Public Key Infrastructure Management

About PKI management (GUI)

A public key infrastructure (PKI) management is a network application tool that

- enables graphical configuration of PKI components using GUI.
- provides tabs for configuring and monitoring trustpoints, certificate authorities, keys, and certificates,
- allows administrators to generate, enroll, and manage cryptographic credentials for secure communications, and

Feature history

Feature Name	Release	Description
Enhanced Certificate Management Through GUI	Cisco IOS XE 17.3.1	The PKI Management page now includes tabs for Trustpoints, CA Server, Key Pair Generation, and Certificate Management operations.

Tabs for PKI management in GUI

- **Trustpoints tab:** Add, create, or enroll a new trustpoint, view the current trustpoints and their usage.
- **CA Server tab**: Enable or disable Certificate Authority (CA) server functionality. This is required for generating a self-signed certificate (SSC).
- **Key Pair Generation tab**: Generate key pairs.
- **Certificate Management tab**: Generate and manage certificates, and perform all certificate-related operations.

Restriction: CSR generation on the GUI may hang indefinitely

The controller's GUI-based certificate management feature relies on Embedded Event Manager (EEM) scripts. If TACACS command authorization is enabled, the user is authenticated on the GUI but the controller does not pass the user details to the EEM environment. As a result, the user is not authorized, and the user cannot enter the configuration mode using the EEM scripts.

The restriction applies if you have this command-authorization configuration:

```
aaa authorization commands 1 MethodName group GroupName local if-authenticated
aaa authorization commands 15 MethodName group GroupName local if-authenticated
ip http authentication aaa command-authorization 1 MethodName
ip http authentication aaa command-authorization 15 MethodName
```

To resolve this issue, enter this command before you generate the Certificate Signing Request (CSR) using the GUI. For proper authorization, configure the desired username.

```
event manager session cli username <username>
```

After you issue the CSR using the GUI, remove this configuration.

The restriction does not affect CSR generation through the CLI.

Configuration Tasks

Authenticate and enroll a Public Key Infrastructure (PKI) trustpoint (GUI)

Use this procedure to add and authenticate a Public Key Infrastructure (PKI) trustpoint to enable certificate-based security for your device.

Before you begin

Obtain the enrollment URL and certificate authority information from your network administrator.

Procedure

Step 1 Choose **Configuration** > **Security** > **Public Key Infrastructure (PKI) Management**.

Step 2 In the **Public Key Infrastructure (PKI) Management** window, click the **Trustpoints** tab.

Step 3 In the **Add Trustpoint** dialog box, provide this information:

a) In the **Label** field, enter the RSA key label.
b) In the **Enrollment URL** field, enter the enrollment URL.
c) Check the **Authenticate** check box to authenticate the Public Certificate from the enrollment URL.
d) In the **Subject Name** section, enter the **Country Code**, **State**, **Location**, **Organization**, **Domain Name**, and **Email Address**.
e) Check the **Key Generated** check box to view the available RSA keypairs. Choose an option from the **Available RSA Keypairs** drop-down list.
f) Check the **Enroll Trustpoint** check box.
g) In the **Password** field, enter the password.
h) In the **Re-Enter Password** field, confirm the password.
i) Click **Apply to Device**.

The new trustpoint is added to the trustpoint name list.

The new trustpoint is now listed in the trustpoint name list and is ready for use.

What to do next

After enrolling the trustpoint, configure it for use with your security policies or certificate-based authentication features.

Generate an AP self-signed certificate (GUI)

Create a self-signed certificate (SSC) for APs on a virtual controller using the graphical interface.

Use this procedure only for virtual controllers.

- Cisco Catalyst 9800-CL Wireless Controller for Cloud
- Cisco Catalyst 9800-40 Wireless Controller
- Cisco Catalyst 9800-80 Wireless Controller
- Cisco Catalyst 9800-L Wireless Controller (Copper uplink)
- Cisco Catalyst 9800-L Wireless Controller (Fiber uplink)

Procedure

Step 1 Choose **Configuration** > **Security** > **PKI Management**.
Step 2 In the **AP SSC Trustpoint** area, click **Generate** to generate an AP SSC trustpoint.
Step 3 From the **RSA Key-Size** drop-down list, choose a key size.
Step 4 From the **Signature Algorithm** drop-down list, choose an option.
Step 5 From the **Password Type** drop-down list, choose a password type.
Step 6 In the **Password** field, enter a password. The valid range is between 8 and 32 characters.
Step 7 Click **Apply to Device**.

The controller creates and applies a new self-signed certificate for the AP.

Add the CA server (GUI)

Register a new certificate authority (CA) server in the system using the graphical user interface.

Perform this task when you need to establish a new certificate authority for PKI management.

Procedure

Step 1 Choose **Configuration** > **Security** > **PKI Management**.

Step 2 In the **PKI Management** window, click the **CA Server** tab.

Step 3 In the **CA Server** section, click the **Shutdown Status** to enable the status. If you choose the shutdown status as **Enabled**, enter and confirm the password.

Step 4 If you choose the shutdown status as **Disabled**, you must enter the **Country Code**, **State**, **Location**, **Organization**, **Domain Name**, and **Email Address**.

Step 5 Click **Apply** to add the CA server.

Step 6 Click **Remove CA Server** to delete the CA server.

The certificate authority server is added and configured as specified.

Add an RSA or EC Key for PKI trustpoint (GUI)

To enable certificate-based authentication, add an RSA or EC key to a PKI trustpoint.

Procedure

Step 1 Choose **Configuration > Security** > **PKI Management**.

Step 2 In the **PKI Management** window, click the **Key Pair Generation** tab.

Step 3 In the **Key Pair Generation** section, click **Add**.

Step 4 In the dialog box that is displayed, provide this information:

Note
To allow Japanese characters in **Key Name** field, ensure that the line vty configuration includes "exec-character-bits 8".

a) **Note**
To allow Japanese characters in **Key Name** field, ensure that the line vty configuration includes "exec-character-bits 8".

In the **Key Name** field, enter the key name.

b) In the **Key Type** options, select either **RSA Key** or **EC Key**.

c) In the **Modulus Size** field, enter the modulus value for the RSA key or the EC key. The default modulus size for the RSA key is 4096 and the default value for the EC key is 521.

d) Check the **Key Exportable** check box to export the key. By default, this is checked.

e) Click **Generate**.

A new RSA or EC key is created for the PKI trustpoint and is ready for use in certificate operations.

Add and manage certificates

To add and manage certificates, use one of these methods.

Generate and import a certificate signing request (CSR)

Secure the system by adding and managing device certificates.

Perform this task when onboarding a new device, renewing expiring certificates, or updating trust relationships.

Before you begin

- When configuring a password for the .pfx file, avoid using these ASCII characters: "*, ^, (), [], \, ", and +". Using these ASCII characters results in a configuration error and prevents the certificate from being imported to the controller.
- Ensure you have the required certificate files and CA information.

Before you begin

You can add and manage certificates using either of the following methods:

Procedure

Step 1 Choose **Configuration** > **Security** > **PKI Management** > **Add Certificate**.

Step 2 Click **Generate Certificate Signing Request**.

a) In the **Certificate Name** field, enter the certificate name.
b) From the **Key Name** drop-down list, choose an RSA key pair. (Click the plus (+) icon under the **Key Pair Generation** tab to create new RSA key pairs.).
c) Enter values in the **Country Code**, **Location**, **Organization**, **State**, **Organizational Unit**, and the **Domain Name** fields.
d) Click **Generate**.
The generated Certificate Signing Request (CSR) is displayed on the right. Click **Copy** to copy and save a local copy. Click **Save to Device** to save the generated CSR to the /bootflash/csr directory.

Note
If an IP address is used on the Domain Name field the controller creates the CSR without a Subject Alternative Name (SAN), since the IP address is not supported as an attribute in the SAN field of the CSR when the CSR is generated from the controller.

Step 3 Click **Authenticate Root CA**.

a) From the **Trustpoint** drop-down list, choose the trustpoint label generated in Step 2, or any other trustpoint label that you want to authenticate.
b) In the **Root CA Certificate (.pem)** field, copy and paste the certificate that you have received from the CA.

Note
Ensure that you copy and paste the PEM Base64 certificate of the issuing CA of the device certificate.

c) Click **Authenticate**.

Step 4 Click **Import Device Certificate**.

a) From the **Trustpoint** drop-down list, choose the trustpoint label that was generated in Step 2, or any other trustpoint label that you want to authenticate.
b) In the **Signed Certificate (.pem)** field, copy and paste the signed certificate that you received, from your CA.
c) Click **Import**.

This completes the device certificate import process and the certificate can now be assigned to features.

Import a PKCS12 certificate

Import a PKCS12 certificate into the system to enable secure authentication and encryption for network communications.

Use this task when you need to install a PKCS12 certificate file for system, server, or application authentication.

The certificate can be located on any of these sources: FTP, SFTP, TFTP, SCP, or Desktop (HTTPS).

Before you begin

Obtain the PKCS12 certificate file and its password.

Procedure

Step 1 Click **Import PKCS12 Certificate**.

Step 2 From the **Transport Type** drop-down list, choose either **FTP**, **SFTP**, **TFTP**, **SCP**, or **Desktop (HTTPS)**.

Transport Type	Action
For **FTP**, **SFTP**, and **SCP**	enter values in the **Server IP Address (IPv4/IPv6)**, **Username**, **Password**, **Certificate File Path**, **Certificate Destination File Name**, and **Certificate Password** fields.
For **TFTP**	enter values in the **Server IP Address (IPv4/IPv6)**, **Certificate File Path**, **Certificate Destination File Name**, and **Certificate Password** fields.
For **Desktop (HTTPS)**	enter values in the **Source File Path** and **Certificate Password** fields.

Step 3 Click **Import**.

The system imports the PKCS12 certificate. You see a confirmation message when the process completes successfully.