]** を選択します。

ステップ 2 外部ユーザーが所属する Active Directory グループを外部 ID ソースとして追加します。

Active Directory グループを追加する方法については、外部 ID ソースとしての Active Directoryを参照してください。

ステップ 3 Active Directory からユーザーグループを追加します。

Active Directory ユーザーを追加する方法については、ユーザーの追加方法を参照してください。

ステップ 4 Cisco ISE の GUI で、[メニュー（Menu）] アイコン（☰）をクリックし、**[管理（Administration）] > [管理者アクセス（Admin Access）] > [認証（Authentication）] > [認証方式（Authentication Method）]** を選択します。

ステップ 5 [ID ソース（Identity Source）] ドロップダウンリストから [AD：<参加ポイント名>（AD:<Join Point Name>）] を選択します。

ステップ 6 [パスワードベース（Password Based）] または [クライアント証明書ベース（Client Certificate Based）] のいずれかの認証を対応するオプションボタンをクリックして選択します。

ステップ 7 **[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [管理者（Administrators）] > [管理者グループ（Admin Groups）]** を選択します。

ステップ 8 管理グループのリストから [ERS 管理者（ERS Admin）] グループまたは [ERS オペレータ（ERS Operator）] をクリックします。

ステップ 9 [追加（Add）] をクリックして外部グループをメンバーユーザーとして管理者グループに追加します。

ステップ 10 [保存（Save）] をクリックします。

（注） Cisco ISE リリース 3.1 では、Cisco ISE GUI（[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [認証（Authentication）]）で管理者アクセス用に外部 ID ストアが設定されている場合、内部管理者ユーザーに ERS 管理者ロールを割り当てることはできません。外部管理者ユーザーのみに ERS 管理者ロールを割り当てることができます。

外部 RESTful サービスソフトウェア開発キット

独自のツールを作成するには、外部 RESTful サービス（ERS）のソフトウェア開発キット（SDK）ページを使用できます。URL https://<ISE-ADMIN-NODE>:9060/ers/sdk で、外部 RESTful サービス SDK にアクセスできます。**[ERS管理者（ERS Admin）]** のロールを持つユーザーのみが、外部 RESTful サービス SDK にアクセスできます。

SDK は、次のコンポーネントで構成されています。

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

システム時刻とネットワークタイムプロトコルサーバー設定の指定

Cisco ISE では、NTP サーバーを 3 台まで設定することができます。正確な時刻を維持し、異なるタイムゾーンの間で時刻を同期するために NTP サーバーを使用します。また、Cisco ISE が認証済みの NTP サーバーのみを使用する必要があるかどうかを指定したり、そのために 1 つまたは複数の認証キーを入力することもできます。

すべての Cisco ISE ノードを協定世界時（UTC）のタイムゾーンに設定することを推奨します（特に Cisco ISE ノードが分散展開されてインストールされている場合）。この手順では、展開内のさまざまなノードからのレポートとログのタイムスタンプが常に同期されるようにします。

Cisco ISE は、NTP サーバーの公開キー認証をサポートしています。NTP バージョン 4 は対称キー暗号化を使用します。また、公開キー暗号化に基づく新しい Autokey セキュリティモデルも提供します。公開キー暗号化は、対称キー暗号化よりも安全であると見なされています。これは、セキュリティが各サーバーによって生成され、公開されないプライベート値に基づいているためです。Autokey セキュリティモデルでは、すべてのキー配布および管理機能には公開値のみが含まれているため、キーの配布と保管が大幅に簡素化されます。

コンフィギュレーション モードで Cisco ISE の CLI から NTP サーバーに Autokey セキュリティモデルを設定できます。敵味方識別（IFF）システムは最も広く採用されているシステムであるため、このシステムを使用することを推奨します。

始める前に

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

展開内にプライマリとセカンダリの両方のCisco ISEノードがある場合は、各ノードのユーザーインターフェイスにログインし、システム時刻とNetwork Time Protocol（NTP）サーバーの設定を行います。

ステップ1 Cisco ISEのGUIで[メニュー（Menu）]アイコン（☰）をクリックし、**[管理（Administration）]** > **[システム（System）]** > **[設定（Settings）]** > **[システム時刻（System Time）]** を選択します。

ステップ2 [NTPサーバーの設定（NTP Server Configuration）]領域で、NTPサーバーの一意のIPアドレス（IPv4またはIPv6または完全修飾ドメイン名（FQDN））を入力します。

ステップ3 （オプション）秘密キーを使用してNTPサーバーを認証する場合に、指定したサーバーのいずれかが認証キーによる認証を必要としている場合は、[NTP認証キー（NTP Authentication Keys）]タブをクリックし、1つ以上の認証キーを指定します。次の手順を実行します。

a) [追加（Add）]をクリックします。

b) [キーID（Key ID）]フィールドと[キー値（Key Value）]フィールドに必要な値を入力します。[HMAC]ドロップダウンリストから、必要なハッシュメッセージ認証コード（HMAC）値を選択します。[キーID（Key ID）]フィールドは1～65535の数値をサポートし、[キー値（Key Value）]フィールドは最大15文字の英数字をサポートします。

c) [OK]をクリックします。

d) [NTPサーバーの設定（NTP Server Configuration）]タブに戻ります。

ステップ4 （オプション）公開キー認証を使用してNTPサーバーを認証するには、CLIからCisco ISEにAutokeyセキュリティモデルを設定します。Cisco ISEのリリースについては、『Cisco Identity Services Engine CLIリファレンス』の **ntp server** コマンドと **crypto** コマンドを参照してください。

ステップ5 [保存（Save）]をクリックします。

（注） 3つ以上のNTPサーバーを使用すると、サーバーの1つに障害が発生した、または2つのサーバーが同期しない場合でも、ネットワーク全体での正確な時刻の同期を保証します。https://insights.sei.cmu.edu/blog/best-practices-for-ntp-services を参照してください。

システムの時間帯の変更

一度設定すると、管理ポータルからのタイムゾーンの編集はできません。タイムゾーン設定を変更するには、Cisco ISE CLIで次のコマンドを入力します。

clock timezone タイムゾーン

clock timezone コマンドの詳細については、『Cisco Identity Services Engine CLIリファレンスガイド』を参照してください。

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

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

通知をサポートするための SMTP サーバーの設定

次の目的で電子メール通知を送信できるように、Cisco ISE の SMTP サーバーを設定します。

- アラーム。
- スポンサーがログインクレデンシャルとパスワードのリセット手順に関する電子メール通知をゲストに送信する場合。
- ゲストが自身を正常に登録した後でログインクレデンシャルを自動的に受け取る場合と、ゲストアカウントが期限切れになる前にゲストに求められるアクション。

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

次の表に、電子メールを送信する分散 Cisco ISE 環境内のノードを示します。

表 *5:* 電子メールを送信する *Cisco ISE* ノード

電子メールの目的	電子メールを送信するノード
ゲストアクセスの有効期限	プライマリポリシー管理ノード（PAN）
アラーム	MnTモニターリングおよびトラブルシューティング ノード（MnT）
ゲストポータルとスポンサーポータルからのスポンサー通知とゲスト通知	ポリシーサービスモード（PSN）
パスワードの有効期限	プライマリ PAN

Simple Mail Transfer Protocol（SMTP）サーバーを設定するには、[メニュー（Menu）] アイコン（☰）をクリックし、**[管理（Administration）] > [システム（System）] > [設定（Settings）] > [SMTP サーバー（SMTP Server）]** の順に選択します。次のフィールドを設定します。

- [SMTP サーバーの設定（SMTP Server Settings）] 領域で、次の手順を実行します。
  - [SMTP サーバー（SMTP Server）]：アウトバウンド SMTP サーバーのホスト名を入力します。
  - [SMTPポート（SMTP Port）]：SMTP ポート番号を入力します。SMTP サーバーに接続するには、このポートが開かれている必要があります。
  - [接続タイムアウト（Connection Timeout）]：Cisco ISE が新しい接続を開始する前に SMTP サーバーへの接続を待機する最大時間を入力します。タイムアウト値は秒単位で設定します。
- セキュアな SMTP サーバーと通信するには、[暗号化設定（Encryption Settings）] で [TLS/SSL 暗号化を使用（Use TLS/SSL Encryption）] をオンにします。セキュアソケットレイヤ（SSL）を使用する場合は、SMTP サーバーのルート証明書を Cisco ISE の信頼できる証明書に追加します。
- [認証設定（Authentication Settings）] 領域で、[パスワード認証を使用する（Use Password Authentication）] チェックボックスをオンにして、SSL の代わりに認証にユーザー名とパスワードを使用します。

インタラクティブヘルプ

インタラクティブヘルプを使用すると、簡単にタスクを完了するためのヒントとステップバイステップのガイダンスが提供され、ユーザーは Cisco ISE で効果的に作業することができます。

この機能はデフォルトでイネーブルになっています。この機能を無効にするには、[メニュー（Menu）] アイコン（☰）をクリックし、**[管理（Administration）] > [システム（System）] > [設定（Settings）] > [インタラクティブヘルプ（Interactive Help）]** を選択し、[インタラクティブヘルプの有効化（Enable Interactive Help）] チェックボックスをオフにします。

[表示（Show）] ボタンをクリックして、[インタラクティブヘルプ（Interactive Help）] メニューを表示します。

Google Chrome シークレットウィンドウから Cisco ISE 管理者ポータルにアクセスする場合、[インタラクティブヘルプ（Interactive Help）] を表示してアクセスするには、サードパーティの Cookie を有効にする必要があります。「Third-party cookie controls in Incognito mode」を参照してください。

セキュアなロック解除クライアントメカニズムの有効化

セキュアなロック解除クライアントメカニズムは、Cisco ISE の CLI でルートシェルへのアクセスを一定期間にわたって提供します。セッションを終了するか、または閉じた場合、ルートアクセスも無効になります。

セキュアなロック解除機能は、同意トークンツールを使用して実装されます。同意トークンは、お客様とシスコの両方からの相互の同意が得られた後でのみ、信頼できる方法でシスコ製品の特権アクセスを安全に付与するための統一された多要素認証方式です。

Cisco ISE CLI でルートシェルを有効にするには、次の手順を実行します。

ステップ 1 Cisco ISE CLI で、**permit rootaccess** と入力します。

```
ise/admin# permit rootaccess
1. Generate Challenge Token Request
2. Enter Challenge Response for Root Access
3. Show History
4. Exit
Enter CLI Option:
```

ステップ 2 オプション **1** を選択して、同意トークンチャレンジを生成します。

```
1. Generate Challenge Token Request
2. Enter Challenge Response for Root Access
3. Show History
4. Exit
Enter CLI Option:
1
Generating Challenge.....................................
Challenge String (Please copy everything between the asterisk lines exclusively):
********************************************************************************
GlOX7gAAQEAAQAAAEAgAEAAAAAMACmIxgb0hitBAQLUwvXeD3pnJ4HnJy30MQAEAAADhAGAAUUUHAAZUUVMQlQIAANUUUAPCcJIDL2NQDNjgwLIFm2mEtOWI0ZS0wZjY1ITdlZDlMQ1M2L2NQo=
********************************************************************************
Starting background timer of 15mins
1. Generate Challenge Token Request
2. Enter Challenge Response for Root Access
3. Show History
4. Exit
Enter CLI Option:
```

ステップ 3 同意トークンチャレンジを Cisco テクニカル アシスタンス センター（TAC）に送信します。

Cisco TAC は、送信される同意トークンチャレンジを使用して同意トークン応答を生成します。

ステップ 4 オプション **2** を選択してから、Cisco TAC により提供された同意トークン応答を入力します。

```
Enter CLI Option:
2
Please input the response when you are ready .....................
[redacted]
Response Signature Verified successfully !
Granting shell access
sh-4.2# ls
```

（注） 応答の署名の検証が成功すると、特権アクセスが有効になります。

次のタスク

シェルモードを終了するには、**exit** コマンドを実行します。

```
sh-4.2# exit
exit
Root shell exited
```

オプション **3** を選択して、ルートアクセスセッションの履歴を表示します。

```
1. Generate Challenge Token Request
2. Enter Challenge Response for Root Access
3. Show History
4. Exit
Enter CLI Option:
3
**********************************
        SN No : 1
**********************************
Challenge
3[redacted]=
 generated at 2019-06-12 15:40:01.000
**********************************
        SN No : 2
**********************************
```

連邦情報処理標準モードのサポート

Cisco ISE は、組み込みの連邦情報処理標準（FIPS）140-2 検証済み暗号化モジュール、Cisco Common Cryptographic Module（証明書 #1643 および証明書 #2100）を使用します。FIPS 準拠要求の詳細については、『FIPS Compliance Letter』を参照してください。

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

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

Cisco ISE にインストールされている証明書で使用されている暗号アルゴリズムまたはそのパラメータが FIPS でサポートされていない場合には、証明書を再発行する必要があります。

FIPS モードを有効にすると、次の機能が影響を受けます。

- SSL を介した Lightweight Directory Access Protocol（LDAP）

Cisco ISE による FIPS 140-2 準拠の有効化の手段として、RADIUS の共有秘密とキー管理が使用されます。FIPS モードが有効になると、FIPS 非準拠アルゴリズムを使用するすべての機能は失敗します。

FIPS モードを有効にする場合：

- EAP-TLS、PEAP、TEAP、EAP-TTLS および EAP-FAST ですべての FIPS 非準拠暗号スイートは無効になります。
- SSH ですべての FIPS 非準拠暗号スイートは無効になります。
- 証明書と秘密キーには、FIPS 準拠ハッシュと暗号化アルゴリズムのみを使用する必要があります。
- RSA 秘密キーには、2048 ビット以上を指定する必要があります。
- ECDSA 秘密キーには、224 ビット以上を指定する必要があります。
- ECDSA サーバー証明書は TLS 1.2 のみで機能します。
- DHE 暗号は、すべての ISE TLS クライアントの DH パラメータが 2048 ビット以上の場合に機能します。
- 3DES 暗号は、サーバーとして機能する Cisco ISE に使用できません。
- SHA-1 は証明書の生成に使用できません。
- SHA-1 はクライアント証明書で使用できません。
- EAP-FAST の匿名 PAC プロビジョニングオプションは無効です。
- ローカル SSH サーバーは FIPS モードで動作します。
- RADIUS は次のプロトコルをサポートしていません。
  - EAP-MD5
  - PAP
  - CHAP
  - MS-CHAPv1
  - MS-CHAPv2
  - LEAP

FIPS モードを有効にすると、展開内のすべてのノードが自動的に再起動されます。Cisco ISE はローリング再起動を実行します。具体的には、最初にプライマリ PAN を再起動し、その後でセカンダリノードを 1 つずつ再起動します。そのため、設定を変更する前にダウンタイムを計画することをお勧めします。

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

Cisco ISE での連邦情報処理標準モードの有効化

Cisco ISE で FIPS モードを有効化するには、次の手順に従います。

ステップ 1 Cisco ISE GUI で、[メニュー（Menu）] アイコン（☰）をクリックし、**[管理（Administration）] > [システム（System）] > [設定（Settings）] > [FIPSモード（FIPS Mode]** の順に選択します。

ステップ 2 [FIPSモード（FIPS Mode）] ドロップダウンリストから [有効（Enabled）] を選択します。

ステップ 3 [保存（Save）] をクリックして、マシンを再起動します。

次のタスク

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

- 自己署名証明書の生成 （81 ページ）。
- 証明書署名要求の作成と認証局への送信 （106 ページ）。
- ネットワーク デバイス定義の設定に記載されているとおり、RADIUS認証を設定します。

共通アクセスカード機能を使用して管理者アカウントの許可を有効にすることができます。許可のために共通アクセスカード機能を使用することは、厳密にはFIPS 140の要件ではありませんが、セキュアアクセスの手法としてよく知られており、複数の環境でFIPS 140準拠を強化するために使用されています。

管理者共通アクセスカード認証用の Cisco ISE の設定

始める前に

- （オプション）Cisco ISE で FIPS モードを有効にします。FIPS モードは証明書ベースの認証には必要ありませんが、この2つのセキュリティ手段は多くの場合、組み合わせて使用されます。Cisco ISE を FIPS 140 準拠の環境に展開し、共通アクセスカード証明書ベースの認証を使用する予定の場合は、FIPS モードを有効にし、適切な秘密キーと暗号化/復号化設定を最初に指定します。
- Cisco ISE のドメイン ネーム サーバー（DNS）が Active Directory に設定されていることを確認します。
- Active Directory のユーザーとユーザー グループ メンバーシップが、管理者証明書ごとに定義されていることを確認します。

Cisco ISE による管理者の認証と許可を、ブラウザから送信された共通アクセスカードベースのクライアント証明書に基づいてできるようにします。これには、次を設定します。

- 外部 ID ソース（次の例では Active Directory）
- 管理者が所属する Active Directory のユーザーグループ

- ユーザーの ID を証明書の中で見つける方法
- Active Directory ユーザーグループから Cisco ISE RBAC 権限へのマッピング
- クライアント証明書に署名する認証局（信頼）証明書
- クライアント証明書が CA によって失効させられたかどうかを判断する方法

Cisco ISE にログインする場合、クレデンシャルを認証するために 共通アクセスカードを使用できます。

ステップ 1 FIPS モードを有効にすると、システムの再起動が求められます。認証局証明書もインポートする場合は、再起動を遅らせることができます。

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

ステップ 3 ガイドラインに従って証明書認証プロファイルを設定します。

[プリンシパル名 X.509 属性（Principal Name X.509 Attribute）] フィールドでは、証明書内で管理者ユーザー名が格納されている属性を選択します。共通アクセスカードの場合は、カード上の署名証明書が通常は Active Directory でのユーザーの検索に使用されます。プリンシパル名は、この証明書の [サブジェクトの代替名（Subject Alternative Name）] 拡張情報（具体的には、この拡張情報の [別の名前（Other Name）] フィールド）にあります。したがって、ここでは、属性として [サブジェクト代替名：別の名前（Subject Alternative Name - Other Name）] を選択します。

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

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

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

ステップ 5 外部管理者グループを作成して、Active Directory グループにマッピングします。Cisco ISE の GUI で、[メニュー（Menu）] アイコン（☰）をクリックし、**[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [管理者（Administrators）] > [管理者グループ（Admin Groups）]** の順に選択します。外部システム管理者グループを作成します。

ステップ 6 外部管理者グループに RBAC 権限を割り当てる管理者認証ポリシーを設定します。

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

ステップ 7 認証局証明書を Cisco ISE の信頼できる証明書ストアにインポートするには、**[管理（Administration）]** > **[システム（System）]** > **[証明書（Certificates）]** > **[証明書ストア（Certificate Store）]** > **[信頼できる証明書（Trusted Certificates）]** の順に選択します。

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

a) [インポート（Import）] をクリックし、[証明書ファイル（Certificate File）] 領域で [ファイルの選択（Choose File）] をクリックします。
b) [クライアント認証を信頼（Trust for client authentication）] と [Syslog（syslog）] チェックボックスをオンにします。
c) [送信（Submit）] をクリックします。

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

ステップ 8 失効ステータス確認のための認証局証明書を設定します。

a) **[管理（Administration）]** > **[システム（System ）]** > **[証明書（Certificates）]** > **[OSCP クライアントプロファイル（OSCP Client Profile）]** の順に選択します。
b) [追加（Add）] をクリックします。
c) 対応するフィールドに OSCP サーバーの名前、説明（任意）、サーバーの URL を入力します。
d) **[管理（Administration）]** > **[システム（System）]** > **[証明書（Certificates）]** > **[証明書ストア（Certificate Store）]** の順に選択します。
e) クライアント証明書に署名できる認証局証明書のそれぞれについて、その認証局の失効ステータスチェックを行う方法を指定します。リストから認証局証明書を選択して [編集（Edit）] をクリックします。[編集（Edit）] ページで、OCSP または証明書失効リスト（CRL）検証、あるいはその両方を選択します。OCSP を選択した場合は、認証局に使用する OCSP サービスを選択します。CRL を選択した場合は、CRL Distribution URL などの設定パラメータを指定します。

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

a) [認証方式（Authentication Method）] タブで、[クライアント証明書ベース（Client Certificate Based）] オプションボタンを選択します。
b) [証明書認証プロファイル（Certificate Authentication Profile）] ドロップダウンリストから、以前に設定した証明書認証プロファイルを選択します。
c) [ID ソース（Identity Source）] から Active Directory インスタンス名を選択します。
d) [保存（Save）] をクリックします。

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

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

サポートされる共通アクセス カード標準

Cisco ISE は、共通アクセスカード認証デバイスを使用して自身を認証する米国政府ユーザーをサポートします。共通アクセスカードは特定の従業員を識別する一連の X.509 クライアント証明書を含む電子チップの認識票です。共通アクセスカードによるアクセスには、カードを挿入し PIN を入力するカードリーダーが必要です。カードからの証明書が Windows の証明書ストアに転送されます。Windows の証明書ストアは、Cisco ISE などのローカル ブラウザで実行されているアプリケーションで使用可能です。

Cisco ISE での共通アクセス カードの動作

Cisco ISE 認証がクライアント証明書を介してのみ行われるように、管理ポータルを設定できます。ユーザー ID またはパスワードを必要とするクレデンシャルベースの認証は許可されません。クライアント証明書ベースの認証では、共通アクセスカードを挿入して PIN を入力してから、ブラウザのアドレスフィールドに Cisco ISE 管理ポータルの URL を入力します。ブラウザによって証明書が Cisco ISE に転送され、Cisco ISE はログイン セッションを証明書の内容に基づいて認証および許可します。このプロセスが完了すると、[Cisco ISEモニターリングおよびトラブルシューティング（Cisco ISE Monitoring and Troubleshooting）] ホームページに表示され、ユーザーには適切な RBAC 権限が与えられます。

Diffie-Hellman アルゴリズムを使用したセキュアな SSH キー交換

Diffie-Hellman-Group14-SHA1 Secure Shell（SSH） キー交換のみを許可するように Cisco ISE を設定すします。Cisco ISE の CLI コンフィギュレーション モードから次のコマンドを入力します。

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

次に例を示します。

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

セキュア syslog 送信のための Cisco ISE の設定

始める前に

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

- 展開内のすべての Cisco ISE ノードに適切なサーバー証明書が設定されていることを確認します。FIPS 140 に準拠するように設定するには、証明書キーのキーサイズは 2048 ビット以上にする必要があります。
- 管理ポータルの FIPS モードを有効にします。
- デフォルト ネットワーク アクセス認証ポリシーが、あらゆるバージョンの SSL プロトコルを許可しないことを確認します。FIPS 認定アルゴリズムとともに、FIPS モードで TLS プロトコルを使用します。
- 展開内のすべてのノードがプライマリ PAN に登録されていることを確認します。また、展開の少なくとも 1 つのノードに、セキュア syslog レシーバ（TLS サーバー）としての動作が有効になっているモニターリングペルソナが含まれることも確認します。
- syslog でサポートされている RFC 標準規格を確認します。お使いのバージョンの Cisco ISE リリースの『Cisco Identity Services Engine ネットワークコンポーネントの互換性』ガイドを参照してください。

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

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

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

（注） UDP syslog を MnT ノードに配信するために Cisco ISE メッセージングサービスの使用を有効にした場合、Cisco ISE リリース 2.6 以降のリリースには、TLS 保護された UDP syslog が含まれます。参照先 Cisco ISE メッセージングサービスを介した syslog

セキュア syslog リモート ロギング ターゲットの設定

Cisco ISE システム ログは、さまざまな目的のために、ログ コレクタによって収集され保存されます。セキュアな syslog ターゲットを設定するには、モニターリングペルソナが有効になっている Cisco ISE ノードをログコレクタとして選択します。

ステップ 1 Cisco ISE 管理ポータルにログインします。

ステップ 2 Cisco ISE の GUI で、[メニュー（Menu）] アイコン（☰）をクリックして、**[管理（Administration）]** > **[システム（System）]** > **[ロギング（Logging）]** > **[リモート ロギング ターゲット（Remote Logging Targets）]** を選択します。

ステップ 3 [追加（Add）] をクリックします。

ステップ 4 セキュア syslog サーバーの名前を入力します。

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

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

ステップ 7 展開内の Cisco ISE モニターリングノードのホスト名と IP アドレスを [ホスト/IP アドレス（Host/IP Address）] フィールドに入力します。

ステップ 8 [ポート（Port）] フィールドに、ポート番号として *6514* を入力します。セキュア syslog レシーバは TCP ポート 6514 をリッスンします。

ステップ 9 [ファシリティコード（Facility Code）] ドロップダウンリストから syslog ファシリティコードを選択します。デフォルト値は [LOCAL6] です。

ステップ 10 対応する設定を有効にするには、次のチェックボックスをオンにします。

a) **[このターゲットのアラームを含める（Include Alarms For This Target）]**

b) **[RFC 3164 に準拠する（Comply to RFC 3164）]**

c) **[サーバー ID チェックを有効にする（Enable Server Identity Check）]**

ステップ 11 [サーバーダウンの場合はメッセージをバッファする（Buffer Messages When Server is Down）] チェックボックスをオンにします。このオプションがオンの場合、Cisco ISE は、セキュアな syslog レシーバが到達不能な場合にはログを格納し、セキュアな syslog レシーバを定期的に検査し、セキュア syslog レシーバが起動するとログを転送します。

a) [バッファサイズ（MB）（Buffer Size (MB)）] フィールドにバッファサイズを入力します。

b) Cisco ISE がセキュアな syslog レシーバを定期的に確認するように、[再接続時間（秒）（Reconnect Time (Sec)）] フィールドに再接続タイムアウト値を入力します。タイムアウト値は秒単位で設定します。

ステップ 12 [CA 証明書の選択（Select CA Certificate）] ドロップダウンリストから、Cisco ISE がセキュアな syslog サーバーに提示する必要がある CA 証明書を選択します。

ステップ 13 セキュアな syslog を設定するときに、[サーバー証明書の検証を無視（Ignore Server Certificate validation）] チェックボックスがオフになっていることを確認します。

ステップ 14 **[送信（Submit）]** をクリックします。

リモート ロギング ターゲットの設定

次の表では、外部の場所（syslog サーバー）を作成してロギングメッセージを保存するために使用する [リモートロギングターゲット（Remote Logging Targets）] ウィンドウのフィールドについて説明します。このウィンドウにアクセスするには、**[管理（Administration）]** > **[システム（System）]** > **[ロギング （Logging）]** > **[リモートロギングターゲット（Remote Logging Targets）]** を選択し、[追加（Add）] をクリックします。

表 *6:* リモート ロギング ターゲットの設定

フィールド名	使用上のガイドライン
名前（**Name**）	新しいsyslogターゲットの名前を入力します。
ターゲット タイプ（**Target Type**）	ドロップダウンリストから、該当するターゲットタイプを選択します。デフォルト値は [UDP Syslog] です。

フィールド名	使用上のガイドライン
説明（**Description**）	新しいターゲットの簡単な説明を入力します。
IP アドレス（IP Address）	ログを格納する宛先マシンの IP アドレスまたはホスト名を入力します。Cisco ISE は、ロギング用に IPv4 形式と IPv6 形式をサポートします。
ポート（**Port**）	宛先マシンのポート番号を入力します。
ファシリティ コード（**Facility Code**）	ロギングに使用する必要がある syslog ファシリティコードをドロップダウンリストから選択します。有効なオプションは、Local0 ～ Local7 です。
最大長（**Maximum Length**）	リモートログターゲットメッセージの最大長を入力します。有効な値は 200 ～ 1024 バイトです。
サーバー ダウン時のバッファ メッセージ（**Buffer Message When Server Down**）	このチェックボックスは、[ターゲットタイプ（Target Type）] ドロップダウンリストから [TCP Syslog] または [セキュアな syslog（Secure Syslog）] を選択すると表示されます。TCP syslog ターゲットまたはセキュアな syslog ターゲットが使用できないときに syslog メッセージを Cisco ISE がバッファできるようにするには、このチェックボックスをオンにします。Cisco ISE は、ターゲットへの接続が再開されるとターゲットへのメッセージの送信を再試行します。接続が再開されると、メッセージは最も古いものから順に送信されます。バッファされたメッセージは、常に新しいメッセージの前に送信されます。バッファがいっぱいになると、古いメッセージが廃棄されます。
バッファ サイズ（MB）（**Buffer Size (MB)**）	各ターゲットのバッファサイズを設定します。デフォルトでは、100 MB に設定されます。バッファサイズを変更するとバッファがクリアされ、特定のターゲットのバッファリングされた既存のすべてのメッセージが失われます。
再接続タイムアウト（秒）（**Reconnect Timeout (Sec)**）	サーバーがダウンした場合に TCP とセキュアな syslog を破棄するまで保存する期間を設定する期間を秒単位で入力します。

フィールド名	使用上のガイドライン
CA 証明書の選択（Select CA Certificate）	このドロップダウンリストは、[ターゲットタイプ（Target Type）] ドロップダウンリストから [セキュアな syslog（Secure Syslog）] を選択すると表示されます。ドロップダウンリストからクライアント証明書を選択します。
サーバー証明書有効性を無視（Ignore Server Certificate validation）	このチェックボックスは、[ターゲットタイプ（Target Type）] ドロップダウンリストから [セキュアな syslog（Secure Syslog）] を選択すると表示されます。サーバー証明書の認証を無視し、syslog サーバーを許可するには、Cisco ISE のこのチェックボックスをオンにします。デフォルトでは、このオプションが無効になっているときにシステムが FIPS モードでない限り、このオプションはオフに設定されます。

関連トピック

- Cisco ISE ロギング メカニズム
- Cisco ISE システム ログ
- Cisco ISE メッセージ カタログ
- 収集フィルタ
- イベント抑制バイパス フィルタ
- リモート syslog 収集場所の設定
- 収集フィルタの設定

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

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

ステップ 1 Cisco ISE 管理ポータルで、[メニュー（Menu）] アイコン（☰）をクリックし、**[管理（Administration）]** > **[システム（System）]** > **[ロギング（Logging）** > **[ロギングカテゴリ（Logging Categories）]** を選択します。

ステップ 2 [管理および運用の監査（Administrative and Operational Audit）] ロギングカテゴリの横にあるオプション ボタンをクリックし、次に [編集（Edit）] をクリックします。

ステップ 3 [ログ重大度レベル（Log Severity Level）] ドロップダウンリストから [警告（WARN）] を選択します。

ステップ 4 [ターゲット（Targets）] エリアで、以前に作成したセキュアな syslog リモートロギングターゲットを、[選択済み（Selected）] エリアに移動します。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 次のロギングカテゴリを有効にする場合は、このタスクを繰り返し行います。これらのロギングカテゴリは両方とも、デフォルトログの重大度レベルとして [情報（INFO）] を持ち、編集できません。

- [AAA 監査（AAA Audit）]
- [ポスチャおよびクライアント プロビジョニングの監査（Posture and Client Provisioning Audit）]

ロギングカテゴリの設定

次の表では、ロギングカテゴリを設定するために使用可能なフィールドについて説明します。ログの重大度レベルを設定し、ロギングカテゴリのログにロギングターゲットを選択します。このウィンドウにアクセスするには、**[管理（Administration）]** > **[システム（System）]** > **[ロギング（Logging）]** > **[ロギングカテゴリ（Logging Categories）]** の順にクリックします。

表示するロギングカテゴリの横のオプションボタンをクリックし、[編集（Edit）] をクリックします。次の表では、ロギングカテゴリの編集ウィンドウに表示されるフィールドについて説明します。

表 *7:* ロギング カテゴリの設定

フィールド名	使用上のガイドライン
名前（Name）	ロギング カテゴリの名前を表示します。

フィールド名	使用上のガイドライン
ログの重大度レベル（**Log Severity Level**）	一部のロギングカテゴリでは、この値はデフォルトで設定されており、編集できません。一部のロギングカテゴリでは、次の重大度レベルのいずれかをドロップダウンリストから選択できます。 • [重大（FATAL）]：緊急事態レベル。このレベルは、Cisco ISE を使用できず、必要なアクションをただちに実行する必要があることを意味します。 • [エラー（ERROR）]：このオプションは深刻な状態またはエラー状態を示します。 • [警告（WARN）]：このオプションは、通常の状態ではあるが重大な状態を示します。これは、多くのロギングカテゴリに設定されるデフォルトのレベルです。 • [情報（INFO）]：このレベルは情報メッセージを示します。 • [デバッグ（DEBUG）]：このレベルは、診断バグメッセージを示します。
ローカル ロギング（**Local Logging**）	ローカルノードでこのカテゴリのロギングイベントを有効にするには、このチェックボックスをオンにします。
ターゲット（**Targets**）	この領域では、左右の矢印アイコンを使用し、[使用可能（Available）] 領域と [選択済み（Selected）]領域間でターゲットを移動して、ロギングカテゴリのターゲットを選択できます。[使用可能（Available）] 領域には、ローカル（事前定義済み）と外部（ユーザー定義）の両方の既存のロギングターゲットが含まれています。[選択済み（Selected）] 領域（最初は空）には、カテゴリに選択されたターゲットが表示されます。

関連トピック

Cisco ISE メッセージ コード
リモート syslog 収集場所の設定
メッセージ コードの重大度レベルの設定

TCP syslog コレクタと UDP syslog コレクタの無効化

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

（注） UDP syslog を MnT ノードに配信するために Cisco ISE メッセージングサービスの使用を有効にした場合、Cisco ISE リリース 2.6 以降のリリースには、TLS 保護された UDP syslog が含まれます。Cisco ISE メッセージングサービスを介した syslogを参照してください

ステップ 1 Cisco ISE の GUI で、[メニュー（Menu）] アイコン（☰）をクリックして、**[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [リモート ロギング ターゲット（Remote Logging Targets）]** を選択します。

ステップ 2 TCP または UDP syslog コレクタの横にあるオプションボタンをクリックします。

ステップ 3 [編集（Edit）] をクリックします。

ステップ 4 [ステータス（Status）] ドロップダウン リストから [無効化（Disabled）] を選択します。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 すべての TCP または UDP syslog コレクタが無効になるまで、このプロセスを繰り返します。

デフォルトのセキュア syslog コレクタ

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

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

[リモートロギングターゲット（Remote Logging Targets）] ウィンドウにこの情報を表示できます（**[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [リモートロギングターゲット（Remote Logging Targets）]**を選択）。デフォルトの syslog コレクタは削除できません。また、デフォルトの syslog コレクタの次のフィールドは更新できません。

- **名前（Name）**
- **ターゲット タイプ（Target Type）**
- **IP/ホストアドレス（IP/Host address）**
- **ポート（Port）**

Cisco ISE の新規インストール時に、**Default Self-signed Server Certificate** という名前の証明書が信頼できる証明書ストアに追加されます。この証明書は、[クライアント認証と syslog 用に信頼する（Trust for Client authentication and Syslog）] の使用方法の場合にマークされ、セキュアなsyslogの使用方法で利用できるようになります。展開を設定する場合または証明書を更新する場合には、関連する証明書をセキュア syslog ターゲットに割り当てる必要があります。

Cisco ISE のアップグレード時に、ポート 6514で MnT ノードを指す既存のセキュアな syslog ターゲットがある場合、ターゲットの名前と設定は保持されます。アップグレード後は、これらのsyslogターゲットを削除することはできません。また、次のフィールドを編集することもできません。

- **名前（Name）**
- **ターゲット タイプ（Target Type）**
- **IP/ホストアドレス（IP/Host address）**
- **ポート（Port）**

アップグレードの時点でこのようなターゲットが存在しない場合、新規インストールの場合と同様にデフォルトのセキュアなsyslogターゲットが作成されますが、証明書のマッピングは行われません。これらのsyslogターゲットに関連証明書を割り当てることができます。どの証明書にもマッピングされていないセキュアなsyslogターゲットをロギングカテゴリにマッピングしようとすると、Cisco ISE は次のメッセージを表示します。

```
log_target_name の証明書を設定してください（Please configure the certificate for log_target_name）
```

オフライン メンテナンス

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

メンテナンス時間が1時間を超える場合は、メンテナンスの時点でノードを登録解除し、ノードを展開に再び追加するときにノードを再登録します。

処理があまり行われていない時間帯にメンテナンスをスケジュールすることが推奨されます。

（注）

1. キューに格納されているメッセージの数が 1,000,000 を超えるか、または Cisco ISE ノードが 6 時間を超えてオフラインになっている場合には、データの複製の問題が発生している可能性があります。
2. プライマリ MnT ノードでメンテナンスを行う場合は、メンテナンスアクティビティを実行する前に、MnT ノードの操作バックアップを作成しておくことを推奨します。

エンドポイント ログイン クレデンシャルの設定

[エンドポイントログイン設定（Endpoint Login Configuration）] ウィンドウでは、Cisco ISE がクライアントにログインできるようにログインクレデンシャルを設定します。このウィンドウで設定されたログインクレデンシャルは、次の Cisco ISE 機能で使用されます。

Cisco ISE の GUIで、[メニュー（Menu）] アイコン（☰）をクリックし、**[管理（Administration）]** > **[システム（System）]** > **[設定（Settings）]** > **[エンドポイントスクリプト（Endpoint Scripts）]** > **[設定（Settings）]** を選択します。

次のタブが表示されます。

- [Windows ドメインユーザー（Windows Domain User）] : Cisco ISE が SSH 経由でクライアントにログインするために使用する必要があるドメインクレデンシャルを設定します。[+（Plus）] アイコンをクリックして、必要な数の Windows ログインを入力します。ドメインごとに、[ドメイン（Domain）]、[ユーザー名（Username）]、および [パスワード（Password）] の各フィールドに必要な値を入力します。ドメインクレデンシャルを設定すると、[Windows ローカルユーザー（Windows Local User）] タブで設定されたローカルユーザー クレデンシャルは無視されます。
- [Windows ローカルユーザー（Windows Local User）] : Cisco ISE が SSH 経由でクライアントにアクセスするために使用するローカルアカウントを設定します。このローカルアカウントで、PowerShell と PowerShell をリモートで実行できる必要があります。
- [MAC ローカルユーザー（MAC Local User）] : Cisco ISE が SSH 経由でクライアントにアクセスするために使用するローカルアカウントを設定します。このローカルアカウントで、PowerShell と PowerShell をリモートで実行できる必要があります。[ユーザー名（Username）] フィールドに、ローカルアカウントのアカウント名を入力します。Mac OS アカウント名を表示するには、端末で次のコマンドを実行します。

```
whoami
```

Cisco ISE での証明書の管理

証明書は、個人、サーバー、会社、または別のエンティティを識別し、そのエンティティを公開キーに関連付ける電子文書です。自己署名証明書は、作成者によって署名されます。証明書は、自己署名したり、外部の CA がデジタルで署名したりできます。CA 署名付きデジタル証明書は、業界標準であり、自己署名証明書よりセキュアです。

証明書は、ネットワークに対するセキュアなアクセスを提供するために使用されます。証明書は、エンドポイントに対して Cisco ISE ノードを識別し、そのエンドポイントと Cisco ISE ノード間の通信を保護します。

Cisco ISE は、次の目的で証明書を使用します。

- Cisco ISE ノード間の通信。
- Cisco ISE と syslog やフィードサーバーなどの外部サーバー間の通信。

- Cisco ISE と、ゲスト、スポンサー、BYOD ポータルなどのエンドユーザーポータル間の通信。

Cisco ISE 管理ポータルを通じて、展開内のすべてのノードの証明書を管理します。

セキュアなアクセスを可能にするための Cisco ISE での証明書の設定

Cisco ISE は、公開キーインフラストラクチャ（PKI）に依存し、エンドポイントおよび管理者の両方とのセキュアな通信とマルチノード展開内の複数の Cisco ISE ノード間のセキュアな通信を実現しています。PKI は X.509 デジタル証明書に依存して、メッセージの暗号化と復号化のための公開キーの転送、およびユーザーとデバイスを表す他の証明書の信頼性の検証を行います。Cisco ISE の管理ポータルでは、次の 2 つのカテゴリの X.509 証明書を管理できます。

- システム証明書：これらはクライアント アプリケーションに対して Cisco ISE ノードを識別するサーバー証明書です。各 Cisco ISE ノードには独自のシステム証明書があり、対応する秘密キーとともにノードに格納されています。

（注） Cisco ISE は、同じ秘密キーを持つ複数の証明書をインポートできません。証明書が更新され、秘密鍵を変更せずにインポートされた場合、既存の証明書はインポートされた証明書に置き換えられます。

- 信頼できる証明書：これらの証明書は、ユーザーやデバイスから受信した公開キーの信頼を確立するために使用される CA 証明書です。信頼できる証明書ストアには、Simple Certificate Enrollment Protocol（SCEP）から配信された証明書も含まれます。これにより、モバイルデバイスを企業ネットワークに登録できるようになります。信頼できる証明書はプライマリ PAN で管理され、Cisco ISE 展開内の他のすべてのノードに自動的に複製されます。

分散展開では、証明書を PAN の証明書信頼リスト（CTL）のみにインポートする必要があります。この証明書はセカンダリ ノードに複製されます。

Cisco ISE で証明書認証が証明書による確認機能のわずかな違いの影響を受けないようにするために、ネットワークに展開されているすべての Cisco ISE ノードには小文字のホスト名を使用してください。

証明書の使用

Cisco ISE に証明書をインポートする場合は、証明書の使用目的を指定します。Cisco ISE の GUI で、[メニュー（Menu）] アイコン（☰）をクリックし、**[管理（Administration）]** > **[システム（System）]** > **[証明書（Certificates）]** > **[システム証明書（System Certificates]** を選択して、**[インポート（Import）]** をクリックします。

次の使用方法の 1 つ以上を選択します。

- [管理者（Admin）]：ノード間通信と管理者ポータルの認証。
- [EAP 認証（EAP Authentication）]：TLS ベースの EAP 認証。
- [RADIUS DTLS]： RADIUS DTLS サーバー認証。
- [ポータル（Portal）]：すべての Cisco ISE エンドユーザーポータルとの通信。
- [SAML]：SAML 応答が正しい ID プロバイダから受信されていることを確認。
- [pxGrid]：pxGrid コントローラとの通信。

管理ポータル（使用方法は管理）、pxGrid コントローラ（使用方法は pxGrid）との通信、および TLS ベースの EPA 認証（使用方法は EAP 認証）のための各ノードからさまざまな証明書を関連付けます。ただし、これらの各目的に各ノードから関連付けることができる証明書は 1 つのみです。

Web ポータル要求を処理できる展開に複数の PSN がある場合、Cisco ISE には一意の ID が必要です。この ID で、ポータルの通信に使用する必要がある証明書を識別します。ポータルでの使用に指定された証明書を追加またはインポートする場合、証明書グループタグを定義して、それを展開内の各ノードの対応する証明書に関連付けます。この証明書グループタグを対応するエンドユーザーポータル（ゲスト、スポンサー、およびパーソナルデバイスポータル）に関連付けます。この証明書グループタグは一意の ID で、Cisco ISE が各ポータルと通信する際に使用する必要がある証明書を識別する場合に役立ちます。ポータルごとに各ノードから指定できる証明書は 1 つのみです。

（注） EAP-TLS クライアント証明書では、以下の暗号に KeyUsage=Key Agreement と ExtendedKeyUsage=Client Authentication が必要です。

- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-ECDSA-AES256-SHA384

EAP-TLS クライアント証明書では、以下の暗号に KeyUsage=Key Encipherment と ExtendedKeyUsage=Client Authentication が必要です。

- AES256-SHA256
- AES128-SHA256
- AES256-SHA
- AES128-SHA
- DHE-RSA-AES128-SHA
- DHE-RSA-AES256-SHA
- DHE-RSA-AES128-SHA256
- DHE-RSA-AES256-SHA256
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-SHA384
- ECDHE-RSA-AES128-SHA256
- ECDHE-RSA-AES256-SHA
- ECDHE-RSA-AES128-SHA
- EDH-RSA-DES-CBC3-SHA
- DES-CBC3-SHA
- RC4-SHA
- RC4-MD5

この要件をバイパスするには、[管理（Administration）] > [システム（System）] > [設定（Settings）] > [セキュリティ設定（Security Settings）] の順に選択し、[目的の検証なしで証明書を受け入れる（Accept Certificates without Validating Purpose）] チェックボックスをオンにします。

Cisco ISE の証明書の一致

展開内で Cisco ISE ノードをセットアップすると、ノードが相互に通信します。システムは各 ISE ノードの FQDN を調べ、FQDN が一致することを確認します（たとえば ise1.cisco.com と ise2.cisco.com、またはワイルドカード証明書を使用している場合は *.cisco.com）。また、外部マシンから Cisco ISE サーバーに証明書が提示される場合、認証のために提示される外部証明書が、Cisco ISE サーバーの証明書と照合されます。2 つの証明書が一致すると、認証は成功します。

Cisco では、Cisco ノード間（2 ノードの場合）、または Cisco と pxGrid の間で照合が実行されます。

Cisco ISE は、サブジェクト名の一致を次のようにして確認します。

1. Cisco ISE により証明書のサブジェクト代替名の拡張が確認されます。サブジェクト代替名に 1 つ以上の DNS 名が含まれている場合は、それらの DNS 名の 1 つが Cisco ISE ノードの FQDN に一致している必要があります。ワイルドカード証明書が使用されている場合、ワイルドカード ドメイン名は Cisco ISE ノードの FQDN ドメインに一致している必要があります。
2. サブジェクト代替名に DNS 名が存在しない場合、またはサブジェクト代替名全体が欠落している場合は、証明書の **[サブジェクト（Subject）]** フィールドの一般名または証明書の **[サブジェクト（Subject）]** フィールドのワイルドカードドメインが、ノードの FQDN に一致している必要があります。
3. 一致しない場合、証明書は拒否されます。

（注） Cisco ISE にインポートされる X.509 証明書は、プライバシー強化メール（PEM）または識別符号化規則（DER）形式である必要があります。証明書チェーン（システム証明書、およびその証明書に署名する一連の信頼された証明書）が含まれたファイルはインポートすることができますが、特定の制限の対象となります。

X.509 証明書の有効性

X.509 証明書が有効なのは、指定された特定の日付までです。システム証明書が期限切れになった場合、その証明書に依存する Cisco ISE 機能が影響を受けます。Cisco ISE は、有効期限が 90 日以内になると、システム証明書の有効期間の残りについて通知します。この通知は、いくつかの方法で表示されます。

- 配色された有効期限の状態アイコンが、**[システム証明書（System Certificates）]** ウィンドウに表示されます。このウィンドウを表示するには、**[Menu（メニュー）]** アイコン（☰）をクリックし、**[管理（Administration）]** > **[システム（System）]** > **[証明書の管理（Certificate Management）]** > **[システム証明書（System Certificates）** を選択します。
- 期限切れメッセージが Cisco ISE システム診断レポートに表示されます。このウィンドウを表示するには、**[メニュー（Menu）]** アイコン（☰）をクリックし、**[操作（Operations）]**>

[レポート（Reports）] > [レポート（Reports）] > [診断（Diagnostics）] > [システム診断（System Diagnostic）] を選択します。

- 有効期限のアラームは、有効期限の 90 日前、60 日前、30 日間に生成されます。有効期限のアラームは、有効期限前の最後の 30 日間には毎日生成されます。

失効した証明書が自己署名証明書の場合は、この証明書を編集して有効期限を延長できます。認証局署名付き証明書の場合は、認証局から新しい証明書を取得するのに十分な期間を確保する必要があります。

Cisco ISE での公開キーインフラストラクチャの有効化

PKI は、セキュアな通信を可能にし、デジタル署名を使用してユーザーの ID を確認する暗号化技術です。

ステップ 1 展開内の各ノードで次のシステム証明書を設定します。

- EAP-TLS などの TLS 対応認証プロトコル。
- 管理ポータルの認証。
- ブラウザと REST クライアントを使用した Cisco ISE Web ポータルへのアクセスの許可。
- pxGrid コントローラへのアクセスの許可。

デフォルトで、Cisco ISE ノードには EAP 認証と、管理ポータル、エンドユーザーポータル、および pxGrid コントローラへのアクセスに使用される自己署名証明書があらかじめインストールされています。一般的な企業環境では、この自己署名証明書は、信頼できる CA によって署名されたサーバー証明書に置き換えられます。

ステップ 2 信頼できる証明書ストアに、ユーザーとの信頼を確立するために使用される CA 署名証明書と、Cisco ISE に提示されるデバイス証明書を配置します。

ルート CA 証明書と 1 つ以上の中間 CA 証明書で構成されている証明書チェーンでユーザーまたはデバイス証明書の信頼性を確認するには、次の手順を実行します。

- ルート CA に関連する信頼オプションを有効にします。

  Cisco ISE の GUI で、[メニュー（Menu）] アイコン（☰）をクリックし、**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [証明書の管理（Certificate Management）] > [信頼できる証明書（Trusted Certificates）]** を選択します。このウィンドウで、ルート CA 証明書のチェックボックスをオンにし、[編集（Edit）] をクリックします。[使用状況（Usage）] 領域で、[信頼先（Trusted For）] 領域内の必要なチェックボックスをオンにします。

- ルート CA の [信頼（Trust）] オプションを有効にしない場合は、CA 署名証明書チェーン全体を信頼できる証明書ストアにインポートします。

ノード間の通信では、Cisco ISE 展開内の各ノードに所属する管理者システム証明書を検証する信頼証明書を、信頼できる証明書ストアに配置する必要があります。デフォルトの自己署名証明書をノード間通信に

使用するには、この証明書をCisco ISEの各ノードの[システム証明書（System Certificates）]ウィンドウからエクスポートし、信頼できる証明書ストアにインポートします。自己署名証明書をCA署名証明書で置き換える場合に必要なのは、適切なルートCA証明書と中間CA証明書を信頼できる証明書ストアに配置することだけです。この手順を完了するまでは、ノードをCisco ISE展開に登録できません。

展開内でクライアントとPSNの間のセキュアな通信に自己署名証明書を使用する場合、BYODユーザーがある場所から別の場所に移動すると、EAP-TLSユーザー認証は失敗します。一部のPSN間で提供される必要があるこのような認証要求の場合、外部で署名されたCA証明書を使用してクライアントとPSNの間の通信を保護するか、または外部のCAによって署名されたワイルドカード証明書を使用する必要があります。

公開署名証明書を取得する場合、またはCisco ISE展開がFIPSモードで動作する場合は、すべてのシステム証明書および信頼できる証明書がFIPS準拠であることを確認する必要があります。つまり、各証明書のキー サイズが2048バイト以上であり、SHA-1またはSHA-256暗号化を使用する必要があります。

（注） スタンドアロンのCisco ISEまたはPANからバックアップを取得した後に、展開内の1つ以上のノードの証明書設定を変更する場合は、データを復元するために別のバックアップを取得する必要があります。そうしないで古いバックアップを使用してデータを復元すると、ノード間の通信が失敗する可能性があります。

ワイルドカード証明書

ワイルドカード証明書はワイルドカード表記（ドメイン名の前にアスタリスクとピリオドの形式）を使用しており、組織内の複数のホスト間で証明書を共有できます。たとえば、証明書サブジェクトの[CN]値はaaa.ise.localなどの汎用ホスト名であり、SANフィールドには、同じ汎用ホスト名とDNS.1=aaa.ise.localやDNS.2=*.ise.localなどのワイルドカード表記が含まれます。

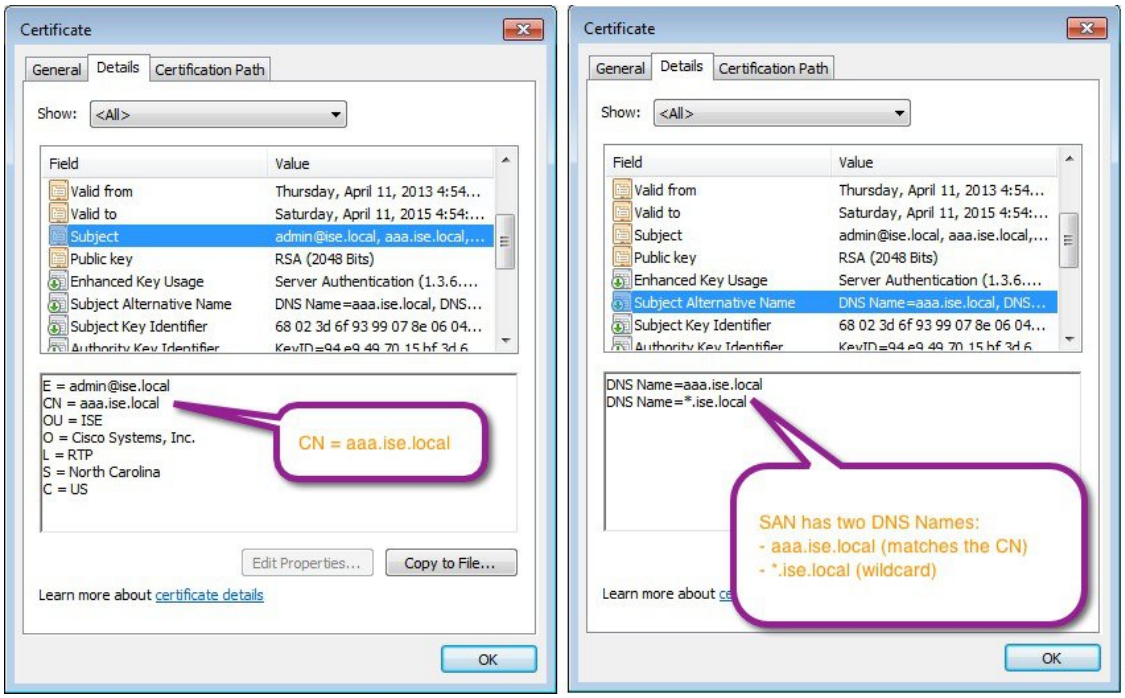
psn.ise.localのように、*.ise.localを使用してワイルドカード証明書を設定すると、その同じ証明書を使用して、次のようなDNS名が「.ise.local」で終了する他のすべてのホストを保護することができます：

- aaa.ise.local
- psn.ise.local
- mydevices.ise.local
- sponsor.ise.local

ワイルドカード証明書は通常の証明書と同じ方法で通信を保護し、要求は同じ検証方式を使用して処理されます。

次の図に、Webサイトの保護に使用されるワイルドカード証明書の例を示します。

図 *6:* ワイルドカード証明書の例



Cisco ISE のワイルドカード証明書のサポート

Cisco ISE はワイルドカード証明書をサポートしています。以前のリリースの Cisco ISE では、HTTPS に対して有効になったすべての証明書を検証し、[共通名（Common Name）] フィールドがホストの FQDN と正確に一致することを確認していました。フィールドが一致しない場合、その証明書は HTTPS 通信に使用できませんでした。

以前のリリースの Cisco ISE では、[共通名（Common Name）] 値を使用して、url-redirect A-V ペア文字列の変数を置き換えていました。この共通名の値は、すべての Centralized Web Authentication（CWA）、オンボーディング、ポスチャ リダイレクションなどに使用されました。

Cisco ISE は共通名として ISE ノードのホスト名を使用します。

HTTPS と拡張認証プロトコル通信用のワイルドカード証明書

SSL/TLS トンネリングを使用する 管理（Web ベースのサービス）と EAP プロトコルに対して、Cisco ISE でワイルドカードサーバー証明書を使用できます。ワイルドカード証明書を使用する場合は、Cisco ISE の各ノードに固有の証明書を生成する必要はありません。また、証明書の警告を防ぐために、SAN フィールドに複数の FQDN 値を入力する必要もありません。SAN フィールドでアスタリスク（*）を使用して展開内の複数のノードで単一の証明書を共有することができ、証明書名の不一致による警告を防止することができます。ただし、ワイルドカード証明書の使用は、各 Cisco ISE ノードに固有のサーバー証明書を割り当てる場合よりも安全性が低いと見なされます。

ゲストポータルに公開ワイルドカード証明書を割り当て、ルート CA 証明書を使用してサブ CA をインポートする場合、Cisco ISE サービスが再起動されるまで証明書チェーンは送信されません。

（注） ワイルドカード証明書を使用する場合は、セキュリティを強化するためにドメイン領域を分割することを推奨します。たとえば、*.example.com の代わりに *.amer.example.com を使用して領域を分割することができます。ドメインを分割しないと、重大なセキュリティ問題が発生する可能性があります。

ワイルドカード証明書では、ドメイン名の前にアスタリスク（*）とピリオドが使用されます。たとえば、証明書のサブジェクト名の共通名の値は aaa.ise.local などの汎用ホスト名になり、SAN フィールドには *.ise.local のようなワイルドカード文字が入力されます。Cisco ISE は、ワイルドカード証明書（提示される識別子の一番左の文字がワイルドカード文字（*））をサポートします。たとえば、*.example.com または *.ind.example.com です。提示される識別子に他の文字とワイルドカード文字が含まれた証明書はサポートされません。たとえば、abc*.example.com、a*b.example.com、または *abc.example.com です。

URL リダイレクションの完全修飾ドメイン名

認証プロファイルのリダイレクトは、中央 Web 認証、デバイス登録 Web 認証、ネイティブサプリカントのプロビジョニング、モバイルデバイスの管理、クライアントのプロビジョニング、およびポスチャサービスのために実行されます。Cisco ISE が認証プロファイルのリダイレクトを作成すると、結果の cisco-av-pair には次のような文字列が含まれます。

url-redirect=https://ip:port/guestportal/gateway?sessionId=SessionIdValue&action=cwa

この要求を処理するときに、Cisco ISE は文字列の一部のキーワードを実際の値で置き換えます。たとえば、SessionIdValue は、要求の実際のセッション ID に置き換えられます。eth0 インターフェイスの場合、Cisco ISE は URL 内の IP を Cisco ISE ノードの FQDN で置き換えます。eth0 以外のインターフェイスの場合、Cisco ISE は URL 内の IP アドレスを使用します。インターフェイス eth1 から eth3 にはホストのエイリアス（名前）を割り当てることができます。このエイリアスは Cisco ISE が URL リダイレクション中に IP アドレスの代わりに置き換えることができます。

これを行うために、次のように、Cisco ISE CLI の ISE /admin(config)# プロンプトからコンフィギュレーション モードで **ip host** コマンドを使用します。

ip host *IP_address host-alias FQDN-string*

ここで、*IP_address* はネットワーク インターフェイス（eth1 または eth2 または eth3）の IP アドレスで、*host-alias* はネットワーク インターフェイスに割り当てる名前です。*FQDN-string* は、ネットワーク インターフェイスの完全修飾ドメイン名です。このコマンドを使用して、ネットワーク インターフェイスに *host-alias* または *FQDN-string* あるいはその両方を割り当てることができます。

ip host コマンドの使用例：ip host a.b.c.d sales sales.amerxyz.com

eth0 以外のインターフェイスにホストエイリアスを割り当てたら、**application start ise** コマンドを使用して Cisco ISE でアプリケーション サービスを再起動します。

このホストエイリアスのネットワーク インターフェイスとの関連付けを削除するには、次のようにこのコマンドの **no** 形式を使用します。

no ip host *IP_address host-alias FQDN-string*

ホストのエイリアスの定義を表示するには、**show running-config** コマンドを使用します。

FQDN-string を指定している場合は、その FQDN で URL 内の IP アドレスが置き換えられます。ホストエイリアスのみを指定した場合は、Cisco ISE はそのホストエイリアスと設定された IP ドメイン名を結合して完全な FQDN を形成し、URL 内の IP アドレスをその FQDN で置き換えます。ネットワーク インターフェイスをホストのエイリアスにマッピングしない場合は、URL 内のネットワーク インターフェイスの IP アドレスが使用されます。

クライアントのプロビジョニング、ネイティブサプリカント、またはゲストフローに対して eth0 以外のインターフェイスを使用する場合は、eth0 以外のインターフェイスの IP アドレスまたはホストエイリアスが PSN 証明書の SAN フィールドに適切に設定されていることを確認します。

ワイルドカード証明書を使用する利点

- コスト削減：サードパーティ CA によって署名された証明書は、特にサーバーの数が増えると高額になります。ワイルドカード証明書は、Cisco ISE 展開内の複数ノードで使用できます。
- 運用効率：ワイルドカード証明書により、すべての PSN が EAP と Web サービス用に同じ証明書を共有できます。証明書を 1 回作成して、すべての PSN に適用することにより、コストを大幅に削減できるだけでなく、証明書の管理も簡素化されます。
- 認証エラーの削減：ワイルドカード証明書は、クライアントがプロファイル内に信頼できる証明書を保存しており、そのクライアントが iOS のキーチェーン（署名ルートが信頼されている）に従っていない Apple iOS デバイスで発生する問題に対処します。iOS クライアントが最初に PSN と通信する際、このクライアントはその PSN の証明書を（信頼できる CA が署名している場合でも）明示的に信頼しません。ワイルドカード証明書を使用すると、この証明書がすべての PSN で同一になるため、ユーザーは証明書の受け入れを 1 回行えばよく、その後の異なる PSN に対する認証はエラーやプロンプトが表示されることなく進行します。
- 簡略化されたサプリカントの設定：たとえば、PEAP-MSCHAPv2 と信頼できるサーバー証明書がある Microsoft Windows サプリカントでは、各サーバー証明書を信頼するように指定することが必要とされており、そのように指定しない場合は、そのクライアントが別の PSN を使用して接続を行うと、各 PSN 証明書を信用するように、ユーザーにプロンプトが出される可能性があります。ワイルドカード証明書を使用すると、各 PSN の個別の証明書ではなく、単一のサーバー証明書を信頼するだけで済みます。
- ワイルドカード証明書を使用すると、プロンプトの提示が減り、よりシームレスな接続が実現されることにより、ユーザー エクスペリエンスが改善されます。

ワイルドカード証明書を使用することの欠点

次に、ワイルドカード証明書の使用に関連するセキュリティ上の考慮事項の一部を説明します。

- 監査性と否認防止性の低下
- 秘密キーの露出の増加
- 一般的ではなく、管理者により理解されていない

ワイルドカード証明書は各 Cisco ISE ノードで固有のサーバー証明書を使用するよりも安全性が低いと見なされています。ただし、コスト、およびその他の運用関連の要因がセキュリティリスクに勝っています。

Cisco 適応型セキュリティアプライアンスなどのセキュリティデバイスも、ワイルドカード証明書をサポートしています。

ワイルドカード証明書を展開する場合には注意が必要です。たとえば、*.company.local を使用して証明書を作成したとします。該当の秘密キーを攻撃者が回復できた場合、攻撃者は company.local ドメイン内のすべてのサーバーをスプーフィングすることができます。したがって、このタイプの危険を回避するために、ドメイン領域を分割することがベストプラクティスと見なされています。

この想定される問題に対処し、利用範囲を制限するために、ワイルドカード証明書を使用して組織の特定のサブドメインを保護することもできます。ワイルドカードを指定する一般名のサブドメイン領域に、アスタリスク（*）を追加します。

たとえば、*.ise.company.local に対してワイルドカード証明書を設定すると、その証明書は次のような、DNS 名が「.ise.company.local」で終わるすべてのホストを保護するために使用できます。

- psn.ise.company.local
- mydevices.ise.company.local
- sponsor.ise.company.local

ワイルドカード証明書の互換性

ワイルドカード証明書は通常、証明書サブジェクトの共通名としてリストされているワイルドカードを使用して作成されます。Cisco ISE は、このタイプの作成をサポートします。ただし、すべてのエンドポイントサプリカントが証明書サブジェクトのワイルドカード文字をサポートしているわけではありません。

テスト済みのすべての Microsoft ネイティブサプリカント（販売が終了している Windows Mobile を含む）の一部は、証明書サブジェクトのワイルドカード文字をサポートしていません。

Cisco AnyConnect Network Access Manager など、[サブジェクト（Subject）] フィールドでのワイルドカード文字の使用をサポートできる他のサプリカントを使用できます。

また、DigiCert の Wildcard Plus など、証明書のサブジェクト代替名に特定のサブドメインを含めることで、互換性のないデバイスを使用するように設計された、特別なワイルドカード証明書を使用することもできます。

Microsoft サプリカントの制限はワイルドカード証明書の使用にとって妨げになるように見えますが、Microsoft のネイティブサプリカントを含む、セキュアなアクセスについてテスト済みのすべてのデバイスを使用できるようにする代替の方法があります。

これを行うには、サブジェクトにワイルドカード文字を使用する代わりに、[サブジェクト代替名（Subject Alterative Name）] フィールドでワイルドカード文字を使用する必要があります。[サブジェクト代替名（Subject Alternative Name）] フィールドには、ドメイン名（DNS 名）を確認するように指定された拡張子が保持されます。詳細については、RFC 6125 と RFC 2128 を参照してください。

証明書階層

管理ポータルには、すべてのエンドポイント、システム、および信頼できる証明書の証明書階層または信頼書信頼チェーンが表示されます。証明書階層には、証明書、すべての中間 CA 証明書、およびルート証明書が含まれています。たとえば、管理ポータルからシステム証明書を表示すると、デフォルトの対応するシステム証明書の詳細が表示されます。証明書階層は、証明書の上部に表示されます。詳細を表示するには、その階層で証明書をクリックします。自己署名証明書には階層または信頼チェーンがありません。

証明書のリストウィンドウで、[ステータス（Status）] 列に次のアイコンのいずれかが表示されます。

- 緑色のアイコン：有効な証明書（有効な信頼チェーン）を示します。
- 赤色のアイコン：エラーを示します（たとえば、信頼証明書の欠落または期限切れ）。
- 黄色のアイコン：証明書が期限切れ間近であることを警告し、更新処理を求めます。

システム証明書

Cisco ISE システム証明書は、展開内のその他のノードおよびクライアント アプリケーションに対して Cisco ISE ノードを識別するサーバー証明書です。システム証明書の用途は次のとおりです。

- Cisco ISE 展開でノード間通信に使用されます。これらの証明書の[使用方法（Usage）]領域で[管理（Admin）]チェックボックスをオンにします。
- Cisco ISE Web ポータルに接続するブラウザおよび REST クライアントで使用されます。これらの証明書の [使用方法（Usage）] 領域の [ポータル（Portal）] チェックボックスをオンにします。
- PEAP および EAP-FAST を使用する外部 TLS トンネルを形成するために使用されます。EAP-TLS、PEAP、および EAP-FAST による相互認証の場合、[使用方法（Usage）] 領域の [EAP 認証（EAP Authentication）] チェックボックスをオンにします。

- RADIUS DTLS サーバー認証に使用されます。
- SAML ID プロバイダとの通信に使用されます。この証明書の [使用方法（Usage）] 領域の [SAML] チェックボックスをオンにします。[SAML] オプションを選択すると、その他のサービスにこの証明書を使用することはできません。

  SAML 証明書は、ポスチャサービスや Cisco ISE と Cisco Smart Software Manager 間のライセンス通信など、複数の Cisco ISE サービスで使用されます。Cisco ISE から SAML 証明書を削除すると、関連するサービスが中断されます。
- pxGrid コントローラとの通信に使用されます。これらの証明書の [使用方法（Usage）] 領域の [pxGrid] チェックボックスをオンにします。

Cisco ISE 展開の各ノードに有効なシステム証明書をインストールします。デフォルトでは、インストール時に Cisco ISE ノードに 2 つの自己署名証明書と、内部 Cisco ISE CA により署名された 1 つの証明書が作成されます。

- [EAP]、[管理（Admin）]、[ポータル（Portal）]、および [RADIUS DTLS] のための自己署名サーバー証明書（キー サイズは 2048 で 1 年間有効です）。
- SAML ID プロバイダとの安全な通信に使用できる自己署名 SAML サーバー証明書（キー サイズは 2048 で 1 年間有効です）。
- pxGrid クライアントとの安全な通信に使用できる内部 Cisco ISE CA 署名付きサーバー証明書（キー サイズは 4096 で 1 年間有効です）。

展開をセットアップし、セカンダリノードを登録すると、pxGrid コントローラ用の証明書が自動的にプライマリノードの CA 署名付き証明書に置き換わります。したがってすべての pxGrid 証明書が同一 PKI トラスト階層の一部となります。

（注）

- ワイルドカードシステム証明書をエクスポートして、（ノード間通信用に）他のノードにインポートする場合は、必ず証明書と秘密キーをエクスポートして、暗号化パスワードを指定してください。インポート時は、証明書、秘密キー、および暗号化パスワードが必要です。
- Cisco ISE では、EAP-TLS 認証の信頼できる証明書およびエンドポイント証明書に対してのみ、RSASSA-PSS アルゴリズムの使用がサポートされています。証明書を表示すると、署名アルゴリズムは、アルゴリズム名ではなく、1.2.840.113549.1.1.10 としてリストされます。

  Cisco ISE では、署名アルゴリズムとして RSASSA-PSS を使用するシステム証明書はサポートされていません。これは、サーバー証明書、ルート証明書、および中間 CA 証明書に適用されます。
- クラウド形成テンプレート（CFT）を使用して Cisco ISE を AWS に展開すると、[システム証明書（System Certificates）] ウィンドウに DefaultISE.ise.com ベースの証明書が表示される場合があります。これは、Cisco ISE の機能には影響しません。CA 証明書が再生成されると、それらの追加の証明書はアクティブにならず、無視できます。

お使いのリリースでサポートされているキーと暗号については、該当バージョンの『Cisco Identity Services Engine ネットワークコンポーネントの互換性』ガイドを参照してください。

セキュリティを強化するために、自己署名証明書をCA署名付き証明書で置き換えることを推奨します。CA署名付き証明書を取得するには、以下を行う必要があります。

1. 証明書署名要求の作成と認証局への送信 （106 ページ）
2. 信頼できる証明書ストアへのルート証明書のインポート （97 ページ）
3. 証明書署名要求への CA 署名付き証明書のバインド （106 ページ）

ISE コミュニティ リソース

How To: Implement ISE Server-Side Certificates

Cisco Identity Services Engine の証明書更新に関する設定ガイド

システム証明書の表示

[システム証明書（System Certificate）] ウィンドウに、Cisco ISE に追加されたすべてのシステム証明書のリストが表示されます。

始める前に

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

ステップ 1 **[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [システム証明書（System Certificates）]** を選択します。

ステップ 2 [システム証明書（System Certificates）] ウィンドウには、次の列が表示されます。

- [フレンドリ名（Friendly Name）]：証明書の名前。
- [使用方法（Usage）]：この証明書が使用されるサービス。
- [ポータルグループタグ（Portal group tag）]：ポータルを使用するように指定された証明書に対してのみ適用できます。このフィールドはポータルに使用する必要がある証明書を指定します。
- [発行先（Issued To）]：証明書のサブジェクトの共通名。
- [発行元（Issued By）]：証明書発行者の共通名
- [有効期限の開始（Valid From）]：証明書の作成日付（「Not Before」証明書属性）。
- [期限日（Expiration Date）]：証明書の有効期限（「Not After」証明書属性）。有効期限の横に次のアイコンが表示されます。
  - 緑色のアイコン：期限切れまで 91 日以上。
  - 青色のアイコン：期限切れまで 90 日以内。
  - 黄色のアイコン：期限切れまで 60 日以内。

- オレンジ色のアイコン：期限切れまで 30 日以内。
- 赤色のアイコン： 期限切れ。

システム証明書のインポート

管理者ポータルから、任意の Cisco ISE ノードのシステム証明書をインポートできます。

（注） プライマリ PAN 上の管理者ロール証明書の証明書を変更すると、他のすべてのノード上のサービスが再起動されます。プライマリ PAN の再起動が完了すると、システムによって一度に 1 つのノードが再起動されます。

始める前に

- クライアントブラウザで実行しているシステムに、システム証明書と秘密キーファイルがあることを確認します。
- インポートするシステム証明書が外部 CA によって署名されている場合は、関連するルート CA および中間 CA の証明書を信頼できる証明書ストアにインポートします（**[管理（Administration）]** > **[システム（System）]** > **[証明書（Certificates）]** > **[信頼できる証明書（Trusted Certificates）]**）。
- インポートするシステム証明書に、CA フラグが true に設定された基本制約拡張が含まれている場合は、キー使用拡張が存在すること、および keyEncipherment ビットと keyAgreement ビットのいずれかまたは両方が設定されていることを確認します。
- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 **[管理（Administration）]** > **[システム（System）]** > **[証明書（Certificates）]** > **[システム証明書（System Certificates）]** 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。
[証明書インポートウィザード（Certificate Import Wizard）] ウィンドウが表示されます。

ステップ 3 インポートする証明書の値を入力します。

ステップ 4 **[送信（Submit）]** をクリックします。

システム証明書のインポート設定

次の表では、サーバー証明書をインポートするために使用できる **[システム証明書のインポート（Import System Certificate）]** ウィンドウのフィールドについて説明します。このウィンド

ウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして、**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [システム証明書（System Certificates）]** です。[インポート（Import）] をクリックします。

表 *8*: システム証明書のインポート設定

フィールド名	説明
ノードの選択（Select Node）	（必須）システム証明書をインポートする Cisco ISE ノードをドロップダウンリストから選択します。
証明書ファイル（Certificate file）	（必須）**[ファイルの選択（Choose File）]** の順にクリックして、ローカルシステムから証明書ファイルを選択します。
秘密キー ファイル（Private key file）	（必須）**[ファイルの選択（Choose File）]** の順にクリックして、ローカルシステムから秘密キーファイルを選択します。
パスワード（Password）	（必須）秘密キーファイルを復号化するためのパスワードを入力します。
フレンドリ名（Friendly Name）	証明書のフレンドリ名を入力します。名前を指定しない場合は、Cisco ISE により <common name> # <issuer> # <nnnnn> の形式で自動的に名前が作成されます。ここで、 <nnnnn> は固有の 5 桁の数字です。
ワイルドカード証明書の許可（Allow Wildcard Certificates）	ワイルドカード証明書をインポートする場合は、このチェックボックスをオンにします。ワイルドカード証明書では、ワイルドカード表記（ドメイン名の前にアスタリスク（*）およびピリオド）が使用されます。ワイルドカード証明書は、組織内の複数のホスト間で共有されます。 このチェックボックスをオンにすると、Cisco ISE は展開内の他のすべてのノードにこの証明書をインポートします。
証明書の拡張の検証（Validate Certificate Extensions）	Cisco ISE に証明書の拡張の検証を許可する場合は、このチェックボックスをオンにします。このチェックボックスをオンにし、かつインポートする証明書に CA フラグが true に設定された基本制約拡張が含まれている場合は、キー使用拡張が存在することを確認します。keyEncipherment ビットと keyAgreement ビットのいずれかまたは両方を設定する必要があります。

フィールド名	説明
使用方法（Usage）	このシステム証明書を使用する必要があるサービスを選択します。 • [管理者（Admin）]：管理ポータルとの通信および展開内の Cisco ISE ノード間の通信の保護に使用されるサーバー証明書。 （注） プライマリ PAN 上の管理者ロール証明書の証明書を変更すると、他のすべての Cisco ISE ノード上のサービスが再起動されます。 • [EAP 認証（EAP Authentication）]：SSL トンネリングまたは TLS トンネリングの EAP プロトコルを使用する認証に使用されるサーバー証明書。 • [RADIUS DTLS]：RADIUS DTLS 認証に使用するサーバー証明書。 • [pxGrid]：pxGrid クライアントとサーバーの間の通信を保護するクライアントおよびサーバー証明書。 • **[ISE メッセージングサービス（ISE Messaging Service）]**：**Cisco ISE メッセージングを介した Syslog** 機能に使用されます。組み込みの UDP syslog 収集ターゲット（LogCollector および LogCollector2）用の MnT WAN 存続を有効にします。 • [SAML]：SAML ID プロバイダとのセキュアな通信に使用するサーバー証明書。SAML 用の使用を目的とした証明書は、管理者認証や EAP 認証などのその他のサービスのために使用することはできません。 • [ポータル（Portal）]：すべての Cisco ISE Web ポータルとの通信を保護するために使用されるサーバー証明書

関連トピック

システム証明書 （76 ページ）
システム証明書の表示 （78 ページ）
システム証明書のインポート （79 ページ）

自己署名証明書の生成

自己署名証明書を生成することで、新しいローカル証明書を追加します。自己署名証明書は、内部テストと評価のニーズに対してのみ使用することを推奨します。実稼働環境に Cisco ISE を展開することを計画している場合は、可能な限り CA 署名付き証明書を使用して、実稼働ネットワーク全体でより均一な受け入れが行われるようにします。

（注） 自己署名証明書を使用しており、Cisco ISE ノードのホスト名を変更する場合は、 Cisco ISE ノードの管理ポータルにログインし、古いホスト名が使用されている自己署名証明書を削除してから、新しい自己署名証明書を生成します。そうしないと、Cisco ISE は古いホスト名が使用された自己署名証明書を引き続き使用します。

始める前に

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

自己署名証明書の設定

次の表では、[自己署名証明書の生成（Generate Self Signed Certificate）] ウィンドウのフィールドについて説明します。このウィンドウでは、ノード間通信、EAP-TLS 認証、Cisco ISE Web ポータル、およびpxGrid コントローラとの通信用のシステム証明書を作成できます。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして、**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [システム証明書（System Certificates）]**の順に選択します。[自己署名証明書の生成（Generate Self Signed Certificate）] をクリックします。

表 *9:* 自己署名証明書の設定

フィールド名	使用上のガイドライン
ノードの選択（Select Node）	（必須）システム証明書を生成するノードをドロップダウンリストから選択します。
Common Name（CN）	（SAN を指定しない場合に必須）デフォルトでは、共通名は自己署名証明書を生成する Cisco ISE ノードの FQDN です。
組織ユニット（Organization Unit）（OU）	組織ユニット名。Engineering など。
組織（Organization）（O）	組織名。Cisco など。
都市（City）（L）	（省略不可）都市名。San Jose など。
州（State）（ST）	（省略不可）州名。California など。
国（Country）（C）	国名。2 文字の ISO 国番号を入力します。US など。

フィールド名	使用上のガイドライン
サブジェクト代替名（**Subject Alternative Name**）（**SAN**）	証明書に関連付けられた IP アドレス、DNS 名、または Uniform Resource Identifier（URI）。
キー タイプ	RSA または ECDSA のいずれかの公開キーの作成に使用するアルゴリズム。
キーの長さ（**Key Length**）	公開キーのビットサイズ。ドロップダウンリストから、RSA に次のいずれかのオプションを選択します。 • 512 • 1024 • 2048 • 4096 ドロップダウンリストから、ECDSA に次のいずれかのオプションを選択します。 • 256 • 384 （注） RSA および ECDSA の公開キーは、同じセキュリティレベルで異なるキー長を持つことがあります。 パブリック CA 署名付き証明書を取得する場合、または FIPS 準拠ポリシー管理システムとして Cisco ISE を展開する場合は、2048 を選択します。
署名するダイジェスト（**Digest to Sign With**）	ドロップダウンリストから、次のハッシュアルゴリズムのいずれかを選択します。 • SHA-1 • SHA-256
証明書ポリシー（**Certificate Policies**）	証明書が従うべき証明書ポリシーの OID または OID のリストを入力します。OID を区切るには、カンマまたはスペースを使用します。
TTL 有効期限（**Expiration TTL**）	証明書が失効するまでの日数を指定します。ドロップダウンリストから値を選択します。

フィールド名	使用上のガイドライン
フレンドリ名（**Friendly Name**）	証明書のフレンドリ名を入力します。名前を指定しない場合は、<common name> # <issuer> # <nnnnn> の形式で自動的に名前が作成されます。ここで、<nnnnn> は固有の 5 桁の数値です。
ワイルドカード証明書の許可（**Allow Wildcard Certificates**）	自己署名ワイルドカード証明書を生成する場合は、このチェックボックスをオンにします。ワイルドカード証明書はワイルドカード表記（ドメイン名の前にアスタリスクとピリオドの形式）を使用し、組織の複数のホスト間で証明書を共有できるようにします。
使用方法（**Usage**）	このシステム証明書を使用する必要があるサービスを選択します。 • [管理者（Admin）]：管理ポータルとの通信および展開内の Cisco ISE ノード間の通信の保護に使用されるサーバー証明書。 • [EAP 認証（EAP Authentication）]：SSL トンネリングまたは TLS トンネリングの EAP プロトコルを使用する認証に使用されるサーバー証明書。 • [RADIUS DTLS]：RADIUS DTLS 認証に使用するサーバー証明書。 • [pxGrid]：pxGrid クライアントとサーバーの間の通信を保護するクライアントおよびサーバー証明書。 • [SAML]：SAML ID プロバイダとのセキュアな通信に使用するサーバー証明書。SAML 用の使用を目的とした証明書は、管理者認証や EAP 認証などのその他のサービスのために使用することはできません。 • [ポータル（Portal）]：すべての Cisco ISE Web ポータルとの通信を保護するために使用されるサーバー証明書。

関連トピック

システム証明書 （76 ページ）
システム証明書の表示 （78 ページ）
自己署名証明書の生成 （81 ページ）

システム証明書の編集

このウィンドウを使用して、システム証明書を編集し、自己署名証明書を更新します。ワイルドカード証明書を編集すると、変更が展開内のすべてのノードに複製されます。ワイルドカード証明書を削除した場合、そのワイルドカード証明書は展開内のすべてのノードから削除されます。

始める前に

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

ステップ 1 **[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [システム証明書（System Certificates）]** を選択します。

ステップ 2 編集する証明書の横にあるチェックボックスをオンにして、[編集（Edit）] をクリックします。

ステップ 3 自己署名証明書を更新するには、**[更新期間（Renewal Period）]** チェックボックスをオンにして、有効期限 TTL（存続可能時間）を日、週、月、または年単位で入力します。ドロップダウンリストから必要な値を選択します。

ステップ 4 [保存（Save）] をクリックします。

[管理者（Admin）] チェックボックスがオンになっている場合、Cisco ISE ノードのアプリケーションサーバーが再起動します。また、その Cisco ISE ノードが展開の PAN である場合は、展開内のその他すべてのノードでもアプリケーションサーバーが再起動します。プライマリ PAN の再起動が完了すると、システムによって一度に 1 つのノードが再起動されます。

（注） Chrome 65 以上を使用して Cisco ISE を起動すると、URL が正しくリダイレクトされたにもかかわらず、BYOD ポータルまたはゲストポータルがブラウザで起動に失敗することがあります。これは、すべての [サブジェクトの別名（Subject Alternative Name）] フィールドに証明書を必要とする、Google で導入された新しいセキュリティ機能が原因です。Cisco ISE リリース 2.4 以降の場合、[サブジェクトの別名（Subject Alternative Name）] フィールドを入力する必要があります。

Chrome 65 以上で起動するには、次の手順に従います。

1. [サブジェクトの別名（Subject Alternative Name）] フィールドに入力することで、Cisco ISE GUI から新しい自己署名証明書を生成します。DNS と IP アドレスの両方を入力する必要があります。

2. Cisco ISE サービスが再起動します。

3. Chrome ブラウザでポータルにリダイレクトされます。

4. ブラウザで [証明書の表示（View Certificate）] > [詳細（Details）] > [コピー（Copy）] の順に選択し、base-64 エンコードを選択して、証明書をコピーします。

5. 高信頼パスで証明書をインストールします。

6. Chrome ブラウザを終了し、ポータルのリダイレクトを試みます。

（注） Win RS4 または RS5 のオペレーティングシステムでブラウザ Firefox 64 以降のリリースのワイヤレス BYOD セットアップを設定する場合は、証明書の例外を追加することができない場合があります。この現象は Firefox 64 以降のリリースの新規インストール時に発生することがあります。以前のバージョンから Firefox 64 以降にアップグレードした場合は発生しません。次の手順では、このような場合でも証明書の例外を追加することができます。

1. BYOD フローのシングル PEAP またはデュアル PEAP または TLS を設定します。
2. Windows のすべてのオプションで CP ポリシーを設定します。
3. エンドクライアント Windows RS4 または Windows RS5 で、Dot1.x または MAB SSID に接続します。
4. ゲストポータルまたは BYOD ポータルにリダイレクトするには、FF64 ブラウザに 何らか URL を入力します。
5. **[例外を追加（Add Exception）]** > **[証明書を追加できない（Unable to add certificate）]** をクリックし、フローを続行します。

回避策として、Firefox 64 の証明書を手動で追加します。Firefox 64 のブラウザで、**[オプション（Options）]** > **[プライバシー&設定（Privacy & Settings）]** > **[証明書の表示（View Certificates）]** > **[サーバー（Servers）]** > **[例外の追加（Add Exception）]** を選択します。

システム証明書の削除

今後使用しないシステム証明書を削除できます。

システム証明書ストアから複数の証明書を一度に削除できますが、管理および EAP 認証に使用する証明書を少なくとも 1 つ所有する必要があります。また、管理、EAP 認証、ポータル、または pxGrid コントローラに使用される証明書は削除できません。ただし、サービスがディセーブルの場合は、pxGrid 証明書を削除できます。

ワイルドカード証明書を削除することを選択した場合、証明書は展開内のすべての Cisco ISE ノードから削除されます。

ステップ 1 Cisco ISE GUI で、**[メニュー（Menu）]** アイコン（☰）をクリックし、**[管理（Administration）]** > **[システム（System）]** > **[証明書（Certificates）]** > **[システム証明書（System Certificates）]**を選択します。

ステップ 2 削除する証明書の隣にあるチェックボックスをオンにし、[削除（Delete）] をクリックします。

警告メッセージが表示されます。

ステップ 3 [はい（Yes）] をクリックして、証明書を削除します。

システム証明書のエクスポート

システム証明書とその証明書に関連付けられている秘密キーをエクスポートできます。証明書とその秘密キーをバックアップ用にエクスポートする場合は、それらを必要に応じて後で再インポートできます。

始める前に

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

ステップ 1 Cisco ISE GUI で、**[メニュー（Menu）]** アイコン（☰）をクリックし、**[管理（Administration）]** > **[システム（System）]** > **[証明書（Certificates）]** > **[システム証明書（System Certificates）]**の順に選択します。

ステップ 2 エクスポートする証明書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）]** をクリックします。

ステップ 3 証明書のみをエクスポートするか、証明書と証明書に関連付けられている秘密キーをエクスポートするかを選択します。

ヒント 値が公開される可能性があるため、証明書に関連付けられている秘密キーのエクスポートは推奨しません。秘密キーをエクスポートする必要がある場合（たとえば、ワイルドカードシステム証明書をエクスポートしてノード間通信用に他の Cisco ISE ノードにインポートする場合）は、その秘密キーの暗号化パスワードを指定します。このパスワードは、証明書を別の Cisco ISE ノードにインポートするときに指定して、秘密キーを復号化する必要があります。

ステップ 4 秘密キーをエクスポートする場合は、パスワードを入力します。パスワードは、8 文字以上にする必要があります。

ステップ 5 [エクスポート（Export）] をクリックして、クライアント ブラウザを実行しているファイル システムに証明書を保存します。

証明書のみをエクスポートする場合、証明書はPEM形式で保存されます。証明書と秘密キーの両方をエクスポートする場合、証明書はPEM形式の証明書と暗号化された秘密キーファイルを含む.zipファイルとしてエクスポートされます。

信頼できる証明書ストア

信頼できる証明書ストアには、信頼に使用される、Simple Certificate Enrollment Protocol（SCEP）用の X.509 証明書が含まれています。

信頼できる証明書ストア内の証明書はプライマリ PAN で管理され、Cisco ISE 展開内の他のすべてのノードに複製されます。Cisco ISE はワイルドカード証明書をサポートしています。

Cisco ISE は、次の目的で信頼できる証明書を使用します。

- エンドポイントによる認証と、証明書ベースの管理者認証を使用してISE-PIC管理ポータルにアクセスする Cisco ISE 管理者による認証に使用するクライアント証明書を確認するため。

- 展開内の Cisco ISE ノード間のセキュアな通信を可能にするため。信頼できる証明書ストアには、展開内の各ノードのシステム証明書との信頼を確立するために必要な CA 証明書のチェーンが含まれている必要があります。
  - 自己署名証明書をシステム証明書に使用する場合は、各ノードの自己署名証明書を PAN の信頼できる証明書ストアに配置する必要があります。
  - CA署名付き証明書をシステム証明書に使用する場合は、CAルート証明書と信頼チェーン内のすべての中間証明書も PAN の信頼できる証明書ストアに配置する必要があります。
- セキュアな LDAP 認証を有効にするには、SSL を経由してアクセスされる LDAP ID ソースを定義するときに、証明書ストアから証明書を選択する必要があります。
- パーソナル デバイス ポータルを使用してネットワークへの登録を準備しているパーソナル デバイスに配信するため。Cisco ISE は、パーソナルデバイスの登録をサポートするために、PSN に SCEP を実装しています。登録するデバイスは、SCEP プロトコルを使用して PSN からクライアント証明書を要求します。PSN には、仲介として機能する登録局（RA）が含まれています。RA は、登録するデバイスからの要求を受信して検証した後、クライアント証明書を発行する外部 CA または内部 Cisco ISE CA にその要求を転送します。CA は RA に証明書を返し、RA が証明書をデバイスに返します。

  Cisco ISE によって使用される各 SCEP CA は、SCEP RA プロファイルによって定義されます。SCEP RA のプロファイルが作成されると、次の 2 つの証明書が信頼できる証明書ストアに自動的に追加されます。
  - CA 証明書（自己署名証明書）
  - CA によって署名された RA 証明書（証明書要求のエージェントの証明書）。

  SCEP プロトコルでは、これらの 2 つの証明書が RA によって登録デバイスに提供されている必要があります。信頼できる証明書ストアにこの2つの証明書を配置すると、これらのノードの RA が使用するために、証明書がすべての PSN ノードに複製されます。

（注） SCEP RA プロファイルが削除されると、関連付けられている CA チェーンが信頼できる証明書ストアからも削除されます。ただし、セキュアな syslog、LDAP、システム、または信頼証明書によって同じ証明書が参照されている場合は、SCEP プロファイルだけが削除されます。

（注）

- Cisco ISE にインポートされる X.509 証明書は、PEM 形式か、または識別符号化規則形式である必要があります。証明書チェーン（システム証明書およびその証明書に署名する一連の信頼された証明書）が含まれたファイルはインポートすることができますが、特定の制限の対象となります。
- ゲストポータルに公開ワイルドカード証明書を割り当て、ルート CA 証明書を使用してサブ CA をインポートする場合、Cisco ISE サービスが再起動されるまで証明書チェーンは送信されません。

ISE コミュニティ リソース

ISE へのサードパーティ CA 証明書のインストール

信頼できる証明書ストアの証明書

信頼できる証明書ストアは、次の信頼できる証明書で事前設定されています。製造業者証明書、ルート証明書、その他の信頼できる証明書。ルート証明書（Cisco Root CA）は、製造業者（Cisco CA Manufacturing）証明書に署名します。これらの証明書は、デフォルトでは無効になっています。展開でエンドポイントとして Cisco IP Phone を使用している場合は、ルート証明書と製造業者証明書を有効にすると電話機用にシスコが署名したクライアント証明が認証されます。

信頼できる証明書のリスト

次の表に、管理ノードに追加された信頼できる証明書のリストが表示される **[信頼できる証明書（Trusted Certificates）]** ウィンドウの列を示します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして、**[管理（Administration）]** > **[システム（System）]** > **[証明書（Certificates）]** > **[信頼できる証明書（Trusted Certificates）]** です。

表 *10 : [[*信頼できる証明書（*Trusted Certificates*）*]* ウィンドウの列

フィールド名	使用上のガイドライン
フレンドリ名（**Friendly Name**）	証明書の名前を表示します。
ステータス（**Status**）	この列には **[有効（Enabled）]** または **[無効（Disabled）]** が表示されます。証明書が無効になっている場合、Cisco ISE は信頼の確立に証明書を使用しません。

フィールド名	使用上のガイドライン
信頼対象（**Trusted for**）	証明書を使用する次のサービスのうち、1つ以上を表示します。 • インフラストラクチャ • シスコ サービス • エンドポイント
発行先（**Issued To**）	証明書件名の共通名を表示します。
発行元（**Issued By**）	証明書発行者の共通名を表示します。
有効期限の開始（**Valid From**）	証明書が発行された日付と時刻を表示します。この値は、「Not Before」証明書属性とも呼ばれます。
期限日（**Expiration Date**）	証明書の有効期限が切れる日付と時刻を表示します。この値は、「Not After」証明書属性とも呼ばれます。
有効期限ステータス（**Expiration Status**）	証明書の有効期限のステータスに関する情報です。このコラムに表示される Informational（情報提供）メッセージには 5 つのアイコンとカテゴリがあります。 • **緑色**：期限切れまで 91 日以上 • **青色**：期限切れまで 90 日以内 • **黄色**：期限切れまで 60 日以内 • **オレンジ色**：期限切れまで 30 日以内 • **赤色**: 期限切れ

関連トピック

信頼できる証明書ストア （87 ページ）
信頼できる証明書の表示 （92 ページ）
信頼できる証明書ストアの証明書のステータス変更 （92 ページ）
信頼できる証明書ストアへの証明書の追加 （92 ページ）

信頼できる証明書の命名の制約

CTL の信頼できる証明書には名前の制約の拡張が含まれている場合があります。この拡張は、証明書チェーンの後続のすべての証明書のサブジェクト名とサブジェクト代替名フィールドの値の名前空間を定義します。Cisco ISE は、ルート証明書で指定された制約を検査しません。

Cisco ISE は、次の名前の制約をサポートしています。

- ディレクトリ名

  ディレクトリ名の制約は、サブジェクトのディレクトリ名またはサブジェクトの別名フィールドのプレフィクスです。次に例を示します。

  - 正しいサブジェクト プレフィクス：

    CA 証明書の名前の制約：Permitted: O=Cisco

    クライアント証明書のサブジェクト：O=Cisco,CN=Salomon

  - 不正なサブジェクト プレフィクス：

    CA 証明書の名前の制約：Permitted: O=Cisco

    クライアント証明書のサブジェクト：CN=Salomon,O=Cisco

- DNS
- E メール
- URI（URI の制約は、http://、https://、ftp://、または ldap:// のような URI プレフィクスで始まる必要があります）。

Cisco ISE は、次の名前の制約をサポートしていません。

- IPアドレス
- OtherName

信頼できる証明書にサポートされていない制約が含まれており、検証中の証明書に該当のフィールドが含まれていない場合は、Cisco ISE がサポートされない制約を検証できないため、その証明書は拒否されます。

信頼できる証明書内の名前の制約の定義例を次に示します。

```
X509v3 Name Constraints: critical
                Permitted:
                  othername:<unsupported>
                  email:.abcde.at
                  email:.abcde.be
                  email:.abcde.bg
                  email:.abcde.by
                  DNS:.dir
                  DirName: DC = dir, DC = emea
                  DirName: C = AT, ST = EMEA, L = AT, O = ABCDE Group, OU = Domestic
                  DirName: C = BG, ST = EMEA, L = BG, O = ABCDE Group, OU = Domestic
                  DirName: C = BE, ST = EMEA, L = BN, O = ABCDE Group, OU = Domestic
                 DirName: C = CH, ST = EMEA, L = CH, O = ABCDE Group, OU = Service Z100

                  URI:.dir
                  IP:172.23.0.171/255.255.255.255
                Excluded:
                  DNS:.dir
                  URI:.dir
```

受け入れ可能なクライアント証明書のサブジェクトは、次のように上記の定義に一致します。

```
Subject: DC=dir, DC=emea, OU=+DE, OU=OU-Administration, OU=Users, OU=X1,
CN=cwinwell
```

信頼できる証明書の表示

[信頼できる証明書（Trusted Certificates）] ウィンドウに、Cisco ISE で使用可能なすべての信頼できる証明書が一覧表示されます。信頼できる証明書を表示するには、スーパー管理者またはシステム管理者である必要があります。

始める前に

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

ステップ 1 すべての証明書を表示するには、[メニュー（Menu）] アイコン（☰）をクリックし、**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）]**を選択します。表示される [信頼できる証明書（Trusted Certificates）] ウィンドウにはすべての信頼できる証明書のリストが表示されます。

ステップ 2 [信頼できる証明書（Trusted Certificate）] のチェックボックスをオンにし、[編集（Edit）]、[表示（View）]、[エクスポート（Export）]、または [削除（Delete）] をクリックして必要なタスクを実行します。

信頼できる証明書ストアの証明書のステータス変更

証明書のステータスが有効になっている必要があります。これにより、Cisco ISE が信頼の確立にこの証明書を使用できるようになります。証明書が信頼できる証明書ストアにインポートされると、この証明書は自動的に有効になります。

ステップ 1 Cisco ISE の GUI で、[メニュー（Menu）] アイコン（☰）をクリックし、**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）]** を選択します。

ステップ 2 ISE-PIC GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）]**の順に選択します。

ステップ 3 有効または無効にする証明書の隣にあるチェックボックスをオンにし、[編集（Edit）] をクリックします。

ステップ 4 [ステータス（Status）] ドロップダウン リストからステータス条件を選択します。

ステップ 5 [保存（Save）] をクリックします。

信頼できる証明書ストアへの証明書の追加

[信頼できる証明書ストア（Trusted Certificate Store）] ウィンドウでは、Cisco ISE に CA 証明書を追加できます。

始める前に

- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。
- 追加する証明書は、ブラウザを実行しているコンピュータのファイルシステムにある必要があります。証明書は PEM または DER 形式である必要があります。
- 管理者認証またはEAP認証に証明書を使用するには、基本的な制約を証明書内に定義し、CA フラグを true に設定します。

信頼できる証明書の編集

証明書を信頼できる証明書ストアに追加したら、[編集（Edit）] のオプションを使用して、その証明書をさらに編集できます。

始める前に

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

ステップ 1 Cisco ISE GUI で、**[メニュー（Menu）]** アイコン（☰）をクリックし、**[管理（Administration）]** > **[システム（System）]** > **[証明書（Certificates）]** > **[信頼できる証明書（Trusted Certificates）]**の順に選択します。

ステップ 2 編集する証明書の横にあるチェックボックスをオンにして、[編集（Edit）] をクリックします。

ステップ 3 （オプション）[フレンドリ名（Friendly Name）] フィールドに証明書の名前を入力します。フレンドリ名を指定しない場合、デフォルト名は次の形式で生成されます。

common-name#issuer#nnnnn

ステップ 4 [信頼先（Trusted For）] 領域で必要なチェックボックスをオンにして、証明書の用途を定義します。

ステップ 5 （オプション）[説明（Description）] フィールドに、証明書の説明を入力します。

ステップ 6 [保存（Save）] をクリックします。

信頼できる証明書の設定

次の表では、信頼できる証明書の [編集（Edit）] ウィンドウのフィールドについて説明します。このウィンドウで CA 証明書の属性を編集します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして、**[管理（Administration）]** > **[システム（System）]** > **[証明書（Certificates）]** > **[信頼できる証明書（Trusted Certificates）]** です。編集する信頼できる証明書の横にあるチェックボックスをオンにして、[編集（Edit）] をクリックします。

表 *11* : 信頼できる証明書の編集設定

フィールド名	使用上のガイドライン
証明書発行元（Certificate Issuer）	

フィールド名	使用上のガイドライン
フレンドリ名（**Friendly Name**）	証明書のフレンドリ名を入力します。これはオプションのフィールドです。フレンドリ名を入力しない場合は、次の形式でデフォルト名が生成されます。 *common-name#issuer#nnnnn*
ステータス（**Status**）	ドロップダウンリストから [有効（Enabled）] または [無効（Disabled）] を選択します。証明書が無効になっている場合、Cisco ISE は信頼の確立に証明書を使用しません。
説明（**Description**）	（任意）説明を入力します。
使用方法（Usage）	
ISE 内の認証用に信頼する（Trust for authentication within ISE）	この証明書で（他の Cisco ISE ノードまたは LDAP サーバーからの）サーバー証明書を確認する場合は、このチェックボックスをオンにします。
クライアント認証および **syslog** 用に信頼する（**Trust for client authentication and Syslog**）	（[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た場合に限り適用可能）この証明書を使用して次を行う場合は、このチェックボックスをオンにします。 • EAP プロトコルを使用した Cisco ISE に接続するエンドポイントを認証します。 • syslog サーバーを信頼します。
シスコ サービスの認証用に信頼する（**Trust for authentication of Cisco Services**）	フィードサービスなどの外部シスコサービスを信頼するためにこの証明書を使用する場合は、このチェックボックスをオンにします。

フィールド名	使用上のガイドライン
証明書ステータスの検証（Certificate Status Validation）	Cisco ISE は、特定の CA が発行するクライアントまたはサーバー証明書の失効ステータスをチェックする 2 とおりの方法をサポートしています。1 つめの方法は、Online Certificate Status Protocol（OCSP）を使用して証明書を検証することです（OCSP は、CA によって保持される OCSP サービスに要求を行います）。2 つめの方法は、Cisco ISE に CA からダウンロードした証明書失効リスト（CRL）と照合して証明書を検証することです。どちらの方法も、OCSP を最初に使用してステータスを判断できないときに限り CRL を使用する場合に使用できます。
OCSP サービスに対して検証する（Validate Against OCSP Service）	OCSP サービスに対して証明書を検証するには、このチェックボックスをオンにします。このボックスをオンにするには、まず OCSP サービスを作成する必要があります。
OCSP が不明なステータスを返した場合は要求を拒否する（Reject the request if OCSP returns UNKNOWN status）	証明書ステータスが OCSP サービスによって判断されなかった場合に要求を拒否するには、このチェックボックスをオンにします。このチェックボックスをオンにした場合、OCSP サービスによって不明なステータス値が返されると、Cisco ISE は現在評価しているクライアントまたはサーバー証明書を拒否します。
OCSP応答側が到達不能な場合は要求を拒否する（Reject the request if OCSP Responder is unreachable）	OCSP 応答側が到達不能な場合に Cisco ISE が要求を拒否するには、このチェックボックスをオンにします。
CRL のダウンロード（Download CRL）	Cisco ISE で CRL をダウンロードするには、このチェックボックスをオンにします。
CRL 配信 URL（CRL Distribution URL）	CA から CRL をダウンロードするための URL を入力します。認証局証明書で指定されている場合、このフィールドは自動的に読み込まれます。URL は「http」、「https」、または「ldap」で始まる必要があります。
CRL の取得（Retrieve CRL）	CRL は、自動的または定期的にダウンロードできます。ダウンロードの時間間隔を設定します。

フィールド名	使用上のガイドライン
ダウンロードが失敗した場合は待機する（If download failed, wait）	Cisco ISE が CRL を再度ダウンロードするまでに Cisco ISE に必要な試行を待機する必要がある時間間隔を設定します。
CRL を受信しない場合 CRL 検証をバイパスする（Bypass CRL Verification if CRL is not Received）	このチェックボックスをオンにした場合、クライアント要求は CRL が受信される前に受け入れられます。このチェックボックスをオフにした場合、選択した CA によって署名された証明書を使用するすべてのクライアント要求は、Cisco ISE によって CRL ファイルが受信されるまで拒否されます。
CRL がまだ有効でないか、または期限切れの場合は無視する（Ignore that CRL is not yet valid or expired）	Cisco ISE で開始日と期限日を無視し、まだアクティブでないかまたは期限切れの CRL を引き続き使用し、CRL の内容に基づいて EAP-TLS 認証を許可または拒否する場合は、このチェックボックスをオンにします。 Cisco ISE で [有効日（Effective Date）] フィールドの開始日と [次の更新（Next Update）] フィールドの期限日を CRL ファイルでチェックする場合は、このチェックボックスをオフにします。CRL がまだアクティブではないか、または期限切れの場合、その CA によって署名された証明書を使用するすべての認証は拒否されます。

関連トピック

信頼できる証明書ストア （87 ページ）
信頼できる証明書の編集 （93 ページ）

信頼できる証明書の削除

今後使用しない信頼できる証明書を削除できます。ただし、Cisco ISE 内部 CA 証明書は削除しないでください。Cisco ISE 内部 CA 証明書を削除できるのは、展開全体の Cisco ISE ルート証明書チェーンを置き換える場合のみです。

ステップ 1 **[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）]** を選択します。

ステップ 2 削除する証明書の隣にあるチェックボックスをオンにし、[削除（Delete）] をクリックします。

警告メッセージが表示されます。Cisco ISE 内部 CA 証明書を削除するには、次のいずれかのオプションをクリックします。

- [削除（Delete）]：Cisco ISE 内部 CA 証明書を削除する場合。Cisco ISE 内部 CA によって署名されたすべてのエンドポイント証明書は無効になり、エンドポイントはネットワークに参加できません。エンドポイントをネットワークで再度有効にするには、信頼できる証明書ストアに同じ Cisco ISE 内部 CA 証明書をインポートします。
- [削除および取消（Delete & Revoke）]：Cisco ISE 内部 CA 証明書を削除して取り消します。Cisco ISE 内部 CA によって署名されたすべてのエンドポイント証明書は無効になり、エンドポイントはネットワークにアクセスできません。この操作は取り消すことができません。展開全体の Cisco ISE ルート証明書チェーンを置き換える必要があります。

ステップ 3 [はい（Yes）] をクリックして、証明書を削除します。

信頼できる証明書ストアからの証明書のエクスポート

始める前に

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

（注） 内部 CA から証明書をエクスポートし、そのエクスポートされた証明書を使用してバックアップから復元する場合は、CLI コマンド **application configure ise** を使用する必要があります。Cisco ISE CA 証明書およびキーのエクスポート （140 ページ）を参照してください。

ステップ 1 Cisco ISE の GUI で、[メニュー（Menu）] アイコン（☰）をクリックし、**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）]** を選択します。

ステップ 2 エクスポートする証明書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）] をクリックします。一度に 1 つの証明書のみをエクスポートできます。

ステップ 3 選択した証明書は、クライアントブラウザを実行しているファイルシステムに PEM 形式でダウンロードされます。

信頼できる証明書ストアへのルート証明書のインポート

ルート CA 証明書および中間 CA 証明書をインポートするとき、信頼できる CA 証明書を使用する対象のサービスを指定できます。

外部ルート CA 証明書をインポートするときに、次のタスクのステップ 5 で、[管理者認証に基づく証明書への信頼（Trust for certificate based admin authentication）] オプションを有効にします。

始める前に

証明書署名要求に署名し、デジタルで署名された CA 証明書を返した CA のルート証明書と他の中間証明書が必要です。

ステップ 1 Cisco ISE の GUI で、[メニュー（Menu）] アイコン（☰）をクリックし、**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）]** 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 [証明書ストアへの新しい証明書のインポート（Import a new Certificate into the Certificate Store）] ウィンドウで、[ファイルの選択（Choose File）] をクリックし、CA によって署名され、返されたルート CA 証明書を選択します。

ステップ 4 **[フレンドリ名（Friendly Name）]**を入力します。

[フレンドリ名（Friendly Name）]を入力しないと、Cisco ISE により、このフィールドには、*common-name#issuer#nnnnn* 形式（、*nnnnn* は一意の番号）で名前が自動的に入力されます。後で証明書を編集して、[フレンドリ名（Friendly Name）] を変更できます。

ステップ 5 この信頼できる証明書を使用するサービ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 6 （任意）[説明（Description）] フィールドに証明書の説明を入力します。

ステップ 7 [送信（Submit）] をクリックします。

次のタスク

信頼できる証明書ストアに中間 CA 証明書をインポートします（該当する場合）。

信頼できる証明書のインポート設定

次の表では、CA 証明書を Cisco ISE に追加するために使用できる [信頼できる証明書のインポート（Trusted Certificate Import）] ウィンドウのフィールドについて説明します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして、**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）] > [インポート（Import）]**の順に選択します。

表 *12 :* 信頼できる証明書のインポート設定

フィールド名	説明
証明書ファイル（Certificate file）	[参照（Browse）] をクリックして、ブラウザを実行しているコンピュータから証明書ファイルを選択します。
フレンドリ名（Friendly Name）	証明書のフレンドリ名を入力します。名前を指定しない場合は、Cisco ISE により <common name>#<issuer>#<nnnnn> の形式で自動的に名前が作成されます。ここで、<nnnnn> は固有の 5 桁の数値です。

フィールド名	説明
ISE 内の認証用に信頼する（Trust for authentication within ISE）	この証明書を（他の ISE ノードまたは LDAP サーバーから）サーバー証明書の検証に使用する場合は、このチェックボックスをオンにします。
クライアント認証および syslog 用に信頼する（Trust for client authentication and Syslog）	（[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た場合に限り適用可能）この証明書を使用して次を行う場合は、このチェックボックスをオンにします。 • EAP プロトコルを使用した ISE に接続するエンドポイントの認証 • syslog サーバーの信頼
シスコ サービスの認証用に信頼する（Trust for authentication of Cisco Services）	フィードサービスなどの外部シスコ サービスを信頼するためにこの証明書を使用する場合は、このチェックボックスをオンにします。
証明書の拡張の検証（Validate Certificate Extensions）	（[クライアント認証用に信頼する（Trust for client authentication）] オプションと [証明書拡張の検証を有効にする（Enable Validation of Certificate Extensions）] オプションの両方をオンにした場合のみ）「keyUsage」拡張が存在し、「keyCertSign」ビットが設定されていることと、CA フラグが true に設定された基本制約拡張が存在することを確認します。
説明（Description）	任意で説明を入力します。

関連トピック

信頼できる証明書ストア （87 ページ）
証明書チェーンのインポート （99 ページ）
信頼できる証明書ストアへのルート証明書のインポート （97 ページ）

証明書チェーンのインポート

証明書ストアから受信した証明書チェーンを含む単一のファイルから、複数の証明書をインポートすることができます。ファイル内のすべての証明書は PEM の形式であり、証明書は次の順序に並べられている必要があります。

- ファイル内の最後の証明書は、CA によって発行されたクライアント証明書またはサーバー証明書である必要があります。

- 前にあるすべての証明書は、ルート CA 証明書と、発行された証明書の署名のチェーンにあるすべて中間 CA 証明書である必要があります。

証明書チェーンのインポートは、次の 2 ステップのプロセスです。

1. Cisco ISE 管理ポータルで信頼できる証明書ストアに証明書チェーンファイルをインポートします。この操作により、最後の 1 つを除き、すべての証明書がファイルから信頼できる証明書ストアにインポートされます。
2. CA 署名付き証明書のバインド操作を使用して証明書チェーン ファイルをインポートします。この操作により、最後の証明書がローカル証明書としてファイルからインポートされます。

Cisco ISE ノード間通信の信頼できる証明書のインストール

展開をセットアップする場合、セカンダリノードを登録する前に、セカンダリノードの管理者証明書の検証に使用される適切な CA 証明書を PAN の CTL に配置する必要があります。PAN の CTL に入力する手順は、シナリオに応じて異なります。

- セカンダリノードが Cisco ISE 管理ポータルとの通信に CA 署名付き証明書を使用する場合は、セカンダリノードの CA 署名付き証明書、関連する中間証明書（ある場合）、および（セカンダリノードの証明書に署名した CA の）ルート CA 証明書を PAN の CTL にインポートする必要があります。
- セカンダリノードが Cisco ISE 管理ポータルとの通信に自己署名証明書を使用する場合は、PAN の CTL にセカンダリノードの自己署名証明書をインポートできます。

（注）

- 登録されたセカンダリノードの管理者証明書を変更する場合は、セカンダリノードの管理者証明書の検証に使用できる適切な CA 証明書を取得し、PAN の CTL にインポートする必要があります。
- 展開内でクライアントと PSN の間のセキュアな通信に自己署名証明書を使用する場合、BYOD ユーザーがある場所から別の場所に移動すると、EAP-TLS ユーザー認証は失敗します。一部の PSN 間で提供される必要があるこのような認証要求の場合、外部で署名された CA 証明書を使用してクライアントと PSN の間の通信を保護するか、または外部の CA によって署名されたワイルドカード証明書を使用する必要があります。

外部 CA から発行された証明書に基本制約が定義されており、CA フラグが true に設定されていることを確認します。ノード間通信用の CA 署名付き証明書のインストール：

ステップ 1 証明書署名要求の作成と認証局への送信 （106 ページ）

ステップ 2 信頼できる証明書ストアへのルート証明書のインポート （97 ページ）
ステップ 3 証明書署名要求への CA 署名付き証明書のバインド （106 ページ）

Cisco ISE でのデフォルトの信頼できる証明書

Cisco ISE の信頼できる証明書ストア（[メニュー（Menu）] （☰）アイコンをクリックし、**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）]**を選択）には、デフォルトで使用可能な証明書がいくつか含まれています。これらの証明書は、セキュリティ要件を満たすためにストアに自動的にインポートされます。ただし、これらすべてを使用する必要はありません。次の表に記載されている場合を除き、すでに使用可能になっている証明書ではなく、自分で選択した証明書を使用できます。

表 *13* : デフォルトの信頼できる証明書

信頼できる証明書の名前	シリアル番号	証明書の目的	証明書を含む Cisco ISE リリース
Baltimore CyberTrust Root CA	02 00 00 B9	この証明書は、一部の地域で cisco.com が使用する CA チェーン内のルート CA 証明書として機能することができます。また、この証明書は、https://s3.amazonaws.com でホストされている ISE 2.4 のポスチャ/CP 更新 XML ファイルでも使用されていました。	リリース 2.4 以降。
DST Root CA X3 Certificate Authority	44 AF B0 80 D6 A3 27 BA 89 30 39 86 2E F8 40 6B	この証明書は、cisco.com が使用する CA チェーンのルート CA 証明書として機能することができます。	リリース 2.4 以降。
Thawte Primary Root CA	34 4E D5 57 20 D5 ED EC 49 F4 2F CE 37 DB 2B 6D	この証明書は、cisco.com と perfigo.com が使用する CA チェーンのルート CA 証明書として機能することができます。	リリース 2.4 以降。

信頼できる証明書の名前	シリアル番号	証明書の目的	証明書を含む Cisco ISE リリース
VeriSign Class 3 Public Primary Certification Authority	18 DA D1 9E 26 7D E8 BB 4A 21 58 CD CC 6B 3B 4A	この証明書は、VeriSign Class 3 Secure Server CA-G3 のルート CA 証明書として機能します。 Cisco ISE でプロファイラ フィード サービスを設定する場合は、この証明書を使用する必要があります。	リリース 2.4 以降。
VeriSign Class 3 Secure Server CA - G3	6E CC 7A A5 A7 03 20 09 B8 CE BC F4 E9 52 D4 91	これは、2020 年 2 月 7 日に期限切れになる中間 CA 証明書です。この証明書を更新する必要はありません。 証明書を削除するには、下記のタスクを実行します。	リリース 2.4 以降。
Cisco CA Manufacturing	6A 69 67 B3 00 00 00 00 00 03	この証明書は、Cisco ISE に接続している特定のシスコデバイスが使用する場合があります。この証明書はデフォルトでは無効になっています。	リリース 2.4 および 2.6。
Cisco Manufacturing CA SHA2	02	この証明書は、管理者認証、エンドポイント認証、および展開インフラストラクチャフローの CA チェーン内で使用できます。	リリース 2.4 以降。
Cisco Root CA 2048	5F F8 7B 28 2B 54 DC 8D 42 A3 15 B5 68 C9 AD FF	この証明書は、Cisco ISE に接続している特定のシスコデバイスが使用することができます。この証明書はデフォルトでは無効になっています。	リリース 2.4 以降。

信頼できる証明書の名前	シリアル番号	証明書の目的	証明書を含むCisco ISEリリース
Cisco Root CA M2	01	この証明書は、管理者認証、エンドポイント認証、および展開インフラストラクチャフローのCAチェーン内で使用できます。	リリース 2.4 以降。
DigiCert Root CA	02 AC 5C 26 6A 0B 40 9B 8F 0B 79 F2 AE 46 25 77	Facebookを使用したゲストログインを使用しているフローには、この証明書を使用する必要があります。	リリース 2.4 以降。
DigiCert SHA2 High Assurance Server CA	04 E1 E7 A4 DC 5C F2 F3 6D C0 2B 42 B8 5D 15 9F	Facebookを使用したゲストログインを使用しているフローには、この証明書を使用する必要があります。	リリース 2.4 以降。
HydrantID SSL ICA G2	75 17 16 77 83 D0 43 7E B5 56 C3 57 94 6E 45 63 B8 EB D3 AC	シスコサービスで信頼されています。	リリース 2.4 および 2.6。
QuoVadis Root CA 2	05 09	この証明書は、プロファイラ、ポスチャ、およびクライアントプロビジョニングフロー内で使用する必要があります。	リリース 2.4 以降。
Cisco ECC Root CA	01	この証明書は、Cisco ISE で使用されるシスコの信頼ルートストアバンドルの一部です。	リリース 2.6。
Cisco Licensing Root CA	01	この証明書は、Cisco ISE で使用されるシスコの信頼ルートストアバンドルの一部です。	リリース 2.6 以降。
Cisco Root CA 2099	01 9A 33 58 78 CE 16 C1 C1	この証明書は、Cisco ISE で使用されるシスコの信頼ルートストアバンドルの一部です。	リリース 2.6 以降。

信頼できる証明書の名前	シリアル番号	証明書の目的	証明書を含む Cisco ISE リリース
Cisco Root CA M1	2E D2 0E 73 47 D3 33 83 4B 4F DD 0D D7 B6 96 7E	この証明書は、Cisco ISE で使用されるシスコの信頼ルートストアバンドルの一部です。	リリース 2.6 以降。
Cisco RXC-R2	01	この証明書は、Cisco ISE で使用されるシスコの信頼ルートストアバンドルの一部です。	リリース 2.6 以降。
DigiCert Global Root CA	08 3B E0 56 90 42 46 B1 A1 75 6A C9 59 91 C7 4A	この証明書は、Cisco ISE で使用されるシスコの信頼ルートストアバンドルの一部です。	リリース 2.6 以降。
Cisco ECC Root CA 2099	03	この証明書は、Cisco ISE で使用されるシスコの信頼ルートストアバンドルの一部です。	リリース 2.6 以降。

Cisco ISE からのデフォルトの信頼できる証明書の削除

- 信頼できるすべての証明書を表示するには、Cisco ISE の GUI で、[メニュー（Menu）] アイコン（☰）をクリックし、**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）]** を選択します。
- 削除する証明書をエクスポートして保存します。これにより、必要に応じて再度インポートできるようになります。

  エクスポートする証明書のチェックボックスをクリックし、上にあるメニューバーの [エクスポート（Export）] をオンにします。キーチェーンがシステムにダウンロードされます。
- 証明書を削除します。削除する証明書のチェックボックスをオンにし、上部のメニューバーの [削除（Delete）] をクリックします。CA チェーン、セキュアな syslog、またはセキュアな LDAP によって使用されている場合は、その証明書を削除することはできません。
- CA チェーン、セキュアな syslog、および それが含まれている syslog から証明書を削除するために必要な設定変更を行います。その後で、証明書を削除します。
- 証明書を削除したら、関連するサービス（証明書の目的を参照）が想定どおりに動作していることを確認します。

古いシステムと信頼できる証明書

古い証明書は、展開内のどのノードにも属していない証明書です。これらの冗長な証明書は、システムおよび信頼できる証明書ストアに大量に蓄積される可能性があり、メモリ不足と遅延の問題につながります。Cisco ISE リリース 3.1 以降、そのような冗長な証明書は **[古い証明書（Stale Certificate）]** ステータスを持ち、それらを確認して削除できるようになりました。

古いシステム証明書と信頼できる証明書の確認

古いシステム証明書と信頼できる証明書を識別するために、次のチェックが実行されます。

古いシステム証明書	古い信頼できる証明書
• **[発行先（Issued To）]** フィールドをチェックして、展開内のいずれかのノードのホスト名が発行されたシステム証明書の一部であるかどうかを確認します。一致するものがない場合、システム証明書は古いと見なされます。 • 発行されたシステム証明書の **[SAN拡張（SAN Extension）]** フィールドは、展開内のノードの FQDN と一致する必要があります。一致するものがない場合、システム証明書は古いと見なされます。 （注） ワイルドカード証明書は、古い証明書の検証を受けません。	• 内部 CA 証明書のステータスを確認するときに、ステータスが **[非アクティブ（Inactive）]** と表示され、**[StatusChangeReason]** が **[CertSuperseded]** の場合、信頼できる証明書は古いと見なされます。 • [発行先（Issued To）] フィールドをチェックして、展開内のいずれかのノードのホスト名が発行された信頼できる証明書の一部であるかどうかを確認します。一致するものがない場合、信頼できる証明書は古いと見なされます。

証明書署名要求

CA が署名付き証明書を発行するには、証明書署名要求を作成して CA に送信する必要があります。

作成した証明書署名要求のリストは、**[証明書署名要求（Certificate-Signing Requests）]** ウィンドウに表示されます。このウィンドウを表示するには、**[メニュー（Menu）]** アイコン（☰）をクリックし、**[管理（Administration）]** > **[システム（System）]** > **[証明書（Certificates）]** > **[証明書署名要求（Certificate-Signing Requests）]**。CA から署名を取得するには、証明書署名要求をエクスポートし、その証明書を CA に送信する必要があります。証明書は CA によって署名され、返されます。

Cisco ISE の管理ポータルから証明書を一元的に管理できます。展開内のすべてのノードの証明書署名要求を作成し、それらをエクスポートできます。その後、証明書署名要求を CA に送信し、CA から署名付き証明書を取得し、CA によって返されたルートおよび中間 CA 証明書を信頼できる証明書ストアにインポートし、証明書署名要求に CA 署名付き証明書をバインドする必要があります。

証明書署名要求の作成と認証局への送信

証明書署名要求（CSR）を生成して、展開内のノードの CA 署名付き証明書を取得できます。展開内の特定のノードまたは展開内のすべてのノード用の証明書署名要求（CSR）を生成できます。

ステップ 1 **[管理（Administration）]** > **[システム（System）]** > **[証明書（Certificates）]** > **[証明書署名要求（Certificate Signing Requests）]** を選択します。

ステップ 2 **[証明書署名要求（CSR）の生成（Generate Certificate-Signing Requests (CSR)）]** をクリックして、証明書署名要求を生成します。

ステップ 3 証明書署名要求を生成するための値を入力します。表示されるウィンドウの各フィールドについては、信頼できる証明書の設定 （93 ページ）を参照してください。

ステップ 4 （オプション）ダウンロードする署名要求のチェックボックスをオンにし、**[エクスポート（Export）]** をクリックして要求をダウンロードします。

ステップ 5 「 **-----BEGIN CERTIFICATE REQUEST-----** 」から「 **-----END CERTIFICATE REQUEST-----** 」までのすべてのテキストをコピーし、選択した CA の証明書要求に要求の内容を貼り付けます。

ステップ 6 署名済みの証明書をダウンロードします。

CA によっては、署名付き証明書が電子メールで送信される場合があります。署名付き証明書は、zip ファイルの形式で、Cisco ISE の信頼できる証明書ストアに追加する必要がある、新規発行の証明書と CA のパブリック署名証明書が含まれています。デジタル署名された CA 証明書、ルート CA 証明書、および他の中間 CA 証明書（該当する場合）をクライアントブラウザを実行するローカルシステムにダウンロードできます。

証明書署名要求への CA 署名付き証明書のバインド

CA がデジタル署名付き証明書を返してから、その証明書を証明書署名要求にバインドする必要があります。Cisco ISE 管理者ポータルから展開内のすべてのノードに対してバインド操作を実行できます。

始める前に

- デジタル署名付き証明書、および関連するルート中間 CA 証明書を CA から受け取る必要があります。
- 信頼できる証明書ストアに関連するルート CA 証明書と中間 CA 証明書をインポートします（**[メニュー（Menu）]** アイコン（☰）をクリックし、**[管理（Administration）]** > **[システム（System）]** > **[証明書（Certificates）]** > **[信頼できる証明書（Trusted Certificates）]** を選択します）。

ステップ 1 **[管理（Administration）]** > **[システム（System）]** > **[証明書（Certificates）]** > **[証明書署名要求（Certificate Signing Requests）]** を選択します。

ステップ 2 CA 署名付き証明書とバインドする必要がある証明書署名要求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 **[証明書のバインド（Bind Certificate）]** をクリックします。

ステップ 4 表示される [CA 署名付き証明書（Bind CA Signed Certificate）] ウィンドウで、**[ファイルの選択（Choose File）]** をクリックし、CA 署名付き証明書を選択します。

ステップ 5 [フレンドリ名（Friendly Name）] フィールドに値を入力します。

ステップ 6 Cisco ISE に証明書の拡張の検証を許可する場合は、[証明書の拡張の検証（Validate Certificate Extensions）] チェックボックスをオンにします。

[証明書の拡張の検証（Validate Certificate Extensions）] オプションが有効になっており、インポートする証明書に CA フラグが True に設定された基本制約拡張が含まれている場合は、キー使用拡張が存在すること、および keyEncipherment ビットと keyAgreement ビットのいずれかまたは両方が設定されていることを確認します。

（注） Cisco ISE では、EAP-TLS クライアント証明書にデジタル署名のキー使用拡張を使用する必要があります。

ステップ 7 （オプション）[使用方法（Usage）] 領域で、この証明書が使用されるサービスをオンにします。

この情報は、証明書署名要求の生成時に [使用方法（Usage）] オプションを有効にした場合は自動入力されます。また、後で証明書を編集して使用方法を指定することもできます。

プライマリ PAN で使用方法が **[管理者（Admin）]** の証明書を変更すると、他のすべてのノードでサービスが再起動します。プライマリ PAN 再起動後にシステムは一度に 1 つのノードを再起動します。

ステップ 8 **[送信（Submit）]** をクリックして証明書署名要求を CA 署名付き証明書とバインドします。

この証明書の使用方法が Cisco ISE ノード間通信用としてマークされている場合は、Cisco ISE ノードのアプリケーションサーバーが再起動します。

このプロセスを繰り返して、証明書署名要求と展開内の他のノード上の CA 署名付き証明書をバインドします。

次のタスク

信頼できる証明書ストアへのルート証明書のインポート （97 ページ）

証明書署名要求のエクスポート

始める前に

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

ステップ 1 **[管理（Administration）]** > **[システム（System）]** > **[証明書（Certificates）]** > **[証明書署名要求（Certificate Signing Requests）]** を選択します。

ステップ 2 エクスポートする証明書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）] をクリックします。

ステップ 3 証明書署名要求がローカルファイルシステムにダウンロードされます。

証明書署名要求の設定

Cisco ISE では、1 つの要求で、管理者ポータルから展開内のすべてのノードの証明書署名要求を生成することができます。また、展開内の単一ノードか、または複数両方のノードのどちらの証明書署名要求を生成するのかを選択することもできます。単一ノードの証明書署名要求を生成する場合、ISE は証明書サブジェクトの [CN=] フィールドの特定ノードの完全修飾ドメイン名（FQDN）を自動的に置き換えます。証明書の [サブジェクト代替名（Subject Alternative Name (SAN)）] フィールドにエントリを含めることを選択した場合、他の SAN 属性に加えて ISE ノードの FQDN を入力する必要があります。展開内のすべてのノードの証明書署名要求を生成することを選択した場合は、[ワイルドカード証明書の許可（Allow Wildcard Certificates）] チェックボックスをオンにして、[SAN] フィールド（DNS 名）にワイルドカード表記で FQDN を入力します（*.amer.example.com など）。EAP 認証に証明書を使用する場合は、[CN=] フィールドにワイルドカード値を入力しないでください。

ワイルドカード証明書を使用することにより、各 Cisco ISE ノードに固有の証明書を生成する必要がなくなります。また、証明書の警告を防ぐために、SAN フィールドに複数の FQDN 値を入力する必要もありません。SAN フィールドでアスタリスク（*）を使用すると、展開内の複数の両方のノードで単一の証明書を共有できるようになり、証明書名の不一致による警告を防止することができます。ただし、ワイルドカード証明書は、各 Cisco ISE ノードに固有のサーバー証明書を割り当てる場合よりも安全性が低いと見なされます。

次の表では、認証局（CA）が署名可能な証明書署名要求の生成に使用できる [証明書署名要求（Certificate Signing Request）] ページのフィールドについて説明します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして、**[管理（Administration）]** > **[システム（System）]** > **[証明書（Certificates）]** > **[証明書管理（Certificate Management）]** > **[証明書署名要求（Certificate Signing Request）]** の順に選択します。

表 *14 :* 証明書署名要求の設定

フィールド	使用上のガイドライン
証明書の用途（**Certificate(s) will be used for**）	

フィールド	使用上のガイドライン
	証明書を使用するサービスを選択します。 **Cisco ISE ID 証明書** • [複数使用（Multi-Use）]：複数のサービス（管理者、EAP-TLS認証、pxGrid、およびポータル）に使用されます。複数使用の証明書は、クライアントとサーバー両方のキーの用途を使用します。署名 CA の証明書テンプレートは、コンピュータまたはマシン証明書テンプレートと呼ばれます。このテンプレートには、次のプロパティがあります。 • [キーの用途（Key Usage）]：デジタル署名（署名） • [キーの拡張用途（Extended Key Usage）]：TLS Web サーバー認証（1.3.6.1.5.5.7.3.1）および TLS Web クライアント認証（1.3.6.1.5.5.7.3.2） • [管理者（Admin）]：サーバー認証に使用されます（管理者ポータルとの通信および展開内の ISE ノード間の通信を保護するため）。署名 CA の証明書テンプレートは、Web サーバー証明書テンプレートと呼ばれます。このテンプレートには、次のプロパティがあります。 • [キーの用途（Key Usage）]：デジタル署名（署名） • [キーの拡張用途（Extended Key Usage）]：TLS Web サーバー認証（1.3.6.1.5.5.7.3.1） • [EAP 認証（EAP Authentication）]：サーバー認証に使用されます。署名 CA の証明書テンプレートは、コンピュータまたはマシン証明書テンプレートと呼ばれます。このテンプレートには、次のプロパティがあります。 • [キーの用途（Key Usage）]：デジタル署名（署名） • [キーの拡張用途（Extended Key Usage）]：TLS Web サーバー認証（1.3.6.1.5.5.7.3.1） （注） EAP-TLS クライアント証明書にデジタル署名キー使用法を使用する必要があります。 • [RADIUS DTLS]：RADIUS DTLS サーバーの認証に使用されます。このテンプレートには、次のプロパティがあります。 • [キーの用途（Key Usage）]：デジタル署名（署名） • [キーの拡張用途（Extended Key Usage）]：TLS Web サーバー認証（1.3.6.1.5.5.7.3.1） • [ISEメッセージングサービス（ISE Messaging Service）]：Cisco ISE

フィールド	使用上のガイドライン
	メッセージングを介したSyslog機能に使用されます。組み込みのUDP syslog収集ターゲット（LogCollectorおよびLogCollector2）用のMnT WAN存続を有効にします。 • [キーの用途（Key Usage）]：デジタル署名（署名） • [キーの拡張用途（Extended Key Usage）]：TLS Webサーバー認証（1.3.6.1.5.5.7.3.1） • [ポータル（Portal）]：サーバー認証に使用されます（すべてのISE Webポータルとの通信を保護するため）。署名CAの証明書テンプレートは、コンピュータまたはマシン証明書テンプレートと呼ばれます。このテンプレートには、次のプロパティがあります。 • [キーの用途（Key Usage）]：デジタル署名（署名） • [キーの拡張用途（Extended Key Usage）]：TLS Webサーバー認証（1.3.6.1.5.5.7.3.1） • [pxGrid]：クライアント認証とサーバー認証の両方に使用されます（pxGridクライアントとサーバー間の通信を保護するため）。署名CAの証明書テンプレートは、コンピュータまたはマシン証明書テンプレートと呼ばれます。このテンプレートには、次のプロパティがあります。 • [キーの用途（Key Usage）]：デジタル署名（署名） • [キーの拡張用途（Extended Key Usage）]：TLS Webサーバー認証（1.3.6.1.5.5.7.3.1）およびTLS Webクライアント認証（1.3.6.1.5.5.7.3.2） • [SAML]：SAML IDプロバイダ（IdP）とのセキュア通信に使用するサーバー証明書。SAMLでの使用を目的とした証明書は、管理者認証やEAP認証などのその他のサービスのために使用することはできません。 • [キーの用途（Key Usage）]：デジタル署名（署名） • [キーの拡張用途（Extended Key Usage）]：TLS Webサーバー認証（1.3.6.1.5.5.7.3.1）

フィールド	使用上のガイドライン

	（注） 拡張キーの使用状況属性に任意の目的のオブジェクト識別子のための 2.5.29.37.0 の値が含まれている証明書を使用しないことをお勧めします。拡張キーの使用状況属性に任意の目的のオブジェクト識別子のための 2.5.29.37.0 の値が含まれている証明書を使用する場合、証明書は無効と見なされ、次のエラー メッセージが表示されます。
	`source=local ; type=fatal ; message="unsupported certificate"`
	
	Cisco ISE 認証局証明書
	• [ISE ルート CA（ISE Root CA）]：（内部 CA サービスにのみ適用可能）プライマリ PAN のルート CA および PSN の下位 CA を含む内部 CA 証明書チェーン全体を再生成するために使用されます。
	• [ISE 中間 CA（ISE Intermediate）]：（ISE が外部 PKI の中間 CA として機能する場合に内部CAサービスにのみ適用可能）プライマリ PAN の中間 CA 証明書および PSN の下位 CA 証明書の生成に使用されます。署名 CA の証明書テンプレートは、下位認証局と呼ばれます。このテンプレートには、次のプロパティがあります。
	  • [基本制約（Basic Constraints）]：重要、認証局
	  • [キーの用途（Key Usage）]：証明書の署名、デジタル署名
	  • [キーの拡張用途（Extended Key Usage）]：OCSP 署名（1.3.6.1.5.5.7.3.9）
	• [ISE OCSP 応答側証明書の更新（Renew ISE OCSP Responder Certificates）]：（内部CAサービスにのみ適用可能）展開全体のISE OCSP応答側証明書の更新に使用されます（証明書署名要求ではありません）。セキュリティ上の理由から、ISE OCSP 応答側証明書を 6 ヵ月ごとに更新することを推奨します。

ワイルドカード証明書の許可（Allow Wildcard Certificates）	証明書の [SAN] フィールドの CN/DNS 名にワイルドカード文字（*）を使用するには、このチェックボックスをオンにします。このチェックボックスをオンにすると、展開内のすべてのノードが自動的に選択されます。左端のラベルの位置にアスタリスク（*）ワイルドカード文字を使用する必要があります。ワイルドカード証明書を使用する場合は、セキュリティを強化するためにドメイン領域を分割することを推奨します。たとえば、*.example.com の代わりに *.amer.example.com を使用して領域を分割することができます。ドメインを分割しないと、セキュリティ上の問題が発生する可能性があります。

フィールド	使用上のガイドライン
これらのノードの CSR の生成（Generate CSRs for these Nodes）	証明書を生成するノードの隣のチェックボックスをオンにします。展開内の選択されたノードの CSR を生成するには、[ワイルドカード証明書の許可（Allow Wildcard Certificates）] オプションをオフにします。
共通名（Common Name）（CN）	デフォルトでは、共通名は証明書署名要求を生成する ISE ノードの FQDN です。$FQDN$ は ISE ノードの FQDN を意味します。展開内の複数ノードの証明書署名要求を生成すると、証明書署名要求の [共通名（Common Name）] フィールドは各 ISE ノードの FQDN に置き換えられます。
組織ユニット（Organization Unit）（OU）	組織ユニット名。Engineering など。
組織（Organization）（O）	組織名。Cisco など。
都市（City）（L）	（省略不可）都市名。San Jose など。
州（State）（ST）	（省略不可）州名。California など。
国（Country）（C）	国名。2 文字の ISO 国番号を入力する必要があります。US など。
サブジェクト代替名（Subject Alternative Name）（SAN）	証明書に関連付けられている IP アドレス、DNS 名、Uniform Resource Identifier（URI）、またはディレクトリ名。 • [DNS 名（DNS Name）]：DNS 名を選択した場合は、ISE ノードの完全修飾ドメイン名を入力します。[ワイルドカード証明書の許可（Allow Wildcard Certificates）] オプションをオンにした場合は、ワイルドカード表記（ドメイン名の前にアスタリスクとピリオドを入力）を指定します。*.amer.example.com など。 • [IP アドレス（IP Address）]：証明書に関連付けられる ISE ノードの IP アドレス。 • [ユニフォーム リソース識別子（Uniform Resource Identifier）]：証明書に関連付ける URI。 • [ディレクトリ名（Directory Name）]：RFC 2253 に従って定義される識別名（DN）の文字列表現。DN 間はカンマ（,）で区切ります。「dnQualifier」RDN の場合は、カンマをエスケープし、区切り文字としてバックスラッシュ カンマ「\,」を使用します。たとえば、CN=AAA,dnQualifier=O=Example\,DC=COM,C=IL などです。

フィールド	使用上のガイドライン
キータイプ（Key Type）	RSA または ECDSA の公開キーの作成に使用するアルゴリズムを指定します。
キーの長さ（Key Length）	公開キーのビット サイズを指定します。 RSA には、次のオプションを使用できます。 • 512 • 1024 • 2048 • 4096 ECDSA には、次のオプションを使用できます。 • 256 • 384 （注） RSA および ECDSA の公開キーは、同じセキュリティ レベルで異なるキー長を持つことがあります。 パブリック CA の署名付き証明書を取得するか、FIPS 準拠ポリシー管理システムとして Cisco ISE を展開する場合は 2048 以上を選択します。
署名するダイジェスト（Digest to Sign With）	ハッシュ アルゴリズム SHA-1 または SHA-256 を選択します。
証明書ポリシー（Certificate Policies）	証明書が従うべき証明書ポリシーの OID または OID のリストを入力します。OID を区切るには、カンマまたはスペースを使用します。

関連トピック

証明書署名要求 （105 ページ）
証明書署名要求の作成と認証局への送信 （106 ページ）
証明書署名要求への CA 署名付き証明書のバインド （106 ページ）

ポータルで使用する証明書のセットアップ

Web ポータル要求を処理できる展開に複数の PSN がある場合、Cisco ISE には一意の ID が必要です。この ID で、ポータルの通信に使用する必要がある証明書を識別します。ポータルでの使用に指定された証明書を追加またはインポートする場合、証明書グループタグを定義して、それを展開内の各ノードの対応する証明書に関連付けます。この証明書グループタグを対応するエンドユーザーポータル（ゲスト、スポンサー、およびパーソナルデバイスポータル）に関連付けます。この証明書グループタグは一意の ID で、Cisco ISE が各ポータルと通信する

際に使用する必要がある証明書を識別する場合に役立ちます。ポータルごとに各ノードから指定できる証明書は 1 つのみです。

（注） Cisco ISE は TCP ポート 8443（またはポータルが使用するように設定したポート）でポータル証明書を提示します。

ステップ 1 証明書署名要求の作成と認証局への送信 （106 ページ）。

すでに定義済みの証明書グループ タグを選択するか、ポータル用に新しく作成する必要があります。たとえば、mydevicesportal などです。

ステップ 2 信頼できる証明書ストアへのルート証明書のインポート （97 ページ）。

ステップ 3 証明書署名要求への CA 署名付き証明書のバインド （106 ページ）。

CA 署名付き証明書へのデフォルトのポータル証明書グループ タグの再割り当て

デフォルトでは、すべての Cisco ISE ポータルは自己署名証明書を使用します。ポータルに CA 署名付き証明書を使用する場合は、デフォルトのポータル証明書グループ タグを CA 署名付き証明書に割り当てることができます。既存の CA 署名付き証明書を使用するか、または CSR を生成して、ポータルに使用する新しい CA 署名付き証明書を取得できます。1 つの証明書から別の証明書にポータル グループ タグを再割り当てすることができます。

（注） 既存の証明書を編集する場合、証明書に関連付けられているポータル タグ（ゲスト）がいずれかのポータルですでに使用されている場合は、デフォルトのポータル証明書グループ タグまたは他のポータル グループ タグをこの証明書に再割り当てすることはできません。「ゲスト」ポータル タグを使用しているポータルのリストが表示されます。

次に、CA 署名付き証明書にデフォルトのポータル証明書グループ タグを再割り当てする手順について説明します。

ステップ 1 **[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [システム証明書（System Certificates）]** を選択します。

このタグを使用するポータルのリストを表示するには、デフォルトのポータル証明書グループ タグの横にある i アイコンにマウス ポインタを合わせます。このタグが割り当てられているポータル証明書がある展開内の ISE ノードを表示することもできます。

ステップ 2 ポータルに使用する CA 署名付き証明書の横にあるチェックボックスをオンにして、[編集（Edit）] をクリックします。

いずれのポータルでも使用されていない CA 署名付き証明書を選択してください。

ステップ 3 [使用方法（Usage）] 領域で、[ポータル（Portal）] チェックボックスをオンにして、デフォルトのポータル証明書グループ タグを選択します。

ステップ 4 [保存（Save）] をクリックします。

警告メッセージが表示されます。

ステップ 5 [はい（Yes）] をクリックして、CA 署名付き証明書にデフォルトのポータル証明書グループ タグを再割り当てします。

ノードの登録前のポータル証明書タグの関連付け

展開内のすべてのポータルに「デフォルト ポータル証明書グループ」タグを使用する場合は、新しい ISE ノードを登録する前に、関連する CA 署名付き証明書をインポートし、サービスとして「ポータル」を選択し、この証明書に「デフォルト ポータル証明書グループ」タグを関連付けます。

展開に新しいノードを追加すると、デフォルトの自己署名証明書が「デフォルト ポータル証明書グループ」タグに関連付けられ、このタグを使用するようにポータルが設定されます。

新しいノードの登録後、証明書グループ タグの関連付けは変更できません。したがって、展開にノードを登録する前に、次を実行してください。

ステップ 1 自己署名証明書を作成し、サービスとして「ポータル」を選択し、別の証明書グループ タグ（たとえば、tempportaltag）を割り当てます。

ステップ 2 新しく作成した証明書グループ タグ（tempportaltag）を使用するようにポータル設定を変更します。

ステップ 3 デフォルト自己署名証明書を編集し、ポータル ロールを削除します。

このオプションは、デフォルト ポータル証明書グループ タグとデフォルト自己署名証明書との関連付けを削除します。

ステップ 4 次のいずれかを実行します。

オプション	説明
CSR の生成	CSR を生成するときは、次を実行します。 **1.** この証明書を使用する「ポータル」をサービスとして選択し、「デフォルト ポータル証明書グループ」タグを関連付けます。 **2.** CSR を CA に送信し、署名付きの証明書を取得します。 **3.** 信頼できる証明書ストアに証明書に署名した CA のルートおよび他の中間証明書をインポートします。 **4.** CSR に CA 署名付き証明書をバインドします。
秘密キーと CA 署名付き証明書のインポート	CA 署名付き証明書をインポートするときは、次を実行します。

オプション	説明
	1. この証明書を使用する「ポータル」をサービスとして選択し、「デフォルト ポータル証明書グループ」タグを関連付けます。 2. 信頼できる証明書ストアに証明書に署名した CA のルートおよび他の中間証明書をインポートします。
既存の CA 署名付き証明書の編集	既存の CA 署名付き証明書を編集するときは、次を実行します。 この証明書を使用する「ポータル」をサービスとして選択し、「デフォルト ポータル証明書グループ」タグを関連付けます。

ステップ 5 展開に ISE ノードを登録します。
展開内のポータル構成は「デフォルト ポータル証明書グループ」タグに設定され、ポータルは新しいノードの「デフォルト ポータル証明書グループ」タグに関連付けられた CA 署名付き証明書を使用するように設定されます。

ユーザーおよびエンドポイントの証明書の更新

デフォルトでは、Cisco ISE は証明書が期限切れになったデバイスからの要求を拒否します。ただし、このデフォルト動作を変更し、このような要求を処理し、ユーザーに証明書の更新を求めるように ISE を設定できます。

ユーザーが証明書を更新することを許可する場合は、要求をさらに処理する前に証明書が更新されたかどうかを判断する許可ポリシールールを設定することを推奨します。証明書が期限切れになったデバイスからの要求を処理することで、潜在的なセキュリティ脅威が発生する可能性があります。組織のセキュリティが侵害されていないことを保証するには、適切な許可プロファイルおよびルールを設定する必要があります。

あるデバイスは有効期限の前後に証明書を更新できます。ただし、Windows デバイスでは、期限切れになる前にだけ証明書を更新できます。Apple iOS、Mac OSX、および Android デバイスでは、有効期限の前または後に証明書を更新できます。

ポリシー条件で証明書更新に使用されるディクショナリ属性

Cisco ISE 証明書ディクショナリには、ユーザーに証明書更新を許可するポリシー条件で使用される次の属性が含まれます。

- [有効期限までの日数（Days to Expiry）]：この属性は、証明書が有効な日数を指定します。この属性を使用して、許可ポリシーで使用できる条件を作成できます。この属性には、0 ～ 15 の値を指定できます。0 の値は、証明書の有効期限がすでに切れていることを示します。1 の値は、証明書の有効期限が切れるまで 1 日未満であることを示します。
- [有効期限切れ（Is Expired）]：このブール属性は、証明書が有効期限切れかどうかを示します。証明書の有効期限が近く、有効期限切れではない場合にのみ証明書更新を許可する場合は、許可ポリシー条件でこの属性を使用します。

証明書更新用の許可ポリシー条件

許可ポリシーでCertRenewalRequiredの単純条件（デフォルトで使用可能）を使用すると、Cisco ISE が要求を処理する前に証明書（有効期限切れまたはまもなく有効期限が切れる）を更新できます。

証明書を更新するための CWA リダイレクト

ユーザー証明書が期限切れになる前に失効している場合、Cisco ISE は、CA がパブリッシュした CRL をチェックして認証要求を拒否します。失効した証明書の期限が切れている場合は、CA が CRL でこの証明書をパブリッシュしない可能性があります。このシナリオでは、失効した証明書が Cisco ISE によって更新される可能性があります。このことを避けるために、証明書を更新する前に、要求が中央 Web 認証（CWA）にリダイレクトされ、完全認証が実行されるようにします。CWA のユーザーをリダイレクトするには、許可プロファイルを作成する必要があります。

ユーザーによる証明書の更新を許可する Cisco ISE の設定

ユーザーが証明書を更新できるように Cisco ISE を設定するには、この手順で示すタスクを実行する必要があります。

始める前に

WLC で制限されたアクセス ACL を設定して、CWA 要求をリダイレクトします。

ステップ 1 許可されるプロトコルの設定の更新 （118 ページ）
ステップ 2 CWA リダイレクションの許可ポリシー プロファイルの作成 （119 ページ）
ステップ 3 証明書を更新する許可ポリシールールの作成 （120 ページ）
ステップ 4 ゲストポータルでの BYOD 設定の有効化 （120 ページ）

許可されるプロトコルの設定の更新

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [認証（Authentication）] > [許可されるプロトコル（Allowed Protocols）] > [デフォルト ネットワーク アクセス（Default Network Access）]** を選択します。

ステップ 2 PEAP および EAP-FAST プロトコルの EAP-TLS プロトコルおよび EAP-TLS 内部方式の下の [許可ポリシーの証明書更新を可能にするために失効した証明書の認証を許可（Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy）] チェックボックスをオンにします。

EAP-TLS プロトコルを使用する要求が NSP フローを通過します。

PEAP および EAP-FAST プロトコルについては、要求を処理するように Cisco ISE 向け Cisco AnyConnect を手動で設定する必要があります。

ステップ 3 **[送信（Submit）]** をクリックします。

次のタスク

CWA リダイレクションの許可ポリシー プロファイルの作成 （119 ページ）

CWA リダイレクションの許可ポリシー プロファイルの作成

始める前に

WLC で制限されたアクセス ACL が設定されていることを確認します。

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）]** 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 許可プロファイルの名前を入力します。たとえば、CertRenewal_CWA です。

ステップ 4 [共通タスク（Common Tasks）] 領域の [Web リダイレクション（CWA、DRW、MDM、NSP、CPP）（Web Redirection (CWA, DRW, MDM, NSP, CPP)）] チェックボックスをオンにします。

ステップ 5 ドロップダウン リストの [中央集中 Web 認証（Centralized Web Auth）] および制限されたアクセス ACL を選択します。

ステップ 6 [証明書更新メッセージの表示（Display Certificates Renewal Message）] チェックボックスをオンにします。

url-redirect 属性値が変更され、この値に証明書が有効である日数が含まれます。

ステップ 7 [送信（Submit）] をクリックします。

（注） Cisco ISE 1.2 で無線デバイスの次のデバイス登録 WebAuth（DRW）ポリシーを設定している場合：

- 条件 = (Wireless_MAB AND Network Access:UseCase EQUALS HostLookup) およびプロファイル = Wireless-drw-redirect を含む DRW-Redirect ポリシー
- 条件 = (Wireless_MAB AND Network Access:UseCase EQUALS HostLookup) およびプロファイル = Wireless-Permit を含む DRW-Allow ポリシー

ISE 1.3 以上のバージョンにアップグレードした後は、DRW-Allow ポリシー条件を次のように更新する必要があります。

- 条件 = (Wireless_MAB AND Network Access:UseCase EQUALS Guest Flow) およびプロファイル = Wireless-Permit

次のタスク

証明書を更新する許可ポリシールールの作成 （120 ページ）

証明書を更新する許可ポリシールールの作成

始める前に

中央 Web 認証リダイレクションの許可プロファイルが作成されていることを確認します。

[管理（Administration）]>[システム（System）]>[設定（Settings）]>[ポリシーセット（Policy Sets）] でポリシー セットを有効にします。

ステップ 1 **[ワーク センター（Work Centers）]>[デバイス管理（Device Administration）]>[ポリシー セット（Policy Sets）]** を選択します。

ステップ 2 [上を作成（Create Above）] をクリックします。

ステップ 3 新しいルールの名前を入力します。

ステップ 4 次の単純条件と結果を選択します。

CertRenewalRequired EQUALS True の場合は、権限用に以前に作成した許可プロファイル（CertRenewal_CWA）を選択します。

ステップ 5 [保存（Save）] をクリックします。

（注） Cisco ISE では、一度に最大 50 の認証ポリシーをロードできますが、次のポリシーセットをロードするまでに約 10 秒の遅延があります。

（注） 作成されたポリシーのリストから特定の認証ポリシーを検索する場合。検索バーで指定されたポリシー名は、以下のポリシーのリストで強調表示されますが、フィルタ処理はされません。

次のタスク

証明書が期限切れになったデバイスを持つ企業ネットワークにアクセスした場合は、[更新（Renew）] をクリックして、デバイスを再設定します。

ゲストポータルでの BYOD 設定の有効化

ユーザーがパーソナル デバイス証明書を更新できるようにするには、選択したゲスト ポータルで BYOD 設定を有効にする必要があります。

ステップ 1 **[ワークセンター（Work Center）]>[ゲストアクセス（Guest Access）]>[ポータルとコンポーネント（Portals & Components）]>[ゲストポータル（Guest Portals）]** を選択します。

a) 目的の CWA ポータルを選択して、[編集（Edit）] をクリックします。

ステップ 2 [BYOD 設定（BYOD Settings）] から [従業員にネットワークでのパーソナルデバイスの使用を許可する（Allow employees to use personal devices on the network）] チェックボックスをオンにします。

ステップ 3 [保存（Save）] をクリックします。

Apple iOS デバイスの証明書更新の失敗

ISE を使用して Apple iOS デバイスのエンドポイント証明書を更新する場合、「プロファイル済みでインストールできませんでした（Profiled Failed to Install）」エラー メッセージが表示される場合があります。このエラー メッセージは、同じポリシー サービス ノード（PSN）または別の PSN で、期限切れ間近または期限切れのネットワーク プロファイルが更新のプロセス時に使用されるものとは異なる管理者 HTTPS 証明書によって署名されている場合に表示されます。

回避策としては、展開内のすべての PSN で管理者 HTTPS 用にマルチドメイン SSL 証明書（通称 Unified Communications Certificates（UCC））またはワイルドカード証明書を使用します。

証明書定期チェックの設定

Cisco ISE は、証明書失効リスト（CRL）を定期的にチェックします。このウィンドウを使用して、自動的にダウンロードされた CRL に対して進行中のセッションを確認するように Cisco ISE を設定できます。OCSP または CRL のチェックを毎日開始する時刻と、OCSP サーバーまたは CRL を再度チェックする前に Cisco ISE が待機する時間間隔を時間単位で指定できます。

次の表では、[証明書定期チェックの設定（Certificate Periodic Check Settings）] ウィンドウのフィールドについて説明します。このページを使用して、証明書（OCSP または CRL）のステータスを確認する時間間隔を指定できます。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして、**[管理（Administration）]** > **[システム（System）]** > **[証明書（Certificates）]** > **[証明書管理（Certificate Management）]** > **[証明書定期チェックの設定（Certificate Periodic Check Settings）]** の順に選択します。

表 *15 :* 証明書定期チェックの設定

フィールド名	使用上のガイドライン
証明書チェックの設定	
自動的に取得されたCRLに対する進行中のセッションのチェック（Check ongoing sessions against automatically retrieved CRL）	Cisco ISE が自動的にダウンロードされた CRL に対する進行中のセッションをチェックするようにするには、このチェックボックスをオンにします。
CRL/OCSP の定期的な証明書チェック	

フィールド名	使用上のガイドライン
最初のチェック時刻（**First check at**）	CRL または OCSP のチェックを毎日開始する時刻を指定します。00:00 ～ 23:59 の時間範囲の値を入力します。
チェック間隔（**Check every**）	CRL または OCSP サーバーを再度チェックする前に Cisco ISE が待機する時間間隔を時間単位で指定します。

関連トピック

OCSP サービス （163 ページ）
OCSP クライアント プロファイルの追加 （166 ページ）

Cisco ISE CA サービス

証明書は、自己署名したり、外部の認証局（CA）がデジタルで署名したりできます。Cisco ISE 内部認証局（ISE CA）は、従業員が企業ネットワークでパーソナル デバイスを使用できるように、一元的なコンソールからエンドポイントのデジタル証明書を発行し、管理します。CA 署名付きデジタル証明書は、業界標準であり、よりセキュアです。プライマリ PAN は、ルート CA です。ポリシー サービス ノード（PSN）は、プライマリ PAN の下位 CA です（SCEP RA）。ISE CA には次の機能があります。

- 証明書の発行：ネットワークに接続するエンドポイントの証明書署名要求（CSR）を検証し、署名します。
- キー管理：PAN ノードと PSN ノードの両方でキーと証明書を生成し、セキュアに保存します。
- 証明書ストレージ：ユーザーやデバイスに発行された証明書を保存します。
- Online Certificate Status Protocol（OCSP）サポート：OCSP 応答側に証明書の有効性を確認する手段を提供します。

CA サービスがプライマリ管理ノードで無効になっている場合でも、CA サービスはセカンダリ管理ノードの CLI で実行中として表示されます。理想的には、CA サービスは無効として表示される必要があります。これは、Cisco ISE の既知の問題です。

Cisco ISE 証明書フィンガープリント

証明書フィンガープリントプロセスは、証明書の即時発行者のフィンガープリント SHA256 を評価し、信頼できる証明書と照合するために使用されます。これにより、複数の CA が異なるドメインをサポートするためのセキュアなメカニズムが適用され、802.1x プロトコルに対して信頼できる CA をロックすることもできます。

ポリシー条件で証明書を更新する前に、発行者：フィンガープリント SHA-256 証明書が Cisco ISE 展開に追加されていることを確認します。

（注） 信頼できる証明書をポリシーで設定した後は、その証明書を削除できません。**[信頼できる証明書（Trusted Certificates）]** ウィンドウの、**[この信頼できる証明書はポリシーセットで参照される（This Trusted Certificate Refered by Policy Sets）]** セクションに、次のメッセージが表示されます。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして、**[管理（Administration）]** > **[システム（System）]** > **[証明書（Certificates）]** > **[信頼できる証明書（Trusted Certificates）]** を選択します。

証明書はポリシーで使用されているため、削除できません（`Certificate cannot be deleted because it is used in a policy`）。証明書を削除するには、最初にポリシー条件を変更してください（`To delete the certificate, please modify policy condition first`）。

Cisco ISE の証明書フィンガープリントを設定するには、次の順序に従って手順を実行します。

1. 内部ユーザーを作成します。詳細については、『*Cisco Identity Services Engine* リリース *3.0* 管理者ガイド』の「アセットの可視性」の章にある「ユーザーの追加」のセクションを参照してください。
2. ネットワークデバイスを追加します。詳細については、『*Cisco Identity Services Engine* リリース *3.0* 管理者ガイド』の「基本的なセットアップ」の章にある「Cisco ISE でのネットワークデバイスの追加」のセクションを参照してください。
3. **外部証明書**に外部 CA をインポートします。詳細については、『*Cisco Identity Services Engine* リリース *3.0* 管理者ガイド』の「基本的なセットアップ」の章にある「システム証明書のインポート」のセクションを参照してください。

   SCEP プロトコルを使用して Issuer-Fingerprint SHA-256 証明書をインポートすることもできます。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[管理（Administration）]** > **[システム（System）]** > **[証明書（Certificates）]** > **[認証局（Certificate Authority）]** > **[外部 CA 設定（External CA Settings）]** を選択します。表示される **[SCEP RA プロファイルの追加（Add SCEP RA Profile）]** ウィンドウで、[追加（Add）] をクリックします。**[名前（Name）]** フィールドに、証明書名を入力します。**[URL]** フィールドに、CA サーバーの URL を入力します。[テスト接続（Test Connection）] をクリックします。
4. SHA-256 フィンガープリントを使用したポリシーの作成。
5. SHA-256 フィンガープリントを使用した認証ポリシーの作成とマッピング
6. 認証ポリシーの作成。
7. PRRT ログの確認。

SHA-256 フィンガープリントを使用したポリシーの作成

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[ポリシー（Policy）]** > **[ポリシーセット（Policy Set）]** の順に選択します。

ステップ 2 表示される [ポリシーセット（Policy Set）] ウィンドウで [設定（Settings）] をクリックし、ドロップダウンリストから [新しい行の挿入（insert a new row）] を選択します。

ステップ 3 [新しいポリシー名（New Policy Name）] フィールドに名前を入力します。

ステップ 4 ポリシーの [説明（Description）] を入力します。

ステップ 5 [条件（Conditions）] 列の下にある新しい [ポリシーセット名（Policy Set Name）] の横にある [追加（Add）]（+）アイコンをクリックします。

ステップ 6 表示される [条件スタジオ（Condition Studio）] ウィンドウで、[クリックして属性を追加（Click to Add Attribute）] フィールドをクリックします。

ステップ 7 [すべてのディクショナリ（All Dictionary）] ドロップダウンリストから、[ネットワークアクセスとプロトコル（Network Access-Protocol）]（[ディクショナリと属性（Dictionary-Attribute）]）の組み合わせを選択します。

ステップ 8 論理条件を作成するには、[等号（Equals）] 演算子を選択します。

ステップ 9 [リストから選択するか入力する（Choose from List or Type）] ドロップダウンリストから [RADIUS] を選択します。

ステップ 10 [使用（Use）] をクリックします。

ステップ 11 表示される [ポリシーセット（Policy Set）] ウィンドウの [許可されるプロトコル/サーバーの順序（Allowed Protocols/ Server Sequence）] ドロップダウンリストから、[デフォルトのネットワークアクセス（Default Network Access）] を選択します。

ステップ 12 [保存（Save）] をクリックします。

SHA-256 フィンガープリントを使用した認証ポリシーの作成とマッピング

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[ポリシー（Policy）]** > **[ポリシーセット（Policy Sets）]** > **[デフォルト（Default）]** の順に選択します。

ステップ 2 [認証ポリシー（Authentication Policy）] をクリックします。

ステップ 3 設定アイコンをクリックし、[新しい行の挿入（insert a new row）] を選択します。

ステップ 4 [認証ルール名（Authentication Rule Name）] ウィンドウに名前を入力します。

ステップ 5 ルール名の横にある [追加（Add）] アイコン（[+]）をクリックします。

ステップ 6 表示される [条件スタジオ（Condition Studio）] ウィンドウで、[クリックして属性を追加（Click to add Attributes）] フィールドをクリックします。

ステップ 7 [すべてのディクショナリ（All Dictionary）] ドロップダウンリストから、**CERTIFICATE-Issuer- Fingerprint SHA-256**（[ディクショナリと属性（Dictionary-Attribute）]）の組み合わせを選択します。

ステップ 8 論理条件を作成するには、[等号（Equals）] 演算子を選択します。

ステップ 9 [リストまたはタイプから選択（Choose from List or Type）] ドロップダウンリストから [Cisco Manufacturing CA SHA2 fingerprint sha256] を選択します。

ステップ 10 [使用（Use）] をクリックします。

ステップ 11 表示される [ポリシーセット（Policy Set）] ウィンドウの [許可されるプロトコル/サーバーの順序（Allowed Protocols/ Server Sequence）] ドロップダウンリストから、[Preloaded_Certificate_Profile] を選択します。

ステップ 12 [保存（Save）] をクリックします。

認証ポリシーの作成

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[ポリシー（Policy）]** > **[ポリシーセット（Policy Sets）]** > **[デフォルト（Default）]** を選択します。

ステップ 2 [認証ポリシー（Authorization Policy）] をクリックします。

ステップ 3 設定アイコンをクリックし、ドロップダウンリストから [新しい行の挿入（insert a new row）] を選択します。

ステップ 4 [認証ルール名（Authentication Rule Name）] ウィンドウで、名前を入力します。

ステップ 5 ルール名の横にある [追加（Add）] アイコン（[+]）をクリックします。

ステップ 6 表示される [条件スタジオ（Condition Studio）] ウィンドウで、[クリックして属性を追加（Click to add Attributes）] フィールドをクリックします。

ステップ 7 [すべてのディクショナリ（All Dictionary）] ドロップダウンリストから、**CERTIFICATE-Issuer- Fingerprint SHA-256**（[ディクショナリと属性（Dictionary-Attribute）]）の組み合わせを選択します。

ステップ 8 論理条件を作成するには、[等号（Equals）] 演算子を選択します。

ステップ 9 [リストまたはタイプから選択（Choose from List or Type）] ドロップダウンリストから、[Cisco Root CA 2099 フィンガープリント SHA（Cisco Root CA 2099 fingerprint sha）] を選択します。

ステップ 10 [使用（Use）] をクリックします。

ステップ 11 表示された [ポリシーセット（Policy Set）] ウィンドウの [許可されるプロトコル/サーバーの順序（Allowed Protocols/ Server Sequence）] ドロップダウンリストから、[PermitAccess] を選択します。

ステップ 12 [保存（Save）] をクリックします。

PRRT ログの確認

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[操作（Operations）]** > **[RADIUS]** > **[ライブログ（Live Logs）]** の順に選択します。

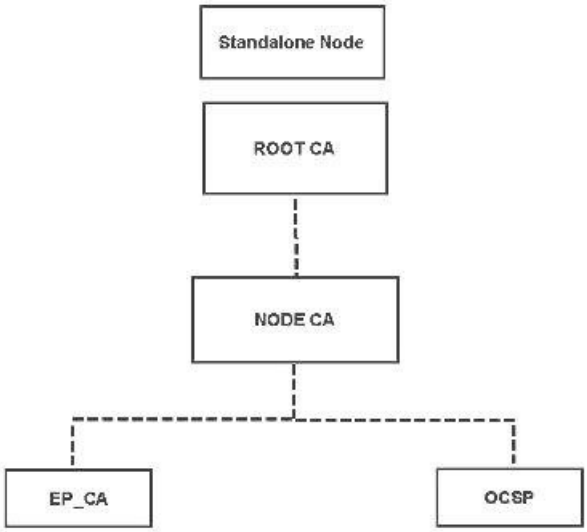
ステップ 2 表示される [ライブログ（Live Logs）] ウィンドウで、最新のログの詳細をクリックします。

ステップ 3 表示される [認証の詳細（Authentication Details）] ウィンドウで、[発行者：フィンガープリント SHA-256（Issuer-Fingerprint SHA-256）] 列の SHA-256 値を確認し、[発行者：フィンガープリント SHA-256（Issuer-Fingerprint SHA-256）] 証明書が正常に追加され、検証されていることを確認します。

管理ノードとポリシーサービスノードでプロビジョニングされるCisco ISE CA 証明書

インストール後に、Cisco ISE ノードはルート CA 証明書およびノード CA 証明書でプロビジョニングされ、エンドポイントの証明書が管理されます。

図 *7:* スタンドアロンノードでプロビジョニングされる *Cisco ISE CA* 証明書

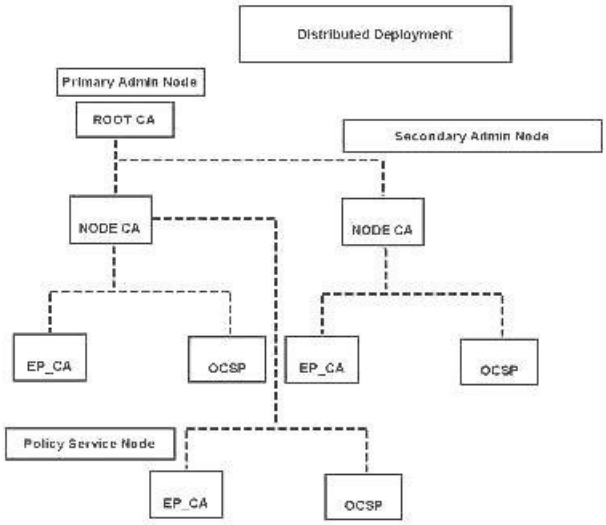


展開をセットアップすると、プライマリ管理ノード（PAN）として指定したノードがルート CA になります。PAN には、ルート CA 証明書と、ルート CA によって署名されたノード CA 証明書があります。

PAN にセカンダリ管理ノードを登録すると、ノード CA 証明書が生成され、プライマリ管理ノードでルート CA によって署名されます。

PAN に登録したポリシー サービス ノード（PSN）には、エンドポイント CA と、PAN のノード CA によって署名された OCSP 証明書がプロビジョニングされます。ポリシー サービス ノード（PSN）は、PAN の下位 CA です。ISE CA を使用すると、PSN のエンドポイント CA によってネットワークにアクセスするエンドポイントに証明書が発行されます。

図 *8 :* 展開内の管理ノードおよびポリシーサービスノードでプロビジョニングされる *Cisco ISE CA* 証明書



Cisco ISE と相互運用するための CA の要件

Cisco ISE で CA サーバーを使用しているときは、次の要件を満たしている必要があります。

- キー サイズは 1024、2048、またはそれ以上にする必要があります。CA サーバーでは、キー サイズは証明書テンプレートを使用して定義されます。サプリカント プロファイルを使用して Cisco ISE でキー サイズを定義できます。
- キーの使用法では、拡張された署名と暗号化を許可する必要があります。
- SCEP プロトコルを介して GetCACapabilities を使用する場合は、暗号化アルゴリズムと要求ハッシュがサポートされている必要があります。RSA と SHA1 を使用することをお勧めします。
- Online Certificate Status Protocol（OCSP）がサポートされます。これは BYOD では直接使用されませんが、OCSP サーバーとして機能できる CA は証明書失効に使用できます。

（注） Cisco ISE は、PEAP、EAP-TLS などの標準 EAP 認証用の Enterprise Java Beans 認証局（EJBCA）をサポートします。プロキシ SCEP の EJBCA サポートを有効にするには、EJBCA で [エンドエンティティ プロファイル制限の有効化（Enable End Entity Profile Limitations）] オプション（[システム（System）]>[基本設定（Basic Configurations）] の下）を無効にする必要があります。

- エンタープライズ PKI を使用して Apple iOS デバイスの証明書を発行する場合は、SCEP テンプレートでキーの使用法を設定し、[キーの暗号化（Key Encipherment）] オプションを有効にする必要があります。

Microsoft CA を使用する場合は、証明書テンプレートのキー使用法拡張機能を編集します。[暗号化（Encryption）] 領域で、[キーの暗号化でのみキーの交換を許可する（Allow key exchange only with key encryption (key encipherment)）] オプションボタンをクリックし、[ユーザーデータの暗号化を許可する（Allow encryption of user data）] チェックボックスもオンにします。

- Cisco ISE は、EAP-TLS 認証の信頼できる証明書およびエンドポイント証明書に対して、RSASSA-PSS アルゴリズムの使用をサポートしています。証明書を表示すると、署名アルゴリズムは、アルゴリズム名ではなく、1.2.840.113549.1.1.10 としてリストされます。

（注） BYOD フローに Cisco ISE 内部の CA を使用する場合、管理証明書は（外部 CA で）RSASSA-PSS アルゴリズムを使用して署名できません。Cisco ISE 内部の CA は、このアルゴリズムを使用して署名された管理証明書を検証できず、要求が失敗します。

証明書ベースの認証のためのクライアント証明書の要件

Cisco ISE による証明書ベースの認証では、クライアント証明書が次の要件を満たしている必要があります。

表 *16 :* クライアント *RSA* および *ECC* の証明書要件

RSA		
サポートされているキーサイズ	1024、2048、および 4096 ビット	
サポートされているセキュアハッシュ アルゴリズム（SHA）	SHA-1 および SHA-2（SHA-256 を含む）	
ECC [12]		
サポートされる曲線タイプ	P-192、P-256、P-384、および P-521	
サポートされているセキュアハッシュ アルゴリズム（SHA）	SHA-256	
クライアントマシンのオペレーティングシステムとサポートされている曲線タイプ		
Windows	8 以降	P-256、P-384、P-521

Android	4.4 以降 （注） Android 6.0 は、ECC 証明書をサポートするために 2016 年 5 月のパッチが必要です。	すべての曲線タイプ（P-192 曲線タイプをサポートしていない Androidv6.0 を除く）。

[1] Windows 7 と Apple iOS は、EAP-TLS 認証用の ECC をネイティブでサポートしていません。

[2] Cisco ISE のこのリリースでは、Mac OS X デバイスでの ECC 証明書の使用はサポートされていません。

Cisco ISE CA チェーンの再生成

Cisco ISE CA チェーンを再生成すると、ルート CA、ノード CA、およびエンドポイント CA 証明書を含むすべての証明書が再生成されます。PAN または PSN のドメイン名またはホスト名を変更すると、ISE CA チェーンを再生する必要があります。以前のリリースから 2.0 以降にアップグレードするときには、2 つのルート階層から 1 つのルート階層に移行するように ISE CA チェーンを再生成することをお勧めします。

システム証明書を再生成すると、ルート CA または中間 CA 証明書のいずれでも、ISE メッセージングサービスが再起動して新しい証明書チェーンがロードされます。監査ログは、ISE メッセージングサービスが再び利用可能になるまで失われます。

（注） 展開で Cisco ISE の内部 CA を置き換えるたびに、完全な証明書チェーンを取得するように ISE メッセージングサービスも更新する必要があります。

Cisco ISE 内部 CA チェーンを再生成すると、チェーン内のすべての証明書の [有効期限の開始（Valid From）] フィールドに、再生成の 1 日前の日付が表示されます。

ドメインまたはホスト名に変更があり、ルート CA チェーンが再生成されると、システム証明書を含むすべての証明書（SAML 証明書を除く）が新しいドメインまたはホスト名で更新されます。SAML 証明書は個別に再生成する必要があります。

外部 CA による Cisco ISE メッセージング証明書のサポート

外部 CA によって署名された Cisco ISE メッセージング証明書は、EKU クライアントおよびサーバー認証（pxgrid など）で設定する必要があります。pxgrid テンプレートを設定するには、https://community.cisco.com/t5/security-documents/deploying-certificates-with-cisco-pxgrid-using-an-external/ta-p/3639677 を参照してください。

楕円曲線暗号化証明書のサポート

Cisco ISE CA サービスが、楕円曲線暗号化（ECC）アルゴリズムに基づく証明書をサポートするようになりました。ECC は、より小さいキー サイズを使用している場合でも、他の暗号化アルゴリズムよりも高いセキュリティとパフォーマンスを提供します。

次の表では、ECC および RSA のキー サイズとセキュリティ強度を比較しています。

ECC のキー サイズ（ビット単位）	**RSA のキー サイズ（ビット単位）**
160	1024
224	2048
256	3072
384	7680
521	15360

キー サイズが小さいため、暗号化が迅速になります。

Cisco ISE では、次の ECC 曲線タイプがサポートされています。曲線タイプまたはキー サイズが大きくなると、セキュリティが強化されます。

- P-192
- P-256
- P-384
- P-521

ISE は、証明書の EC 部分の明示的なパラメータをサポートしていません。明示的なパラメータで証明書をインポートしようとすると、「証明書の検証に失敗しました」というエラーが表示されます。名前付き ECParameters のみがサポートされています。

Cisco ISE CA サービスは、BYOD フローを介して接続するデバイスの ECC 証明書をサポートします。また、証明書プロビジョニング ポータルから ECC 証明書を生成することもできます。

（注） 次の表に、ECC をサポートしているオペレーティング システムおよびバージョンと、サポートされている曲線タイプを示します。デバイスがサポートされているオペレーティング システムを実行していない場合、またはサポートされているバージョンでない場合には、代わりに RSA ベースの証明書を使用することもできます。

オペレーティング システム	サポートされるバージョン	サポートされる曲線タイプ
Windows	8 以降	P-256、P-384、P-521
Android	4.4 以降 （注） Android 6.0 は、ECC 証明書をサポートするために 2016 年 5 月のパッチが必要です。	すべての曲線タイプ（P-192 曲線タイプをサポートしていない Android 6.0 を除く）。

Windows 7 と Apple iOS は、EAP-TLS を介した認証用の ECC をネイティブでサポートしていません。Cisco ISE のこのリリースでは、Mac OS X デバイスでの ECC 証明書の使用はサポートされていません。

Enrollment over Secure Transport（EST）プロトコルを備えた BYOD フローが適切に機能しない場合は、次のことを確認します。

- 証明書サービス エンドポイント サブ CA 証明書チェーンが完全であること。証明書チェーンが完全かどうかを確認するには：

  1. [管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [認証局（Certificate Authority）] > [認証局証明書（Certificate Authority Certificates）] の順に選択します。
  2. 確認する証明書の横にあるチェック ボックスをオンにして、[表示（View）]をクリックします。

- CA および EST サービスが起動し、実行されていることを確認します。サービスが実行されていない場合は、[管理（Administration）]>[システム（System）]>[証明書（Certificates）] > [認証局（Certificate Authority）] > [内部CAの設定（Internal CA Settings）] に移動して CA サービスを有効にします。

- 2.0 以前の ISE バージョンから Cisco ISE 2.x にアップグレードしている場合は、アップグレード後に ISE ルート CA 証明書チェーンを置き換えます。手順は次のとおりです。

  1. [管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [証明書の管理（Certificate Management）] > [証明書署名要求（Certificate Signing Requests）] の順に選択します。

2. [証明書署名要求（CSR）の生成（Generate Certificate Signing Requests (CSR)）] をクリックします。
3. [1つ以上の証明書の使用先（one or more Certificates will be used for）] ドロップダウンリストから ISE ルート CA を選択します。
4. [ISE ルート CA 証明書チェーンの置き換え（Replace ISE Root CA Certificate Chain）] をクリックします。

（注） Cisco ISE のこのリリースでは、EST クライアントが Cisco ISE に存在する EST サーバーに対して直接認証を行うことはサポートされていません。

Android または Windows エンドポイントでのオンボーディング時に、要求が ECC ベースの証明書用である場合には、ISE が EST フローをトリガーします。

（注） 認証プロファイルで静的 IP アドレス、FQDN、またはホスト名とともに EST プロトコルを使用すると、Android クライアントでの BYOD フローが失敗することがあります。回避策は、EST の代わりに SCEP を使用することです。ネイティブ サプリカント プロファイルで SCEP を設定できます。詳細については、「ネイティブ サプリカント プロファイルの作成」を参照してください。

Cisco ISE 認証局証明書

[認証局（CA）証明書（Certificate Authority (CA) Certificates）] ページには、内部 Cisco ISE CA に関連するすべての証明書が表示されます。以前のリリースでは、これらの CA 証明書は信頼できる証明書ストアにありましたが、現在は [CA 証明書（CA Certificates）] ページに移動しています。これらの証明書は、このページにノード方式で表示されます。ノードを展開して、その特定のノードの ISE CA 証明書をすべて表示することができます。プライマリおよびセカンダリ管理ノードには、ルート CA、ノード CA、下位 CA、OCSP レスポンダ証明書があります。展開内の他のノードには、エンドポイント下位 CA および OCSP 証明書があります。

Cisco ISE CA サービスを有効にすると、すべてのノードでこれらの証明書が自動的に生成され、インストールされます。また、ISE ルート CA チェーン全体を置き換えると、すべてのノードでこれらの証明書が自動的に再生成され、インストールされます。手動による介入は必要ありません。

Cisco ISE CA 証明書は **Certificate Services** <**エンドポイント サブ *CA*/ノード *CA*/ルート *CA*/*OCSP* レスポンダ**>-<ノードのホスト名>#証明書番号という命名規則に従います。

[CA 証明書（CA Certificates）] ページで Cisco ISE CA 証明書を編集、インポート、エクスポート、削除、表示できます。

Cisco ISE CA 証明書の編集

証明書を Cisco ISE CA 証明書ストアに追加したら、編集の設定を使用して、その証明書をさらに編集できます。

始める前に

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

ステップ 1 **[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [認証局（Certificate Authority）] > [認証局証明書（Certificate Authority Certificates）]** の順に選択します。。

ステップ 2 ISE-PIC GUI で [メニュー（Menu）] アイコン（☰）をクリックして、 の順に選択します。

ステップ 3 編集する証明書の横にあるチェックボックスをオンにして、[編集（Edit）] をクリックします。

ステップ 4 必要に応じて編集可能なフィールドを変更します。フィールドの説明については、信頼できる証明書の設定 （93 ページ）を参照してください。

ステップ 5 [保存（Save）] をクリックして、証明書ストアに対して行った変更を保存します。

Cisco ISE CA 証明書のエクスポート

Cisco ISE ルート CA およびノード CA 証明書をエクスポートするには、次の手順を実行します。

始める前に

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

ステップ 1 **[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [認証局（Certificate Authority）] > [認証局証明書（Certificate Authority Certificates）]** の順に選択します。

ステップ 2 ISE-PIC GUI で [メニュー（Menu）] アイコン（☰）をクリックして、 の順に選択します。

ステップ 3 エクスポートする証明書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）] をクリックします。一度に 1 つの証明書のみをエクスポートできます。

ステップ 4 クライアント ブラウザを実行しているファイル システムに Privacy Enhanced Mail ファイルを保存します。

Cisco ISE CA 証明書のインポート

エンドポイントが別の展開の Cisco ISE CA によって発行された証明書を使用してネットワークへの認証を試みる場合、Cisco ISE ルート CA、ノード CA、エンドポイント サブ CA 証明書をその展開から Cisco ISE の信頼できる証明書ストアにインポートする必要があります。

始める前に

- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。
- ISE ルート CA、ノード CA、エンドポイント サブ CA 証明書を、エンドポイント証明書が署名されている展開からエクスポートし、ブラウザが実行されているコンピュータのファイル システムに保存します。

ステップ 1 エンドポイントが認証されている展開の管理者用ポータルにログインします。

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 Certificates）]** を選択します。

ステップ 3 [インポート（Import）] をクリックします。

ステップ 4 必要に応じてフィールドの値を設定します。詳細については、信頼できる証明書のインポート設定 （98 ページ）を参照してください。

クライアント証明書ベースの認証が有効である場合は、Cisco ISE により展開内の各ノードのアプリケーション サーバーが再起動されます（最初に PAN のアプリケーション サーバーが再起動され、続いて追加のノードのアプリケーション サーバーが 1 つずつ再起動されます）。

証明書テンプレート

証明書テンプレートには、そのテンプレートに基づいて認証局（CA）によって発行されたすべての証明書に共通のプロパティが含まれています。証明書テンプレートは、件名、サブジェクト代替名（SAN）、キー タイプ、キー サイズ、使用する必要がある SCEP RA プロファイル、証明書の有効期間、証明書がクライアントまたはサーバーの認証またはその両方に使用される必要があるかどうかを指定した拡張キーの使用状況（EKU）を定義します。内部 Cisco ISE CA（ISE CA）は、証明書テンプレートを使用し、そのテンプレートに基づいて証明書を発行します。

Cisco ISE には、次の ISE CA のデフォルトの証明書テンプレートが付属しています。必要に応じて、追加の証明書テンプレートを作成できます。デフォルトの証明書テンプレートは次のとおりです。

- CA_SERVICE_Certificate_Template：Cisco ISE を認証局として使用するその他のネットワーク サービス用。たとえば、ASA VPN ユーザーに対し証明書を発行するには、ISE の設定時にこの証明書テンプレートを使用します。この証明書テンプレートでは、有効期間のみを変更できます。
- EAP_Authentication_Certificate_Template：EAP 認証用。
- pxGrid_Certificate_Template：証明書プロビジョニング ポータルから証明書を生成するときの pxGrid コントローラ用。

証明書テンプレート名の拡張子

Cisco ISE の内部 CA には、エンドポイント証明書を作成するために使用された証明書テンプレートを表す拡張子が含まれています。内部 CA によって発行されたすべてのエンドポイント証明書には、証明書テンプレート名の拡張子が含まれています。この拡張子は、そのエンドポイント証明書を作成するために使用された証明書テンプレートを表します。拡張子の ID は 1.3.6.1.4.1.9.21.2.5 です。CERTIFICATE: テンプレート名属性を許可ポリシーの条件に使用して、評価の結果に基づいて適切なアクセス権限を割り当てることができます。

許可ポリシー条件での証明書テンプレート名の使用

許可ポリシー ルールで証明書テンプレート名の拡張子を使用できます。

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 ルールを表示するデフォルトのポリシー セットを展開します。

ステップ 2 新しいルールを追加するか、既存のルールを編集します。次に、Compliant_Device_Access ルールを編集する例を示します。

a) Compliant_Device_Access ルールを編集します。
b) [属性/値の追加（Add Attribute/Value）] を選択します。
c) ディクショナリから、**CERTIFICATE: Template Name** 属性と **Equals** 演算子を選択します。
d) 証明書テンプレート名の値を入力します。たとえば、EAP_Authentication_Certificate_Template などです。

ステップ 3 [保存（Save）] をクリックします。

pxGrid コントローラ用の Cisco ISE CA 証明書の展開

Cisco ISE CA は、証明書プロビジョニング ポータルから証明書を生成するための pxGrid コントローラの証明書テンプレートを提供します。

始める前に

pxGrid クライアントの証明書署名要求（CSR）を生成し、CSR の内容をクリップボードにコピーします。

ステップ 1 ネットワーク アクセス ユーザー アカウントを作成します（[管理（Administration）] > [ID の管理（Identity Management）] > [ID（Identities）] > [ユーザー（Users）] > [追加（Add）]）。

ユーザーが割り当てられているユーザー グループをメモします。

ステップ 2 証明書プロビジョニング ポータルの設定を編集します（[管理（Administration）]>[デバイス ポータル管理（Device Portal Management）] > [証明書プロビジョニング（Certificate Provisioning）]）。

a) 証明書プロビジョニング ポータルを選択して、[編集（Edit）] をクリックします。

b) [ポータル設定（Portal Settings）] ドロップダウン リストをクリックします。[承認済みグループの設定（Configure authorized groups）] の選択可能なリストから、ネットワーク アクセス ユーザーが属すユーザー グループを選択して、選択済みリストに移動します。

c) [証明書プロビジョニング ポータル設定（Certificate Provisioning Portal Settings）] ドロップダウン リストをクリックします。[pxGrid_Certificate_Template] を選択します。詳細については、「証明書プロビジョニング ポータルのポータル設定」を参照してください。

d) ポータル設定を保存します。

ステップ 3 証明書プロビジョニング ポータルを起動します。[ポータル テスト URL（Portal test URL）] リンクをクリックします。

a) 手順 1 で作成したユーザー アカウントを使用して証明書プロビジョニング ポータルにログインします。

b) AUP を受け入れ、[続行（Continue）] をクリックします。

c) [処理の選択（I want to）] ドロップダウン リストから、[単一の証明書の生成（証明書署名要求あり）（Generate a single certificate (with certificate signing request)）] を選択します。

d) [証明書署名要求の詳細（Certificate Signing Request Details）] フィールドに、クリップボードから CSR の内容を貼り付けます。

e) [証明書のダウンロード形式（Certificate Download Format）] ドロップダウン リストから、[PKCS8 形式（PKCS8 format）] を選択します。

（注） [PKCS12 形式（PKCS12 format）] を選択する場合は、1 つの証明書ファイルを証明書ファイルとキー ファイルに分けて変換する必要があります。Cisco ISE にインポートする前に、証明書とキー ファイルはバイナリ DER エンコードまたは PEM 形式にする必要があります。

f) [証明書テンプレートの選択（Choose Certificate Template）] ドロップダウン リストから、[pxGrid_Certificate_Template] を選択します。

g) 証明書のパスワードを入力します。

h) [生成（Generate）] をクリックします。

証明書が生成されます。

i) 証明書をエクスポートします。

証明書チェーンとともに証明書がエクスポートされます。

ステップ 4 pxGrid クライアントの信頼できる証明書ストアに Cisco ISE CA チェーンをインポートします。

BYOD の MAC ランダム化

Android および iOS デバイスは、デフォルトでランダム MAC アドレスプロパティを使用するようになっています。ランダム MAC アドレス機能が有効になっているデバイスは、接続するすべての SSID にランダム MAC アドレスを使用します。Cisco ISE およびモバイルデバイス管理（MDM）システムは、サービスのために接続している SSID に応じて、同じデバイスの異なる MAC アドレスを受信します。したがって、GUID と呼ばれる一意の識別子が Cisco ISE プロビジョニングサービスによって生成され、両方のシステムで同じ値を使用してエンドポイントが識別されます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [認証局（Certificate Authority）] > [証明書テンプレート（Certificate Templates）]** を選択します。

ステップ 2 [EAP 証明書テンプレート（EAP Certificate Template）] 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 [編集（Edit）] をクリックします。

ステップ 4 [サブジェクト代替名（SAN）（Subject Alternative Name (SAN)）] ドロップダウンリストで、[MAC アドレスと GUID（MAC Address and GUID）] を選択します。

BYOD フローでランダムおよび変更 MAC アドレスを処理するために、Cisco ISE プロビジョニングサービスは Windows、iOS、および Android エンドポイントの GUID 値を生成します。BYOD フローでランダム MAC アドレスを処理するために、GUID 値を証明書のサブジェクト代替名（SAN）に含めるように設定している場合は、AD ユーザーを認証する [証明書認証プロファイル（Certificate Authentication Profile）] を設定するときに、ID 検証の証明書属性として [サブジェクト - 一般名（Subject - Common Name）] を選択します。TLS ベース認証の証明書認証プロファイルの作成 （144 ページ）

ステップ 5 [保存（Save）] をクリックします。

Simple Certificate Enrollment Protocol プロファイル

ユーザーがネットワークで登録できるさまざまなモバイルデバイスの証明書のプロビジョニング機能を有効にするために、1 つ以上の Simple Certificate Enrollment Protocol（SCEP）認証局（CA）プロファイル（Cisco ISE 外部 CA 設定と呼ばれます）を設定して、Cisco ISE に複数の CA の場所を指定できます。複数のプロファイルを使用できる利点は、ハイ アベイラビリティを実現し、指定した CA の場所の間でロードバランシングを実行できることです。特定の SCEP CA への要求に 3 回連続して応答がなかった場合、Cisco ISE は特定のサーバーが使用不能であると宣言し、次に負荷が小さく応答時間が短い既知の CA に自動的に移動し、サーバーがオンラインに復帰するまで、定期的なポーリングを開始します。

Microsoft SCEP サーバーを Cisco ISE と相互運用するように設定する方法については、次を参照してください。

http://www.cisco.com/en/US/solutions/collateral/ns340/ns414/ns742/ns744/docs/howto_60_byod_certificates.pdf

発行された証明書

管理者ポータルには、内部 ISE CA によってエンドポイントに対して発行されたすべての証明書のリストが示されます（[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [エンドポイント証明書（Endpoint Certificates）]）。[発行された証明書（Issued Certificates）] ページでは、証明書ステータスを一目で確認できます。証明書が失効している場合は、[ステータス（Status）] 列の上にマウス カーソルを移動すると、失効の理由を確認できます。[証明書テンプレート（Certificate Template）] 列の上にマウス カーソルを移動すると、キー タイプ、キー サイズ、曲線タイプ、サブジェクト、サブジェクト代替名（SAN）、証明書の有効性などの詳細情報を表示できます。エンドポイント証明書クリックして、証明書を表示できます。

ISE CA によって発行されたすべての証明書（BYOD フローを介して自動的にプロビジョニングされた証明書と証明書プロビジョニング ポータルから取得された証明書）は、[エンドポイント証明書（Endpoint Certificates）] ページにリストされます。このページからこれらの証明書を管理できます。

たとえばuser7に発行された証明書を確認する場合は、[フレンドリ名（Friendly Name）] フィールドの下に表示されるテキスト ボックスに 「user7」 と入力します。このユーザーにCisco ISEによって発行されたすべての証明書が表示されます。フィルタをキャンセルするには、テキスト ボックスから検索語を削除します。また、[拡張フィルタ（Advanced Filter）] オプションを使用して、さまざまな検索基準に基づいてレコードを表示することもできます。

この [エンドポイント証明書（Endpoint Certificates）] ページには、必要に応じてエンドポイント証明書を取り消すためのオプションもあります。

[証明書管理概要（Certificate Management Overview）] ページには、展開内の各 PSN ノードによって発行されたエンドポイント証明書の合計数が表示されます。また、失効した証明書の合計数と失敗した証明書の合計数をノードごとに確認することもできます。このページのデータは任意の属性に基づいてフィルタリングできます。

[エンドポイント証明書の概要（Endpoint Certificate Overview）] ウィンドウ発行および失効した証明書

次の表で、[証明書管理の概要（Certificate Management Overview）][発行および失効した証明書の概要（Overview of Issued and Revoked Certificates）] ウィンドウのフィールドについて説明します。展開内の PSN ノードがエンドポイントに証明書を発行します。このウィンドウでは、展開内の各 PSN ノードが発行するエンドポイント証明書に関する情報を示します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして、**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [概要（Overview）]** です。

表 *17*：発行された証明書と失効した証明書

フィールド	使用上のガイドライン
ノード名（Node Name）	証明書を発行したポリシー サービス ノード（PSN）の名前。
[発行された証明書（Certificates Issued）]	PSN ノードが発行したエンドポイント証明書の数。
[取り消された証明書（Certificates Revoked）]	失効したエンドポイント証明書（PSN ノードが発行した証明書）の数。
[証明書要求（Certificates Requests）]	PSN ノードが処理した証明書ベースの認証要求の数。

フィールド	使用上のガイドライン
[失敗した証明書（Certificates Failed）]	PSN ノードが処理する失敗した認証要求の数。

関連トピック

発行された証明書 （137 ページ）
ユーザーおよびエンドポイントの証明書の更新 （117 ページ）
証明書を使用してパーソナル デバイスを許可するための Cisco ISE の設定 （143 ページ）
ユーザーによる証明書の更新を許可する Cisco ISE の設定 （118 ページ）
エンドポイント証明書の失効 （163 ページ）

Cisco ISE CA 証明書およびキーのバックアップと復元

PAN に障害が発生し、セカンダリ管理ノードを外部 PKI のルート CA または中間 CA として機能させるために昇格する場合に備え、Cisco ISE CA 証明書およびキーをセキュアにバックアップして、セカンダリ管理ノードにこれらを復元できるようにする必要があります。Cisco ISE 設定のバックアップには、CA 証明書とキーは含まれていません。CA 証明書およびキーをリポジトリにエクスポートおよびインポートするには、代わりにコマンドラインインターフェイス（CLI）を使用する必要があります。**application configure ise** コマンドには、CA 証明書およびキーのバックアップと復元のためのエクスポートおよびインポートのオプションが含まれています。

信頼できる証明書ストアからの次の証明書が、セカンダリ管理ノードで復元されます。

- Cisco ISE ルート CA 証明書
- Cisco ISE サブ CA 証明書
- Cisco ISE エンドポイント RA 証明書
- Cisco ISE OCSP 応答側証明書

次の場合、Cisco ISE CA 証明書およびキーのバックアップおよび復元が必要となります。

- 展開内にセカンダリ管理ノードが存在する
- Cisco ISE CA ルート チェーン全体を置き換える
- 外部 PKI の下位 CA として機能するように Cisco ISE ルート CA を設定する
- リリース 1.2 からそれ以降のリリースにアップグレードする
- 設定のバックアップからデータを復元する。この場合、最初に Cisco ISE CA ルート チェーンを再生成し、次に ISE CA 証明書およびキーのバックアップと復元を行う必要があります。

（注） 展開で Cisco ISE の内部 CA を置き換えるたびに、完全な証明書チェーンを取得するように ISE メッセージング サービスも更新する必要があります。

Cisco ISE CA 証明書およびキーのエクスポート

CA 証明書およびキーを PAN からエクスポートし、セカンダリ管理ノードでインポートする必要があります。このオプションでは、PAN がダウンした場合にセカンダリ管理ノードでエンドポイントの証明書を発行および管理し、セカンダリ管理ノードを PAN に昇格させることができます。

始める前に

CA 証明書およびキーを格納するためのリポジトリを作成したことを確認します。

ステップ 1 Cisco ISE CLI から、**application configure ise** コマンドを入力します。

ステップ 2 7 を入力して、証明書およびキーをエクスポートします。

ステップ 3 リポジトリの名前を入力します。

ステップ 4 暗号キーを入力します。

エクスポートされた証明書のリスト、件名、発行者、およびシリアル番号とともに成功メッセージが表示されます。

例：

```
 The following 4 CA key pairs were exported to repository 'sftp' at 'ise_ca_key_pairs_of_ise-vm1':
        Subject:CN=Cisco ISE Self-Signed CA of ise-vm1
        Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
        Serial#:0x621867df-568341cd-944cc77f-c9820765

        Subject:CN=Cisco ISE Endpoint CA of ise-vm1
        Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
        Serial#:0x7027269d-d80a406d-831d5c26-f5e105fa

        Subject:CN=Cisco ISE Endpoint RA of ise-vm1
        Issuer:CN=Cisco ISE Endpoint CA of ise-vm1
        Serial#:0x1a65ec14-4f284da7-9532f0a0-8ae0e5c2

        Subject:CN=Cisco ISE OCSP Responder Certificate of ise-vm1
        Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
        Serial#:0x6f6d4097-21f74c4d-8832ba95-4c320fb1
ISE CA keys export completed successfully
```

Cisco ISE CA 証明書およびキーのインポート

セカンダリ管理ノードを登録したら、PAN から CA 証明書およびキーをエクスポートし、セカンダリ管理ノードにインポートします。

ステップ 1 Cisco ISE CLI から、**application configure ise** コマンドを入力します。

ステップ 2 8 を入力して、CA 証明書およびキーをインポートします。

ステップ 3 リポジトリの名前を入力します。

ステップ 4 インポートするファイルの名前を入力します。ファイル名は **ise_ca_key_pairs_of_<vm hostname>** 形式である必要があります。

ステップ 5 ファイルを復号化するための暗号キーを入力します。

処理が正常に完了したことを知らせるメッセージが表示されます。

例：

```
The following 4 CA key pairs were imported:
        Subject:CN=Cisco ISE Self-Signed CA of ise-vm1
        Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
        Serial#:0x21ce1000-8008472c-a6bc4fd9-272c8da4

        Subject:CN=Cisco ISE Endpoint CA of ise-vm1
        Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
        Serial#:0x05fa86d0-092542b4-8ff68ed4-f1964a56

        Subject:CN=Cisco ISE Endpoint RA of ise-vm1
        Issuer:CN=Cisco ISE Endpoint CA of ise-vm1
        Serial#:0x77932e02-e8c84b3d-b27e2f1c-e9f246ca

        Subject:CN=Cisco ISE OCSP Responder Certificate of ise-vm1
        Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
        Serial#:0x5082017f-330e412f-8d63305d-e13fd2a5

Stopping ISE Certificate Authority Service...
Starting ISE Certificate Authority Service...
ISE CA keys import completed successfully
```

（注） エクスポートされたキーファイルの暗号化は、Cisco ISE リリース 2.6 で導入されました。Cisco ISE リリース 2.4 以前のバージョンからのキーのエクスポート、および Cisco ISE リリース 2.6 以降のバージョンでのキーのインポートは成功しません。

プライマリ PAN および PSN でのルート CA および下位 CA の生成

展開をセットアップする場合、Cisco ISE は、Cisco ISE CA サービスの PSN のプライマリ PAN と下位の CA 証明書でルート CA を生成します。ただし、プライマリ PAN または PSN のドメイン名またはホスト名を変更する場合は、プライマリ PAN でルート CA、PSN で下位 CA をそれぞれ再生成する必要があります。

PSN のホスト名を変更する場合は、プライマリ PAN および PSN でそれぞれルート CA と下位 CA を再生成する代わりに、ホスト名を変更する前に PSN を登録解除し、再登録できます。新しい下位証明書は PSN 上で自動的にプロビジョニングされます。

（注） PXgrid および IMS 証明書は、それぞれの証明書が外部で署名されている場合、ルート CA の再生成中に内部 CA によって置き換えられません。

PXgrid 証明書の内部 CA による署名を変更する場合は、自己署名 Pxgrid 証明書を生成し、ルート CA を再生成します。

Cisco ISE メッセージングサービス証明書の内部 CA による署名を変更する場合は、CSR ページから Cisco ISE メッセージングサービス証明書を再生成します。

ステップ 1 を選択します。**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [証明書署名要求（Certificate Signing Requests）]** を選択します。

ステップ 2 [証明書署名要求（CSR）の生成（Generate Certificate Signing Requests (CSR)）] をクリックします。

ステップ 3 [証明書の使用先（Certificate(s) will be used for）] ドロップダウン リストから ISE ルート CA を選択します。

ステップ 4 [ISE ルート CA 証明書チェーンの置き換え（Replace ISE Root CA Certificate chain）] をクリックします。

ルート CA と下位 CA 証明書が、展開内のすべてのノードに対して生成されます。

外部 PKI の下位 CA としての Cisco ISE ルート CA の設定

外部 PKI の下位 CA として機能する PAN のルート CA が必要な場合は、ISE 中間 CA 証明書署名要求を生成して、外部 CA に送信し、ルートおよび CA 署名付き証明書を入手して、ルート CA 証明書を信頼できる証明書ストアにインポートし、CA 署名付き証明書を CSR にバインドします。この場合、外部 CA はルート CA、プライマリ PAN は外部 CA の下位 CA、PSN はプライマリ PAN の下位 CA です。

ステップ 1 **[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [証明書署名要求（Certificate Signing Requests）]** を選択します。

ステップ 2 [証明書署名要求（CSR）の生成（Generate Certificate Signing Requests (CSR)）] をクリックします。

ステップ 3 [証明書の使用目的（Certificate(s) will be used for）] ドロップダウン リストから [ISE 中間 CA（ISE Intermediate CA）] を選択します。

ステップ 4 [生成（Generate）] をクリックします。

ステップ 5 CSR をエクスポートし、外部 CA に送信して、CA 署名付き証明書を取得します。

ステップ 6 信頼できる証明書ストアに外部 CA のルート CA 証明書をインポートします。

ステップ 7 CSR に CA 署名付き証明書をバインドします。

次のタスク

展開にセカンダリ PAN がある場合は、プライマリ PAN から Cisco ISE CA 証明書およびキーのバックアップを取得し、セカンダリ PAN で復元します。サーバー証明書とルート証明書は、セカンダリ PAN に自動的に複製されます。この複製によって、管理ノードに障害が発生した場合に、セカンダリ PAN が外部 PKI の下位 CA として機能するようになります。

証明書を使用してパーソナル デバイスを許可するための Cisco ISE の設定

ネットワークに接続するエンドポイント（パーソナルデバイス）の証明書を発行し、管理するように Cisco ISE を設定できます。内部 Cisco ISE CA サービスを使用して、エンドポイントから証明書署名要求に署名したり、外部 CA に CSR を転送したりすることができます。

始める前に

- プライマリ PAN から Cisco ISE CA 証明書およびキーのバックアップを取得し、ディザスタリカバリのため、安全な場所に保管してください。

ステップ 1 Employee ユーザーグループへのユーザーの追加 （144 ページ）。
内部 ID ストアまたは Microsoft Active Directory などの外部 ID ストアにユーザーを追加できます。

ステップ 2 TLS ベース認証の証明書認証プロファイルの作成 （144 ページ） を

ステップ 3 TLS ベース認証の ID ソース順序の作成 （145 ページ）。

ステップ 4 クライアント プロビジョニング ポリシーの作成：

a) 認証局の設定 （145 ページ）
b) CA テンプレートの作成 （147 ページ）
c) クライアント プロビジョニング ポリシーで使用されるネイティブ サプリカント プロファイルの作成 （150 ページ）
d) Cisco からの Windows および Mac OS X オペレーティングシステムのエージェントリソースのダウンロード （151 ページ）
e) Apple iOS、Android および MAC OS X デバイスのクライアント プロビジョニング ポリシー ルールの作成 （151 ページ）

ステップ 5 TLS ベース認証の Dot1X 認証ポリシー ルールの設定 （152 ページ）

ステップ 6 TLS ベース認証用の許可ポリシー ルールを設定します。

a) 中央 Web 認証とサプリカント プロビジョニング フローの許可プロファイルの作成 （153 ページ）
b) 許可ポリシー ルールの作成 （153 ページ）

パーソナル デバイスからワイヤレス SSID に接続するときに ECC RSA ベースの証明書を使用すると、2 回目のパスワード入力を行うよう求められます。

Employee ユーザーグループへのユーザーの追加

次の手順では、Cisco ISE ID ストアの Employee ユーザー グループにユーザーを追加する方法について説明します。外部 ID ストアを使用した場合でも、ユーザーを追加できる Employee ユーザー グループがあることを確認します。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [ID（Identities）] > [ユーザー（Users）]** 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 ユーザーの詳細情報を入力します。

ステップ 4 [パスワード（Passwords）] セクションで、[ログインパスワード（Login Password）] と [TACACS+イネーブルパスワード（TACACS+ Enable Password）] を選択し、ネットワーク デバイスにアクセス レベルを設定します。

ステップ 5 [ユーザー グループ（User Group）] ドロップダウン リストから [従業員（Employee）] を選択します。

Employee ユーザー グループに属するすべてのユーザーが同じ権限セットを共有します。

ステップ 6 **[送信（Submit）]** をクリックします。

次のタスク

TLS ベース認証の証明書認証プロファイルの作成 （144 ページ）

TLS ベース認証の証明書認証プロファイルの作成

ネットワークに接続するエンドポイントの認証に証明書を使用するには、Cisco ISE で証明書認証プロファイルを定義するか、またはデフォルトの Preloaded_Certificate_Profile を編集する必要があります。証明書認証プロファイルには、プリンシパルユーザー名として使用する必要がある証明書フィールドが含まれています。たとえば、ユーザー名が [一般名（Common Name）] フィールドにある場合は、証明書認証プロファイルを [プリンシパル ユーザー名（Principal Username）] が [サブジェクト - 一般名（Subject - Common Name）] であるとして定義できます。これは ID ストアに照らして確認できます。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [証明書認証プロファイル（Certificate Authentication Profile）]** を選択します。

ステップ 2 証明書認証プロファイルの名前を入力します。たとえば、CAP となります。

ステップ 3 [サブジェクト - 一般名（Subject - Common Name）] に [プリンシパル ユーザー名 X509 属性（Principal Username X509 Attribute）] を選択します。

ステップ 4 [保存（Save）] をクリックします。

次のタスク

TLS ベース認証の ID ソース順序の作成 （145 ページ）

TLS ベース認証の ID ソース順序の作成

証明書認証プロファイルを作成したら、Cisco ISE が証明書の属性を取得し、定義した ID ソースを ID ソース順序で照合できるように、証明書認証プロファイルを ID ソース順序に追加します。

始める前に

次のタスクが完了していることを確認します。

- Employee ユーザー グループへのユーザーの追加。
- 証明書ベースの認証の証明書認証プロファイルの作成。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [ID ソース順序（Identity Source Sequences）]** 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 ID ソース順序の名前を入力します。たとえば、Dot1X となります。

ステップ 4 [証明書認証プロファイルの選択（Select Certificate Authentication Profile）] チェックボックスをオンにし、作成した証明書認証プロファイル、つまり CAP を選択します。

ステップ 5 ユーザー情報を含む ID ソースを [認証検索リスト（Authentication Search List）] 領域の [選択済み（Selected）] リスト ボックスに移動します。

追加の ID ソースを追加すると、一致が見つかるまで Cisco ISE は、これらのデータ ストアを順に検索します。

ステップ 6 [ユーザーが見つからなかったとして処理し、順序内の次のストアに進む（Treat as if the user was not found and proceed to the next store in the sequence）] オプション ボタンをクリックします。

ステップ 7 **[送信（Submit）]** をクリックします。

次のタスク

認証局の設定 （145 ページ）

認証局の設定

CSR への署名に外部 CA を使用する場合、外部 CA を設定する必要があります。外部 CA 設定は Cisco ISE の以前のリリースでは、SCEP RA プロファイルと呼ばれていました。Cisco ISE CA を使用する場合、CA 設定を明示的に設定する必要はありません。[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [内部 CA 設定（Internal CA Settings）] で、内部 CA 設定を確認できます。

ユーザーのデバイスが検証済みの証明書を受信すると、証明書はデバイス上の次の表の場所に置かれます。

表 *18*：デバイス証明書の場所

デバイス	証明書ストレージの場所	アクセス方式
iPhone/iPad	標準の証明書ストア	[設定（Settings）] > [一般（General）] > [プロファイル（Profile）]
Android	暗号化された証明書ストア	エンドユーザーに不可視です。 （注） 証明書は、[設定（Settings）] > [ロケーションおよびセキュリティ（Location & Security）] > [ストレージのクリア（Clear Storage）] を使用して削除できます。
Windows	標準の証明書ストア	**/cmd** プロンプトから mmc.exe を起動するか、または証明書スナップインで表示します。
Mac	標準の証明書ストア	[アプリケーション（Application）] > [ユーティリティ（Utilities）] > [キーチェーン アクセス（Keychain Access）]

始める前に

証明書署名要求（CSR）への署名に外部認証局（CA）を使用する場合は、外部 CA の URL が必要となります。

ステップ 1 **[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [外部 CA 設定（External CA Settings）]** 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 外部 CA 設定の名前を入力します。たとえば、EXTERNAL_SCEP などです。

ステップ 4 [URL] テキスト ボックスに、外部 CA サーバーの URL を入力します。

外部 CA が到達可能かどうかを確認するには、[テスト接続（Test Connection）] をクリックします。追加 CA サーバーの URL を入力するには、[+] ボタンをクリックします。

ステップ 5 **[送信（Submit）]** をクリックします。

次のタスク

CA テンプレートの作成 （147 ページ）

CA テンプレートの作成

証明書テンプレートは、（内部または外部 CA のために）使用する必要がある SCEP RA プロファイル、キー タイプ、キー サイズ、曲線タイプ、サブジェクト、サブジェクト代替名（SAN）、証明書の有効期間、拡張キーの使用状況を定義します。この例では、内部 Cisco ISE CA を使用すると想定します。外部 CA テンプレートの場合、有効期間は外部 CA によって決定され、指定することはできません。

新しい CA テンプレートを作成するか、デフォルトの証明書テンプレート EAP_Authentication_Certificate_Template を編集できます。

デフォルトでは、次の CA テンプレートが Cisco ISE で使用できます。

- CA_SERVICE_Certificate_Template：ISE CA を使用する他のネットワーク サービス用。たとえば、ASA VPN ユーザーに対し証明書を発行するには、ISE の設定時にこの証明書テンプレートを使用します。
- EAP_Authentication_Certificate_Template：EAP 認証用。
- pxGrid_Certificate_Template：証明書プロビジョニング ポータルから証明書を生成する際の pxGrid コントローラ用。

（注） ECC キー タイプを使用する証明書テンプレートは、内部 Cisco ISE CA とのみ使用することができます。

始める前に

CA が設定されていることを確認します。

ステップ 1 **[管理（Administration）] > [システム（System）] > [CA サービス（CA Service）] > [内部 CA 証明書テンプレート（Internal CA Certificate Template）]** を選択します。

ステップ 2 内部 CA テンプレートの名前を入力します。たとえば、Internal_CA_Template とします。

ステップ 3 （オプション）[組織ユニット（Organizational Unit）]、[組織（Organization）]、[都市（City）]、[州/都道府県（State）]、[国（Country）] フィールドに値を入力します。

証明書テンプレート フィールド（[組織ユニット（Organizational Unit）]、[組織（Organization）]、[都市（City）]、[州（State）]、および [国（Country）]）の UTF-8 文字はサポートしていません。UTF-8 文字を証明書テンプレートで使用すると、証明書プロビジョニングが失敗します。

証明書を生成する内部ユーザーのユーザー名が、証明書の共通名として使用されます。Cisco ISE 内部 CA は、「+」または「*」の文字を [共通名（Common Name）] フィールドでサポートしていません。ユーザー名に「+」または「*」の特殊文字が含まれていないことを確認してください。

ステップ 4 サブジェクト代替名（SAN）および証明書の有効期間を指定します。

ステップ 5 キー タイプを指定します。RSA または ECC を選択します。

次の表に、ECC をサポートしているオペレーティング システムおよびバージョンと、サポートされている曲線タイプを示します。デバイスがサポートされているオペレーティング システムを実行していない場合、またはサポートされているバージョンでない場合には、代わりに RSA ベースの証明書を使用することもできます。

オペレーティング システム	サポートされるバージョン	サポートされる曲線タイプ
Windows	8 以降	P-256、P-384、P-521
Android	4.4 以降 （注） Android 6.0 は、ECC 証明書をサポートするために 2016 年 5 月のパッチが必要です。	すべての曲線タイプ（P-192 曲線タイプをサポートしていない Android 6.0 を除く）。

Windows 7 と Apple iOS は、EAP-TLS 認証用の ECC をネイティブでサポートしていません。Cisco ISE のこのリリースでは、Mac OS X デバイスでの ECC 証明書の使用はサポートされていません。

ネットワークのデバイスがサポートされていないオペレーティング システム（Windows 7、MAC OS X、Apple iOS）を実行する場合は、キー タイプとして RSA を選択することを推奨します。

ステップ 6 （RSA キー タイプを選択する場合に適用）キー サイズを指定します。1024 以上のキー サイズを選択する必要があります。

ステップ 7 （ECC キー タイプを選択する場合にのみ適用）曲線タイプを指定します。デフォルトは P-384 です。

ステップ 8 ISE 内部 CA を SCEP RA プロファイルとして選択します。

ステップ 9 有効期間を日数単位で入力します。デフォルトは 730 日です。有効な範囲は 1 ～ 730 です。

ステップ 10 拡張キーの使用状況を指定します。証明書をクライアント認証に使用する場合は、[クライアント認証（Client Authentication）] チェック ボックスにマークを付けます。証明書をサーバー認証に使用する場合は、[サーバー認証（Server Authentication）] チェック ボックスにマークを付けます。

ステップ 11 [送信（Submit）] をクリックします。

内部 CA 証明書テンプレートが作成され、クライアント プロビジョニング ポリシーによって使用されます。

次のタスク

クライアント プロビジョニング ポリシーで使用されるネイティブ サプリカント プロファイルの作成 （150 ページ）

内部 CA の設定

次の表では、[内部 CA の設定（Internal CA Settings）] ウィンドウのフィールドについて説明します。内部 CA の設定を表示し、このウィンドウから内部 CA サービスを無効にできます。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして、**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [認証局（Certificate Authority）] > [内部 CA 設定（Internal CA Settings）]**の順に選択します。

表 *19* : 内部 *CA* の設定

フィールド名	使用上のガイドライン
認証局の無効化（Disable Certificate Authority）	内部 CA サービスを無効にするには、このボタンをクリックします。
ホスト名（Host Name）	CA サービスを実行している Cisco ISE ノードのホスト名。
ペルソナ（Personas）	CA サービスを実行しているノードで有効な Cisco ISE ノードのペルソナ。たとえば、管理、ポリシー サービスなどです。
ロール（Role(s)）	CA サービスを実行する Cisco ISE ノードが担当するロール。たとえば、スタンドアロンまたはプライマリまたはセカンダリです。
CA、EST、および OCSP 応答側のステータス（CA, EST & OCSP Responder Status）	有効または無効
OCSP 応答側 URL（OCSP Responder URL）	OCSP サーバーにアクセスするための Cisco ISE ノードの URL。
SCEP URL	SCEP サーバーにアクセスするための Cisco ISE ノードの URL。

関連トピック

Cisco ISE CA サービス （122 ページ）
証明書を使用してパーソナル デバイスを許可するための Cisco ISE の設定 （143 ページ）

クライアントプロビジョニングポリシーで使用されるネイティブサプリカントプロファイルの作成

ネイティブサプリカントプロファイルを作成して、ユーザーがパーソナルデバイスを企業ネットワークに含めることができます。Cisco ISE では、異なるオペレーティング システムごとに異なるポリシー ルールを使用します。各クライアント プロビジョニング ポリシー ルールには、どのオペレーティング システムにどのプロビジョニング ウィザードを使用するかを指定するネイティブ サプリカント プロファイルが含まれています。

始める前に

- Cisco ISE で CA 証明書テンプレートを設定します。
- TCP ポート 8905 および UDP ポート 8905 を開き、クライアントエージェントとサプリカントのプロビジョニングウィザードのインストールを有効にします。ポートの使用法の詳細については、『*Cisco Identity Services Engine Hardware Installation Guide*』の付録「Cisco ISE Appliance Ports Reference」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）] > [クライアント プロビジョニング（Client Provisioning）] > [リソース（Resources）]** を選択します。

ステップ 2 **[追加（Add）] > [ネイティブ サプリカント プロファイル（Native Supplicant Profile）]** を選択します。

ステップ 3 ネイティブ サプリカント プロファイルの名前を入力します。たとえば、EAP_TLS_INTERNAL となります。

ステップ 4 [オペレーティング システム（Operating System）] ドロップダウン リストから [すべて（ALL）] を選択します。

（注） MAC OS バージョン 10.10 のユーザーは、デュアル SSID PEAP フローに対してプロビジョニングされた SSID に手動で接続する必要があります。

ステップ 5 [有線（Wired）] または [無線（Wireless）] チェックボックスをオンにします。

ステップ 6 [許可されるプロトコル（Allowed Protocol）] ドロップダウン リストから [TLS] を選択します。

ステップ 7 以前に作成した CA 証明書テンプレートを選択します。

ステップ 8 **[送信（Submit）]** をクリックします。

次のタスク

Cisco からの Windows および Mac OS X オペレーティングシステムのエージェントリソースのダウンロード （151 ページ）

Cisco からの Windows および Mac OS X オペレーティングシステムのエージェントリソースのダウンロード

Windows および Mac OS X オペレーティング システムでは、Cisco サイトからリモート リソースをダウンロードする必要があります。

始める前に

ネットワークのプロキシ設定が正しく設定されていることを確認し、適切なリモート ロケーションにアクセスして、クライアント プロビジョニング リソースを Cisco ISE にダウンロードできることを確認します。

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [リソース（Resources）] > [クライアント プロビジョニング（Client Provisioning）] > [リソース（Resources）]** を選択します。

ステップ 2 **[追加（Add）] > [Cisco サイトのエージェント リソース（Agent resources from Cisco site）]** を選択します。

ステップ 3 [Windows] および [MAC OS X] パッケージの隣にあるチェックボックスをオンにします。必ず最新バージョンを含めます。

ステップ 4 [保存（Save）] をクリックします。

次のタスク

Apple iOS、Android および MAC OS X デバイスのクライアント プロビジョニング ポリシー ルールの作成 （151 ページ）

Apple iOS、Android および MAC OS X デバイスのクライアント プロビジョニング ポリシー ルールの作成

クライアント プロビジョニング リソース ポリシーは、どのユーザーがリソース（エージェント、エージェント コンプライアンス モジュール、エージェント カスタマイズ パッケージ/プロファイル）のどのバージョン（または複数のバージョン）をログイン時およびユーザー セッション開始時に Cisco ISE から受信するかを決定します。

エージェント コンプライアンス モジュールをダウンロードすると、システムで使用している既存のモジュールがあれば常にそれが上書きされます。

従業員が iOS、Android、および MAC OS X デバイスを持ち込むことができるようにするには、[クライアント プロビジョニング ポリシー（Client Provisioning Policy）] ページでこれらの各デバイスのポリシー ルールを作成する必要があります。

始める前に

必要なネイティブ サプリカント プロファイルを設定し、[クライアント プロビジョニング ポリシー（Client Provisioning Policy）] ページから必要なエージェントをダウンロードしておく必要があります。

ステップ 1 **[ポリシー（Policy）]** > **[クライアント プロビジョニング（Client Provisioning）]** を選択します。
ステップ 2 Apple iOS、Android および MAC OS X デバイスのクライアント プロビジョニング ポリシー ルールの作成
ステップ 3 [保存（Save）] をクリックします。

次のタスク

TLS ベース認証の Dot1X 認証ポリシー ルールの設定 （152 ページ）

TLS ベース認証の Dot1X 認証ポリシー ルールの設定

このタスクは、TLS ベース認証の Dot1X 認証ポリシー ルールを更新する方法を示します。

始める前に

TLS ベース認証用に作成された証明書認証プロファイルが存在することを確認します。

ステップ 1 **[ポリシー（Policy）]** > **[ポリシー セット（Policy Sets）]** を選択します。
ステップ 2 [表示（View）] 列から矢印アイコン をクリックすると、[設定（Set）] ビュー画面が開き、認証ポリシーを表示、管理、および更新できます。

デフォルトのルールベースの認証ポリシーには、Dot1X 認証用のルールが含まれます。

ステップ 3 Dot1X 認証ポリシー ルールの条件を編集するには、[条件（Conditions）] 列のセルにカーソルを合わせ、 をクリックします。条件スタジオが開きます。
ステップ 4 Dot1X ポリシー ルールの [アクション（Actions）] 列で、歯車アイコンをクリックし、必要に応じてドロップダウンメニューから、挿入または複製オプションのいずれかを選択して新しいポリシー セットを挿入します。
[ポリシー セット（Policy Sets）] テーブルに新しい行が表示されます。
ステップ 5 ルールの名前を入力します。たとえば、eap-tls と入力します。
ステップ 6 [条件（Conditions）] 列から、（+）記号をクリックします。
ステップ 7 [条件スタジオ（Conditions Studio）] ページで必要な条件を作成します。[エディタ（Editor）] セクションで、[クリックして属性を追加する（Click To Add an Attribute）] テキスト ボックスをクリックし、必要なディクショナリと属性（たとえば、Network Access:UserName Equals User1）を選択します。

ライブラリ条件を [クリックして属性を追加する（Click To Add An Attribute）] テキスト ボックスにドラッグ アンド ドロップできます。

ステップ 8 [使用（Use）] をクリックします。
ステップ 9 デフォルト ルールは、そのままにします。
ステップ 10 [保存（Save）] をクリックします。

次のタスク

中央 Web 認証とサプリカント プロビジョニング フローの許可プロファイルの作成 （153 ページ）

中央 Web 認証とサプリカント プロビジョニング フローの許可プロファイルの作成

許可プロファイルを定義して、証明書ベースの認証の成功後にユーザーに付与するアクセスを決定します。

始める前に

ワイヤレス LAN コントローラ（WLC）に必要なアクセス コントロール リスト（ACL）が設定されていることを確認します。WLC での ACL の作成方法については、『*TrustSec How-To Guide: Using Certificates for Differentiated Access*』を参照してください。

この例では、WLC で次の ACL が作成されていると仮定します。

- NSP-ACL：ネイティブ サプリカント プロビジョニング用
- BLACKHOLE：ブロックリストに登録されているデバイスへのアクセスの制限
- NSP-ACL-Google：Android デバイスのプロビジョニング

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）]** を選択します。

ステップ 2 新しい許可プロファイルを作成するには、[追加（Add）] をクリックします。

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）] ドロップダウン リストから、[ACCESS_ACCEPT] を選択します。

ステップ 5 中央 Web 認証、Google Play の中央 Web 認証、ネイティブ サプリカント プロビジョニング、および Google のネイティブ サプリカント プロビジョニングの許可プロファイルを追加するには、[追加（Add）] をクリックします。

ステップ 6 [保存（Save）] をクリックします。

次のタスク

許可ポリシー ルールの作成 （153 ページ）

許可ポリシー ルールの作成

Cisco ISE は、許可ポリシー ルールを評価し、ポリシー ルールで指定された許可プロファイルに基づいてネットワーク リソースへのアクセス権をユーザーに付与します。

始める前に

必要な許可プロファイルを作成済みであることを確認します。

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 デフォルトのルールの上に追加のポリシー ルールを挿入します。

ステップ 3 [保存（Save）] をクリックします。

CA サービス ポリシーのリファレンス

ここでは、Cisco ISE CA サービスを有効にする前に作成する必要がある許可ポリシー ルールおよびクライアント プロビジョニング ポリシー ルールの詳細情報について説明します。

証明書サービスのクライアント プロビジョニング ポリシー ルール

ここでは、Cisco ISE 証明書サービスを使用している場合に作成する必要があるクライアント プロビジョニング ポリシー ルールについて説明します。次の表に詳細を示します。

ルール名	ID グループ	オペレーティング システム	その他の条件	結果
iOS	任意（Any）	Apple iOS すべて	条件	EAP_TLS_INTERNAL（以前に作成したネイティブ サプリカント プロファイル）。外部 CA を使用している場合は、外部 CA 用に作成したネイティブ サプリカント プロファイルを選択します。
Android	任意（Any）	Android	条件	EAP_TLS_INTERNAL（以前に作成したネイティブ サプリカント プロファイル）。外部 CA を使用している場合は、外部 CA 用に作成したネイティブ サプリカント プロファイルを選択します。

ルール名	ID グループ	オペレーティングシステム	その他の条件	結果
MAC OS X	任意（Any）	MACOSX	条件	ネイティブ サプリカントの設定で、次を指定してください。 1. [設定ウィザード（Config Wizard）]：シスコのサイトからダウンロードした MAC OS X サプリカントのウィザードを選択します。 2. ウィザードのプロファイル：以前作成した EAP_TLS_INTERNAL ネイティブ サプリカントのプロファイルを選択します。外部 CA を使用している場合は、外部 CA 用に作成したネイティブ サプリカント プロファイルを選択します。

証明書サービスの許可プロファイル

ここでは、Cisco ISE で証明書ベースの認証を有効にするために作成する必要がある許可プロファイルについて説明します。ワイヤレス LAN コントローラ（WLC）の ACL（NSP-ACL および NSP-ACL-Google）がすでに作成されている必要があります。

- CWA：このプロファイルは、中央 Web 認証フローを使用するデバイス用です。[Web 認証（Web Authentication）] チェックボックスをオンにして、ドロップダウン リストから [中央集中（Centralized）] を選択し、ACL テキスト ボックスに NSP-ACL を入力します。
- CWA_GooglePlay：このプロファイルは、中央 Web 認証フローを使用する Android デバイス用です。このプロファイルによって、Android デバイスは Google Play ストアにアクセスし、Cisco Network Setup Assistant をダウンロードできます。[Web 認証（Web Authentication）] チェックボックスをオンにして、ドロップダウン リストから [中央集中（Centralized）] を選択し、ACL テキスト ボックスに NSP-ACL-Google を入力します。
- NSP：このプロファイルは、サプリカント プロビジョニング フローを使用する非 Android デバイス用です。[Web 認証（Web Authentication）] チェックボックスをオンにして、ドロップダウン リストから [サプリカント プロビジョニング（Supplicant Provisioning）] を選択し、ACL テキスト ボックスに NSP-ACL を入力します。
- NSP-Google：このプロファイルは、サプリカント プロビジョニング フローを使用する Android デバイス用です。[Web 認証（Web Authentication）] チェックボックスをオンにして、ドロップダウン リストから [サプリカント プロビジョニング（Supplicant Provisioning）] を選択し、ACL テキスト ボックスに NSP-ACL-Google を入力します。

デフォルトの Blackhole_Wireless_Access 許可プロファイルを確認します。高度な属性設定を次のように設定する必要があります。

- Cisco:cisco-av-pair = url-redirect=https://*ip:port*/blockedlistportal/gateway?portal=*PortalID*
- Cisco:cisco-av-pair = url-redirect-acl=BLACKHOLE

証明書サービスの許可ポリシー ルール

ここでは、Cisco ISE CA サービスを有効にするときに作成する必要がある許可ポリシー ルールについて説明します。

- 企業資産：このルールは、802.1X および MSCHAPV2 プロトコルを使用して企業のワイヤレス SSID に接続する企業のデバイス用です。
- Android_SingleSSID：このルールは、Google Play ストアにアクセスして、プロビジョニングのために Cisco Network Setup Assistant をダウンロードする Android デバイス用です。このルールは、シングル SSID 設定に固有です。
- Android_DualSSID：このルールは、Google Play ストアにアクセスして、プロビジョニングのために Cisco Network Setup Assistant をダウンロードする Android デバイス用です。このルールは、デュアル SSID 設定に固有です。
- CWA：このルールは、中央 Web 認証フローを使用するデバイス用です。
- NSP：このルールは、EAP-TLS 認証の証明書を使用するネイティブ サプリカント プロビジョニング フローを使用するデバイス用です。
- EAP-TLS：このルールは、サプリカント プロビジョニング フローを完了したデバイスおよび証明書でプロビジョニングされるデバイス用です。デバイスには、ネットワークへのアクセス権限が付与されます。

次の表に、Cisco ISE CA サービスの許可ポリシー ルールを設定するときに選択する必要がある属性および値を示します。この例では、Cisco ISE で対応する許可プロファイルも設定しているものと想定します。

ルール名	条件	権限（適用される許可プロファイル）
企業資産	Corp_Assets AND（Wireless 802.1X AND Network Access:AuthenticationMethod EQUALS MSCHAPV2）	PermitAccess
Android_SingleSSID	（Wireless 802.1X AND Network Access:AuthenticationMethod EQUALS MSCHAPV2 AND Session:Device-OS EQUALS Android）	NSP_Google
Android_DualSSID	（Wireless_MAB AND Session:Device-OS EQUALS Android）	CWA_GooglePlay
CWA	Wireless_MAB	CWA
NSP	（Wireless 802.1X AND Network Access:AuthenticationMethod EQUALS MSCHAPV2）	NSP
EAP-TLS	（Wireless 802.1X AND Network Access:AuthenticationMethod EQUALS x509_PKI	PermitAccess

Cisco ISE CA による ASA VPN ユーザーへの証明書の発行

ISE CA は、ASA VPN 経由で接続しているクライアント マシンに証明書を発行します。この機能を使用して、ASA VPN 経由で接続しているエンド デバイスに証明書を自動的にプロビジョニングできます。

Cisco ISE は、Simple Certificate Enrollment Protocol（SCEP）を使用して登録を行い、証明書をクライアント マシンにプロビジョニングします。AnyConnect クライアントは、HTTPS 接続で ASA に SCEP 要求を送信します。ASA は、Cisco ISE と ASA の間に確立された HTTP 接続を介して Cisco ISE に要求を中継する前に、要求を評価し、ポリシーを適用します。Cisco ISE CA からの応答はクライアントに中継されます。ASA は、SCEP メッセージの内容を読み取ることはできず、Cisco ISE CA のプロキシとして機能します。Cisco ISE CA は、クライアントからの SCEP メッセージを復号化し、暗号化された形式で応答を送信します。

ISE CA SCEP URL は http://<*IP Address or FQDN of ISE CA server*>:9090/auth/caservice/pkiclient.exe です。ISE ノードの FQDN を使用する場合は、ASA に接続されている DNS サーバーが FQDN を解決できる必要があります。

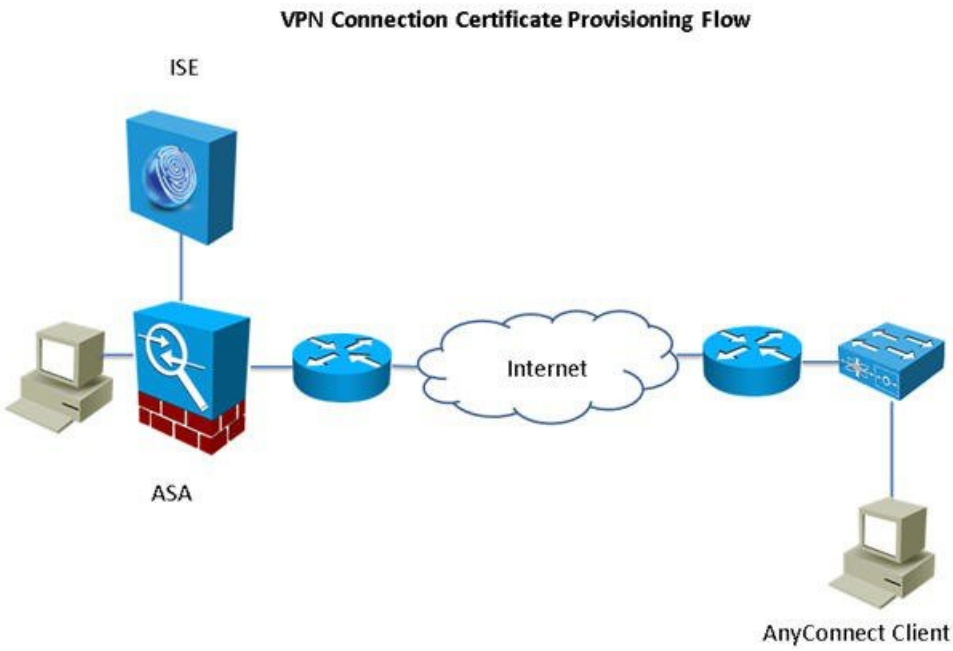
AnyConnect クライアント プロファイルの期限が切れる前に、証明書の更新を設定できます。証明書がすでに期限切れの場合、更新フローは新規登録と同様です。

サポートされているバージョンは次のとおりです。

- ソフトウェア バージョン 8.x を実行する Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス
- Cisco AnyConnect VPN バージョン 2.4 以降

VPN 接続の証明書プロビジョニングフロー

図 *9 : ASA VPN* ユーザーの証明書プロビジョニング



1. ユーザーが VPN 接続を開始します。
2. AnyConnect クライアントは、クライアント マシンをスキャンし、固有デバイス識別子（たとえば IMEI）などの属性を ASA に送信します。
3. ASA はクライアントからの証明書ベースの認証を要求します。証明書がないため、認証は失敗します。
4. ASA は、ユーザー名/パスワードを使用してプライマリ ユーザー認証（AAA）に進み、情報を認証サーバー（ISE）に渡します。
    1. 認証が失敗すると、接続はただちに終了します。
    2. 認証が成功すると、制限付きアクセスが許可されます。aaa.cisco.sceprequired 属性を使用して証明書を要求するクライアント マシンでダイナミック アクセス ポリシー

（DAP）を設定できます。この属性の値を「true」に設定し、ACL および Web ACL を適用できます。

5. VPN 接続は、関連するポリシーと ACL が適用された後に確立されます。クライアントは、AAA 認証が成功し、VPN 接続が確立された後にのみ、SCEP のキー生成を開始します。
6. クライアントは、SCEP 登録を開始し、HTTP を介して ASA に SCEP 要求を送信します。
7. ASA は、要求のセッション情報を検索し、セッションが登録を許可されている場合は、ISE CA に要求をリレーします。
8. ASA は ISE CA からの応答をクライアントにリレー バックします。
9. 登録が成功すると、クライアントにユーザーに対する設定可能メッセージが表示され、VPN セッションが接続解除されます。
10. ユーザーは証明書を使用して再度認証を行うことができ、正常な VPN 接続が確立されます。

ASA VPN ユーザーに証明書を発行する Cisco ISE CA の設定

ASA VPN ユーザーに証明書をプロビジョニングするには、Cisco ISE および ASA で次の設定を行う必要があります。

始める前に

- VPN ユーザー アカウントが Cisco ISE の内部または外部の ID ソースに存在することを確認します。
- ASA および Cisco ISE のポリシー サービス ノードが同じ NTP サーバーを使用して同期されていることを確認します。

ステップ 1 Cisco ISE で ASA をネットワーク アクセス デバイスとして定義します。ネットワーク デバイスとして ASA を追加する方法については、Cisco ISE でのネットワークデバイスの追加 （159 ページ） を参照してください。

ステップ 2 ASA でのグループ ポリシーの設定 （160 ページ）。

ステップ 3 SCEP 登録用の AnyConnect 接続プロファイルの設定 （161 ページ）。

ステップ 4 ASDM での VPN クライアント プロファイルの設定 （161 ページ）。

ステップ 5 ASA への Cisco ISE CA 証明書のインポート。

Cisco ISE でのネットワークデバイスの追加

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

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

始める前に

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

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

ステップ 2 [追加（Add）] をクリックします。

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

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

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

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

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

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

ステップ 9 **[送信（Submit）]** をクリックします。

ASA でのグループ ポリシーの設定

ASA でグループ ポリシーを設定し、SCEP 登録要求を転送するための AnyConnect 用の ISE CA URL を定義します。

ステップ 1 Cisco ASA ASDM にログインします。

ステップ 2 左側の [リモートアクセスVPN（Remote Access VPN）] ナビゲーション ペインから、[グループポリシー（Group Policies）] をクリックします。

ステップ 3 [追加（Add）] をクリックして、グループ ポリシーを作成します。

ステップ 4 グループ ポリシーの名前を入力します。たとえば、ISE_CA_SCEP のようになります。

ステップ 5 [SCEP転送URL（SCEP forwarding URL）] フィールドで、[継承（Inherit）] チェックボックスをオフにして、ポート番号を含む ISE SCEP URL を入力します。

ISE ノードの FQDN を使用する場合は、ASA に接続されている DNS サーバーが ISE ノードの FQDN を解決できる必要があります。

例：

http://ise01.cisco.com:9090/auth/caservice/pkiclient.exe.

ステップ 6 [OK] をクリックして、グループ ポリシーを保存します。

SCEP 登録用の AnyConnect 接続プロファイルの設定

ISE CA サーバー、認証方式、および ISE CA SCEP URL を指定するには、ASA で AnyConnect 接続プロファイルを設定します。

ステップ 1 Cisco ASA ASDM にログインします。

ステップ 2 左側の [リモートアクセスVPN（Remote Access VPN）] ナビゲーション ペインから、[AnyConnect接続プロファイル（AnyConnect Connection Profiles）] をクリックします。

ステップ 3 [追加（Add）] をクリックして、接続プロファイルを作成します。

ステップ 4 接続プロファイルの名前を入力します。たとえば、Cert-Group と入力します。

ステップ 5 （オプション）[エイリアス（Aliases）]フィールドに接続プロファイルの説明を入力します。たとえば、SCEP-Call-ASA とします。

ステップ 6 [認証（Authentication）] 領域で、次の情報を指定します。

- [方式（Method）] : [両方（Both）] オプション ボタンをクリックします
- [AAAサーバーグループ（AAA Server Group）] : [管理（Manage）] をクリックして ISE サーバーを選択します

ステップ 7 [クライアントアドレスの割り当て（Client Address Assignment）] 領域で、使用する DHCP サーバーおよびクライアント アドレス プールを選択します。

ステップ 8 [デフォルトグループポリシー（Default Group Policy）] 領域で、[管理（Manage）] をクリックし、ISE SCEP URL とポート番号で作成したグループ ポリシーを選択します。

例：

たとえば、ISE_CA_SCEP のようになります。

ステップ 9 **[詳細設定（Advanced）]>[一般（General）]** を選択し、この接続プロファイルに対して [Simple Certificate Enrollment Protocolを有効にする（Enable Simple Certificate Enrollment Protocol）] チェックボックスをオンにします。

ステップ 10 [OK] をクリックします。
AnyConnect 接続プロファイルが作成されます。

次のタスク

ASDM での VPN クライアント プロファイルの設定

SCEP 登録用に AnyConnect で VPN クライアント プロファイルを設定します。

ステップ 1 Cisco ASA ASDM にログインします。

ステップ 2 左側の [リモートアクセスVPN（Remote Access VPN）] ナビゲーション ペインから、[AnyConnectクライアントプロファイル（AnyConnect Client Profile）] をクリックします。

ステップ 3 使用するクライアント プロファイルを選択して [編集（Edit）] をクリックします。

ステップ 4 左側の [プロファイル（Profile）] ナビゲーション ペインで、[証明書の登録（Certificate Enrollment）] をクリックします。

ステップ 5 [証明書の登録（Certificate Enrollment）] チェックボックスをオンにします。

ステップ 6 次のフィールドに値を入力します。

- [証明書失効しきい値（Certificate Expiration Threshold）]：AnyConnect がユーザーに対して証明書の失効が近づいていることを証明書の有効期限の何日前に警告するか（SCEP が有効な場合はサポートされません）。デフォルトは 0（警告は表示しない）です。値の範囲は 0 ～ 180 日です。
- [自動SCEPホスト（Automatic SCEP Host）]：SCEP 証明書取得が設定されている ASA のホスト名および接続プロファイル（トンネル グループ）を入力します。ASA の完全修飾ドメイン名（FQDN）または接続プロファイル名を入力してください。たとえば、ホスト名 asa.cisco.com、接続プロファイル名 Cert_Group などです。
- [CA URL]：SCEP CA サーバーを識別します。ISE サーバーの FQDN または IP アドレスを入力します。たとえば、http://ise01.cisco.com:9090/auth/caservice/pkiclient.exe などです。

ステップ 7 証明書の内容をクライアントが要求する方法を定義する値を [証明書の内容（Certificate Contents）] に入力します。

ステップ 8 [OK] をクリックします。
AnyConnect クライアント プロファイルが作成されます。詳細については、お使いのバージョンの AnyConnect の『Cisco AnyConnect Secure Mobility Client』を参照してください。

ASA への Cisco ISE CA 証明書のインポート

Cisco ISE 内部 CA 証明書を ASA にインポートします。

始める前に

Cisco ISE 内部 CA 証明書をエクスポートします。**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [認証局（Certificate Authority）] > [認証局証明書（Certificate Authority Certificates）]** に移動します。[証明書サービスノードCA（Certificate Services Node CA）] および [証明書サービスルートCA（Certificate Services Root CA）] 証明書の横にあるチェックボックスをオンにして、これらの証明書を一度に 1 つずつエクスポートします。

ステップ 1 Cisco ASA ASDM にログインします。

ステップ 2 左側の [リモート アクセス VPN（Remote Access VPN）] ナビゲーション ペインから、**[証明書管理（Certificate Management）] > [CA 証明書（CA Certificates）]** を選択します。

ステップ 3 [追加（Add）] をクリックして Cisco ISE 内部 CA 証明書を選択し、ASA にインポートします。

エンドポイント証明書の失効

従業員のパーソナル デバイスに対して発行された証明書を取り消す必要がある場合は、[エンドポイント証明書（Endpoint Certificates）] ページから取り消すことができます。たとえば、従業員のデバイスが盗難されたり、紛失したりした場合には、Cisco ISE 管理者ポータルにログインし、そのデバイスに発行された証明書を [エンドポイント証明書（Endpoint Certificates）] ページから取り消すことができます。フレンドリ名、デバイスの一意の ID、シリアル番号に基づいて、このページのデータをフィルタリングできます。

PSN（サブ CA）が侵害された場合は、[エンドポイント証明書（Endpoint Certificates）] ページの [発行元（Issued By）] フィールドでフィルタリングすることによって、その PSN によって発行されたすべての証明書を取り消すことができます。

従業員に対して発行された証明書を取り消すときに、アクティブなセッション（その証明書を使用して認証された）がある場合、セッションは即座に終了します。証明書を取り消すと、その直後に、許可されていないユーザーはリソースにアクセスできなくなります。

ステップ 1 **[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [認証局（Certificate Authority）] > [発行された証明書（Issued Certificates）]** を選択します。

ステップ 2 取り消すエンドポイント証明書の隣にあるチェックボックスをオンにし、[失効（Revoke）] をクリックします。

フレンドリ名とデバイス タイプに基づいて証明書を検索できます。

ステップ 3 証明書を取り消す理由を入力します。

ステップ 4 [Yes] をクリックします。

OCSP サービス

Online Certificate Status Protocol（OCSP）は、x.509 デジタル証明書のステータスのチェックに使用されるプロトコルです。このプロトコルは証明書失効リスト（CRL）に代わるものであり、CRL の処理が必要となる問題に対処します。

Cisco ISE には HTTP を介して OCSP サーバーと通信し、認証で証明書のステータスを検証する機能があります。OCSP のコンフィギュレーションは、Cisco ISE で設定されるいずれかの認証局（CA）証明書から参照できる再利用可能な設定オブジェクトで設定されます。

CRL 検証と OCSP 検証の両方または一方を CA ごとに設定できます。両方を選択すると、Cisco ISE では最初に OCSP を介した検証が実行されます。プライマリ OCSP サーバーとセカンダリ OCSP サーバーの両方で通信の問題が検出された場合、または特定の証明書に対して不明のステータスが返された場合、Cisco ISE は CRL チェックの実行に切り替えます。

Cisco ISE CA サービスの Online Certificate Status Protocol レスポンダ

Cisco ISE CA OCSP 応答側は、OCSP クライアントと通信するサーバーです。Cisco ISE CA の OCSP クライアントには、Cisco ISE の内部 OCSP クライアントと適応型セキュリティ アプライアンス（ASA）の OCSP クライアントがあります。OCSP クライアントは、RFC 2560、5019 で定義されている OCSP 要求/応答構造を使用して、OCSP 応答側と通信する必要があります。

Cisco ISE CA は、OCSP 応答側に証明書を発行します。OCSP 応答側は、着信要求をポート 2560 でリッスンします。このポートは、OCSP トラフィックのみを許可するように設定されています。

OCSP 応答側は RFC 2560、5019 で規定された構造に従って要求を受け入れます。OCSP 要求ではナンス拡張がサポートされます。OCSP 応答側は証明書のステータスを取得し、OCSP 応答を作成して署名します。OCSP 応答は、OCSP 応答側ではキャッシュされませんが、クライアントでは最大 24 時間 OCSP 応答をキャッシュすることができます。OCSP クライアントでは、OCSP 応答の署名を検証する必要があります。

PAN 上の自己署名 CA 証明書（ISE が外部 CA の中間 CA として機能する場合は、中間 CA 証明書）によって、OCSP 応答側証明書が発行されます。PAN 上のこの CA 証明書によって、PAN および PSN の OCSP 証明書が発行されます。この自己署名 CA 証明書は、展開全体に対するルート証明書でもあります。展開全体のすべての OCSP 証明書が、これらの証明書を使用して署名された応答を ISE で検証するために、信頼できる証明書ストアに格納されます。

（注） Cisco ISE は OCSP レスポンダサーバーから thisUpdate 値を受信します。この値は、最後の証明書失効からの時間を示します。thisUpdate 値が 7 日より大きい場合、Cisco ISE で OCSP 証明書の検証が失敗します。

OCSP 証明書のステータスの値

OCSP サービスでは、所定の証明書要求に対して次の値が返されます。

- [良好（Good）]：ステータスの問い合わせへの肯定的な応答を示します。証明書が失効していないこと、および状態が次の時間間隔（存続可能時間）値までは良好であることを示します。
- [失効（Revoked）]：証明書は失効しています。
- [不明（Unknown）]：証明書のステータスは不明です。この OCSP 応答側の CA で証明書が発行されなかった場合、OCSP サービスはこの値を返します。
- [エラー（ERROR）]：OCSP 要求に対する応答を受信しませんでした。

OSCP 証明書の自動更新

Cisco ISE リリース 3.1 累積パッチ 2 以降では、次のルールが OCSP 証明書の更新に適用されます。

- マルチノード Cisco ISE 展開の場合、Cisco ISE GUI を介してパッチをインストールすると、OCSP 証明書が自動的に更新されます。Cisco ISE CLI を介してパッチをインストールする場合は、OCSP 証明書を手動で更新することをお勧めします。
- スタンドアロン Cisco ISE 展開の場合、Cisco ISE GUI、または Cisco ISE CLI のどちらを介してパッチをインストールしたかに関わらず、OCSP 証明書が自動的に更新されます。
- パッチ2をアンインストールする場合は、OCSP証明書を手動で更新する必要があります。

OCSP ハイ アベイラビリティ

Cisco ISE では CA ごとに最大 2 つの OCSP サーバーを設定でき、それらのサーバーはプライマリおよびセカンダリ OCSP サーバーと呼ばれます。各 OCSP サーバー設定には、次のパラメータが含まれます。

- [URL]：OCSP サーバーの URL。
- [ナンス（Nonce）]：要求で送信される乱数。このオプションにより、リプレイ アタックで古い通信を再利用できないことが保証されます。
- [応答の検証（Validate Response）]：Cisco ISE は OCSP サーバーから受信した応答の署名を検証します。

Cisco ISE がプライマリ OCSP サーバーと通信しているときに、タイムアウト（5 秒）が発生した場合、Cisco ISE はセカンダリ OCSP サーバーに切り替えます。

Cisco ISE はプライマリ サーバーの再使用を試行する前に、設定可能な期間セカンダリ OCSP サーバーを使用します。

OCSP の障害

3 つの一般的な OCSP 障害のシナリオは次のとおりです。

- OCSP キャッシュまたは OCSP クライアント側（Cisco ISE）の失敗による障害。
- 失敗した OCSP 応答側のシナリオ。例：

  最初のプライマリ OCSP 応答側が応答せず、セカンダリ OCSP 応答側が Cisco ISE OCSP 要求に応答します。

  Cisco ISE OCSP 要求からエラーまたは応答が受信されません。

  OCSP 応答側が、Cisco ISE OCSP 要求への応答を提供しないか、失敗の OCSP 応答のステータスを返している可能性があります。OCSP 応答のステータス値は次のようになります。

  - tryLater

- signRequired
- unauthorized
- internalError
- malformedRequest

  OCSP 要求には、多数の日時チェック、署名の有効性チェックなどがあります。詳細については、エラー状態を含むすべての可能性のある状態について説明している『*RFC 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP*』を参照してください。

- 失敗した OCSP レポート

OCSP クライアント プロファイルの追加

[OCSP クライアント プロファイル（OCSP Client Profile）] ページを使用して、Cisco ISE に新しい OCSP クライアント プロファイルを追加できます。

始める前に

認証局（CA）が非標準ポート（80 または 443 以外）で OCSP サービスを実行している場合は、そのポートで Cisco ISE と CA 間の通信を可能にするためにスイッチで ACL を設定する必要があります。次に例を示します。

permit tcp <*source ip*> <*destination ip*> **eq** <*OCSP* ポート番号 >

ステップ 1 **[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [証明書管理（Certificate Management）] > [OCSP クライアントプロファイル（OCSP Client Profile）]** を選択します。

ステップ 2 OCSP クライアント プロファイルを追加するための値を入力します。

ステップ 3 **[送信（Submit）]** をクリックします。

OCSP クライアント プロファイル設定

次の表では、OCSP クライアントプロファイル設定を行うために使用できる [OCSP クライアント プロファイル（OCSP Client Profile）] ウィンドウのフィールドについて説明します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして、**[管理（Administration）] > [証明書（Certificates）] > [証明書管理（Certificate Management）] > [OCSP クライアント プロファイル（OCSP Client Profile）]** を選択します。

表 *20 : OCSP* クライアント プロファイル設定

フィールド名	使用上のガイドライン
名前（Name）	OCSP クライアント プロファイル名。

フィールド名	使用上のガイドライン
説明（**Description**）	任意で説明を入力します。
OCSP応答側の設定（Configure OCSP Responder）	
セカンダリ サーバーの有効化（**Enable Secondary Server**）	ハイ アベイラビリティのセカンダリ OCSP サーバーを有効にするには、このチェックボックスをオンにします。
常にプライマリ サーバーに最初にアクセスする（**Always Access Primary Server First**）	このオプションは、セカンダリ サーバーへの移動を試行する前にプライマリ サーバーをチェックする場合に使用します。プライマリが以前にチェックされ、応答しないことがわかっている場合にも、Cisco ISE はセカンダリ サーバーに移動する前にプライマリ サーバーへの要求の送信を試行します。
[n分経過後にプライマリ サーバーにフォールバック（Fallback to Primary Server After Interval *n* Minutes）]	このオプションは、Cisco ISE がセカンダリ サーバーに移動してから、再度プライマリ サーバーにフォールバックする場合に使用します。この場合、その他の要求はすべてスキップされ、テキスト ボックスで設定した時間セカンダリ サーバーが使用されます。許可される時間の範囲は 1 ～ 999 分です。
プライマリ サーバーとセカンダリ サーバー（Primary and Secondary Servers）	
URL	プライマリおよびセカンダリ OCSP サーバーの URL を入力します。
ナンス拡張サポートの有効化（**Enable Nonce Extension Support**）	ナンスが OCSP 要求の一部として送信されるように設定できます。ナンスには、OCSP 要求の疑似乱数が含まれます。応答で受信される数値は要求に含まれる数値と同じであることが検証されています。このオプションにより、リプレイ アタックで古い通信を再利用できないことが保証されます。
応答の署名の検証（**Validate Response Signature**）	OCSP レスポンダは、次のいずれかの証明書を使用して応答に署名します。 • CA 証明書 • CA 証明書とは別の証明書 Cisco ISE が応答の署名を検証するためには、OCSP 応答側が応答を証明書とともに送信する必要があります。そうでない場合、応答の検証は失敗し、証明書のステータスは利用できません。RFC に従い、OCSP は異なる証明書を使用して応答に署名できます。このことは、OCSP が Cisco ISE による検証用に応答に署名した証明書を送信する限り当てはまります。OCSP が Cisco ISE で設定されているものとは異なる証明書を使用して応答に署名した場合、応答の検証は失敗します。

フィールド名	使用上のガイドライン
Authority Information Access（AIA）に指定されたOCSP URLを使用する（Use OCSP URLs specified in Authority Information Access (AIA)）	Authority Information Access の拡張で指定されている OCSP URL を使用するには、オプション ボタンをクリックします。
応答キャッシュ（Response Cache）	
[キャッシュ エントリの存続可能時間 n 分(Cache Entry Time To Live *n* Minutes)]	キャッシュ エントリが期限切れになる時間を分単位で入力します。OCSP サーバーからの各応答には nextUpdate 値が含まれています。この値は、証明書のステータスがサーバーで次にいつ更新されるかを示します。OCSP 応答がキャッシュされるとき、2 つの値（1 つは設定から、もう 1 つは応答から）が比較され、この 2 つの最小値の時間だけ応答がキャッシュされます。nextUpdate 値が 0 の場合、応答はまったくキャッシュされません。Cisco ISE は設定された時間 OCSP 応答をキャッシュします。キャッシュは複製されず、永続的でもないため、Cisco ISE が再起動するとキャッシュはクリアされます。次の理由により、OCSP キャッシュは OCSP 応答を保持するために使用されます。 • 既知の証明書に関する OCSP サーバーからのネットワーク トラフィックと負荷を低減するため • 既知の証明書のステータスをキャッシュすることによって Cisco ISE のパフォーマンスを向上させるため デフォルトでは、キャッシュは内部 CA OCSP クライアント プロファイルに対し 2 分に設定されています。エンドポイントが最初の認証から 2 分以内にもう一度認証すると、OCSP のキャッシュが使用され、OCSP レスポンダには問い合わせされません。エンドポイントの証明書がキャッシュ期間内に失効した場合、以前の OCSP のステータス [良好（Good）] が使用され、認証は成功します。キャッシュを 0 分に設定すると、応答はキャッシュされません。このオプションでは、セキュリティは向上しますが、認証のパフォーマンスは低下します。
キャッシュのクリア（Clear Cache）	OCSP サービスに接続されているすべての認証局のエントリをクリアするには、[キャッシュのクリア（Clear Cache）] をクリックします。 展開内で、[キャッシュのクリア（Clear Cache）] はすべてのノードと相互作用して、処理を実行します。このメカニズムでは、展開内のすべてのノードが更新されます。

関連トピック

OCSP サービス （163 ページ）
Cisco ISE CA サービスの Online Certificate Status Protocol レスポンダ （164 ページ）
OCSP 証明書のステータスの値 （164 ページ）
OCSP ハイ アベイラビリティ （165 ページ）
OCSP の障害 （165 ページ）
OCSP 統計情報カウンタ （169 ページ）
OCSP クライアント プロファイルの追加 （166 ページ）

OCSP 統計情報カウンタ

Cisco ISE では、OCSP カウンタを使用して、OCSP サーバーのデータと正常性をロギングおよびモニターリングします。ロギングは 5 分ごとに実行されます。Cisco ISE はモニターリング ノードに syslog メッセージを送信し、それはローカル ストアに保持されます。ローカル ストアには過去 5 分のデータが含まれています。Cisco ISE が syslog メッセージを送信した後、カウンタは次の間隔について再計算されます。つまり、5 分後に、新しい 5 分間の間隔が再度開始されます。

次の表に、OCSP syslog メッセージとその説明を示します。

表 *21 : OCSP Syslog* メッセージ

メッセージ	説明
OCSPPrimaryNotResponsiveCount	応答のないプライマリ要求の数
OCSPSecondaryNotResponsiveCount	応答のないセカンダリ要求の数
OCSPPrimaryCertsGoodCount	プライマリ OCSP サーバーを使用して返された所定の CA の「良好な」証明書の数
OCSPSecondaryCertsGoodCount	プライマリ OCSP サーバーを使用して返された所定の CA の「良好な」ステータスの数
OCSPPrimaryCertsRevokedCount	プライマリ OCSP サーバーを使用して返された所定の CA の「失効した」ステータスの数
OCSPSecondaryCertsRevokedCount	セカンダリ OCSP サーバーを使用して返された所定の CA の「失効した」ステータスの数
OCSPPrimaryCertsUnknownCount	プライマリ OCSP サーバーを使用して返された所定の CA の「不明の」ステータスの数
OCSPSecondaryCertsUnknownCount	セカンダリ OCSP サーバーを使用して返された所定の CA の「不明の」ステータスの数

メッセージ	説明
OCSPPrimaryCertsFoundCount	プライマリの送信元からのキャッシュ内に見つかった証明書の数
OCSPSecondaryCertsFoundCount	セカンダリの送信元からのキャッシュ内に見つかった証明書の数
ClearCacheInvokedCount	一定間隔の後にキャッシュのクリアがトリガーされた回数
OCSPCertsCleanedUpCount	t 間隔の後にクリーンアップされたキャッシュ エントリの数
NumOfCertsFoundInCache	キャッシュから実行された要求の数
OCSPCacheCertsCount	OCSP キャッシュ内に見つかった証明書の数

管理者のアクセス ポリシーの設定

RBAC ポリシーは if-then 形式で表され、ここで if は RBAC 管理者グループの値、および「then」は RBAC 権限の値になります。

[RBACポリシー（RBAC policies）] ウィンドウ（[メニュー（Menu）] アイコン（☰）をクリックして、**[管理（Administration）]**>**[システム（System）]**>**[管理者アクセス（Admin Access）]**>**[許可（Authorization）]** > **[RBACポリシー（RBAC Policy）]** を選択）には、デフォルトポリシーのリストが含まれています。これらのデフォルトポリシーは編集または削除できません。ただし、読み取り専用管理ポリシーのデータ アクセス許可は編集できます。[RBAC ポリシー（RBAC policies）] ページでは、特に職場の管理者グループ用にカスタム RBAC ポリシーを作成し、パーソナライズされた管理者グループに適用できます。

制限付きメニュー アクセスを割り当てるときには、データ アクセス権限により、指定されているメニューを使用するために必要なデータに管理者がアクセスできることを確認してください。たとえばデバイス ポータルへのメニュー アクセスを付与するが、エンドポイント ID グループへのデータ アクセスを許可しないと、管理者はポータルを変更できません。

（注） 管理者ユーザーは、エンドポイントの MAC アドレスを、読み取り専用アクセス権を持つエンドポイント ID グループから、フルアクセス権を持つエンドポイント ID グループに移動できます。その逆はできません。

始める前に

- ロールベース アクセス コントロール（RBAC）ポリシーを定義するすべての管理者グループを作成します。

- これらの管理者グループが、個々の管理者ユーザーにマッピングされていることを確認します。
- メニューアクセス権限やデータアクセス権限など、RBAC権限を設定していることを確認します。

ステップ1 **[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [許可（Authorization）] > [RBACポリシー（RBAC Policy）]** を選択します。

[RBAC ポリシー（RBAC Policies）] ページには、デフォルトの管理者グループ用にすぐに使用できる定義済みの一連のポリシーが含まれています。これらのデフォルト ポリシーは編集または削除できません。ただし、デフォルトの読み取り専用管理ポリシーのデータ アクセス許可は編集できます。

ステップ2 デフォルト RBAC ポリシー ルールのいずれかの隣にある [操作（Action）] をクリックします。

ここでは、新しい RBAC ポリシーを挿入し、既存の RBAC ポリシーを複製し、既存の RBAC ポリシーを削除できます。

ステップ3 [新しいポリシーの挿入（Insert New Policy）] をクリックします。

ステップ4 [ルール名（Rule Name）]、[RBAC グループ（RBAC Group(s)）]、および [権限（Permissions）] フィールドに値を入力します。

RBACポリシーの作成時に、複数のメニューアクセス権限とデータアクセス権限を選択することはできません。

ステップ5 [保存（Save）] をクリックします。

管理者アクセスの設定

Cisco ISE では、セキュリティ強化のために管理者アカウントにルールを定義できます。管理インターフェイスへのアクセスを制限したり、強力なパスワードの使用やパスワードの定期的な変更を管理者に強制することができます。Cisco ISEの[管理者アカウントの設定（Administrator Account Settings）] で定義するパスワードポリシーは、すべての管理者アカウントに適用されます。

Cisco ISE では、管理者パスワードに UTF-8 文字は使用できません。

同時管理セッションとログインバナーの最大数の設定

同時管理 GUI または CLI（SSH）セッションの最大数、および管理 Web または CLI インターフェイスにアクセスする管理者を手助け、ガイドするログインバナーを設定できます。管理者のログイン前後に表示されるログインバナーを設定できます。デフォルトでは、これらのログインバナーは無効になっています。ただし、個々の管理者アカウントの同時セッションの最大数を設定することはできません。

始める前に

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

ステップ 1 **[管理（Administration）]** > **[システム（System）]** > **[管理者アクセス（Admin Access）]** > **[設定（Settings）]** > **[アクセス（Access）]** > **[セッション（Session）]** を選択します。

ステップ 2 GUI および CLI インターフェイスを介した同時管理セッションの、許可する最大数を入力します。同時管理 GUI セッションの有効範囲は 1 ～ 20 です。同時管理 CLI セッションの有効範囲は 1 ～ 10 です。

ステップ 3 Cisco ISE で管理者がログインする前にメッセージを表示する場合は、[プリログイン バナー（Pre-login banner）] チェックボックスをオンにして、テキスト ボックスにメッセージを入力します。

ステップ 4 Cisco ISE で管理者がログインした後にメッセージを表示する場合は、[ポストログイン バナー（Post-login banner）] チェックボックスをオンにして、テキスト ボックスにメッセージを入力します。

ステップ 5 [保存（Save）] をクリックします。

関連トピック

IP アドレスの選択からの Cisco ISE への管理アクセスの許可 （172 ページ）

IP アドレスの選択からの Cisco ISE への管理アクセスの許可

Cisco ISE では、管理者が Cisco ISE 管理インターフェイスにアクセスできる IP アドレスのリストを設定することができます。

管理者アクセスコントロール設定は、管理ペルソナ、ポリシーサービスペルソナ、またはモニターリングペルソナを担う Cisco ISE ノードに対してのみ適用できます。これらの制限は、プライマリ ノードからセカンダリ ノードに複製されます。

始める前に

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

ステップ 1 Cisco ISE の GUI で、[メニュー（Menu）] アイコン（☰）をクリックし、次を選択します**[管理（Administration ）]** > **[システム（System）]** > **[管理者アクセス（Admin Access）]** > **[設定（Settings）]** > **[アクセス（Access）]** > **[IP アクセス（IP Access）]** を選択します。

ステップ 2 [リストされている IP アドレスのみに接続を許可する（Allow only listed IP addresses to connect）] オプションボタンをクリックします。

（注） 管理アクセスにはポート 161（SNMP）の接続を使用します。ただし、IP アクセス制限が設定されている場合は、実行元のノードで管理アクセスが設定されていないと snmpwalk が失敗します。

ステップ 3 [アクセス制限の IP リストの設定（Configure IP List for Access Restriction）] 領域で、[追加（Add）] をクリックします。

ステップ 4 [IP CIDR の追加（Add IP CIDR）] ダイアログボックスで、[IP アドレス（IP Address）] フィールドに IP アドレスをクラスレスドメイン間ルーティング（CIDR）形式で入力します。

（注） このIPアドレスは、IPv4またはIPv6アドレスにすることができます。ISEノードに複数のIPv6アドレスを設定できます。

ステップ 5 [CIDR 形式のネットマスク（Netmask in CIDR format）] フィールドにサブネットマスクを入力します。

ステップ 6 [OK] をクリックします。ステップ 4 ～ 7 を繰り返して、他の IP アドレス範囲をこのリストに追加します。

ステップ 7 [保存（Save）] をクリックして、変更内容を保存します。

ステップ 8 [IP アクセス（IP Access）] ウィンドウを更新するには、[リセット（Reset）] をクリックします。

Cisco ISE の MnT セクションへのアクセスの許可

Cisco ISE では、管理者が Cisco ISE の MnT セクションにアクセスできるノードのリストを設定することができます。

始める前に

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

ステップ 1 Cisco ISE ホームページから、**[管理（Administration）]** > **[システム（System）]** > **[管理者アクセス（Admin Access）]** > **[設定（Settings）]** > **[アクセス（Access）]** を選択します。

ステップ 2 [MnTアクセス（MnT Access）] タブをクリックします。

ステップ 3 展開内または展開外のいずれかのノードまたはエンティティが MnT に syslog を送信できるようにするには、[MnTへの接続を任意のIPアドレスに許可します（Allow any IP address to connect to MnT）] ラジオボタンをクリックします。展開内のノードまたはエンティティのみが syslog を MnT に送信できるようにするには、[MnTへの接続を展開内のノードのみに許可します（Allow only the nodes in the deployment to connect to MnT）] ラジオボタンをクリックします。

（注） ISE 2.6 P2 以降では、デフォルトで [MnTにUDP syslogを伝送するためにISEメッセージングサービスを使用（Use ISE Messaging Service for UDP Syslogs delivery to MnT）]Cisco ISE メッセージングサービスを介した syslogがオンになっていて、展開外の他のエンティティからの syslog を受信することはできません。

管理者アカウントのパスワード ポリシーの設定

Cisco ISE では、セキュリティ向上のために管理者アカウントにパスワード ポリシーを作成することもできます。パスワードベースまたはクライアント証明書ベースの管理者認証のいずれが必要かを定義できます。ここで定義したパスワードポリシーは、Cisco ISE 内のすべての管理者アカウントに適用されます。

（注）

- 内部管理者ユーザーの電子メール通知は root@host に送信されます。電子メール アドレスは設定できません。多くの SMTP サーバーがこの電子メールを拒否します。

  未解決の不具合 CSCui5583 を確認できます。これは、電子メールアドレスの変更を許可する拡張機能です。

- Cisco ISE では、管理者パスワードに UTF-8 文字は使用できません。

始める前に

- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。
- 展開内で自動フェールオーバー設定が有効になっている場合は、オフにします。管理ノードの自動フェールオーバーのサポートを参照してください

  認証方式を変更すると、アプリケーション サーバー プロセスが再起動されます。これらのサービスが再起動されるまで遅延が発生する場合があります。このサービスの再起動の遅延により、セカンダリ管理ノードの自動フェールオーバーが開始される場合があります。

ステップ 1 Cisco ISE の GUI で、[メニュー（Menu）] アイコン（☰）をクリックし、**[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [認証（Authentication）]** 選択します。

ステップ 2 次のいずれかの認証方式のオプションボタンをクリックします。

- [パスワードベース（Password Based）]：管理者ログインに標準ユーザー ID とパスワードクレデンシャルを使用します。[ID ソース（Identity Source）] ドロップダウンリストから [内部（Internal）] または [外部（External）] を選択します。

  （注） LDAP などの外部 ID ストアを設定しており、それを認証ソースとして使用して管理者ユーザーにアクセス権を付与する場合は、その ID ソースを [ID ソース（Identity Source）] リスト ボックスから選択する必要があります。

- [クライアント証明書ベース（Client Certificate Based）]：証明書ベースのポリシーを指定するには、このオプションを選択します。[証明書認証プロファイル（Certificate Authentication Profile）] ドロップダウンリストから、既存の認証プロファイルを選択します。[ID ソース（Identity Source）] ドロップダウンリストから必要な値を選択します。

ステップ 3 [パスワードポリシー（Password Policy）] タブをクリックし、Cisco ISE の GUI と CLI のパスワード要件を設定するために必要な値を入力します。

ステップ 4 [保存（Save）] をクリックして、管理者パスワード ポリシーを保存します。

（注） 外部IDストアを使用してログイン時に管理者を認証する場合は、管理者プロファイルに適用されるパスワードポリシーにこの設定値が設定されている場合でも、外部IDストアが依然として管理者のユーザー名とパスワードを認証することに注意してください。

関連トピック

管理者パスワード ポリシーの設定

管理者アカウントのアカウント無効化ポリシーの設定 （175 ページ）

管理者アカウントのロック設定または一時停止設定 （175 ページ）

管理者アカウントのアカウント無効化ポリシーの設定

Cisco ISE では、設定した連続日数の間に管理者アカウントが認証されなかった場合は、管理者アカウントを無効にすることができます。

ステップ 1 Cisco ISE の GUI で、[メニュー（Menu）] アイコン（☰）をクリックし、**[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [認証（Authentication）] > [アカウント無効化ポリシー（Account Disable Policy）]**を選択します。

ステップ 2 [非アクティブになってから *n* 日後にアカウントを無効にする（Disable account after n days of inactivity）] チェックボックスをオンにして、対応するフィールドに日数を入力します。

このオプションでは、管理者アカウントが指定した日数の間非アクティブだった場合に管理者アカウントを無効にすることができます。ただし、**[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [管理者（Administrators）] > [管理ユーザー（Admin Users）]** ウィンドウの [非アクティブアカウントを無効化しない（Inactive Account Never Disabled）] オプションを使用して、このアカウント無効化ポリシーから個々の管理者アカウントを除外することができます。

管理者アカウントを無効にして後で有効にすると、24 時間以上アクティブのままになりません。管理者アカウントを無効にしてもアクティブなままにしたい場合は、[*n*日間の非アクティブ後にアカウントを無効にする（Disable account after n days of inactivity）] チェックボックスをオフのままにします。

ステップ 3 [保存（Save）] をクリックして、管理者のグローバル アカウント無効化ポリシーを設定します。

管理者アカウントのロック設定または一時停止設定

Cisco ISE では、指定されたログイン試行失敗回数を超えた管理者アカウント（パスワードベースの内部管理者アカウントと証明書ベースの管理者アカウントを含む）をロックまたは一時停止できます。

ステップ 1 Cisco ISE の GUI で、[メニュー（Menu）] アイコン（☰）をクリックし、**[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [認証（Authentication）] > [設定のロック/一時停止（Lock/Suspend Settings）]** を選択します。

ステップ 2 [ログイン試行が間違っているアカウントを一時停止またはロックする（Suspend or Lock Account With Incorrect Login Attempts）] チェックボックスをオンにして、アクションを実行するまでの試行失敗の回数を入力します。有効な範囲は、3 ～ 20 です。次のオプションのいずれかのオプションボタンをクリックします。

- [*n* 分間アカウントを一時停止（Suspend Account For n Minutes）]：指定した間違ったログイン試行回数を超えるアカウントを一時停止するには、このオプションを選択します。有効な範囲は、15 ～ 1440 です。
- [アカウントのロック（Lock Account）]：指定した間違ったログイン試行回数を超えるアカウントをロックするには、このオプションを選択します。

エンドユーザーにヘルプデスクに連絡してアカウントのロックを解除するよう要求するなどの、修復を依頼するカスタムの電子メール メッセージを入力することができます。

（注） Cisco ISE リリース 2.3 以前では、[パスワードポリシー（Password Policy）] タブ（**[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [認証（Authentication）] > [パスワードポリシー（Password Policy）]**）で [ロック/一時停止の設定（Lock / Suspend Settings）] を使用できます。

管理者のセッション タイムアウトの設定

Cisco ISE を使用すると、管理 GUI セッションが非アクティブであっても依然として接続状態である時間を決定できます。分単位の時間を指定することができ、その時間が経過すると Cisco ISE は管理者をログアウトします。セッションのタイムアウト後、管理者は、Cisco ISE 管理者ポータルにアクセスするには再びログインする必要があります。

始める前に

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

ステップ 1 **[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [設定（Settings）] > [セッション（Session）] > [セッションのタイムアウト（Session Timeout）]** を選択します。

ステップ 2 アクティビティがない場合に管理者をログアウトするまでに Cisco ISE が待機する時間（分）を入力します。デフォルト値は 60 分です。有効な範囲は 6 ～ 100 分です。

ステップ 3 [保存（Save）] をクリックします。

アクティブな管理セッションの終了

Cisco ISE では、すべてのアクティブな管理セッションが表示され、そこからセッションを選択し、必要が生じた場合はいつでも終了できます。同時管理 GUI セッションの最大数は 20 です。GUI セッションの最大数に達した場合、スーパー管理者グループに属する管理者がログインして一部のセッションを終了できます。

始める前に

次のタスクを実行するには、スーパー管理者である必要があります。

ステップ 1 **[管理（Administration）]** > **[システム（System）]** > **[管理者アクセス（Admin Access）]** > **[設定（Settings）]** > **[セッション（Session）]** > **[セッション情報（Session Info）]** を選択します。

ステップ 2 終了するセッション ID の隣にあるチェックボックスをオンにし、[無効化（Invalidate）] をクリックします。

管理者の名前の変更

Cisco ISE では、Cisco ISE GUI からユーザー名を変更できます。

始める前に

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

ステップ 1 Cisco ISE 管理ポータルにログインします。

ステップ 2 Cisco ISE GUI の右上隅にある [歯車（gear）] アイコン（⚙）をクリックし、ドロップダウンリストから [アカウント設定（Account Settings）] を選択します。

ステップ 3 表示される [管理者ユーザー（Admin User）] ダイアログボックスに新しいユーザー名を入力します。

ステップ 4 変更するアカウントに関するその他の詳細を編集します。

ステップ 5 [保存（Save）] をクリックします。

管理者アクセスの設定

これらのセクションで、管理者のアクセス設定を行うことができます。

管理者パスワード ポリシーの設定

次の表では、管理者パスワードが満たす必要のある基準を定義するために使用できる [パスワードポリシー（Password Policy）] ウィンドウのフィールドについて説明します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして、**[管理（Administration）]** > **[システム（System）]** > **[管理アクセス（Admin Access）]** > **[認証（Authentication）]** > **[パスワードポリシー（Password Policy）]** の順に選択します。

表 *22 :* 管理者パスワード ポリシーの設定

フィールド名	使用上のガイドライン
最小長（**Minimum Length**）	パスワードの最小長（文字数）を指定します。デフォルトは 6 文字です。

フィールド名	使用上のガイドライン
パスワードに使用できない文字（**Password may not contain**）	[管理者名またはその文字の逆順（Admin name or its characters in reverse order）]：このチェックボックスをオンにして、管理者ユーザー名またはその文字の逆順でのパスワードとしての使用を制限します。
	[Ciscoまたはその文字の逆順（Cisco or its characters in reverse order）]：このチェックボックスをオンにして、単語「Cisco」またはその文字の逆順でのパスワードとしての使用を制限します。
	[この単語またはその文字の逆順（This word or its characters in reverse order）]：このチェックボックスをオンにして、定義したすべての単語またはその文字の逆順でのパスワードとしての使用を制限します。
	[4 回以上連続する繰り返し文字の使用（Repeated characters four or more times consecutively）]：このチェックボックスをオンにして、4回以上連続する繰り返し文字のパスワードとしての使用を制限します。

フィールド名	使用上のガイドライン
	[辞書の単語、その文字の逆順、または文字の置き換え（Dictionary words, their characters in reverse order or their letters replaced with other characters]：辞書の単語、単語の文字の逆順での使用、または単語の文字の置き換えでのパスワードとしての使用を制限します。 「s」を「$」、「a」を「@」、「o」を「0」、「l」を「1」、「i」を「!」、「e」を「3」などに置き換えることはできません。たとえば、「Pa $$ w0rd」は許可されません。 • [デフォルトの辞書（Default Dictionary）]：Cisco ISE でデフォルトの Linux 辞書を使用するには、このオプションを選択します。デフォルトの辞書には約 480,000 件の英単語が含まれています。 このオプションは、デフォルトで選択されます。 • [カスタム辞書（Custom Dictionary]：カスタマイズした辞書を使用するには、このオプションを選択します。**[ファイルの選択（Choose File）]** をクリックし、カスタム辞書ファイルを選択します。このテキスト ファイルでは、単語が改行文字で区切られており、拡張子は .dic、サイズは 20 MB 以下である必要があります。
パスワードには選択したタイプの文字がそれぞれ 1 文字以上含まれている必要があります（Password must contain at least one character of each of the selected types）	管理者のパスワードに含める必要がある文字のタイプのチェックボックスをオンにします。次の 1 つまたは複数のオプションを選択します。 • **英文字の小文字** • **英文字の大文字** • **数字** • **英数字以外の文字**

フィールド名	使用上のガイドライン
パスワード履歴（**Password History**）	同じパスワードが繰り返し使用されるのを防ぐために、新しいパスワードと異なっている必要がある以前のパスワードの数を指定します。[パスワードは以前の *n* バージョンとは異なる必要があります（Password must be different from the previous n versions）] チェックボックスをオンにし、対応するフィールドに数字を入力します。 ユーザーがパスワードを再使用できない日数を入力します。[パスワードを *n* 日以内に再利用することはできません（Cannot reuse password within n days）] をオンにし、対応するフィールドに数字を入力します。
パスワードライフタイム（**Password Lifetime**）	次のオプションのチェックボックスをオンにして、指定した期間後にパスワードを変更するようユーザーに強制します。 • [管理者パスワードは作成後または最終変更後 *n* 日で有効期限が切れます（Administrator passwords expire n days after creation or last change）]：パスワードを変更しない場合に管理者アカウントが無効になるまでの時間（日数）。有効な範囲は 1 ～ 3,650 日です。 • [パスワードの有効期限の *n* 日前に管理者に電子メールリマインダを送信します（Send an email reminder to administrators n days prior to password expiration）]：パスワードが期限切れになることを管理者に通知するまでの時間（日数）。有効な範囲は 1 ～ 3,650 日です。
ネットワークデバイスの機密データの表示	
管理者パスワードが必要（**Require Admin Password**）	共有秘密やパスワードなどのネットワークデバイスの機密データを表示するために管理者ユーザーがログインパスワードを入力するようにする場合には、このチェックボックスをオンにします。

フィールド名	使用上のガイドライン
[パスワードを *n* 分間キャッシュします（Password cached for n Minutes）]	管理者ユーザーによって入力されたパスワードは、この期間キャッシュされます。管理ユーザーはこの間、ネットワークデバイスの機密データを表示するのにパスワードの再入力を求められることはありません。有効な範囲は 1 ～ 60 分です。

関連トピック

Cisco ISE 管理者
新しい管理者の作成

セッション タイムアウトおよびセッション情報の設定

次の表では、セッションタイムアウトを定義し、アクティブな管理セッションを終了するために使用できる[セッション（Session）]ウィンドウのフィールドについて説明します。ウィンドウにアクセスするには、[メニュー（Menu）]アイコン（☰）をクリックし、**[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [設定（Settings）] > [セッション（Session）]** の順に選択します。

表 *23*：セッション タイムアウトおよびセッション情報の設定

フィールド名	使用上のガイドライン
セッションのタイムアウト（Session Timeout）	
セッション アイドル タイムアウト（Session Idle Timeout）	アクティビティがない場合に管理者をログアウトするまでに Cisco ISE が待機する時間（分）を入力します。デフォルト値は 60 分です。有効な範囲は 6 ～ 100 分です。
セッション情報（Session Info）	
無効化（Invalidate）	終了するセッション ID の隣にあるチェックボックスをオンにし、[無効化（Invalidate）]をクリックします。

関連トピック

管理者アクセスの設定 （171 ページ）
管理者のセッション タイムアウトの設定 （176 ページ）
アクティブな管理セッションの終了 （176 ページ）

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