証明書の管理

- 公開キーインフラストラクチャ管理について（GUI） （1 ページ）
- PKI トラストポイントの認証と登録（GUI） （1 ページ）
- 認証局サーバーの追加（GUI） （3 ページ）
- PKI トラストポイントの RSA または EC キーの追加（GUI） （3 ページ）
- 証明書の追加と管理 （3 ページ）

公開キーインフラストラクチャ管理について（GUI）

[Public Key Infrastructure (PKI) Management] ページには、次のタブが表示されます。

[Trustpoints] タブ：新しいトラストポイントを追加、作成、または登録するために使用します。このページには、コントローラに設定されている現在のトラストポイントとトラストポイントのその他の詳細も表示されます。トラストポイントがいずれかの機能に使用されているかどうかも確認できます。たとえば、Webadmin や AP 接続（ワイヤレス管理インターフェイス）などの機能。

[CA Server] タブ：コントローラの認証局（CA）サーバー機能を有効または無効にするために使用します。コントローラで自己署名証明書（SSC）を生成するためには、CA サーバー機能を有効にする必要があります。

[Key Pair Generation] タブ：キーペアを生成するために使用します。

[Certificate Management] タブ：証明書の生成と管理、およびコントローラ上でのすべての証明書関連操作の実行に使用します。

PKI トラストポイントの認証と登録（GUI）

手順

ステップ 1 **[Configuration]** > **[Security]** > **[PKI Management]** を選択します。

ステップ 2 [PKI Management] ウィンドウで、[Trustpoints] タブをクリックします。

ステップ 3 [Add Trustpoint] ダイアログボックスで、次の情報を入力します。

a) [Label] フィールドに、RSA キーラベルを入力します。
b) [Enrollment URL] フィールドに、登録 URL を入力します。
c) [Authenticate] チェックボックスをオンにして、登録 URL の公開証明書を認証します。
d) [Subject Name] セクションで、[Country Code]、[State]、[Location]、[Organisation]、[Domain Name]、および [Email Address] を入力します。
e) [Key Generated] チェック ボックスをオンにして、使用可能な RSA キーペアを表示します。[Available RSA Keypairs] ドロップダウンリストからオプションを選択します。
f) [Enroll Trustpoint] チェックボックスをオンにします。
g) [Password] フィールドにパスワードを入力します。
h) [Re-Enter Password] フィールドで、パスワードを確認します。
i) [Apply to Device] をクリックします。

新しいトラストポイントがトラストポイント名リストに追加されます。

AP 自己署名証明書の生成（GUI）

（注） この項は、仮想コントローラ（クラウド向け Cisco Catalyst 9800-CL ワイヤレスコントローラ）にのみ有効であり、アプライアンスベースのコントローラ（Cisco Catalyst 9800-40 ワイヤレスコントローラ、Cisco Catalyst 9800-80 ワイヤレスコントローラ、Cisco Catalyst 9800-L ワイヤレスコントローラ（銅線アップリンク）、および Cisco Catalyst 9800-L ワイヤレスコントローラ（光ファイバアップリンク））には適用されません。

手順

ステップ 1 **[Configuration]** > **[Security]** > **[PKI Management]** を選択します。
ステップ 2 [AP SSC Trustpoint] 領域で、[Generate] をクリックして AP SSC トラストポイントを生成します。
ステップ 3 [RSA Key-Size] ドロップダウンリストから、キー サイズを選択します。
ステップ 4 [Signature Algorithm] ドロップダウンリストから、オプションを選択します。
ステップ 5 [Password Type] ドロップダウンリストから、パスワードタイプを選択します。
ステップ 6 [Password] フィールドに、パスワードを入力します。有効な範囲は 8 ～ 32 文字です。
ステップ 7 [Apply to Device] をクリックします。

認証局サーバーの追加（GUI）

手順

ステップ 1 **[Configuration]** > **[Security]** > **[PKI Management]** を選択します。

ステップ 2 [PKI Management] ウィンドウで、[CA Server] タブをクリックします。

ステップ 3 [CA Server] セクションで、[Shutdown Status] トグルボタンをクリックして、ステータスを有効にします。シャットダウンステータスとして [Enabled] を選択した場合は、パスワードを入力して確認する必要があります。

ステップ 4 シャットダウンステータスとして [Disabled] を選択した場合は、[Country Code]、[State]、[Location]、[Organisation]、[Domain Name]、および [Email Address] を入力する必要があります。

ステップ 5 [Apply] をクリックして CA サーバーを追加します。

ステップ 6 CA サーバーを削除するには、[Remove CA Server] をクリックします。

PKIトラストポイントのRSAまたはECキーの追加（GUI）

手順

ステップ 1 [Configuration] > [Security] > [PKI Management] を選択します。

ステップ 2 [PKI Management] ウィンドウで、[Key Pair Generation] タブをクリックします。

ステップ 3 [Key Pair Generation] セクションで、[Add] をクリックします。

ステップ 4 表示されるダイアログボックスで、次の情報を指定します。

a) [Key Name] フィールドに、キーの名前を入力します。

b) [Key Type] オプションで、[RSA Key] または [EC Key] を選択します。

c) [Modulus Size] フィールドに、RSA キーまたは EC キーのモジュラス値を入力します。RSA キーのデフォルトのモジュラスサイズは 4096 で、EC キーのデフォルト値は 521 です。

d) キーをエクスポートするには、[Key Exportable] チェックボックスをオンにします。デフォルトでは、このチェックボックスはオンになっています。

e) [Generate] をクリックします。

証明書の追加と管理

証明書を追加および管理するには、次のいずれかの方法を使用します。

方法 1

手順

ステップ 1 [Configuration] > [Security] > [PKI Management] > [Add Certificate] を選択します。

ステップ 2 [Generate Certificate Signing Request] をクリックします。

a) [Certificate Name] フィールドに証明書名を入力します。

b) [Key Name] ドロップダウンリストから、RSA キーペアを選択します（[Key Pair Generation] タブの下にあるプラス [+] アイコンをクリックして、新しい RSA キーペアを作成します）。

c) [Country Code]、[Location]、[Organisation]、[State]、[Organizational Unit]、および [Domain Name] フィールドに値を入力します。

d) [Generate] をクリックします。
生成された証明書署名要求（CSR）が右側に表示されます。[Copy] をクリックして、ローカルコピーをコピーして保存します。[Save to Device] をクリックして、生成された CSR を /bootflash/csr ディレクトリに保存します。

ステップ 3 [Authenticate Root CA] をクリックします。

a) [Trustpoint] ドロップダウンリストから、ステップ 2 で生成されたトラストポイントラベル、または認証する他のトラストポイントラベルを選択します。

b) [Root CA Certificate (.pem)] フィールドに、CA から受け取った証明書をコピーして貼り付けます。

（注） デバイス証明書の発行元 CA の PEM Base64 証明書をコピーして貼り付けてください。

c) [認証（Authenticate）] をクリックします。

ステップ 4 [Import Device Certificate] をクリックします。

a) [Trustpoint] ドロップダウンリストから、ステップ 2 で生成されたトラストポイントラベル、または認証する他のトラストポイントラベルを選択します。

b) [Signed Certificate (.pem)] フィールドに、CA から受け取った署名証明書をコピーして貼り付けます。

c) [Import] をクリックします。

これでデバイス証明書のインポートプロセスが完了し、証明書を機能に割り当てることができます。

方法 2

手順

[Import PKCS12 Certificate] をクリックします。

（注） さまざまな転送タイプを使用して、証明書チェーン全体をPKCS12形式でインポートできます。

a) [Transport Type] ドロップダウンリストから、[FTP]、[SFTP]、[TFTP]、[SCP]、または [Desktop (HTTPS)] のいずれかを選択します。

[FTP]、[SFTP]、および [SCP] の場合、[Server IP Address (IPv4/IPv6)]、[Username]、[Password]、[Certificate File Path]、[Certificate Destination File Name]、および [Certificate Password] フィールドに値を入力します。

[TFTP] の場合は、[Server IP Address (IPv4/IPv6)]、[Certificate File Path]、[Certificate Destination File Name]、および [Certificate Password] フィールドに値を入力します。

[Desktop (HTTPS)] の場合、[Source File Path] および [Certificate Password] フィールドに値を入力します。

b) **[インポート (Import)]** をクリックします。