Locally significant certificates

- Locally significant certificates, on page 1
- Provisioning locally significant certificates, on page 4
- AP certificate renewal (LSC), on page 24
- MIC and LSC APs joining the controller, on page 30
- LSC fallback APs, on page 35
- Configuring controller self-signed certificate for wireless AP join, on page 38

Locally significant certificates

A locally significant certificate (LSC) is a PKI certificate that

- provides mutual authentication between Cisco Embedded Wireless Controller on Catalyst Access Points and Lightweight Access Points (LAPs)
- generates certificates directly on APs and embedded wireless controllers, and
- enables organizations to use their own PKI for better security control and Certificate Authority (CA) management.

LSC provisioning and communication process

You need to provision the new LSC certificate on the embedded wireless controller and then the Lightweight Access Point (LAP) from the CA Server.

The LAP communicates with the embedded wireless controller using the CAPWAP protocol. Any request to sign the certificate and issue the CA certificates for LAP and embedded wireless controller itself must be initiated from the embedded wireless controller. The LAP does not communicate directly with the CA server. The CA server details must be configured on the embedded wireless controller and must be accessible.

The embedded wireless controller makes use of the Simple Certificate Enrollment Protocol (SCEP) to forward certReqs generated on the devices to the CA and makes use of SCEP again to get the signed certificates from the CA.

The SCEP is a certificate management protocol that the PKI clients and CA servers use to support certificate enrollment and revocation. It is widely used in Cisco and supported by many CA servers. In SCEP, HTTP is used as the transport protocol for the PKI messages. The primary goal of SCEP is the secure issuance of certificates to network devices. SCEP is capable of many operations, but for our release, SCEP is utilized for the following operations:

- CA and Router Advertisement (RA) Public Key Distribution
- Certificate Enrollment

Certificate provisioning in controllers

Certificate provisioning in controllers is a security process that you use to:

- Install new Locally Significant Certificate (LSC) certificates (both Certificate Authority (CA) certificates and device certificates) on the controller
- Use Simple Certificate Enrollment Protocol (SCEP) to receive Certificate Authority (CA) certificates from the CA server during initial setup when the controller has no certificates, and
- Push the same Certificate Authority (CA) certificates to Access Points (APs) when you provision the Access Points (APs) with Locally Significant Certificates (LSCs).

RSA keypair recommendations

These recommendations apply when configuring PKI certificates with RSA keypairs:

Note We recommend that you use a new RSA keypair name for the newly configured PKI certificate. If you want to reuse an existing RSA keypair name (that is associated with an old certificate) for a new PKI certificate, do either of the following:

- Do not regenerate a new RSA keypair with an existing RSA keypair name. Instead, reuse the existing RSA keypair name. All certificates associated with the existing RSA keypair become invalid when you regenerate a new RSA keypair with an existing name.
- Remove the old PKI certificate configurations before reusing the existing RSA keypair name for the new PKI certificate.

How device certificate enrollment works

When your Lightweight Access Point (LAP) and controller request Certificate Authority (CA)-signed certificates, they send the certRequest as a PKCS#10 message. The Certificate Authority (CA) receives a PKCS#10 certRequest. The Certificate Authority (CA) requires additional information to authenticate the identity of the requester and verify that the request is unaltered.

Summary

The key components involved in the device certificate enrollment process are:

- Lightweight Access Point (LAP) and controller: request Certificate Authority (CA)-signed certificates by sending PKCS#10 messages. These messages contain Subject Name, Public Key, and other attributes.
- Certificate Authority (CA): transforms the certRequest into an X.509 certificate after authentication and verification

- PKCS#10 certRequest: contains digitally signed certificate request information including Subject Name and Public Key
- Simple Certificate Enrollment Protocol (SCEP) client: provides functionality to wrap PKCS#10 in PKCS#7 Signed Data message type

Workflow

Your device certificate enrollment process works through these stages:

1. The Lightweight Access Point (LAP) and controller create a PKCS#10 certificate request containing the Subject Name, Public Key, and other attributes to be included in the X.509 certificate, and digitally sign it with the Private Key of the requester.
2. The PKCS#10 is wrapped in a PKCS#7 Signed Data message type as part of the Simple Certificate Enrollment Protocol (SCEP) client functionality, and the PKCSReq message is sent to the controller.
3. The Certificate Authority (CA) receives the PKCS#10 certRequest and authenticates the identity of the requester and verifies that the request is unaltered.
4. The Certificate Authority (CA) transforms the certRequest into an X.509 certificate.

Result

Upon successful enrollment operation, both the Certificate Authority (CA) and device certificates are available on the controller.

How certificate provisioning works on lightweight APs

Certificate provisioning enables lightweight APs (LAPs) to obtain new signed X.509 certificates while operating in CAPWAP mode. This process ensures secure communications between APs and controllers using updated security credentials.

Summary

The key components involved in certificate provisioning on lightweight APs are:

- Lightweight Access Point (LAP): Initiates certificate requests and receives new certificates while in CAPWAP mode
- Controller: Acts as a CA proxy to help obtain signed certificates from the Certificate Authority for the LAP
- Certificate Authority (CA): Signs and validates certificate requests to issue new X.509 certificates
- LWAPP payloads: Transport mechanism for certificate requests and responses between LAP and controller

Workflow

These stages describe how certificate provisioning works on lightweight APs:

1. The LAP sends a certificate request to the controller to obtain a new signed X.509 certificate.

   The controller acts as a CA proxy and helps obtain the certificate request signed by the CA for the LAP.

2. The certificate requests and certificate responses are transmitted between the LAP and controller using LWAPP payloads.
3. Both the LSC CA and LAP device certificates are installed in the LAP, and the system reboots automatically.
4. When the system comes up after reboot, the AP sends the LSC device certificate to the controller as part of the JOIN Request because it is configured to use LSCs.

   As part of the JOIN Response, the controller sends the new device certificate and validates the inbound LAP certificate with the new CA root certificate.

What's next

To configure, authorize, and manage certificate enrollment with the existing PKI infrastructure for controller and AP, you need to use the LSC provisioning functionality.

Restrictions for locally significant certificates

- The locally significant certificate (LSC) workflow differs in FIPS and WLANCC mode. Your Certificate Authority (CA) server must support Enrollment over Secure Transport (EST) protocol. Your CA server must also issue EC certificates in FIPS and WLANCC mode.
- The Elliptic Curve Digital Signature Algorithm (ECDSA) cipher works only if both your AP and controller have EC certificates provisioned with LSC.
- EC certificates (LSC-EC) can be provisioned only if CA server supports EST (and not SCEP).
- You must configure FIPS and CC security modes to provision EC certificates.

Provisioning locally significant certificates

Configure RSA key for PKI trustpoint

Generate RSA cryptographic keys for PKI trustpoint authentication and secure communications.

RSA keys are essential components of PKI infrastructure, providing the cryptographic foundation for certificate-based authentication and encryption on wireless controllers.

Before you begin

Ensure the device is in a stable operational state and has sufficient processing resources for key generation.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Generate RSA key for PKI trustpoint.

Example:

```
Device(config)# crypto key generate rsa exportable general-keys modulus key-size label
RSA-key-label
```

Example:

```
Device(config)# crypto key generate rsa exportable
general-keys modulus 2048 label lsc-tp
```

exportable is an optional keyword. You may or may not want to configure an exportable-key. If selected, you can export the key out of the box, if required.

- *key-size*: Size of the key modulus. The valid range is from 2048 to 4096.
- *RSA-key-label*: RSA key pair label.

Step 3 Return to privileged EXEC mode.

Example:

```
Device(config)# end
```

The RSA key is successfully generated and labeled for use with PKI trustpoint configurations.

Configure PKI trustpoint parameters

Configure a PKI trustpoint with RSA key parameters for certificate enrollment and authentication.

PKI trustpoints define the relationship between the device and a Certificate Authority (CA), enabling secure certificate-based authentication and encryption.

Before you begin

Ensure the CA server is accessible and configured to accept certificate requests.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Create a new trustpoint for an external CA server.

Example:

```
Device(config)# crypto pki trustpoint trustpoint-name
```

Example:

```
Device(config)# crypto pki trustpoint microsoft-ca
```

The *trustpoint-name* refers to the trustpoint name.

Step 3 Specify the URL of the CA on which your router should send certificate requests.

Example:

```
Device(ca-trustpoint)# enrollment url HTTP-URL
```

Example:

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

HTTP-URL: URL of the file system where your router should send certificate requests. An IPv6 address can be added in the URL enclosed in brackets. For example: http://[2001:DB8:1:1::1]:80. For more enrollment method options, see the enrollment url (ca-trustpoint) command page.

Step 4 Create subject name parameters for the trustpoint.

Example:

```
Device(ca-trustpoint)# subject-name subject-name
```

Example:

```
Device(ca-trustpoint)# subject-name C=IN, ST=KA, L=Bengaluru, O=Cisco,
CN=eagle-eye/emailAddress=support@abc.com
```

Step 5 Map RSA key with that of the trustpoint.

Example:

```
Device(ca-trustpoint)# rsakeypair RSA-key key-size
```

Example:

```
Device(ca-trustpoint)# rsakeypair ewlc-tp1
```

- *RSA-key*: RSA key pair label.
- *key-size*: Signature key length. Range is from 360 to 4096.

Step 6 Configure revocation checking method.

Example:

```
Device(ca-trustpoint)# revocation {crl | none | ocsp}
```

Example:

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

Step 7 Return to privileged EXEC mode.

Example:

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

The PKI trustpoint is now configured with the specified parameters and ready for certificate enrollment operations.

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.

Authenticate and enroll the PKI trustpoint with CA server (CLI)

Establish secure communication between the device and Certificate Authority by authenticating and enrolling a PKI trustpoint.

PKI trustpoints enable secure certificate-based authentication. The authentication process fetches the CA certificate, while enrollment generates and submits a certificate request to obtain a client certificate.

Before you begin

Ensure the PKI trustpoint is configured and the CA server is accessible.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Fetch the CA certificate.

Example:

```
Device(config)# crypto pki authenticate trustpoint-name
```

Example:

```
Device(config)# crypto pki authenticate microsoft-ca
```

Step 3 Accept the CA certificate.

Example:

```
Device(config)# % Do you accept this certificate? [yes/no]:
yes Trustpoint CA certificate accepted.
```

Step 4 Enroll the client certificate.

Example:

```
Device(config)# crypto pki enroll trustpoint-name
```

Example:

```
Device(config)# crypto pki enroll microsoft-ca
%
% 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.
```

Step 5 Enter a challenge password to the CA server.

Example:

```
Device(config)# password
```

Example:

```
Device(config)# abcd123
```

Step 6 Re-enter the challenge password to the CA server.

Example:

```
Device(config)# password
```

Example:

```
Device(config)# abcd123
```

Step 7 Include the router serial number in the subject name.

Example:

```
Device(config)# % Include the router serial number
in the subject name? [yes/no]: yes
```

Step 8 Exclude IP address from the subject name.

Example:

```
Device(config)# % Include an IP address
in the subject name? [no]: no
```

Step 9 Request certificate from CA.

Example:

```
Device(config)#
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
```

```
% The 'show crypto pki certificate verbose
client' command will show the fingerprint.
```

Step 10 Return to privileged EXEC mode.

Example:

```
Device(config)# end
```

The PKI trustpoint is authenticated and enrolled with the CA server, enabling secure certificate-based communication.

Configure AP join attempts with LSC certificate

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points**.

Step 2 In the **All Access Points** window, click the LSC Provision name.

Step 3 From the **Status** drop-down list, choose a status to enable LSC.

Step 4 From the **Trustpoint Name** drop-down list, choose the trustpoint.

Step 5 In the **Number of Join Attempts** field, enter the number of retry attempts that will be permitted.

Step 6 Click **Apply**.

Configure AP join attempts with LSC certificate (CLI)

Configure the maximum number of AP join failure attempts with a newly provisioned LSC certificate to ensure proper fallback to MIC when needed.

When APs attempt to join with LSC certificates and exceed the configured failure limit, they automatically fall back to using their Manufacturer Installed Certificate (MIC) for authentication.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Specify the maximum number of AP join failure attempts with the newly provisioned LSC certificate.

Example:

```
Device(config)# ap lsc-provision join-attempt number-of-attempts
```

Example:

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

When the number of AP joins exceed the specified limit, AP joins back with the Manufacturer Installed Certificate (MIC).

Step 3 Return to privileged EXEC mode.

Example:

```
Device(config)# end
```

Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

The AP join attempt limit with LSC certificate is now configured. APs will fall back to MIC authentication after exceeding the specified number of failed join attempts.

Configure subject-name parameters in LSC certificate

Configure the subject-name parameters that will be included in LSC certificates generated by access points.

Subject-name parameters define the identity information included in Local Significant Certificate (LSC) requests generated by access points. These parameters include geographical and organizational details that identify the certificate holder.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Specify the attributes to be included in the subject-name parameter of the certificate request generated by an AP.

Example:

```
Device(config)# ap lsc-provision subject-name-parameter
country country-str state state-str city city-str domain domain-str org
org-str email-address email-addr-str
```

Example:

```
Device(config)# ap lsc-provision subject-name-parameter
country India state Karnataka city Bangalore domain domain1 org
Right email-address adc@gfe.com
```

Step 3 Return to privileged EXEC mode.

Example:

```
Device(config)# end
```

The subject-name parameters are now configured for LSC certificate generation on access points.

Configure key size for LSC certificate

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Specify the size of keys to be generated for the LSC on AP.

Example:

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

Example:

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

Valid key size options are 2048, 3072, or 4096 bits.

Step 3 Return to privileged EXEC mode.

Example:

```
Device(config)# end
```

Alternatively, you can also press Ctrl-Z to exit global configuration mode.

Configure trustpoint for LSC provisioning on an AP

Establish a trustpoint for Local Significant Certificate (LSC) provisioning to enable secure communication between access points and the controller.

LSC provisioning allows access points to obtain certificates from a designated trustpoint, enhancing network security through certificate-based authentication.

Before you begin

Ensure the trustpoint is properly configured and accessible on the network.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Specify the trustpoint with which the LSC is provisioned to an AP.

Example:

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

Example:

```
Device(config)# ap lsc-provision trustpoint microsoft-ca
```

The *tp-name* is the trustpoint name.

Step 3 Return to privileged EXEC mode.

Example:

```
Device(config)# end
```

The trustpoint for LSC provisioning is now configured and ready to provision certificates to access points.

Configure an AP LSC provision list (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points**.

Step 2 In the **All Access Points** window, click the corresponding LSC Provision name.

Step 3 From the **Status** drop-down list, choose a status to enable LSC.

Step 4 From the **Trustpoint Name** drop-down list, choose a trustpoint.

Step 5 In the **Number of Join Attempts** field, enter the number of retry attempts that are allowed.

Step 6 From the **Key Size** drop-down list, choose a key.

Step 7 In the **Edit AP Join Profile** window, click the **CAPWAP** tab.

Step 8 In the **Add APs to LSC Provision List** section, click **Select File** to upload the CSV file that contains AP details.

Step 9 Click **Upload File**.

Step 10 In the **AP MAC Address** field, enter the AP MAC address. and add them. (The APs added to the provision list are displayed in the **APs in provision List** .)

Step 11 In the **Subject Name Parameters** section, enter the following details:

- **Country**
- **State**
- **City**
- **Organization**
- **Department**
- **Email Address**

Step 12 Click **Apply**.

Configure an AP LSC provision list (CLI)

Add access points to the LSC provision list for certificate-based authentication.

The LSC provision list allows you to specify which access points can use locally significant certificates for authentication with the wireless controller.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Add the AP to the LSC provision list.

Example:

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

Example:

```
Device(config)# ap lsc-provision
mac-address 001b.3400.02f0
```

Note
You can provision a list of APs using the **ap lsc-provision provision-list** command.

(Or)

You can provision all the APs using the **ap lsc-provision** command.

Step 3 Return to privileged EXEC mode.

Example:

```
Device(config)# end
```

The AP is now added to the LSC provision list and can use locally significant certificates for authentication.

Configure LSC provisioning for all the APs (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points**.

Step 2 In the **Access Points** window, expand the **LSC Provision** section.

Step 3 Set **Status** to **Enabled** state.

Note
If you set **Status** to **Provision List**, LSC provisioning will be configured only for APs that are a part of the provision list.

Step 4 From the **Trustpoint Name** drop-down list, choose the appropriate trustpoint for all APs.

Step 5 In the **Number of Join Attempts** field, enter the number of retry attempts that the APs can make to join the embedded wireless controller.

Step 6 From the **Key Size** drop-down list, choose the appropriate key size of the certificate:

- **2048**
- **3072**
- **4096**

Step 7 In the **Add APs to LSC Provision List** section, click **Select File** to upload the CSV file that contains the AP details.

Step 8 Click **Upload File**.

Step 9 In the **AP MAC Address** field, enter the AP MAC address. (The APs that are added to the provision list are displayed in the **APs in Provision List** section.)

Step 10 In the **Subject Name Parameters** section, enter the following details:

a. **Country**

b. **State**

c. **City**

d. **Organization**

e. **Department**

f. **Email Address**

Step 11 Click **Apply**.

Configure LSC provisioning for all APs (CLI)

Enable LSC (Local Significant Certificate) provisioning across all access points to enhance security through automatic certificate management.

LSC provisioning allows access points to automatically obtain and manage security certificates, reducing manual certificate deployment overhead while maintaining secure wireless communications.

Before you begin

Ensure you have administrative access to the wireless controller and that all APs are properly registered with the controller.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Enable LSC provisioning for all APs.

Example:

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

By default, LSC provisioning is disabled for all APs.

Step 3 Return to privileged EXEC mode.

Example:

```
Device(config)# end
```

LSC provisioning is now enabled for all access points, allowing them to automatically obtain and manage security certificates.

Configure LSC provisioning for the APs in the provision list

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Enable LSC provisioning for a set of APs configured in the provision list.

Example:

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

Step 3 Return to privileged EXEC mode.

Example:

```
Device(config)# end
```

Alternatively, you can also press Ctrl-Z to exit global configuration mode.

Unprovisioning Local Significant Certificates

To unprovision the Local Significant Certificates (LSC), complete the following steps:

1. Move the chassis to WLAN Common Criteria (WLANCC) mode.
2. Reload the APs by provisioning LSC and the wireless management trustpoint. For more information, refer to Configure LSC provisioning and management trustpoint, on page 15 .
3. Remove Federal Information Processing Standard (FIPS) and WLANCC. For more information, refer to Remove FIPS and WLAN common criteria, on page 16 .
4. Remove LSC provisioning. For more information, refer to Remove LSC provisioning, on page 17 .

Configure LSC provisioning and management trustpoint

Before you begin

Identify the name of the standby access point using the **show chassis** command when an EWC (Embedded Wireless Controller) HA pair is configured.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure the AP LSC Provisioning parameters.

Example:

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

Step 3 Configure the management trustpoint for LSC authentication.

Example:

```
Device(config)# wireless management trustpoint trustpoint-name
```

Step 4 Save the configuration.

Example:

```
Device# copy running-config startup-config
```

The standby AP joins the controller. The HA pair is not yet formed at this point.

Step 5 Reload the internal AP.

Example:

```
Device# wireless ewc-ap ap reload
```

This will also reload the controller on the AP.

The standby AP starts the controller and becomes the new active AP for the HA pair.

Remove FIPS and WLAN common criteria

Disable FIPS and WLAN common criteria to allow for standard operation of the device.

This procedure is applicable in scenarios where FIPS compliance is no longer required, and the device needs to operate in a non-FIPS mode.

Before you begin

Ensure that the device is currently configured for FIPS and WLAN common criteria.

Procedure

	Command or Action	Purpose
Step 1	Enter global configuration mode. **Example:** `Device# configure terminal`	
Step 2	Configure the AP DTLS version. **Example:**	

	Command or Action	Purpose
	`Device(config)# ap dtls-version dtls_1_2`	
Step 3	Configure the AP DTLS ciphersuite. **Example:** `Device(config)# ap dtls-cipher ECDHE-ECDSA-AES256-GCM-SHA384`	
Step 4	Disable WLAN CC on the controller. **Example:** `Device(config)# no wireless wlancc`	
Step 5	Disable the authorization key for FIPS. **Example:** `Device(config)# no fips authorization-key`	
Step 6	Return to privileged EXEC mode. **Example:** `Device(config)# end`	
Step 7	Save the configuration. **Example:** `Device# write memory`	
Step 8	Reload the device. **Example:** `Device# reload`	

The device is now configured to operate without FIPS and WLAN common criteria.

Remove LSC provisioning

Before you begin

Wait for the standby AP to come up.

Procedure

	Command or Action	Purpose
Step 1	Enter global configuration mode. **Example:** `Device# configure terminal`	
Step 2	Disable AP LSC provisioning parameters. **Example:** `Device(config)# no ap lsc-provision`	
Step 3	Disable AP DTLS cipher suite.	

	Command or Action	Purpose
	Example: `Device(config)# no ap dtls-cipher ECDHE-ECDSA-AES256-GCM-SHA384`	
Step 4	Disable the DTLS version. **Example:** `Device(config)# no ap dtls-version dtls_1_2`	
Step 5	Disable the wireless management trustpoint. **Example:** `Device(config)# no wireless management trustpoint`	
Step 6	Save the configuration changes. **Example:** `Device# copy running-config startup-config`	
Step 7	Reload the internal AP. **Example:** `Device# wireless ewc-ap ap reload`	

The LSC provisioning has been successfully removed from the wireless controller.

Import a CA certificate to the trustpool (GUI)

PKI Trustpool Management is used to store a list of trusted certificates (either downloaded or built in) used by the different services on the controller. This is also used to authenticate a multilevel CA certificate. The built in CA certificate bundle in the PKI trustpool receives automatic updates from Cisco if they are not current, are corrupt, or if certain certificates need to be updated.

Perform this task to manually update the CA certificates in the PKI trustpool.

Note If your LSC has been issued by an intermediate CA, you must import the complete chain of CA certificates into the trustpool. Otherwise, you will not be able to provision the APs without the complete chain being present on the controller. The import step is not required if the certificate has been issued by a root CA.

Follow these steps to import a CA certificate to the trustpool using GUI:

Procedure

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

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

Step 3 Click **Import**.

Step 4 In the **CA Certificate** field, copy and paste the CA certificate. Link together the multiple CA certificates in **.pem** format.

Step 5 Click **Apply to Device**.

Import a CA certificate to the trustpool

Import a CA certificate to establish trust relationships for secure communications.

The trustpool stores CA certificates that the device uses to validate certificates presented by other entities during secure communications.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Import the root certificate to the trustpool.

Example:

```
Device(config)# crypto pki trust pool import terminal
% Enter PEM-formatted CA certificate.
% End with a blank line or "quit" on a line by itself.
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
Aug 23 02:47:33.450: %PKI-6-TRUSTPOOL_DOWNLOAD_SUCCESS:
Trustpool Download is successful
```

You need to paste the CA certificate from the **digicert.com**.

Step 3 Return to privileged EXEC mode.

Example:

```
Device(config)# end
```

The CA certificate is successfully imported to the trustpool and can be used for certificate validation.

Clean the CA certificates imported in trustpool (GUI)

Procedure

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

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

Step 3 Click **Clean**.

Note
This erases the downloaded CA certificate bundles. However, it does not erase the built-in CA certificate bundles.

Step 4 Click **Yes**.

Clean CA certificates imported in trustpool (CLI)

You cannot delete a specific CA certificate from the trustpool. However, you can clear all the CA certificates that are imported to the Trustpool.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Erase the downloaded CA certificate bundles.

Example:

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

This command does not erase the built-in CA certificate bundles.

Step 3 Return to privileged EXEC mode.

Example:

```
Device(config)# end
```

Alternatively, you can also press Ctrl-Z to exit global configuration mode.

Create a new trustpoint dedicated to a single CA certificate

Establish a trustpoint that is specifically configured for a single Certificate Authority (CA) certificate to enable secure PKI operations.

A trustpoint represents a Certificate Authority (CA) or identity certificate that is used for PKI operations. Creating a dedicated trustpoint for a single CA certificate helps organize and manage different certificate authorities in the network.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Create a trustpoint.

Example:

```
Device(config)# crypto pki trustpoint tp-name
```

Example:

```
Device(config)# crypto pki trustpoint tp_name
```

Step 3 Create an enrollment terminal for the trustpoint.

Example:

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

Step 4 Exit from the trustpoint configuration.

Example:

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

Step 5 Authenticate the trustpoint.

Example:

```
Device(config)# crypto pki authenticate tp-name
```

Example:

```
Device(config)# crypto pki authenticate tp_name
<<< PASTE CA-CERT in PEM format followed by quit >>>
```

The trustpoint is now created and authenticated with the CA certificate, ready for PKI operations.

Verify LSC configuration

Use show commands to verify Local Security Certificate (LSC) configuration. View wireless management trustpoint details and Local Security Certificate (LSC) provision-related configuration for your access points.

To view the wireless management trustpoint details, use this command:

```
Device# show wireless management trustpoint

Trustpoint  Name : microsoft-ca
Certificate Info : Available
Certificate Type : LSC
Certificate Hash : 9e5623adba5307facf778e6ea2f5082877ea4beb
 Private key Info : Available
```

To view the Local Security Certificate (LSC) provision-related configuration details for an AP, use this command:

```
Device# show ap lsc-provision summary

AP LSC-provisioning : Disabled
Trustpoint used for LSC-provisioning : microsoft-ca
LSC Revert Count in AP reboots : 10

AP LSC Parameters :
```

```
Country : IN
State : KA
City : BLR
Orgn : ABC
Dept : ABC
Email : support@abc.com
Key Size : 2048

AP LSC-provision List : Enabled
Total number of APs in provision list: 3

Mac Address
-----------
0038.df24.5fd0
2c5a.0f22.d4ca
e4c7.22cd.b74f
```

```
Device# show ap lsc-provision summary

AP LSC-provisioning : Disabled
Trustpoint used for LSC-provisioning : lsc-root-tp
Certificate chain status : Available
Number of certs on chain : 2
Certificate hash : 7f9d05183deecac4e5a79db65d538245685e8e30
LSC Revert Count in AP reboots : 1

AP LSC Parameters :
Country : IN
State : KA
City : BLR
Orgn : ABC
Dept : ABC
Email : support@abc.com
Key Size : 2048
EC Key Size : 384 bit

AP LSC-provision List :

Total number of APs in provision list: 2

Mac Addresses :
--------------
1880.90f5.1540
2c5a.0f70.84dc
```

Configure management trustpoint to LSC

Procedure

Step 1 Choose **Administration** > **Management** > **HTTP/HTTPS**.

Step 2 In the **HTTP Trust Point Configuration** section, set **Enable Trust Point** to the **Enabled** state.

Step 3 From the **Trust Points** drop-down list, choose the appropriate trustpoint.

Step 4 Save the configuration.

Configure management trustpoint to LSC (CLI)

Configure management trustpoint to enable Local Significant Certificate (LSC) authentication for access points.

After LSC provisioning, the APs will automatically reboot and join at the LSC mode after bootup. Similarly, if you remove the AP LSC provisioning, the APs reboot and join at non-LSC mode.

In EWC, the internal APs will not automatically reboot. You should manually reboot the internal AP to make it work in LSC and non-LSC mode.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure the management trustpoint to LSC.

Example:

```
Device(config)# wireless management trustpoint trustpoint-name
```

Example:

```
Device(config)# wireless management trustpoint microsoft-ca
```

The internal AP will not able to join before a reload, so follow the steps given below to reload the internal AP.

Step 3 Return to privileged EXEC mode.

Example:

```
Device(config)# end
```

Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Step 4 Save the configuration.

Example:

```
Device# copy running-config startup-config
```

Step 5 Reload the internal AP.

Example:

```
Device# wireless ewc-ap ap reload
```

This will also reload the controller on the AP.

The management trustpoint is now configured for LSC authentication, and access points will join using LSC mode after rebooting.

AP certificate renewal (LSC)

AP certificate renewal (LSC)

AP certificate renewal (LSC) is a feature that

- allows the renewal of Locally Significant Certificates (LSCs) for Access Points before their expiration
- ensures that the APs can continue to provide seamless services by renewing their certificates in a timely manner
- enables the controller to orchestrate this process to minimize service disruption. The process focuses on automatic renewal mechanisms that do not require manual intervention.

LSC provisioning and renewal methods

This feature supports LSC provisioning for Access Points from two sources. You can provision from the controller through proxy-enrollment or from the Cisco Catalyst Center through secure AP onboarding. These certificates are crucial for your Access Points because they authenticate network communications. This renewal process is essential. Without a valid certificate, Access Points may lose network connectivity and affect network services.

The controller uses these methods to renew certificates:

- **Gradual Succession**: A method where Access Points are renewed one at a time, which is suitable when the number of Access Points that are due for renewal is under a certain threshold.
- **Staggered Rollover**: Access Points are renewed in a staggered fashion, minimizing the impact on radio coverage when the number of Access Points is larger.
- **One-Shot Renewal**: All affected Access Points are renewed simultaneously, which can be disruptive and should be used as a last resort.

Benefits of AP certificate renewal (LSC)

- **Automated Renewal Process**: Reduces the need for manual certificate updates, ensuring continuous service.
- **Seamless Network Operations**: Minimizes network downtime by renewing certificates before they expire.
- **Enhanced Security**: Maintains a high level of security by ensuring that all Access Points have valid certificates.
- **Scalable Management**: Supports staggered AP renewal to reduce impact on network operations.

Requirements for AP certificate renewal (LSC)

Configure the controller and access points to use locally significant certificates before you proceed with certificate renewal.

- Provision the locally significant certificates through the controller (proxy-enrollment) or Cisco Catalyst Center-PNP workflows.
- Define the maintenance windows if scheduling is required for renewal.

Restrictions for AP certificate renewal (LSC)

These restrictions for access point certificate renewal (Local Significant Certificate) are:

- Only one Local Significant Certificate is supported per access point.
- Enable either staggered or one-shot renewal, not both.
- Local Significant Certificate renewal applies to Cisco Wave 2 access points and newer models; older access points do not support this feature.
- The staggered algorithm does not apply to access points in bridge mode. All Local Significant Certificate renewals for bridge mode access points occur at the same time.

Configure AP certificate auto-renewal (LSC) (GUI)

Follow these steps to configure AP certificate auto-renewal (LSC):

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points** > **LSC Provision**.

Step 2 In the **LSC Renewal** section, check the **LSC Auto-Renewal** check box and follow these steps:

a. Enter a value for due time. The valid range is 5 to 60.

b. From the **Renewal Schedule** drop-down list, select an existing calendar profile schedule or click the icon to create a new calendar profile. For more information about creating a calendar profile, see the **Configuring a Calendar Profile (GUI)** and **Configuring a Calendar Profile (CLI)**.

c. Use the slider to enable **Syslog** messages for the LSC renewal updates.

d. From the **Renewal Mode** drop-down list, choose either *One Shot* or *Staggered*.

- If you choose One Shot, all impacted AP LSCs renew in a single iteration.
- If you choose Staggered, the system staggers the LSC renewal configuration for the APs and follow these steps:
  - Enter a value for the iteration expiry to set the expiry time for each iteration.
  - From the **AP LSC Renewal per Iteration** drop-down list, choose one of the following options to configure the percentage of APs to be renewed per iteration: 5%, 15%, or 25%.
  - Enable the **Client Steering** slider to move clients attached to APs undergoing renewal to other APs.
  - Enable the **Client Deauthentication** slider to deauthenticate clients associated with the AP before it starts upgrading.

- From the **Accounting Percentage** drop-down list, select the percentage of APs that should join the controller after each iteration to consider the renewal successful.
- Use the slider to configure **Accounting Action**. If you select **Terminate**, the renewal stops if the configured percentage of APs does not join the controller. If you select **Ignore**, the renewal continues regardless.

Step 3 Click **Apply**.

Configure AP certificate renewal (LSC) (CLI)

Follow these steps to configure AP certificate renewal (LSC) in the controller:

Procedure

Step 1 Enter configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure LSC provisioning on an AP.

Example:

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

Step 3 Configure AP certificate renewal.

Example:

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

Step 4 Renew AP LSCs automatically within the specified number of days.

Example:

```
Device(config)# ap lsc-provision renew due-time number-of-days
```

The valid range is from 5 to 60 days, with a default value of 30 days.

Step 5 Renew all AP LSCs in a single iteration.

Example:

```
Device(config)# ap lsc-provision renew one-shot
```

Note
The one-shot AP LSC renewal feature is disabled by default.

Step 6 Renew AP LSCs automatically in a staggered manner.

Example:

```
Device(config)# ap lsc-provision renew staggered timeout iteration-timeout-in-mins
```

Staggered AP LSC renewal is enabled by default.

Note
You cannot use one-shot and staggered renewal methods at the same time.

iteration-timeout-in-mins: The valid range is from 5 to 60 minutes.

Step 7 Configure time schedule for auto-renewal within a maintenance window.

Example:

```
Device(config)# ap lsc-provision renew scheduler calendar-profile
```

No scheduler is enabled by default.

When no scheduler is applied, the device auto-renews AP LSCs at 24-hour intervals and is triggered daily at 12:00 AM local time.

Note
You must configure the calendar-profile definition beforehand. For more information, see **Configuring a Calendar Profile (CLI)**.

You have successfully configured AP certificate renewal (LSC).

Configure forced renewal of AP certificate (LSC) for individual or multiple APs (GUI)

Follow these steps to configure forced renewal of AP certificate (LSC) for individual or multiple APs via GUI:

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Bulk AP Provisioning**.
Step 2 On the **Select Parameters** page, check the **Renew LSC** check box to renew the LSC for all selected APs.
Step 3 Click **Next**.

Configure forced renewal of AP Certificate (LSC) based on site tag (GUI)

Before you begin

Follow these steps to configure force renewal of AP certificate (LSC) based on site tag:

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Tags**.
Step 2 In the **Site** tab, check the check box for the required site tag.
Step 3 Click **Renew LSC** and follow these steps:

a. Enter the due time in days. The value must be between 1 and 60.

b. Click **Apply to Device**.

Configure forced renewal of AP Certificate (LSC) based on site tag (CLI)

Follow these steps to configure the forced renewal of an AP certificate (LSC) based on a site tag using the CLI:

Procedure

Step 1 Enable privileged EXEC mode.

Example:

```
Device# enable
```

Enter your password if prompted.

Step 2 Renew a specific site-tag AP that is set to expire within the specified time.

Example:

```
Device# ap lsc renew due-time number-of-days site-tag site-tag-name
```

number-of-days: The valid range is from 1 to 60 days.

The configuration of the forced renewal of an AP Certificate (LSC) based on a site tag is complete.

Configure forced renewal of all APs (GUI)

Follow these steps to configure forced renewal of all APs (GUI):

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points**.

Step 2 From the **Select an Action** drop-down list, choose **Renew LSC**.

The **Renew LSC** pop-up window is displayed.

Step 3 Enter a due time value in minutes between 5 and 60.

Step 4 Click **Apply to Device**.

Verify AP certificate renewal (LSC)

Lists the various show commands and their outputs during the verification of the AP Certificate Renewal (LSC).

Verify LSC configuration

To verify LSC provision-related configuration details for an AP, use this command:

```
Device# show ap lsc-provision info
AP name     Ethernet MAC     Radio MAC      LSC authentication  LSC workflow    Cert expiry
   Last renew attempt  Last renew failure
=============================================================================================
AP-abc      1111.2222.3333  aaaa.bbbb.ccc0  Port-802.1x         PNP Onboarding  <time-stamp>
  <time-stamp>/NA     reason-code
AP-123      1234.5678.9012  dddd.eeee.fff0  DTLS                SCEP proxy      <time-stamp>
  <time-stamp>/NA     reason-code
AP-xyz      1010.1010.1010  abcd.efab.cde0  DTLS, Port-802.1x   SCEP proxy      <time-stamp>
  <time-stamp>/NA     reason-code
                                      0.0.0.0                          372            64
              AGL          Enabled
```

Verify staggered LSC renewal upgrade configuration

To verify progress and status of staggered LSC renewal upgrade, use this command:

```
Device# show ap upgrade
Status: In progress
From version:
To version: Unknown

Started at: 10/23/2025 08:16:01 IST
Configured percentage: 15
Percentage complete: 0
Expected time of completion: 10/23/2025 08:24:01 IST

Client steering: Enabled
Client de-authentication: Enabled
Accounting percentage: 90%
Iteration expiry time: 15 minutes

Progress Report
---------------
Iterations
----------
Iteration              Start time                        End time                   AP
count
-------------------------------------------------------------------------------------------------
0                      10/23/2025 08:16:01 IST           10/23/2025 08:16:01 IST     0

1                      10/23/2025 08:16:01 IST           10/23/2025 08:18:05 IST     1

2                      10/23/2025 08:18:05 IST           ONGOING                     0


Upgraded
--------
Number of APs: 0
AP Name                          Radio MAC              Iteration       Status
    Site
-------------------------------------------------------------------------------------------------
```

```
In Progress
-----------
Number of APs: 1
AP Name                          Radio MAC
-------------------------------------------------
1815W                            00be.7517.d980

Remaining
---------
Number of APs: 6
AP Name                          Radio MAC
-------------------------------------------------
9166-1                           10f9.20fd.5400
non-9120-1                       488b.0a47.d8c0
9136_1                           687d.b45f.1610
9120-Dev                         a00f.3704.f3a0
9162-antenna                     ecf4.0c0e.9920
9176+alpine                      ecf4.0c92.bac0

APs not handled by Rolling AP Upgrade
-------------------------------------
AP Name                          Radio MAC               Status          Reason for not
handling by Rolling AP Upgrade
-------------------------------------------------------------------------------------------------------------
```

MIC and LSC APs joining the controller

Support for MIC and LSC APs joining the controller

Support for MIC and LSC access points joining the controller is an authorization policy feature that

- allows MIC APs to join LSC-deployed controllers without requiring LSC provisioning
- enables LSC and MIC APs to coexist on the same controller simultaneously, and
- eliminates the need to provision LSC on MIC APs before moving them to LSC-deployed controllers.

Authorization policy behavior changes

The authorization policy behavior differs between software releases:

- **Cisco IOS XE Bengaluru 17.4.1 and earlier**: If your APs have default certificates (Manufacturing Installed Certificates [MIC] or Secure Unique Device Identifier [SUDI]), they cannot join an LSC-deployed controller, where the management certificate of the controller is an LSC. To resolve this issue, provision LSC on your APs. Use the provisioning controller before you move them to the LSC-deployed controller.
- **Cisco IOS XE Bengaluru 17.5.1 onwards**: The new authorization policy configuration allows MIC APs to join the LSC-deployed controller, so that LSC APs and MIC APs can coexist on the controller.

Recommendations and limitations

When you configure the CA server with manual enrollment to accept certificate signing request (CSR), the controller monitors for the CA server response. If the CA server does not respond for 10 minutes, the fallback mode activates.

- Cisco Wave 2 APs regenerate CSR, and a fresh CSR is sent to the CA server.
- Cisco IOS APs restart, and then Cisco IOS APs send a fresh CSR, which is in turn sent to the CA server.

The locally significant certificate (LSC) feature on the controller does not work with password challenge authentication. Therefore, for LSC to work, you must disable password challenge on the CA server.

If you are using Microsoft CA, use Windows Server 2012 or later as the CA server.

MIC and LSC access point authentication

Summary

The Manufacturer Installed Certificate (MIC) and Local Significant Certificate (LSC) access point authentication configuration involves these stages:

- Controller: Manages authentication policies and trustpoint configuration for secure access point connections
- Access points: Require certificate-based authentication to join the controller
- LSC trustpoint: Provides local significant certificate authentication mechanism
- AP certificate policy: Defines authentication requirements and allowed access point lists

Workflow

The key components involved in the MIC and LSC access point authentication configuration are:

1. The network administrator configures the LSC trustpoint on the LSC deployed controller using CLI.

   Configure LSC on the controller (CLI), on page 32

2. The network administrator enables the AP certificate policy on access points using CLI.

   Enable the AP certificate policy on the APs (CLI), on page 32

3. The network administrator configures the AP policy certificate using the GUI interface.

   Configure the AP policy certificate (GUI), on page 34

4. The network administrator configures the allowed list of APs to join the controller using CLI.

   Configure the allowed list of APs to join the controller (CLI), on page 34

Result

Access points are properly authenticated and authorized to join the controller with secure certificate-based authentication enabled.

Configure LSC on the controller (CLI)

The server certificate used by the controller for CAPWAP-DTLS (Control and Provisioning of Wireless Access Points - Datagram Transport Layer Security) is based on the following configuration.

Before you begin

- Ensure that you enable LSC by setting the appropriate trustpoints for the following wireless management services:
  - AP join process: CAPWAP DTLS server certificate
  - Mobility connections: Mobility DTLS certificate
  - NMSP (Network Mobility Services Protocol) and CMX (Connected Mobile Experiences) connections: NMSP TLS certificate

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure the LSC trustpoint in the LSC-deployed controller.

Example:

```
Device(config)# wireless management trustpoint trustpoint-name
```

Enable the AP certificate policy on the APs (CLI)

Enable AP certificate policy during CAPWAP-DTLS handshake to allow MIC APs to join the controller.

- If the management trustpoint is a locally significant certificate (LSC), by default, manufacturing installed certificate (MIC) APs fail to join the controller. This configuration acts as an enable or disable configuration knob that allows MIC APs to join the controller.
- This configuration is a controller authorization to allow APs to join MIC at the time of Datagram Transport Layer Security (DTLS) handshake.

To prevent manufacturing installed certificate (MIC) expiry failures, ensure that you configure a policy, as shown here:

- Create a certificate map and add the rules:

```
configure terminal
crypto pki certificate map map1 1
issuer-name co Cisco Manufacturing CA
```

Note You can add multiple rules and filters under the same map. The rule mentioned in the example above specifies that any certificate whose issuer-name contains *Cisco Manufacturing CA* (case insensitive) is selected under this map.

- Use the certificate map under the trustpool policy:

```
configure terminal
crypto pki trustpool policy
match certificate map1 allow expired-certificate
```

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure the trustpoint name for the controller certificate chain.

Example:

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

Note
The allow-mic-ap trustpoint command is required only for the virtual controller (Cisco Catalyst 9800-CL Wireless Controller for Cloud). In all the other appliance controller platforms, the default certificate is selected. This default certificate is manufacturer-installed SUDI.

Step 3 Enable the AP certificate policy during CAPWAP-DTLS handshake.

Example:

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

Step 4 Enable the AP certificate policy as MIC.

Example:

```
Device(config)# ap auth-list ap-cert-policy mac-address H.H.H policy-type mic
```

Example:

```
Device(config)# ap auth-list ap-cert-policy mac-address 1111.1111.1111 policy-type mic
```

The AP certificate policy is now enabled and configured for MIC APs to join the controller during CAPWAP-DTLS handshake.

Configure the AP policy certificate (GUI)

Procedure

Step 1 Choose **Configuration > Wireless > Access Points**

Step 2 In the **All Access Points** window, click **AP Certificate Policy**.

Step 3 In the **AP Policy Certificate** window, complete the following actions:

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

b) From the **Trustpoint Name** drop-down list, choose the required trustpoint.

c) Click **Add MAC or Serial Number** to add a MAC address or a serial number manually or through a .csv file.
The **Add MAC or Serial Number** window is displayed.

d) Click the **AP Authlist Type** and enter the MAC address or the serial number. Upload the .csv file or enter the MAC address in the list box.
The newly added MAC address and serial numbers are displayed under **List of MAC Address and Serial Numbers**.

e) Click **Apply**.

The AP certificate policy is added to the **AP Inventory** window.

Note
To add a new AP with MIC, perform Step 1 to Step 3 described in Configuring the AP Policy Certificate (GUI) section. To add a new AP with LSC, perform the procedure described in the Configuring AP LSC Provision List (GUI) and Step 1 to Step 3 in the Configuring the AP Policy Certificate (GUI) section.

Configure the allowed list of APs to join the controller (CLI)

Create an allowed list of access points that can join the controller based on MAC address or serial number authentication.

The allowed list of APs can either be populated based on the Ethernet MAC address or based on the serial number of the APs.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure the AP certificate policy based on the Ethernet MAC address or based on the assembly serial number of the AP.

Example:

```
Device(config)# ap auth-list ap-cert-policy mac-address AP-Ethernet-MAC-address policy-type
 mic
```

Example:

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

Example:

```
Device(config)# ap auth-list ap-cert-policy mac-address 00b0.e192.0d98 policy-type mic
```

The AP certificate policy is configured and the specified access points are added to the allowed list for joining the controller.

Verifying the configuration status

To verify if the APs have been authorized by the AP certificate policy, use this command:

```
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
```

To verify the AP certificate policy on the MAC address and the serial number of the AP, use these commands:

```
Device# show ap auth-list ap-cert-policy mac-address
MAC address      AP cert policy
---------------------------------
1111.2222.3333   MIC
```

```
Device# show ap auth-list ap-cert-policy serial-number
Serial number    AP cert policy
-------------------------------
F1234567890      MIC
```

Note If you set an invalid trustpoint (not SSC), the **allow-mic-ap policy** does not enable. If you set an invalid trustpoint, this error displays on the console:

```
Device(config)# ap auth-list ap-cert-policy allow-mic-ap trustpoint lsc-root-tp
Dec 18 07:38:29.944: %CERT_MGR_ERRMSG-3-CERT_MGR_GENERAL_ERR: Chassis 1 R0/0: wncd: General
 error: MIC AP Policy trustpoint: 'lsc-root-tp' cert-chain type is LSC, It must be either
MIC or vWLC-SSC
```

LSC fallback APs

LSC fallback APs

LSC fallback is a state that

- occurs when an AP configured with LSC for CAPWAP fails to establish DTLS connection after reaching the maximum number of retry attempts
- causes the AP to revert to its default certificate (MIC) for CAPWAP authentication, and

- provides a backup authentication method when LSC-based CAPWAP connection attempts fail.

LSC fallback process

When you configure an AP with LSC for CAPWAP but it fails to establish a DTLS connection, the AP reboots. The AP then retries for a certain number of times. For information on how to configure an AP with LSC, see Configure AP join attempts with LSC certificate (CLI), on page 9.

The AP falls back to its default certificate (MIC) for CAPWAP after maximum number of failures. The AP fallback state is referred to as the LSC fallback.

Note MIC is also known as SUDI certificate.

Troubleshoot LSC fallback state

This task enables you to identify access points in LSC fallback state and understand the recovery process when APs fail to establish proper LSC connections with the controller.

When an AP in LSC fallback state joins the controller, it generates specific syslog messages and is held in a misconfigured state. The AP does not broadcast WLAN or SSID configurations in this state, which permits the admin to examine the reason for previous failures and recover APs.

Procedure

Step 1 Identify the syslog message generated when an AP in LSC fallback state joins the controller.

Example:

```
Jun 15 23:24:14.836: %APMGR_TRACE_MESSAGE-3-WLC_GEN_ERR: Chassis 1 R0/0: wncd: Error
in AP: 'AP2c5a.0f70.84dc' with address 70db.9888.cc20 is joined with MIC, while configuration

requires LSC. No WLANs will be pushed.
```

The controller allows such an AP to be joined with MIC (when AP certificate policy allows it) and AP is held in misconfigured state.

Note
The AP does not broadcast WLAN or SSID configurations in such state. This permits the admin to examine the reason for previous failures and recover APs.

Step 2 Use **show wireless summary** to identify LSC fallback APs.

Example:

```
Device# show wireless summary
…
Access Point Summary
…
DTLS LSC fallback APs     20 (No WLANs will be pushed to these APs)
…
For more information on DTLS LSC fallback APs,
    execute 'wireless config validate' and look for reported errors in
```

```
    'show wireless config validation status' CLI output.

Use 'show ap config general | inc AP Name | LSC fallback' to list DTLS LSC fallback APs.
Examine LSC fallback reasons / DTLS handshake failures with LSC then
    issue 'ap lsc dtls-fallback clear-certificate / clear-flag' to recover APs
```

You have successfully identified LSC fallback APs and understand the commands available for further investigation and recovery.

Recover from LSC fallback

Recover APs from LSC fallback state and restore normal LSC functionality for CAPWAP DTLS connections.

When LSC fallback occurs, APs may require recovery actions to restore normal operation. Recovery options depend on whether you want to retain the LSC certificate or clear it completely.

Procedure

Choose one of the following recovery methods based on your requirements:

- To clear the LSC fallback flag and retain the LSC certificate, use the **ap lsc dtls-fallback clear-flag** command to instruct the AP to reload.

  Note
  The AP reuses the LSC for CAPWAP DTLS connection post the reload.

- To clear the LSC certificate completely, use the **ap lsc dtls-fallback clear-certificate** command to clear LSC and instruct the AP to reload.

  Note
  The AP uses MIC for CAPWAP-DTLS post the reload. If LSC is used for Dot1x port authentication then further recovery is needed on switch port for AP authentication.

Note

- The **ap lsc dtls-fallback clear-flag** command is sufficient to retain LSC on AP. Both **ap lsc dtls-fallback clear-flag** and **ap lsc dtls-fallback clear-certificate** commands are not required at the same time.
- APs must be in connected state when issuing the recovery command. You will need to reissue the command, if any **LSC fallback** AP joins afterwards.

The access point reloads and recovers from the LSC fallback state according to the selected recovery method.

Configuring controller self-signed certificate for wireless AP join

Use cases for controller self-signed certificate for wireless AP join

You need controller self-signed certificates in specific circumstances to enable wireless APs to join the controller successfully.

Controller self-signed certificate use cases

These situations require controller self-signed certificates:

- The Cisco Catalyst 9800-CL platform is not equipped with manufacturer-installed SUDI certificates. Configure self-signed certificates on these controllers.
- Some APs running earlier software and using a Manufacturer Installed Certificate (MIC) issued by a SHA1 Cisco Trusted CA cannot join controllers with SHA2 SUDI certificates. During the CAPWAP join process, these APs display a bad certificate error and fail the DTLS handshake.

Workaround: To support AP upgrades, configure a self-signed certificate for the controller as a workaround for the second use case. After updating all APs, delete the self-signed certificates. Then, revert to the SUDI certificate.

Note This workaround does not apply to Embedded Wireless Controllers running on Catalyst 9000 series switches. It is only valid for hardware appliance controllers such as Cisco Catalyst 9800-40, 9800-80, and 9800-L.

Prerequisites for controller self-signed certificate for wireless AP join

- Ensure that the VLAN interface is up and that the IP address is reachable.
- Ensure that the **ip http server** is enabled. For more information, see Enabling HTTP Server .
- Set the **clock calendar-valid** command appropriately. For more information, see *Configure clock calendar.*
- Check whether the PKI CA server is configured. If it is, delete the existing CA server configuration.

Note The **show crypto pki server** command output should not display anything.

Configure clock calendar (CLI)

Set the clock calendar to ensure accurate timekeeping on the device.

This configuration is necessary for time-sensitive operations and logging on the device.

Before you begin

Access to the device with appropriate privileges to enter global configuration mode.

Follow these steps to configure clock calendar:

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Enable clock calendar.

Example:

```
Device(config)# clock calendar-valid
```

Step 3 Exit configuration mode.

Example:

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

The clock calendar is now configured and operational on the device.

Enable HTTP server using CLI

Enable the HTTP server to allow web-based management of the device.

This configuration is applicable for devices that require HTTP access for management purposes.

Before you begin

Ensure you have administrative access to the device.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Enable the HTTP server on your IP or IPv6 system.

Example:

```
Device(config)# ip http server
```

Enables the HTTP server on your IP or IPv6 system, including a Cisco web browser user interface. By default, the HTTP server uses the standard port 80.

Step 3 Enable the secure HTTP server on your IP or IPv6 system.

Example:

```
Device(config)# ip http secure-server
```

Enables the secure HTTP server on your IP or IPv6 system, providing encrypted access to the web interface.

Step 4 Exit configuration mode.

Example:

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

The HTTP server is now enabled, allowing web-based management of the device.

Configure CA server (CLI)

Deploy a CA server to manage certificates for devices in the network.

This configuration is essential for environments that require secure communication through certificates.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Generate RSA keys for the CA server.

Example:

```
Device(config)# crypto key generate rsa general-keys modulus size_of_key_module label
keypair_name
```

Configures a certificate for the controller.

When you generate RSA keys, you are prompted to enter a modulus length. A longer modulus length might be more secure, but it takes longer to generate and to use.

Note
The recommended key-pair name is *WLC_CA* and key modulus is *2048* bits.

Step 3 Enable the IOS certificate server.

Example:

```
Device(config)# crypto pki server certificate_server_name
```

Enables IOS certificate server.

Note
The *certificate_server_name* must be the same name as the *keypair_name*.

Step 4 Configure the issuer name for the CA certificate.

Example:

```
Device(cs-server)# issuer-name O=Cisco Virtual Wireless LAN Controller, CN=CA-vWLC
```

Configures X.509 distinguished name for the issuer CA certificate.

Note
You need to configure the same *issuer-name* as suggested for AP join.

Step 5 Grant certificate requests automatically.

Example:

```
Device(cs-server)# grant auto
```

Grants certificate requests automatically.

Step 6 (Optional) Specify the hash function for the signature used in the granted certificates.

Example:

```
Device(cs-server)# hash sha256
```

Specifies the hash function for the signature used in the granted certificates.

Step 7 (Optional) Specify the lifetime in days of a CA certificate.

Example:

```
Device(cs-server)# lifetime ca-certificate time-interval
```

Specifies the lifetime in days of a CA certificate.

Step 8 (Optional) Specify the lifetime in days of a granted certificate.

Example:

```
Device(cs-server)# lifetime certificate time-interval
```

Specifies the lifetime in days of a granted certificate.

Step 9 Set the CA key and CA certificate archive format and password.

Example:

```
Device(cs-server)# database archive pkcs12 password 0 cisco123
```

Sets the CA key and CA certificate archive format and password to encrypt the file.

Step 10 Enable the certificate server.

Example:

```
Device(cs-server)# no shutdown
```

Enables the certificate server.

Note
Issue this command only after you have completely configured your certificate server.

Step 11 Return to privileged EXEC mode.

Example:

```
Device(cs-server)# end
```

Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

The CA server is now configured and ready to manage certificates for devices in the network.

Configure trustpoint (CLI)

Configure a trustpoint to enable secure communication with a Certificate Authority (CA).

This configuration is necessary for devices that require secure communications and certificate management.

Before you begin

Ensure you have access to the device and the necessary permissions to configure trustpoints.

Follow these steps to configure trustpoint using CLI commands:

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Generate RSA keys for the trustpoint.

Example:

```
Device(config)# crypto key generate rsa exportable general-keys modulus
size-of-the-key-modulus label label
```

When you generate RSA keys, you are prompted to enter a modulus length. A longer modulus length might be more secure, but it takes longer to generate and to use.

Step 3 Create a new trustpoint for an external CA server.

Example:

```
Device(config)# crypto pki trustpoint trustpoint_name
```

Here, *trustpoint_name* refers to the trustpoint name.

Note
Ensure that same names are used for key-pair (*label*) and *trustpoint_name*.

Step 4 Map RSA key with that of the trustpoint.

Example:

```
Device(ca-trustpoint)# rsakeypair RSA_key
```

Maps RSA key with that of the trustpoint.

- RSA_key—Refers to the RSA key pair label.
- key_size—Refers to the signature key length. The value ranges from 360 to 4096.

Step 5 Create subject name parameters for the trustpoint.

Example:

```
Device(ca-trustpoint)# subject-name subject_name
```

Specifies the subject name for the trustpoint.

Step 6 Check revocation.

Example:

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

Specifies whether to check for certificate revocation.

Step 7 Specify the hash algorithm.

Example:

```
Device(ca-trustpoint)# hash sha256
```

Specifies the hash algorithm to be used.

Step 8 Specify the serial number.

Example:

```
Device(ca-trustpoint)# serial-number
```

Specifies the serial number for the trustpoint.

Step 9 (Optional) Set certificate key-usage purpose.

Example:

```
Device(ca-trustpoint)# eku request server-auth client-auth
```

Sets the extended key usage for the certificate.

Step 10 Enable password for the trustpoint.

Example:

```
Device(ca-trustpoint)# password 0 password
```

Step 11 Enroll the URL for the CA server.

Example:

```
Device(ca-trustpoint)# enrollment url url
```

Replace the dummy IP with management VLAN interface IP of the controller where CA server is configured.

Step 12 Exit the configuration mode.

Example:

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

The trustpoint is now configured and ready for use with the CA server.

Authenticate and enroll the PKI trustpoint with CA server

Authenticate and enroll the PKI trustpoint to establish a secure connection with the Certification Authority (CA) server.

This procedure is used in environments where a PKI trustpoint needs to be authenticated and enrolled with a Certification Authority (CA) server for certificate management.

Before you begin

Ensure that the Certification Authority (CA) server is reachable and the trustpoint is properly configured.

Follow these steps to authenticate and enroll the PKI trustpoint with CA server:

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Authenticate the PKI trustpoint with the CA server.

Example:

```
Device(config)# crypto pki authenticate trustpoint-name
Certificate has the following attributes:
Fingerprint MD5: 64C5FC9A C581D827 C25FC3CF 1A7F42AC
Fingerprint SHA1: 6FAFF812 7C552783
6A8FB566 52D95849 CC2FC050
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
```

Fetches the CA certificate.

Step 3 Enroll the PKI trustpoint for a client certificate.

Example:

```
Device(config)# crypto pki enroll trustpoint-name
Enter following answers for UI interaction:
% Include an IP address in the subject name? [no]: no
Request certificate from CA? [yes/no]: yes
```

Step 4 Exit global configuration mode.

Example:

```
Device(config)# end
```

Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.

The PKI trustpoint is now authenticated and enrolled with the Certification Authority (CA) server, allowing for secure certificate management.

Tag wireless management trustpoint name

Tag a wireless management trustpoint name for identification and management purposes.

This configuration is used in environments where wireless management trustpoints need to be clearly identified for management and security.

Before you begin

Ensure you have the necessary privileges to enter global configuration mode.

Procedure

	Command or Action	Purpose
Step 1	Enter global configuration mode. **Example:** `Device# configure terminal`	
Step 2	Tag the wireless management trustpoint name. **Example:** `Device(config)# wireless management trustpoint trustpoint-name`	
Step 3	Exit global configuration mode. **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.

The wireless management trustpoint name is successfully tagged and can be used for management purposes.

Disable PKI server

Disable the PKI server to prevent it from issuing certificates.

This procedure is used in scenarios where the PKI server is no longer needed or must be temporarily disabled.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Create a new server for an external CA server.

Example:

```
Device(config)# crypto pki server certificate-server-name
```

The *certificate-server-name* refers to the server name.

Note
Here, server_name refers to the server name.

Step 3 Disable the certificate server.

Example:

```
Device(cs-server)# shutdown
```

Update purpose string to \

Step 4 Return to privileged EXEC mode.

Example:

```
Device(cs-server)# end
```

Alternatively, you can also press Ctrl-Z to exit global configuration mode.

The PKI server is now disabled and will not issue certificates.

Verify controller certificates for wireless AP join

Use these commands to verify controller certificates for wireless access point (AP) join.

To view the CA server details, use the command:

```
Device# show crypto pki server
Certificate Server WLC_CA:
Status: enabled
State: enabled
Server's configuration is locked (enter "shut" to unlock it)
Issuer name: O=Cisco Virtual Wireless LAN Controller, CN=CA-vWLC
CA cert fingerprint: 79A3DBD5 59A7E384 73ABD152 C133F4E2
Granting mode is: auto
Last certificate issued serial number (hex): 1
CA certificate expiration timer: 12:04:00 UTC Mar 8 2029
CRL NextUpdate timer: 18:04:00 UTC Mar 11 2019
Current primary storage dir: nvram:
Database Level: Minimum - no cert data written to storage
```

To view the trustpoint details, use this command:

```
Device# show crypto pki trustpoint ewlc-tp1 status
Trustpoint ewlc-tp1:
...
State:
Keys generated ..... Yes (General Purpose, exportable)
Issuing CA authenticated ..... Yes
Certificate request(s) ..... Yes
```

To view the wireless management trustpoint details, use this command:

```
Device# do show wireless management trustpoint
Trustpoint Name : ewlc-tp1
Certificate Info : Available
Certificate Type : SSC
Certificate Hash : 4a5d777c5b2071c17faef376febc08398702184e
Private key Info : Available
FIPS suitability : Not Applicable
```

To view the Hypertext Transfer Protocol (HTTP) server status, use this command:

```
Device# show ip http server status | include server status
HTTP server status: Enabled
HTTP secure server status: Enabled
```