PKI Credentials Expiry Alerts

The PKI Credentials Expiry Alerts feature provides a warning mechanism in the form of an alert notification when a CA certificate is on the verge of expiry.

Restrictions for PKI Credentials Expiry Alerts

Alerts are not sent for the following certificates:

- Persistent or temporary self-signed certificates.
- Secure Unique Device Identifier (SUDI) certificates.
- Certificates that belong to a trustpool. Trustpools have their own expiry alerts mechanism.
- Trustpoint clones.

Information About PKI Alerts Notification

Overview of Alerts Notification

The Cisco IOS Certificate Authority (CA) server allows autoenrollment of certificates before a certificate expires to ensure the availability of certificates for applications during authentication. However, network outages, clock update problems, and overloaded CAs can impede certificate renewal, thereby resulting in subsystems going offline because no valid certificates can be used for authentication. The PKI Credentials Expiry Alerts feature provides a mechanism by which a CA client sends a notification to a syslog server when certificates are on the verge of expiry.

The notifications are sent at the following intervals:

- First notification—This is sent 60 days before the expiry of the certificate.

- Repeated notifications—After the first notification, subsequent notifications are sent every week until a week before the expiry of the certificate. In the last week, notifications are sent every day until the certificate expiry date.

The notifications are in a *warning* mode when the certificate is valid for more than a week. The notifications are in an *alert* mode when a certificate's validity is less than a week. The notifications include the following information:

- Truspoint the certificate is associated with
- Certificate type
- Serial number of the certificate
- Certificate issuer name
- Number of days remaining for the certificate to expire
- Whether the certificate is enabled with autoenrollment
- Whether a shadow certificate is available for the corresponding certificate

Note Alert notifications are sent either via the syslog server or Simple Network Management Protocol (SNMP) traps. Notifications stop when a trustpoint is configured with autoenrollment and the corresponding shadow or rollover certificate is present, and the shadow or rollover certificate's start time is either the same or earlier than the certificate's end time.

This feature cannot be disabled and requires no additional configuration tasks. The **show crypto pki timers** command is enhanced to display the timer expiry information. The following is a sample output from the **show crypto pki timers detail** command that displays the timer when a certificate is about to expire. When this timer expires, a notification is sent to the syslog server.

```
Device# show crypto pki timers detail

PKI Timers
|       14:36.150  (2019-10-30T11:33:30Z)
  |       14:36.150  (2019-10-30T11:33:30Z) SESSION CLEANUP
  |2569d23:56:19.461  (2026-11-12T11:15:13Z) SHADOW test

Expiry Alert Timers
|659d 5:56:19.599  (2021-08-19T17:15:13Z)
  |659d 5:56:19.599  (2021-08-19T17:15:13Z) ID(test)
  |2875d 4:45:18.562  (2027-09-13T16:04:12Z) CA(test)

Trustpool Timers
|3464d 9:06:48.463  (2029-04-24T20:25:42Z)
  |3464d 9:06:48.463  (2029-04-24T20:25:42Z) TRUSTPOOL
```

The following is a syslog message that is displayed on the device:

```
Device#

Dec 16 10:24:13.533: %PKI-4-CERT_EXPIRY_WARNING: ID Certificate belonging to trustpoint tp
 will expire in 60 Days 0 hours 0 mins 0 secs.
Issuer-name cn=CA
Subject-name hostname=Router
```

```
Serial-number 02
Auto-Renewal: Not Enabled
```

PKI Traps

PKI trap ease the monitoring and operations of a PKI deployment by retrieving certificate information of the devices in the network. The root device sends SNMP traps at regular intervals to the network management system (NMS) based on the threshold configured in the device. The traps are sent in the following scenarios:

- A new certificate is installed—An SNMP trap (new certificate notification) is sent to the SNMP server containing information about the certificate, such as, certificate serial number, certificate issuer name, certificate subject name, trustpoint name, certificate type, and certificate start and end date.
- A certificate is about to expire—An SNMP trap (certificate expiry notification) is sent to the SNMP server at regular intervals starting from 60 days to one week before the certificate's end date. In the week leading up to the expiration of the certificate, the trap is sent everyday. The trap contains certificate information, such as, certificate serial number, certificate issuer name, trustpoint name, certificate type, and certificate's remaining lifetime.

To enable PKI traps, use the **snmp-server enable traps pki** command.

Note If the shadow or rollover certificate's start time is later than the certificate's end time, traps are sent stating that the shadow certificate is not yet valid. However, no traps are sent if a shadow certificate available for the same trustpoint, and the shadow certificate becomes active.

Additional References for PKI Credentials Expiry Alerts

Related Documents

Related Topic	Document Title
Cisco IOS Commands	Cisco IOS Master Command List, All Releases
Security Commands	• Cisco IOS Security Command Reference Commands A to C • Cisco IOS Security Command Reference Commands D to L • Cisco IOS Security Command Reference Commands M to R • Cisco IOS Security Command Reference Commands S to Z

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Overview of Cisco TrustSec

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for Overview of Cisco TrustSec

Feature Name	Releases	Feature Information
IPv6 enablement - Inline Tagging	Cisco IOS XE Fuji 16.8.1	The support for IPv6 is introduced.