# Cisco Nexus 9000 Series Switches Conversion from Cisco NX-OS to Cisco ACI-Mode

**Revised: June 21, 2022**

# New and Changed Information

The following table provides an overview of the significant changes up to this current release. The table does not provide an exhaustive list of all changes or of the new features up to this release.

***Table 1: New Features and Changed Information***

| Cisco APIC Release Version | Feature | Description |
|---|---|---|
| 1.0(2j) | Initial release | -- |

## Overview

This article provides information on the Nexus 9000 (N9K) Series Switch Conversion process from NX-OS standalone mode to ACI mode. This information applies to switches that are running a Cisco NX-OS release prior to 6.1(2)I3(3). Refer to the *Cisco Nexus 9000 Series NX-OS Software Upgrade and Downgrade Guide* here: http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/6-x/upgrade/guide/b_Cisco_Nexus_9000_Series_NX-OS_Software_Upgrade_and_Downgrade_Guide_Release_6x.html for instructions on converting switches that are running Cisco NX-OS Release 6.1(2)I3(3) or later.

**Note** For the Nexus 9508, Supervisor 2 must be removed from the chassis before starting the upgrade process. After upgrading Supervisor 1 in Slot 1, remove Supervisor 1 from Slot 1. Next, insert Supervisor 2 into Slot 1, and the upgrade process can be done again to upgrade Supervisor 2. The switch must be running the NX-OS standalone version, which can be verified by issuing the **<show version>** command (shown as follows) and checking the image file name. If the image file name starts with n9000, it is the standalone version. If it starts with aci-n9000, it is the ACI version.

Output for **<show version>**

```
Software
   BIOS: version 07.06
   NXOS: version 6.1(2)I2(2)
   BIOS compile time: 03/02/2014
   NXOS image file is: bootflash:///n9000-dk9.6.1.2.I2.2.bin
   NXOS compile time: 4/21/2014 1:00:00 [04/21/2014 08:32:28]
```

## ACI Image Management

This section describes the three methods you can use to get an ACI image from a source to your destination (the location of the Nexus device being converted).

### Procedure

**Step 1** Copy the ACI image from APIC via SCP as follows:

a) Set the IP on the mgmt0 interface on Nexus to allow connectivity between this interface and APIC.

b) Enable the SCP feature on the Nexus device **<features scp-server>**.

c) On the APIC CLI, SCP the firmware image from APIC to the Nexus device **<sco -r.firmware/fwrepos/fwrepo/(switch-image-name) admin@(IP of Nexus):(switch-image-name)>**

**Step 2** Copy the ACI image from a USB drive to Nexus as follows:

a) Plug the USB drive into the Supervisor USB slot.

b) Check the contents using **<dir usb1:> or <dir usb2:>**.

c) Copy the ACI image from USB to switch using **<copy usb(#):(ACI Image Name) bootflash:>**

**Step 3** Copy the ACI image from another SCP server (not APIC) as follows:

a) Set the management VRF default gateway using **<vrf context management> + <ip route 0.0.0.0/0 (gateway IP)>**.

b) Set the mgmt0 interface with the IP address using **<int mgmt 0> + <ip address (IP)>**.

c) Test the connectivity to the file server.

d) Copy the ACI .gbin image to switch bootflash using SCP **<copy scp: bootflash:>**.

---

### Example

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)#vrf context management
switch(config-vrf)# ip route 0.0.0.0/0 10.122.141.97
switch(config-vrf)# int mgmt 0
switch(config-if) ip address 10.122.141.102/27
switch(config-if) ping 172.18.217.253 vrf management
PING 172.18.217.253): 56 data bytes
64 bytes from 172.18.217.253: icmp_seq=0 ttl=120 time=0.941 ms
64 bytes from 172.18.217.253: icmp_seq=1 ttl=120 time=0.528 ms
64 bytes from 172.18.217.253: icmp_seq=2 ttl=120 time=0.335 ms
64 bytes from 172.18.217.253: icmp_seq=3 ttl=120 time=0.298 ms
64 bytes from 172.18.217.253: icmp_seq=4 ttl=120 time=0.322 ms
```

## EPLD Verification and Upgrade Process

### Before you begin

Prior to converting the Nexus device to ACI, you must verify that the EPLD does not require upgrades. The process for this verification and upgrade (if necessary) is as follows:

1. Download the latest version of EPLD from CCO. Model-specific EPLD images can be found at software.cisco.com/download by navigating to the specific model switch you are working with.
2. Transfer the EPLD image to the Nexus switch using the USB drive method or SCP method, which was previously described in this document.
3. Check the**<show install all impact epld (epld image name)>** command output to see if there are any upgrades required with the downloaded EPLD image from Step 1. If there are no upgrades required, move onto the next section.

   • The following shows the command output for **<show install all impact epld (epld image name)>**:

```
switch(config)# show install all impact epld bootflash:n9000-epld.6.1.2.I2.3.img
Compatibility check:
Module       Type        Upgradable     Impact Reason
------ ----------------- ---------- ---------- ------
     1             SUP         Yes   disruptive Module Upgradable
     2       Expansion         Yes   disruptive Module Upgradable
```

```
Retrieving EPLD versions... Please wait.
Images will be upgraded according to following table:
Module Type          EPLD Running-Version New-Version Upg-Required
------ ---- ------------ ---------------- ----------- ------------
     1 SUP  MI FPGA             0x14       0x14           No
     1 SUP  IO FPGA             0x13       0x13           No
     2 SUP  MI FPGA2            0x15       0x15           No
switch(config)#
```

4. If there is an upgrade required, issue the **<install epld bootflash:(epld image) module all>** command to install the new EPLD image.
    - The following figure is an example of a switch that needs to be upgraded:

```
switch(config)# show install all impact epld bootflash:n9000-epld.6.1.2.I2.3.img
Compatibility check:
Module       Type        Upgradable     Impact Reason
------ ----------------- ---------- ---------- ------
     1             SUP         Yes   disruptive Module Upgradable
     2       Expansion         Yes   disruptive Module Upgradable
Retrieving EPLD versions... Please wait.
Images will be upgraded according to following table:
Module Type          EPLD Running-Version New-Version Upg-Required
------ ---- ------------ ---------------- ----------- ------------
     1 SUP  MI FPGA             0x08       0x09          Yes
     1 SUP  IO FPGA             0x07       0x07           No
     2 SUP  MI FPGA2            0x15       0x15           No
switch(config)#
```

## Booting to a New ACI Image

### Before you begin

Now that you have the ACI image on the device and your EPLDs are verified as OK, you can boot the ACI image.

1. To boot into the ACI image, configure the switch so that it does not boot from NX-OS using the **<no boot nxos>** command.
2. Save the configuration **<copy running-config startup-config>**.
    - The following figure shows the command output for **<copy running-config startup-config>**:

```
switch(config)# no boot nxos
switch(config)# reload
!!!WARNING! there is unsaved configuration!!!
This command will reboot the system. (y/n)? [n] y
```

3. Reload the switch using the **<reload>** command.
4. After reloading the switch, the switch boots into the loader prompt. While in the loader, you can set the switch to boot the ACI image using the **<boot (ACI image name)>** command.
5. After booting up the ACI image (seen in the following figure), log into the switch using the administrator account.

**Note** There is no password required.

- The following figure shows the User Access Verification banner:

```
User Access Verification
(none) login: admin
*******************************************************************************
     Fabric discovery in progress, show commands are not fully functional
     Logout and Login after discovery to continue to use show commands.
*******************************************************************************
```

6. After booting to the ACI image and logging in, you can copy and install the certificates (if necessary).

## Certificate Verification

### Before you begin

For Nexus 9000 devices shipped prior to May 2014, certificate installation may be required. The process of verifying these certificates is as follows.

**Note** The process for gathering and installing certificates (if necessary) is in the next few sections of this article.

### Procedure

**Step 1** Log in as an administrator and run the following command to verify if Cisco certifications are installed: **<openssl asn1parse < /securedata/ssl/server.crt>**.

**Step 2** In the output, look for `PRINTABLESTRING` and if `Cisco Manufacturing CA` is there, then the correct certifications are installed. If `INSIEME` or `INSIEME NETWORKS` is listed here, the Cisco certificate installation is required, which is explained in the next section of this article.

## Certificate Generation and Installation

### Before you begin

If certificates are required for installation, a TAC case must be opened so that a TAC engineer can perform this procedure. The following steps explain how to generate certifications for your device and install them:

1. Record the PID and serial number of the chassis using the**<show inventory>** command. It is usually the first entry in the output.

```
Switch(config)# show inventory
NAME: "Chassis", DESCR: "Nexus9000 C93128TX chassis"
PID: N9K-C93128TX       ,  VID: V02 ,  SN: SAL:
NAME: "slot 1", DESCR: "1/10G-1 Ethernet Module"
PID: N9K-C93128TX       ,  VID: V02 ,  SN: SAL:
NAME: "slot 2", DESCR: "40G Ethernet Expansion Module"
PID: N9K-M12PQ          ,  VID: V01 ,  SN: SAL:
NAME: "Power Supply 1", DESCR: "Nexus9000 C93128TX Chassis Power Supply"
PID: N9K-PAC-1200W      ,  VID: V01 ,  SN: DCH:
NAME: "Power Supply 2", DESCR: "Nexus9000 C93128TX Chassis Power Supply"
PID: N9K-PAC-1200W      ,  VID: V01 ,  SN: DCH:
```

2. For the 9336 MiniSpine, use the serial number from the output of the **<show sprom backplane>** command.

```
switch# show sprom backplane
DISPLAY backplane sprom contents:
Common block:
 Block Signature : 0xabab
 Block Version   : 3
 Block Length    : 160
 Block Checksum  : 0x15c2
 EEPROM Size     : 65535
 Block Count     : 5
 FRU Major Type  : 0x6001
 FRU Minor Type  : 0x0
 OEM String      : Cisco Systems, Inc.
 Product Number  : N5K-C9336PQ
 Serial Number   : SAL
 Part Number     : 73-15298-01
 Part Revision   : 1
 Mfg Deviation   : 0
 H/W Version     : 0.2010
 Mfg Bits        : 0
 Engineer Use    : 0
 snmpOID         :
```

3. Open the certification generator (TAC accessible only) in a browser and enter the PID and serial number gathered in the previous step, along with your email address. This page generates certifications and keys for the device and email the files to the given email address.

4. Transfer the .crt and .key.pem files to the Nexus switch using the USB drive method or SCP method as previously described in this document.

```
(none)# scp scpuser@172.18.217.37:FGE    .N9K-C9508_client.crt /bootflash
The authenticity of host '172.18.217.37 (172.18.217.37)' can't be established.
RSA key fingerprint is
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '172.18.217.37' (RSA) to the list of known hosts.
scpuser@172.18.217.37's password:
Fnone)# scp scpuser@172.18.217.37:FGE    .N9K-C9508_client.key.pem00:00
hashe)# scp scpuser@172.18.217.37:FGE    .N9K-C9508_client.key.pe /bootflash
scpuser@172.18.217.37's password:
FGE    .N9K-C9508_client.key.pem         100%  B87    0.9KB/s  00:00
(none)#
```

5. After copying the two files to bootflash, copy them into /var/tmp using <cp (source filepath) (dest filepath)> so they can be installed. You cannot install from /bootflash due to permissions. If you try to run the act_util with the files from /bootflash, an error occurs, as seen below:

```
(none)# dir /bootflash
FGE18170ABF.N9K-C9508_client.crt         auto-s
FGE18170ABF.N9K-C9508_client.key.pem     disk_log.txt
aci-n9000-dk9.11.0.0.802b.gbin           mem_log.txt
9508_client.crtl rsa_file FGE:           .N9K-C9508_client.key.pem      N9K-C
 Sem init vals 1 1
 Sem init vals 1 1
 Sem init vals 1 1
 Sem init vals 1 1
 Sem init vals 1 1
 Sem init vals 1 1
 Sem init vals 1 1
```

```
act_util Version = 1.1.0
RSA Key (FGE    .N9K-C9508_client.key.pem) & Certificate (FGE   .N9K-C9508_client.crt) insall
act2_dev->port = 0x00000000
act2_dev->port = 0x00000001
act2_dev->port = 0x00000070
Block length should be = 0x00001008
endian = 0
Opening key file FGE    .N9K-C9508_client.key.pem
rsa_read_file ERR1 - Unable to open file FGE    .N9K-C9508_client.key.pem


# FAILED : act2_util ##
```

6. Next, install the certifications using the following command (act_util commands are only usable from root): **<act_util rsa_file (key file) (cert file)>** Enter **Y** when prompted with "Do you want to program this to sprom?"

7. Verify the certifications were installed correctly by using the **<act_util keypair_show 0>** or **<act_util keypair_show 1>**. 0 is for TOR/c1, 1 is for Spine/c8. If the certifications were installed correctly, no error shows:

   -
   ```
   (none)# act_util keypair_show 1
   act_util Version - 1.1.0
   Keypair_show inst 1
   ACT2 set to simple mode

   ACT2_RAW_OBJECT : 4222379
   Loop 0 - Object number 4222379, Object type:1 , Object size: 1024
   ACT2_RAW_Object : 4223424
   Loop 1 - Object number 4223424, Object type:1 , Object size: 4104
   Yay you're great! Expected size: 4104 > read size of 4104
   Printing SPROM info...

   ##Block #1 - 5W RSA Block ###
   Block Signature : 0xabab
   Block Version : 3
   Block Null : 0
   Block Length : 160
   Block Checksum : 0x18c9
   RSA_Key :
   <--Output truncated-->
   ```

8. Reload the switch.

9. After reloading the switch, log in as an administrator and run the following command to verify the certifications are installed: **<openssl asn1parse < /securedata/ssl/server.crt>** In the output, look for `PRINTABLESTRING` and if `Cisco Manufacturing CA` is there, it was successful.

   -
   ```
   (none)# openssl asn1parse <  /securedata/ssl/server.crt
   WARNING: can't open config file: /usr/lib/ssl/openssl.cnf
       0:d=0  hl=4 l= 957 cons: SEQUENCE
       4:d=0  hl=4 l= 677 cons: SEQUENCE
       8:d=0  hl=2 l=   3 cons: cont [ 0 ]
      10:d=0  hl=2 l=   1 prim: INTEGER           :02
      13:d=0  hl=2 l=  10 prim: INTEGER           :4B8321610000000321EE
      25:d=0  hl=2 l=  13 cons: SEQUENCE
      27:d=0  hl=2 l=   9 prim: OBJECT            :sha1WithRSAEncryption
      38:d=0  hl=2 l=   0 prim: NULL
      40:d=0  hl=2 l=  57 cons: SEQUENCE
      42:d=0  hl=2 l=  22 cons: SET
      44:d=0  hl=2 l=  20 cons: SEQUENCE
      46:d=0  hl=2 l=   3 prim: OBJECT            :organizationName
   ```

```
   51:d=0  hl=2 l=  13 prim: PRINTABLESTRING    :Cisco Systems
   66:d=0  hl=2 l=  31 cons: SET
   68:d=0  hl=2 l=  29 cons: SEQUENCE
   70:d=0  hl=2 l=   3 prim: OBJECT              :commonName
   75:d=0  hl=2 l=  22 prim: PRINTABLESTRING     :Cisco Manufacturing CA
   99:d=0  hl=2 l=  30 cons: SEQUENCE
<--Output truncated-->
```

Your Nexus 9000 switch is now running in ACI mode.

**Americas Headquarters**
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

**Asia Pacific Headquarters**
CiscoSystems(USA)Pte.Ltd.
Singapore

**Europe Headquarters**
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.