Locally Significant Certificates

Information About Locally Significant Certificates

This module explains how to configure the Cisco Embedded Wireless Controller on Catalyst Access Points and Lightweight Access Points (LAPs) to use the Locally Significant Certificate (LSC). If you choose the Public Key Infrastructure (PKI) with LSC, you can generate the LSC on the APs and embedded wireless controllers. You can then use the certificates to mutually authenticate the embedded wireless controller and the APs.

In Cisco embedded wireless controllers, you can configure the embedded wireless controller to use an LSC. Use an LSC if you want your own PKI to provide better security, have control of your Certificate Authority (CA), and define policies, restrictions, and usages on the generated certificates.

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

The new LSC certificates, both CA and device certificates, must be installed on the controller.

With the help of SCEP, CA certificates are received from the CA server. During this point, there are no certificates in the controller. After the **get** operation of obtaining the CA certificates, are installed on the controller. The same CA certificates are also pushed to the APs when the APs are provisioned with LSCs.

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, reuse the existing RSA keypair name. Regenerating a new RSA keypair with an existing RSA keypair name will make all the certificates associated with the existing RSA keypair invalid.
- Manually remove the old PKI certificate configurations first, before reusing the existing RSA keypair name for the new PKI certificate.

Device Certificate Enrollment Operation

For both the LAP and the controller that request a CA-signed certificate, the certRequest is sent as a PKCS#10 message. The certRequest contains the Subject Name, Public Key, and other attributes to be included in the X.509 certificate, and must be digitally signed by the Private Key of the requester. These are then sent to the CA, which transforms the certRequest into an X.509 certificate.

The CA that receives a PKCS#10 certRequest requires additional information to authenticate the requester's identity and verify if the request is unaltered. (Sometimes, PKCS#10 is combined with other approaches, such as PKCS#7 to send and receive the certificate request or response.)

The PKCS#10 is wrapped in a PKCS#7 Signed Data message type. This is supported as part of the SCEP client functionality, while the PKCSReq message is sent to the controller. Upon successful enrollment operation, both the CA and device certificates are available on the controller.

Certificate Provisioning on Lightweight Access Point

In order to provision a new certificate on LAP, while in CAPWAP mode, the LAP must be able to get the new signed X.509 certificate. In order to do this, it sends a certRequest to the controller, which acts as a CA proxy and helps obtain the certRequest signed by the CA for the LAP.

The certReq and the certResponses are sent to the LAP with the LWAPP payloads.

Both the LSC CA and the LAP device certificates are installed in the LAP, and the system reboots automatically. The next time when the system comes up, because it is configured to use LSCs, the AP sends the LSC device certificate to the controller as part of the JOIN Request. As part of the JOIN Response, the controller sends the new device certificate and also validates the inbound LAP certificate with the new CA root certificate.

What to Do 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

- LSC workflow is different in FIPS+WLANCC mode. CA server must support Enrollment over Secure Transport (EST) protocol and should be capable of issuing EC certificates in FIPS+WLANCC mode.
- Elliptic Curve Digital Signature Algorithm (ECDSA) cipher works only if both AP and controller are having EC certificates, provisioned with LSC.
- EC certificates (LSC-EC) can be provisioned only if CA server supports EST (and not SCEP).
- FIPS + CC security modes is required to be configured in order to provision EC certificate.

Provisioning Locally Significant Certificates

Configuring RSA Key for PKI Trustpoint

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**crypto key generate rsa** [**exportable**] **general-keys modulus** *key_size* **label** *RSA_key* **Example:** `Device(config)# crypto key generate rsa exportable general-keys modulus 2048 label lsc-tp`	Configures RSA key for PKI trustpoint. **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*: RSA key pair label.

Step 3	**end**
	Example:
	`Device(config)# end`
		Returns to privileged EXEC mode.

Configuring PKI Trustpoint Parameters

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**crypto pki trustpoint** *trustpoint_name* **Example:** `Device(config)# crypto pki trustpoint microsoft-ca`	Creates a new trustpoint for an external CA server. Here, *trustpoint_name* refers to the trustpoint name.
Step 3	**enrollment url** *HTTP_URL* **Example:** `Device(ca-trustpoint)# enrollment url http://CA_server/certsrv/mscep/mscep.dll`	Specifies the URL of the CA on which your router should send certificate requests. **url** *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	**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`
		Creates subject name parameters for the trustpoint.

Step 5	**rsakeypair** *RSA_key key_size* **Example:** `Device(ca-trustpoint)# rsakeypair ewlc-tp1`	Maps RSA key with that of the trustpoint. • *RSA_key*: RSA key pair label. • *key_size*: Signature key length. Range is from 360 to 4096.

Step 6	**revocation** {**crl** | **none** | **ocsp**}
	Example:
	`Device(ca-trustpoint)# revocation none`
		Checks revocation.

Step 7	**end**
	Example:
	`Device(ca-trustpoint)# end`
		Returns to privileged EXEC mode.

Authenticating and Enrolling a PKI Trustpoint (GUI)

Procedure

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

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

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

a) In the **Label** field, enter the RSA key label.
b) In the **Enrollment URL** field, enter the enrollment URL.
c) Check the **Authenticate** check box to authenticate the Public Certificate from the enrollment URL.
d) In the **Subject Name** section, enter the **Country Code**, **State**, **Location**, **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.

Authenticating and Enrolling the PKI Trustpoint with CA Server (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**crypto pki authenticate** *trustpoint_name* **Example:** `Device(config)# crypto pki authenticate microsoft-ca`	Fetches the CA certificate.

Step 3	**yes**
	Example:
	`Device(config)# % Do you accept this certificate? [yes/no]:`
	`yes Trustpoint CA certificate accepted.`	

Step 4	**crypto pki enroll** *trustpoint_name* **Example:**	Enrolls the client certificate.

	Command or Action	Purpose

	`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	**password** **Example:** `Device(config)# abcd123`	Enters a challenge password to the CA server.
Step 6	**password** **Example:** `Device(config)# abcd123`	Re-enters a challenge password to the CA server.

Step 7	**yes**
	Example:
	`Device(config)# % Include the router serial number`
	`in the subject name? [yes/no]: yes`	

Step 8	**no**
	Example:
	`Device(config)# % Include an IP address`
	`in the subject name? [no]: no`	

Step 9	**yes**
	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	**end**
	Example:
	`Device(config)# end`
		Returns to privileged EXEC mode.

Configuring AP Join Attempts with LSC Certificate (GUI)

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**.

Configuring AP Join Attempts with LSC Certificate (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap lsc-provision join-attempt** *number_of_attempts* **Example:** `Device(config)# ap lsc-provision join-attempt 10`	Specifies the maximum number of AP join failure attempts with the newly provisioned LSC certificate. When the number of AP joins exceed the specified limit, AP joins back with the Manufacturer Installed Certificate (MIC).

Step 3	**end**
	Example:
	`Device(config)# end`
		Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Subject-Name Parameters in LSC Certificate

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose

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

Step 3	**end**
	Example:
	`Device(config)#` **`end`**
		Returns to privileged EXEC mode.

Configuring Key Size for LSC Certificate

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

Step 2	**ap lsc-provision key-size**{ **2048** | **3072** | **4096**}}
	Example:
	`Device(config)#` **`ap lsc-provision key-size`**
	 `2048`
		Specifies the size of keys to be generated for the LSC on AP.

Step 3	**end**
	Example:
	`Device(config)#` **`end`**
		Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Trustpoint for LSC Provisioning on an Access Point

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**ap lsc-provision trustpoint** *tp-name* **Example:** `Device(config)# ap lsc-provision trustpoint microsoft-ca`	Specifies the trustpoint with which the LCS is provisioned to an AP. *tp-name*: The trustpoint name.

Step 3	**end**
	Example:
	`Device(config)# end`
		Returns to privileged EXEC mode.

Configuring 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**.

Configuring an AP LSC Provision List (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap lsc-provision mac-address** *mac-addr* **Example:** `Device(config)# ap lsc-provision mac-address 001b.3400.02f0`	Adds the AP to the LSC provision list. **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	**end**
	Example:
	`Device(config)# end`
		Returns to privileged EXEC mode.

Configuring 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**.

Configuring LSC Provisioning for All APs (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap lsc-provision** **Example:** `Device(config)# ap lsc-provision`	Enables LSC provisioning for all APs. By default, LSC provisioning is disabled for all APs.

Step 3	**end**
	Example:
	`Device(config)# end`
		Returns to privileged EXEC mode.

Configuring LSC Provisioning for the APs in the Provision List

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**ap lsc-provision provision-list** **Example:** `Device(config)# ap lsc-provision provision-list`	Enables LSC provisioning for a set of APs configured in the provision list.

Step 3	**end**
	Example:
	`Device(config)# end`
		Returns to privileged EXEC mode. 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 Configuring LSC Provisioning and Management Trustpoint, on page 12.
3. Remove Federal Information Processing Standard (FIPS) and WLANCC. For more information, refer to Removing FIPS and WLAN Common Criteria, on page 13.
4. Remove LSC provisioning. For more information, refer to Removal of LSC Provisioning, on page 14.

Configuring LSC Provisioning and Management Trustpoint

Before you begin

When EWC HA pair is used note the name of the Standby Access Point. Use the **show chassis** command.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap lsc-provision** **Example:** `Device(config)# ap lsc-provision`	Configures the AP LSC Provisioning parameters.
Step 3	**wireless management trustpoint** *trustpoint_name* **Example:** `Device(config)# wireless management trustpoint trustpoint-name`	Configures the management trustpoint to LSC.

	Command or Action	Purpose
Step 4	**copy running-config startup-config** **Example:** `Device#  copy running-config startup-config`	Saves the configuration. Wait for the standby AP to join the controller. The HA pair will not be formed at this point.
Step 5	**wireless ewc-ap ap reload** **Example:** `Device# wireless ewc-ap ap reload`	Reloads the internal AP. This will also reload the controller on the AP. Standby AP starts the controller and becomes new Active for HA pair.

Removing FIPS and WLAN Common Criteria

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap dtls-version dtls_1_2** **Example:** `Device(config)# ap dtls-version dtls_1_2`	Configures the AP DTLS version.
Step 3	**ap dtls-cipher** *ECDHE-ECDSA-AES256-GCM-SHA384* **Example:** `Device(config)# ap dtls-cipher ECDHE-ECDSA-AES256-GCM-SHA384`	Configures the AP DTLS ciphersuite.
Step 4	**no wireless wlancc** **Example:** `Device(config)# no wireless wlancc`	Disables WLAN CC on the controller.
Step 5	**no fips authorization-key** **Example:** `Device(config)# no fips authorization-key`	Disables the authorization key for FIPS.

Step 6	**end**
	Example:
	`Device(config)# end`
		Returns to privileged EXEC mode.

Step 7	**write memory** **Example:**	Saves the configuration.

	Command or Action	Purpose
	`Device# write memory`	
Step 8	**reload** **Example:** `Device# reload`	Reloads the internal AP to move on to non-FIPS and non-CC mode.

Removal of LSC Provisioning

Before you begin

Wait for the standby AP to come up.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**no ap lsc-provision** **Example:** `Device(config)# no ap lsc-provision`	Disables AP LSC provisioning parameters.
Step 3	**no ap dtls-cipher ECDHE-ECDSA-AES256-GCM-SHA384** **Example:** `Device(config)# no ap dtls-cipher ECDHE-ECDSA-AES256-GCM-SHA384`	Disables AP DTLS cipher suite.
Step 4	**no ap dtls-version dtls_1_2** **Example:** `Device(config)# no ap dtls-version dtls_1_2`	Disables the DTLS version.
Step 5	**no wireless management trustpoint** **Example:** `Device(config)# no wireless management trustpoint`	Disables the wireless management trustpoint.
Step 6	**copy running-config startup-config** **Example:** `Device# copy running-config startup-config`	Saves the configuration changes.

	Command or Action	Purpose
Step 7	**wireless ewc-ap ap reload** **Example:** `Device# wireless ewc-ap ap reload`	Reloads the internal AP.

Importing 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.

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**.

Importing a CA Certificate to the Trustpool (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

Step 2	**crypto pki trust pool import terminal**
	Example:
	`Device(config)# crypto pki trust pool import terminal`
	`% Enter PEM-formatted CA certificate.`
		Imports the root certificate. For this, you need to paste the CA certificate from the **digicert.com**.

	Command or Action	Purpose

	`% 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`	

Step 3	**end**
	Example:
	`Device(config)# end`
		Returns to privileged EXEC mode.

Cleaning 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**.

Cleaning 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

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**crypto pki trustpool clean** **Example:** `Device(config)# crypto pki trustpool clean`	Erases the downloaded CA certificate bundles. However, it does not erase the built-in CA certificate bundles.

	Command or Action	Purpose

Step 3	**end**
	Example:
	`Device(config)# end`
		Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Creating a New Trustpoint Dedicated to a Single CA Certificate

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**crypto pki trustpoint** *tp-name* **Example:** `Device(config)# crypto pki trustpoint tp_name`	Creates a trustpoint.
Step 3	**enrollment terminal** **Example:** `Device(ca-trustpoint)# enrollment terminal`	Creates an enrollment terminal for the trustpoint.
Step 4	**exit** **Example:** `Device(ca-trustpoint)# exit`	Exits from the truspoint configuration.

Step 5	**crypto pki authenticate** *tp-name*
	Example:
	`Device(config)# crypto pki authenticate tp_name`
	`<<< PASTE CA-CERT in PEM format followed by quit >>>`
		Authenticates the trustpoint.

Verifying LSC Configuration

To view the details of the wireless management trustpoint, use the following 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 LSC provision-related configuration details for an AP, use the following 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
```

Configuring Management Trustpoint to LSC (GUI)

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.

Configuring Management Trustpoint to LSC (CLI)

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

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless management trustpoint** *trustpoint_name* **Example:** `Device(config)# wireless management trustpoint microsoft-ca`	Configures the management trustpoint to LSC. The internal AP will not able to join before a reload, so follow the steps given below to reload the internal AP.

Step 3	**end**
	Example:
	`Device(config)# end`
		Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Step 4	**copy running-config startup-config** **Example:** `Device# copy running-config startup-config`	Saves the configuration.
Step 5	**wireless ewc-ap ap reload** **Example:** `Device# wireless ewc-ap ap reload`	Reloads the internal AP. This will also reload the controller on the AP.

Information About MIC and LSC Access Points Joining the Controller

Overview of Support for MIC and LSC Access Points Joining the Controller

In Cisco IOS XE Bengaluru 17.4.1 and earlier releases, APs with a default certificate (Manufacturing Installed Certificates [MIC]) or Secure Unique Device Identifier [SUDI]) fail to join a Locally Significant Certificate-deployed (LSC-deployed) controller, where the management certificate of the controller is an LSC. To resolve this issue, you must provision LSC on these APs using the provisioning controller before moving them to the LSC-deployed controller.

From Cisco IOS XE Bengaluru 17.5.1 onwards, the new authorization policy configuration allows MIC APs to join the LSC-deployed controller, so that the LSC and MIC APs can coexist in the controller at the same time.

Recommendations and Limitations

- When the CA server is configured with manual enrollment (manual intervention) to accept Certificate Signing Request (CSR), the controller waits for the CA server to send the pending response. If there is no response from the CA server for 10 minutes, the fallback mode comes into effect.
  - 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.
- Locally significant certificate (LSC) on the controller does not work on the password challenge. Therefore, for LSC to work, you must disable password challenge on the CA server.
- If you are using Microsoft CA, we recommend that you use Windows Server 2012 or later as the CA server.

Configuration Workflow

1. #unique_893
2. #unique_894
3. #unique_895
4. #unique_896

Configuring LSC on the Controller (CLI)

The server certificate used by the controller for CAPWAP-DTLS 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 and CMX connections: NMSP TLS certificate

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**[no] wireless management trustpoint** *trustpoint-name* **Example:** `Device(config)# wireless management trustpoint trustpoint-name`	Configures the LSC trustpoint in the LSC-deployed controller.

Enabling the AP Certificate Policy on the APs (CLI)

- If the management trustpoint is an LSC, by default, 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 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

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**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`	Configures the trustpoint name for the controller certificate chain. **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	**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 during CAPWAP-DTLS handshake.
Step 4	**ap auth-list ap-cert-policy** {**mac-address** *H.H.H* | **serial-number** *serial-number-ap*} **policy-type mic** **Example:** `Device(config)# ap auth-list ap-cert-policy mac-address 1111.1111.1111 policy-type mic`	Enables the AP certificate policy as MIC.

Configuring 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.

Configuring the Allowed List of APs to Join the Controller (CLI)

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

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap auth-list ap-cert-policy** {**mac-address** *AP-Ethernet-MAC-address* | **serial-number** *AP-serial-number*} **policy-type mic** **Example:** `Device# ap auth-list ap-cert-policy mac-address 00b0.e192.0d98 policy-type mic`	Configures the AP certificate policy based on the Ethernet MAC address or based on the assembly serial number of the AP.

Verifying the Configuration Status

To verify if the APs have been authorized by the AP certificate policy, use the following 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 the following 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** is not enabled. If you set an invalid trustpoint, the following error is displayed 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 Access Points

Information About LSC Fallback APs

When an AP is configured with LSC for CAPWAP but fails to establish DTLS connection, the AP reboots and retries for certain number of times. For information on how an AP configures with LSC, see Configuring AP Join Attempts with LSC Certificate (CLI), on page 7.

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

Note MIC is also known as SUDI certificate.

Troubleshooting LSC Fallback State

When an AP in **LSC fallback** state joins the controller, the following syslog is generated:

```
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.

You can identify the **LSC fallback** APs using **show wireless summary** as follows:

```
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
```

Recovery Steps

- Use the **ap lsc dtls-fallback clear-flag** to clear the LSC fallback flag on AP and instruct AP to reload.

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

- Use the **ap lsc dtls-fallback clear-certificate** to clear LSC and instruct 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.