Overview of Trustpoints on Catalyst 9800

Note The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Certificate-based authentication is a method to identify a user, device or machine before they can be granted access to a network. A wireless network comprising of a Wireless LAN Controller (WLC), hereafter referred to as controller, Access Points (AP) and clients, commonly uses certificate-based authentication to validate the identities of peer devices when participating in services such as AP Join, Management Access and Web Authentication. Each service can use different sets of client and server certificates.

But how do devices get their digital identities?

To begin with, each participating device (controller, access point, and client) has its own device certificate and a Certificate Authority (CA) certificate that validates its authenticity. A closer look at the certificates available on the Catalyst 9800 controller shows the following types:

- Cisco installed Manufacturing Installed Certificate (MIC) - On physical appliances (Catalyst 9800-40, Catalyst 9800-80, Catalyst 9800-L), these are by default, factory installed, and widely known as the Cisco installed MIC or Secure Unique Device Identifier (SUDI) device certificate. In addition to this, controllers and access points have a Cisco Manufacturing Certificate Authority (CA) certificate that is used to sign and validate device certificates.
    - Wireless LAN Controller self-signed certificate for virtual controller - The Catalyst 9800-CL, (the virtual instance of the controller) does not come with any manufacturing certificate. In the absence of an identity certificate, it relies on the self-signed certificate that has to be generated by the Day 0 wizard or manually using a script and validated by the local Cisco IOS Certificate Authority. This acts as the Catalyst 9800-CL's local identity certificate and is used for AP Join, Mobility connection and Network Mobility Services Protocol-Connected Mobile Experience (NMSP-CMX) connections.
- IOS-XE device self-signed certificate- The default self-signed certificate is auto-generated during the controller's initial startup if any HTTPS, SSH or NETCONF service is configured on the controller.

The above default certificates provide an easy and out of the box method of early trust between peer devices. However, if you want to provide better security, then you can consider using

- Third-party validated certificates, including Locally Significant Certificates (LSC).

Third-party certificates require a PKI framework that enables encryption of public keys and digital certificates. Along with different authentication protocols, the PKI model works with Certificate Authorities, Root Certificates and asymmetric key encryption to ensure that the digital certificates are securely exchanged over encrypted tunnels during a client and server exchange.

On Catalyst 9800 controllers, these digital certificates are configured and held in containers called trustpoints and used when the devices initiate a secure communication with the other network devices. Trustpoint is one of the most important configuration entities for a PKI client. A trustpoint includes the identity certificate of the CA that signed the device certificate, CA-specific trustpoint configuration parameters, and an association with an enrolled identity certificate.

Trustpoints provide a mapping between the identity certificate and the application/service that needs the certificate. For example, for the SSL/HTTPS server functionality, the *ip http secure-trustpoint <trustpoint name>* tells the controller what identity certificate to present to an SSL client. Depending on your requirement, you can configure many trustpoints.

A Case for Trustpoints

Identity validation using certificates spans across a range of functions and protocols in the Catalyst 9800 wireless environment. Certificates are primarily used for authentication when an Access Point joins the controller using with CAPWAP with DTLS, for Web Administration and Web Authentication using HTTP with TLS and for Local EAP Authentication. Certificates are also used when the controller communicates with Cisco Connected Mobile Experience (CMX), Cisco Digital Network Architecture Center (DNA Center) and Digital Network Architecture Spaces (DNA Spaces). Some of these exchanges require additional configuration whereas others do not require any action from your side.

These scenarios are outlined in the following sections along with their default behaviour and recommended actions.

Use a Trustpoint to Secure Web Administration on Catalyst 9800

The admin interface of the Catalyst 9800 web user interface (WebUI) is usually accessed securely over HTTPS from a remote workstation over a web browser for web administration purposes.

Default behaviour

When you enable a secure HTTP connection, the controller automatically picks one of its certificates, to the best of its judgement, even if none is configured for the HTTP secure server. This can be a self-signed certificate that may be used for future SSL handshakes between the remote workstation (client) and the HTTPS server. However, a self-certified (self-signed) certificate does not provide adequate security, and the connecting client

generates a notification that the certificate is self-certified, and the user has the opportunity to accept or reject the connection.

If you want a dedicated third-party certificate to be used for future SSL handshakes between the controller and the connecting client, it is best to configure a trustpoint to use this certificate. Once an identity certificate is configured and found, it always takes precedence over a self-signed certificate.

We recommend that you point/map the HTTPS application to use controller's trusted third-party certificate for increased security.

Use a Trustpoint to Secure Web Authentication on Catalyst 9800

Web authentication is a Layer 3 authentication method available on the Catalyst 9800 controller and widely used for guest access configuration. Web authentication allows users to get authenticated through a web browser on a wireless client, with minimal configuration on the client side.

Depending on the web policy configured on the controller, your guest user completes the authentication either with a username and password, or by entering the email address or by getting redirected to a particular web page before getting access to the guest portal. This portal is hosted on the controller internally as a predefined page, or hosted on the controller as a customized page, or hosted on an external server.

Many a times these guest WLANs are open with no Layer 2 authentication, hence we need to provide a means to protect the user credentials between the controller and the guest client.

Default behaviour

When guest users try to access the web policy page on a Windows system using the browser, they receive a security warning because of the standard self-signed certificate that is installed on the controller by default. In some other cases, systems that use the automatic web portal detection system, display a pop-up with the login page, once they detect that a user is connected to a web authentication network.

To avoid this warning for guest users, we recommend you deploy a third-party certificate signed by a trusted certificate authority because disabling the https encryption might compromise the security.

Additionally, for clients to trust the web authentication certificate, we recommend that you define a hostname that matches the Common Name (CN) in the certificate. This is possible both from the controller's CLI or the GUI.

You can configure it through the global parameter setting for webauth, where you can define the hostname for the Virtual IP address being used for web authentication. For instructions on how to configure it, refer here in *Recommendations and Limitations.*

Use a Trustpoint to Secure AP Join and Configure Mobility Tunnel on Catalyst 9800

Access Point (AP) Join

The controller and access points use CAPWAP and DTLS protocols to manage and encrypt data exchange with one another. The management interface on the controller handles the communication between these two entities.

Default behaviour

All appliance controller platforms (Catalyst 9800-40, 9800-80, 9800-L) and access points are shipped with a Cisco-installed Manufacturing Installed Certificate (MIC) device certificate. Additionally, controllers and access points have a Cisco Manufacturing Certificate Authority (CA) certificate that is used to sign and validate device certificates.

After an access point discovers a controller, it needs to join the controller. An AP can join a controller only after the controller and the AP verify each other's identity as part of the DTLS handshake.

A variation of the MIC on the Catalyst 9800-CL (the virtual controller) is a self-signed certificate, as the virtual controller does not have a MIC. The virtual controller relies on the self-signed certificate that has to be generated by the Day 0 wizard when you select it, once the wireless management interface has been enabled and the country configuration has been setup for AP Join. You can also automate this with a script. Refer to the Workflow to Configure a Trustpoint for a Self-signed Certificate on Catalyst 9800-CL to know how to set up a trustpoint on the Catalyst 9800-CL for AP Join.

Optionally, APs can use Locally Significant Certificates (LSC) to prove their identity. LSCs are created by an enterprise PKI managed by your company and are installed on the controller and the AP to provide more granular control. By default, LSC certificates are not installed on the controller and APs.

Mobility tunnel

Mobility Tunnel is a secure link between two controllers where data is encrypted and exchanged using CAPWAP and DTLS. When you configure a peer controller, the MIC certificate is used to create the tunnel. However, in case of a Catalyst 9800-CL, in the absence of a MIC, the self-signed certificate is used to configure a peer controller and will require you to add the self-signed certificate hash when configuring the mobility group.

Use a Trustpoint for Secure Connection between Catalyst 9800 and Cisco CMX

Cisco Connected Mobile Experiences (CMX) is a software solution that uses location and other intelligence from Cisco wireless infrastructure to generate analytics and deliver relevant services to customers on their mobile devices. Cisco CMX allows client authentication through the custom portal. This is similar to configuring web authentication where clients are redirected to the customized portal hosted on CMX.

Cisco CMX communicates with the Catalyst 9800 wireless controller using the Network Mobility Services Protocol (NMSP), which runs over a connection-oriented (TLS) transport. This transport provides a secure 2-way connectivity and is convenient when both the controller and CMX are on- premise and there is direct IP connectivity between them.

The controller verifies the peer and the host based on the certificate that is sent by the CMX when a connection is established. However, Root CAs are not preinstalled on the controller.

Use a Trustpoint to Secure Connection between Catalyst 9800 and Cisco DNA Center

The Cisco DNA Center can be used to deploy a wireless network using a mix of Catalyst 9800 and Catalyst 9800-CL devices.

When the DNA Center discovers the controller, a pre-defined trustpoint is pushed to the controller.

```
sdn-network-infra-iwan
```

This installs the DNA Center certificate on the controller and issues a certificate for Assurance. You can check the status using the command below.

```
show crypto pki certificates verbose sdn-network-infra-iwan
```

```
show crypto pki trustpoint sdn-network-infra-iwan status
```

Use a Trustpoint to Secure Connection between Catalyst 9800 and Cisco DNA Spaces

You can connect the Catalyst 9800 Series controller to Cisco DNA Spaces using the WLC Direct Connect option. However, the controller must have a third-party certificate that is used for identity validation when the controller tries to connect to Cisco DNA Spaces using the WLC Direct Connect option. Add the certificate using the following commands:

```
Device#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)#ip name-server<DNS ip>
Device(config)#ip domain-lookup
Device(config)#crypto pki trustpool import url https://www.cisco.com/security/pki/trs/ios.p7b

Reading file from http://www.cisco.com/security/pki/trs/ios.p7b
Loading http://www.cisco.com/security/pki/trs/ios.p7b !!!
% PEM files import succeeded.
```

Use a Trustpoint for Local EAP Authentication on Catalyst 9800

Local EAP is an authentication method that allows users and wireless clients to be authenticated locally on the controller. It is designed for use in remote offices that want to maintain connectivity to wireless clients when the backend system becomes disrupted or the external authentication server goes down. When you enable local EAP, the controller serves as the authentication server and the local user database, so it removes dependence on an external authentication server. Local EAP retrieves user credentials from the local user database or the LDAP backend database to authenticate users. Local EAP supports LEAP, EAP-FAST, EAP-TLS, P EAPv0/MSCHAPv2, and PEAPv1/GTC authentication between the Catalyst 9800 controller and wireless clients.

Local EAP authentication requires the controller to set up a trustpoint as the controller needs to send the certificate for the client. Since clients do not trust the controller's default certificate, you will need to install a certificate trustpoint on the Catalyst 9800 controller that the client will trust (or import it manually in the client trust store).