Workflow to Configure a Trustpoint for a Self-signed Certificate on Catalyst 9800-CL

The Catalyst 9800-CL or the virtual controller does not have a Manufacturing Installed Certificate (MIC). On Day 0, you have to explicitly generate a self-signed certificate, get it signed by your local IOS CA and import it using the Simple Certificate Enrollment Protocol (SCEP). Next, you need to map it to the wireless management interface, since the CAPWAP connection between the AP and controller uses the wireless management interface for authentication.

The configuration is possible using the CLI or Day 0 wizard on the WebUI of the virtual controller. However, we recommend that you use the script below to complete the configuration.

Before you begin

- Ensure that the VLAN interface is up and the IP is reachable.

```
Device#show ip interface brief
Interface              IP-Address      OK?    Method Status      Protocol
GigabitEthernet0/1     unassigned      YES    unset  up          up
GigabitEthernet0/2     unassigned      YES    NVRAM  administratively down up
VLAN1                  unassigned      YES    NVRAM  administratively down  up
VLAN56                 9.9.56.40       YES    NVRAM  up          up
```

```
Device#ping 9.9.56.40
 Type escape sequence to abort.
     Sending 5, 100-byte ICMP Echos to 9.9.56.40, timeout is 2 seconds:
     !!!!!
     Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

- Enable the HTTP Server

  The certificate server supports Simple Certificate Enrollment Protocol (SCEP) over HTTP. The HTTP server must be enabled on the virtual controller for the certificate server to use SCEP. If the HTTP server is not enabled, only manual PKCS12 enrollment is supported.

  To enable the HTTP server, use the following command:

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

- Synchronize the clock

  Mark the hardware clock as authoritative using the following command:

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

Create a certificate for the AP to join the virtual controller. It can either be created automatically when you select the option on the Day 0 flow or by using a command.

To configure the self-signed certificate, complete this command on the controller:

	Command	Purpose
Step 1	**enable** `Device>enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** `Device#config t`	Enters global configuration mode.
Step 3	**wireless management interface vlan** *Vlan interface number* `Device(config)#wireless management interface vlan 122`	Specify the interface for the wireless management interface.
Step 4	**end** `Device#end`	Returns to privileged EXEC mode.
Step 5	**wireless config vwlc-ssc key-size** [**1024** | **2048** | **3072**] **signature-algo** [**sha1** | **sha256** | **sha384**]**password** [**0** | **7**] *password* `Device#wireless config vwlc-ssc key-size 2048 signature-algo sha256 password 0 cisco123`	Automates the creation of a self-signed certificate to be used for AP Join and assigns it to the Wireless Management Interface (WMI) automatically. **Note** This exec cli is not supported on native IPv6 deployments. We recommend that you use the Day 0 to generate a self-signed certificate for the Catalyst 9800-CL or manually configure the trustpoint.

Step 6	**show wireless management trustpoint**
	`Device#show wireless management trustpoint`
	`Trustpoint Name : ewlc-default-tp`
	`Certificate Info : Available`
	`Certificate Type : SSC`
	`Certificate Hash :`
	`e55e61b683181ff0999ef317bb5ec7950ab86c9e`
	`Private key Info : Available`
		Verifies the certificate installation.

This completes the trustpoint configuration for AP Join from the virtual controller.

In case you had skipped the Day 0 flow on the GUI for certificate/trustpoint configuration APs will not able to join. To configure this, on the virtual controller WebUI, go to **Configuration** > **Security** > **PKI Management**. In the **AP SSC Trustpoint** section and click **Generate** and enter the relevant details. For APs to join, map this trustpoint to the controller's wireless management interface. Refer to Assign Trustpoint for AP Join with MIC or SSC using the WebUI for further details.