Workflow to Configure a Trustpoint for a Third-party Certificate on Catalyst 9800

Third-party certificates on the Catalyst 9800 controller can be used for any of the use cases discussed above. Creating a trustpoint and the RSA key pair starts the process of requesting a certificate from the CA server. The name of the trustpoint, the public RSA key pair of the host and additional details like the subject name, domain name are bundled in the certificate request, thereby binding them together. Catalyst 9800 supports EC key pair as well, but this document focuses on the RSA key pair only.

There are many ways to enroll your trustpoint and receive a certificate from the CA. Depending on the configuration, you can:

- Enroll the Trustpoint automatically.

  The Catalyst 9800 controller supports automatic certificate enrollment protocols like Simple Certificate Enrollment Protocol (SCEP) and Enrollment over Secure Tunnel (EST) to forward and receive certificate requests generated on the controller to the CA.

- Enroll the Trustpoint manually.

  The Catalyst 9800 controller supports manual enrollment that uses the PKCS#12 Certificate Signing Request (CSR) mechanism to issue certificates for the controller. Subsequent to the CSR request, the signed certificate for the controller, together with the CA root certificate, are uploaded to the controller. Note that it is also possible to use OpenSSL or any other utility to generate the keys and the CSR.

After the request is approved, the CA signs the request with its private key and returns the completed certificate to the controller. The controller writes the certificate to a storage area such as NVRAM and uses it to communicate with other devices.

Configuration is possible both from the controller's CLI or from the controller's WebUI. You can use the method that suits you better.

What to do next

Configuration Using the Catalyst 9800 CLI, on page 2	Step 1	Create RSA Key
	Step 2	Create Trustpoint
	Step 3	Authenticate and enroll trustpoint manually OR Authenticate and enroll trustpoint automatically
	Step 4	Assign Trustpoint
Configuration Using the Catalyst 9800 WebUI, on page 25	Step 1	Create RSA Key
	Step 2	Create, authenticate and enroll trustpoint manually OR Create, authenticate and enroll trustpoint automatically
	Step 3	Assign Trustpoint

- Configuration Using the Catalyst 9800 CLI, on page 2
- Configuration Using the Catalyst 9800 WebUI, on page 25

Configuration Using the Catalyst 9800 CLI

The following steps show how to generate an RSA key, configure a trustpoint, request a certificate from an external Certificate Authority using manual enrollment or automatic enrollment and finally use the trustpoint for a particular service.

The progress bar is a visual indication of the steps that you are expected to complete in the module before you move on to the next configuration step.

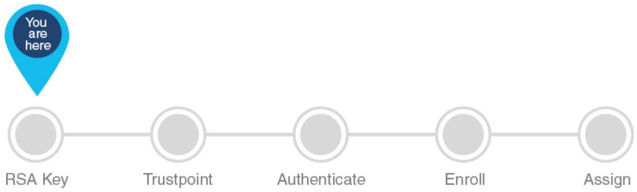
RSA Key
Trustpoint
Authenticate
Enroll
Assign

What to do next

Create an RSA Key Pair using the CLI, on page 2

Create an RSA Key Pair using the CLI

Keys in a PKI system are used to encrypt and decrypt data. A key pair (a public and a private key) is required before you can obtain a certificate for your controller. The end host (here the controller) must generate a pair of keys and exchange the public key with the certification authority (CA) to obtain a certificate and enroll in a PKI. To generate key pairs, perform the following procedure on the controller's CLI:



Before you begin

Ensure that you have an understanding of the PKI framework.

Step 1 **enable**

Example:

```
Device>enable
```

Enables privileged EXEC mode. Enter your password, if prompted.

Step 2 **configure terminal**

Example:

```
Device#configure terminal
```

Enters global configuration mode.

Step 3 **crypto key generate rsa**

Example:

```
Device(config)#crypto key generate rsa
```

Generates one, general-purpose RSA key pair. The default key modulus is 1024. To specify other modulus sizes, use the **modulus** keyword.

Step 4 **crypto key generate rsa label** *key-pair-label*

Example:

```
Device(config)#crypto key generate rsa general-keys label ewlc-keys
```

(Optional) Assigns a label to each key pair. The label is referenced by the trustpoint that uses the key pair. Hence, we recommend that you use the same name for both key pair and trustpoint. If you do not assign a label, the key pair is automatically labeled, *Default-RSA-Key*.

Here we have named the key, *ewlc-keys*.

Step 5 **exit**

Example:

```
Device(config)#exit
```

Exits global configuration mode and returns to privileged EXEC mode.

Step 6 **show crypto key mypubkey rsa** *name of key*

Example:

```
Device#show crypto key mypubkey rsa ewlc-keys
```

(Optional) Displays the RSA public keys of your controller.

Verifies key pairs that you have generated.

Step 7 **write memory**

Example:

```
Device#write memory
```

Saves the keypair you have generated into secure storage.

This concludes the successful creation of an RSA keypair.

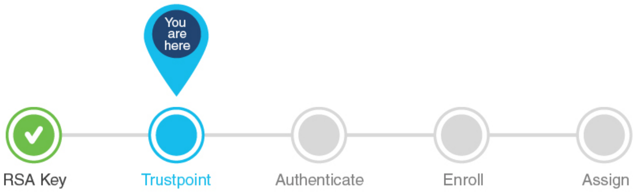
RSA Key
Trustpoint
Authenticate
Enroll
Assign

What to do next

Create a Trustpoint using the CLI, on page 4

Create a Trustpoint using the CLI

Trustpoints help to manage and track CAs and certificates that are used by the different services on the controller. Trustpoints work with RSA key pairs, hence we recommend that you use the same name for the key pair and trustpoint during configuration. To configure a trustpoint, perform the following steps:



Before you begin

Ensure that you have created a RSA keypair to be associated with the trustpoint.

Step 1 **enable**

Example:

```
Device>enable
```

Enables privileged EXEC mode. Enter your password, if prompted.

Step 2 **configure terminal**

Example:

```
Device#configure terminal
```

Enters global configuration mode.

Step 3 **crypto pki trustpoint** *trustpoint-name*

Example:

```
Device(config)#crypto pki trustpoint ewlc-cert
```

Creates a trustpoint that corresponds to the CA from which the controller needs to receive a certificate. Enters the crypto ca trustpoint configuration mode, which controls CA-specific trustpoint parameters that you will start configuring.

Step 4 Do one of the following:

- **enrollment url** *url*

  ```
  Device(config-ca-trustpoint)#enrollment url http://<CA server IP>/certsrv/mscep/mscep.dll
  ```

  ```
  Device(ca-trustpoint)#enrollment url http://10.29.67.142:80/certsrv/mscep/mscep.dll
  ```

Requests automatic enrollment using SCEP with the specified trustpoint and configures the enrollment URL.

- **enrollment terminal**

  ```
  Device(config-ca-trustpoint)#enrollment terminal
  ```

Requests manual enrollment with the specified trustpoint by pasting the certificate received from the CA into the terminal.

Step 5 **subject-name** *subject_name*

Example:

```
Device(config-ca-trustpoint)#subject-name C=MX, ST=Nuevo Leon, L=Guadalupe, O=lab-wireless,
OU=mex-wireless, CN=public-guest.lab-kcg.com
```

Creates subject name parameters for the trustpoint.

Table 1: Subject Name Parameters

Field	Description
Domain Name/Common Name	Refers to the subject to which the certificate will be issued to. The fully qualified domain name (FQDN) of the controller. This must match exactly what you type in your web browser to reach the controller, or you will receive a name mismatch error. Depending on what your certificate requirement is for (webauth, webadmin, AP join) You must specify either the virtual IP address of your 9800 controller, the hostname associated with the virtual IP address of your 9800 controller, the management IP address or the hostname associated with the management IP address.
Country Code	The two-letter ISO code for the country where your organization is located.
State	The state/region where your organization is located. This shouldn't be abbreviated.
Location	The place where your organization is located.
Organisation	The legal name of your organization. This should not be abbreviated and should include suffixes such as Inc, Corp, or LLC.
Email Address	An email address used to contact your organization.

Step 6 **rsakeypair** *RSA_key*

Example:

```
Device(ca-trustpoint)#rsakeypair ewlc-keys
```

Maps RSA key with that of the trustpoint.

Step 7 **revocation**{**crl** | **none** | **ocsp**}

Example:

```
Device(ca-trustpoint)#revocation none
```

Sets one or more methods for revocation checking: CRL, OCSP, and none.

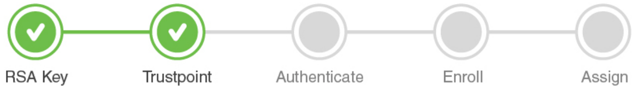
Step 8 **exit**

Example:

```
Device(ca-trustpoint)#exit
```

Exits global configuration mode and returns to privileged EXEC mode.

This concludes the successful creation of an RSA keypair and a trustpoint.



What to do next

Authenticate and Enroll the Trustpoint using the CLI , on page 6

Authenticate and Enroll the Trustpoint using the CLI

Certificate enrollment, which is the process of obtaining a certificate from a certification authority (CA), occurs between the end host that requests the certificate and the CA. Each peer that participates in the public key infrastructure (PKI) must enroll with a CA. You can choose to enroll the trustpoint manually or automatically. Select from the options below.

Authenticate and Enroll a Trustpoint Manually using the CLI , on page 6

OR

Authenticate and Enroll a Trustpoint Automatically using the CLI, on page 10

Authenticate and Enroll a Trustpoint Manually using the CLI

Manual certificate enrollment can be set up via TFTP or the manual cut-and-paste method. Both options can be used if your CA does not support SCEP or if a network connection between the controller and CA is not possible.

This configuration shows how to manually enroll, obtain and install the CA server certificate and the controller's device certificate. It uses an existing enterprise CA (Windows Certificate Server 2012) and does not cover the steps to set up a Windows Certificate Server CA from scratch. This procedure involves the following.

- Authenticate the trustpoint - Obtain and accept issuer-certificate of CA-server used to sign the device certificate.
- Enroll the trustpoint - Obtain the signed device certificate from the Certificate Authority by creating a Certificate Signing Request (CSR) and submitting the CSR to the CA.

- Install the certificate - Load the cetificate into the Wireless LAN Controller.

To authenticate , enroll and install the trustpoint manually using the cut-and-paste method, perform the following procedure on the controller:

You are here
RSA Key
Trustpoint
Authenticate
Enroll
Assign

Before you begin

Before you authenticate and enroll a trustpoint you should:

- have created an RSA key pair and a trustpoint and specified the enrollment method as manual by issuing the command **Device(config-ca-trustpoint)# enrollment terminal pem** . See step 4 of Create a Trustpoint using the CLI, on page 4 to configure this.
- understand the certificate extensions and procedure to convert it to a format, acceptable to the controller.
- understand the transport type that you will use to import the certificate or certificate chain from your CA in case the keys and Certificate Signing Request were generated outside the controller.

Step 1 Go to your enterprise CA page in the browser usually (*https://<CA-ip>/certserv*). Authenticate as administrator and click **Download a CA certificate**, **Certificate Chain** or **CRL**.

Step 2 In the **Encoding Method**, click the **Base 64 encoded radio** button and click **Download CA Certificate**.

Step 3 Copy the Base 64 encoded CA certificate contents into a notepad.

Step 4 Log into the controller's CLI either by SSH or Telnet and enter the following commands to import the CA certificate to the controller.

a) enable

Example:

```
Device>enable
```

Enables privileged EXEC mode. Enter your password if prompted.

b) **configure terminal**

Example:

```
Device#configure terminal
```

Enters global configuration mode.

c) **crypto pki authenticate** *trustpoint*

Example:

```
Device(config)#crypto pki authenticate ewlc-cert
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
-----BEGIN CERTIFICATE-----
*Issuing CA certificate*
-----END CERTIFICATE-----
```

```
Certificate has the following attributes:
Fingerprint MD5: DD05391A 05B62573 A38C18DD CDA2337C
Fingerprint SHA1: 596DD2DC 4BF26768 CFB14546 BC992C3F F1408809
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported
```

This step authenticates the trustpoint and imports the Issuer CA certificate for the configured trustpoint. In other words, having the issuer certificate ensures that the controller trusts the CA that issues the device certificate. Ensure that the issuer certificate that will sign the controller's CSR is in .pem format. The certificate in this example is named **ewlc-cert** but you can chose the name you prefer, to differentiate between your certificates.

Note In case you have several levels of CAs, you must paste the issuing CA certificate here, i.e. the CA that issued your device certificate and only that one, not the chain. You will then need to create a trustpoint for each extra level of CA and repeat this step only for each of those trustpoints (i.e. authenticate a CA for each level).

d) **cypto pki enroll** *trustpoint*

Example:

```
Device(config)#crypto pki enroll ewlc-cert
% Start certificate enrollment ..
% The subject name in the certificate will include: C=MX, ST=Nuevo Leon, L=Guadalupe,
O=lab-wireless, OU=mex-wireless, CN=public-guest.lab-kcg.com
% The subject name in the certificate will include: 9800 WLC-karlcisn-Public.lab-kcg.com
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Display Certificate Request to terminal? [yes/no]: yes
Certificate Request follows:
-----BEGIN CERTIFICATE REQUEST-----
*9800 WLC CSR*
-----END CERTIFICATE REQUEST-----
---End - This line not part of the certificate request--- Redisplay enrollment request? [yes/no]:
no
```

Generates a certificate for signing data and depending on the type of keys that you have configured, for encrypting data. The certificate request will be displayed on the console terminal so that it can be manually copied (or cut) to be sent to the CA.

Step 5 Send the full string of the certificate to the CA to get it signed.

Example:

```
-----BEGIN CERTIFICATE REQUEST-----
*9800 WLC CSR*
-----END CERTIFICATE REQUEST-----
```

Step 6 Go to your enterprise CA page in the browser usually (*https://<CA-ip>/certsrv*). Authenticate as administrator and click **Request a certificate**.

Step 7 Click the **Advanced Certificate Request** and enter the CSR details in the Certificate Template drop-down list, by selecting, **Web Server** and **Submit**.

Step 8 Click the **Base 64 encoded** radio button and download the certificate.

Note Ensure that your **Base 64 encoded** certificate is in .pem format. If it is in a different format, you will need to convert it to a format acceptable by the controller. See the procedure on how to convert to a different format in the Troubleshooting section of this guide.

Step 9 Log into the controller CLI either by SSH or Telnet and enter the following commands to import the device certificate that you received from your CA to the controller.

- If the keys and CSR were generated on the controller.

a) **crypto pki import** *trustpoint* **certificate**

Example:

```
Device(config)#crypto pki import ewlc-cert certificate
Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself
-----BEGIN CERTIFICATE-----
 *9800 WLC Signed Certificate*
 -----END CERTIFICATE-----
 quit
 % Router Certificate successfully imported
```

Import and install the signed device certificate that you got from your CA into the controller.

b) **show crypto pki certificates** *trustpoint-name*

Example:

```
Device# do sh crypto pki certificates ewlc-cert
Certificate
Status: Available
Certificate Serial Number (hex): 00A2020356CF31C818 Certificate Usage: General Purpose
Issuer:
cn=CA-KCG-lab
ou=lab-mex-wireless
o=mex-wireless
l=Guadalupe
st=Nuevo Leon
c=MX
Subject:
Name: *.lab-kcg.com
cn=*.lab-kcg.com
ou=lab-mex-wireless
o=mex-wireless
l=Benito Juarez
st=CDMX
c=MX
Validity Date:
start date: 17:14:54 UTC Feb 15 2018
end date: 17:14:54 UTC Mar 11 2023
Associated Trustpoints: ewlc-cert
Storage: nvram:CA-KCG-lab#C818.cer
```

Verifies that the enrollment process was successful by displaying certificate details issued for the controller and the CA certificate for the trustpoint.

- If the keys and CSR were generated outside the WLC

a) **crypto pki import** *trustpoint certificate-filename* **pkcs12** *tftp://TFTP-IP trustpoint certificate-filename* **password** *trustpoint-cert-password*

Example:

```
Device(config)#crypto pki import manual-tp pkcs12 tftp://9.7.44.186/xxx/9800_vwlc_ssc.pfx password
 cisco123
% Importing pkcs12...Reading file from tftp://9.7.44.186/xxx/9800_vwlc_ssc.pfx
Loading xxx/9800_vwlc_ssc.pfx from 9.7.44.186 (via Vlan39): !
[OK - 3709 bytes]

CRYPTO_PKI: Imported PKCS12 file successfully.
sangudla-wlc(config)#
Mar 19 11:04:11.925: %PKI-6-TRUSTPOINT_CREATE: Trustpoint: manual-tp created succesfully
Mar 19 11:04:11.926: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named manual-tp has been generated or
```

```
imported by pki-pkcs12
Mar 19 11:04:11.935: %PKI-6-PKCS12_IMPORT_SUCCESS: PKCS #12 import in to trustpoint manual-tp
successfully imported.
```

Import the certificate using the TFTP server and install the signed device certificate that you got from your CA into the controller.

Note Ensure that there are no spaces after the password.

b) **show crypto pki certificate**

Example:

```
Device#do sh crypto pki certificate ewlc-cert
Certificate
Status: Available
Certificate Serial Number (hex): 00A2020356CF31C818 Certificate Usage: General Purpose
Issuer:
cn=CA-KCG-lab
ou=lab-mex-wireless
o=mex-wireless
l=Guadalupe
st=Nuevo Leon
c=MX
Subject:
Name: *.lab-kcg.com
cn=*.lab-kcg.com
ou=lab-mex-wireless
o=mex-wireless
l=Benito Juarez
st=CDMX
c=MX
Validity Date:
start date: 17:14:54 UTC Feb 15 2018
end date: 17:14:54 UTC Mar 11 2023
Associated Trustpoints: ewlc-cert
Storage: nvram:CA-KCG-lab#C818.cer
```

Verifies that the enrollment process was successful by displaying certificate details issued for the controller and the CA certificate for the trustpoint.

This concludes the successful authentication and subsequent enrollment of the trustpoint. It means that the certificate requested by the controller from the CA server is available and ready to be assigned to a specific service.

RSA Key
Trustpoint
Authenticate
Enroll
Assign
s

What to do next

Assign a Trustpoint for a Specific Service using the CLI, on page 19

Authenticate and Enroll a Trustpoint Automatically using the CLI

The following configuration shows how to request a certificate from an external Certificate Authority using automatic enrollment . It does not include the steps for setting up a Windows Server 2012 Standard R2, neither does it cover the steps for setting up the Simple Certificate Enrollment Protocol (SCEP) server. Refer to the

SCEP document listed in Additional References for Trustpoint Configuration on Catalyst 9800 for specific configuration details.

With SCEP, the CA and device certificates are received from the CA server, and later installed automatically on the controller.

This procedure involves the following.

- Authenticate the trustpoint - Obtain and accept issuer-certificate of CA-server used to sign the device certificate.
- Enroll the trustpoint - Obtain the signed device certificate from the Certificate Authority over SCEP.
- Install the certificate - Load the cetificate into the Wireless LAN Controller.

You can use automatic enrollment for any certificate. In this example, we will specifically talk about Locally Significant Certificates that are used for AP Join. Once you receive the certificates, you will need to provision the AP with the certificate.

Note Since LSCs can be used for both AP Join and 802.1x port authorization, the AP Authorization state is by default set to use for CAPWAAP-DTLS sessions.

Note that this document does not talk about the additional configurations required if you want to use the LSC for 802.1x port authorization.

To authenticate, enroll and install the certificate automatically using the SCEP server perform the following procedure on the controller:

Before you begin

Before you authenticate and enroll a trustpoint you should:

- have an set up an external Certificate Authority and SCEP server and have a good understanding of these.
- have created a RSA key pair and a trustpoint and specified the enrollment method as automatic by issuing the command **Device(config-ca-trustpoint)#enrollment url http://<CA serverIP>/certsrv/mscep/mscep.dll>**. This means that certificates will be obtained from the specified Certificate Authority sever over SCEP. See step 4 of Create a Trustpoint using the CLI, on page 4

You are here
RSA Key
Trustpoint
Authenticate
Enroll
Assign

Step 1 **enable**

Example:

```
Device>enable
```

Enables privileged EXEC mode. Enter your password, if prompted.

Step 2 **configure terminal**

Example:

```
Device#configure terminal
```

Enters global configuration mode.

Step 3 **crypto pki authenticate** *trustpoint*

Example:

```
Device(config)#crypto pki authenticate ewlc-cert
  Certificate has the following attributes: Certificate has the following attributes:
 Fingerprint MD5: DD05391A 05B62573 A38C18DD CDA2337C
 Fingerprint SHA1: 596DD2DC 4BF26768 CFB14546 BC992C3F F1408809
 % Do you accept this certificate? [yes/no]: yes
 Trustpoint CA certificate accepted.
 % Certificate successfully imported
```

Authenticate the trustpoint. This step imports the CA certificate for the configured trustpoint to ensure that the controller trusts your CA.

Note This step assumes that you have already obtained a Base 64 encoded CA certificate from the CA represented by the trustpoint.

Step 4 **crypto pki enroll** *trustpoint*

Example:

```
Device(config)#crypto pki enroll ewlc-cert
%
 % Start certificate enrollment ..
 % Create a challenge password. You will need to verbally provide this
 password to the CA Administrator in order to revoke your certificate.
 For security reasons your password will not be saved in the configuration.
 Please make a note of it.
 Password:
 Re-enter password:
% The subject name in the certificate will include: C=MX, ST= Nuevo Leon, L= Guadalupe, O=
lab-wireless, CN=public-guest.lab-kcg.com, OU=mex-wireless
% The subject name in the certificate will include: 9800-L.xyz.local
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
```

Enrolls the controller with the trustpoint. Generates a certificate for signing data and depending on the type of keys that you have configured, for encrypting data.

To complete enrollment, obtain a certificate for the certificate request generated by the **crypto pki enroll** command from the CA represented by the applicable trustpoint.

Step 5 **exit**

Example:

```
Device(config)#exit
```

Exits global configuration mode and enters privileged EXEC mode.

Step 6 **write memory**

Example:

```
Device#write memory
```

Saves your entries in the configuration file.

Step 7 **show crypto pki certificates**

Example:

```
Device#show crypto pki certificates ewlc-cert
```

Verifies that the enrollment process was successful by displaying certificate details issued for the controller and the CA certificate for the trustpoint.

```
Certificate
 Status: Available
 Certificate Serial Number (hex): 00A2020356CF31C818
 Certificate Usage: General Purpose
 Issuer:
 cn=CA-KCG-lab
 ou=lab-mex-wireless
 o=mex-wireless
 l=Guadalupe
 st=Nuevo Leon
 c=MX
 Subject:
 Name: *.lab-kcg.com
 cn=*.lab-kcg.com
 ou=lab-mex-wireless
 o=mex-wireless
 l=Benito Juarez
 st=CDMX
 c=MX
 Validity Date:
 start date: 17:14:54 UTC Feb 15 2018
 end date: 17:14:54 UTC Mar 11 2023
 Associated Trustpoints: cert-name
 Storage: nvram:CA-KCG-lab#C818.cer
```

This concludes the successful authentication and subsequent enrollment of the trustpoint. In other words, it means that the certificate requested by the controller from the CA server is available and ready to be used by a specific service.

RSA Key
Trustpoint
Authenticate
Enroll
Assign

What to do next

If you are using the LSC certificate for AP Join, first provision the AP with the LSC. Refer to Provision Access Points with Locally Significant Certificates using the CLI, on page 15. Next assign the trustpoint for AP Join using LSC, refer to Assign a Trustpoint for AP Join with LSC using the CLI, on page 19.

OR

If you want to use the automatically obtained certificate for any other service, refer to Assign a Trustpoint for a Specific Service using the CLI, on page 19

Configure AP with MIC/SUDI to join Controller with LSC using the CLI

Starting from release 17.5, you can onboard an AP with a MIC/SUDI certificate to join a LSC deployed controller. Earlier, an AP with the default MIC/SUDI certificate would fail to join a controller whose wireless management trustpoint had been set to use an LSC. You would need to separately provision the AP with the LSC on a staging server before it could join the controller using the LSC. With release 17.5, the new authorization policy on the AP allows APs with MIC to join an LSC deployed controller.

To enable authorization on the AP's certificate policy perform the following task on the controller:

Step 1 **enable**

Example:

```
Device>enable
```

Enables privileged EXEC mode. Enter your password if prompted.

Step 2 **configure terminal**

Example:

```
Device#configure terminal
```

Enters global configuration mode.

Step 3 **ap auth-list ap-cert-policy allow-mic-ap**

Example:

```
Device(config)#ap auth-list ap-cert-policy allow-mic-ap
```

Enables the AP certificate policy which allows APs with MIC to join during a CAPWAP-DTLS handshake.

Step 4 **ap auth-list ap-cert-policy allow-mic-ap trustpoint** *trustpoint-name*

Example:

```
Device(config)# ap auth-list ap-cert-policy allow-mic-ap trustpoint trustpoint-name
```

Note The trustpoint configuration is required only for the virtual controller since it uses a self-signed certificate.

Configures the trustpoint name for the controller certificate chain. When APs join the virtual controller, they need to Device(config)# ap auth-list ap-cert-policy allow-mic-ap trustpoint trustpoint-name be aware of the trustpoint being used by the wireless management interface. In all other appliance controller platforms, the default MIC certificate will be selected. This default certificate is manufacturer installed SUDI.

Step 5 **ap auth-list ap-cert-policy** {**mac-address** *AP-Ethenet MAC-address* | **serial number** *AP serial-number*} **policy-type mic**

Example:

```
(config)#ap auth-list ap-cert-policy mac-address
1111.2222.3333 policy-type mic
```

```
(config)#ap auth-list ap-cert-policy serial-number
FGL2125ANSD policy-type mic
```

Configures the list of APs based on Ethernet MAC address or based on the assembly serial number of the AP, that should join using MIC.

Step 6 **exit**

Example:

```
Device(config)#exit
```

Exits global configuration mode and enters privileged EXEC mode.

Step 7 **show ap auth-list ap-cert-policy**

Example:

```
Device#show ap auth-list ap-cert-policy
Authorize APs joining with MIC : ENABLED
MIC AP policy trustpoint
Name : CISCO_IDEVID_SUDI
Certificate status : Available
Certificate Type : MIC
Certificate Hash : xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
```

Verifies if the AP has been authorized to join using MIC.

Step 8 **show ap auth-list ap-cert-policy mac-address**

Example:

```
Device#show ap auth-list ap-cert-policy mac-address
MAC address AP cert policy
---------------------------------
00a2.891e.0fe8 MIC
00a3.8e4a.7632 MIC
1111.2222.3333 MIC
2c5a.0f70.84dc MIC
5c71.0d2e.a2cc MIC
f4db.e643.a0d6 MIC
```

```
Device#show ap auth-list ap-cert-policy serial-number
Serial number AP cert policy
--------------------------------
FGL2125ANSD MIC
```

Verifies if the AP has been selected for the authorization policy, based on its MAC address or serial number.

What to do next

If you want the AP to use the LSC, provision it using the steps in Provision Access Points with Locally Significant Certificates using the CLI, on page 15.

Provision Access Points with Locally Significant Certificates using the CLI

Other than Manufacturer Installed Certificate (MIC) or Secure Unique Device Identifier (SUDI) certificates, Access Points (AP) can also be provisioned with Locally Significant Certificates (LSC). For APs to be provisioned with LSCs, the controller acts as a proxy for the AP and any request to issue and sign the CA certificate is initiated by the controller. Once the controller receives the third-party certificates, they are pushed from the controller to the AP and next the APs are provisioned with the LSC.

Other than Manufacturer Installed Certificate (MIC) or Secure Unique Device Identifier (SUDI) certificates, Access Points (AP) can also be provisioned with Locally Significant Certificates (LSC). For APs to be provisioned with LSCs, the controller acts as a proxy for the AP and any request to issue and sign the CA certificate is initiated by the controller. Once the controller receives the third-party certificates, they are pushed from the controller to the AP and next the APs are provisioned with the LSC.

For LSC certificates that have been issued by an intermediate certificate authority:

- Ensure that you select the associated trustpoint and RSA key pair , created earlier while provisioning the AP.
- Ensure that you import the complete chain of CA certificates into the Trustpool using the command.

  ```
  Device(config)#crypto pki trustpool import
  ```

  The complete chain should be present on the controller, otherwise you will not be able to provision the AP. This step is not required, if the certificate has been issued by a root CA.

To provision the APs with the certificates perform the following task on the controller:

Before you begin

Before you start assigning the trustpoint for a specific service ensure that

- The trustpoint is valid.
- There is an RSA key pair.

Step 1 **enable**

Example:

```
Device>enable
```

Enables privileged EXEC mode. Enter your password, if prompted.

Step 2 **configure terminal**

Example:

```
Device#configure terminal
```

Enters global configuration mode.

Step 3 **ap lsc-provision subject-name-parameter**

Example:

```
Device(config)#ap lsc-provision subject-name-parameter country <country state <state> city <city>
domain <department> org <organization> email-address <mail address>
```

Configure subject name parameters for AP's device certificate.

Step 4 **ap lsc-provision join-attempt** *number of attempts*

Example:

```
Device(config)#ap lsc-provision join-attempt 10
```

Enter the number of unsuccesful join-attempts after which the AP uses the MIC to join the controller.

Step 5 **ap lsc-provision trustpoint** *trustpoint name*

Example:

```
Device(config)#ap lsc-provision trustpoint trustpoint-name
```

Selects the previously created trustpoint to be associated with this LSC.

Step 6 **ap lsc-provision key-size** *key size*

Example:

```
Device(config)#ap lsc-provision key-size 2048
```

Step 7 **ap lsc-provision mac-address**

Example:

```
Device(config)#ap lsc-provision mac-address 25-2e-65-43-eb-93
```

If LSC is required only on specific group of APs, configure an allowed list of AP mac-addresses.

Step 8 **ap lsc-provision**

Example:

```
Device(config)#ap lsc-provision
```

Enables LSC provisioning for all the APs joining the controller.

Step 9 **ap lsc-provision provision-list**

Example:

```
Device(config)#ap lsc-provision provision-list
```

Enables LSC provisioning for the allowed list of APs.

Step 10 **exit**

Example:

```
Device(config)#exit
```

Exits global configuration mode and enters privileged EXEC mode.

Step 11 **show ap lsc-provision summary**

Example:

```
Device#show ap lsc-provision summary
AP LSC-provisioning : Enabled for all APs
Trustpoint used for LSC-provisioning : AP-LSC
    Certificate chain status : Available
    Number of certs on chain : 2
    Certificate hash : 323b32f425e374f127d1e52541a5242b8f629e2a
LSC Revert Count in AP reboots : 4
AP LSC Parameters :
Country : MX
State : CDMX
City : Juarez
Orgn : Cisco TAC
Dept : Wireless TAC
Email : xyz@cisco.com
Key Size : 2048
EC Key Size : 384 bit

AP LSC-provision List :

Total number of APs in provision list: 2

Mac Addresses :
--------------
xxxx.xxxx.xxxx
xxxx.xxxx.xxxx
```

Verifies the details about the AP LSC provisioning configuration, along with the list of APs added to the provision list.

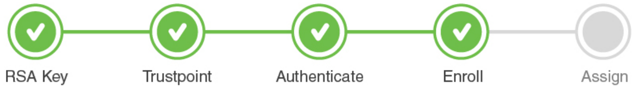
Step 12 **show crypto**

Example:

```
AP3802#show crypto

[...]

------------------------------------------------------------------------------
LSC: Enabled
----------------------------- Device Certificate -----------------------------
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            73:00:00:00:0b:9e:c4:2e:6c:e1:54:84:96:00:00:00:00:00:0b
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: DC=local, DC=chuu-domain, CN=CHUU-WIN12-CA
        Validity
            Not Before: May 13 01:22:13 2020 GMT
            Not After : May 13 01:22:13 2022 GMT
        Subject: C=MX, ST=CDMX, L=Juarez, O=Cisco TAC,
CN=ap3g3-286F7FCF53AC/emailAddress=josuvill@cisco.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)

----------------------------- Root Certificate -------------------------------
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            32:61:fb:93:a8:0a:4a:97:42:5b:5e:32:28:29:0d:32
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: DC=local, DC=chuu-domain, CN=CHUU-WIN12-CA
        Validity
            Not Before: May 10 05:58:01 2019 GMT
            Not After : May 10 05:58:01 2024 GMT
        Subject: DC=local, DC=chuu-domain, CN=CHUU-WIN12-CA
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
```

Verifies the certificates installed in the AP from the AP CLI and ensures that both CA Root certificate and Device certificate are present

This concludes the successful authentication and subsequent enrollment of the trustpoint. It means that the certificate requested by the controller from the CA server is available and ready to be assigned to a specific service.



What to do next

Once the certificate is fully installed, the AP reboots, and starts the join process with the new certificate. Now that you have the LSC certificate installed on the AP, assign the certificate following the steps in Assign a Trustpoint for AP Join with LSC using the CLI, on page 19.

Assign a Trustpoint for a Specific Service using the CLI

Now that the trustpoint configuration is complete, how do you make use of the new certificates that have been created?

The following sections show how to assign the trustpoint to a specific service so that the right certificate is used for the right purpose. This step concludes your trustpoint configuration.

You are here
RSA Key
Trustpoint
Authenticate
Enroll
Assign

Assign a Trustpoint for AP Join with MIC or SSC using the CLI

The wireless management interface is used for AP Join. Note that both for physical controllers and for virtual controllers, no additional configuration is required to assign the trustpoint. The physical controller uses the default MIC or SUDI and the virtual controller uses the self-signed certificate.

However, if you have not generated the self-signed certificate for virtual controllers on Day 0, follow the procedure outlined in Workflow to Configure a Trustpoint for a Self-signed Certificate on Catalyst 9800-CL.

This concludes the workflow of configuring a trustpoint.

What to do next

The above workflow should help you successfully configure a trustpoint. In case you have trustpoint configuration issues, refer to the resolutions to common problem scenarios listed in Troubleshoot Common Issues for Certificate Configuration.

Assign a Trustpoint for AP Join with LSC using the CLI

When configured to use a Locally Significant Certificate (LSC), Access Points join the Controllers using an LSC. To set the wireless management trustpoint to use an LSC for AP Join, perform the following procedure:

Before you begin

- You should have configured a trustpoint for LSC and should have received a certificate from a third-party.
- The AP must have been provisioned with the LSC. For more information on how to do this refer to Provision Access Points with Locally Significant Certificates using the CLI, on page 15.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device>enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device#configure terminal`	Enters global configuration mode.
Step 3	**wireless management trustpoint AP-LSC** **Example:** `Device(config)#wireless management trustpoint AP-LSC`	Assigns the LSC trustpoint for AP Join.
Step 4	**exit** **Example:** `Device(config)#exit`	Exits global configuration mode and returns to privileged EXEC mode.

Step 5	**show wireless management trustpoint**
	Example:
	`Device#show wireless management trustpoint`
	Example:
	`Device#show wireless management trustpoint`
		(Optional) Verifies that the wireless management is using the LSC trustpoint for AP Join.
		`show wireless management trustpoint`
		`Trustpoint Name : AP-LSC`
		`Certificate Info : Available`
		`Certificate Type : LSC`
		`Certificate Hash :`
		`feaa1751353f947f2311c0b7ab4c38206037bcd8`
		`Private key Info : Available`
		`FIPS suitability : Not Applicable`

This concludes the workflow of configuring a trustpoint.

RSA Key
Trustpoint
Authenticate
Enroll
Assign

Assign a Trustpoint for Web Authentication using the CLI

By default, web authentication uses the IOS XE device self-signed certificate to secure the connection between the user and the guest portal. If you want web authentication to use another certificate instead of the self-signed certificate, you must assign it through the web authentication parameter map.

Note Note that when you configure a trustpoint for web authentication purposes, the controller does not present the entire chain, but presents only the device and the CA certificate.

Before you begin

- Ensure that a certificate is installed on your controller.

Step 1 **enable**

Example:

```
Device>enable
```

Enables privileged EXEC mode. Enter your password if prompted.

Step 2 **configure terminal**

Example:

```
Device#configure terminal
```

Enters global configuration mode.

Step 3 **parameter-map type webauth global**

Example:

```
Device(config)#parameter-map type webauth global
```

Creates the parameter map.

Step 4 **trustpoint** *webauth cert*

Example:

```
Device(config-params-parameter-map)#trustpoint webauth-cert
```

Configures trustpoint for local web authentication.

Step 5 **virtual-ip ipv4** *ip-address* **virtual-host** *virtual hostname*

Example:

```
Device(config-params-parameter-map)#virtual-ip ipv4 192.0.2.1 virtual-host
test9800.eu-central-1.compute.internal
```

Ensures that the client trusts the web authentication certificate that has the matching hostname in the Common Name (CN) parameter of the certificate.

Step 6 **exit**

Example:

```
Device(config-params-parameter-map)#exit
```

Exits parameter configuration mode and returns to privileged EXEC mode.

Step 7 **show parameter-map type webauth global**

Example:

```
Device#sh parameter-map type webauth global
Parameter Map Name                : global
  Type                            : webauth
  Auth-proxy Init State time      : 120 sec
  Webauth max-http connection     : 100
  Webauth logout-window           : Enabled
  Webauth success-window          : Enabled
  Consent Email                   : Disabled
```

```
Sleeping-Client               : Disabled
Webauth intercept https       : Disabled
Webauth Captive Bypass        : Disabled
Webauth bypass intercept ACL  :
Trustpoint name               : webauth-cert
HTTP Port                     : 80
Watch-list:
  Enabled                     : no
Webauth login-auth-bypass:
```

Verifies that the WebAuth service is using the correct trustpoint.

This concludes the workflow of configuring a trustpoint.

RSA Key
Trustpoint
Authenticate
Enroll
Assign

Assign a Trustpoint for Webadmin using the CLI

By default, the HTTPS service uses the self-signed certificate generated by the controller's HTTPS server . If you want the HTTPS service to use a third-party certificate instead of the self-signed certificate, you must assign it using the CLI. Before assignning a new certificate, you must have completed the tasks mentioned below.

Note Note that when you configure a trustpoint for web admin purposes, the controller does not present the entire chain, but presents only the device and the CA certificate.

Before you begin

- Ensure that a certificate has been created for webadmin specifically and is saved.
- Ensure that the HTTP server has been restarted for this configuration to take effect.

Step 1 **enable**

Example:

```
Device>enable
```

Enables privileged EXEC mode. Enter your password if prompted.

Step 2 **configure terminal**

Example:

```
Device#configure terminal
```

Enters global configuration mode.

Step 3 **ip http secure-trustpoint** *trustpoint name*

Example:

```
Device(config)#ip http secure-server trustpoint ewlc-cert
```

Assigns the trustpoint to the HTTPS service.

Step 4 **show ip http server secure status**

Example:

```
Device#show ip http server secure status
HTTP secure server status: Enabled
HTTP secure server port: 443
HTTP secure server ciphersuite:
3des-ede-cbc-sha aes-128-cbc-sha
aes-256-cbc-sha dhe-aes-128-cbc-sha
ecdhe-rsa-3des-ede-cbc-sha
rsa-aes-cbc-sha2 rsa-aes-gcm-sha2
dhe-aes-cbc-sha2 dhe-aes-gcm-sha2
ecdhe-rsa-aes-cbc-sha2 ecdhe-rsa-aes-gcm-sha2
HTTP secure server TLS version: TLSv1.2
TLSv1.1 TLSv1.0
HTTP secure server client authentication:
Disabled
HTTP secure server trustpoint: ewlc-cert
HTTP
```

Verifies that the HTTPS service is using the correct trustpoint.

This concludes the workflow of configuring a trustpoint.

Assign a Trustpoint for Local EAP Authentication using the CLI

To assign a trustpoint for Local EAP authentication, perform the following procedure on the controller:

Before you begin

Ensure that the controller and the client each have their own device certifcate. They must also have a root certificate for the controller and a CA certificate for the client.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device>enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device#configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**eap profile** *profile-name* **Example:** `Device(config)#eap profile mylocapeap`	Configures an eap profile and specifies a profile name.
Step 4	**method peap** **Example:** `Device(config-eap-profile)#method peap`	Adds an allowed method for e.g. EAP-PEAP.
Step 5	**pki-trustpoint** *certificate name* **Example:** `Device(config-eap-profile)#pki-trustpoint admincert`	Sets the default pki trustpoint to be used for local eap authentication.
Step 6	**exit** **Example:** `Device(config)#exit`	Exits EAP configuration.

Step 7	**show run eap profiles**
	Example:
	`Device#show run eap profiles`
	`eap profile md5`
	`method md5`
	`end`
	
	`eap profile TLS`
	`method tls`
	`pki-trustpoint Self`
	`end`
	
	`eap profile MD5`
	`method md5`
	`end`
	
	`eap profile FAST`
	`method fast`
	`end`
		Shows the trustpoint configured for the EAP profile.

This completes the workflow for configuring a trustpoint.

RSA Key
Trustpoint
Authenticate
Enroll
Assign

What to do next

The above workflow should help you successfully configure a trustpoint. In case you have trustpoint configuration issues, refer to the resolutions to common problem scenarios listed in Troubleshoot Common Issues for Certificate Configuration.

Configuration Using the Catalyst 9800 WebUI

The following steps show how to generate an RSA key, configure a trustpoint, request a certificate from an external Certificate Authority using manual enrollment or automatic enrollment and finally use the trustpoint for a particular service.

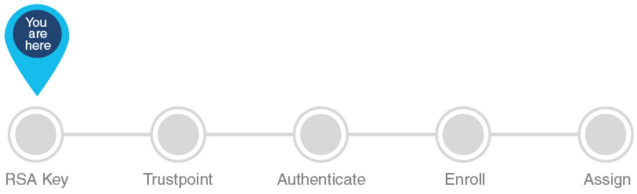
The progress bar is a visual indication of the steps that you are expected to complete in the module before you move on to the next configuration step.

What to do next

Create an RSA Key Pair using the GUI, on page 25

Create an RSA Key Pair using the GUI

Keys in a PKI system are used to encrypt and decrypt data. A key pair (a public and a private key) is required before you can obtain a certificate for your controller. The end host (here the controller) must generate a pair of keys and exchange the public key with the certification authority (CA) to obtain a certificate and enroll in a PKI. To generate a key pair, complete this task on the controller's GUI:



Before you begin

Ensure that you have an understanding of the PKI framework.

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

Step 2 In the **Key Pair Generation** section, click **Add**.

a) Enter the **Key Name**. The label is referenced by the trustpoint that uses the key pair. If you do not assign a label, the key pair is automatically labeled, *Default-RSA-Key*.
b) In the **Key Type** options, select either **RSA Key** or **EC Key**. The default modulus size for the RSA key is 4096 and the default value for the EC key is 521.
c) In the **Modulus Size** field, enter the modulus value for the RSA key or the EC key.
d) Check the **Key Exportable** check box to export the key for backup or archive purposes. By default, this field is enabled.
e) Click **Generate**.

This successfully concludes the creation of a keypair.

RSA Key
Trustpoint
Authenticate
Enroll
Assign

What to do next

Create, Authenticate and Enroll a Trustpoint using the WebUI, on page 26

Create, Authenticate and Enroll a Trustpoint using the WebUI

Certificate enrollment, which is the process of obtaining a certificate from a certificate authority (CA), occurs between the end host that requests the certificate and the CA. Each peer that participates in the public key infrastructure (PKI) must enroll with a CA. You can choose to enroll the trustpoint manually or automatically after you have created a trustpoint. Select from the options below.

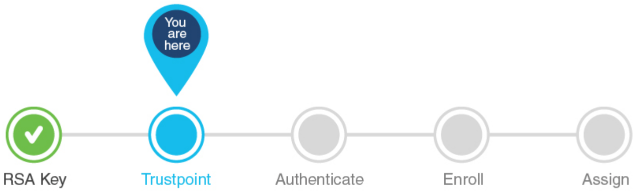
Create, Authenticate and Enroll a Trustpoint Manually using the WebUI, on page 26

OR

Create, Authenticate and Enroll a Trustpoint Automatically using the WebUI, on page 28

Create, Authenticate and Enroll a Trustpoint Manually using the WebUI

Trustpoints help to manage and track CAs and certificates that are used by the different services on the controller. Trustpoints work with RSA key pairs, hence we recommend that you use the same name for the key pair and trustpoint during configuration. A trustpoint needs to be declared to send certificate requests for the controller and also for obtaining the certificate authority's (CA) certificate. To create, authenticate and enroll a trustpoint manually perform this procedure on the controller's WebUI:



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.

Table 2: Subject Name Parameters

Field	Description
Domain Name/Common Name	The fully qualified domain name (FQDN) of the WLC server. This must match exactly what you type in your web browser to reach the controller, or you will receive a name mismatch error. Depending on what your certificate requirement is (for webauth,webadmin, AP join), you must specify either the virtual IP address of your 9800 controller, the hostname associated with the virtual IP address of your 9800 controller, the management IP address or the hostname associated with the management IP address.
Country Code	The two-letter ISO code for the country where your organization is located.
State	The state/region where your organization is located. This shouldn't be abbreviated.
Location	The place where your organization is located.
Organisation	The legal name of your organization. This should not be abbreviated and should include suffixes such as Inc, Corp, or LLC.
Email Address	An email address used to contact your organization.

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 Issuer CA** .

a) From the **Trustpoint** drop-down list, choose the trustpoint label generated above, or any other trustpoint label that you want to authenticate.

b) In the **Issuer CA Certificate (.pem)** field, copy and paste the certificate of the issuer CA received in .pem format that signed the CSR.

Note This step assumes that you already have the PEM Base64 certificate of the issuing CA. Ensure that you copy and paste the PEM Base64 certificate of the issuing CA that signs the device certificate.

c) Click **Authenticate**.

Step 4 Depending on whether you received a PEM certificate or a PKCS12 certificate, select the import and install method.

- Import .PEM certificate for the device

a) From the **Trustpoint** drop-down list, choose the trustpoint label that was generated earlier for a particular service.

b) Copy the paste the certificate contents received from the CA and click **Import**.

- Import PKCS12 certificate for the device

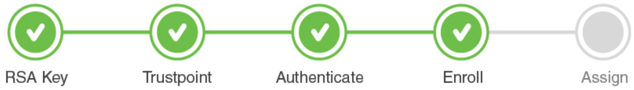
a) From the **Transport Type** drop-down list, choose either **FTP**, **SFTP**, **TFTP**, **SCP**, or **Desktop (HTTPS)**.

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**.

This concludes the successful authentication and subsequent enrollment of the trustpoint. In other words, it means that the certificate requested by the controller from the CA server is available and ready to be used by a specific service.



If you have issues with certificates and formats, check Troubleshoot Common Issues for Certificate Configuration to find a solution to your problem.

What to do next

Assign a Trustpoint for a Specific Service using the WebUI, on page 32

Create, Authenticate and Enroll a Trustpoint Automatically using the WebUI

A trustpoint is an abstract container for an identity certifcate that can be used to secure communication between the client and the server. A trustpoint needs to be declared to send certificate requests for the controller and also for obtaining the certificate authority's (CA) certificate.

The following procedure shows how to request a certificate from an external Certificate Authority using automatic enrollment. It does not include the steps for setting up a Windows Server 2012 Standard R2, neither does it cover the steps for setting up the Simple Certificate Enrollment Protocol (SCEP) server. Refer to the SCEP document listed in Additional References for Trustpoint Configuration on Catalyst 9800 for specific configuration details. With SCEP, the CA and device certificates are received from the CA server, and later installed automatically on the controller.

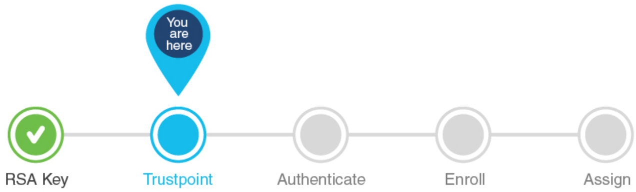
You can use automatic enrollment for any certificate. In this example, we will specifically talk about Locally Significant Certificates that are used for AP Join. Once you receive the certificates, you will need to provision the AP with the certificate.

Note

Since LSCs can be used for both AP Join and 802.1x port authorization, the AP Authorization state is by default set to use for CAPWAAP-DTLS sessions.

Note that this document does not talk about the additional configurations required if you want to use the LSC for 802.1x port authorization.

To create, authenticate and enroll the trustpoint to request and receive a certificate from a third-party, complete this task on the controller's WebUI:s



Before you begin

You should have created a RSA key pair to be associated with the trustpoint.

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 a unique label for the trustpoint.

b) Select the **Enrollment Type** as **SCEP** and enter the enrollment URL in the **Enrollment URL** field, to automatically request and download a CA certificate from the CA server.

c) Check the **Authenticate** check box to authenticate the Trustpoint and get the CA server certificate.

d) In the **Subject Name** section, enter the **Country Code**, **State**, **Location**, **Organisation**, **Domain Name**, and **Email Address**.

Table 3: Subject Name Parameters

Field	Description
Domain Name/Common Name	The fully qualified domain name (FQDN) of the controller server. This must match exactly what you type in your web browser to reach the controller, or you will receive a name mismatch error. Depending on what your certificate requirement is (for webauth,webadmin, AP join), you must specify either the virtual IP address of your 9800 controller, the hostname associated with the virtual IP address of your 9800 controller, the management IP address or the hostname associated with the management IP address.
Country Code	The two-letter ISO code for the country where your organization is located.
State	The state/region where your organization is located. This shouldn't be abbreviated.
Location	The place where your organization is located.
Organisation	The legal name of your organization. This should not be abbreviated and should include suffixes such as Inc, Corp, or LLC.
Email Address	An email address used to contact your organization.

e) Check the **Key Generated** check box to view the available RSA keypairs. Choose an option from the **Available RSA Keypairs** drop-down list to associate the keypair with the trustpoint.

f) Check the **Enroll Trustpoint** check box to request the certificate for the controller from the Certificate Authority.

g) In the **Password** field, enter the password.

Also called the challenge password, this password must match the challenge password for your CA. In the Certificate Signing request template, you must enter the same challenge password that was configured for the SCEP server, otherwise the authentication between the controller and CA fails.

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.

This concludes the successful authentication and subsequent enrollment of the trustpoint. It means that the certificate requested by the controller from the CA server is available and ready to be assigned to a specific service.

What to do next

If you are using the LSC certificate for AP Join, first provision the AP with the LSC. Refer to Provision Access Points with Locally Significant Certificates, using the WebUI, on page 31. Next assign the trustpoint for AP Join using LSC, refer to Assign Trustpoint for AP Join with LSC using the WebUI, on page 33 .

OR

If you want to use the automatically obtained certificate for any other service, refer to the other services in Assign a Trustpoint for a Specific Service using the WebUI, on page 32 .

Configure AP with MIC/SUDI to join Controller with LSC on WebUI

Starting from release 17.5, you can onboard an AP with a MIC/SUDI certificate to join a LSC deployed controller. Earlier, an AP with the default MIC/SUDI certificate would fail to join a controller whose wireless management trustpoint had been set to use an LSC. You would need to separately provision the AP with the LSC on a staging server before it could join the controller using the LSC. With release 17.5, the new authorization policy on the AP allows MIC APs to join LSC deployed controller.

To enable sauthorization on the AP's certificate policy perform the following task on the controller:

Before you begin

Step 1 Configure the AP certificate policy by navigating to **Configuration** > **Wireless** > **Access Points** > **All Access Points** page and expand **AP Certificate Policy**.

a) Tap the **Authorize APs joining with MIC** toggle button to enable AP authorization.

b) Select the **Trustpoint** that should be used by the controller for AP Join. This configuration is required only for the virtual controllers that use a self-signed certificate for AP Join. In case of appliance controllers, the deafult is always the MIC/ SUDI certificate.

Step 2 Build a list of APs that should be allowed to join the controller with this configuration by adding to the **List of MAC Address and Serial Numbers**.

a) Configure the AP Authlist by selecting between **MAC Address** or **Serial Number** of the APs and enter the relevant details in the box below.

b) You can also upload a .csv file containing the above details. The AP Certificate Policy is added to the existing AP Inventory page.

Step 3 Click **Apply** to save the configuration.

What to do next

If you want the AP to use the LSC, provision it using the steps in Provision Access Points with Locally Significant Certificates, using the WebUI, on page 31.

Provision Access Points with Locally Significant Certificates, using the WebUI

Other than the Manufacturing Installed Certificate (MIC) or the Secure Unique Device Identifier (SUDI) certificates, Access Points can also be provisioned with Locally Significant Certificates (LSC). For APs to be provisioned with LSCs, the controller acts as a proxy for the AP and any request to issue and sign the CA certificate is initiated by the controller. Once the controller receives the third-party certificates, they are pushed from the controller to the AP and next the APs are provisioned with the LSC.

From release 17.5, for LSC certificates that have been issued by an intermediate certificate authority:

- ensure that you select the associated trustpoint and RSA key pair, created earlier while provisioning the AP.
- ensure that you import the complete chain of CA certificates into the Trustpool. Go to **Configuration** > **PKI Management** > **Trustpool** tab and use the **Import** button to import the CA certificate. The complete chain should be present on the controller, otherwise you will not be able to provision the AP. This step is not required, if the certificate has been issued by a Root CA.

To provision the APs with the certificates, perform the following task on the controller:

Before you begin

Step 1 Choose **Configuration** > **Wireless** > **Access Points** and expand the **LSC Provision** drop-down list.

Step 2 In the **Subject Name Parameters** section, enter the following details and click **Apply**.

Table 4: Subject Name Parameters

Field	Description
Domain Name/Common Name	The fully qualified domain name (FQDN) of the controller. This must match exactly what you type in your web browser to reach the WLC, or you will receive a name mismatch error.
Country Code	The two-letter ISO code for the country where your organization is location.
State	The state/region where your organization is located. This shouldn't be abbreviated.
Location	The place where your organization is located.
Organisation	The legal name of your organization. This should not be abbreviated and should include suffixes such as Inc, Corp, or LLC.
Email Address	An email address used to contact your organization.

Step 3 Enable LSC provisioning from the **Status** dropdown.

Step 4 Use the **Trustpoint Name** drop-down list to select the previously defined trustpoint associated with the LSC and the key associated with the trustpoint. Enter the retry attempts for the AP to join the controller. After the defined number of attempts, the AP will attempt to join using the MIC.

Step 5 If you want to trigger AP Provisioning using LSC, you can do so in the **Add APs to LSC Provision List** section, by selecting a CSV file containing the AP MAC address details and uploading it or by or addding specific APs defined in the MAC address list.

If you have selected the correct Trustpoint Name, then the **Certificate chain status** and **Number of certificates on chain** reflects the availability of the certificate along with the number of associated chain of certificates. If the status shows as **Not Available** then you must see if the entire chain has been imported or not. Depending on whether you enrolled the certificate automatically or manually, re-import the chain using the procedure in the respective sections.

Step 6 Click **Apply** to trigger AP LSC enrollment.

APs begin certificate request, download, and installation. Once the certificate is fully installed, the AP reboots, and starts the join process with the new certificate.

What to do next

Once the certificate is fully installed, the AP reboots, and starts the join process with the new certificate. Now that you have the LSC certificate installed on the AP, assign the certificate following the steps in Assign Trustpoint for AP Join with LSC using the WebUI, on page 33 .

Assign a Trustpoint for a Specific Service using the WebUI

Now that the trustpoint configuration is complete, how do you make use of the new certificates that have been created? The following sections show how to assign the trustpoint to a specific service so that the right certificate is used for the right purpose. This step concludes your trustpoint configuration.

You are here
RSA Key
Trustpoint
Authenticate
Enroll
Assign

Assign Trustpoint for AP Join with MIC or SSC using the WebUI

The wireless management interface is used for AP Join. In case the AP joins a physical controller, no additional configuration is required on the controller as it uses the default MIC/SUDI. The same is applicable for virtual controllers that have a self-signed certiificate.

However, for virtual controllers, if you have not generated the self-signed certificate on Day 0, the controller's management interface needs to be configured to use its self-signed certificate for AP Join. To do so, perform the following procedure on the controller's WebUI:

Before you begin

You should have a self-signed certificate for the virtual controller. This step is required only if you have not generated a certificate on Day 0. Follow the procedure to generate a self-signed certificate for the virtual controller as outlined in Workflow to Configure a Trustpoint for a Self-signed Certificate on Catalyst 9800-CL.

Step 1 On the **Configuration** > **Interface** > **Wireless** page, select the **VLAN Interface Name**.

Step 2 In the **Edit Management Interface** page, select the **Trustpoint** from the drop-down list. This is the self-signed certificate of the virtual controller.

Step 3 Click **Update & Apply to Device**.

This concludes the workflow of configuring a trustpoint.

RSA Key
Trustpoint
Authenticate
Enroll
Assign

What to do next

The above workflow should help you successfully configure a trustpoint. In case you have trustpoint configuration issues, refer to the resolutions to common problem scenarios listed in Troubleshoot Common Issues for Certificate Configuration.

Assign Trustpoint for AP Join with LSC using the WebUI

Since the wireless management interface is used for AP Join, APs can join the controller using MIC as well as a third-party certificate also known as the Locally Significant Certificate (LSC). If the wireless management interface was previously configured to use the MIC and now you want the LSC to be used for AP Join, you will need to set the trustpoint on the wireless management interface to use the LSC. To do so, perform the following procedure on the controller's WebUI:

Before you begin

- You should have configured a trustpoint for LSC and should have received a certificate from a third-party.
- The AP must have been provisioned with the LSC. For more information on how to do this refer to Provision Access Points with Locally Significant Certificates, using the WebUI, on page 31

Step 1 On the **Configuration** > **Interface** > **Wireless** page, select the **VLAN Interface Name**.

Step 2 In the **Edit Management Interface** page, select the **Trustpoint** that represents the LSC, from the drop-down list.

Step 3 Click **Update & Apply to Device**.

This concludes the workflow of configuring a trustpoint.

RSA Key
Trustpoint
Authenticate
Enroll
Assign

What to do next

The above workflow should help you successfully configure a trustpoint. In case you have trustpoint configuration issues, refer to the resolutions to common problem scenarios listed in Troubleshoot Common Issues for Certificate Configuration.

Assign Trustpoint for Web Admin using the WebUI

Point the HTTPS service to use the certificate for the web login portal. To do so, perform the following procedure on the controller's WebUI:

Step 1 On the **Administration** > **Management** > **HTTP/HTTPS/Netconf** page, tap to **Enable Trustpoint** under **HTTP Trust Point Configuration**.

Step 2 Select the trustpoint from the drop-down list that should be used for web admin authentication.

Step 3 Click **Apply**, for the configuration to take effect.

This completes the workflow of configuring a trustpoint.

RSA Key
Trustpoint
Authenticate
Enroll
Assign

What to do next

The above workflow should help you successfully configure a trustpoint. In case you have trustpoint configuration issues, refer to the resolutions to common problem scenarios listed in Troubleshoot Common Issues for Certificate Configuration.

Assign Trustpoint for Web Authentication using the WebUI

By default, web authentication uses the IOS XE device self-signed certificate to secure the connection between the user and the guest portal. If you want web authentication to use another certificate instead of the self-signed certificate, you must assign it through the web authentication parameter map.

Note Note that when you configure a trustpoint for web authentication purposes, the controller does not present the entire chain, but presents only the device and the CA certificate.

Point the **Web Auth Parameter** to use the trustpoint for web authentication. To do so, perform the following procedure on the controller's WebUI:

Before you begin

Ensure that a certificate is installed on your controller.

Step 1 On the **Configuration** > **Security** > **Web Auth** page, select the **global** parameter.

Step 2 In the **Edit Web Auth Parameter** page, select the **Trustpoint** from the drop-down list that should be used for web authentication.

Step 3 Click **Update & Apply**.

This concludes the workflow of configuring a trustpoint.

What to do next

The above workflow should help you successfully configure a trustpoint. In case you have trustpoint configuration issues, refer to the resolutions to common problem scenarios listed in Troubleshoot Common Issues for Certificate Configuration.

Assign Trustpoint for Local EAP Authentication

Point the EAP profile to use the trustpoint for local eap authentication. To do so, perform the following procedure on the controller's WebUI:

Before you begin

Ensure that the controller and the client each have their own device certifcate. They must also have a root certificate for the controller and a CA certificate for the client. Also,you must have a trustpoint configured for local EAP authentication.

Step 1 Go to the **Configuration** > **Security** > **Local EAP** > **Local EAP Profile** page, and select the profile.

Step 2 Select the trustpoint from the drop-down list that should be used for Local EAP Authentication.

Step 3 Click **Apply**, for the configuration to take effect.

This concludes the workflow for configuring a trustpoint.

What to do next

The above workflow should help you successfully configure a trustpoint. To verify, you can go to **Configuration** > **Security** > **PKI Management** > **Trustpoints** tab to view the Trustpoint, its details and the related service using it.

In case you have trustpoint configuration issues, refer to the resolutions to common problem scenarios listed in Troubleshoot Common Issues for Certificate Configuration.