

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.

Introduction

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

- The auto-renewal of the `sdn-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: Upgrade Catalyst Center to **2.3.7.11** or **2.3.7.9 PSMU60** or **2.3.7.10 PSMU110**. The SMU (Software Maintenance Update) will be available for upgrade under **System > Software Management** in the Cisco Catalyst Center GUI.

Option 2: Upgrade the effected Cisco IOS XE device to **17.12.5 or later** of a Cisco recommended release.

Option 3: Force-push telemetry from the Catalyst Center GUI and update the hash algorithm for the trustpoint to **sha512** on the device as follows:

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

Identifying the impacted Cisco IOS XE device:

Step 1: Validate 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=C9300-48U_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 to 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:

(a.) For multiple Cisco IOS XE devices this template can be pushed from Catalyst Center by provisioning CLI templates from Design > CLI Templates tools:

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

(b.) Force Telemetry Push After Hash Update

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

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 will not automatically clear the issue. To recover existing failed systems, select Option 3.