SUDI99 Certificate Support

SUDI certificates

A Secure Unique Device Identity (SUDI) is a device credential that

- provides device-specific authentication during secure connection handshakes
- is provisioned in a secure hardware chip during manufacturing, and
- supports multiple certificates for interoperability with diverse network environments.

Feature history

This table provides release and related information about the feature explained in this section.

This feature is also available in all the releases subsequent to the one in which they are introduced in, unless noted otherwise.

Table 1: Feature history for SUDI99 certificate support

Feature Name	Release Information	Feature Description
SUDI99 certificate support	Cisco IOS XE Dublin 17.7.1	This feature allows a network administrator to use SUDI99 certificates for authentication during secure connection handshakes enhancing security through device-specific credentials

SUDI certificates validate device identity, ensuring only genuine devices connect to Cisco networks. They play a crucial role in maintaining the security of network infrastructure.

Note Some existing SUDI certificates, such as those used in controller and AP platforms, are set to expire in May 2029. To ensure continued secure authentication, the SUDI refresh program migrates SW-SUDI SHA1 certificates to the new SUDI99 certificates with extended validity.

Software selection for SUDI trustpoint certificates

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 2: 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 3: 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 Avoid using expired certificates for device authentication to prevent service disruption.

SUDI99 certificate and software support

The table lists the SUDI99 certificate and software support:

Table 4: 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 Controllers	SUDI99 Certificate Support	Software Support for SUDI99 Migration
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

Backward compatibility refers to the Cisco Catalyst 9800 Series Wireless Controllers maintaining their functionality with legacy systems by using existing certificates for devices that cannot validate SUDI99.

- If your device (AP or controller) cannot validate the SUDI99 certificate, the controller switches to an older certificate (SHA2-2037) for the 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.

- In FIPS mode, install the new SUDI CA certificates on the earlier version of Cisco CMX, or upgrade to the latest version.

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

Restrictions of SUDI99 certificates

- Incorrectly programmed SUDI99 certificates are rejected during trustpoint initialization at bootup, reverting to previous mappings.
- We recommend ensuring accurate certificate programming to avoid service disruptions during migration.
- User can verify the SUDI certificate status using the **show platform sudi pki** command.

Disable SUDI99 migration (GUI)

SHA1 SUDI certificates on hardware controllers have an imminent expiry date and devices using expired certificates face disruption in service.

Controllers come programmed with newer certificates in their secure hardware chip, ensuring a smooth migration to the latest SUDI99 certificate issued by CMCA-III authority. These certificates are enabled by default and are valid till December 2099.

Follow this procedure if you wish to continue using the current certificate:

Procedure

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

Disable SUDI99 migration (CLI)

The SUDI99 certificate is set as the default trustpoint in supported hardware units.

Follow the below steps to disable it:

Procedure

Step 1 Form the high availability pair in HA deployments.

Example:

```
no platform sudi cmca3
```

Step 2 Save the configuration.

Step 3 Reload the controller to disable the SUDI certificate and fall back to the older trustpoint certificate.

What to do next

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