Certificate Management

About Public Key Infrastructure Management (GUI)

The Public Key Infrastructure (PKI) Management page displays the following tabs:

Trustpoints tab: Used to add, create or enroll a new trustpoint. This page also displays the current trustpoints configured on the controller and other details of the trustpoint. You can also view if the trustpoint is in use for any of the features. For example, Webadmin or AP join (Wireless Management Interface), and others.

CA Server tab: Used to enable or disable the Certificate Authority (CA) server functionality on the controller. The CA server functionality should be enabled for the controller to generate a Self Signed Certificate (SSC).

Key Pair Generation tab: Used to generate key pairs.

Certificate Management tab: Used to generate and manage certificates, and perform all certificate related operations, on the controller.

Authenticating and Enrolling a PKI Trustpoint (GUI)

Procedure

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

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

Step 3 In the **Add Trustpoint** dialog box, provide the following 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**, **Organisation**, **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.

Generating an AP Self-Signed Certificate (GUI)

Note This section is valid only for virtual controllers (Cisco Catalyst 9800-CL Wireless Controller for Cloud) and not applicable for appliance based controllers (Cisco Catalyst 9800-40 Wireless Controller, Cisco Catalyst 9800-80 Wireless Controller, Cisco Catalyst 9800-L Wireless Controller (Copper Uplink), and 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**.

Adding the Certificate Authority Server (GUI)

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** toggle button, to enable the status. If you choose the shutdown status as **Enabled**, you must enter the password and confirm the same.
Step 4 If you choose the shutdown status as **Disabled**, you must enter the **Country Code**, **State**, **Location**, **Organisation**, **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.

Adding an RSA or EC Key for PKI Trustpoint (GUI)

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 the following information:

a) 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**.

Adding and Managing Certificates

To add and manage certificates, use one of the following methods:

Note While configuring a password for the .pfx file, do not use the following ASCII characters: "*, ^, (), [], \, ", and +"

Using these ASCII characters results in error with bad configuration and does not import the certificate to the controller.

Method 1

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 the **Country Code**, **Location**, **Organisation**, **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.

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.

Method 2

Procedure

Click **Import PKCS12 Certificate** .

Note You can import an entire certificate chain in the PKCS12 format using different transport types.

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

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.

b) Click **Import**.
