Expired Enterprise Certificate Indication and Quarantine

Expired Certificate Indication and Quarantine

Table 1: Feature History

Feature Name	Release Information	Feature Description
Expired Certificate Indication and Quarantine	Cisco IOS XE Catalyst SD-WAN Release 17.16.1a Cisco Catalyst SD-WAN Control Components Release 20.16.1	Cisco SD-WAN Manager indicates when devices or Cisco Catalyst SD-WAN Control Components have expired certificates. Additionally, you can quarantine all edge devices that have expired certificates. Quarantine places devices into the staging status. Quarantined devices keep their control connections to Cisco Catalyst SD-WAN Control Components, but do not handle data plane traffic.

Information About Expired Certificate Indication and Quarantine

Indication of Expired Certificates

A digital certificate is used to authenticate devices in the overlay network. After authentication, devices and Cisco Catalyst SD-WAN Control Components can establish secure sessions with one another. A certificate is issued by a certificate authority and has an expiration date.

Every several minutes, Cisco SD-WAN Manager checks the devices and Cisco Catalyst SD-WAN Control Components in the network for expired certificates. If it detects any expired certificates, Cisco SD-WAN Manager displays a banner with a link to the **Configuration** > **Certificates** > **WAN Edges** page or **Configuration** > **Certificates** > **Control Components** page to show the details of which devices or components require certificate renewal.

Device Quarantine

Quarantine refers to placing devices into a staging state. Quarantined devices keep their control connections to Cisco Catalyst SD-WAN Control Components, but do not handle data plane traffic.

You can quarantine devices that have expired certificates. See Enable Quarantining Devices with Expired Certificates, on page 2.

Quarantining devices with expired certificates enforces the requirement to renew an expired certificate. Removing network elements with expired certificates may be necessary to comply with an organization's network security requirements.

This table shows which devices are subject to automatic quarantine when the quarantine feature is enabled.

Table 2: Automatic Quarantine for Expired Certificate

Device or Control Component	Automatic Quarantine, When Quarantine Enabled?
Hardware devices using a certificate	Yes
Hardware devices using an on-box trusted platform module (TPM) secure unique device identifier (SUDI) certificate	No
Software devices	Yes
Cisco Catalyst SD-WAN Control Components	No

Multitenancy

In a multitenancy scenario, enabling quarantine for expired certificates is possible only at the provider level and applies to all tenants.

Enable Quarantining Devices with Expired Certificates

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.

Step 2 Click **Device Quarantine**.

Step 3 Enable device quarantine.

View and Remedy Devices in Expired Certificate Quarantine

Cisco SD-WAN Manager can quarantine devices with expired certificates. See Information About Expired Certificate Indication and Quarantine, on page 1. It does not quarantine Cisco SD-WAN Control Components.

Before you begin

Enable quarantine for expired certificates. See Enable Quarantining Devices with Expired Certificates, on page 2.

Procedure

Step 1 Open the **Configuration** > **Certificates** > **WAN Edges** page to show a table with details of which devices require certificate renewal.

If Cisco SD-WAN Manager is displaying a banner message indicating that one or more devices are quarantined for expired certificates, click the link in the banner message to open the page.

In the table, an exclamation point icon indicates a problem with a device. Hover over the icon to display the details of the problem, such as an expired certificate. If a device is quarantined, the **Validate** column for the device shows **staging**.

Step 2 To remove a device from quarantine, renew its certificate. See Generate a WAN Edge Device Certificate Signing Request.