

# Troubleshoot HTTPS Error in DNA Center for SWIM

## Contents

---

### [Introduction](#)

### [Prerequisites](#)

[Requirements](#)

[Components Used](#)

### [Problem](#)

### [Verification](#)

[Network Device status in Cisco DNA Center Inventory](#)

[DNAC-CA certificate installed in Network Device](#)

### [Troubleshooting](#)

[Communication from Network Device to Cisco DNA Center in Network Device through port 443](#)

[HTTPS client source-interface in Network Device](#)

[Date sync](#)

[Debugs](#)

---

## Introduction

This document describes a procedure to troubleshoot problems with HTTPS protocol in SWIM process for Cisco DNA Center in Cisco IOS® XE platforms.

## Prerequisites

### Requirements

You must have access Cisco DNA Center through GUI with ADMIN ROLE privilege and switch CLI.

### Components Used

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

## Problem

There is a common error that Cisco DNA Center / Software Image Management (SWIM) displays after Image Update Readiness Check:

"HTTPS is NOT reachable / SCP is reachable"

HTTPS is NOT reachable / SCP is reachable

**Expected:** Cisco DNA Center certificate has to be installed successfully and Device should be able to reach DNAC (10.10.10.10) via HTTPS.

**Action:** Reinstall Cisco DNA Center certificate. DNAC (10.10.10.10) certificate installed automatically on device when device is assigned to a Site, please ensure device is assigned to a site for HTTPS transfer to work. Alternatively DNAC certificate (re) install is attempted when HTTPS failure detected during image transfer.

This error describes that HTTPS protocol is not reachable; however, Cisco DNA Center is going to use SCP protocol to transfer Cisco IOS® XE image to the network device.

One disadvantage for using SCP is the amount of time to distribute the image. HTTPS is faster than SCP.

## Verification

### Network Device status in Cisco DNA Center Inventory

Navigate to **Provision** > **Inventory** > Change Focus to **Inventory**

Verify **Reachability** and **Manageability** for the network device to upgrade. The status for the device must be **Reachable** and **Managed**.

If the network device has any other status in Reachability and Manageability, fix the problem before moving to the next steps.

### DNAC-CA certificate installed in Network Device

Go to the network device and run the command:

```
show running-config | sec crypto pki
```

You must see DNAC-CA trustpoint and DNAC-CA chain. If you cannot see DNAC-CA trustpoint, chain or both, you need to [Update Telemetry Settings](#) in order push DNAC-CA certificate.

If device controllability is disable, install DNAC-CA certificate manually with the next steps:

- In a web browser type [https://<dnac\\_ipaddress>/ca/pem](https://<dnac_ipaddress>/ca/pem) and download the .pem file
- Save the .pem file in your local computer
- Open .pem file with a text editor application
- Open network device CLI
- Verify any old DNA-CA certificate with the command `show run | in crypto pki trustpoint DNAC-CA`
- If there is an old DNA-CA certificate, remove DNAC-CA cert with the command `no crypto pki trustpoint DNAC-CA` in config mode
- Run the commands in configuration mode in order to install DNAC-CA cert:

```
crypto pki trustpoint DNAC-CA
enrollment mode ra
enrollment terminal
usage ssl-client
revocation-check none
exit
crypto pki authenticate DNAC-CA
```

- Paste the .pem text file
- Enter yes when prompted
- Save the configuration

## Troubleshooting

### Communication from Network Device to Cisco DNA Center in Network Device through port 443

Run the HTTPS file transfer test in your network device

```
copy https://<DNAC_IP>/core/img/cisco-bridge.png flash:
```

This test transfers a PNG file from Cisco DNA Center to the switch.

This output describes the file transfer is successful

```
MXC.TAC.M.03-1001X-01#copy https://10.x.x.x/core/img/cisco-bridge.png flash:
Destination filename [cisco-bridge.png]?
Accessing https://10.x.x.x/core/img/cisco-bridge.png...
Loading https://10.x.x.x/core/img/cisco-bridge.png
4058 bytes copied in 0.119 secs (34101 bytes/sec)
MXC.TAC.M.03-1001X-01#
```

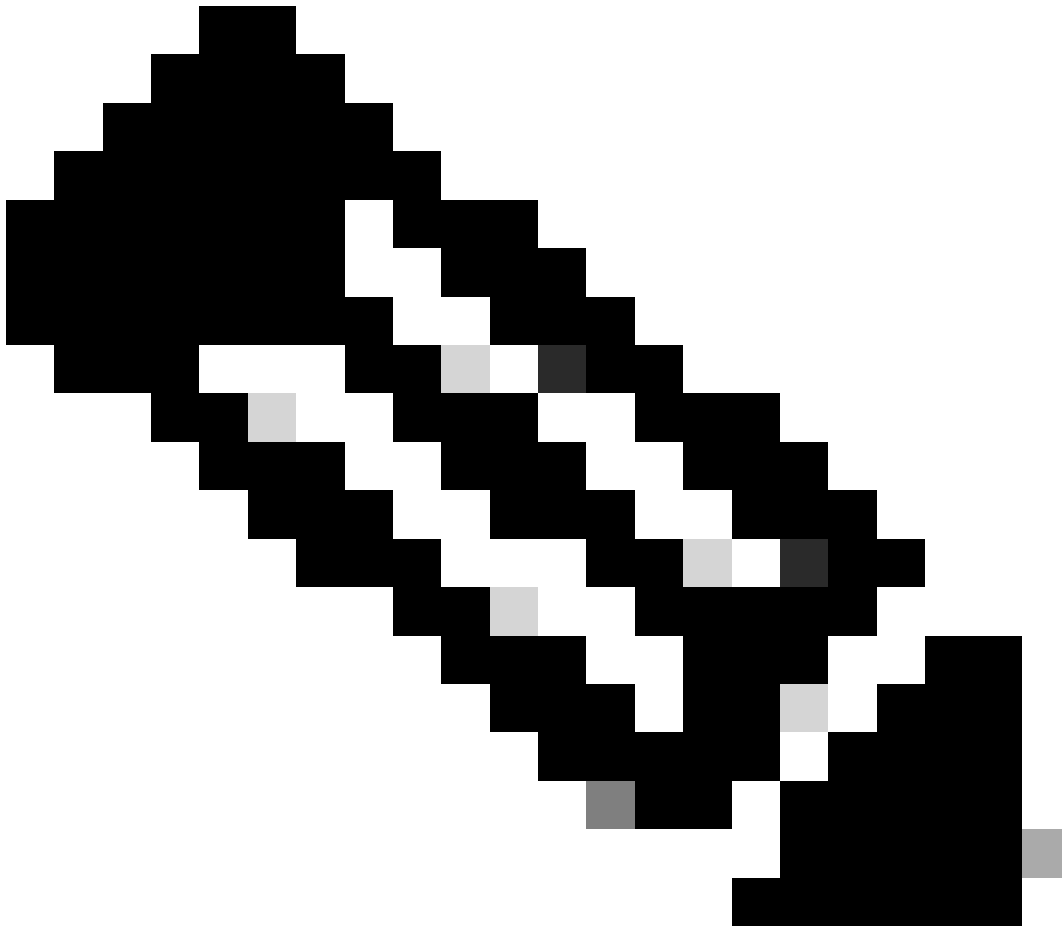
If you get the next output, the file transfer failed:

```
MXC.TAC.M.03-1001X-01#$/10.x.x.x/core/img/cisco-bridge.png flash:
Destination filename [cisco-bridge.png]?
Accessing https://10.x.x.x/core/img/cisco-bridge.png...
%Error opening https://10.x.x.x/core/img/cisco-bridge.png (I/O error)
MXC.TAC.M.03-1001X-01#
```

Take the next actions:

- Verify if firewall is blocking port 443, 80, and 22.
- Verify if there is an access-list in network device blocking port 443 or HTTPS protocol.

- Do a packet capture into the network device while file transfer is happening.
- 



**Note:** After you finish to test HTTPS file transfer, remove cisco-bridge.png file with the command `delete flash:cisco-bridge.png`

---

## HTTPS client source-interface in Network Device

Verify in your network device client source-interface is configured correctly.

You can run the command `show run | in http client source-interface` in order to validate the configuration:

```
MXC.TAC.M.03-1001X-01#show run | in http client source-interface
ip http client source-interface GigabitEthernet0
MXC.TAC.M.03-1001X-01#
```

HTTPS transfer file test is going to fail if the device has an incorrect source interface or the source interface is missing.

Take a look at the example:

Lab device has the ip address 10.88.174.43 in Inventory Cisco DNA Center:

Inventory screenshot:

Device Name	IP Address	Device Family	Reachability ⓘ	EoX Status ⓘ	Manageability ⓘ
<a href="#">MXC.TAC.M.03-1001X-01.etelecut.mx</a>	10.88.174.43	Routers	🟢 Reachable	🟡 Not Scanned	🟢 Managed

HTTPS file transfer test failed:

```
MXC.TAC.M.03-1001X-01#copy https://10.x.x.x/core/img/cisco-bridge.png flash:
Destination filename [cisco-bridge.png]?
%Warning:There is a file already existing with this name
Do you want to over write? [confirm]
Accessing https://10.x.x.x/core/img/cisco-bridge.png...
%Error opening https://10.x.x.x/core/img/cisco-bridge.png (I/O error)
MXC.TAC.M.03-1001X-01#
```

Verify source-interface:

```
<#root>

MXC.TAC.M.03-1001X-01#show run | in source-interface
ip ftp source-interface GigabitEthernet0

ip http client source-interface GigabitEthernet0/0/0

ip tftp source-interface GigabitEthernet0
ip ssh source-interface GigabitEthernet0
logging source-interface GigabitEthernet0 vrf Mgmt-intf
```

Verify interfaces:

```
MXC.TAC.M.03-1001X-01#show ip int br | ex unassigned
Interface IP-Address OK? Method Status Protocol
GigabitEthernet0/0/0 1.x.x.x YES manual up up
GigabitEthernet0 10.88.174.43 YES TFTP up up

MXC.TAC.M.03-1001X-01#
```

According with Inventory screenshot, Cisco DNA Center discovered the device using the interface GigabitEthernet0 instead of GigabitEthernet0/0/0

You need to modify with the correct source interface in order to fix the problem.

```
MXC.TAC.M.03-1001X-01#conf t
Enter configuration commands, one per line. End with CNTL/Z.
MXC.TAC.M.03-1001X-0(config)#ip http client source-interface GigabitEthernet0
MXC.TAC.M.03-1001X-0(config)#
```

```
MXC.TAC.M.03-1001X-01#show run | in source-interface
ip ftp source-interface GigabitEthernet0
ip http client source-interface GigabitEthernet0
ip tftp source-interface GigabitEthernet0
ip ssh source-interface GigabitEthernet0
logging source-interface GigabitEthernet0 vrf Mgmt-intf
MXC.TAC.M.03-1001X-01#
```

```
MXC.TAC.M.03-1001X-01#copy https://10.x.x.x/core/img/cisco-bridge.png flash:
Destination filename [cisco-bridge.png]?
Accessing https://10.x.x.x/core/img/cisco-bridge.png...
Loading https://10.x.x.x/core/img/cisco-bridge.png
4058 bytes copied in 0.126 secs (32206 bytes/sec)
MXC.TAC.M.03-1001X-01#
```

---

**Note:** After you finish to test HTTPS file transfer, remove cisco-bridge.png file with the command `delete flash:cisco-bridge.png`

---

## Date sync

Verify that network device has correct date and clock with the command `show clock`

Take a look the lab scenario where DNAC-CA certificate was missing in LAB device. Telemetry update was pushed; however, DNAC-CA certificate installation failed due to:

```
Jan 1 10:18:05.147: CRYPTO_PKI: trustpoint DNAC-CA authentication status = 0
%CRYPTO_PKI: Cert not yet valid or is expired -
start date: 01:42:22 UTC May 26 2023
end date: 01:42:22 UTC May 25 2025
```

As you can see, the cert is valid; however, the error said that cert not yet valid or is expired.

Verify network device time:

```
MXC.TAC.M.03-1001X-01#show clock
10:24:20.125 UTC Sat Jan 1 1994
MXC.TAC.M.03-1001X-01#
```

There is an error with the date and time. In order to fix this problem, you can configure a ntp server or configure manually the clock with the command `clock set` in privilege mode.

Manual clock configuration example:

```
MXC.TAC.M.03-1001X-01#clock set 16:20:00 25 september 2023
```

NTP configuration example:

```
MXC.TAC.M.03-1001X-0(config)#ntp server vrf Mgmt-intf 10.81.254.131
```

## Debugs

You can run debugs to troubleshoot HTTPS problem:

```
debug ip http all
debug crypto pki transactions
debug crypto pki validation
debug ssl openssl errors
```





**Note:** After you finish to troubleshoot the network device, stop the debugs with the command `undebg all`

---