SUDI99 Certificate Support

SUDI99 Certificate Support

Cisco Catalyst 9800 Series Wireless Controllers use Secure Unique Device Identity (SUDI) certificates as device certificates for authentication during secure connection handshakes. These certificates are provisioned in a secure hardware chip, which can hold multiple certificates, during the manufacturing process.

Note Some of the certificates used in the controller and AP platforms are expiring in May 2029 and require migration to a new set of certificates. SUDI99 certificate support is addressing this migration scenario. SUDI99 is valid until December 2099.

The Cisco IOS XE software supports two slots for initializing SUDI certificates from the secure hardware chip. This SUDI99 migration change will rearrange certificate-to-trustpoint mapping as follows:

Table 1: Existing Software Selection for SUDI Trustpoint Certificates

Trustpoint Name	Software Selection Among Programmed Certificate Chains
CISCO_IDEVID_SUDI	CMCA2 SHA2 SUDI (SHA2-2037)
CISCO_IDEVID_SUDI_LEGACY	CMCA SHA1 SUDI

Table 2: New Software Selection for SUDI Trustpoint Certificates

Trustpoint Name	Software Selection Among Programmed Certificate Chains
CISCO_IDEVID_SUDI	CMCA-III SHA2 SUDI99
CISCO_IDEVID_SUDI_LEGACY	CMCA2 SHA2 SUDI (SHA2-2037)

Caution Performing device authentication using expired certificates may lead to service disruption.

The following table lists the SUDI99 certificate and software support:

Table 3: SUDI99 Certificate and Software Support

Cisco Catalyst 9800 Controllers	SUDI99 Certificate Support	Software Support for SUDI99 Migration
Cisco Catalyst 9800-CL Wireless Controller for Cloud	Not supported.	—
Cisco Catalyst 9800 Series Wireless Controllers • 9800-40 • 9800-80 • 9800-L	Supported	Yes. From Cisco IOS XE Cupertino 17.7.1.
Cisco Embedded Wireless Controller on Catalyst Access Points. • 9105AXI • 9115AXI • 9115AXE • 9117AXI • 9120AXI • 9120AXE • 9120AXP • 9130AXI • 9130AXE	Supported	Yes. From Cisco IOS XE Cupertino 17.7.1.
Cisco Embedded Wireless Controller on Catalyst Switches • 9300 Series • 9400 Series • 9500 Series • 9500H Series	Not supported.	—

Backward Compatibility

The Cisco Catalyst 9800 Series Wireless Controllers have a default wireless management trustpoint. Some applications use this management trustpoint certificate. If a device (AP or controller) cannot validate the SUDI99 certificate, then the controller uses an older certificate (SHA2-2037) as its device certificate for that particular connection.

For NMSP-TLS connections with Cisco CMX, the client certificate is not validated in default security mode. However, in FIPS mode, Cisco CMX validates the controller certificate.

If Cisco CMX is deployed in FIPS mode, explicitly install the new SUDI CA certificates on the Cisco CMX running the earlier version of Cisco CMX or upgrade Cisco CMX to the latest version.

Some applications, such as HTTPS, RADSEC, and WebAuth, do not use SUDI certificate as their default trustpoint. But, it is possible to configure SUDI trustpoint explicitly in them. The SUDI refresh program alters the certificate selection for such services. However, there is no functional impact.

Restrictions

If a SUDI99 certificate is incorrectly programmed in a device, it is rejected during trustpoint initialization at bootup, and trutpoint-to-certificate mapping falls back to the old behaviour. User can verify the SUDI certificate status using the **show platform sudi pki** command.

Disabling SUDI99 Migration Using CLI

The SUDI99 certificate is set as the default trustpoint in supported hardware units. You can disable it using the **no platform sudi cmca3** command. In high availability (HA) deployments, form the HA pair, and then run the command. Then, save the configuration and reload the controller to disable the SUDI certificate and fall back to the older trustpoint certificate.

To check the certificate validation status, use the **show platform sudi pki** command.

Disabling SUDI99 Migration (GUI)

SHA1 SUDI certificates on hardware controllers have an imminent expiry date and devices using expired certificates face disruption in service. To ensure a smooth migration to the latest SUDI99 certificate issued by CMCA-III authority, the controllers have been programmed with newer certificates in their secure hardware chip. These certificates are enabled by default and are valid till December 2099.

Follow the procedure given below, if you do not wish to migrate at this point.

Procedure

Step 1 On the **Configuration > Security > PKI Management > Trustpoint** tab, go to the **SUDI Status** section.

Step 2 Disable the **Cisco Manufacturing CA III certificate** to continue using the older certificate that is mapped to an existing Trustpoint.

Step 3 Click **Apply**

What to do next

Reload the device for the configuration to take effect.