SSE Connector Certificate Expiry Warnings and Automatic Renewal Process

Contents

Issue

Users receive certificate expiry warnings in their Cisco SSE (Secure Service Edge) daily maintenance reports indicating that connector certificates expire within 30 days. The maintenance report shows warnings such as "Cert Expiry Warning (<=30 days)" for connected SSE connectors, causing concern about whether action is required to maintain connectivity and secure access operations.

The specific warning appears in the daily maintenance report format:

```
*** CISCO SSE DAILY MAINTENANCE REPORT ***
Report Time : 2026-05-12T12:18:07Z
Total : 2 connector(s)

SUMMARY
------------------------------------------------
- Cert Expiry Critical (<=7 days) : 0
- Cert Expiry Warning (<=30 days) : 2
- Vulnerable (CVE) : 0
- Upgrade Failed : 0
- Outdated Base Version : 0
- Stale Status (>24h no update) : 0

========================================
WARNING -- CERTIFICATES EXPIRING WITHIN 30 DAYS
========================================
------------------------------------------------
- Hostname : <>
- ID : <>
- Status : connected
- Cert Expires : 2026-06-02T00:13:52Z
- Version : v2.0.94
------------------------------------------------
- Hostname : <>
- ID : <>
- Status : connected
- Cert Expires : 2026-05-28T23:12:35Z
```

Environment

- Cisco Secure Access (SSE) platform with Remote Connectors deployed
- SSE connectors showing "connected" status in maintenance reports
- Connector versions including v2.0.94 and similar releases
- Daily maintenance reporting enabled for certificate monitoring

Resolution

The certificate expiry warnings in SSE daily maintenance reports are normal behavior and do not require any action on your part. The SSE platform handles certificate renewal automatically through this process.

Certificate Renewal Behavior

Cisco SSE connector certificates renew automatically without your intervention. The warning notifications serve as informational alerts about upcoming renewal activities rather than action items requiring manual certificate management.

Required Conditions for Automatic Renewal

To ensure successful automatic certificate renewal, verify these conditions are met:

Step 1: Verify Remote Connector Status

Ensure the Remote Connector (RC) remains running and is not shut down during the certificate renewal period. The connector must maintain its operational state to complete the automatic renewal process.

Step 2: Verify Network Connectivity

Confirm that firewall rules do not block Remote Connector communication with Cisco SSE services. The RC requires outbound connectivity to complete certificate renewal operations.

Monitoring and Validation

After the certificate expiration dates pass, the daily maintenance reports no longer show certificate expiry warnings for the renewed certificates. The connector status must remain connected throughout the renewal process.

If additional validation is required after certificate renewal, such as verifying renewal events in logs or confirming post-renewal connectivity, detailed log analysis can be performed to validate the renewal completion.

Cause

The certificate expiry warnings are generated by the SSE platform proactive monitoring system, which alerts users about certificates approaching their expiration dates within a 30-day window. This is designed behavior to provide visibility into certificate lifecycle management, even though the renewal process is automated.

Related Content

- Cisco Secure Access Documentation
- Cisco Secure Access Remote Connector Documentation
- Cisco Technical Support & Downloads