Cisco APIC-EM のセキュリティ保護

Cisco APIC-EMのセキュリティについて

Cisco APIC-EMでは基本機能をサポートするためにマルチレイヤ アーキテクチャが必要です。マルチレイヤ アーキテクチャは、次のコンポーネントで構成されています。

- 外部ネットワーク：外部ネットワークは、ネットワークの一方の管理者およびアプリケーションと、もう一方の内部ネットワークまたはクラウド内のGrapevineルートおよびクライアントの間に存在します。管理者とアプリケーションの両方がこの外部ネットワークを使用して Grapevine ルートとクライアントにアクセスします。
- 内部ネットワーク：内部ネットワークは Grapevine ルートとクライアントの両方で構成されます。
- デバイス管理ネットワーク：このネットワークは、コントローラで管理および監視されるデバイスで構成されています。デバイス管理ネットワークは上記の外部ネットワークと基本的に同じであることに注意してください。これは管理者またはノースバウンドアプリケーションから物理的または論理的にセグメント化される可能性があります。

重要　あらゆるレイヤ間通信およびレイヤ内通信では、暗号化、認証およびセグメント化による保護が必要です。

（注）　内部ネットワーク内のクライアントで実行されるさまざまなサービスについては、第4章「*Cisco APIC-EM*サービス」を参照してください。

PKI および Cisco APIC-EM

Cisco APIC-EMは公開キーインフラストラクチャ（PKI）を基盤としてセキュアな通信を提供しています。PKI は、認証局、デジタル証明書、公開キーと秘密キーで構成されます。

認証局（CA）は証明書要求を管理して、ホスト、ネットワークデバイス、ユーザなどの参加エンティティにデジタル証明書を発行します。CA は参加エンティティに対して集中型のキー管理を行います。

公開キー暗号化に基づくデジタル署名は、ホスト、デバイス、個々のユーザをデジタル認証します。RSA 暗号化システムなどの公開キー暗号化では、各エンティティが秘密キーと公開キーの両方を含むキー ペアを持ちます。秘密キーは公開されず、これを所有するホスト、デバイスまたはユーザ以外は知りません。一方、公開キーは誰もが知っているものです。これらのキーの一方で暗号化されたものは、他方のキーで復号化できます。署名は、送信者の秘密キーを使用してデータを暗号化したときに作成されます。受信者は、送信者の公開キーを使用してメッセージを復号化することで、署名を検証します。このプロセスでは、受信者が送信者の公開キーのコピーを取得していて、そのキーが確実に送信者のものであり、送信者を装っている他者のものではないことを確信している必要があります。

デジタル証明書は、デジタル署名と送信者を結び付けるものです。デジタル証明書には、名前、シリアル番号、企業、部署または IP アドレスなど、ユーザまたはデバイスを特定する情報を含んでいます。また、エンティティの公開キーのコピーも含まれています。証明書に署名する CA は、受信者が明示的に信頼する第三者機関であり、アイデンティティの正当性を立証し、デジタル証明書を作成します。

CA の署名を検証するには、受信者は、CA の公開キーを認識している必要があります。一般的にはこのプロセスはアウトオブバンドか、インストール時に行われる操作によって処理されます。たとえば、通常の Web ブラウザでは、デフォルトで、複数の CA の公開キーが設定されています。

Cisco APIC-EM の PKI プレーン

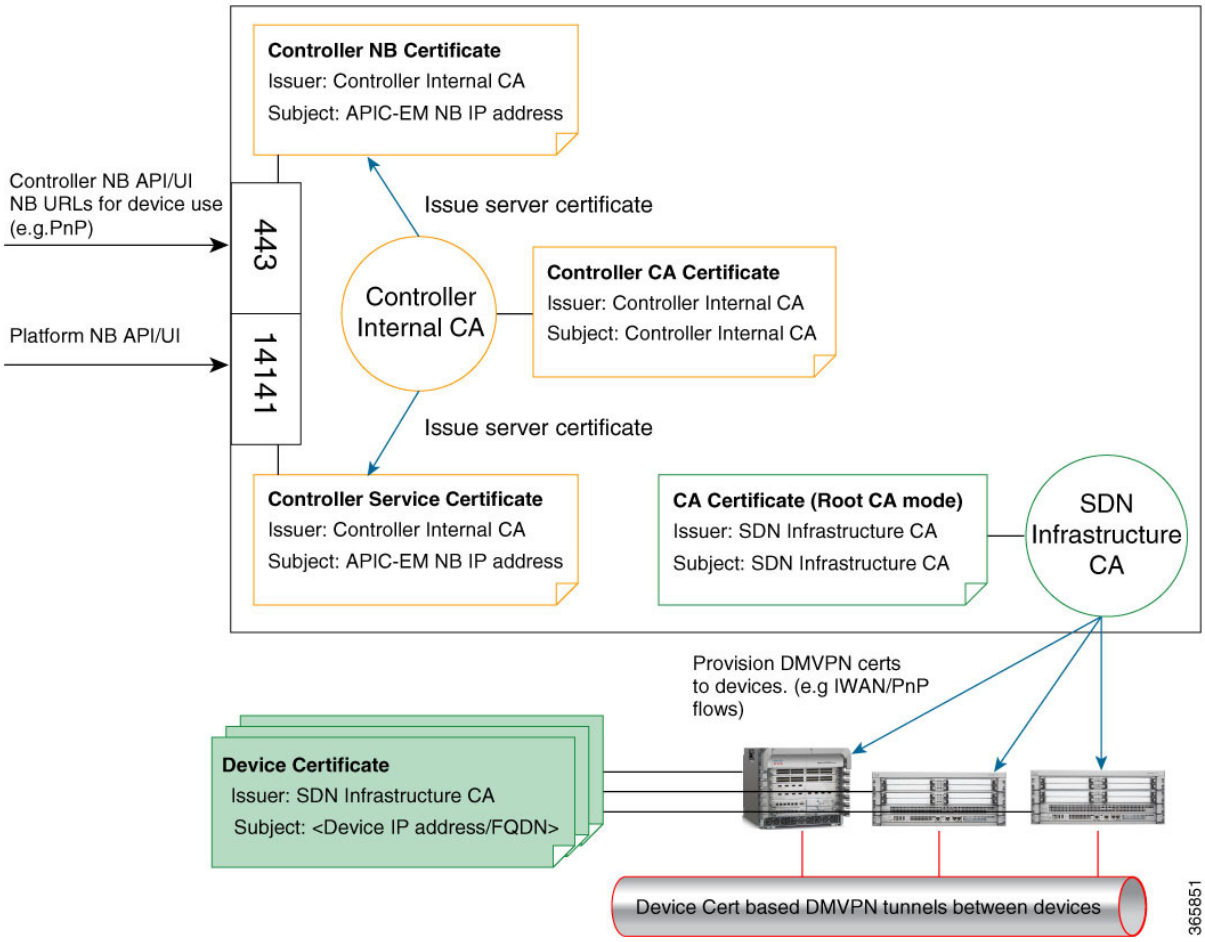
Cisco APIC-EMは、次の別個の PKI プレーンで PKI ベースの接続を提供します。

- コントローラ PKI プレーン：コントローラがクライアント/サーバ モデルのサーバである HTTPS 接続。接続はコントローラのサーバ証明書によって保護されます。コントローラのサーバ証明書は自己署名される（デフォルト）か、外部CAによって発行されます（推奨）。
- デバイス PKI プレーン：ネットワークのコントロール プレーンでのデバイス間の DMVPN 接続。接続に関与している両方のデバイスのデバイス ID 証明書によって相互認証および保護されます。これらの証明書とキーは、Cisco APIC-EMコントローラが提供するプライベート CA（デバイス PKI CA）によって管理されます。
- Grapevine サービス PKI プレーン：Grapevine ルートが管理するこの内部 PKI プレーンは、マルチホスト クラスタでの Grapevine サービス間の通信を保護します。Grapevine サービス PKI プレーンには外部からアクセスできないため、詳細については省略します。

次に示すのは、Cisco APIC-EMの PKIプレーン、認証局、および証明書の概略図です。コントローラ PKI プレーンはコントローラ内部 CA を使用して、外部要求に応じてコントローラ NB 証明書およびコントローラCA証明書を提供します。GrapevinePKIプレーンは同じコントローラ内部CAを使用して、コントローラ サービスからの内部要求に応じてコントローラ サービス証明書を提供

します。デバイス PKI プレーンは SDN インフラストラクチャ CA を使用して、IWAN および PnP デバイスに CA 証明書（この概略図ではルート CA モード）を提供します。

図 *1*：*Cisco APIC-EM* の *PKI* プレーン



次の表の使用例で示すように、Cisco APIC-EMPKI プレーンはさまざまな信頼関係またはドメインをサポートしています。

表 *1*：*Cisco APIC-EM* の *PKI* プレーン

	認証	暗号化	使用例
コントローラ PKI プレーン：外部発信者が開始するコントローラへの接続			

	認証	暗号化	使用例
HTTPS	発信者はユーザ名とパスワードまたはサービス チケッを提示し、コントローラはサーバ証明書を提示します。	はい	シスコ ネットワーク プラグ アンド プレイ（PnP）モバイル アプリや Cisco Prime Infrastructure などの REST クライアント
HTTPS	一方向：コントローラはサーバ証明書を提示します。	はい	シスコ ネットワーク プラグ アンド プレイ（PnP）のプロビジョニング ワークフロー
デバイス PKI プレーン：デバイス間の接続			
DMVPN	Cisco APIC-EMコントローラ内のプライベート CA によって発行された証明書およびキーを使用するインターネット キー エクスチェンジ バージョン 2（IKEv2）による相互認証。	はい	デバイス間の DMVPN 接続

（注） この導入ガイドのセキュリティ コンテンツと説明では、主にコントローラ PKI プレーンを扱います。デバイス PKI プレーンについては、『*PKI Planes in Cisco APIC-EM Technote*』を参照してください。

コントローラ PKI プレーン

外部発信者がコントローラへのHTTPS接続を開始すると、コントローラはサーバ証明書を提示します。この接続には次のようなものがあります。

- HTTPS を介した Cisco APIC-EMGUI へのログイン
- HTTPS を介した Grapevine API（ポート 14141）へのログイン
- HTTPS を介した NB REST API の呼び出し

NB REST API の発信者が NB REST API の呼び出しや、ファイル（デバイス イメージ、コンフィギュレーションなど）のダウンロードを目的として、コントローラへの HTTPS 接続を開始すると、コントローラ（サーバ）は接続を要求した発信者（クライアント）にサーバ証明書を提示します。

HTTPS の代わりに HTTP を使用する NB REST API は、trustpool バンドルをダウンロードする API（GET /ca/trustpool）とコントローラの証明書をダウンロードする API（GET /ca/pem）の 2 つのみです。他のすべての NB REST API は HTTPS を使用します。

コントローラ側開始のデバイスへの接続は、コントローラ PKI プレーン内では行われないことに注意してください。接続に SSH または SNMPv3 が使用されても、CA がキーの管理に関与しないため、接続は PKI ベースとは見なされません。コントローラは、検出、タグの管理、デバイスへのポリシーのプッシュ、デバイスとの通信などを行う目的で、REST 発信者に代わってデバイスへの接続を開始することができます。古いデバイスとの互換性を保つために必要な場合は、検出に TELNET プロトコルを使用できますが、安全性が低いのでこの PKI の説明では扱いません。

デバイス PKI プレーン

IWAN 管理対象のコントロール プレーン デバイス間では、ダイナミック マルチポイント VPN（DMVPN）接続が形成されます。Cisco APIC-EM が提供するプライベート認証局（デバイス PKI CA）は、これらの DMVPN 接続を保護する証明書およびキーをプロビジョニングします。PKI ブローカ サービスは、IWAN GUI の管理者または /certificate-authority および /trust-point NB REST API を使用する REST 発信者の指示に従って、これらの証明書とキーを管理します。

（注） デフォルト モードでは、Cisco APIC-EMのデバイス PKI CA を外部 CA への下位/中間 CA にすることはできません。これらの 2 つの PKI プレーン（コントローラの接続用とデバイス間の DMVPN 接続用）は互いに完全に独立しています。現在のリリースでは、IWAN デバイスの相互対話の証明書はデバイス PKI CA でのみ管理されます。外部 CA では、デバイスが DMVPN トンネル作成および関連操作で互いに示す IWAN 固有の証明書を管理できません。

デバイス PKI プレーン モード

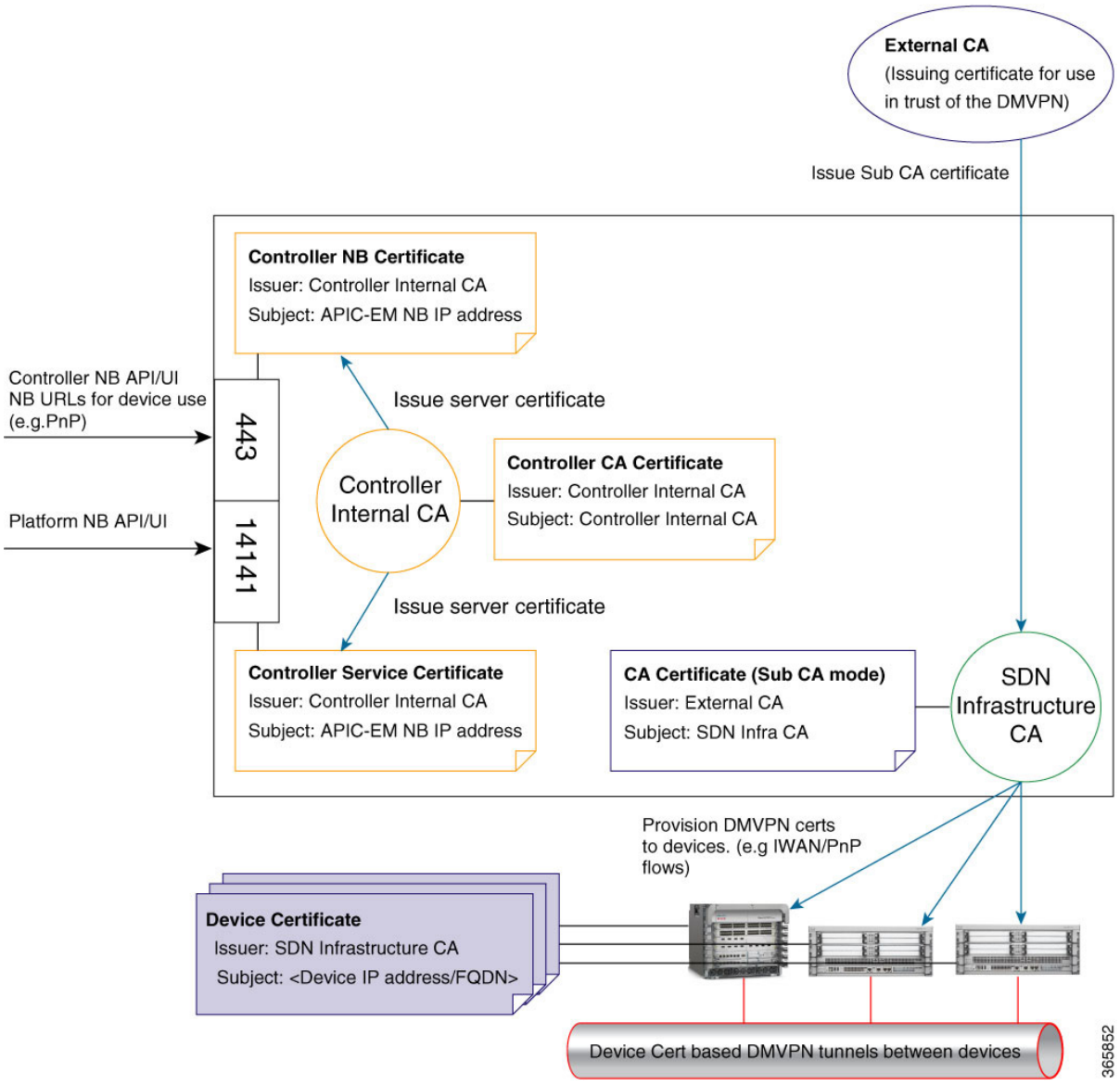
デバイス PKI プレーンでは、次の 2 つのモードがサポートされます。

- ルート モード：Cisco APIC-EMコントローラによって提供されるプライベート CA は他の CA と連携しません。これはコントローラのデフォルト モードです。
- サブ CA モード：サブ CA モードでは、Cisco APIC-EMコントローラによって提供されるプライベート CA を外部 CA への中間 CA にすることができます。つまり、デバイス間の通信を保護する証明書とキーはコントローラのプライベート CA が引き続き管理しますが、この CA はその外部 CA より下位の位置になります。このモードは、管理者（ROLE_ADMIN）が有効にする必要があります。

PKI モードをルートからサブ CA（下位 CA）に変更すると、階層が変わり、コントローラのプライベート CA が外部 CA より下位になります。次に示すのは、サブ CA モードのデバイス PKI プレーンによる別個の PKI プレーンの概略図です。

次の概略図に、デバイス PKI プレーンのサブ CA モードを示します。この概略図では、ルート CA がコントローラの外部にあります。デバイス PKI プレーンのルート CA モードの概略図については、Cisco APIC-EM の PKI プレーン，（2 ページ）を参照してください。

図 *2*：デバイス *PKI* プレーン：サブ *CA* モード



関連トピック

PKI 証明書ロールをルートから下位へ変更する，（33 ページ）

デバイス証明書のライフタイムの設定, （32 ページ）

デバイス PKI 通知

Cisco APIC-EMは、トラブルシューティングとサービサビリティの両方に役立つデバイス PKI 通知を提供します。

重要 この項で説明するデバイス PKI 通知は、コントローラ接続ではなく、デバイス間の DMVPN 接続でのみアクティブになります。

次のデバイス PKI 通知を使用できます。

- システム通知：ユーザ アクションが必要であることを示す通知。これらの通知は、GUI の [Global]ツールバーからアクセス可能な [Systems Notifications] ビューに表示されます。
- 監査ログ通知：コントローラの [Audit Log]GUI を使用して表示できるシステム ログの通知。コントローラの GUI に監査ログを表示する方法については、『*Cisco Application Policy Infrastructure Controller Enterprise Module Troubleshooting Guide*』を参照してください。

次の PKI システム通知タイプがサポートされています。

- 情報
  - 新しいトラスト ポイント作成
  - 新しい PKCS12 ファイルの作成
  - デバイス証明書の登録の完了
  - デバイス証明書の更新の完了
  - デバイス証明書の失効
- 警告
  - 部分的な失効：到達不能なデバイスまたはトラスト ポイントが使用中
  - 証明書の有効期間の 80 パーセントが経過した登録の遅延
  - サービス起動の遅延
- 重大
  - 認証局ハンドシェイクの失敗
  - 登録の失敗
  - 失効の失敗
  - 更新の失敗

次の監査ログ通知は、システム ログで確認できます。

- デバイス登録
- デバイスへの証明書のプッシュ
- デバイス証明書の更新
- デバイス証明書の失効

PKI 証明書の管理

Cisco APIC-EMは、次の別個の PKI プレーンで PKI ベースの接続を提供します。

- コントローラ PKI プレーン：このプレーンにより、コントローラがクライアント/サーバ モデルのサーバである HTTPS 接続が確立され、接続はコントローラのサーバ証明書によって保護されます。
- デバイス PKI プレーン：このプレーンにより、ネットワークのコントロールプレーンでデバイス間の DMVPN 接続が確立され、接続に関与している両方のデバイスのデバイス ID 証明書によって相互認証および保護されます。これらの証明書およびキーは、Cisco APIC-EMコントローラが提供するプライベート CA（デバイス PKI CA）によって発行されます。

この章に記載されている次の PKI 証明書の管理手順は、デバイス PKI プレーンのみを対象としています。

- PKI 証明書ロールをルートから下位へ変更する，（33 ページ）：この手順では、プライベート CA の CA 証明書を外部 CA によって署名された証明書に置き換える必要があります。
- デバイス証明書のライフタイムの設定，（32 ページ）：この手順を使用すると、IWAN 管理対象デバイス間の接続を保護できます。

Cisco APIC-EMコントローラ証明書および秘密キーのサポート

Cisco APIC-EMは、セッション（HTTPS）の認証に使用される PKI 証明書管理機能（コントローラ PKIプレーン）をサポートします。これらのセッションでは、認証局（CA）と呼ばれる一般に認められた信頼されたエージェントを使用します。Cisco APIC-EMは PKI 証明書管理機能を使用して、既知の CA から X.509 証明書をインポートし、保存して管理します。インポートされた証明書はコントローラ自体の ID 証明書になり、コントローラは認証用にクライアントにこの証明書を示します。クライアントは、NB API のアプリケーションやネットワーク デバイスです。

Cisco APIC-EMはコントローラの GUI を使用して次のファイル（PEM または PKCS ファイル形式）をインポートできます。

- X.509 証明書
- 秘密キー

（注） 秘密キーに対し、Cisco APIC-EMは RSA キーのインポートをサポートします。DSA、DH、ECDH および ECDSA キー タイプをインポートしないでください。これらはサポートされません。 また、独自のキー管理システムで秘密キーを保護する必要があります。

インポート前に、既知の認証局（CA）から有効な X.509 証明書と秘密キーを取得するか、独自の自己署名証明書を作成する必要があります。インポートした後、X.509 証明書および秘密キーに基づいたセキュリティ機能が自動的に有効化されます。Cisco APIC-EMはこの証明書を要求するデバイスやアプリケーションに証明書を提供します。ノースバウンド API アプリケーションおよびネットワーク デバイスのどちらも、コントローラとの信頼関係の確立にこれらのクレデンシャルを使用できます。

IWAN の設定およびネットワーク PnP 機能では、ネットワーク内のデバイス間の信頼性を確保するために、PKI の trustpool を含む追加手順が使用されます。この手順については、次の「*Cisco APIC-EMTrustpool* サポート」の項を参照してください。

（注） 自己署名証明書をコントローラで使用したり、コントローラにインポートすることはお勧めしません。既知の認証局（CA）から有効な X.509 証明書をインポートすることをお勧めします。さらに、ネットワーク PnP 機能が正しく動作するように、デフォルトで Cisco APIC-EMにインストールされている自己署名証明書を、既知の認証局により署名された証明書に置き換える必要があります。

Cisco APIC-EMはインポートされた X.509 証明書と秘密キーを一度に 1 つのみサポートします。2 番目の証明書および秘密キーのインポート時に、最初に（既存の）インポートされた証明書および秘密キー値が上書きされます。

（注） 外部 IP アドレスがコントローラに対し何らかの理由で変更される場合、変更された、または新しい IP アドレスを含む新しい証明書をインポートし直す必要があります。

関連トピック

コントローラのサーバ証明書のインポート，（25 ページ）

Cisco APIC-EM コントローラ証明書チェーンのサポート

Cisco APIC-EMは GUI を介してコントローラに証明書および秘密キーをインポートできます。

コントローラにインポートする証明書（コントローラ証明書）につながる証明書チェーンに関連する下位証明書は、これらの下位CAのルート証明書と一緒に単一のファイルに追加してインポートする必要があります。これらの証明書を追加する場合は、認定の実際のチェーンと同じ順序で追加する必要があります。

たとえば、ルート証明書（ルート CA）で既知の信頼できる CA が中間 CA 証明書（CA1）に署名したと仮定します。次に、この証明書 CA1 が別の中間 CA 証明書（CA2）に署名するとします。

最後に CA 証明書（CA2）がコントローラ証明書（Controller_Certificate）に署名した CA であると仮定します。この例では、コントローラに作成およびインポートする必要のある PEM ファイルは、次のファイルの上部（最初）からファイルの下部（最後）までの順序である必要があります。

1. Controller_Certificate（ファイルの上部）
2. CA2 証明書
3. CA1 証明書

単一ファイルの作成のためにコントローラの証明書にルートおよび下位証明書を追加する要件は、PEM ファイルにのみ適用されます。インポートのためにルート証明書にルートおよび中間証明書を追加する要件は、PKCS ファイルには必要ありません。

関連トピック

コントローラのサーバ証明書のインポート，（25 ページ）

Cisco APIC-EM コントローラの CA 署名付き証明書の取得

次の手順を実行して、Cisco APIC-EMにインポートして使用する CA 署名付き証明書を取得できます。

1. Cisco APIC-EMクラスタの IP アドレスまたは DNS 解決可能 FQDN を特定します。
2. 証明書署名要求（CSR）の共通名としてその IP アドレスを使用します。
3. 次に示す手順に従って、CSR を作成します。
4. 選択した認証局（CA）に作成した CSR を送信します。
5. CA から署名付き証明書を受信します。
6. コントローラの GUI を使用して、コントローラに証明書をインストールします。

（注） この手順の例は、Cisco APIC-EMがインストールされているホストで実行されています。Linux OS または Apple Macintosh コンピュータでも、この手順を実行して CSR と秘密キーを生成できます。この手順は、Cisco APIC-EMがインストールされているホストで実行する必要はありません。

はじめる前に

この手順を行うには、次の項目に関する知識が必要です。

- OpenSSL アプリケーションの使用方法

• 公開キー インフラストラクチャおよびデジタル証明書

ステップ 1 セキュア シェル（SSH）クライアントを使用し、設定ウィザードを使用して指定した IP アドレスでホスト（物理または仮想）にログインします。
SSH クライアントで入力する IP アドレスは、ネットワーク アダプタ用に設定した IP アドレスです。この IP アドレスは、ホストを外部ネットワークに接続します。

ステップ 2 プロンプトが表示されたら、Linux のユーザ名（「grapevine」）と SSH アクセス用のパスワードを入力します。

ステップ 3 次のコマンドを入力して、秘密キーと CSR を作成します。

```
$ openssl req -out CSR.csr -new -newkey rsa:2048 -nodes -keyout privateKey.key

Generating a 2048 bit RSA private key
..........................................................+++
........+++
writing new private key to 'privateKey.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
```

ステップ 4 必要に応じてお客様固有の情報を使用して証明書プロンプトに応答します。
共通名の IP アドレスについては、この要求が複数ホストのCisco APIC-EM導入向けである場合は、複数ホストに予定された仮想IPアドレスを入力します。この要求が単一のCisco APIC-EMアプライアンスまたは VM 向けである場合は、eth0 IP アドレスを入力します。

次に例を示します。

```
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:CA
Locality Name (eg, city) []:San Jose
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Cisco
Organizational Unit Name (eg, section) []:Cloud Unit
Common Name (e.g. server FQDN or YOUR name) []:209.165.201.22
Email Address []:myemail@email.com
```

ステップ 5 追加の属性フィールドには値を入力せずに、Enter を押します。

```
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:

An optional company name []:
```

Enterを押すと、2 つのファイル（CSR と秘密キー）が生成されます。

ステップ 6 ホストで生成された 2 つのファイル（CSR と秘密キー）を検索します。

2 つのファイルは privateKey.key と CSR.csr です。

たとえば、次のコマンドを使用してファイルに関する情報を表示します。

```
$ ls -ltr
total 8

-rw-rw-r-- 1 grapevine grapevine 1708 Apr 18 15:39 privateKey.key
-rw-rw-r-- 1 grapevine grapevine 1054 Apr 18 15:39 CSR.csr
```

ステップ 7 privateKey.key ファイルを保護します。

（注） 秘密キーは決して送信しないでください。ネットワークの安全な場所に保管します。

ステップ 8 CSR.csr ファイルから CSR コンテンツをコピー アンド ペーストして、署名用に CA に送信します。

（注） 組織が独自の CA を実行していない限り、通常は CA が trustpool CA となります。

この例では、次の太字の内容が、コピーされて署名用に CA に送信され証明書の返送先となる CSR です。

```
$ cat CSR.csr

-----BEGIN CERTIFICATE REQUEST-----
MIIC0jCCAboCAQAwgYwxCzAJBgNVBAYTAlVTMQswCQYDVQQIDAJDQTERMA8GA1UE
MRYwFAYDVQQDDA0xNzIuMjQuMTAwLjU1MSAwHgYJKoZIhvcNAQkBFhFteWVtYWls
QGVtYWlsLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAONJ7M96
rXjg/kwWcfJUlJJG2agLv7EAIxaB7He84fSdNMVXsJmuYBwZBWuZ9t/h3AKs/n/t
MRYwFAYDVQQDDA0xNzIuMjQuMTAwLjU1MSAwHgYJKoZIhvcNAQkBFhFteWVtYWls
QGVtYWlsLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAONJ7M96
rXjg/kwWcfJUlJJG2agLv7EAIxaB7He84fSdNMVXsJmuYBwZBWuZ9t/h3AKs/n/t
87nugrgW7SmI4F1wLsVg8KU2X0bmHoke6yCkhCPykQXJR2blMWp/OBc0ASMTIdhH
XRju1y/5
-----END CERTIFICATE REQUEST-----
(grapevine)
```

重要 1 つのルート CA 証明書ではなく、CA 証明書のチェーン（CA 自体のパブリック ルート証明書を含む）が返送されることがあります。この場合は、GUI を使用してコントローラに証明書をインポートする前に、Cisco APIC-EM コントローラ証明書チェーンのサポート, （10 ページ）で説明されている CA 証明書の追加ルールに従ってください。

ステップ 9 組織の CA 管理者によって署名付き証明書（たとえば MyCert.pem）が提供されたら、**MyCert.pem** および **privateKey.key** をCisco APIC-EM GUI 証明書のページにドラッグ アンド ドロップします。この手順の詳細については、次を参照してください。コントローラのサーバ証明書のインポート, （25 ページ）

（注） CA 管理者から取得した MyCert.pem ファイルの内容は、Base64 エンコードされた PEM 形式の CSR コンテンツのように見えるはずです。このコンテンツを表示するには、取得したファイルで **cat** コマンドを実行します。ファイルの内容が **cat** コマンド出力でバイナリ ファイルのように見える場合は、次のリンクにあるコンバータを使用して、ファイルの内容を PEM 形式に変換します。

https://www.sslshopper.com/ssl-converter.html

関連トピック

コントローラのサーバ証明書のインポート，（25 ページ）

Cisco APIC-EMTrustpool サポート

Cisco APIC-EMおよびCisco IOS デバイスは trustpool と呼ばれる特別な PKI 証明書ストアをサポートします。trustpool は信頼できる認証局（CA）を特定する X.509 証明書を保持します。Cisco APIC-EMおよびネットワークのデバイスは trustpool バンドルを使用して、相互の信頼関係、およびそれぞれの CA との信頼関係を管理します。コントローラはこの PKI 証明書ストアを管理し、プール内の証明書が失効したり、再発行されたりした場合、またはその他の理由で変更する必要がある場合は、管理者（ROLE_ADMIN）がコントローラの GUI を使って証明書を更新することができます。

（注） また、Cisco APIC-EMは trustpool 機能を使用して、GUI でアップロードする証明書ファイルが有効な trustpool CA 署名付き証明書であるかどうかを判別します。

Cisco APIC-EMには、ios.p7b という名前のシスコの署名付き trustpool バンドルがデフォルトでプリインストールされています。この trustpool バンドルは、シスコのデジタル署名証明書で署名されているので、サポートされているシスコのネットワーク デバイスによりネイティブで信頼されます。この trustpool バンドルは、シスコのネットワーク デバイスが純正のアプリケーションおよびサービスとの信頼を確立するために重要です。このCisco PKIのtrustpoolバンドル ファイルは、シスコの Web サイト（Cisco InfoSec）にあります。

リンクは次の場所にあります。http://www.cisco.com/security/pki/

コントローラのネットワーク PnP 機能のために、コントローラにより制御および監視されているサポート対象のシスコ デバイスは、このファイルをインポートする必要があります。サポートされているシスコ デバイスは最初のブート時に、コントローラにアクセスしてこのファイルをインポートします。

Cisco APIC-EMtrustpool の管理機能は次のように動作します。

1. ネットワーク PnP 機能をサポートするネットワーク内のシスコ デバイスをブートします。

   すべてのシスコ デバイスがネットワーク PnP 機能をサポートするわけでは**ない**ことに注意してください。サポート対象のシスコ デバイスのリストについては、『*Release Notes for Cisco Network Plug and Play*』を参照してください。

2. PnP の最初のフローの一部として、これらのサポート対象のシスコ デバイスは、HTTP を使用して trustpool バンドルを Cisco APIC-EMから直接ダウンロードします。

3. シスコ デバイスは、ネットワーク PnP トラフィック フローごとの詳細なデバイス設定およびプロビジョニングを取得するために Cisco APIC-EMと通信できる状態になります。

重要 HTTP プロキシ ゲートウェイがコントローラとこれらのシスコ デバイスの間に存在する場合、コントローラにプロキシ ゲートウェイの証明書をインポートするための追加の手順を実行します。プロキシ ゲートウェイ証明書のインポート，（30 ページ）を参照してください。

（注） trustpool 内の証明書の期限切れ、再発行、またはその他の理由で、trustpool バンドルの新しいバージョンへの更新が必要になる場合があります。コントローラに存在する trustpool バンドルの更新が必要になったときは、コントローラの GUI を使用していつでも更新できます。コントローラはシスコ クラウド（シスコ認定の trustpool バンドルが含まれている）にアクセスして最新の trustpool バンドルをダウンロードできます。ダウンロード後に、コントローラは、現在の古い trustpool バンドル ファイルを上書きします。実際には、[Certificate]ウィンドウまたは [Proxy Gateway Certificate] ウィンドウを使用して CA から新しい証明書をインポートする前、または [Update] ボタンがグレー表示ではなくアクティブな場合はいつでも、trustpool バンドルを更新できます。

関連トピック

Trustpool バンドルのインポート，（28 ページ）

セキュリティおよびシスコ ネットワーク プラグ アンド プレイ

シスコ ネットワーク プラグ アンド プレイ（PnP）アプリケーションを使用して、Cisco APIC-EM はサポート対象のシスコ ネットワーク デバイスからの HTTPS 要求に応答し、これらのデバイスがイメージおよび目的の設定をダウンロードしてインストールすることを許可します。デバイスでコントローラからこれらのファイルをダウンロードできるようにするには、コントローラとデバイス間の最初のインタラクションで信頼関係を確立する必要があります。

シスコ ネットワーク プラグアンドプレイの一部のシナリオでは、ネットワーク構成でコントローラと PnP 対応デバイス間にプロキシ ゲートウェイを配置することができます。たとえば、IWAN 展開では、ブランチ ルータは最初のプロビジョニング時に DMZ でプロキシ ゲートウェイを通じてCisco APIC-EMと通信できます。プロキシ ゲートウェイが存在するかどうかに応じて、デバイスとの最初のトランザクション時にコントローラによって提供された信頼情報はプロキシ ゲートウェイまたはコントローラの証明書発行者に対応できます（対応するサーバ証明書が有効な CA 署名付きでない場合）。一方、プロキシまたは非プロキシのケースでは、証明書が単に自己署名証明書である場合は、その証明書はデバイスによって信頼ストアにダウンロードされます。

（注） Cisco APIC-EMまたはプロキシ ゲートウェイに自己署名証明書を使用することは決して推奨しません。公的に検証可能なCA発行の証明書を使用して、コントローラとプロキシゲートウェイ（存在する場合）にインストールすることを強く推奨します。

コントローラまたはプロキシ ゲートウェイ（存在する場合）に有効な CA 発行の証明書を使用すると、PnP 対応デバイスはすべての既知の CA ルート証明書を含む trustpool バンドル（ios.p7b）をダウンロードできます。これにより、デバイスはコントローラまたはプロキシ ゲートウェイへのセキュアな接続を確立でき、それらのデバイスのさらなるプロビジョニングと操作が可能になります。このような証明書に有効な CA 署名または自己署名がされていない場合、コントローラまたはコントローラの前にあるプロキシ ゲートウェイへのセキュアな接続を先に進めるために、デバイスは発行元の CA の証明書または自己署名証明書をダウンロードする必要があります。インストールされる証明書の特性に応じて、Cisco APIC-EMは、関連する信頼できる証明書のデバイスへの自動ダウンロードを促進します。ただし、プロキシ ゲートウェイが存在する場合は、コントローラによって同様の事前プロビジョニングを促進するためのプロビジョニング GUI が提供されます。

関連トピック

プロキシ ゲートウェイ証明書のインポート, （30 ページ）

CLI を使用した TLS バージョンの設定

外部ネットワーク（HTTPS を使用してコントローラに接続しているノースバウンド REST API ベースのアプリケーション、ブラウザ、ネットワーク デバイス）からCisco APIC-EMへのノースバウンド REST API 要求は、Transport Layer Security（TLS）プロトコルを使用して安全に行われます。Cisco APIC-EMは、TLS バージョン 1.0、1.1、および 1.2 をサポートします。

デフォルトでクライアントがコントローラとの通信に使用できる最小 TLS バージョンは、バージョン 1.0 です。ネットワーク デバイスの IOS/XE バージョンが 1.0 以降のバージョンをサポートできる場合は、コントローラの最小 TLS バージョンを上位のバージョンに設定することを強くお勧めします。ただし、Cisco APIC-EM制御下にあるすべてのネットワーク デバイスがその上位バージョンをサポートできることを事前に確認してください。

重要 コントローラの TLS バージョンが 1.2 に設定されている場合、下位の TLS バージョン（1.0 または 1.1）で接続を開始したクライアントは拒否され、このクライアントからの通信はすべて失敗します。コントローラの TLS バージョンが 1.0 に設定されている場合、上位の TLS バージョン（1.1 または 1.2）で接続を開始したクライアントは許可されます。TLS 1.0 未満のバージョン（SSLv3 や SSLv2 など）は、Cisco APIC-EMでサポートされません。

コントローラの TLS バージョンを設定するには、ホスト（物理または仮想）にログインして CLI を使用します。

はじめる前に

Cisco APIC-EMが正常に導入され、動作している必要があります。

この手順を実行するには、Grapevine への SSH アクセス権限が必要です。

重要 このセキュリティ機能は、Cisco APIC-EMのポート 443 および 14141 に適用されます。この手順を実行すると、コントローラ インフラストラクチャへのポート 14141 上のトラフィックが数秒間無効になることがあります。したがって、TLS の設定は頻繁に行わないようにするか、ピーク以外の時間帯またはメンテナンス期間中にのみ行ってください。

ステップ 1 セキュア シェル（SSH）クライアントを使用し、設定ウィザードを使用して指定した IP アドレスでホスト（物理または仮想）にログインします。

（注） SSH クライアントで入力する IP アドレスは、ネットワーク アダプタ用に設定した IP アドレスです。この IP アドレスは、ホストを外部ネットワークに接続します。

ステップ 2 プロンプトが表示されたら、SSH アクセス用の Linux ユーザ名（「grapevine」）とパスワードを入力します。

ステップ 3 プロンプトに grape config display コマンドを入力して、デフォルトの最小 TLS バージョンを表示します。

```
$ grape config display

PROPERTY                          VALUE
------------------------------------------------------------------------
client_grow_timeout               150
client_heartbeat_timeout          120
client_idle_timeout               60
enable_policy                     True
enable_secure_tunnel              True
enable_service_rollback           False
host_cpu_threshold                0.9
host_datastore_threshold          1.0
host_heartbeat_timeout            120
host_memory_threshold             0.00999999977648
https_proxy
https_proxy_password
https_proxy_username
load_multiplier                   1.0
max_spare_capacity                1
policy_startup_delay              120
tls_minimum                       1_0

(grapevine)
```

上記のコマンド出力は、現在の TLS の最小バージョンが 1.0 であることを示しています。

ステップ 4 プロンプトに grape config update tls_minimum 1_2 コマンドを入力して、TLS バージョン 1.2 に更新します。

```
$ grape config update tls_minimum 1_2
Config updated successfully
```

```
(grapevine)
```

TLS バージョンを 1.1 に更新するには、grape config update tls_mimimum 1_1 コマンドを入力します。

ステップ 5 プロンプトに再度 grape config display コマンドを入力して、新しい最小 TLS バージョンを表示します。

```
$ grape config display

PROPERTY                          VALUE
------------------------------------------------------------------------
client_grow_timeout               150
client_heartbeat_timeout          120
client_idle_timeout               60
enable_policy                     True
enable_secure_tunnel              True
enable_service_rollback           False
host_cpu_threshold                0.9
host_datastore_threshold          1.0
host_heartbeat_timeout            120
host_memory_threshold             0.00999999977648
https_proxy
https_proxy_password
https_proxy_username
load_multiplier                   1.0
max_spare_capacity                1
policy_startup_delay              120
tls_minimum                       1_2

(grapevine)
```

最小 TLS バージョンは、TLS 1.2 バージョンを示す *1_2* と表示されます。

関連トピック

外部ネットワーク セキュリティ
デバイス管理ネットワーク セキュリティ

複数ホストの通信のための IPSec トンネリングの設定

マルチホストクラスタ内のホスト間通信に使用されるデフォルトのトンネリングプロトコルは、インターネット プロトコル セキュリティ（IPsec）です。以前のコントローラ リリース バージョンのデフォルトのトンネリング プロトコルは、Generic Routing Encapsulation（GRE）でした。マルチホスト クラスタ内のホスト間の通信は、IPSec を使用してより安全に行うことができます。ホスト間の現在のトンネリング設定が GRE である場合は、設定ウィザードを使用して IPSec によるセキュア トンネリングを有効にすることができます。

ホスト間の通信のセキュリティを強化するには、次の手順で説明するステップを実行します。手順の概要は次のとおりです。

1 既存のマルチホスト クラスタを分解する（ステップ 1 ～ 6）。

2 クラスタの最後のホストで IPSec トンネリングを有効にする（ステップ 7 ～ 11）。

3 IPSec トンネリングを有効にしたホスト以外でマルチホスト クラスタを再構築する（ステップ 11 ～ 21）。

（注） Cisco APIC-EMがマルチホスト クラスタ内にある間は、セキュア トンネル モード（IPSec トンネリング）を有効または無効にしないでください。設定ウィザードは、複数ホスト クラスタ内にある間のそのような変更をサポートしていません。

はじめる前に

Cisco APIC-EMが正常に導入され、動作している必要があります。

現在のトンネリング プロトコルは、IPSec ではなく GRE です。

この手順を実行するには、Grapevine への SSH アクセス権限が必要です。

ステップ 1 Secure Shell（SSH）クライアントを使用して、クラスタ内の 1 つのホストにログインします。
プロンプトが表示されたら、Linux のユーザ名（「grapevine」）と SSH アクセス用のパスワードを入力します。

ステップ 2 grape config display コマンドを入力して、現在の GRE トンネリング設定を表示して確認します。

```
$ grape config display
```

GRE 設定の場合、enable_secure_tunnel 値は false に設定されます。

ステップ 3 次のコマンドを入力して設定ウィザードにアクセスします。

```
$ config_wizard
```

ステップ 4 [Welcome to the APIC-EM Configuration Wizard!]画面を確認し、クラスタからホストを削除するオプションを選択します。

- [Remove this host from its APIC-EM cluster]

ステップ 5 オプション [proceed]とともにメッセージが表示されるので、クラスタからこのホストを削除します。
開始するには、[proceed>>]を選択します。[proceed>>]を選択した後、設定ウィザードはクラスタからのこのホストの削除を開始します。
このプロセスの最後に、このホストはクラスタから削除されます。

ステップ 6 クラスタの 2 番目のホストで上記の手順（ステップ 1 ～ 4）を繰り返します。これにより、マルチホスト クラスタが分解されます。

重要 最後に削除したクラスタ内の最後のホストをメモします。その最後のホストで以降のステップ（IPSec トンネリングの有効化）を実行する必要があります。たとえば、クラスタに 3 つのホスト（A、B、C）があり、最初にホスト A を削除して、次にホスト B を削除する場合は、ホスト C で IPSec を有効にする必要があります。

ステップ 7 Secure Shell（SSH）クライアントを使用して、クラスタの最後のホストにログインし、config_wizard コマンドを実行します。

```
$ config_wizard
```

ステップ 8 [INTER-HOST COMMUNICATION]画面にアクセスするまで、設定ウィザードの現在の設定値を確認して、[next>>] をクリックします。

ステップ 9 [yes]を選択して、複数ホスト クラスタ内のホスト間の通信用に IPSec トンネリングを設定します。
「yes」と入力すると、このステップで IPSec トンネリングを設定することになります。

ステップ 10 設定ウィザード プロセスの最後のステップに到達するまで [next>>]をクリックします。

ステップ 11 [proceed>>]をクリックして、設定ウィザードによって Cisco APIC-EM の導入に対する設定変更を保存および適用します。
設定プロセスの最後に、「CONFIGURATION SUCCEEDED!」というメッセージが表示されます。

次に、以前に複数ホストクラスタ内にあった他のホストにログインし、設定ウィザードを使用して、クラスタを再構成します（ホスト間に設定された IPSec トンネリングを使用します）。

ステップ 12 セキュア シェル（SSH）クライアントを使用して、クラスタ内の他のホストのいずれかにログインします。
プロンプトが表示されたら、Linux のユーザ名（「grapevine」）と SSH アクセス用のパスワードを入力します。

ステップ 13 次のコマンドを入力して設定ウィザードにアクセスします。

```
$ config_wizard
```

ステップ 14 [Welcome to the APIC-EM Configuration Wizard!]画面を確認し、[Create a new APIC-EM cluster] オプションを選択します。

（注） 他の（2 番目の）ホストを IPSec トンネリングが有効なホストに参加させると、他の（2 番目の）ホストで IPSec トンネリングが自動的に設定されます。

ステップ 15 設定ウィザードを使用してクラスタの再作成に進みます。
この手順とプロセスに関する詳細情報については、 を参照してください。

ステップ 16 設定プロセスの最後に、[proceed>>]をクリックし、設定ウィザードにより設定の変更を保存して適用します。
「CONFIGURATIONSUCCEEDED!」というメッセージが表示されます。

ステップ 17 Secure Shell（SSH）クライアントを使用して、3 番目のホストにログインし、設定ウィザードを使用して、新しい複数ホスト クラスタに参加します。
プロンプトが表示されたら、Linux のユーザ名（「grapevine」）と SSH アクセス用のパスワードを入力します。

ステップ 18 次のコマンドを入力して設定ウィザードにアクセスします。

```
$ config_wizard
```

ステップ 19 [Welcome to the APIC-EM Configuration Wizard!]画面を確認し、[Add this host to an existing APIC-EM cluster] オプションを選択します。

（注） このホストを IPSec トンネリングが有効な新しい複数ホスト クラスタに追加すると、このホストで IPSec トンネリングが自動的に設定されます。

ステップ 20 設定ウィザードを使用して、クラスタへのこのホストの追加に進みます。
この手順とプロセスに関する詳細情報については、*Cisco Application Policy Infrastructure Controller Enterprise Module Installation Guide*を参照してください。

ステップ 21 設定プロセスの最後に、[proceed>>]をクリックし、設定ウィザードにより設定の変更を保存して適用します。
「CONFIGURATIONSUCCEEDED!」というメッセージが表示されます。

この手順が終了すると、クラスタが更新され、IPSec トンネリングが設定されます。

関連トピック

内部ネットワーク セキュリティ

パスワード要件

Cisco APIC-EMのパスワードポリシーは、コントローラ GUI へのログイン、Grapevine ルートへの SSH ログイン、ノースバウンド API 要求およびトラブルシューティングのための Grapevine コンソールへのログインでのパスワード値を管理します。Cisco APIC-EMはパスワード ポリシーに準拠していないパスワードを拒否します。パスワードが拒否されると、コントローラが拒否理由を説明するエラー メッセージを表示します。

新規または変更されたパスワードは次の基準を満たす必要があります。

- パスワードの文字数が 8（最小） ～ 127（最大）文字である。
- タブまたは改行を含まない。
- 次の中から少なくとも 3 つのカテゴリの文字を含む。
  - 大文字のアルファベット
  - 小文字のアルファベット
  - 数字
  - 特殊文字

特殊文字には、スペース文字、または以下のいずれかの文字（または文字の組み合わせ）が含まれます。

```
! @ # $ % ^ & * ( ) - =  + _ { } [ ] \\ | ; : " ' , < . > ? /
:: #! ./ ;; >> << () **
```

たとえば、`Splunge!` は、長さが 8 文字以上で、1 文字以上の大文字のアルファベット、1 文字以上の小文字のアルファベット、1 文字以上の特殊文字（!）が含まれているため、有効なパスワードです。

関連トピック

パスワード ポリシーの設定, （39 ページ）

Cisco APIC-EM ポート リファレンス

次の表に、着信トラフィックを許可する Cisco APIC-EMポートと、発信トラフィックに使用されるCisco APIC-EM ポートを示します。コントローラでこれらのポートが着信および発信の両方のトラフィック フローに対して開かれていることを確認する必要があります。

（注） ネットワークでポート 22 および 14141 へのアクセスが適切に保護されていることを確認します。たとえば、プロキシ ゲートウェイや、これらのポートにアクセスするための安全なサブネットを設定することができます。

表 *2* : ***Cisco APIC-EM***着信トラフィック ポート リファレンス

ポート番号	許可されるトラフィック	プロトコル（**TCP** または **UDP**）
22	SSH	TCP
67	bootps	UDP
80	HTTP	TCP
123	NTP	UDP
162	SNMP	UDP
443 [1]	HTTPS	TCP

ポート番号	許可されるトラフィック	プロトコル（TCP または UDP）
500	ISAKMP 特定の導入でファイアウォールを介して複数のホストを導入するためには、IPSec ISAKMP（Internet Security Association and Key Management Protocol）UDP ポート 500 の通過が許可されている必要があります。	UDP
14141	Grapevine API	TCP
16026	SCEP	TCP

[1] Cisco APIC-EM を使用してこのポート用の TLS バージョンを設定できます。詳細については、次のサイトを参照してください。CLI を使用した TLS バージョンの設定, （16 ページ）

表 *3* : *Cisco APIC-EM*発信トラフィック ポート リファレンス

ポート番号	許可されるトラフィック	プロトコル（TCP または UDP）
22	SSH（ネットワーク デバイスへ）	TCP
23	Telnet（ネットワーク デバイスへ）	TCP
53	DNS	UDP

ポート番号	許可されるトラフィック	プロトコル（TCP または UDP）
80	ポート 80 は発信プロキシ設定に使用できます。 さらに、8080 など、その他の共通のポートもプロキシが Cisco APIC-EM 設定ウィザードで設定されているときに使用できます（プロキシがすでにネットワークで使用されている場合）。 （注） シスコでサポートしている証明書および trustpool にアクセスするには、次の URL でコントローラからシスコのアドレスへの発信 IP トラフィックを許可するようにネットワークを設定することができます。 http://www.cisco.com/security/pki/	TCP
123	NTP	UDP
161	SNMP エージェント	UDP
443 [2]	HTTPS	TCP
500	ISAKMP 特定の導入でファイアウォールを介して複数のホストを導入するためには、IPSec ISAKMP（Internet Security Association and Key Management Protocol）UDP ポート 500 の通過が許可されている必要があります。	UDP

[2] Cisco APIC-EM を使用してこのポート用の TLS バージョンを設定できます。詳細については、次のサイトを参照してください。CLI を使用した TLS バージョンの設定, （16 ページ）

セキュリティの設定

コントローラのサーバ証明書のインポート

Cisco APIC-EMは、コントローラへのX.509証明書と秘密キーのインポートおよび保存をサポートしています。インポートした証明書と秘密キーを使用して、Cisco APIC-EM、NB API アプリケーション、およびネットワーク デバイスの間に安全で信頼性の高い環境を構築できます。

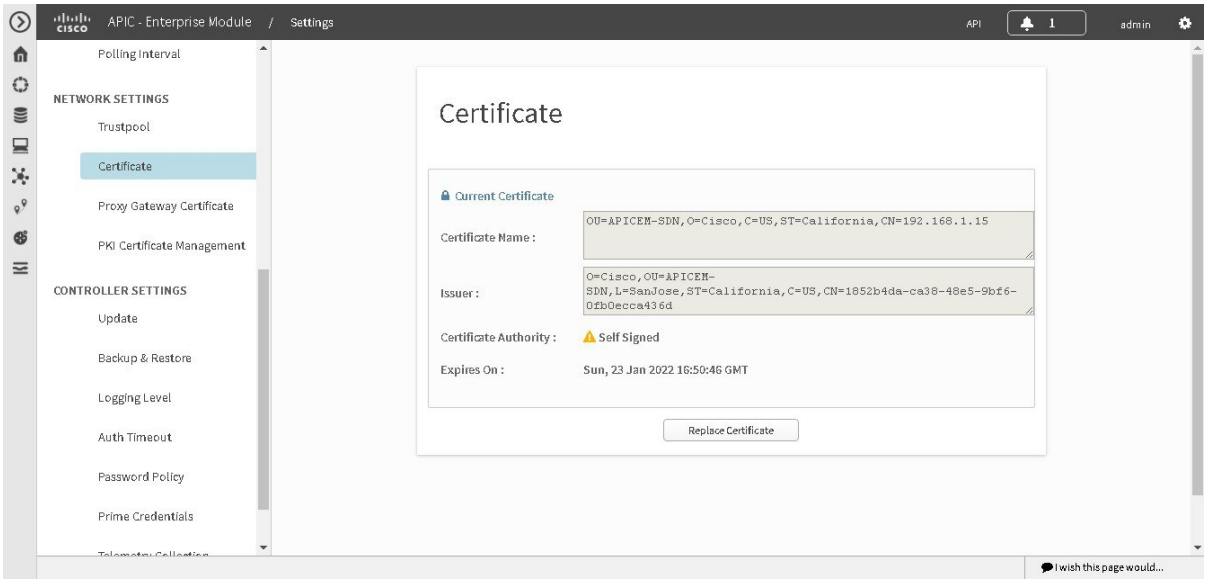
（注）

マルチホスト導入で、コントローラHTTPSサーバの有効なCA発行証明書を取得する場合は、注文時に証明書の共通名としてマルチホストに割り当てた仮想 IP アドレスを使用します。その代わりにホスト名を使用する場合は、ホスト名がマルチホスト導入の仮想IPアドレスにDNS解決できることを確認します。

単一ホストCisco APIC-EMですでに外部 IP アドレス用に購入済みの CA 発行証明書がある場合は、単一ホストの元々の物理 IP アドレスをマルチホスト導入の仮想 IP アドレスとして使用することをお勧めします。この方法を使用すれば、CA 発行証明書への投資を削減でき、外部クライアント アプリケーションは引き続き同じ IP アドレスを使用して Cisco APIC-EMサービスにアクセスできます。

Cisco APIC-EMGUI の [Certificate] ウィンドウを使用して、証明書と秘密キーをインポートします。

図 *3*：証明書の設定ウィンドウ



重要 Cisco APIC-EM自体は、外部 CA と直接やり取りしないため、証明書失効リストをチェックしません。また、外部CA がサーバ証明書の失効を確認する方法はありません。コントローラは自動的にサーバ証明書を更新しないことにも注意してください。期限切れまたは失効済みのサーバ証明書を交換するには、ROLE_ADMIN ユーザ側の明示的なアクションが必要です。コントローラには外部CA によるサーバ証明書の失効を検出する直接的な方法はありませんが、管理者に対して運用中のサーバ証明書と自己署名キーの有効期限を通知します。

はじめる前に

Cisco APIC-EMが正常に導入され、動作している必要があります。

インポートする X.509 証明書と秘密キーは既知の認証局（CA）から取得する必要があります。

管理者（ROLE_ADMIN）権限、およびすべてのリソースへのアクセス権（RBAC スコープを [ALL] に設定）またはグループ化するすべてのリソースを含む RBAC スコープが必要です。たとえば、特定のリソース セットを含むグループを作成するには、これらのリソースへのアクセス権が必要です（グループ化するすべてのリソースをカスタム RBAC スコープとして設定）。

Cisco APIC-EM を使用してタスクを実行するために必要なユーザ権限と RBAC スコープについては、「Cisco APIC-EM の設定」の章の「ユーザ設定」を参照してください。

ステップ 1 [Home]ウィンドウで、画面右上の [admin] または [Settings] アイコン（歯車）をクリックします。

ステップ 2 ドロップダウン メニューの [Settings]リンクをクリックします。

ステップ 3 [Settings]ナビゲーション ウィンドウで、[Certificate] をクリックして [Certificate] ウィンドウを表示します。

ステップ 4 [Certificate]ウィンドウで、現在の証明書データを確認します。
このウィンドウを最初に表示したときには、現在の証明書データとしてコントローラの自己署名証明書が表示されます。自己署名証明書の有効期限は、数年後の日付に設定されています。

（注） [Expiration Date and Time]は、グリニッジ標準時（GMT）値で表示されます。証明書の有効期限の 2 ヵ月前に、コントローラの GUI にシステム通知が表示されます。

[Certificate]ウィンドウに表示されるその他のフィールドは次のとおりです。

- [Certificate Name]：証明書の名前。
- [Issuer]：発行者名は、証明書に署名して発行したエンティティを識別します。
- [Certificate Authority]：自己署名または CA 名。
- [Expiration On]：証明書の有効期限。

ステップ 5 現在の証明書を交換するには、[Replace Certificate]ボタンをクリックします。
次の新しいフィールドが表示されます。

- [Certificate]：証明書データを入力するフィールド
- [Private Key]：秘密キーデータを入力するフィールド

ステップ 6 [Certificate]フィールドで、証明書のファイル形式タイプを選択します。

- [PEM]：プライバシー強化メールファイル形式
- [PKCS]：公開キー暗号化標準ファイル形式

Cisco APIC-EMにインポートする証明書として上記のファイル タイプのいずれかを選択します。

ステップ 7 [PEM]を選択した場合、次のタスクを実行します。

- [Certificate]フィールドで、[Drag n' Drop a File Here] フィールドにファイルをドラッグ アンド ドロップして、PEM ファイルをインポートします。

  （注） PEM ファイルの場合、有効な PEM 形式の拡張子（.pem、.cert、.crt）が必要です。証明書の最大ファイル サイズは 10 KB です。

- [Private Key]フィールドで、[Drag n' Drop a File Here] フィールドにファイルをドラッグ アンド ドロップして、秘密キーをインポートします。
  - [Encrypted]ドロップダウン メニューから秘密キーの暗号化オプションを選択します。
  - 暗号化を選択した場合は、[Passphrase]フィールドに秘密キーのパスフレーズを入力します。

    （注） 秘密キーの場合は、有効な秘密キー形式の拡張子（.pem または .key）が必要です。

ステップ 8 [PKCS]を選択した場合、次のタスクを実行します。

- [Certificate]フィールドで、[Drag n' Drop a File Here] フィールドにファイルをドラッグ アンド ドロップして、PKCS ファイルをインポートします。

  （注） PKCS ファイルの場合、有効な PKCS 形式の拡張子（.pfx、.p12）が必要です。証明書の最大ファイル サイズは 10 KB です。

- [Certificate]フィールドで、[Passphrase] フィールドを使用して証明書のパスフレーズを入力します。

  （注） PKCS の場合は、インポートした証明書もパスフレーズを必要とします。

- [Private Key]フィールドで、ドロップダウン メニューを使用して秘密キーの暗号化オプションを選択します。
- [Private Key]フィールドで、暗号化を選択した場合は、[Passphrase] フィールドに秘密キーのパスフレーズを入力します。

ステップ 9 [Upload/Activate]ボタンをクリックします。

ステップ 10 [Certificate]ウィンドウに戻り、更新された証明書データを確認します。
[Certificate]ウィンドウに表示される情報が変更されて、新しい証明書の名前、発行元、および認証局が反映されます。

関連トピック

Cisco APIC-EMコントローラ証明書および秘密キーのサポート, （9 ページ）
Cisco APIC-EM コントローラ証明書チェーンのサポート, （10 ページ）
Cisco APIC-EM コントローラの CA 署名付き証明書の取得, （11 ページ）

Trustpool バンドルのインポート

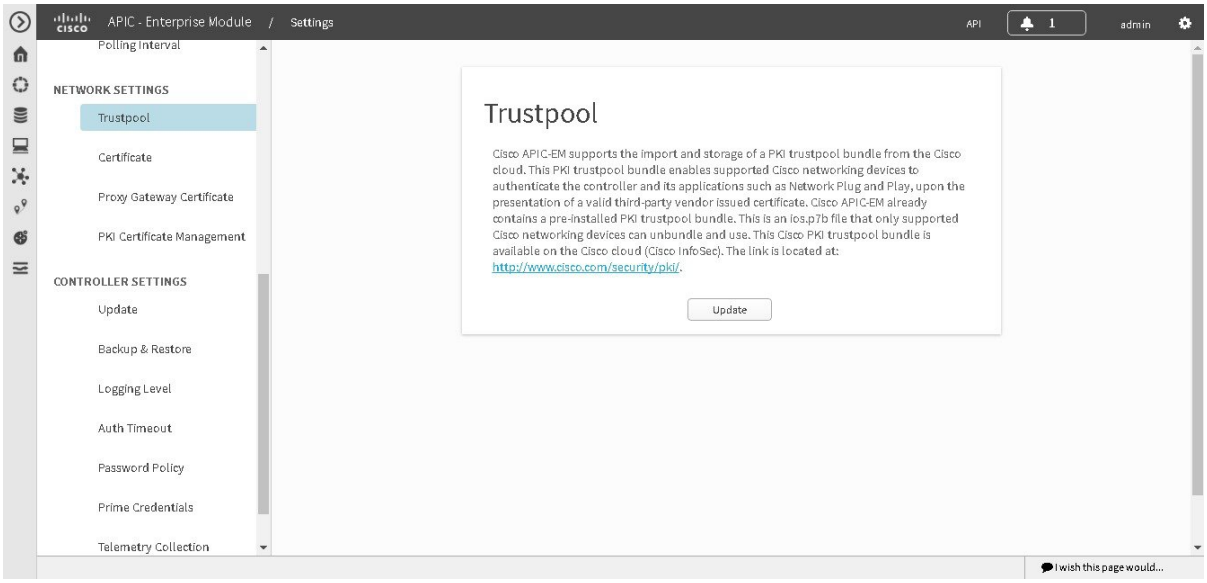
Cisco APIC-EMには、プリインストールされた Cisco trustpool バンドル（Cisco Trusted External Root Bundle）が含まれています。Cisco APIC-EMは、更新された Cisco trustpool バンドルのインポートと保存もサポートします。trustpool バンドルは、サポート対象のシスコ ネットワーキング デバイスがコントローラおよびそのアプリケーション（ネットワーク PnP など）との信頼関係を確立するために使用されます。

（注） Cisco trustpool バンドルは、サポートされるシスコ デバイスのみがバンドル解除および使用できる ios.p7b ファイルです。この ios.p7b ファイルには、シスコ自身を含む有効な認証局のルート証明書が含まれます。この Cisco trustpool バンドルは、シスコ クラウド（Cisco InfoSec）で使用できます。リンクは http://www.cisco.com/security/pki/ にあります。

trustpool バンドルを使用すると、すべてのネットワーク デバイス証明書およびコントローラ証明書を管理するために、同じ CA を安全かつ簡単に使用できます。trustpool バンドルは、コントローラが自身の証明書およびプロキシ ゲートウェイ証明書（存在する場合）を検証して有効な CA 署名証明書であるかどうかを判断するために使用されます。trustpool バンドルは、Network PnP 対応デバイスで PnP ワークフローを開始するときにアップロードすることもできるため、これらのデバイスがその後の HTTPS ベース接続でコントローラを信頼できるようになります。

Cisco APIC-EMGUI の [Trustpool] ウィンドウを使用して、Cisco trustpool バンドルをインポートします。

図 *4*：*[Trustpool]* ウィンドウ



はじめる前に

Cisco APIC-EMが正常に導入され、動作している必要があります。

管理者（ROLE_ADMIN）権限、およびすべてのリソースへのアクセス権（RBACスコープを[ALL]に設定）またはグループ化するすべてのリソースを含むRBAC スコープが必要です。たとえば、特定のリソース セットを含むグループを作成するには、これらのリソースへのアクセス権が必要です（グループ化するすべてのリソースをカスタム RBAC スコープとして設定）。

Cisco APIC-EM を使用してタスクを実行するために必要なユーザ権限と RBAC スコープについては、「Cisco APIC-EM の設定」の章の「ユーザ設定」を参照してください。

ステップ 1 [Home]ウィンドウで、画面右上の [admin] または [Settings] アイコン（歯車）をクリックします。

ステップ 2 ドロップダウン メニューの [Settings]リンクをクリックします。

ステップ 3 [Settings]ナビゲーション ウィンドウで、[Trustpool] をクリックして [Trustpool] ウィンドウを表示します。

ステップ 4 [Trustpool]ウィンドウの [Update] ボタンを確認します。
ios.p7b ファイルの更新バージョンが使用可能で、インターネット アクセスを利用できる場合は、コントローラの [Trustpool]ウィンドウで [Update]ボタンがアクティブになっています。インターネット アクセスがない場合や、ios.p7b ファイルの更新バージョンが存在しない場合、[Update]ボタンは非アクティブのままです。

ステップ 5 [Update]ボタンをクリックして、trustpoolバンドルの新規ダウンロードおよびインストールを開始します。

（注） 新しい trustpool バンドルがダウンロードされ、コントローラにインストールされると、コントローラはサポート対象のシスコ デバイスがこの trustpool バンドルをダウンロードできるようにします。

関連トピック

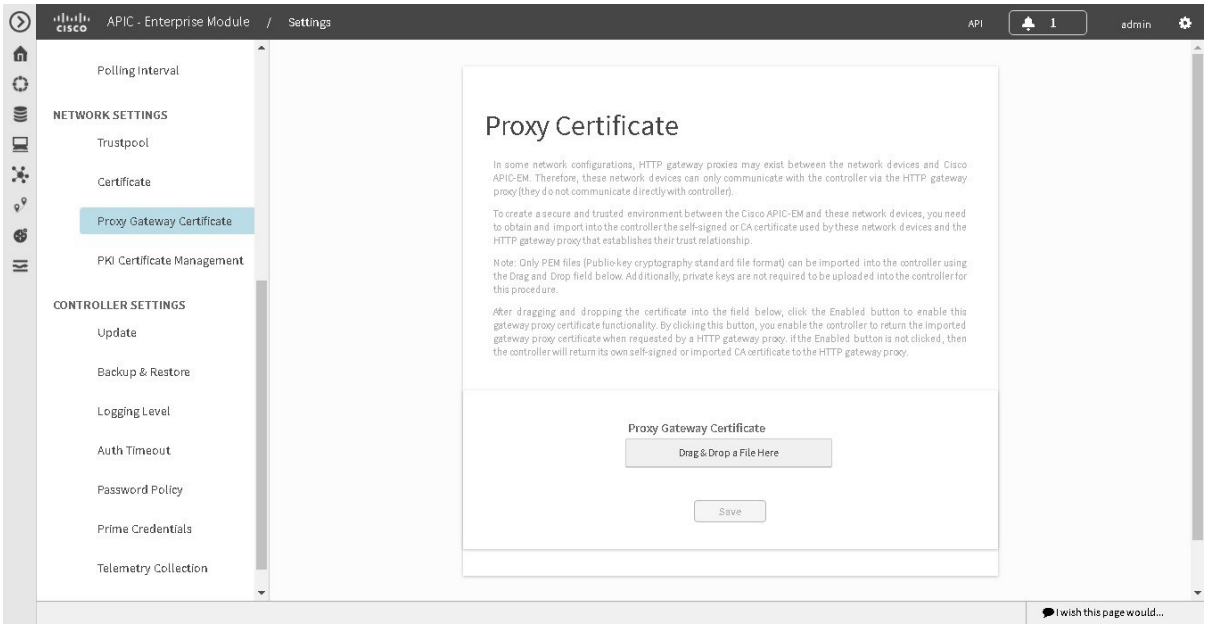
Cisco APIC-EMTrustpool サポート，（14 ページ）

プロキシ ゲートウェイ証明書のインポート

ネットワーク構成によっては、Cisco APIC-EMとその管理対象リモート ネットワーク（IWAN および PnP ネットワーク デバイスを含む）の間にプロキシ ゲートウェイが存在する場合があります。一般的なポート（80 や 443 など）は DMZ 内のゲートウェイ プロキシをパス スルーします。そのため、コントローラ用に設定されたネットワーク デバイスからの SSL セッションはプロキシ ゲートウェイで終了します。したがって、これらのリモート ネットワーク内にあるネットワーク デバイスは、プロキシゲートウェイ経由でのみコントローラと通信できます。ネットワーク デバイスがコントローラまたはプロキシ ゲートウェイ（存在する場合）との安全で信頼性の高い接続を確立するためには、関連する CA ルート証明書または特定の状況下ではサーバ自体の証明書を使用して、PKI 信頼ストアが適切にプロビジョニングされている必要があります。

コントローラとその管理対象リモートネットワークの間にプロキシゲートウェイが存在するネットワーク トポロジでは、次の手順に従ってプロキシ ゲートウェイ証明書をコントローラにインポートします。

図 *5*：*[Proxy Gateway Certificate]* ウィンドウ



はじめる前に

Cisco APIC-EMが正常に展開され、動作している必要があります。

ネットワーク内のコントローラとその管理対象リモート ネットワーク（IWAN および PnP ネットワーク デバイスを含む）の間に HTTP プロキシ ゲートウェイが存在します。これらのネットワーク デバイスは、Cisco APIC-EMコントローラとそのサービスに到達するために、プロキシ ゲートウェイの IP アドレスを使用します。

プロキシ ゲートウェイで現在使用している証明書ファイルがあります。証明書ファイルのコンテンツは、次のいずれかで構成されます。

- PEM 形式のプロキシ ゲートウェイの証明書、および自己署名された証明書。
- PEM形式のプロキシ ゲートウェイの証明書、および有効な既知の CA によって発行された証明書。
- PEM 形式のプロキシ ゲートウェイの証明書とそのチェーン。

デバイスおよびプロキシ ゲートウェイで使用される証明書は、次の手順に従ってコントローラにインポートする必要があります。

ステップ 1 [Home]ウィンドウで、画面右上の [admin] または [Settings] アイコン（歯車）をクリックします。

ステップ 2 ドロップダウン メニューの [Settings]リンクをクリックします。

ステップ 3 [Settings]ナビゲーション ウィンドウで、[Proxy Gateway Certificate] をクリックして [Proxy Certificate] ウィンドウを表示します。

ステップ 4 [Proxy Gateway Certificate]ウィンドウで、現在のプロキシ ゲートウェイ証明書データを確認します（存在する場合）。

（注） [Expiration Date and Time]は、グリニッジ標準時（GMT）値で表示されます。証明書の有効期限の 2 ヵ月前に、コントローラの GUI にシステム通知が表示されます。

ステップ 5 プロキシ ゲートウェイ証明書を追加するには、自己署名証明書または CA 証明書を [Drag n' Drop a File Here]フィールドにドラッグ アンド ドロップします。

（注） このフィールドを使用してコントローラにインポートできるのは、PEM ファイル（公開キー暗号化標準ファイル形式）のみです。また、秘密キーは必要ではなく、この手順でコントローラにアップロードされません。

ステップ 6 [Save]ボタンをクリックします。

ステップ 7 [Proxy Gateway Certificate]ウィンドウを更新して、更新されたプロキシ ゲートウェイ証明書データを表示します。

[Proxy Gateway Certificate]ウィンドウに表示される情報が変更されて、新しい証明書の名前、発行元、および認証局が反映されます。

関連トピック

セキュリティおよびシスコ ネットワーク プラグ アンド プレイ，（15 ページ）

PKI 証明書の管理

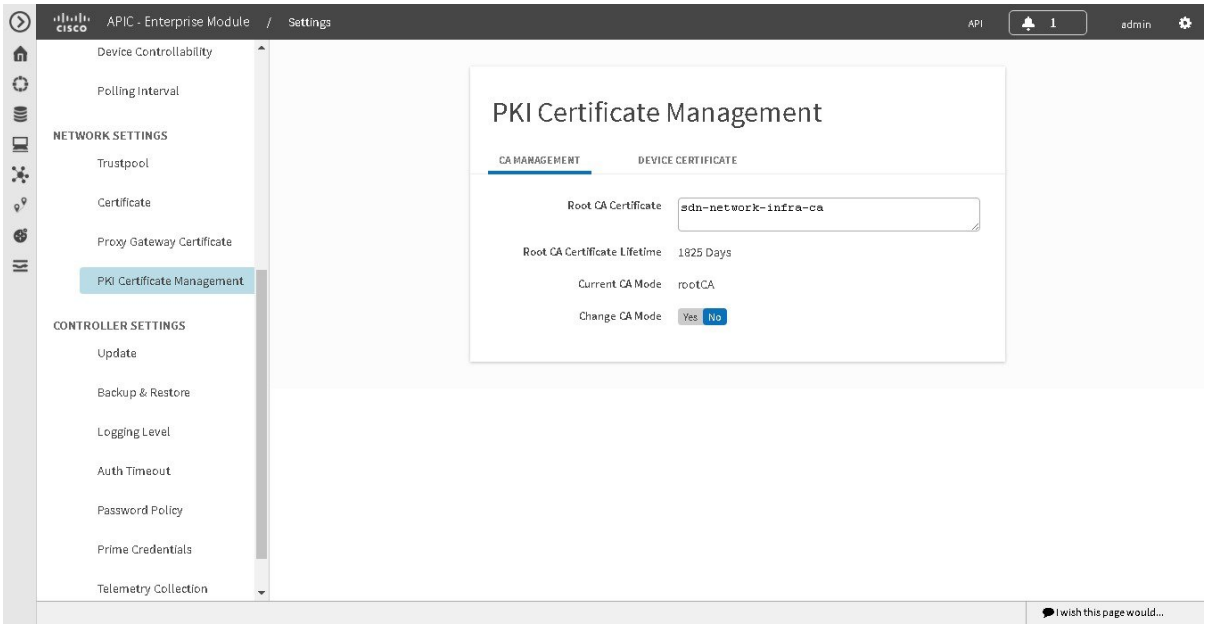
デバイス証明書のライフタイムの設定

Cisco APIC-EMでは、コントローラのプライベート（内部）CA によって管理およびモニタされるネットワーク デバイスの証明書のライフタイムをユーザが変更できます。証明書のライフタイムに対するコントローラのデフォルト値は 365 日です。コントローラの GUI を使用して証明書のライフタイム値を変更すると、それ以降にコントローラに証明書を要求したネットワーク デバイスには、このライフタイム値が割り当てられます。

（注） デバイス証明書のライフタイム値を CA 証明書のライフタイム値より大きくすることはできません。さらに、設定されたデバイスの証明書のライフタイムより CA 証明書のライフタイムの残り時間が短い場合、デバイスでは CA 証明書の残りのライフタイムと同じ値が証明書のライフタイムに使用されます。

デバイス証明書のライフタイムを変更するには、Cisco APIC-EMGUI の [PKI Certificate Management] ウィンドウを使用します。

図 *6*：*[PKI Certificate Management]* ウィンドウ



はじめる前に

Cisco APIC-EMが正常に導入され、動作している必要があります。

管理者（ROLE_ADMIN）権限、およびすべてのリソースへのアクセス権（RBACスコープを[ALL]に設定）またはグループ化するすべてのリソースを含むRBACスコープが必要です。たとえば、特定のリソースセットを含むグループを作成するには、これらのリソースへのアクセス権が必要です（グループ化するすべてのリソースをカスタムRBACスコープとして設定）。

Cisco APIC-EMを使用してタスクを実行するために必要なユーザ権限とRBACスコープについては、「Cisco APIC-EMの設定」の章の「ユーザ設定」を参照してください。

ステップ1 [Home]ウィンドウで、画面右上の[admin]または[Settings]アイコン（歯車）をクリックします。

ステップ2 ドロップダウンメニューの[Settings]リンクをクリックします。

ステップ3 [Settings]ナビゲーションウィンドウで、[PKI Certificate Management]をクリックして[PKI Certificate Management]ウィンドウを表示します。

ステップ4 [Device Certificate]タブをクリックします。

ステップ5 デバイス証明書とデバイス証明書の現在のライフタイムを確認します。

ステップ6 [Device Certificate Lifetime]フィールドに、新しい値（日数）を入力します。

ステップ7 [Apply]ボタンをクリックします。

次の作業

[PKI Certificate Management]ウィンドウを更新して、デバイス証明書の新しいライフタイム値を確認します。

関連トピック

デバイス PKI プレーン モード, （6 ページ）

PKI 証明書ロールをルートから下位へ変更する

Cisco APIC-EMでは、ユーザがデバイスPKI CAのロールをルートCAから下位CAに変更できます。

コントローラのプライベートCAをルートCAから下位CAに変更する場合は、次の点に注意してください。

- コントローラを下位CAとして機能させる場合は、ルートCA（Microsoft CAなど）がすでに存在し、コントローラを下位CAとして承認することが前提となります。
- 下位CAが完全に設定されない限り、コントローラは内部ルートCAとして機能し続けます。
- この手順の説明に従ってコントローラの証明書署名要求（CSR）ファイルを生成し、手動で外部ルートCAによって署名する必要があります。

（注） この間、コントローラは引き続き内部ルートCAとして機能します。

- 外部ルート CA によって CSR に署名したら、この手順の後半の説明に従い、GUI を使用してこの署名済みファイルをコントローラに再度インポートする必要があります。

  インポート後は、コントローラが下位 CA として初期化され、下位 CA の既存の機能がすべて提供されます。

- 内部ルート CA から下位 CA への切り替えは、自動的にはサポートされないため、内部ルート CA でデバイスが設定されていないことが前提となります。設定済みのデバイスが存在する場合は、下位CAに切り替える前に、ネットワーク管理者が手動で既存のデバイスID証明書を無効化する必要があります。

- 下位 CA のロールオーバー プロビジョニングは行われないことに注意してください。したがって、下位証明書には可能な限り長い証明書の有効期間（2 年以上）を選択することを推奨します。

- コントローラでは下位 CA 証明書の有効期限に関する警告は表示されません。

- GUI に表示される下位 CA 証明書の有効期間は、証明書自体から読み取られます。システム時刻と照合して計算されるわけではありません。したがって、有効期間が 1 年の証明書を今日インストールし、次の 7 月に GUI で確認しても、GUI 上では証明書の有効期間が 1 年として表示されます。

- 下位 CA 証明書に PEM 形式以外は使用できません。

- Cisco IOS XE の暗号 PKI インポートの制限により、サイズが 4 KB を超える PKCS バンドル（デバイス証明書、デバイス キー、および下位 CA 証明書で構成）をデバイスでインポートすることはできません。これが問題となるのは、Cisco APIC-EM のデバイス PKI CA を複数の X509 属性や長い X509 属性が定義された下位 CA 証明書を使用するサブ CA モードに変更することで、デバイス PKCS バンドルのサイズが 4 KB を超過する場合です。この問題を回避するには、最小限の属性を指定して発行した下位CA証明書を取得します。たとえば、CDP 配布および OCSP 設定は指定しないでください。

  次のコマンド出力では、ファイル サイズに影響する可能性がある下位 CA 証明書の内容例と、内容を最小限に抑える必要がある証明書のフィールドを示します。

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            2e:00:00:00:0e:28:d7:1f:24:a1:1e:ef:70:00:00:00:00:00:0e
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: DC=com, DC=apic-em, CN=apic-em-CA
        Validity
            Not Before: Oct 18 19:56:54 2016 GMT
            Not After : Oct 19 19:56:54 2016 GMT
        Subject: CN=sdn-network-infra-subca
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:cd:a7:65:a4:c4:64:e6:e0:6b:f2:39:c0:a2:3b:
                    <snip>
                    85:a3:44:d1:a2:b3:b1:f5:ff:28:e4:12:41:d3:5f:
                    bf:e9
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                D2:DD:FA:E4:A5:6A:3C:81:29:51:B2:17:ED:82:CE:AA:AD:91:C5:1D
            X509v3 Authority Key Identifier:
```

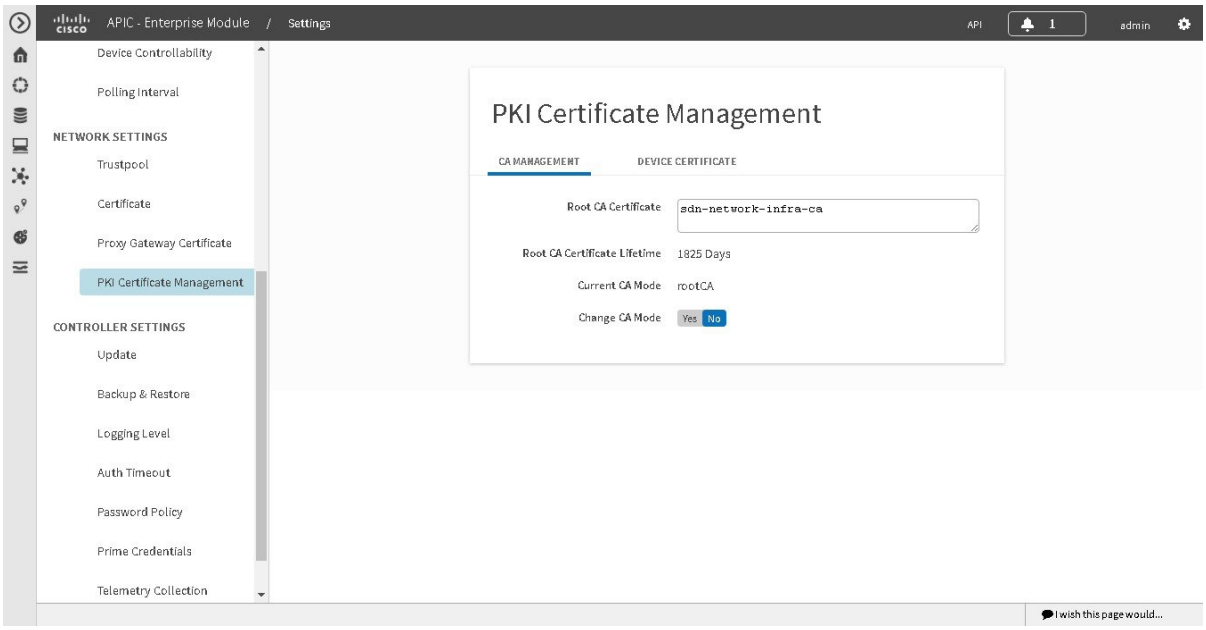
```
            keyid:62:6F:C7:83:42:82:5F:54:51:2B:76:B2:B7:F5:06:2C:76:59:7F:F8

        X509v3 Basic Constraints: critical
            CA:TRUE
        X509v3 Key Usage: critical
            Digital Signature, Certificate Sign, CRL Sign
        1.3.6.1.4.1.311.21.7:
            0-.%+.....7.....#...I......^...Q...._...S..d...
Signature Algorithm: sha256WithRSAEncryption
     18:ce:5b:90:6b:1d:5b:b4:df:fa:d3:8e:80:51:6f:46:0d:19:
```

- 下位 CA は上位の CA と連携しないため、上位のレベルでの証明書の失効を認識しません。そのため、下位 CA からネットワーク デバイスに証明書失効に関する情報が伝えられることはありません。下位 CA にこの情報がないため、すべてのネットワーク デバイスは CDP 送信元としてのみ下位 CA を使用します。

Cisco APIC-EMGUI の [PKI Certificate Management] ウィンドウを使用して、コントローラのプライベート（内部）CA のロールをルート CA から下位 CA に変更します。

図 *7*：*[PKI Certificate Management]* ウィンドウ



はじめる前に

Cisco APIC-EMが正常に導入され、動作している必要があります。

管理者（ROLE_ADMIN）権限、およびすべてのリソースへのアクセス権（RBACスコープを[ALL]に設定）またはグループ化するすべてのリソースを含む RBAC スコープが必要です。たとえば、特定のリソース セットを含むグループを作成するには、これらのリソースへのアクセス権が必要です（グループ化するすべてのリソースをカスタム RBAC スコープとして設定）。

Cisco APIC-EM を使用してタスクを実行するために必要なユーザ権限と RBAC スコープについては、「Cisco APIC-EM の設定」の章の「ユーザ設定」を参照してください。

コントローラのプライベート（内部）PKI 証明書を下位に置くルート CA 証明書のコピーが必要です。

ステップ 1 [Home]ウィンドウで、画面右上の [admin] または [Settings] アイコン（歯車）をクリックします。

ステップ 2 ドロップダウン メニューの [Settings]リンクをクリックします。

ステップ 3 [Settings]ナビゲーション ウィンドウで、[PKI Certificate Management] をクリックして [PKI Certificate Management] ウィンドウを表示します。

ステップ 4 [CA Management]タブをクリックします。

ステップ 5 GUI で既存のルートまたは下位 CA 証明書の設定情報を確認します。

Root CA Certificate	現在のルート CA 証明書（内部または外部ルート CA 証明書）を表示します。
Root CA Certificate Lifetime	現在のルート CA 証明書の現在のライフタイム値（日数）を表示します。
Current CA Mode	現在の CA モード（ルート CA または下位 CA）を表示します。
Change to Sub CA mode	ルート CA から下位 CA に変更する場合に使用するボタンです。

ステップ 6 [CA Management]タブで、[Change to Sub CA mode] の [Yes] をクリックします。

ステップ 7 [CA Management]タブで [Next] をクリックします。

ステップ 8 表示される [Root CA to Sub CA]の警告内容を確認します。

- ルート CA から下位 CA に変更するプロセスは元に戻すことができません。
- ルート CA モードで登録された、または証明書が発行されたネットワーク デバイスがないことを確認する必要があります。誤ってルート CA モードで登録されたネットワーク デバイスがある場合は、ルート CA から下位 CA に変更する前に取り消す必要があります。
- ネットワーク デバイスは、この下位 CA の設定プロセスが完了してからオンラインにする必要があります。

ステップ 9 [OK]をクリックして続行します。
[PKI Certificate Management]ウィンドウの表示が変わり、[Import External Root CA Certificate] フィールドが表示されます。

ステップ 10 [Import External Root CA Certificate]フィールドにルート CA 証明書をドラッグ アンド ドロップして、[Upload] をクリックします。
ルート CA 証明書がコントローラにアップロードされ、証明書署名要求（CSR）の生成時に使用されます。

アップロードプロセスが完了すると、「Certificate Uploaded Successfully」メッセージが表示されます。

ステップ 11 アップロード プロセスの完了後に成功メッセージが表示されたら、[Next]をクリックして続行します。
コントローラによって CSR が生成されて表示されます。

ステップ 12 コントローラによって生成された証明書署名要求（CSR）を GUI で確認し、次のいずれかの操作を実行します。

- CSR ファイルのローカル コピーをダウンロードするには、[Download]リンクをクリックします。

  この CSR ファイルを電子メールに添付してルート CA に送信できます。

- CSR ファイルのコンテンツをコピーするには、[Copy to the Clipboard]リンクをクリックします。

  この CSR コンテンツを電子メールまたは電子メールの添付ファイルに貼り付けてルート CA に送信できます。

ステップ 13 ルート CA に CSR ファイルを送信します。
CSR ファイルはルート CA に送信する必要があります。その後、コントローラにインポートする必要がある下位 CA ファイルがルート CA から返されます。

ステップ 14 ルート CA から下位 CA ファイルを受信したら、もう一度コントローラの GUI にアクセスし、[PKI Certificate Management]ウィンドウに戻ります。

ステップ 15 [CA Management]タブをクリックします。

ステップ 16 [CA Management]タブで [Change CA mode] の [Yes] ボタンをクリックします。
[Yes]をクリックすると、GUI ビューに CSR が表示されます。

ステップ 17 CSR が表示された GUI ビューで [Next]をクリックします。
[PKI Certificate Management]ウィンドウの表示が変わり、[Import Sub CA Certificate] フィールドが表示されます。

ステップ 18 [Import Sub CA Certificate]フィールドに下位 CA 証明書をドラッグ アンド ドロップして、[Apply] をクリックします。
下位 CA 証明書がコントローラにアップロードされます。

アップロードが完了すると、GUI ウィンドウが変化して [CA Management]タブに下位 CA モードが表示されます。

ステップ 19 [CA Management]タブのフィールドを確認します。

Sub CA Certificate	現在の下位 CA 証明書を表示します。
External Root CA Certificate	ルート CA 証明書を表示します。
Sub CA Certificate Lifetime	下位 CA 証明書のライフタイム値（日数）を表示します。
Current CA Mode	[SubCA] モードと表示されます。

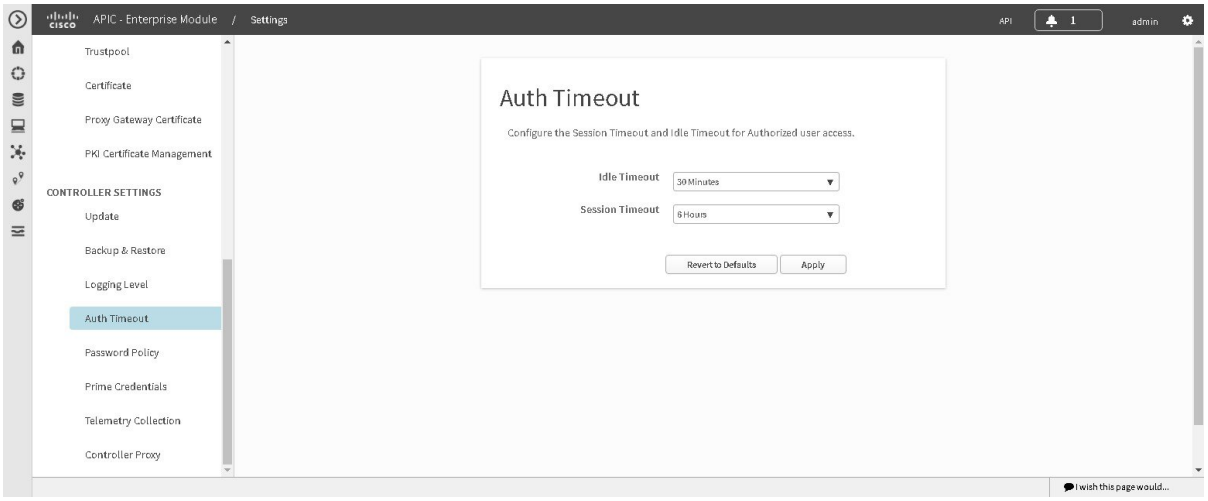
関連トピック

デバイス PKI プレーン モード, （6 ページ）

認証タイムアウトの設定

Cisco APIC-EMの GUI の [Authentication Timeout] ウィンドウを使用して、ユーザがクレデンシャル（ユーザ名とパスワード）を使ってコントローラに再びログインする必要がある認証タイムアウトを設定できます。

図 *8*：*[Authentication Timeout]* ウィンドウ



次のような認証タイムアウト値を設定できます。

- Idle timeout：Cisco APIC-EMが非アクティブなために、コントローラが再認証（適切なクレデンシャルを使用して再度ログインする）を要求するまでの間隔を設定できます。アイドルタイムアウトはAPIベースです。つまりアイドルタイムアウトとはコントローラがAPIの使用中にアイドル状態になる時間のことであり、GUIのマウスクリックまたはドラッグは関係ありません。
- Session timeout：コントローラが再認証（適切なクレデンシャルを使用して再度ログインする）を要求するまでの間隔を設定できます。これは強制的な再認証です。

（注） セッションがアイドル タイムアウトになる約 2 ～ 3 分前に、ポップアップ警告を GUI に表示して、セッションがアイドル タイムアウト間近であることを示し、現在のセッションを継続するかどうかを確認します。警告と約 2 ～ 3 分以内に発生するセッションのアイドル タイムアウトを無視するには [Cancel]をクリックします。さらに 30 分のセッションを続けるには、[OK]をクリックします。

はじめる前に

Cisco APIC-EMが正常に導入され、動作している必要があります。

管理者（ROLE_ADMIN）権限、およびすべてのリソースへのアクセス権（RBACスコープを[ALL]に設定）またはグループ化するすべてのリソースを含む RBAC スコープが必要です。たとえば、特定のリソース セットを含むグループを作成するには、これらのリソースへのアクセス権が必要です（グループ化するすべてのリソースをカスタム RBAC スコープとして設定）。

Cisco APIC-EM を使用してタスクを実行するために必要なユーザ権限と RBAC スコープについては、「Cisco APIC-EM の設定」の章の「ユーザ設定」を参照してください。

ステップ 1 [Home]ウィンドウで、画面右上の [admin] または [Settings] アイコン（歯車）をクリックします。

ステップ 2 ドロップダウン メニューの [Settings]リンクをクリックします。

ステップ 3 [Settings]ナビゲーション ウィンドウで [Authentication Timeout] をクリックして、[Authentication Timeout] ウィンドウを表示します。

ステップ 4 （任意）[Idle timeout]ドロップダウン メニューを使用して、アイドル タイムアウトの値を設定します。
アイドル タイムアウト値を最大 1 時間まで 5 分単位で設定できます。デフォルト値は 30 分です。

ステップ 5 （任意）[Session Timeout]ドロップダウン メニューを使用して、セッション タイムアウトの値を設定します。
セッション タイムアウト値を最大 24 時間まで 30 分単位で設定できます。デフォルト値は 6 時間です。

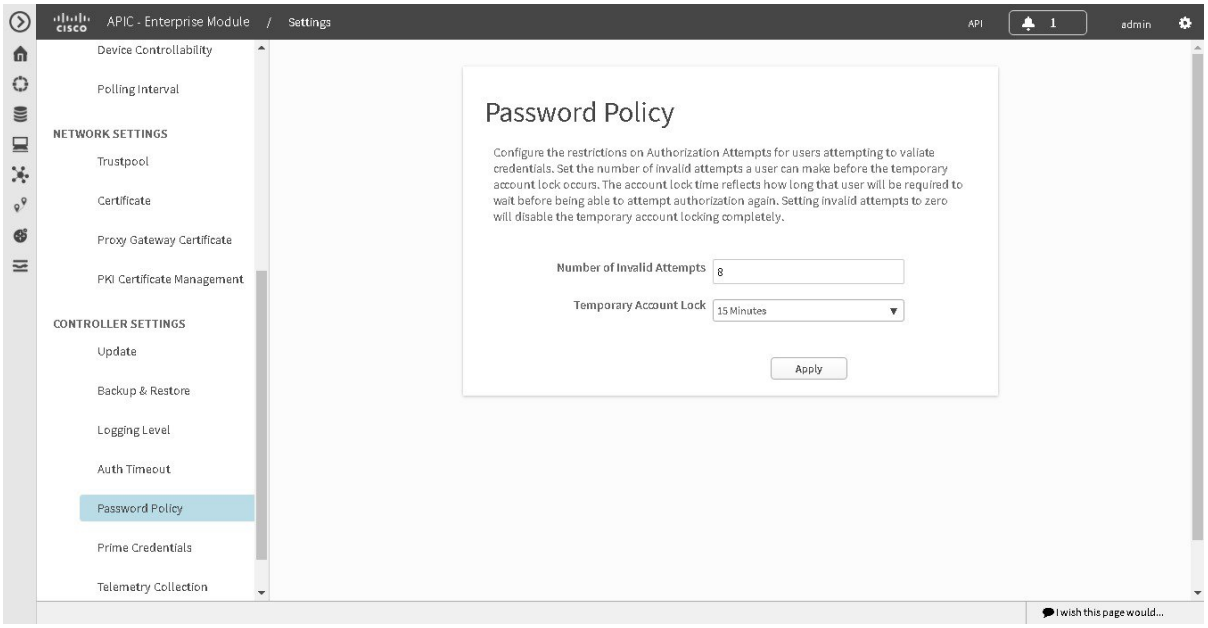
ステップ 6 [Apply]ボタンをクリックして、コントローラに設定を適用します。
コントローラに認証タイムアウトのデフォルト値を復元するには、[Revert to Defaults]ボタンをクリックします。

パスワード ポリシーの設定

管理者は、Cisco APIC-EMへの無効なユーザ ログインの連続試行回数を制御できます。管理者が設定したしきい値を超えると、そのユーザのアカウントがロックされ、アクセスは拒否されます。また、管理者はユーザ アカウントがロックされる時間も設定できます。設定された時間が経過するまで、ユーザ アカウントはロックされたままになります。

[Password Policy]ウィンドウを使用して、Cisco APIC-EM のこれらのコントローラ アクセス パラメータを設定します。

図 *9*：*[Password Policy]* ウィンドウ



次のパスワード ポリシー機能がサポートされています。

- 管理者は、コントローラへの無効なユーザ ログインの連続試行回数を設定できます。無効なユーザ ログインの連続試行回数は 0 ～ 10 回に設定できます。デフォルト値は 8 回です。無効な試行回数を 0 に設定すると、無効なパスワードを試行したユーザをロックする機能がディセーブルになります。
- 管理者はユーザ アカウントがロックされる時間を設定できます。ユーザ アカウントの許容ロック時間の範囲は 1 ～ 3600 秒で、900 秒がデフォルト値です。
- 無効なログインの連続試行回数が原因でユーザ アカウントがロックされると、設定済みのロックアウト時間が経過するまでは、正しいクレデンシャルを入力してもログインに失敗します。
- 管理者は、ユーザ アカウントをいつでもロック解除できます。

  導入に少なくとも 2 つの管理者アカウントを作成することを推奨します。2 つの管理者アカウントがあることで、一方のアカウントが何らかの理由でロックされた場合でも、もう一方のアカウントを使用してロックされたアカウントをロック解除できます。

（注） ユーザ アカウントをロック解除する方法については、『*Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide*』の第 4 章「*Managing Users and Roles*」を参照してください。

- ロックされたユーザアカウントは、設定されたロックアウト時間が経過するとロック解除されます。
- ユーザ アカウントは永続的にロックできません。ただし、アクセスを永続的に拒否する場合、管理者はアカウントを削除できます。

はじめる前に

Cisco APIC-EMが正常に導入され、動作している必要があります。

管理者（ROLE_ADMIN）権限、およびすべてのリソースへのアクセス権（RBACスコープを[ALL]に設定）またはグループ化するすべてのリソースを含むRBAC スコープが必要です。たとえば、特定のリソース セットを含むグループを作成するには、これらのリソースへのアクセス権が必要です（グループ化するすべてのリソースをカスタム RBAC スコープとして設定）。

Cisco APIC-EM を使用してタスクを実行するために必要なユーザ権限と RBAC スコープについては、「Cisco APIC-EM の設定」の章の「ユーザ設定」を参照してください。

ステップ 1 [Home]ウィンドウで、画面右上の [admin] または [Settings] アイコン（歯車）をクリックします。

ステップ 2 ドロップダウン メニューの [Settings]リンクをクリックします。

ステップ 3 [Settings]ナビゲーション ウィンドウで、[Password Policy] をクリックして [Password Policy] ウィンドウを表示します。

ステップ 4 （任意）[Number of Invalid Attempts]ドロップダウン メニューから無効なパスワードの許容される連続試行回数を選択して設定します。

ステップ 5 （任意）[Temporary Account Lock]ドロップダウン メニューからユーザ アカウントをロックする期間を選択して設定します。

ステップ 6 [Apply]ボタンをクリックして、コントローラに設定を適用します。

関連トピック

パスワード要件, （21 ページ）