Restore Telemetry Connectivity Down Due to PKI Certificate Renewal Failures on Catalyst Center-managed IOS-XE Devices Running Releases 17.12.1 through 17.12.4.

Contents

Introduction

Impacted Releases:

Resolution:

- Option 1:When the device certificate is nearing expiration and has not yet expired:
- Option 2: Recommendation is to upgrade Catalyst Center to2.3.7.11 (GSMU 100),if not consider upgrading to2.3.7.9 (PSMU80)or2.3.7.10 (PSMU140).
- Option 3:Upgrade the effectedCisco IOS XEdevice to17.12.5 or laterof a Cisco recommended release.

Identifying the impacted Cisco IOS XE device:

- Step 1: Validate the device certificate and trustpoint status on the impacted Cisco IOS XE device.
- Step 2: Check the error log on the device.
- Step 3: Check the device's telemetry status in Catalyst Center

Additional Information:

FAQ:

Introduction

This document describes the reasons behind telemetry connections failing and how to restore them.

- The auto-renewal of thesdn-network-infra-iwancertificate (Cisco Catalyst Center - Cisco IOS® XE device) can fail on a Cisco IOS XE device due to Cisco bug ID CSCwk39268 on that Cisco IOS XE device's operating system, causing telemetry sent from affected devices to Catalyst Center to go down.
- The certificate is valid for one year and is normally renewed automatically by Catalyst Center around 60 days prior to its' expiration.
- Customers affected by this issue, or likely to be affected, can see a pop-up message in Catalyst Center.

Impacted Releases:

- Catalyst Center releases prior to 2.3.7.11 managing Cisco IOS XE network devices running versions 17.12.1-17.12.4

Resolution:

Customers are required to use **either** of these three options to resolve the issue.

Option 1: When the device certificate is nearing expiration and has not yet expired:

For multiple Cisco IOS XE devices this template can be pushed from Catalyst Center.

1. Access Catalyst Center

Log in to Catalyst Center.

From the main menu, navigate to Design > CLI Templates.

2. Create a template project

Click Add > New Project.

Enter a project name, for example: PKI_Trustpoint_Changes.

Click Continue.

3. Create a new CLI template

Select the newly created project.

Click Add > New Template.

Enter a template name, for example: Configure_sdn_network_infra_iwan_Trustpoint.

Set Template Type to Regular Template.

Set the Software Type to Cisco IOS XE.

Select the appropriate device family or series for the intended Cisco IOS XE devices.

Click Continue.

4. Add the CLI Configuration

In the Template Editor, enter these commands:

```
crypto pki trustpoint sdn-network-infra-iwan
no hash sha256
hash sha512
```

5. Commit the template

After saving the template, clickActionsand selectCommit.

Enter a commit message, for example:Update trustpoint hash to sha512.

Confirm the commit.

6. Create a Network Profile

a. Provide a Profile Name
b. Provide a Profile Type, for example Switching
c. Go to “Day-N Template(s)”
d. Attach the Template via Add Template
e. Save the Network Profile
f. Assign the Network Profile to a site

7. Provision the template to a device

On theDesign > CLI Templates page, select the template.

ClickProvision Templates.

Enter a task name, for example:Trustpoint_Update_Device1.

In the device selection step, select**one Cisco IOS XE device only**.

ClickNext.

Review the applicable template assignment.

Since no template variables are used, continue to the next step.

On the Preview screen, verify that the commands are correct.

ClickDeploy Now.

8. Confirm Deployment Status in Catalyst Center:

Navigate toActivities > Tasks.

Verify that the deployment completed successfully.

If the deployment failed, review the task details and error output before retrying.

9. Repeat for additional devices

Repeat this deployment process for each Cisco IOS XE device individually.

Use a separate task name for each device to simplify tracking and troubleshooting.

10. Verify the configuration on the device
After deployment completes, connect to the device's CLI and run:

```
show run | sec crypto pki trustpoint sdn-network-infra-iwan
```

Confirm that the running-configuration includes these lines:

```
crypto pki trustpoint sdn-network-infra-iwan
hash sha512
```

Option 2: Recommendation is to upgrade Catalyst Center to 2.3.7.11 (GSMU 100), if not consider upgrading to 2.3.7.9 (PSMU80) or 2.3.7.10 (PSMU140).

The SMU (Software Maintenance Update) is available under**System > Software Management**in the Catalyst Center GUI, If you are unable to see the SMU, please open a TAC service request and provide your Member ID.

Option 3: Upgrade the effectedCisco IOS XEdevice to17.12.5 or later of a Cisco recommended release.

Identifying the impacted Cisco IOS XE device:

Step 1: Validate the device certificate and trustpoint status on the impacted Cisco IOS XE device.

```
device# show crypto pki certificates verbose sdn-network-infra-iwan
```

Sample Output:

```
Certificate
  Status: Available
  Version: 3
```

```
  Certificate Serial Number (hex): 18831279321B12FA
  Certificate Usage: General Purpose
  Issuer:
    cn=sdn-network-infra-ca
  Subject:
    Name: device.example.net
    cn=C93OO-48U_SN12345678_sdn-network-infra-iwan
    hostname=device.example.net
  Validity Date:
    start date: 11:39:55 cdt Jul 10 2025
    end   date: 11:39:55 cdt Jul 16 2025
    renew date: 06:51:54 cdt Jul 15 2025
  ...
```

Note: If the end date and renew date are before the current date on the device then the certificate has expired.

Step 2: Check the error log on the device.

Sample Output:

```
Device# show logging
%PKI-2-CERT_RENEW_FAIL: Certificate renewal failed for trustpoint sdn-network-infra-iwan
Reason : Failed to get ID certificate from CA server sdn-network-infra-iwan:Certificate renewal failed.
```

Step 3: Check the device's telemetry status in Catalyst Center

Sample Output:

```
Device#show tel con all
Telemetry connections
Index Peer Address Port VRF Source Address State State Description
--------------------------------------------------------------------------------
36284 x.x.x.x 25103 0 x.x.x.x Connecting Connection request made to transport handler
```

Note: In this example the telemetry connection is not up, just in the Connecting state.

Additional Information:

When the device certificate has already expired and the device is in a degraded state, perform these two steps:

Step 1: Force push telemetry from the Catalyst Center GUI

1. Navigate to**Menu > Provision > Inventory**
2. Select the device(s) by hostname
3. Select**Actions > Telemetry > Update Telemetry Settings**
4. Enable Force Configuration Push
5. Proceed through the wizard and submit the task

Step 2: Update the hash algorithm for the trustpoint tosha512 on the device:

```
crypto pki trustpoint sdn-network-infra-iwan
no hash sha256
hash sha512
```

FAQ:

Does installing the SMU fix an already impacted system, or is it preventive?
The SMU is a preventive fix and must be installed before the issue occurs. If the issue has already occurred, installing the SMU does not automatically clear the issue. To recover existing failed systems review the additional information section.