Cisco APIC Installation and ACI Upgrade and Downgrade Guide

First Published: 2016-07-01

Last Modified: 2024-02-21

Trademarks

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS REFERENCED IN THIS DOCUMENTATION ARE SUBJECT TO CHANGE WITHOUT NOTICE. EXCEPT AS MAY OTHERWISE BE AGREED BY CISCO IN WRITING, ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENTATION ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED.

The Cisco End User License Agreement and any supplemental license terms govern your use of any Cisco software, including this product documentation, and are located at: http://www.cisco.com/go/softwareterms.Cisco product warranty information is available at http://www.cisco.com/go/warranty. US Federal Communications Commission Notices are found here http://www.cisco.com/c/en/us/products/us-fcc-notice.html.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any products and features described herein as in development or available at a future date remain in varying stages of development and will be offered on a when-and if-available basis. Any such product or feature roadmaps are subject to change at the sole discretion of Cisco and Cisco will have no liability for delay in the delivery or failure to deliver any products or feature roadmap items that may be set forth in this document.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com go trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

CONTENTS

New and Changed Information

New and Changed Information

Note   Always check the *Cisco Application Policy Infrastructure Controller Release Notes* for the release that you are working with first.

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

Table 1: New and Changed Information

Cisco APIC Release Version	Feature	Description	Where Documented
6.0(3)	Memory-based switch image installation	A switch installs either the 32-bit or 64-bit image based on the switch's amount of memory instead of based on a static mapping.	Guidelines and Limitations for Upgrading or Downgrading, on page 55
6.0(2)	Installing switch software maintenance upgrade patches without reloading	Some switch software maintenance upgrade (SMU) patches do not require you to reload the switch after you install those patches.	
6.0(2)	Auto Firmware Update on Cisco APIC discovery	When you add a new Cisco APIC to the fabric either through Product Returns & Replacements (RMA), cluster expansion, or commission, the Cisco APIC is automatically upgraded to the same version of the existing cluster.	Auto Firmware Update on APIC Discovery, on page 129

Cisco APIC Release Version	Feature	Description	Where Documented
6.0(2)	32-bit and 64-bit Cisco ACI-mode switch images	There are now both 32-bit and 64-bit Cisco ACI-mode switch images. The upgrade process automatically installs the correct image depending on your switch models. **Note** Download the Cisco APIC 6.0(2) or later image and upgrade the Cisco APIC cluster to the downloaded release. Before the upgrade completes, do not download the Cisco ACI-mode switch images to the Cisco APIC.	Guidelines and Limitations for Upgrading or Downgrading, on page 55
5.2(4)	Default interface policy creation	When you upgrade to the 5.2(4) or later release, the Cisco APIC creates some default interface policies automatically.	Default Interface Policies in the 5.2(4) release and later, on page 52
N/A	Reorganization of the document to improve usability.	On July 30, 2021, the content within this document was completely reorganized and rewritten to improve usability. The title of this document was also renamed to the *Cisco APIC Installation and ACI Upgrade and Downgrade Guide* to reflect part of this reorganization work.	
5.2(1)	Switches will automatically upgrade the FPGA/EPLD/BIOS based on the booting ACI switch image during a normal boot-up sequence for certain components, even if it's not an upgrade operation performed through the APICs.	Beginning with release 5.2(1) and Cisco ACI-mode switch release 15.2(1), Cisco ACI-mode switches will automatically upgrade the FPGA/EPLD/BIOS based on the booting Cisco ACI-mode switch image during a normal boot-up sequence for certain components, even if it's not an upgrade operation performed through the Cisco APICs.	Managing FPGA/EPLD/BIOS Firmware, on page 131
5.2(1)	Software Maintenance Upgrade patches	You can install software maintenance upgrade (SMU) patches that contain fixes for specific defects. Because SMU patches can be released much more quickly than a more traditional patch release, you can resolve specific issues in a more timely manner. SMU patches are available for the Cisco APIC and Cisco ACI-mode switches.	Software Maintenance Upgrade Patches, on page 137

Cisco APIC Release Version	Feature	Description	Where Documented
5.1(1)	Enhancements to the upgrade process through the GUI when upgrading the APIC or switch software.	Beginning with release 5.1(1), the upgrade process for the Cisco APIC and switch software through the GUI has been enhanced.	Upgrading or Downgrading with APIC Release 5.1 or Later Using the GUI, on page 89
5.1(1)	Additional validations are performed before an upgrade or downgrade operation is triggered.	When upgrading or downgrading the software, additional validations are performed and warnings are provided as part of the 5.1(1) release if issues are found during those validations.	Upgrading or Downgrading with APIC Release 5.1 or Later Using the GUI, on page 89
4.2(5)	Additional validations are performed before an upgrade or downgrade operation is triggered.	Beginning with release 4.2(5), when you attempt to trigger an upgrade or downgrade operation, before the operation is triggered, additional validations are performed and warnings are provided if issues are found during those validations.	• Upgrading or Downgrading with APIC Releases 4.x or 5.0 Using the GUI, on page 79 • Upgrading or Downgrading with APIC Release 5.1 or Later Using the GUI, on page 89
4.2(5)	Additional information provided when upgrading the controllers.	Beginning with release 4.2(5), additional information may be provided on the status of the upgrade process for the controllers.	• Upgrading or Downgrading with APIC Releases 4.x or 5.0 Using the GUI, on page 79 • Upgrading or Downgrading with APIC Release 5.1 or Later Using the GUI, on page 89
4.2(5)	Additional information provided when upgrading switch nodes in firmware upgrade groups.	Beginning with release 4.2(5), status is provided on the progress of the download of the firmware when upgrading switch nodes in firmware upgrade groups.	• Upgrading or Downgrading with APIC Releases 4.x or 5.0 Using the GUI, on page 79 • Upgrading or Downgrading with APIC Release 5.1 or Later Using the GUI, on page 89
4.2(5)	The number of switches that the system can upgrade at a time has changed.	Beginning with release 4.2(5), by default, the number of switches that the system can upgrade at a time has changed from 20 to unlimited.	• Upgrading or Downgrading with APIC Releases 4.x or 5.0 Using the GUI, on page 79 • Upgrading or Downgrading with APIC Release 5.1 or Later Using the GUI, on page 89

Cisco APIC Release Version	Feature	Description	Where Documented
4.2(1)	Validations are performed before an upgrade or downgrade operation is triggered.	Beginning with release 4.2(1), when you attempt to trigger an upgrade or downgrade operation, before the operation is triggered, some validations are performed and warnings are provided if faults are found during those validations.	• Upgrading or Downgrading with APIC Releases 4.x or 5.0 Using the GUI, on page 79 • Upgrading or Downgrading with APIC Release 5.1 or Later Using the GUI, on page 89
	APIC upgrade and downgrade paths removed from document	The Cisco APIC upgrade and downgrade paths have been removed from this document. Refer to the *Cisco APIC Upgrade/Downgrade Support Matrix* for Cisco APIC upgrade and downgrade paths, available here: https://www.cisco.com/c/dam/en/us/td/docs/Website/datacenter/apicmatrix/index.html	
4.1(2x)	Silent Roll Package Upgrade	A silent roll package upgrade enables you to manually perform an internal package upgrade for ACI switch hardware SDK, drivers, and so on, without upgrading the entire ACI switch software OS.	Silent Roll Package Upgrade, on page 133
	The *Cisco APIC Installation, Upgrade, and Downgrade Guide, Release 4.0(1)* document is no longer available	The *Cisco APIC Installation, Upgrade, and Downgrade Guide, Release 4.0(1)* document is no longer available. All the information that was previously in that document is now available in this document, other than the upgrade and downgrade paths.	
4.0(1)	Bash no longer supported as upgrade method	Starting with Cisco APIC release 4.0(1), you cannot use bash to upgrade the Cisco APIC and switch software. Use the NX-OS style CLI to upgrade the Cisco APIC and switch software instead.	• Upgrading or Downgrading with APIC Releases 4.x or 5.0 Using the GUI, on page 79 • Upgrading or Downgrading with APIC Release 5.1 or Later Using the GUI, on page 89

Cisco APIC Release Version	Feature	Description	Where Documented
4.0(1)	Changes to upgrade procedure using the GUI	The procedures for upgrading the software using the GUI has changed starting with Cisco APIC release 4.0(1).	• Upgrading or Downgrading with APIC Releases 4.x or 5.0 Using the GUI, on page 79 • Upgrading or Downgrading with APIC Release 5.1 or Later Using the GUI, on page 89
3.2(1m)	Cisco APIC long-lived release		Cisco ACI Long-Lived and Short-Lived Releases, on page 7
2.3(1e)	Network Configuration Capabilities and Changes During Mixed OS Operation	Support for additional features was added.	Operations Allowed During Mixed Versions on Cisco ACI Switches, on page 57
2.2(2e)	Network Configuration Capabilities and Changes During Mixed OS Operation	This feature was introduced.	Operations Allowed During Mixed Versions on Cisco ACI Switches, on page 57
2.2(2e)	--	The contents of this guide was reorganized. The High Availability for Cisco APIC Cluster content that was in this guide for earlier releases is now migrated in the *Cisco APIC Getting Started Guide, Release 2.x*.	--
2.2(1n)	High Availability for APIC Cluster	The high availability functionality for a Cisco APIC cluster enables you to operate the Cisco APICs in a cluster in an Active/Standby mode.	This content is available in the *Cisco APIC Getting Started Guide, Release 2.x*
1.3(1g)	The title of this document has been changed.	The old name was Cisco APIC Firmware Management Guide.	

CHAPTER 2

Cisco ACI Long-Lived and Short-Lived Releases

About Long-Lived Releases

Cisco ACI long-lived releases are software releases intended to help you stay on a given release on a long-term basis (up to approximately 18 months), while benefiting from frequent maintenance drops to ensure quality and stability. Cisco may support two long-lived releases at any given point of time. However, active maintenance will be focused primarily on the latest long-lived release. These releases will be maintained for a longer time span than other releases. Long-lived releases are recommended for the deployment of widely adopted functions or for networks that will not be upgraded frequently.

All long-lived releases support upgrade or downgrade to the next or previous long-lived release. See the APIC Upgrade/Downgrade Support Matrix for confirmed support.

Note　Some release branches might be supported as long-lived releases while others might not be supported. For example, there might be three 2.*x* release branches: 2.1, 2.2, and 2.3. However, one of the three 2.*x* release branches might be supported as a long-lived release (2.2), while the other two release branches (2.1 and 2.3) might not be supported as long-lived releases.

About Short-Lived Releases

Cisco ACI short-lived releases are stable, quality releases delivered for new feature functionalities. These releases have limited maintenance support for a duration of six months after the initial release, after which there will be no active maintenance. In addition, these releases will not have an EOS announcement.

As with every Cisco ACI release, upgrades may be supported from two previous releases to the short-lived release. See the APIC Upgrade/Downgrade Support Matrix for confirmed support.

Long-Lived Release Life Cycles

- The life cycle of a major long-lived release starts with the first customer shipment (FCS) of the first minor release.

- The major release then enters the maintenance release introduction phase, in which several releases are made available to address product defects.

- Afterward, the major release transitions to the mature maintenance phase. In this phase, the release receives defect repairs only for severity 1 and severity 2 defects found by the customer. Defects found internally are addressed on a case-by-case basis.

- All long-lived releases support upgrade or downgrade to the next or previous long-lived release last maintenance version respectively

We recommend that customers with new and existing Cisco Nexus 9000 ACI-Mode Switches and Cisco Application Policy Infrastructure Controller (APIC) deployments choose from the following long-lived releases:

Long-Lived Cisco APIC Release Version	Long-Lived Cisco Switch Release Version
5.2(x)	15.2(x)
4.2(x)	14.2(x)

We recommend that you upgrade to the latest maintenance release and patch for a particular long-lived release version. You can download the latest Cisco Nexus 9000 ACI-Mode Switches and Cisco APIC deployments from the appropriate Cisco Software Download pages.

Installing or Recovering Cisco APIC Images

Installation Notes

- For hardware installation instructions, see the Cisco ACI Fabric Hardware Installation Guide.

- Back up your Cisco APIC configuration prior to installing or upgrading to this release. Single Cisco APIC clusters, which should not be run in production, can lose their configuration if database corruption occurs during the installation or upgrade.

- For instructions on how to access the Cisco APIC for the first time, see the Cisco APIC Getting Started Guide.

- Cisco ACI with Microsoft System Center Virtual Machine Manager (SCVMM) or Microsoft Windows Azure Pack only supports ASCII characters. Non-ASCII characters are not supported. Ensure that English is set in the System Locale settings for Windows, otherwise Cisco ACI with SCVMM and Windows Azure Pack will not install. In addition, if the System Locale is later modified to a non-English Locale after the installation, the integration components might fail when communicating with the Cisco APIC and the Cisco ACI fabric.

- For the Cisco APIC Python SDK documentation, including installation instructions, see the Cisco APIC Python SDK Documentation.

  The SDK egg file that is needed for installation is included in the package. The egg filename has the following format:

  ```
  acicobra-A.B_CD-py2.7.egg
  ```

  - *A*: The major release number.

  - *B*: The minor release number.

> • *C*: The maintenance release number.
>
> • *D*: The release letter (patch letter). The letter is in lowercase.

For example, the egg filename for the 5.2(4d) release is as follows:

```
acicobra-5.2_4d-py2.7.egg
```

- Installation of the SDK with SSL support on Unix/Linux and Mac OS X requires a compiler. For a Windows installation, you can install the compiled shared objects for the SDK dependencies using wheel packages.

- The model package depends on the SDK package; be sure to install the SDK package first.

- Beginning with Cisco APIC 6.0 (2), support for a new type of SSL certificate - ECDSA certificate has been enabled. This certificate is not supported on the previous versions of Cisco APIC. If you have deployed the ECDSA certificate and then downgrade to a previous version of Cisco APIC, the Cisco APIC web server will not work. You must update your Cisco APIC web server to use a RSA-based certificate before downgrading to a version lower than Cisco APIC 6.0 (2).

Usage Guidelines

- The Cisco APIC GUI supports the following browsers:

  - Chrome version 59 (at minimum) on Mac and Windows

  - Firefox version 54 (at minimum) on Mac, Linux, and Windows

  - Internet Explorer version 11 (at minimum)

  - Safari 10(at minimum)

Note Restart your browser after upgrading to release 1.3(1).

- The Cisco APIC GUI includes an online version of the Quick Start guide that includes video demonstrations.

- The infrastructure IP address range must not overlap with other IP addresses used in the fabric for in-band and out-of-band networks.

- The Cisco APIC does not provide IPAM services for tenant workloads.

- To reach the Cisco APIC CLI from the GUI: select System > Controllers, highlight a controller, right-click and select "launch SSH". To get the list of commands, press the escape key twice.

- In some of the 5-minute statistics data, the count of ten-second samples is 29 instead of 30.

- For the following services, use a DNS-based host name with out-of-band management connectivity. IP addresses can be used with both in-band and out-of-band management connectivity.

  - Syslog server

  - Call Home SMTP server

- Tech support export server

- Configuration export server

- Statistics export server

- Both leaf and spine switches can be managed from any host that has IP connectivity to the fabric.

- When configuring an atomic counter policy between two endpoints, and an IP is learned on one of the two endpoints, it is recommended to use an IP-based policy and not a client endpoint-based policy.

- When configuring two Layer 3 external networks on the same node, the loopbacks need to be configured separately for both Layer 3 networks.

- All endpoint groups (EPGs), including application EPGs and Layer 3 external EPGs, require a domain. Interface policy groups must also be associated with an Attach Entity Profile (AEP), and the AEP must be associated with domains. Based on the association of EPGs to domains and of the interface policy groups to domains, the ports and VLANs that the EPG uses are validated. This applies to all EPGs including bridged Layer 2 outside and routed Layer 3 outside EPGs. For more information, see the Cisco Fundamentals Guide and the KB: Creating Domains, Attach Entity Profiles, and VLANs to Deploy an EPG on a Specific Port article.

> **Note** In the 1.0(4x) and earlier releases, when creating static paths for application EPGs or Layer 2/Layer 3 outside EPGs, the physical domain was not required. In this release, it is required. Upgrading without the physical domain will raise a fault on the EPG stating "invalid path configuration."

- The only place to associate an EPG with a contract interface is within its own tenant.

- User passwords must meet the following criteria:

    - Minimum length is 8 characters

    - Maximum length is 64 characters

    - Fewer than three consecutive repeated characters

    - At least three of the following character types: lowercase, uppercase, digit, symbol

    - Cannot be easily guessed

    - Cannot be the username or the reverse of the username

    - Cannot be any variation of "cisco", "isco", or any permutation of these characters or variants obtained by changing the capitalization of letters therein

- The power consumption statistics are not shown on leaf switch node slot 1.

- For Layer 3 external networks created through the API or Advanced GUI and updated through the CLI, protocols need to be enabled globally on the external network through the API or Advanced GUI, and the node profile for all the participating nodes needs to be added through the API or Advanced GUI before doing any further updates through the CLI.

- For Layer 3 external networks created through the CLI, you should not to update them through the API. These external networks are identified by names starting with "__ui_".

- The output from "show" commands issued in the NX-OS-style CLI are subject to change in future software releases. Cisco does not recommend using the output from the show commands for automation.

- In this software version, the CLI is supported only for users with administrative login privileges.

- Do not separate virtual private cloud (vPC) member nodes into different configuration zones. If the nodes are in different configuration zones, then the vPCs' modes become mismatched if the interface policies are modified and deployed to only one of the vPC member nodes.

- If you defined multiple login domains, you can choose the login domain that you want to use when logging in to a Cisco APIC. By default, the domain drop-down list is empty, and if you do not choose a domain, the DefaultAuth domain is used for authentication. This can result in login failure if the username is not in the DefaultAuth login domain. As such, you must enter the credentials based on the chosen login domain.

- A firmware maintenance group should contain a maximum of 80 nodes.

- When contracts are not associated with an endpoint group, DSCP marking is not supported for a VRF with a vzAny contract. DSCP is sent to a leaf switch along with the actrl rule, but a vzAny contract does not have an actrl rule. Therefore, the DSCP value cannot be sent.

- We recommend that you should not use a leaf switch as a NTP server for the Cisco ACI fabric.

Conditions for Recovering or Installing Cisco APIC Software Image

This chapter describes how to install or recover a Cisco APIC. You recover the Cisco APIC image when your existing server has a Cisco APIC image that is completely unresponsive, and you want a new Cisco APIC image installed in it.

Note If you have an existing UCS server, skip to the Installing Cisco APIC Software section.

Installing the Cisco APIC image accomplishes the following tasks:

- It erases the existing data on the disks

- It reformats the disks

- It installs a new software image

You can use one of the following methods to install your Cisco APIC software in a server:

- Using a PXE server

- Using virtual media

Note You can use the Cisco APIC ISO image files for installation just as you perform any other virtual media installation. The detailed steps are not described in this document.

Installing the Cisco APIC Software on an APIC Server M1/L1, M2/L2, or M3/L3 Using a PXE Server

This procedure installs the Cisco Application Policy Infrastructure Controller (APIC) software on an APIC server M1/L1, M2/L2, or M3/L3 using a Preboot Execution Environment (PXE) server.

Procedure

Step 1   Configure the PXE server with a standard configuration for Linux.

Step 2   Verify that the PXE configuration file has an entry similar to the following for installing a Cisco APIC software image for release 4.0 or later.

```
label 25
   kernel vmlinuz dd blacklist=isci blacklist=ahci nodmraid noprobe=ata1 noprobe=ata2
noprobe=ata3 noprobe=ata4
   append initrd=initrd root=live:squashfs.img_URL rd.live.img rd.live.debug=1 rd.live.ram=1
 rd.debug atomix.isourl=iso_URL
```

Example:

```
label 25
   kernel ifcimages/vmlinuz dd blacklist=isci blacklist=ahci nodmraid noprobe=ata1
noprobe=ata2 noprobe=ata3 noprobe=ata4
   append initrd=ifcimages/initrd.img
root=live:http://192.0.2.10/myisomount/LiveOS/squashfs.img rd.live.img rd.live.debug=1
rd.live.ram=1 rd.debug atomix.isourl=http://192.0.2.10/aci-apic-dk9.4.0.0.iso
```

Step 3   Download the Cisco APIC .iso image from Cisco.com.

Step 4   Create the mount folder and mount the Cisco APIC .iso image.

```
$ mkdir -p mount_folder
$ mount –t iso9660 –o loop iso_image mount_folder
```

Example:

```
$ cd /home/user
$ mkdir -p myisomount
$ mount –t iso9660 –o loop /local/aci-apic-dk9.4.0.0.iso myisomount
```

Step 5   Verify that the `initrd.img` and `vmlinuz` files are in the mount folder location.

Example:

```
$ ls /home/user/myisomount/images/pxeboot/
initrd.img  vmlinuz
```

Step 6   Copy `vmlinuz` and `intird` from the mounted Cisco APIC .iso image to your tftpboot path.

Example:

```
$ mkdir -p /var/lib/tftpboot/ifcimages
$ cp -f /home/user/myisomount/images/pxeboot/vmlinuz /var/lib/tftpboot/ifcimages/
$ cp -f /home/user/myisomount/images/pxeboot/initrd.img /var/lib/tftpboot/ifcimages/
```

Step 7 Copy the Cisco APIC .iso image and the mount folder to your HTTP root directory.

Example:

```
$ cp -R /local/aci-apic-dk9.4.0.0.iso /var/www/html
$ cp -R /home/user/myisomount /var/www/html
```

Step 8 Add an entry to the PXE configuration (`/var/lib/tftpboot/pxelinux.cfg/default`) so that it points to the kickstart file for the Cisco APIC .iso image.

Example:

```
[root@pxeserver ~]# cat /var/lib/tftpboot/pxelinux.cfg/default
label 25
    kernel ifcimages/vmlinuz dd blacklist=isci blacklist=ahci nodmraid noprobe=ata1
noprobe=ata2 noprobe=ata3 noprobe=ata4
    append initrd=ifcimages/initrd.img
root=live:http://192.0.2.10/myisomount/LiveOS/squashfs.img rd.live.img rd.live.debug=1
rd.live.ram=1 rd.debug atomix.isourl=http://192.0.2.10/aci-apic-dk9.4.0.0.iso
```

You use this information to verify that your PXE menu entry images set up correctly.

Step 9 Restart the PXE servers.

Step 10 Reboot the Cisco APIC and press F12 for network boot.

Step 11 Choose the options configured on the PXE server to boot the Cisco APIC image.

Installing the Cisco APIC Software on an APIC Server M4/L4 Using a PXE Server

This procedure installs the Cisco Application Policy Infrastructure Controller (APIC) software on an APIC server M4/L4 using a Preboot Execution Environment (PXE) server:

Procedure

Step 1 Install the DNSMasq package and an HTTP server package in the PXE server.

Step 2 Download the ISO you wish to install into a path where your PXE server will host the file, such as `/var/www/html.`

Step 3 Unpack or mount the ISO as appropriate.

Example:

```
$ sudo mkdir /mnt/iso /mnt/efi
$ sudo mount -oloop /var/www/html/aci-apic-dk9.6.0.2b.iso /mnt/iso
$ sudo mount -t vfat /mnt/iso/images/efiboot.img /mnt/efi
```

Step 4 Copy the installer EFI files to the PXE server TFTP path, such as /srv/tftp.

Example:

```
$ cp -av /mnt/efi/EFI/BOOT/*.EFI /srv/tftp/
```

Step 5 Unmount the ISO.

Example:

```
$ sudo umount /mnt/efi
$ sudo umount /mnt/iso
```

Step 6 Configure DNSMasq.

Example:

The following text is an example configuration; modify as necessary for your setup. Save this in the /etc/dnsmasq.conf configuration file, overwriting the default configuration.

```
interface=*
bind-interfaces
enable-tftp
tftp-root=/srv/tftp
port=0
log-dhcp
dhcp-no-override

# UEFI PXE clients only.
dhcp-vendorclass=BIOS,PXEClient:Arch:00000

# Boot directly into shim.
dhcp-boot="BOOTX64.EFI"

# Use this option to pass parameters to the installer. Currently only
# atxi.wipe= and atomix.isourl are supported.
dhcp-option-force=129,"atomix.isourl=http://ipaddress-of-PXE-server/path/to/install/iso"

# Create a DHCP range and set the gateway.
dhcp-range=rack-rack1-data0,192.168.41.0,static,255.255.255.0,infinite
dhcp-option=rack-rack1-data0,3,192.168.41.1

# Static mapping for clients.
dhcp-host=52:54:00:a2:34:c0,,192.168.41.2,brick2-data2,infinite
dhcp-host=52:54:00:a2:34:02,,192.168.41.3,brick2-data3,infinite
dhcp-host=52:54:00:a2:34:03,,192.168.41.4,brick2-data4,infinite
```

Step 7 Restart the PXE servers.

Step 8 Reboot the Cisco APIC and press F12 for network boot.

Installing Cisco APIC Using a PXE Server

You can install Cisco Application Policy Infrastructure Controller (APIC) ISO for UEFI, UEFI SecureBoot, and Legacy BIOS systems using a PXE server.

Ensure that you have the following software installed on your system:

```
sudo apt install -y dnsmasq lighttpd syslinux-common pxelinux
```

DNSMasq Configuration

To create a new **dnsmasq** configuration, run the following command:

```
$ sudo systemctl stop dnsmasq
$ sudo mv /etc/dnsmasq.conf /etc/dnsmasq.conf.orig
$ sudo mkdir -p /srv/tftp
```

In the following code snippet, you must enter the IP details of your HTTP server that is hosting ISO and then configure a DHCP subnet range for clients which must be able to reach the HTTP server's IP. After you save your configuration file with the changes, run the following command:

```
sudo systemct restart dnsmasq

interface=*
bind-interfaces
enable-tftp
tftp-root=/srv/tftp
port=0
log-dhcp
dhcp-no-override

dhcp-match=x86PC,  option:client-arch, 0  # matches legacy BIOS x86
dhcp-match=BC_EFI, option:client-arch, 7  # matches UEFI x86-64

# Load different PXE boot image depending on client architecture
pxe-service=tag:x86PC,X86PC,   "Install Linux on x86 BIOS",    pxelinux.0
pxe-service=tag:BC_EFI,BC_EFI, "Install Linux on x86-64 UEFI", bootx64.efi

# Set bootfile name only when tag is "bios" or "uefi"
dhcp-boot=tag:x86PC,pxelinux.0      # for Legacy BIOS detected by dhcp-match above
dhcp-boot=tag:BC_EFI,bootx64.efi    # for UEFI arch detected by dhcp-match above

# Enable PXELinux client options
dhcp-option=tag:x86PC,208,f1:00:74:7e  # pxelinux.magic string

# set boot params, note the ip/network is tied to the netplan config in this layer
dhcp-option-force=129,"atxi.wipe=true atomix.isourl=http://<IP of your HTTP
server>/atomix.iso"

# an example IPV4 subnet range
dhcp-range=192.168.41.3,192.168.41.50,12h
dhcp-lease-max=25
```

HTTP Configuration

The default **lighttpd** configuration file will work as it is with no changes required as it listens on all interfaces for port 80.

> **Note** The name of the file must match the `/etc/dnsmasq.conf` value in the `dhcp-option-force=129` setting. This value is passed into the machine through the DHCP settings and will use the URL to download the **iso** file.
>
> Copy the installer **iso** file to following path:
>
> `/var/www/html/<ISONAME.iso>`

PXELINUX Configuration

Systems that reboot through BIOS/Legacy uses pxelinux to acquire the installer. Ensure that the **tftp** location in the **DNSMasq** configuration file above is used to copy these files and configurations or adjust the commands as needed.

```
sudo mkdir -p /srv/tftp
sudo cp -av /usr/lib/PXELINUX/* /srv/tftp/
sudo cp /usr/lib/syslinux/modules/bios/* /srv/tftp/
sudo mkdir -p /srv/tftp/pxelinux.cfg
```

Copy the following configuration to this `/srv/tftp/pxelinux.cfg/default` location and modify the HTTP URL to match the HTTP server's IP and path to the ISO.

```
DEFAULT atomix-install

label atomix-install
  kernel vmlinuz
  append initrd=initrd.img ro verbose debug console=tty0 console=ttyS0,115200n8
atomix.isourl=http://<HTTP_IP>/<ISO NAME>
  sysappend 3
```

Extracting content from ISO

Once you've acquired the ISO, you need to extract some files from the ISO and place them in certain directories, as shown below:

```
$ sudo mkdir /mnt/iso /mnt/efi
$ sudo mount -oloop /var/www/html/<ISO filename> /mnt/iso
$ sudo mount -t vfat /mnt/iso/images/efiboot.img /mnt/efi
$ cp -av /mnt/efi/EFI/BOOT/BOOTX64.efi /srv/tftp/bootx64.efi
$ cp -av /mnt/efi/EFI/BOOT/GRUBX64.efi /srv/tftp/grubx64.efi
$ cp -av /mnt/iso/isolinux/vmlinuz /srv/tftp/vmlinuz
$ cp -av /mnt/iso/isolinux/initrd.img /srv/tftp/initrd.img
$ sudo umount /mnt/efi
$ sudo umount /mnt/iso
```

Testing

Once you apply the configuration, your test systems must boot into the installer and configure the networking settings and download the ISO through HTTP to the system and proceed with the install.

On the PXE server, you can use the following **dnsmasq** service:

```
sudo journalctl --follow -u dnsmasq
```

✎

Note   Some of the **dnsmasq** log entries may display an error as shown below. However, these errors are not fatal and the UEFI PXE clients in the firmware will try again.

```
Feb 17 01:01:25 ubuntu dnsmasq-dhcp[1201]: 1836224829 sent size: 10 option: 43 vendor-encap
  06:01:08:0a:04:00:50:58:45:ff
Feb 17 01:01:25 ubuntu dnsmasq-tftp[1201]: error 8 User aborted the transfer received from
 192.168.41.3
Feb 17 01:01:25 ubuntu dnsmasq-tftp[1201]: failed sending /srv/tftp/bootx64.efi to
192.168.41.3
Feb 17 01:01:25 ubuntu dnsmasq-tftp[1201]: sent /srv/tftp/bootx64.efi to 192.168.41.3
Feb 17 01:01:47 ubuntu dnsmasq-tftp[1201]: error 3 User provided memory block is too small
 received from 192.168.41.3
Feb 17 01:01:47 ubuntu dnsmasq-tftp[1201]: failed sending /srv/tftp/grubx64.efi to
192.168.41.3
Feb 17 01:02:09 ubuntu dnsmasq-tftp[1201]: sent /srv/tftp/grubx64.efi to 192.168.41.3
```

On the PXE client, the serial console output shows the install and in particular displays how it acquires the ISO.

This is part of the installer output that displays how it acquires the installer **iso** file.

```
++ cmdline=' BOOT_IMAGE=vmlinuz initrd=initrd.img ro verbose debug console=tty0
console=ttyS0,115200n8 atomix.isourl=http://192.168.41.2/atomix.iso ip=192.168.41.41:192.'
++ case "$cmdline" in
++ val='http://192.168.41.2/atomix.iso
ip=192.168.41.41:192.168.41.2:192.168.41.2:255.255.255.0 BOOTIF=01-52-54-00-12-34-56 '
++ val=http://192.168.41.2/atomix.iso
++ echo http://192.168.41.2/atomix.iso
+ ksurl=http://192.168.41.2/atomix.iso
+ '[' -z http://192.168.41.2/atomix.iso ']'
+ '[' -n http://192.168.41.2/atomix.iso ']'
+ '[' -z '' ']'
+ dhclient
[    3.573160] 8021q: adding VLAN 0 to HW filter on device ens4
+ tmpiso=/tmp/atomix.iso
++ seq 1 3
+ for count in $(seq 1 3)
+ '[' http: = https ']'
+ busybox wget --output-document=/tmp/atomix.iso http://192.168.41.2/atomix.iso
Connecting to 192.168.41.2 (192.168.41.2:80)
atomix.iso           100% |*******************************|  842M  0:00:00 ETA
+ break
+ mkdir -p /cdrom
+ mount -o loop,ro /tmp/atomix.iso /cdrom
[    4.896038] ISO 9660 Extensions: RRIP_1991A
+ echo 'Found install image through PXE'
Found install image through PXE
...
```

Installing Cisco APIC Software Using Virtual Media

Installing or upgrading the Cisco Application Policy Infrastructure Controller (APIC) software using virtual media (vMedia) requires the following high-level process:

- Upgrade the Cisco Integrated Management Controller (CIMC) software, if necessary.

- Obtain the relevant Cisco APIC .iso image from Cisco.com.

- Access the CIMC web interface for the controller.

> **Note**　For detailed instructions on accessing the CIMC and managing virtual media, please see the corresponding CIMC Configuration Guide for your controller's version of CIMC software (1.5 or 2.0).

- Mount the .iso image using the CIMC vMedia functionality.

- Boot or power cycle the controller.

- During the boot process, press **F6** to select **Cisco CIMC-Mapped vDVD** as the one-time boot device. You may be required to enter the BIOS password. The default password is **password**.

- Follow the onscreen instructions to install the Cisco APIC software.

Note

- Beginning with Cisco APIC releases 5.3(1) and 6.0(2), we recommend that you install the image through the network using HTTP. Not installing the image through the network may significantly increase the installation time.

  You can provide a URL of the image location when you are prompted with the message "To speed up the install, enter the ISO URL:". Answer the prompts by entering the relevant host networking configuration details, such as the IP address, subnet, gateway, and image path.

  The prompt to speed up the installation lists HTTP and NFS as supported options, but only HTTP is supported.

  Beginning with Cisco APIC release 6.0(2), you can install the image only through the network. You must provide an URL of the image location, or the installation will pause indefinitely. Answer the prompts by entering the relevant host networking configuration details, such as the IP address, subnet, gateway, and image path.

- Enable the CIMC console redirection for Cisco UCS 220 M5 and Cisco UCS 225 M6 servers before you install the Cisco APIC software using the CIMC Virtual Media. You must reboot Cisco APIC for the changes to take effect for next CIMC Virtual Media installation.

Upgrading the CIMC Software

If you upgrade the Cisco APIC software in the Cisco ACI fabric, you might also have to upgrade the version of CIMC that is running on your fabric. Therefore, we recommend that you check the appropriate Cisco APIC Release Notes for the list of the supported CIMC software versions for each Cisco APIC release. The Cisco APIC Release Notes are available on the APIC documentation page.

In order to upgrade the CIMC software, you must first determine the type of UCS C Series server that you have for the Cisco APICs in your fabric.

Cisco APICs use the following UCS C Series servers:

- Cisco UCS 225 M6 (fourth generation appliances APIC-SERVER-M4 and APIC-SERVER-L4)

- Cisco UCS 220 M5 (third generation appliances APIC-SERVER-M3 and APIC-SERVER-L3)

- Cisco UCS 220 M4 (second generation appliances APIC-SERVER-M2 and APIC-SERVER-L2)

- Cisco UCS 220 M3 (first generation appliance APIC-SERVER-M1 and APIC-SERVER-L1)

The Cisco APIC versions of these servers differ from the standard versions in that the Cisco APIC versions are manufactured with an image secured with the Trusted Platform Module (TPM) certificates and an APIC product ID (PID).

The following table provides more information on each of these Cisco APIC servers:

APIC Platform	Corresponding UCS Platform	Description
APIC-SERVER-M1	UCS-C220-M3	Cluster of three Cisco APIC first-generation controllers, with a medium-sized CPU, hard drive, and memory configurations for up to 1000 edge ports.
APIC-SERVER-M2	UCS-C220-M4	Cluster of three Cisco APIC second-generation controllers, with a medium-sized CPU, hard drive, and memory configurations for up to 1000 edge ports.
APIC-SERVER-M3	UCS-C220-M5	Cluster of three Cisco APIC second-generation controllers, with a medium-sized CPU, hard drive, and memory configurations for up to 1000 edge ports.
APIC-SERVER-M4	UCS-C225-M6	Cluster of three Cisco APIC second-generation controllers, with a medium-sized CPU, hard drive, and memory configurations for up to 1000 edge ports.
APIC-SERVER-L1	UCS-C220-M3	Cluster of three Cisco APIC first-generation controllers, with a large-sized CPU, hard drive, and memory configurations for more than 1000 edge ports.
APIC-SERVER-L2	UCS-C220-M4	Cluster of three Cisco APIC second-generation controllers, with a large-sized CPU, hard drive, and memory configurations for more than 1000 edge ports.
APIC-SERVER-L3	UCS-C220-M5	Cluster of three Cisco APIC second-generation controllers, with a large-sized CPU, hard drive, and memory configurations for more than 1000 edge ports.
APIC-SERVER-L4	UCS-C225-M6	Cluster of three Cisco APIC second-generation controllers, with a large-sized CPU, hard drive, and memory configurations for more than 1000 edge ports.

These procedures describe how to upgrade the Cisco APIC CIMC using the Cisco Host Upgrade Utility (HUU). Full instructions for upgrading software using the HUU are provided in Upgrading the Firmware on a Cisco UCS C-Series Server Using the HUU.

Before you begin

- Review the information that is provided in the Cisco APIC Release Notes and confirm which CIMC software image that you should use for the upgrade. The Cisco APIC Release Notes are available on the APIC documentation page.

- Obtain the software image from the Software Download site.

- Confirm that the MD5 checksum of the image matches the one published on Cisco.com.

- Allow for the appropriate amount of time for the upgrade.

  The time needed for the process of upgrading a CIMC version varies, based on the speed of the link between the local machine and the UCS-C chassis, and the source/target software image, as well as other internal component versions.

- Changing the CIMC version might also require changes to the Internet browser and Java software version to run the vKVM.

Note   Upgrading the CIMC version does not affect the production network as the Cisco APICs are not in the data path of the traffic. Also, you do not have to decommission the Cisco APICs when upgrading the CIMC software.

Procedure

Step 1   Log in to the CIMC using the CIMC credentials.

Note that the CIMC credentials may be different from the Cisco APIC credentials.

Step 2   Determine the model of UCS platform for your Cisco APIC through the CIMC GUI.

a)   Locate the PID entry displayed under **Server** > **Summary**.
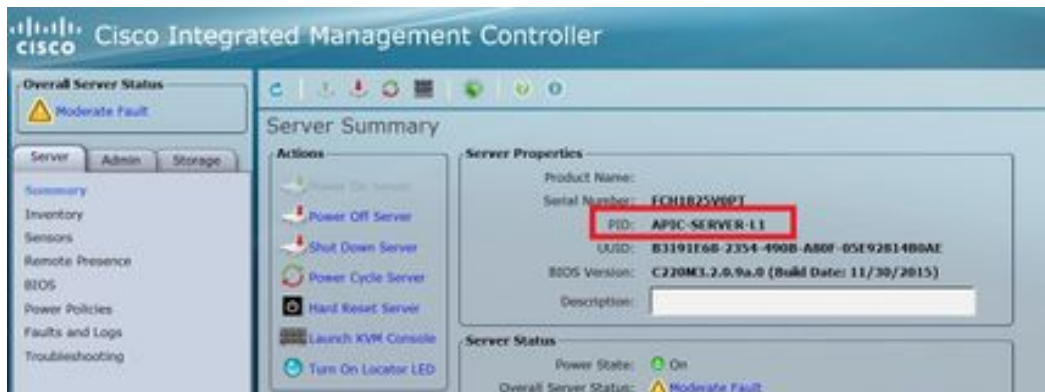
b)   Use the table provided at the beginning of this procedure to find the corresponding UCS platform for the APIC platform displayed in the PID entry.

For example, you would see that the **APIC-SERVER-L1** entry shown in the example above would map to the UCS-C220-M3 platform, based on the information provided at the beginning of this procedure.

Step 3   Locate the appropriate HUU .iso image at https://software.cisco.com/download.

a) In the search window in https://software.cisco.com/download, enter the UCS platform model that you found for your Cisco APIC in the previous step, without the dashes.

Using the example from the previous step, you might enter **UCS C220 M3** in the search window.

b) Click on the link from the search result to show the software that is available for your UCS platform.

c) In the list of software available for your server, locate the firmware entry, which will be shown with an entry such as **Unified Computing System (UCS) Server Firmware**, and click on that firmware link.

d) Locate the **Cisco UCS Host Upgrade Utility** .iso image link and make a note of the release information for this image.

Step 4 Go to the Recommended Cisco APIC and Cisco Nexus 9000 Series ACI-Mode Switches Releases document and locate the row that contains the appropriate entry for your UCS platform and APIC software release.

Keep in mind that the UCS version shown in the table might not be the latest version of CIMC software, based on corresponding APIC release. For example, for the 3.0 branch of the APIC release, the corresponding CIMC software release might be 3.0(3e). While that is not necessarily the latest release of the CIMC software, it is the correct version of the CIMC software for the 3.0 branch of the APIC release.

Step 5 Compare the information from the two sources to verify that you are downloading the correct version of the HUU .iso image.

If you find conflicting information between the two sources, use the information provided in the Recommended Cisco APIC and Cisco Nexus 9000 Series ACI-Mode Switches Releases document as the final word on the correct version of the HUU .iso image for your UCS platform and APIC software release.

Step 6 Download the appropriate HUU .iso image from the https://software.cisco.com/download site.

Step 7 Launch the KVM console from CIMC GUI.
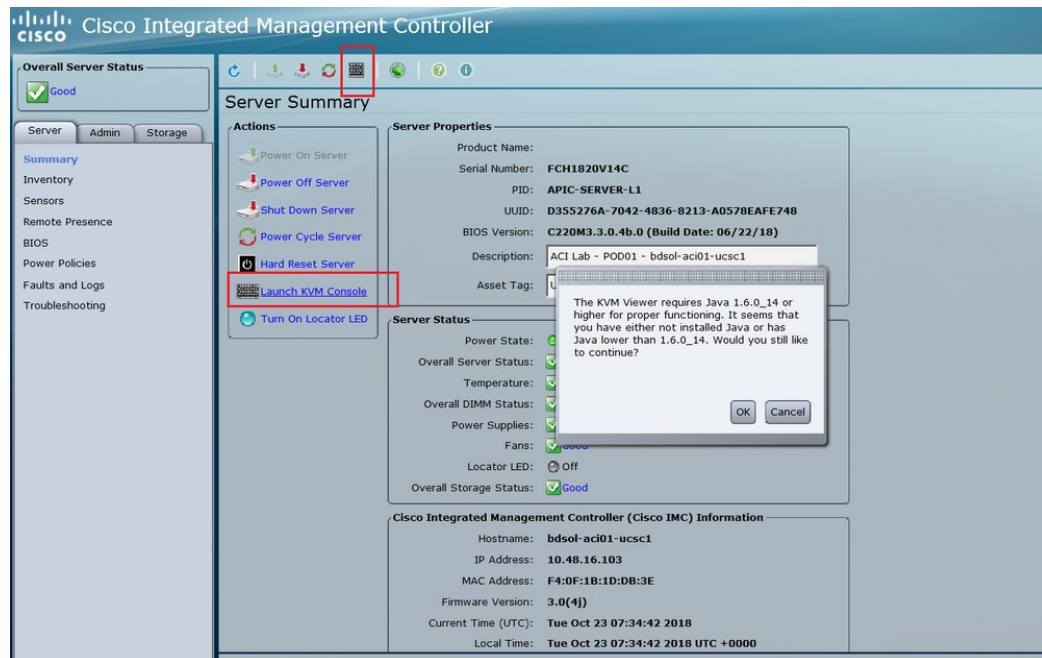
Note If you are having problems opening the KVM console, this is generally an issue with your Java version. Review the information in the Cisco APIC Release Notes, available on the APIC documentation page, for your CIMC version to learn the different workarounds available.

Step 8 In the KVM console, click **Virtual Media** > **Activate Virtual Devices** and accept the session.

Step 9 Click **Virtual Media** > **Map CD/DVD** and navigate to the downloaded HUU .iso image on your PC.

Step 10 Select the downloaded HUU .iso image, then click **Map Device** to map the downloaded ISO on your PC.
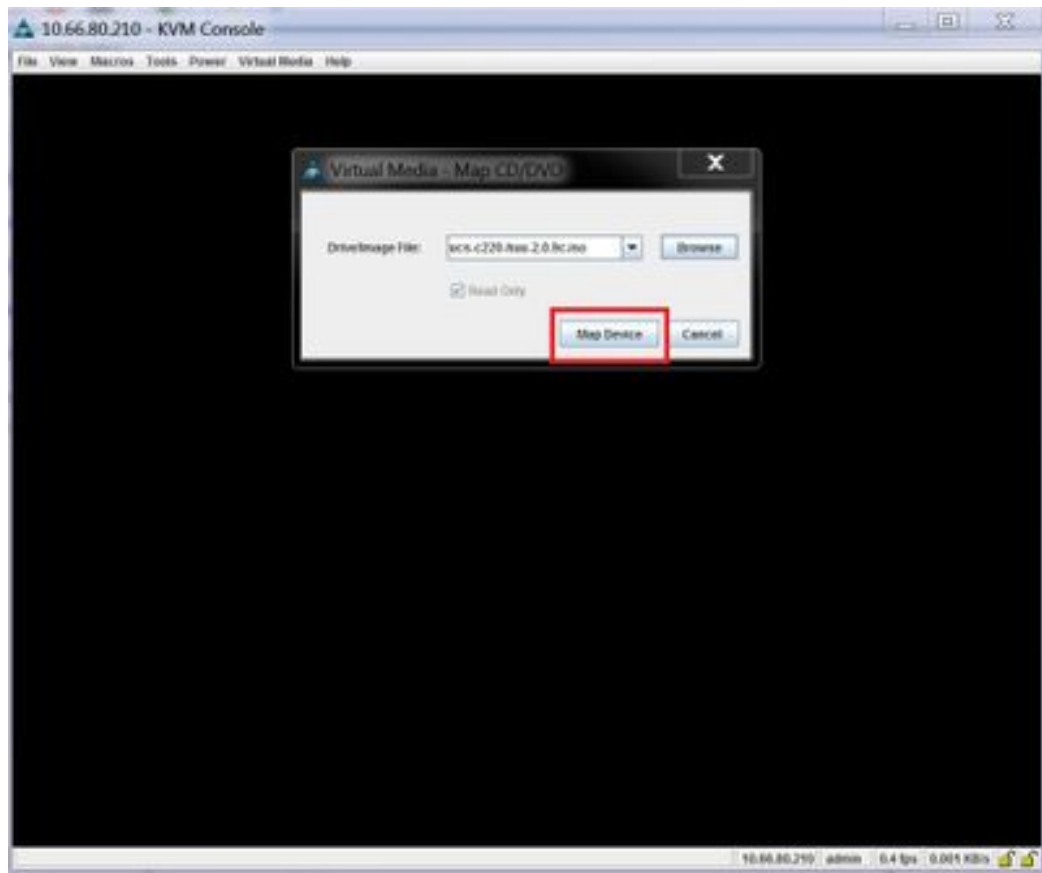
Step 11   Click **Macros** > **Static Macros** > **Ctrl-Alt-Del** to reboot the server.

If you are not able to reboot the server using this option, click **Power** > **Power cycle System** to perform a cold reboot instead.

Step 12   Press **F6** to enter the boot menu so that you can select the mapped DVD that you want to boot from.

You can also create a user-defined macro to perform this action, if you are using a Remote Desktop application, by selecting **Macros** > **User Defined Macros** > **F6**.

Step 13   When prompted, enter the password.

The default password is `password`.

Step 14   When prompted to select the boot device, select the **Cisco vKVM-Mapped vDVD** option, as shown in the figure below.
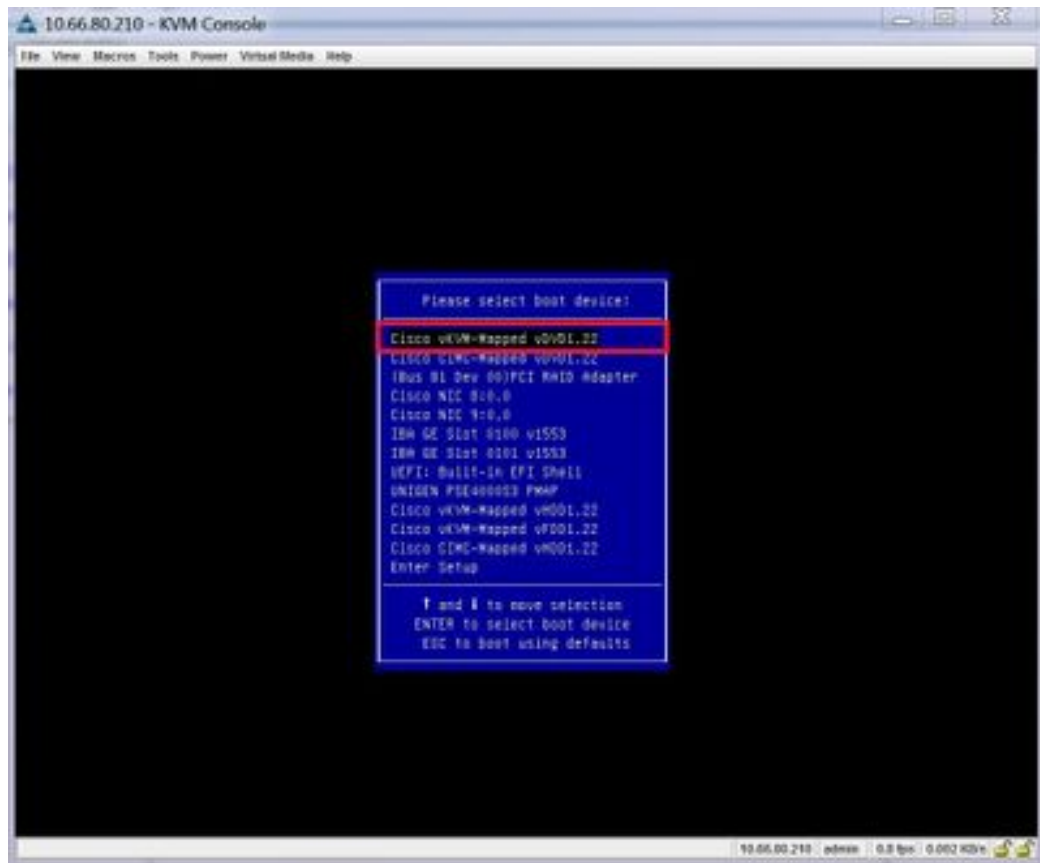
Step 15 Wait for the proces to complete, then accept the terms and conditions when prompted.

It will take around 10-15 minutes for the ISO to be extracted by the HUU, then another 15-20 minutes to copy the firmware and other tools.

Step 16 Make the appropriate selection in the HUU screen, when it appears.

We recommend that you select the **Update All** option to update all the firmware for all components.
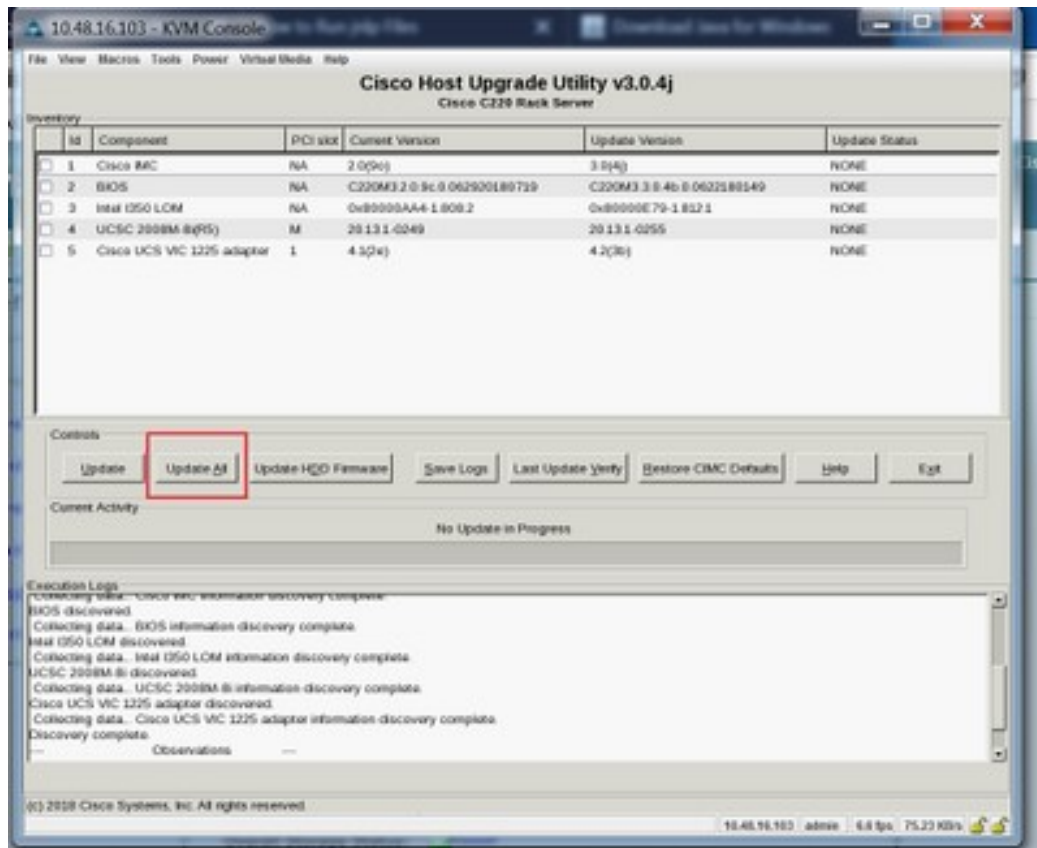
Step 17 If you see a pop-up asking if you want to enable Cisco IMC Secure Boot, select **No** for that option.

Refer to the "Introduction to Cisco IMC Secure Boot" section in the *Cisco UCS C-Series Servers Integrated Management Controller CLI Configuration Guide, Release 4.0* document for more information.

Step 18 Monitor the progress of the updates using the information provided in the **Update Status** column in the HUU.

Step 19 Once you see a status of **PASS** for each component, click **Exit** to reboot the server.

When the server reboots, you will be pushed out of the CIMC GUI. You will need to log back into the CIMC and verify the upgrade has completed successfully.

You can verify the upgrade was completed successfully through the GUI or by booting up the CIMC HUU and selecting **Last Update Verify** to ensure that all of the components passed the upgrade successfully.

Installing the Cisco APIC Software Using CIMC Virtual Media

Use this procedure to install the Cisco APIC software using Cisco Integrated Management Controller (CIMC) Virtual Media.

Note

You will open two console windows in these procedures:

- vKVM console

- Serial over LAN (SOL) console

You will be flipping back and forth between the two console windows, entering certain commands in one or the other console window for most of the steps in this procedure.

Before you begin

Review the information in Upgrading the CIMC Software, on page 19 to determine if you should upgrade your Cisco Integrated Management Controller (CIMC) software before you begin the procedures in this section.

- APIC-M4/L4 servers must be configured with a CIMC connection.

- The Cisco APIC ISO must be available on an HTTP server reachable from the APIC-M4/L4 Server CIMC management interface and the OOB management interface.

- Obtain the relevant Cisco APIC .iso image from Cisco.com and copy the .iso image to the HTTP server.

Procedure

Step 1 Access the vKVM console:

a) Open the Cisco Integrated Management Controller (CIMC) GUI for the controller.

b) For an APIC-M1, M2, M3, L1, L2, or L3 server, from the CIMC GUI, choose **Server** > **Summary** > **Launch KVM**, then select either **Java based KVM** or **HTML based KVM** to access the KVM console.

We recommend using the **Java based KVM** option whenever possible, because it is a more reliable option for larger-sized files.

c) For an APIC-M4/L4 server, from the CIMC GUI, choose **Server** > **Summary** > **Launch vKVM** to access the HTTP-based vKVM console.

Step 2 Access the **Serial over LAN (SOL) console**:

a) From a terminal window, log in to the CIMC console:

```
# ssh admin@cimc_ip
```

Where *cimc_ip* is the CIMC IP address. For example:

```
# ssh admin@192.0.2.1
admin@192.0.2.1's password:
system#
```

b) Change the scope to virtual media:

```
system# scope vmedia
system /vmedia #
```

c) Map the .iso image to the HTTP server:

```
system /vmedia # map-www volume_name http://http_server_ip_and_path iso_file_name
```

Where:

- *volume_name* is the name of the volume.

- *http_server_ip_and_path* is the IP address of the HTTP server and the path to the .iso file location.

- *iso_filename* is the name of the .iso file.

Note that there is a space between the *http_server_ip_and_path* and the *iso_filename*.

For example:

```
system /vmedia # map-www apic http://198.51.100.1/home/images/ aci-apic-dk9.4.0.3d.iso
Server username:
```

d) Check the mapping status:

```
system /vmedia # show mappings detail
```

The **Map-Status** should be shown as **OK**.

e) Connect to SOL to monitor the installation process:

```
system /vmedia # connect host
```

Step 3   **From the KVM console**: Choose **Power** > **Power Cycle System (cold boot)** to power cycle the controller.

Step 4   **From the SOL console**: Watch the screen during the boot process and prepare to press **F6** at the appropriate moment to enter the boot selection menu.

You should first see the following messages as the boot process begins:

```
Cisco Systems, Inc.
Configuring and testing memory..
Configuring platform hardware...
...
```

System bootup messages continue to appear, until the point where you should see the following screen:

```
...
Press <F2> Setup, <F6> Boot Menu, <F7> Diagnostics, <F8> Cisco IMC COnfiguration, <F12>
Network Boot
```

Step 5   **From the SOL console**: When you see the message above, press **F6** to enter the boot selection menu.

You should see `Entering boot selection menu...` if you were able to press **F6** at the appropriate moment. If you miss your opportunity and were not able to press **F6** at the appropriate moment, go back to to power cycle the controller and repeat the process until you are able to press **F6** to enter the boot selection menu.

Step 6   **From the SOL console**: At the boot selection menu, select the **Cisco CIMC-Mapped vDVD1.22** option as the one-time boot device.

```
/--------------------------------\
```

```
| Please select boot device:         |
|------------------------------------|
| (Bus 05 Dev 00)PCI RAID Adapter    |
| UNIGEN PHF16H0CM1-DTE PMAP         |
| Cisco vKVM-Mapped vHDD1.22         |
| Cisco CIMC-Mapped vHDD1.22         |
| Cisco vKVM-Mapped vDVD1.22         |
| Cisco CIMC-Mapped vDVD1.22         |
| Cisco vKVM-Mapped vFDD1.22         |
| UEFI: Built-in EFI Shell           |
| IBA GE Slot 0100 v1585             |
| IBA GE Slot 0101 v1585             |
| Enter Setup                        |
|------------------------------------|
|    ^ and v to move selection       |
|   ENTER to select boot device      |
|    ESC to boot using defaults      |
\------------------------------------/
```

You might also have to enter the BIOS password. The default password is **password**.

Step 7 **From the SOL console**: Enter the following:

a) Determine if you want to enter the ISO URL to speed up the installation process.

During the boot-up process, you might see the following message:

```
To speed up the install, enter iso url in next ten minutes:
```

You have two options at this stage:

- **Enter the ISO URL:** This option will make the installation process go faster. Following is an example HTTP URL that you might enter here:

```
http://10.75.61.1/aci-apic-dk9.4.2.1j.iso
```

If you choose this option, you will be asked to provide the protocol type, as shown in the following example:

```
? http://10.75.61.1/aci-apic-dk9.4.2.1j.iso
++ awk -F '/|:' '{print $4}'
+ urlip=10.75.61.1
+ '[' -z http://10.75.61.1/aci-apic-dk9.4.2.1j.iso ']'
+ '[' -z 10.75.61.1 ']'
+ break
+ '[' -n http://10.75.61.1/aci-apic-dk9.4.2.1j.iso ']'
+ set +e
+ configured=0
+ '[' 0 -eq 0 ']'
+ echo 'Configuring network interface'
Configuring network interface
+ echo 'type static, dhcp, bash for a shell to configure networking, or url to
re-enter the url: '
```

Choose the appropriate protocol type:

- **static:** If you choose this option, you will be asked to enter the interface name, management IP address and gateway. Following is an example of how to find the correct management interface:

```
? static
+ case $ntype in
+ configure_static
+ echo 'Available interfaces'
Available interfaces
```

```
+ ls -l /sys/class/net
total 0
lrwxrwxrwx. 1 root root 0 Sep 26 16:04 enp11s0 ->
../../devices/pci0000:00/0000:00:03.0/0000:06:00.0/0000:07:01.0/0000:09:00.0/0000:0a:00.0/0000:0b:00.0/net/enp11s0
lrwxrwxrwx. 1 root root 0 Sep 26 16:04 enp12s0 ->
../../devices/pci0000:00/0000:00:03.0/0000:06:00.0/0000:07:01.0/0000:09:00.0/0000:0a:01.0/0000:0c:00.0/net/enp12s0
lrwxrwxrwx. 1 root root 0 Sep 26 16:04 enp1s0f0 ->
../../devices/pci0000:00/0000:00:01.0/0000:01:00.0/net/enp1s0f0
lrwxrwxrwx. 1 root root 0 Sep 26 16:04 enp1s0f1 ->
../../devices/pci0000:00/0000:00:01.0/0000:01:00.1/net/enp1s0f1
lrwxrwxrwx. 1 root root 0 Sep 26 16:04 lo -> ../../devices/virtual/net/lo
+ read -p 'Interface to configure: ' interface
Interface to configure:
[anaconda] 1:main* 2:shell  3:log  4:storage-lo> Switch tab: Alt+Tab | Help: F1
```

In the output above, the network interface with the shorter pci numbering corresponds to the two Out-Of-Band management interfaces: `enp1s0f0` (eth1-1) and `enp1s0f1` (eth1-2). If both interfaces are cabled as they should be, you can select either of them. However, if only one interface has a cable connected to it, you must choose the interface that corresponds to the cabled port.

- **dhcp**

Also note that you do not have a space between the *http_server_ip_and_path* and the *iso_filename* for this ISO URL (for example,
`http://198.51.100.1/home/images/aci-apic-dk9.4.0.3d.iso`).

- **Do not enter the ISO URL:** If you do not want to enter the ISO URL, the installation process starts after ten minutes. This option is not supported on Cisco APIC versions 5.3(x) , 6.0(2), and above.

The system starts fetching the ISO at this point.

```
+ read -p 'Interface to configure: ' interface
Interface to configure: enp1s0f0
+ read -p 'address: ' addr
address: 10.75.39.72/24
+ read -p 'gateway: ' gw
gateway: 10.75.39.254
+ ip addr add 10.75.39.72/24 dev enp1s0f0
+ ip link set enp1s0f0 up
+ ip route add default via 10.75.39.254
++ seq 1 2
+ for count in '$(seq 1 2)'
+ ping -c 1 10.75.61.1
PING 10.75.61.1 (10.75.61.1) 56(84) bytes of data.
64 bytes from 10.75.61.1: icmp_seq=1 ttl=125 time=0.875 ms

--- 10.75.61.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.875/0.875/0.875/0.000 ms
+ configured=1
+ break
+ '[' 1 -eq 0 ']'
+ echo 'Fetching http://10.75.61.1/aci-apic-dk9.4.2.1j.iso'
Fetching http://10.75.61.1/aci-apic-dk9.4.2.1j.iso
+ wget -o /dev/null -O /tmp/cdrom.iso http://10.75.61.1/aci-apic-dk9.4.2.1j.iso
```

You can track the status of the process by going to **Tools** > **Stats** in the **KVM console**.

b) Wait until you see the message **poweroff** in the SOL console, then exit from SOL by pressing **Ctrl** and **x** (**Ctrl**+**x**).

c) Change the scope to virtual media again:

```
system# scope vmedia
system /vmedia #
```

d) Unmap the .iso image that you mapped in :

```
system /vmedia # unmap volume_name
```

At the `Save mapping` prompt, enter `yes` if you want to save the mapping or `no` if you do not want to save the mapping. For example:

```
system /vmedia # unmap apic
Save mapping? Enther 'yes' or 'no' to confirm (CTRL-C to cancel) → yes
system /vmedia #
```

e) Connect back to SOL again:

```
system /vmedia #   connect host
```

Step 8 **From the KVM console**: Choose **Power** > **Power on System** to power on the controller.

Step 9 **From the SOL console**: Enter the following:

a) Enter the options for the initial setup, such as fabric name, number of controllers, tunnel endpoint address pool, and infra VLAN ID to complete the installation process.

Performing a Clean Initialization of the ACI Fabric

Do a clean reboot of the fabric when you are bringing up the fabric for the first time, and when your fabric is not healthy, and a clean reboot is your only option to bring the fabric back up. This will remove all configurations from the Cisco APIC and switch nodes. You will then have to start the configuration from scratch or re-import it from a configuration backup.

Procedure

Step 1 Log in to each Cisco APIC through the out-of-band management to stop the Cisco APIC DME applications.

Example:

```
acidiag stop mgmt
```

Step 2 Log in to each switch through the out-of-band management. If out-of-band management is not available, log in using the console. Then, clean reboot the switch one of the following set of commands:

Example:

```
leaf101# setup-clean-config.sh
In progress
In progress
Done
```

```
leaf101# reload
This command will reload the chassis, Proceed (y/n)? [n]: y
```

Or:

```
leaf101# acidiag touch clean
This command will wipe out this device, Proceed? [y/N] y
leaf101# reload
This command will reload the chassis, Proceed (y/n)? [n]: y
```

Step 3   Log in to each Cisco APIC and clean reboot the Cisco APIC as follows:

Example:

```
acidiag touch clean
acidiag reboot
```

Alternatively, if you would also like to re-configure the initial setup parameters, you must also include the acidiag touch setup command, as shown below:

```
acidiag touch clean
acidiag touch setup
acidiag reboot
```

Note   Ignore this error: acidiag: error: curl: (52) Empty reply from server.

The fabric is now clean rebooted, but the nodes are not discovered. You can now post node policies, register the switches using the UI, or import a configuration backup.

ACI Firmware Upgrade Overview

About Firmware Management

There are a few types of firmware in Cisco ACI. The following is a brief list of firmware described in this document. This chapter is primarily focused on the top two types of Cisco ACI firmware: Cisco APIC firmware and switch firmware.

Firmware Type	Description	Example
Cisco APIC Firmware	An operation system of APICs running on APIC appliances.	APIC Release 5.2(1g): *aci-apic-dk9.5.2.1g*
Switch Firmware	An operation system of ACI switches running on Nexus 9000 series.	ACI Switch Release 15.2(1g): *aci-n9000-dk9.15.2.1g.bin*
Software Maintenance Upgrade (SMU) Patch	A patch image for a specific defect on either APICs or ACI switches. See Software Maintenance Upgrade Patches, on page 137 for details.	A patch for CSCaa12345 on APICs with 5.2(1g) release: *aci-apic-patch-CSCaa12345-5.2.1g-S.1.0.x86_64.tgz* A patch for CSCaa12345 on ACI switches with 15.2(1g) release: *aci-n9000-patch-CSCaa12345-15.2.1g-S.1.1.1.rpm*

Firmware Type	Description	Example
Silent Role (SR) Package	A package of firmware for specific hardware components on ACI switches. See Silent Roll Package Upgrade, on page 133 for details.	*aci-srpkg-dk9.1.0.0.bin*

Workflow to Upgrade or Downgrade the Cisco ACI Fabric

Cisco APIC centrally manages the upgrade and downgrade for the entire fabric. The Cisco APIC acts as the repository of the image (for example, the firmware repository) and as the booting server. Leaf switches and spine switches have connectivity to the Cisco APIC through the ACI infra network, and when upgrading or downgrading, the switches download the firmware from the Cisco APIC. This section provides the recommended steps for a successful upgrade or downgrade.

1. Pick your target Cisco APIC and ACI switch releases.

   a. Both Cisco APICs and ACI switches must be upgraded or downgraded to the same release.

   b. Cisco APIC and ACI switch releases that are compatible to each other are described in the form of x.y(z) and 1x.y(z). For instance, Cisco APIC release 5.2(1g) corresponds to ACI switch release 15.2(1g).

   c. Check the *Release Notes* (APIC and ACI switches) for the target release for any open caveats or defects.

2. See the *APIC Upgrade/Downgrade Support Matrix* for the supported upgrade and downgrade paths from your current release.

   a. If your current release and the target release are too far apart, you might need to upgrade or downgrade both your Cisco APICs and switches to an intermediate release suggested in the *APIC Upgrade/Downgrade Support Matrix* first. See Multistep Upgrades and Downgrades, on page 40 for more information.

   b. The *APIC Upgrade/Downgrade Support Matrix* also shows you which UCS HUU release you need to use for your target Cisco APIC release.

3. Review the ACI upgrade architecture.

   See ACI Upgrade/Downgrade Architecture, on page 51 to understand what you should expect along with what you must not perform.

4. Export your configuration for backup.

   See the Cisco ACI Configuration Files: Import and Export document for details. Ensure that AES encryption is enabled.

5. Disable all App Center apps on the Cisco APICs except for the ones that are pre-packaged on the Cisco APIC image.

   See Guidelines for App Center Apps, on page 42 for details.

6. Download both the Cisco APIC and ACI switch firmware to your Cisco APICs.

See the *Downloading APIC and Switch Images on APICs* section for each release for details:

- Releases prior to 4.x: Downloading APIC and Switch Images on APICs, on page 73

- Releases 4.x or 5.0: Downloading APIC and Switch Images on APICs, on page 79

- Release 5.1 or later: Downloading APIC and Switch Images on APICs, on page 90

7. Download ACI switch firmware from your Cisco APICs to each switch.

   Starting from switch release 14.1(1), switches can download the image from Cisco APICs prior to the upgrade or downgrade. See Rule 5 – Save time by downloading switch images beforehand, on page 38 for details.

8. Perform pre-upgrade validations.

   See Pre-Upgrade/Downgrade Checklists, on page 63 for details.

9. Upgrade or downgrade all server components via HUU (CIMC, BIOS, network adapters, RAID controller, and disks) on your Cisco APICs if suggested so by the Support Matrix.

   See Upgrading the CIMC Software, on page 19 for details.

10. Upgrade or downgrade Cisco APICs.

    See the *Upgrading the Cisco APIC* section for each release for details:

    - Releases prior to 4.x: Upgrading or Downgrading the Cisco APIC from Releases Prior to Release 4.x, on page 74

    - Releases 4.x or 5.0: Upgrading or Downgrading the Cisco APIC From Releases 4.x or 5.0, on page 81

    - Release 5.1 or later: Upgrading or Downgrading the Cisco APIC From Releases 5.1x or Later, on page 92

11. Perform pre-upgrade validations.

    See Pre-Upgrade/Downgrade Checklists, on page 63 for details.

12. Upgrade or downgrade the ACI-mode Switches.

    a. Wait until all Cisco APICs become **Fully Fit**.

    b. See the *Upgrading the Leaf and Spine Switches* section for each release for details:

       - Releases prior to 4.x: Upgrading or Downgrading the Leaf and Spine Switches Through APIC Running Prior to Release 4.x, on page 75

       - Releases 4.x or 5.0: Upgrading or Downgrading the Leaf and Spine Switches Through a Cisco APIC Running Releases 4.x or 5.0, on page 84

       - Release 5.1 or later: Upgrading or Downgrading the Leaf and Spine Switches Through APIC Running Release 5.1x or Later, on page 94

       - For release 6.0(2) or later, download both the 32-bit and 64-bit switch images after a successful Cisco APIC upgrade. For more information, see Download Both the 32-bit and 64-bit Cisco ACI-Mode Switch Images (6.0(2) and later), on page 64.

13. If this is a **Multistep Upgrade**, repeat the steps above to upgrade or downgrade from the intermediate release to the target release after the upgrade or downgrade to the immediate release for both Cisco APICs and switches completed and Cisco APIC cluster status is **Fully Fit**.

> **Note** If the Cisco ACI fabric deployment includes Cisco AVS/AVE, upgrade or downgrade the Cisco AVS/AVE to the release compatible with the Cisco APIC. To upgrade or downgrade Cisco AVS/AVE, see the section **Recommended Upgrade Sequence for Cisco APIC, the Fabric Switches, and Cisco ACI Virtual Edge** in the Cisco ACI Virtual Edge Installation Guide.

Guidelines for ACI Switch Upgrades and Downgrades

Following are the guidelines for ACI switch upgrades and downgrades:

Rule 1 – Divide your leaf and spine switches into at least two groups

For example:

- Group ODD: leaf 101, leaf 103, spine 1001
- Group EVEN: leaf 102, leaf104, spine 1002

Rule 2 – Determine how spine switches should be grouped

- Always keep at least one MP-BGP route reflector (RR) spine switch up and running in each pod.
- Always keep at least one spine switch with IPN connectivity up and running in each pod.
- Never perform a graceful upgrade for a spine switch if the given pod has only one spine switch (in the case of multi-pod).

  See Graceful Upgrade or Downgrade of ACI Switches, on page 39 for details.

For example:

Update Group	Pod 1	Pod 2
ODD	leaf 101, leaf 103, leaf 105 **spine 1001 (RR, IPN)** **spine 1003**	leaf 201, leaf 203, leaf 205 **spine 2001 (RR, IPN)** **spine 2003**
EVEN	leaf 102, leaf 104, leaf 106 **spine 1002 (RR, IPN)** **spine 1004**	leaf 202, leaf 204, leaf 206 **spine 2002 (RR, IPN)** **spine 2004**

Where:

- **RR** means a Route Reflector spine switch

- **IPN** means a spine switch connected to IPN

Rule 3 – Determine how leaf switches should be grouped

- Always keep one of the leaf switches in the same vPC pair up and running

- Always keep one of the leaf switches connected to each Cisco Application Policy Infrastructure Controller (APIC) up and running

For example:

Update Group	Pod 1	Pod 2
ODD	**leaf 101 (vPC 11, APIC1)** **leaf 103 (vPC 12, APIC2)** **leaf 105 (vPC 13)** spine 1001	**leaf 201 (vPC 21, APIC3)** **leaf 203 (vPC 22)** **leaf 205 (vPC 23)** spine 2001
EVEN	**leaf 102 (vPC 11, APIC1)** **leaf 104 (vPC 12, APIC2)** **leaf 106 (vPC 13)** spine 1002	**leaf 202 (vPC 21, APIC3)** **leaf 204 (vPC 22)** **leaf 206 (vPC 23)** spine 2002

Where:

- **vPC xx** means one vPC pair

- **APICx** means a leaf switch connected to the Cisco APIC

Rule 4 – Understand the concurrent capacity in switch update groups

General

- Each update/maintenance group should contain a maximum of 80 switch nodes.

- The concurrent capacity (switches that are upgraded or downgraded simultaneously) decides how many switches should be upgraded or downgraded simultaneously within the same update/maintenance group. However, we recommend that you create separate update groups to upgrade or downgraded switches on different schedules instead of relying on the concurrent capacity setting because the concurrent capacity setting doesn't let you manage which switches in the same group are to be upgraded or downgraded at the same time.

- If both leaf nodes in the same vPC pair are in the same switch upgrade or downgrade group, only one of the leaf nodes is upgraded or downgraded at a time regardless of the concurrent capacity.

- Starting from Cisco APIC release 4.1(1), when graceful upgrade or downgrade is enforced and there are no other operational spine switches in the same pod, the upgrade or downgrade is rejected regardless of the concurrent capacity setting.

Prior to Cisco APIC release 4.2(5):

- Even in the same update group, switches are upgraded or downgraded only one pod at a time.

- The default concurrent capacity per group is 20.

If you have more than 20 switches in the same group, you can use upgrade scheduler to change the capacity to unlimited.

See the *Upgrading the Leaf and Spine Switch Software Version* section for details:

- Releases prior to 4.x: Upgrading or Downgrading the Leaf and Spine Switches Through APIC Running Prior to Release 4.x, on page 75

- Releases 4.x or 5.0: Upgrading or Downgrading the Leaf and Spine Switches Through a Cisco APIC Running Releases 4.x or 5.0, on page 84

From Cisco APIC release 4.2(5):

- Switches in the same update group are upgraded or downgraded simultaneously, regardless of pods.

- The default concurrent capacity per group is unlimited.

The above enhancements from Cisco APIC release 4.2(5) take effect as soon as the Cisco APICs are upgraded to 4.2(5) or later. For instance, when the Cisco APICs are upgraded to 4.2(5) and the switches are still at release 13.2(10), the above enhancements will be effective when the switch is upgraded from 13.2(10) to 14.2(5).

This enhancement will help you reduce the time it takes to upgrade your switches.

Rule 5 – Save time by downloading switch images beforehand

Even after you have downloaded Cisco APIC and switch images to the Cisco APIC's firmware repository, the switches still need to download the image from the Cisco APICs. In later releases, this operation can be performed separately from the actual upgrade procedure. This is called pre-download and is equivalent to Step 7 in Workflow to Upgrade or Downgrade the Cisco ACI Fabric, on page 34.

Prior to switch release 14.1(1):

Not supported. Switches download the image from Cisco APICs when the upgrade or downgrade is triggered.

Switch release 14.(1) - 15.0(x):

- Pre-download can be performed through the upgrade scheduler.

- Following is the recommended procedure:

  1. Create update groups with the scheduler set far into the future (such as 10 years in the future). This will trigger switches to download the image from Cisco APICs immediately.

  2. When it's the time to start the upgrade in the maintenance window, edit the same groups and change the **Upgrade Start Time** to **Now**.

- If the current version of the switches is 14.2(5) or later, the Cisco APIC GUI shows the progress of the pre-download.

Switch release 15.1(1) or later:

- Pre-download is built in the GUI workflow natively without using a scheduler.

  1. Switches download the image from the Cisco APICs when you create an update group and click **Begin Download**.

  2. When the pre-download is completed, each switch shows **Ready to Install**.

  3. Perform **Begin Install** for the same group to trigger the upgrade.

The above enhancement (pre-download) from switch release 14.1(1) takes effect only after both the Cisco APICs and the switches are upgraded or downgraded to the corresponding versions. For example, when the Cisco APICs are upgraded to 4.2(7) and the switches are still on 13.2(10), pre-download is not available to upgrade the switches from 13.2(10) to 14.2(7). On the other hand, when the Cisco APICs are upgraded to 5.2(1) and the switches are still in 14.2(7), pre-download is performed through the new Cisco APIC GUI using **Begin Download** for switch upgrades from 14.2(7) to 15.2(1).

Graceful Upgrade or Downgrade of ACI Switches

If you want to isolate a switch from user traffic when performing an upgrade or downgrade procedure, it's helpful to become familiar with the different terms and methods available to better understand what is supported and what is not supported in these situations:

- **Graceful Insertion and Removal (GIR)**: The operation used to isolate a switch from user traffic.

- **Maintenance mode**: Used to isolate a switch from user traffic for debugging purposes. You can put a switch in **maintenance mode** by enabling the **Maintenance (GIR)** field in the **Fabric Membership** page in the Cisco APIC GUI, located at **Fabric** > **Inventory** > **Fabric Membership** (right-click on a switch and choose **Maintenance (GIR)**).

  If you put a switch in **maintenance mode**, that switch is not considered as a part of the operational ACI fabric infra and it will not accept regular Cisco APIC communications. Therefore, performing a firmware upgrade or downgrade for a switch in this state is not supported, because the process may fail or may get stuck in an incomplete status indefinitely if you attempt to perform a firmware upgrade or downgrade on the switch while the switch is in this state.

- **Graceful Upgrade**: Used to reload a switch after it is isolated from user traffic during an upgrade procedure. Switches are programmed to reboot automatically at a certain point during the firmware upgrade process; this operation will automatically perform GIR prior to that reboot. You can find the **Graceful Maintenance** option (releases prior to release 5.1) or the **Graceful Upgrade** option (release 5.1 and later) for a switch in an update group in **Admin** > **Firmware** in the Cisco APIC GUI.

If you wish to halt the procedure after the switch is isolated from user traffic and before it is reloaded in order to ensure the user traffic is flowing through redundant paths, such an operation is currently not supported in ACI.

Guidelines for ACI Switch Graceful Upgrade

All guidelines from Guidelines for ACI Switch Upgrades and Downgrades, on page 36 also apply to **Graceful Upgrade**. However, this section provides more information on several guidelines that are specifically critical for **Graceful Upgrade**.

- As suggested in Rule 2 – Determine how spine switches should be grouped, on page 36, do not upgrade all spine switches in a pod at one time, especially when you are performing a **Graceful Upgrade** in a Multi-Pod setup.

  Otherwise, the upgrade will fail, leaving the spine switches isolated from the fabric indefinitely. This is because, as part of the **Graceful Upgrade** process, IPN connectivity is brought down explicitly on each spine switch being upgraded gracefully so that it can isolate itself from the fabric. Upgrading in this way results in the entire pod, including the spine switches themselves, to lose communication with Cisco APICs and switches in other pods without the means to self-recover.

  Due to this reason, if you are performing a **Graceful Upgrade**, you must put the spine switches from the same pod into different maintenance/update groups such that the switches get upgraded separately. If the pod has only one spine switch, you must disable the **Graceful Upgrade** (or **Graceful Maintenance**) option prior to the upgrade. In case you fail to follow this procedure, refer to the workaround provided in CSCvn28063.

  To avoid this issue, Cisco APIC 4.1(1) release introduced a safe mechanism to reject the upgrade of the last spine switch in a pod when **Grace Upgrade** is enforced. This block mechanism is also described in Rule 4 – Understand the concurrent capacity in switch update groups, on page 37.

- As suggested in Rule 3 – Determine how leaf switches should be grouped, on page 37, you must put Cisco APIC-connected leaf switches into different maintenance/update groups so that two leaf switches connected to the same Cisco APIC are not upgraded at the same time.

Multistep Upgrades and Downgrades

In the Cisco ACI fabric, all nodes (APICs, leaf switches, and spine switches) should be on the same software release or on a compatible software release, where the APIC nodes have the standard release format of x.y(z), and the leaf and spine switches have the switch-specific standard release format of 1x.y(z). For example, if the APIC nodes are on software release 4.2(1), the leaf switches and spine switches should be on the switch-specific compatible software release of 14.2(1).

APIC Upgrade/Downgrade Support Matrix shows the supported upgrade and downgrade paths for your current version and the target version. If those two versions are too far apart, upgrading or downgrading directly to the target version might not be supported.

When upgrading or downgrading to a release that does not have a direct path from your current release, you must upgrade or downgrade all the APICs and switches to an intermediate supported release to which there is a direct path, then upgrade or downgrade from that release to your desired release. Sometimes, you must move through multiple intermediate releases before being able to get to your desired release, upgrading or downgrading both the APICs and switches to the same release each time.

For example, consider the following situation, where the *APIC Upgrade/Downgrade Support Matrix* shows multiple intermediate releases for an upgrade from release 2.3(1) to release 4.2(3):

In this situation, you would perform the upgrade in the following manner:

1. Upgrade the APICs to the 3.1(2) release and the switches to the 13.1(2) release.

2. Verify that all APICs and switches are in the **Fully Fit** state and operational after the upgrade to 3.1(2)/13.1(2).

3. Repeat the same steps for 4.1(2) and 14.1(2).

4. Repeat the same steps for 4.2(3) and 14.2(3).

Upgrading or Downgrading a Huge Fabric

There are situations where you might have different releases in the fabric at the same time, such as when you're upgrading or downgrading a huge fabric with a large number of switches and you're splitting the switches into different maintenance groups, with the upgrades or downgrades occurring over a series of days. In those situations, you can have at most two different APIC and switch software releases in the fabric at any given time. However, supported operations in those situations are limited. See Operations Allowed During Mixed Versions on Cisco ACI Switches, on page 57 for more information.

Upgrading or Downgrading a Cisco Mini ACI Fabric

The Cisco Application Centric Infrastructure (ACI) release 4.0(1) introduced the Cisco mini ACI fabric for small scale deployments. A mini ACI fabric works with a Cisco Application Policy Infrastructure Controller (APIC) cluster consisting of one physical Cisco APIC and two virtual Cisco APICs (vAPICs) running in virtual machines. This reduces the physical footprint and cost of the Cisco APIC cluster, which allows you to deploy the Cisco ACI fabric in scenarios with limited rack space or initial budget. Examples of such a scenario include a colocation facility or a single-room data center. In such cases, a full-scale Cisco ACI installation may not be practical due to the physical footprint or initial cost.

For more information the Cisco mini ACI fabric, including procedures for installing, upgrading, and downgrading, see the *Cisco Mini ACI Fabric and Virtual APICs* document:

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/kb/
Cisco-Mini-ACI-Fabric-and-Virtual-APICs.html

Guidelines for App Center Apps

If you are running apps from https://dcappcenter.cisco.com/ on your Cisco APIC nodes:

- Disable those apps before upgrading or downgrading the APIC software on those APIC nodes.

- Do not install or remove any apps while upgrading or downgrading the APIC software on those APIC nodes.

- Do not perform an app image upgrade while upgrading or downgrading the APIC software on those APIC nodes.

- If you upgraded from a release prior to the 3.2(1) release and you had any apps installed prior to the upgrade, the apps will no longer work. To use the apps again, you must uninstall and reinstall them.

- If you are upgrading to APIC release 5.2(1) or later and you have External Switch App version 1.1 installed, you must remove the app and re-install version 1.2 of the app before you upgrade to APIC release 5.2(1) or later.

After you have completed the APIC software upgrade or downgrade process for the entire fabric (the APIC nodes and switches), re-enable the apps again if you disabled them. You can install or remove apps, or perform an app image upgrade, after the APIC software upgrade or downgrade process is complete.

Determining Current Software Version

Use the procedures in this section to determine the software version that is currently running on the switches and APICs in your fabric.

Determining Current Software Version on APICs

You can determine the software version that is currently running on the APICs in your fabric several ways:

- Click the System Tools icon (⚙) in the upper right corner of the Cisco APIC GUI window, then select **About**.

- Navigate to the **Controllers** page:

  - For releases prior to release 5.1(1), navigate to **Admin** > **Firmware** > **Infrastructure** > **Controllers**. The software version is shown in the **Current Firmware** column in the table on this page.

  - For release 5.1(1) and later, navigate to **Admin** > **Firmware**, then click **Dashboard** in the left navigation window. The software version is shown in the **Firmware** field in the **Controllers** area on the page.

    You can also determine the software version running on each individual APIC by locating the **Controllers** area in this same page. The software version running on each APIC is shown in the **Current Version** column.

Determining Current Software Version on Switches

To determine the software version that is currently running on the leaf and spine switches in your fabric:

- For releases prior to release 5.1(1), navigate to **Admin** > **Firmware** > **Infrastructure** > **Nodes**. The software version is shown in the **Current Firmware** column in the table on this page.

- For release 5.1(1) and later, navigate to **Admin** > **Firmware**, then click **Dashboard** in the left navigation window. The software version is shown in the **Firmware** field in the **Nodes** area on the page.

- For release 5.2(1) and later, you can also use the **Node Summary** tab in **Admin** > **Firmware** > **Nodes**.

About Upgrading or Downgrading with the Scheduler

The scheduler enables you to specify a window of time for operations such as upgrading or downgrading Cisco APIC clusters and switches. The windows of time can be one-time only or it can recur at a specified time and day each week. This section explains how the scheduler works for upgrades or downgrades. For more information about the scheduler, see the *Cisco Application Centric Infrastructure Fundamentals* document.

Note   When performing a Cluster Upgrade, the Cisco APICs must all be the same version for them to join the cluster. There is no automatic upgrade when joining the fabric.

- Cisco APIC Cluster Upgrade—There is a default scheduler object for Cisco APIC upgrades. While the generic scheduler object has several properties, only the start time property is configurable for the Cisco APIC cluster upgrade. If you specify a start time, the Cisco APIC upgrade scheduler is active from the specified start time for the duration of 1 day. Anytime during this active one-day window, if runningVersion != desiredVersion for the controllers, the cluster upgrade will begin. None of the other parameters of the scheduler are configurable for Cisco APIC upgrades. Please note that you can also perform an Cisco APIC upgrade by using a one-time trigger, which does not use the scheduler. This one-time trigger is also called upgrade-now.

- Switch upgrades—A scheduler may be attached to a maintenance group. A scheduler attached to a switch maintenance group has several configurable parameters such as "startTime", "concurCap" and "duration." These parameters are described below:
    - startTime—The start of an active window.
    - concurCap—The number of nodes to upgrade simultaneously.
    - Duration—The length of an active window.

  Anytime during an active window, if runningVersion != desiredVersion for any switch in that group, the switch will be eligible for an upgrade. Among nodes eligible for an upgrade, the following constraints are applied to pick upgrade candidates:
    - No more than the "concurCap" nodes should currently be upgrading.
    - Only one node in a virtual port channel (vPC) pair is upgraded at a time.
    - The Cisco APIC cluster should be healthy before starting a node upgrade.

Note   You have the options of immediate upgrade and scheduler-based upgrade through the GUI, CLI or REST API. For example, with CLI, you can upgrade the switch-group immediately using the **firmware upgrade switch-group** command in the EXEC mode. This command takes priority over any configured scheduled upgrades.

Scheduler Guidelines

The system will react differently if you set an upgrade schedule to a date in the past, depending on whether you are setting a one-time or a recurring upgrade schedule:

- If you set a *one-time* upgrade schedule with a date in the past, the configuration will be rejected by the system.

- If you set a *recurring* upgrade schedule with a date in the past, the scheduler triggers the upgrade immediately. For example, if it is noon on Wednesday and you set a recurring upgrade schedule for every Tuesday at noon, the scheduler will first trigger an upgrade immediately, and then will perform upgrades every Tuesday at noon from that point forward.

Configuring a Scheduler Using the GUI

The trigger scheduler allows you to define one-time or recurring time periods where one or more nodes can be upgraded and rebooted without administrator intervention.

Procedure

Step 1	Access the **Create Trigger Scheduler** window.
Step 2	In the **Create Trigger Scheduler** window, enter a name for the scheduler policy in the **Name** field, then click + in the Schedule Windows area to bring up the **Create Schedule Window** window.
Step 3	In the **Window Type** field, click either **One Time** or **Recurring**, depending on whether you want to configure a one-time or a recurring schedule window.
Step 4	In the **Window Name** field, enter a name for this schedule window. The maximum number of characters for this field is 16.
Step 5	Determine the date and time that you want the schedule window to occur. The options for setting the date and time vary, depending on whether you choose to configure a one-time or a recurring schedule window.

- If you're configuring a *one-time* schedule window, in the **Date** field, enter a date for the one-time schedule window to occur. For this field, use the format YYYY-MM-DD HH:MM:SS AM/PM, or click the down-arrow to select a date and time from a calendar.

Note   If you enter a date and time that is in the past (before the current date and time) for the one-time schedule window, the system will reject that entry.

- If you're configuring a *recurring* schedule window, enter the necessary information in the following fields:

  - **Day**: Select which days that you want the recurring schedule window to occur. Select either a specific day that you want the recurring schedule window to occur every week, or if you want the recurring schedule window to occur every day, on every even day, or on every odd day of the week.

  - **Hour**: Enter the hour that would like to recurring schedule window to occur, using military 24-hour clock values (0-23).

  - **Minute**: Enter the minute that would like to recurring schedule window to occur.

  For example, if you wanted to configure a recurring schedule window for every Tuesday at 11:30 p.m., you would make the following selections:

  - **Day**: Tuesday

  - **Hour**: 22

  - **Minute**: 30

Note   If you enter a date and time that is in the past (before the current date and time) for the recurring schedule window, the scheduler triggers the upgrade immediately. For example, if it is noon on Wednesday and you set a recurring upgrade schedule for every Tuesday at 11:30 pm, the scheduler will first trigger an upgrade immediately, and then will perform upgrades every Tuesday at 11:30 pm from that point forward..

Step 6   In the **Maximum Concurrent Nodes** field, enter the maximum number of nodes that will be allowed to go through concurrent (simultaneous) upgrades.

If you enter **0** in this field, the software will automatically select the default value, depending on whether the nodes are APIC nodes or leaf or spine switches.

- For releases prior to release 4.2(5), the default value "0" for this field is interpreted as 1 for APIC nodes and 20 for leaf or spine switches. The maximum number of nodes per POD that you can enter in this field is 200.

- For release 4.2(5) and forward, the default value "0" for this field is interpreted as 1 for APIC nodes. For leaf or spine switches, the interpretation of the default value "0" for this field has changed from 20 to unlimited. In other words, when entering "0" in this field, the number of leaf or spine switches that can be upgraded at one time is unlimited.

Step 7   In the **Maximum Running Time** field, enter the maximum duration for the schedule window, which is the amount of time that you want to allow for the upgrade process to begin.

For this field, use the format DD:HH:MM:SS, with a maximum of 24 hours (01:00:00:00). Enter `unlimited` if you don't want to have a time limit enforced on the scheduler window.

For example, assume that you entered the following values in these fields:

- **Maximum Concurrent Nodes**: 20

- **Maximum Running Time**: 00:00:30:00

In this case, for this schedule window, you're allowing 20 nodes to upgrade simultaneously, and those 20 nodes will upgrade only if the upgrade process successfully begins within 30 minutes from the start time that

you entered in the fields above. If the upgrade process doesn't begin successfully within 30 minutes, none of the 20 nodes are upgraded at this time, and, if you configured a recurring schedule window, the system will attempt the upgrade for those 20 nodes the next time the scheduler window is set to repeat.

The value that you enter in the **Maximum Running Time** field doesn't affect the amount of time that is needed for the switches in a group to upgrade. For example, entering a value of 5 in the **Maximum Running Time** field only means that the system will abandon the upgrade process for the switches if the upgrades don't begin after 5 minutes; it doesn't mean that the system will stop the upgrade process after 5 minutes. Each switch generally takes about 10 minutes for the upgrade.

Step 8   Click **OK** when you have finished entering the necessary information in the **Create Trigger Scheduler** window.

The **Create Trigger Scheduler** window appears again, with your newly-configured schedule window appearing in the Schedule Windows table.

Step 9   Determine if you want to create additional schedule windows for this trigger scheduler.

Click + in the Schedule Windows area to bring up the **Create Schedule Window** window again, if you want to create more schedule windows for this trigger scheduler.

For example, you might create more schedule windows if you want to configure upgrades to start twice a day, say at 12:00 AM and PM every day, or to configure upgrades on specific days of the week.

Step 10   When you have finished configuring the necessary schedule windows, in the **Create Trigger Scheduler** window, click **Submit**.

The **Select Node Upgrade** window appears again.

Step 11   In the **Select Node Upgrade** window, locate the **Scheduler** field and select the trigger schedule that you just configured.

Step 12   Complete any necessary additional configurations in the **Select Node Upgrade** window, then click **Submit**.

Configuring a Scheduler Using the NX-OS Style CLI

A schedule allows operations, such as configuration import/export or tech support collection, to occur during one or more specified windows of time.

A schedule contains a set of time windows (occurrences). These windows can be one time only or can recur at a specified time and day each week. The options defined in the window, such as the duration or the maximum number of tasks to be run, determine when a scheduled task will execute. For example, if a change cannot be deployed during a given maintenance window because the maximum duration or number of tasks has been reached, that deployment is carried over to the next maintenance window.

Each schedule checks periodically to see whether the APIC has entered one or more maintenance windows. If it has, the schedule executes the deployments that are eligible according to the constraints specified in the maintenance policy.

A schedule contains one or more occurrences, which determine the maintenance windows associated with that schedule. An occurrence can be one of the following:

- Absolute (One Time) Window—An absolute window defines a schedule that will occur only once. This window continues until the maximum duration of the window or the maximum number of tasks that can be run in the window has been reached.

- Recurring Window—A recurring window defines a repeating schedule. This window continues until the maximum number of tasks or the end of the day specified in the window has been reached.

Procedure

	Command or Action	**Purpose**
Step 1	**configure** **Example:** `apic1# configure`	Enters global configuration mode.
Step 2	[**no**] **scheduler** *schedule-name* **Example:** `apic1(config)# scheduler controller schedule myScheduler`	Creates a new scheduler or configures an existing scheduler.
Step 3	[**no**] **description** *text* **Example:** `apic1(config-scheduler)# description 'This is my scheduler'`	Adds a description for this scheduler. If the text includes spaces, it must be enclosed in single quotes.
Step 4	[**no**] **absolute window** *window-name* **Example:** `apic1(config-scheduler)# absolute window myAbsoluteWindow`	Creates an absolute (one time) window schedule.
Step 5	[**no**] **max concurrent nodes** *count* **Example:** `apic1(config-scheduler-absolute)# max concurrent nodes 300`	Sets the maximum number of nodes (tasks) that can be processed concurrently. The range is 0 to 65535. Set to 0 for unlimited nodes.
Step 6	[**no**] **max running time** *time* **Example:** `apic1(config-scheduler-absolute)# max running time 00:01:30:00`	Sets the maximum running time for tasks in the format dd:hh:mm:ss. The range is 0 to 65535. Set to 0 for no time limit.
Step 7	[**no**] **time start** *time* **Example:** `apic1(config-scheduler-absolute)# time start 2016:jan:01:12:01`	Sets the starting time in the format [[[[yyyy:]mmm:]dd:]HH:MM.
Step 8	**exit** **Example:** `apic1(config-scheduler-absolute)# exit`	Returns to scheduler configuration mode.
Step 9	[**no**] **recurring window** *window-name* **Example:**	Creates a recurring window schedule.

	Command or Action	Purpose
	`apic1(config-scheduler)# recurring window myRecurringWindow`	
Step 10	[**no**] **max concurrent nodes** *count* **Example:** `apic1(config-scheduler-recurring)# max concurrent nodes 300`	Sets the maximum number of nodes (tasks) that can be processed concurrently. The range is 0 to 65535. Set to 0 for unlimited nodes.
Step 11	[**no**] **max running time** *time* **Example:** `apic1(config-scheduler-recurring)# max running time 00:01:30:00`	Sets the maximum running time for tasks in the format dd:hh:mm:ss. The range is 0 to 65535. Set to 0 for no time limit.
Step 12	[**no**] **time start** {**daily** *HH:MM* | **weekly** (See usage) *HH:MM*} **Example:** `apic1(config-scheduler-recurring)# time start weekly wednesday 12:30`	Sets the period (daily or weekly) and starting time. If **weekly** is selected, choose from these options: • **monday** • **tuesday** • **wednesday** • **thursday** • **friday** • **saturday** • **sunday** • **even-day** • **odd-day** • **every-day**

Examples

This example shows how to configure a recurring scheduler to run every Wednesday.

```
apic1# configure
apic1(config)# scheduler controller schedule myScheduler
apic1(config-scheduler)# description 'This is my scheduler'
apic1(config-scheduler)# recurring window myRecurringWindow
apic1(config-scheduler-recurring)# max concurrent nodes 300
apic1(config-scheduler-recurring)# max running time 00:01:30:00
apic1(config-scheduler-recurring)# time start weekly wednesday 12:30
```

Configuring a Scheduler Using REST API

A schedule allows operations, such as configuration import/export or tech support collection, to occur during one or more specified windows of time.

A schedule contains a set of time windows (occurrences). These windows can be one time only or can recur at a specified time and day each week. The options defined in the window, such as the duration or the maximum number of tasks to be run, determine when a scheduled task will execute. For example, if a change cannot be deployed during a given maintenance window because the maximum duration or number of tasks has been reached, that deployment is carried over to the next maintenance window.

Each schedule checks periodically to see whether the APIC has entered one or more maintenance windows. If it has, the schedule executes the deployments that are eligible according to the constraints specified in the maintenance policy.

A schedule contains one or more occurrences, which determine the maintenance windows associated with that schedule. An occurrence can be one of the following:

- Absolute (One Time) Window—An absolute window defines a schedule that will occur only once. This window continues until the maximum duration of the window or the maximum number of tasks that can be run in the window has been reached.

- Recurring Window—A recurring window defines a repeating schedule. This window continues until the maximum number of tasks or the end of the day specified in the window has been reached.

Procedure

Step 1   Download the switch image into the repository.

Example:

```
POST URL: https://<ip address>/api/node/mo/uni/fabric.xml
<firmwareRepoP>
 <firmwareOSource name="Switch_Image_download" proto="http" url="http://<ip
address>/<ver-no>"/>
</firmwareRepoP>
```

Step 2   Post the following policies, to create a firmware group that consists of your switches with node IDs 101, 102, 103, 104, and to create a maintenance group with node IDs 101, 102, 103, 104:

Example:

```
POST URL : https://<ip address>/api/node/mo/uni/fabric.xml
<fabricInst>
<firmwareFwP
    name="AllswitchesFwP"
    version="<ver-no>"
    ignoreCompat="true">
</firmwareFwP>

<firmwareFwGrp
    name="AllswitchesFwGrp" >
        <fabricNodeBlk name="Blk101"
            from_="101" to_="101">
        </fabricNodeBlk>
        <fabricNodeBlk name="Blk102"
            from_="102" to_="102">
        </fabricNodeBlk>
        <fabricNodeBlk name="Blk103"
```

```
                            from_="103" to_="103">
            </fabricNodeBlk>
            <fabricNodeBlk name="Blk104"
                from_="104" to_="104">
            </fabricNodeBlk>
<firmwareRsFwgrpp
    tnFirmwareFwPName="AllswitchesFwP">
</firmwareRsFwgrpp>
</firmwareFwGrp>

<maintMaintP
    name="AllswitchesMaintP"
    runMode="pauseOnlyOnFailures" >
</maintMaintP>

<maintMaintGrp
    name="AllswitchesMaintGrp">
        <fabricNodeBlk name="Blk101"
            from_="101" to_="101">
        </fabricNodeBlk>
        <fabricNodeBlk name="Blk102"
            from_="102" to_="102">
        </fabricNodeBlk>
        <fabricNodeBlk name="Blk103"
            from_="103" to_="103">
        </fabricNodeBlk>
        <fabricNodeBlk name="Blk104"
            from_="104" to_="104">
        </fabricNodeBlk>
<maintRsMgrpp
    tnMaintMaintPName="AllswitchesMaintP">
</maintRsMgrpp>
</maintMaintGrp>
</fabricInst>
```

Step 3   Post a policy similar to the following to upgrade all the switches based on a scheduler:

Example:

```
POST URL : https://<ip address>/api/node/mo/uni/fabric.xml
<trigSchedP annotation="" descr="" dn="uni/fabric/schedp-EveryEightHours"
name="EveryEightHours" nameAlias="" ownerKey="" ownerTag="" userdom="">
 <trigRecurrWindowP annotation="" concurCap="unlimited" day="every-day" hour="17" minute="0"
 name="third" nameAlias="" nodeUpgInterval="0" procBreak="none" procCap="unlimited"
timeCap="00:01:00:00.000" userdom=""/>
 <trigRecurrWindowP annotation="" concurCap="unlimited" day="every-day" hour="9" minute="0"
 name="second" nameAlias="" nodeUpgInterval="0" procBreak="none" procCap="unlimited"
timeCap="00:01:00:00.000" userdom=""/>
 <trigRecurrWindowP annotation="" concurCap="unlimited" day="every-day" hour="1" minute="0"
 name="first" nameAlias="" nodeUpgInterval="0" procBreak="none" procCap="unlimited"
timeCap="00:01:00:00.000" userdom=""/>
</trigSchedP>
```

ACI Upgrade/Downgrade Architecture

High Level Summary of APIC Upgrades and Downgrades

When performing an upgrade or downgrade of an APIC cluster, there is a certain sequence of events that occur to allow for the upgrade or downgrade of each APIC separately, along with ensuring that the data on the upgraded or downgraded APIC will be compatible with the target image. Most of these events happen in the background, so it's important to understand what you should expect to see when you trigger an upgrade or downgrade of the APIC cluster.

1. Image is uploaded to the firmware repository. The image is synced to all APIC cluster members.

2. Upgrade or downgrade is triggered to a specific target version.

3. Each APIC in the cluster goes through the process to install the new image in the first grub partition. This happens in parallel to speed up the upgrade or downgrade process.

4. Once the image installation is completed, each APIC takes its turn to go through a data conversion process of the database files in a sequential order. When this occurs, the following events happen:

    a. The Data Management Engine (DME) processes shut down. This includes the nginx web server which services all API requests. Because of this, you will lose access to the UI/API, as well as any other backend application that runs on that APIC.

    b. The database files are converted from the initial version to the target version. The amount of time this takes is dependent on the size of the configuration deployed on the ACI fabric. Because of this, the total time to complete the conversion will vary between deployments.

    When your source version is APIC release 6.0(3) or newer, the database conversion process has been enhanced and users may notice a shorter wait time for this process compared to the previous releases.

Note   *It's critical that there is no disruptive action taken to the APIC at this stage, as it could result in data loss or partial configuration if this stage does not complete successfully.* See Guidelines and Limitations for Upgrading or Downgrading, on page 55 for more information.

    c. The APIC will then reload after the database conversion process has completed successfully and will boot up on the version of software defined in the target version.

5. After the APIC that performed the reload comes back online, the sequence of events outlined in 4, on page 51 happen to the next APIC in the cluster. In the meantime, the APIC that came back online initiates the post upgrade activities as the final check of the database. This process repeats itself until all members of the cluster have been upgraded or downgraded.

6. Prior to Cisco APIC 6.0(6), the upgrade of the APIC cluster was considered complete when all APICs came back online and Fully-Fit regardless of the post upgrade activities. Starting from Cisco APIC 6.0(6), the status of APIC cluster upgrade will transition to "Post Upgrade Pending" until the post upgrade activities are complete on each APIC node. Then, the upgrade status will finally become "Completed".

Note   The post upgrade activities on APIC should be successfully completed before proceeding with the switch upgrades. In general, it is recommended to run the pre-upgrade validation script before the APIC cluster upgrade and before the switch upgrades respectively because the upgrade of the APIC cluster and switches may not occur during the same maintenance window. However, prior to Cisco APIC 6.0(6), it is highly encouraged to run the script before the switch upgrades even when it takes place within the same maintenance window because the script checks not only the pre-upgrade validations but also the status of the post upgrade activities to make sure the fabric is ready to proceed with the switch upgrades after the APIC cluster upgrade.

Note   Starting with Cisco APIC 6.1(1), due to a performance issue in the latest OpenSSH library (CSCwk67958), the post upgrade activities take longer to complete. For instance, the upgrade of APIC Cluster with 3 APICs from release 5.2 to 6.0 was typically in the range of 90 minutes to 120 minutes, which can be much shorter when the source version is 6.0(3) or newer with the enhanced database conversion process mentioned above.

However, when the target version is APIC release 6.1(1) or later, there is an additional increase of around 60 minutes. When the source version is 6.0(3) or newer, the increase due to the openSSH library and the reduction from enhanced database conversion may cancel each other out, and you may see shorter or longer upgrade time than your previous APIC cluster upgrade.

Note that upgrade/downgrade time taken depends on multiple factors - APIC cluster size, configuration, etc. and is an area of constant improvement.

Default Interface Policies in the 5.2(4) release and later

When you upgrade to the 5.2(4) or later release, the Cisco Application Policy Infrastructure Controller (APIC) creates the following default interface policies automatically:

    • CDP (cdpIfPol)

- system-cdp-disabled

- system-cdp-enabled

- LLDP (lldpIfPol)

  - system-lldp-disabled

  - system-lldp-enabled

- LACP (lacpLagPol)

  - system-static-on

  - system-lacp-passive

  - system-lacp-active

- Link Level (fabricHIfPol)

  - system-link-level-100M-auto

  - system-link-level-1G-auto

  - system-link-level-10G-auto

  - system-link-level-25G-auto

  - system-link-level-40G-auto

  - system-link-level-100G-auto

  - system-link-level-400G-auto

- Breakout Port Group Map (infraBrkoutPortGrp)

  - system-breakout-10g-4x

  - system-breakout-25g-4x

  - system-breakout-100g-4x

During the upgrade, if there is already a policy with the exact same name and the exact same parameters as any of these policies, the system takes ownership of those policies and the policies become read-only. If instead the parameters are different, such as the `system-cdp-disabled` has a setting "enabled," then the policies will continue to be user policies. That is, a user can modify the policies.

High Level Summary of Switch Upgrade and Downgrade

When performing an upgrade or downgrade of an ACI switch node, there is a certain sequence of events that occur to the device(s) being upgraded or downgraded. Most of these events happen in the background, so it's important to understand what you should expect to see when you trigger an upgrade of an ACI switch node.

1. The image is pushed from the APIC to the switch.

2. The filesystem and bootflash of the switch is checked to ensure that there is enough space to extract the image.

3. The image is extracted, and the primary grub partition is updated to the target version. The older version is moved into the recovery partition.

4. The BIOS and EPLD images are upgraded if applicable.

5. The switch will do a clean reload, and will re-join the ACI fabric running the newer version of software.

Starting with release 2.1(4), support was added for the third-party Micron Solid State Drive (SSD) firmware auto update. As part of the standard Cisco APIC software upgrade process, the switches will reboot when they upgrade. During that boot-time process, the system will also check the current SSD firmware and will automatically perform an upgrade to the SSD firmware, if necessary. If the system performs an SSD firmware upgrade, the switches will then go through another clean reboot afterward.

Detailed Summary of Switch Upgrade

The following sections provide a detailed summary of switch upgrades.

Understanding Switch Upgrade and Downgrade Stages

During an ACI switch node upgrade or downgrade, the upgrade or downgrade progress will advance based on the stages which have completed.

The following table provides more details on what happens at each stage of this upgrade or downgrade process:

Upgrade Progress	Install Stage	Description
0%	Firmware upgrade queued	Displayed when firmware is being downloaded to the switch from the APIC.
5%	Firmware upgrade in progress	Displayed when the upgrade installer is initiated, and the upgrade process has started.
45%	Firmware upgrade in progress	Displayed after the bootflash check has completed and the image extraction stage has begun.
60%	Firmware upgrade in progress	Image Extraction stage has completed and the grub partition is being updated with the new software information.
70%	Firmware upgrade in progress	The software has been updated on the switch.
80%	Firmware upgrade in progress	The EPLD and BIOS upgrade has begun.
95%	Firmware upgrade in progress	The EPLD and BIOS upgrade has completed, and switch reboot has been initiated.
100%	Upgraded Successfully	The switch has re-joined the fabric after the clean reload running target version of software.

Guidelines and Limitations for Upgrading or Downgrading

- If at any point in time you believe the upgrade or downgrade has either stalled or failed, it is critical that you do not take any of the actions listed below:

  - Do not reload any Application Policy Infrastructure Controller (APIC) in the cluster.

  - Do not decommission any Cisco APIC in the cluster.

  - Do not change the firmware target version back to the original version.

  Instead, follow these guidelines:

  1. View the installer log files outlined in the Troubleshooting section if applicable (see APIC Installer Log Files, on page 126 and ACI Switch Installer Log Files, on page 127). This will help in understanding if there is still activity ongoing on the devices being upgraded or downgraded.

  2. Collect the tech-support files outlined in the Troubleshooting section (see Collecting Tech-Support Files, on page 127).

  3. Contact Cisco TAC if the upgrade or downgrade does not complete successfully and upload the tech-support files to the TAC case after it has been created.

- If you are upgrading to Cisco APIC release 4.2(6o), 4.2(7l), 5.2(1g), or later, ensure that any VLAN encapsulation blocks that you are explicitly using for leaf switch front panel VLAN programming are set as "external (on the wire)." If these VLAN encapsulation blocks are instead set to "internal," the upgrade causes the front panel port VLAN to be removed, which can result in a datapath outage.

- The log record objects are stored only in one shard of a database on one of the Cisco APICs. Because of this, the log records are not accessible while the Cisco APIC is rebooting for an upgrade or downgrade, unlike other objects that can still be read through another Cisco APIC.

- When Cisco APIC is upgraded from Cisco APIC 4.0 or earlier to 5.1(1) or later, the Service Graph is re-rendered. This will result in traffic disruption until the re-rendering is completed, if vzAny-to-vzAny contract with service graph and another contract with service graph use the same service EPG.

- You may experience traffic loss for shared services when you upgrade from Cisco APIC 4.2 to Cisco APIC 5.2. To avoid this you can configure communication between tenants as well as communication between VRF instances within a tenant by using the constructs available within the fabric.

- To upgrade to the Cisco APIC 6.0(2) release or later, you must perform the following procedure:

  1. Download the Cisco APIC 6.0(2) or later image and upgrade the APIC cluster to the downloaded release. Before this step is completed, do not download the Cisco Application Centric Infrastructure (ACI)-mode switch images to the Cisco APIC. The 6.0(2) release has both 32-bit and 64-bit switch images, but releases prior to 6.0(2) do not support 64-bit images. As a result, downloading the 64-bit images at this time might cause errors or unexpected results. However, if your Cisco APICs have the 5.2(8) release or later, except for the 6.0(1) release, you can download the switch images to the Cisco APIC before this step the same as you would with any other upgrade procedure prior to 6.0(2).

  2. Download both the 32-bit and 64-bit Cisco ACI-mode switch images to the Cisco APIC. Downloading only one of the images may result in errors during the upgrade process.

  Beginning with the 6.0(3) release, the switch determines which image to install from the Cisco APIC based on the available memory of the switch instead of based on a static mapping. If the available

memory of the switch is less than or equal to 24 GB, the switch installs the 32-bit image. If the available memory of the switch is greater than or equal to 32 GB, the switch may be upgraded to the 32-bit image first, then upgraded again to the 64-bit image, which results in two reboots during the upgrade process.

Modular spine switches install the 64-bit image regardless of the switch's available memory.

3. Create the maintenance groups and trigger the upgrade procedure as usual. Cisco APIC automatically deploys the correct image to the respective switch during the upgrade process.

CHAPTER 6

Operations Allowed During Mixed Versions on Cisco ACI Switches

Operations Allowed During Mixed Versions on Cisco ACI Switches

The Cisco Application Centric Infrastructure (ACI) fabric essentially has a requirement that all nodes (Cisco Application Policy Infrastructure Controller (APIC), leaf switches, and spine switches) should have the same software release or have a compatible software release, where the Cisco APIC nodes have the standard release format of x.y(z), and the leaf and spine switches have the switch-specific standard release format of 1x.y(z). For example, if the Cisco APIC nodes are on software release 4.1(1), the leaf switches and spine switches should be on the switch-specific compatible version of 14.1(1).

However, this could be a challenging requirement when attempting to upgrade the software for a huge Cisco ACI fabric with a large number of switch nodes, because you would usually split the switch nodes into several different groups (maintenance groups) in this situation, which would allow you to perform the upgrade one group at a time to avoid any service disruptions. Depending on the number of switch nodes or maintenance groups, and the validation process for network traffic, services, and applications, you would be able to upgrade some maintenance groups on one day, but you might have to wait to upgrade the remaining maintenance groups on another day.

Starting with release 2.2(1), some operations can be performed even when all Cisco ACI switches are not yet on the same version due to a software upgrade. This behavior was enhanced in release 2.3(1) to support even more operations that can be performed in this situation. The following tables describe the operations that can be performed when switches are at mixed releases for releases 2.2(1) and 2.3(1) or later.

Supported Operations with Mixed Versions for Each Upgrade Path

Upgrade Path		Supported Operations
From	To	

Upgrade Path		Supported Operations
2.2(x)	Any versions in the supported upgrade path	• Exporting configuration • Collecting techsupport • Physical network change (i.e. reboot, cable replacement etc.) • Policy changes for features introduced prior to the major release[*]
2.3(x) or later	Any versions in the supported upgrade path	• Exporting configuration • Collecting techsupport • Physical network change (examples: reboot and cable replacement) • Policy changes for features introduced prior to the major release[*] • Policy changes for features in Supported Operations with Mixed Versions for Upgrades from Release 2.3(x) or Later, on page 58

[*] This operation is supported only when the upgrade is within the same release train. For example, an upgrade from 3.2(5d) to 3.2(5f), where the releases are still part of the 3.2(5) release train, but the upgrade occurs between the **d** and the **f** versions of that release train.

Supported Operations with Mixed Versions for Upgrades from Release 2.3(x) or Later

Starting from release 2.3(1), Cisco APIC supports the following features in addition to the ones listed above for operations allowed during mixed versions on Cisco ACI switches.

Features	Operations
Contracts	• Creating, updating, and deleting filters, subjects, and contracts. • Exporting and importing contracts. • Adding and deleting provided and consumed contracts in relationship with EPGs. • Adding and deleting provided and consumed contracts in vzAny.

Features	Operations
Endpoint group	• Creating and deleting EPGs. • Adding and deleting VMM, physical, Layer 2 external, and Layer 3 external domain association. • Adding, deleting, and updating static port assignment and statically linking with the node. • Moving an end point from one EPG to another EPG. • Moving an end point from uSeg EPG to base EPG.
Microsegmentation	Adding and updating uSeg EPG.
vMotion	vMotion across a leaf switch.
VM operation	On and off of virtual machines.
Bridge domain	Creating, updating, and deleting bridge domains.
VMM Domain	The following operations are supported only in VMware vDS and Cisco AVS. • Creating and deleting VMM domains. • Adding and updating VLAN pools. • Adding and deleting multicast pools. • Adding and updating VMware vCenter. • Adding and updating vSwitch policies.
Layer 2 or Layer 3 Out	Adding, updating, and deleting Layer 2 external and Layer 3 external domains.
Access Policy	• Adding, updating, and deleting switch policies, interface policies, policy group, Attached Entity Profiles (AEP).
Troubleshooting	• Adding, updating, and deleting SPAN configuration. • Adding, updating, and deleting syslog server.

Features	Operations
Physical network	• Enabling and disabling port status.
	• On and off of a physical server.
	• Moving physical server within and across leaf switches.
	• Reloading spine switches and leaf switches.
	When the reload is stateless, meaning that it is a clean reload in which the configuration is wiped and pulled again from the Cisco APICs, the switches must have the same release as the Cisco APICs.
	• Reloading a spine switch line card, Fibre Channel card, CS card, and SUP card.
	• Decommissioning spine switches and leaf switches.
	• Removing spine switches and leaf switches using the **Remove from Controller** option.
	• Registering a new spine switch and leaf switch.
	The new switch must have the same release as the Cisco APICs.
	• Adding and deleting a virtual port channel domain.
	• Flapping primary link, secondary link, and all the links in the virtual port channel.
	• Flapping all the port channel links, flapping one link in the port channel, flapping NIF ports on FEX, and flapping front panel ports on the leaf switch.
Fabric Policy	• Adding, updating, and deleting NTP server, SNMP, BGP route reflector, Layer 2 MTU policy.
	• Updating Cisco APIC connectivity preferences.

The following definitions are used to describe a Cisco APIC release.

- A Cisco APIC major release contains support for new software features and additional hardware updates. Examples of major releases include 2.2(1n) and 2.1(1h).

- A Cisco APIC minor or maintenance release (MR) contains the bugs fixes and patches from the existing release. Examples of minor or maintenance releases include 2.0(1m) and 2.0(2f).

- A Cisco APIC patch release contains fixes for specific defects. Examples of patch releases include 2.1(1h) and 2.1(1i).

Guidelines and Limitations for Mixed Versions on Cisco ACI-Mode Switches

- You must first upgrade all Cisco Application Policy Infrastructure Controller (APIC) nodes to the newer version to perform the supported operations described in Supported Operations with Mixed Versions for Each Upgrade Path, on page 57. Do not perform any operations until all the Cisco APIC nodes have been successfully and completely upgraded.

- Operations supported with mixed versions do not apply to vPC pair leaf switches running different software versions. vPC pair switches must be running the same software version for any operations.

- Operations supported with mixed versions are only for upgrade scenarios. Those are not applicable and not supported when downgrading the fabric, that is when APICs are running an older version than the switches.

- You can perform operations listed in Supported Operations with Mixed Versions for Each Upgrade Path, on page 57 only when it is regarding a feature that was already supported on the older (from) version.

- Prior to Cisco APIC release 3.0, a red banner warning is displayed, informing you of version differences on the Cisco ACI nodes in the fabric. This banner warning has been removed since Cisco APIC release 3.0.

- If your Cisco APIC is running the 5.2(4) release or later and your switches are running an Cisco ACI-mode switch software release that is earlier than 15.2(4), a vPC domain's interfaces become suspended/down when its peer node is decommissioned. Graceful insertion (maintenance mode) of the vPC peer node will also lead to the same issue because the switch is automatically decommissioned, rebooted, and recommissioned. In the following example scenarios, you will encounter this issue:

    - Your Cisco APIC is running the 5.2(4), 6.0(1), or later release and your vPC switches are running the Cisco ACI-mode switch 14.2(7u) or earlier release.

    - Your Cisco APIC is running the 5.2(4), 6.0(1), or later release and your vPC switches are running the Cisco ACI-mode switch 15.2(3) or earlier release.

  In the following example scenarios, you will not encounter this issue:

    - Your Cisco APIC is running the 5.2(4), 6.0(1), or later release and your vPC switches are running the Cisco ACI-mode switch 14.2(7v), 15.2(4), 16.0(1), or later release.

    - Cisco APIC is running the 5.2(3) release or earlier.

Pre-Upgrade/Downgrade Checklists

Check Basic Information on Your Fabric

Check some basic information on your fabric to ensure that you have everything that you need for a smooth upgrade. Specifically, it is critical that you clear all faults. Although some faults are described as specific issues in Check Configurations and Conditions That May Cause An Upgrade or Downgrade Failure, on page 64, you should always clear any faults before performing an upgrade except for the faults that are expected due to configurations in staging phase.

- Clear all your faults

- Perform a configuration export with AES Encryption

- Verify access to out-of-band IP addresses of all your ACI nodes (all your APIC nodes and switch nodes)

- Verify CIMC access for all your APICs

- Verify console access for all your switches

- Understand **Changes in Behavior** in Release Notes of both APIC and ACI switches for versions between the target and current version

- Understand **Open Issues** and **Known Issues** in Release Notes of both APIC and ACI switches for the target version

Check Configurations and Conditions That May Cause An Upgrade or Downgrade Failure

There are three different tools to perform pre-upgrade validation for Cisco Application Centric Infrastructure (ACI):

- **Pre-Upgrade Validator (APIC)**: A validator embedded in the Cisco Application Policy Infrastructure Controller (APIC) Upgrade Configuration. This is automatically performed when configuring an update group for the Cisco APIC or switches.

- **Pre-Upgrade Validator (App Center app)**: A validator that can be installed on the Cisco APICs as an app that can be downloaded through dcappcenter.cisco.com. After the app is installed, the app enables you to download the latest validation script from Cisco Cloud. This can be run on demand and is supported on release 5.2 and later.

- **Script**: For any feature not currently implemented in the Pre-Upgrade Validator, you can run a standalone script directly on the Cisco APIC to validate any existing issues prior to upgrading. The script supports all versions of software.

  We strongly recommend that you use this tool. To ensure you have ample time to address any issues, please run the validation at least 2 weeks before your maintenance window.

  See https://github.com/datacenter/ACI-Pre-Upgrade-Validation-Script for more details about the script.

See https://datacenter.github.io/ACI-Pre-Upgrade-Validation-Script/validations/ for the list of validations supported by the script along with comparisons with the other tools (Pre-Upgrade Validator (APIC, App Center app)).

Download Both the 32-bit and 64-bit Cisco ACI-Mode Switch Images (6.0(2) and later)

In the Cisco APIC release 6.0(2) and later, download both the 32-bit and 64-bit Cisco ACI-mode switch images to the Cisco APIC. Downloading only one of the images may result in errors during the upgrade process. For more information, see Guidelines and Limitations for Upgrading or Downgrading, on page 55.

Deprecated Managed Objects

The Pre_Upgrade checker script checks for the existence of the following deprecated managed objects on the running version of the software and blocks the upgrade, if they exist in the configuration. You must update your script or code to use the new managed object.

- **Class: config:RsExportDestination**

- **Class: config:RsImportSource**

- **Class: fabric:RsResMonFabricPol**

- **Class: infra:RsResMonInfraPol**

- **Class: fabric:RsResMonCommonPol**

- **Class: trig:Triggered**

- **Class: trig:TriggeredWindow**

- **Class: fv:CCg**

- **Class: fv:RsToCtrct**

- **Class: mgmt:RsOobEpg**

- **Class: mgmt:RsInbEpg**

- **Class: vns:RsCIfAtt**

- **Class: fault:RsHealthCtrlrRetP**

- **Class: fv:PndgCtrctCont**

- **Class: vz:RsAnyToCtrct**

- **Class: fv:PndgCtrctEpgCont**

- **Class: fv:AREpPUpd**

- **Class: vns:Chkr**

- **Class: aaa:RsFabricSetup**

- **Class: ap:PluginPol**

- **Class: tag:ExtMngdInst**

- **Class: telemetry:Server**

- **Class: telemetry:FltPolGrp**

- **Class: telemetry:FilterPolicy**

- **Class: telemetry:FlowServerP**

- **Class: pol:RsFabricSelfCAEp**

- **Class: fabric:PodDhcpServer**

- **Class: fabric:SetupAllocP**

- **Class: fabric:AssociatedSetupP**

- **Class: cloud:AEPgSelector**

- **Class: fv:VmmSelCont**

Checklists for Downgrade

In general, the same checklists as upgrades should be applied to downgrades. On top of that, you need to pay attention to the new features that may not yet be supported on older versions. If you are using such features,

you should disable or change the configurations prior to the downgrade. Otherwise, some functionality will stop working after downgrades.

The following lists some of the example features that you should pay attention to prior to downgrades. However, note that the following list is not complete and we highly recommend that you check the Release Notes or Configuration Guides to confirm that features that you are using are supported on older releases as well.

- The ability to use the DUO application as an authentication method when logging in to Cisco Application Policy Infrastructure Controller (APIC) was introduced as part of the Cisco APIC release 5.0(1). If you are running release 5.0(1) and you have DUO set up as your default authentication method, but then you decide to downgrade from release 5.0(1) to a previous release where DUO was not supported as an authentication method, we recommend that you change the default authentication method from DUO to an option that was available prior to release 5.0(1), such as Local, LDAP, RADIUS, and so on. If you do not change the default authentication method before downgrading in this situation, you will have to log in using the fallback option after the downgrade, then you will have to change the authentication method to an option that was available prior to release 5.0(1) at that point.

  Navigate to **Admin** > **AAA** > **Authentication**, then change the setting in the **Realm** field in the **Default Authentication** area of the page to change the default authentication method before downgrading your system. You will also have to manually delete the DUO login domain after the downgrade.

- Beginning in the 4.2(6) release, SNMPv3 supports the Secure Hash Algorithm-2 (SHA-2) authentication type. If you are running on Cisco APIC release 4.2(6) or later and you are using the SHA-2 authentication type, and then downgrade from Cisco APIC release 4.2(6) to a previous release, the downgrade will be blocked with the following error message:

  ```
  SHA-2authentication type is not supported.
  ```

  You can choose to either change the authentication type to MD5 or delete the corresponding SNMPv3 users to continue.

- Changing the container bridge IP address on Cisco APIC is supported only on Cisco APIC release 4.2(1) or later. If the container bridge IP address on Cisco APIC for AppCenter is configured with a non-default IP address, change it back the default 172.17.0.1/16 prior to downgrading to the older versions than 4.2(1).

- A static route (MO:**mgmtStaticRoute**) for Inband and/or Out-of-band EPG under **Tenants** > **mgmt** > **Node Management EPGs** is supported only on Cisco APIC release 5.1 or later. Delete this configuration and ensure the required service is still reachable via other means prior to the downgrade.

- Newly added microsegment EPG configurations must be removed before downgrading to a software release that does not support it.

- Downgrading the fabric starting with the leaf switch will cause faults such as policy-deployment-failed with fault code F1371.

- If you must downgrade the firmware from a release that supports FIPS to a release that does not support FIPS, you must first disable FIPS on the Cisco ACI fabric and reload all the switches in the fabric for the FIPS configuration change.

- If you have Anycast services configured in your Cisco ACI fabric, you must disable the Anycast gateway feature and stop Anycast services on external devices before downgrading from Cisco APIC 3.2(x) to an earlier release.

- CiscoN9K-C9508-FM-E2 fabric modules must be physically removed before downgrading to releases earlier than Cisco APIC 3.0(1). The same applies to any new modules for their respective supported version.

- If you are downgrading from Cisco APIC release 4.0(1) or later to release 3.2(x) or earlier, you may encounter a minor traffic drop in the fabric due to a difference in QoS classes supported between the releases. For more information, see CSCwa32037.

- If you have remote leaf switches deployed, and you downgrade the Cisco APIC software from release 3.1(1) or later to an earlier release that does not support the remote leaf switches feature, you must decommission the nodes before downgrading. For information about prerequisites to downgrading Remote Leaf switches, see the *Remote Leaf Switches* chapter in the *Cisco APIC Layer 3 Networking Configuration Guide*.

- If the following conditions are met:

  - You are running the 5.2(4) release and the Cisco APIC created one or more system-generated policies.

  - You downgrade the Cisco APIC from the 5.2(4) release, then later upgrade back to the 5.2(4) release.

  Then, one of the following behaviors will occur:

  - If the Cisco APIC finds a policy with the same name and parameters as a system-generated policy that it is trying to create, then the Cisco APIC will take ownership of the policy and you cannot modify the policy. This occurs if you did not modify the policy after downgrading from the 5.2(4) release.

  - If the Cisco APIC finds a policy with the same name as a system-generated policy that the Cisco APIC is trying to create, but the parameters are different, then the Cisco APIC will consider the policy to be a custom policy and you can modify the policy. This occurs if you modified the policy after downgrading from the 5.2(4) release.

  Because of this behavior, you should not modify the system-generated policies after you downgrade from the 5.2(4) release.

- If you are downgrading from a Cisco APIC release that supports the Transport Layer Security (TLS) version 1.3, you enabled TLS 1.3 in a management access policy, and the target Cisco APIC release does not support TLS 1.3, then you must disable TLS 1.3 and instead enable TLS 1.2.

- You must decommission an unsupported leaf switch that is connected to the Cisco APIC and move the cables to the other leaf switch that is part of the fabric before you downgrade the image.

- In the Cisco APIC 6.0(2) release or later, if the cluster's discovery mode is set to "strict" and you want to downgrade to any 4.2 release or earlier, you must first change the discovery mode "permissive."

- The APIC-M4/L4 server is supported in the Cisco APIC 6.0(2) release and later and 5.3(1) release and later. However, if you downgrade from the 6.0(2) or 6.0(3) release to a 5.3 release, you see a pre-upgrade validation warning that the APIC-M4/L4 server is not supported. In this case, you can ignore the warning.

  The following screenshot shows an example of this pre-upgrade validation warning:
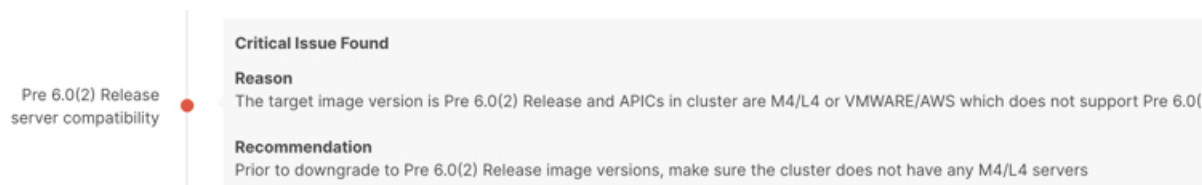
Examples of Pre-Upgrade Validator (APIC)

Example Error Messages and Override Options Through the GUI with APIC Release 4.2(5)

There are three situations where warning messages might appear through the GUI:

- While the query is loading, where you might see a message similar to the following:
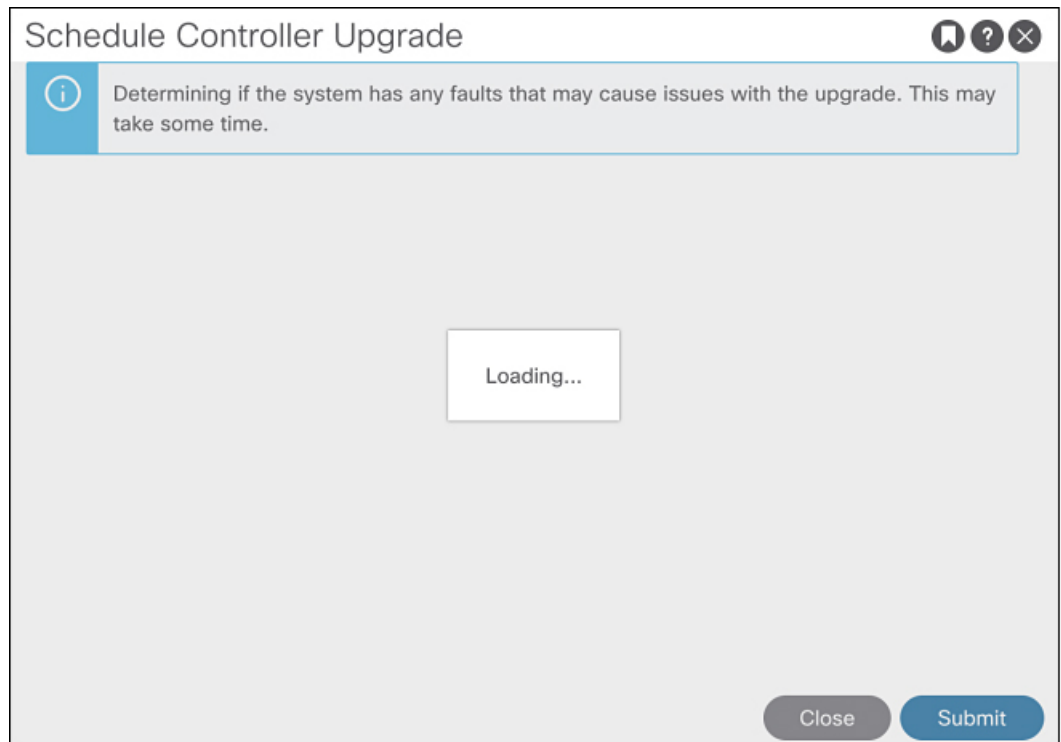
This might occur because it sometimes takes a bit of time to load the data from a query. In this situation, be patient and wait for the system to finish loading the data from the query.

- If the query fails for some reason, you might see a message similar to the following:

This warning will appear if the query failed for some reason (for example, there might be so many faults that the system is overloaded). In this case, it is up to you to verify if there are any faults that might cause an issue with the upgrade.

However, if you want to override the block and proceed with an upgrade or downgrade without addressing the issue with the failed query, check the box next to the **I understand there may be active faults on the system which can lead to unexpected issues, proceed with the upgrade** field. This allows you continue with the upgrade or downgrade process without addressing the issue with the failed query.

• After the fault query is complete, where you might see a message similar to the following:

This warning message will appear when the fault query is complete and the system has found one or more faults. In this situation, click the **Click Here** link to get more information on the faults that the system found.

If possible, we recommend that you resolve the issue that was raised in the fault before proceeding with the upgrade or downgrade process. For more information on these faults and the recommended action for each, see the Cisco APIC System Faults/Events Search Tool and the Cisco ACI System Messages Reference Guide.

However, if you want to override the block and proceed with an upgrade or downgrade without addressing the issue that was raised in the fault, check the box next to the **I understand there are active faults on the system which can lead to unexpected issues, proceed with the upgrade** field. This allows you continue with the upgrade or downgrade process without addressing the faults that were detected.

Example Error Messages and Override Options Through the NX-OS Style CLI

When you attempt to upgrade the software through the NX-OS style CLI:

```
apic# firmware upgrade controller-group
```

You might see an error message similar to the following if faults on the fabric are detected:

```
Error: Migration cannot proceed due to 23 active critical config faults. Resolve the faults
 to proceed
```

If possible, we recommend that you resolve the issue that was raised in the fault before proceeding with the upgrade or downgrade process. For more information on these faults and the recommended action for each, see the Cisco APIC System Faults/Events Search Tool and the Cisco ACI System Messages Reference Guide.

However, if you want to override the block and proceed with an upgrade or downgrade without addressing the issue that was raised in the fault, use the `ignore-validation` option to proceed with the upgrade:

```
apic# firmware upgrade controller-group ignore-validation
```

Upgrading or Downgrading with APIC Releases Prior to 4.x Using the GUI

Note   Ensure that you check and follow these guidelines:

- Workflow to Upgrade or Downgrade the Cisco ACI Fabric, on page 34

- Pre-Upgrade/Downgrade Checklists, on page 63

- Guidelines and Limitations for Upgrading or Downgrading, on page 55

Downloading APIC and Switch Images on APICs

This procedure is to download firmware images of APICs and ACI switches into APIC's firmware repository from an external file server or from your local machine.

Procedure

Step 1   On the menu bar, choose **ADMIN** > **Firmware**, and in the **Navigation** pane, click **Controller Firmware**. In the **Work** pane, the Cisco APICs display the current firmware that is loaded on each controller. Also displayed is a status about when the firmware was last upgraded or downgraded.

Step 2   In the **Navigation** pane, click **Download Tasks**.

Step 3   In the **Work** pane, choose **General** > **Actions**, and click **Create Outside Firmware source**.

Step 4   In the **Create Outside Firmware Source** dialog box, perform the following actions:

a)   In the **Source Name** field, enter a name for the Cisco APIC image file, for example *apic_image*.

b)   In the **Protocol** field, click the **HTTP** radio button.

Note   If you want to download the software image from an http source or a Secure Copy Protocol (SCP) source, click the appropriate radio button and use the format **<SCP server>:/<path>**. An example URL is **10.67.82.87:/home/<username>/ACI/aci-apic-dk9.1.0.2j.iso**.

c)   In the **Url** field, enter the URL from where the image must be downloaded. Click **Submit**.

Wait for the Cisco APIC firmware images to download.

Step 5   In the **Navigation** pane, click **Download Tasks**. In the **Work** pane, click **Operational** to view the download status of the images.

After the download reaches 100% in the **Navigation** pane, click **Firmware Repository**.

In the **Work** pane, the downloaded version numbers and image sizes are displayed.

Upgrading or Downgrading the Cisco APIC from Releases Prior to Release 4.x

Note   If you are upgrading to the release 4.0 or later, make sure to delete all existing switch firmware and maintenance group prior to performing Cisco Application Policy Infrastructure Controller (APIC) upgrades.

See Pre-Upgrade/Downgrade Checklists, on page 63 for details.

Use these GUI-based procedures to upgrade or downgrade the software on the Cisco APICs in your fabric.

If you are not able to upgrade or downgrade the software on the Cisco APICs in your fabric using these GUI-based upgrade procedures for some reason (such as if you received a Cisco APIC through a new order or Product Returns & Replacements (RMA), and the version is old and not able to join the fabric to perform an upgrade using the GUI), you can perform a clean installation of the software on the Cisco APICs through the CIMC instead to upgrade or downgrade your Cisco APIC software. See Installing Cisco APIC Software Using Virtual Media, on page 18 for those procedures.

If you are downgrading the software on the Cisco APICs, the process is identical to the process for upgrading the software, except that the target release that you choose will be earlier than the currently installed release. The text for dialogs, fields, buttons, and other controls in the Cisco APIC GUI specify "upgrade" even though you are downgrading the software.

Before you begin

Ensure that you check and follow these guidelines:

• Workflow to Upgrade or Downgrade the Cisco ACI Fabric, on page 34

• Pre-Upgrade/Downgrade Checklists, on page 63

• Guidelines and Limitations for Upgrading or Downgrading, on page 55

Procedure

Step 1   In the **Navigation** pane, click **Controller Firmware**. In the **Work** pane, choose **Actions** > **Upgrade Controller Firmware Policy**. In the **Upgrade Controller Firmware Policy** dialog box, perform the following actions:

    a) In the **Target Firmware Version** field, from the drop-down list, choose the image version to which you want to upgrade or downgrade.

    b) In the **Apply Policy** field, click the radio button for **Apply now**. Click **Submit**.

    The **Status** dialog box displays the **Changes Saved Successfully** message, and the upgrade or downgrade process begins. The Cisco APICs are upgraded or downgraded serially so that the controller cluster is available during the upgrade or downgrade.

Step 2   Verify the status of the upgrade or downgrade in the **Work** pane by clicking **Controller Firmware** in the **Navigation** pane.

    The controllers upgrade or downgrade in random order. After a controller image is upgraded or downgraded, it drops from the cluster and it reboots with the newer version while the other Cisco APICs in the cluster are still operational. After the controller reboots, it joins the cluster again. Then the cluster converges, and the next controller image starts to upgrade or downgrade. If the cluster does not immediately converge and is not fully fit, the upgrade or downgrade will wait until the cluster converges and is fully fit. During this period, a **Waiting for Cluster Convergence** message is displayed in the **Status** column for each Cisco APIC as it upgrades or downgrades.

    When the Cisco APIC that the browser is connected to is upgraded or downgraded and it reboots, the browser displays an error message.

Step 3   In the browser URL field, enter the URL for the Cisco APIC that has already been upgraded or downgraded, and sign in to the Cisco APIC as prompted.

Upgrading or Downgrading the Leaf and Spine Switches Through APIC Running Prior to Release 4.x

Note   This is a switch upgrade or downgrade procedure using the APIC GUI that is running on release prior to release 4.x. If your APICs are already upgraded to the version 4.x or later, the GUI procedure is different even if switches are still running versions prior to release 14.x. In such a case, check the corresponding section, such as:

    If you are downgrading the software on the Cisco APICs, the process is identical to the process for upgrading the software, except that the target release that you choose will be earlier than the currently installed release. The text for dialogs, fields, buttons, and other controls in the Cisco APIC GUI specify "upgrade" even though you are downgrading the software.

        • Release 4.x or 5.0:

        • Release 5.1 or later:

Before you begin

Ensure that you check and follow these guidelines:

- Wait until all the controllers are upgraded or downgraded to the new firmware version before proceeding to upgrade or downgrade the switch firmware.

- Workflow to Upgrade or Downgrade the Cisco ACI Fabric, on page 34

- Pre-Upgrade/Downgrade Checklists, on page 63

- Guidelines and Limitations for Upgrading or Downgrading, on page 55

Procedure

Step 1   In the **Navigation** pane, right-click **Fabric Node Firmware** and click **Firmware Upgrade Wizard**.
In the **Work** pane, the **Create Firmware Group** dialog box appears.

Step 2   In the **Create Firmware Group** dialog box, perform the following actions:

a) Under **Nodes**, click the **Select All** tab to choose all the nodes in the fabric in the **Selected** column. Click **Next**.

b) Under **Firmware Group**, in the **Group Name** field, enter a group name.

c) In the **Ignore Compatibility Check** field, leave the setting in the default **off** (unchecked) setting, unless you are specifically told to disable the compatibility check feature.

> **Note**   If you choose to disable the compatibility check feature by entering a check mark in the box next to the Ignore Compatibility Check field, you run the risk of making an unsupported upgrade or downgrade to your system, which could result in your system going to an unavailable state.

d) In the **Target Firmware Version** field, from the drop-down list, choose the desired image version to which you want to upgrade or downgrade the switches. Click **Next**.

e) Under **Maintenance Group**, create two maintenance groups for all the switches. For example, create one group with the even-numbered devices and the other group with the odd-numbered devices.

> **Note**   While a single maintenance group will upgrade all leaf and spine switches at the same time, Cisco recommends that you divide your leaf and spine switches into multiple (two or more) maintenance groups to prevent the entire fabric from going down during a software upgrade or downgrade. Dividing up the leaf and spine switches into two or more maintenance groups, composed of roughly equivalent groups of leaf and spine switches, allows continued operation of the fabric during software upgrades by upgrading half (or less) of the fabric nodes at one time.

f) Click the **Create Maintenance Group** tab.

g) In the **Create Maintenance Group** dialog box, in the **Group Name** field, enter a name for the group.

h) In the **Run Mode** field, choose the **Pause only Upon Upgrade Failure** radio button which is the default mode.

i) Check the **Graceful Maintenance** check box if you want to isolate the node from the fabric prior to the reboot that occurs during the upgrade or downgrade operation so that traffic is pro-actively diverted to other available switches.

j) Click **Submit**.

k) Click **Finish**.

In the **Work** pane, all the switches are displayed with the name of the firmware group and the maintenance group under which they are scheduled for upgrade or downgrade.

Step 3   In the **Navigation** pane, expand **Fabric Node Firmware** > **Firmware Groups**, and click the name of the firmware group that you created.
The **Work** pane displays details about the firmware policy that was created earlier.

Step 4   In the **Navigation** pane, expand **Fabric Node Firmware** > **Maintenance Groups**, and click the maintenance group that you created.
The **Work** pane displays details about the maintenance policy.

Step 5   Right-click the maintenance group you created and click **Upgrade Now**.

Step 6   In the **Upgrade Now** dialog box, for **Do you want to upgrade the maintenance group policy now?**, click **Yes**. Click **OK**.

> **Note**   In the **Work** pane, the **Status** displays that all the switches in the group are being upgraded or downgraded simultaneously. The default concurrency in a group is set at 20. Therefore, up to 20 switches at a time will get upgraded or downgraded, and then the next set of 20 switches are upgraded or downgraded. If there are any virtual port channel (vPC) configurations in the fabric, the upgrade or downgrade process will upgrade or downgrade only one switch at a time out of the two switches in a vPC domain regardless of the concurrency setting. In case of any failures, the scheduler pauses and manual intervention is required by the Cisco APIC administrator. Each switch generally takes about 10 minutes for the upgrade or downgrade. The switches will reboot when they upgrade or downgrade, connectivity drops, and the controllers in the cluster will not communicate for some time with the switches in the group. After the switches rejoin the fabric after rebooting, you will see all the switches from the controller node.

Step 7   In the **Navigation** pane, click **Fabric Node Firmware**.
In the **Work** pane, view all the switches listed. In the **Current Firmware** column view the upgrade image details listed against each switch. Verify that the switches in the fabric are upgraded or downgraded to the new image.

Upgrading or Downgrading the Catalog Through APIC Running Prior to Release 4.x

The catalog is used by the upgrade compatibility check that can be turned on and off through **Ignore Compatibility Check**. The catalog image is embedded in an APIC image and is upgraded or downgraded when a Cisco APIC image is upgraded or downgraded. However, if for some reason the catalog image was not upgraded or downgraded along with the APIC image, there is an option to manually upgrade or downgraded the catalog. This procedure is rarely used and not available in the APIC GUI with later releases.

If you are downgrading the software on the Cisco APICs, the process is identical to the process for upgrading the software, except that the target release that you choose will be earlier than the currently installed release. The text for dialogs, fields, buttons, and other controls in the Cisco APIC GUI specify "upgrade" even though you are downgrading the software.

Procedure

Step 1   On the menu bar, choose **ADMIN** > **Firmware**. In the **Navigation** pane, click **Catalog Firmware**.

Step 2   In the **Work** pane, choose **Actions** > **Change Catalog Firmware Policy**.

Step 3   In the **Change Catalog Firmware Policy** dialog box, perform the following actions:

a) In the **Catalog Version** field, choose the desired catalog firmware version.

b) In the **Apply Policy** field, click the **Apply now** radio button to upgrade or downgrade the firmware immediately. Click **Submit**.

c) In the **Work** pane, wait until the image displays that the **Target Firmware version** field matches the image version in the **Current Firmware Version** field.
The Catalog version is now upgraded or downgraded.

Upgrading or Downgrading with APIC Releases 4.x or 5.0 Using the GUI

Note   Ensure that you check and follow these guidelines:

- You must decommission an unsupported leaf switch that is connected to the Cisco APIC and move the cables to the other leaf switch that is part of the fabric before you upgrade or downgrade the image.

Downloading APIC and Switch Images on APICs

This procedure is to download firmware images of APICs and ACI switches into APIC's firmware repository from an external file server or from your local machine.

If you are downgrading the software on the Cisco APICs, the process is identical to the process for upgrading the software, except that the target release that you choose will be earlier than the currently installed release. The text for dialogs, fields, buttons, and other controls in the Cisco APIC GUI specify "upgrade" even though you are downgrading the software.

Procedure

Step 1   On the menu bar, choose **Admin** > **Firmware**.
The Summary window appears, which provides the following information:

- **Nodes** tile — Provides information on the firmware versions used by the physical nodes.

- **Virtual Nodes** tile — Provides information on the firmware versions used by the virtual nodes.

- **Controller** tile — Provides information on the firmware version used by this controller. Also provides information on the catalog version.

- **Controller Storage** tile — Provides information on the storage capacity of each controller.

Step 2   Click the **Images** tab, then click the **Actions** icon and select **Add Firmware to APIC** from the scrolldown menu.
The **Add Firmware to APIC** popup window appears.

Step 3   Determine if you want to import the firmware image from a local or a remote location.

- If you want to import the firmware image from a *local* location, click the **Local** radio button in the **Firmware Image Location** field. Click the **Browse...** button, then navigate to the folder on your local system with the firmware image that you want to import. Go to .

- If you want to import the firmware image from a *remote* location, click the **Remote** radio button in the **Firmware Image Location** field, then perform the following actions:

a) In the **Download Name** field, either select an existing download using the options provided in the scrolldown menu, or enter a name for the Cisco APIC image file to create a new download (for example, *apic_image*).

   Note   You can also delete an existing download task by entering the existing download name in the **Download Name** field, then clicking on the trash icon next to the field.

   The following fields appear if you are creating a new download.

b) In the **Protocol** field, click either the **HTTP** or the **Secure copy** radio button.
c) In the **URL** field, enter the URL from where the image will be downloaded.

- If you selected the **HTTP** radio button in the previous step, enter the http source that you want to use to download the software image.

- If you selected the **Secure copy** radio button in the previous step, enter the Secure Copy Protocol (SCP) source that you want to use to download the software image.

   The format for both HTTP and SCP source is:

   `<HTTP/SCP server IP or FQDN>:/<path>/<filename>`

   An example URL is `10.1.2.3:/path/to/the/image/aci-apic-dk9.5.0.1a.iso`.

   If you selected **SCP** as the protocol, the following fields appear.

d) In the **Username** field, enter your username for secure copy.
e) In the **Authentication Type** field, select the type of authentication for the download. The type can be:

- **Use Password**

- **Use SSH Public/Private Key Files**

   The default is **Use Password**.

f) If you selected **Use Password**, in the **Password** field, enter your password for secure copy.
g) If you selected **SSH Key**, enter the following information:

> • **SSH Key Content**: The SSH Private Key Content.
>
> • **SSH Key Passphrase**: The SSH Key Passphrase that is used for generating the SSH Private Key.

Note   Based on the provided SSH Private Key, APIC internally creates a temporary SSH public key just for this transaction to establish a connection with the remote server. You must ensure that the remote server has the corresponding public key as one of the "authorized_keys". After the authentication check is performed, the temporary public key on APIC is deleted.

You can generate an SSH Private Key (`~/.ssh/id_rsa`) and a corresponding SSH Public Key (`~/.ssh/id_rsa.pub`) on one of the APICs by entering the following:

```
ssh-keygen -t rsa -b 2048 -C "<username>@<apic_name>"
```

Or you can generate them on another machine. For either method, you need to provide the generated private key for each download configuration.

Step 4   Click **Submit**.
Wait for the Cisco APIC firmware images to download.

Step 5   Click the **Images** tab again, if necessary, to view the download status of the images.

After the download reaches 100%, double-click on the row in the table for the firmware image that you downloaded to bring up the **Firmware Details** page for that particular firmware image.

Upgrading or Downgrading the Cisco APIC From Releases 4.x or 5.0

Use these GUI-based upgrade or downgrade procedures to upgrade or downgrade the software on the APICs in your fabric.

If you are not able to upgrade or downgrade the software on the Cisco APICs in your fabric using these GUI-based upgrade or downgrade procedures for some reason (such as if you received an Cisco APIC through a new order or Product Returns & Replacements (RMA), and the version is old and not able to join the fabric to perform an upgrade or downgrade using the GUI), you can perform a clean installation of the software on the Cisco APICs through the CIMC instead to upgrade or downgrade your Cisco APIC software. See Installing Cisco APIC Software Using Virtual Media, on page 18 for those procedures.

If you are downgrading the software on the Cisco APICs, the process is identical to the process for upgrading the software, except that the target release that you choose will be earlier than the currently installed release. The text for dialogs, fields, buttons, and other controls in the Cisco APIC GUI specify "upgrade" even though you are downgrading the software.

Before you begin

Ensure that you check and follow these guidelines:

- Workflow to Upgrade or Downgrade the Cisco ACI Fabric, on page 34

- Pre-Upgrade/Downgrade Checklists, on page 63

- Guidelines and Limitations for Upgrading or Downgrading, on page 55

- You must decommission an unsupported leaf switch that is connected to the Cisco APIC and move the cables to the other leaf switch that is part of the fabric before you upgrade the image.

- If you are upgrading from a Cisco APIC release earlier than 5.0 to a 5.0 or later release and you have an IPv4 host route (/32) or IPv6 host route (/128) that is learned using MP-BGP, if those host routes overlap with a local attached non-pervasive subnet, such as an L3Out SVI subnet, the forwarding information base (FIB) process skips the hardware programming for those host routes. This behavior is intentional. You can avoid this situation by using one of the following workarounds:

  - Do not advertise in the /32 or /128 host route that overlaps with an L3Out interface subnet.

  - Advertise using any subnet other than /32 or /128.

  - Peer directly from the border leaf switches to the same peers as the original nodes where there is peering.

Procedure

Step 1   On the menu bar, choose **Admin** > **Firmware**.
The Summary window appears, which provides the following information:

- **Nodes** tile—Provides information on the firmware versions that are used by the physical nodes.

- **Virtual Nodes** tile—Provides information on the firmware versions that are used by the virtual nodes.

- **Controller** tile—Provides information on the firmware version that is used by this controller. Also provides information on the catalog version.

- **Controller Storage** tile—Provides information on the storage capacity of each controller.

Step 2   Click the **Infrastructure** tab, then click the **Controllers** sub-tab, if it isn't already selected.

Step 3   Choose **Actions** > **Schedule Controller Upgrade**.

The **Schedule Controller Upgrade** dialog box appears.

In some situations, you might see an error message, similar to the following:

Schedule Controller Upgrade

Migration cannot proceed due to 6 active critical config faults. Ack the faults to proceed.

Infra:Following nodes are not in VPC: ['101']

Infra:No Spine with even id is defined as route reflector. All external prefixes will be lost when even maintenance window spines reboot

It's recommended that these faults are resolved before performing a controller upgrade. All unsupported features must be disabled before downgrade to avoid unpredictable behavior.

More Info

☐ I understand there are active faults on the system which can lead to unexpected issues, proceed with the upgrade.

Target Firmware Version: select an option
❶ This field is required

Current Version:

Upgrade Start Time: **Upgrade now** | Upgrade later

Ignore Compatibility Check: ☐

Close | Submit

See the Pre-Upgrade/Downgrade Checklists, on page 63 for items that are checked by the Cisco APIC pre-upgrade validator in your version and other items you should check through the AppCenter pre-upgrade validator, either using a script or manually.

Step 4   In the **Schedule Controller Upgrade** dialog box, perform the following actions:

a) In the **Target Firmware Version** field, from the drop-down list, choose the image version to which you want to upgrade or downgrade.

b) In the **Upgrade Start Time** field, click one of the two radio buttons:

- **Upgrade now**

- **Upgrade later**—Select the day and time when you want the upgrade or downgrade to occur.

  Following are example scenarios for different entries in the **Upgrade later** field and how the system will react in each scenario:

  - **You set the Start Time to a point that is *earlier* than the current time**: The upgrade or downgrade point is set to a point in the past, so the configuration will be rejected by the system.

  - **You set the Start Time to a point that is *later* than the current time**: The upgrade or downgrade starts at the point that you set.

c) In the **Ignore Compatibility Check** field, leave the setting in the default **off** (unchecked) setting, unless you are specifically told to disable the compatibility check feature.

Note   If you choose to disable the compatibility check feature by entering a check mark in the box next to the Ignore Compatibility Check field, you run the risk of making an unsupported upgrade or downgrade to your system, which could result in your system going to an unavailable state.

The **Status** dialog box displays the **Changes Saved Successfully** message, and the upgrade or downgrade process begins. The Cisco APICs are upgraded or downgraded serially so that the controller cluster is available during the upgrade or downgrade.

Step 5   Verify the status of the upgrade or downgrade by clicking the **Controllers** sub-tab again, if necessary, in the **Infrastructure** pane.

The controllers upgrade or downgrade sequentially, in a random order. After a controller image is upgraded or downgraded, it drops from the cluster, and it reboots with the newer version while the other Cisco APICs in the cluster are still operational. After the controller reboots, it joins the cluster again. Then the cluster converges, and the next controller image starts to upgrade or downgrade. If the cluster does not immediately converge and is not fully fit, the upgrade or downgrade waits until the cluster converges and is fully fit. During this period, a **Waiting for Cluster Convergence** message is displayed in the **Status** column for each Cisco APIC as it upgrades or downgrades.

Beginning with Cisco APIC release 4.2(5), additional information may be provided on the status of the upgrade process for the controllers. See **Understanding APIC Upgrade and Downgrade Stages** for a complete description of the different stages for Cisco APIC upgrades.

Note   The actual upgrade process remains the same with release 4.2(5) as it was with previous releases. However, starting with release 4.2(5), additional information is now provided that shows you the stage that you are in during the upgrade process.

Step 6   In the browser URL field, enter the URL for the Cisco APIC that has already been upgraded, and sign in to the Cisco APIC as prompted.

Upgrading or Downgrading the Leaf and Spine Switches Through a Cisco APIC Running Releases 4.x or 5.0

This is a switch upgrade or downgrade procedure using the Cisco Application Policy Infrastructure Controller (APIC) GUI that is running on release 4.x or 5.0. If your Cisco APICs are already upgraded to the release 5.1 or later, the GUI procedure is different even if switches are still running releases prior to 14.x or 15.0. In such a case, check the corresponding section, such as .

If you are downgrading the software on the Cisco APICs, the process is identical to the process for upgrading the software, except that the target release that you choose will be earlier than the currently installed release. The text for dialogs, fields, buttons, and other controls in the Cisco APIC GUI specify "upgrade" even though you are downgrading the software.

Before you begin

Ensure that you check and follow these guidelines:

- Wait until all the controllers are upgraded or downgraded to the new firmware release before proceeding to upgrade or downgrade the switch firmware.

  - Workflow to Upgrade or Downgrade the Cisco ACI Fabric, on page 34

  - Pre-Upgrade/Downgrade Checklists, on page 63

  - Guidelines and Limitations for Upgrading or Downgrading, on page 55

Procedure

Step 1   Verify that all the controllers are upgraded or downgraded to the new firmware release before proceeding. Do not upgrade or downgrade the switch firmware until all the controllers are upgraded or downgraded to the new firmware release first.

Step 2   On the menu bar, choose **Admin** > **Firmware**.
The Summary window appears, which provides the following information:

- **Nodes** tile — Provides information on the firmware releases used by the physical nodes.

- **Virtual Nodes** tile — Provides information on the firmware releases used by the virtual nodes.

- **Controller** tile — Provides information on the firmware release used by this controller. Also provides information on the catalog version.

- **Controller Storage** tile — Provides information on the storage capacity of each controller.

Step 3   Click the **Infrastructure** tab, then click the **Nodes** sub-tab.

Step 4   Click **Actions**, then select **Schedule Node Upgrade**, and perform the following actions.

In some situations, you might see an error message, similar to the following:
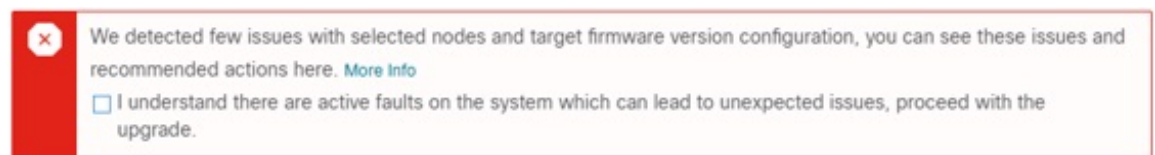
See the Pre-Upgrade/Downgrade Checklists, on page 63 for items that are checked by the Cisco APIC pre-upgrade validator in your release and other items you should check through the AppCenter pre-upgrade validator, either using a script or manually.

a)   In the **Group Type** field, select either **Switch** or **vPod**.

b)   In the **Upgrade Group** field, select either **Existing** or **New**, if this field is available.

Beginning with Release 4.1(2), you can use the **Upgrade Group** field to select whether you are using an existing or new upgrade group.

- **Existing**—Select to use an existing upgrade group. Select the existing upgrade group in the **Upgrade Group Name** field below in this case, then make any changes in the remaining fields in this page if you want to modify any properties for the existing upgrade group.

- **New**—Select to create a new upgrade group. Enter the name of the new upgrade group in the **Upgrade Group Name** field below in this case, then enter information for the remaining fields in this page to create a new upgrade group.

c) In the **Upgrade Group Name** field, select the upgrade group name from the scrolldown menu for an existing upgrade group, or enter a name in the textbox for a new upgrade group.

For releases prior to 4.1(2), either select an existing upgrade group using the options provided in the scrolldown menu, or, to create a new upgrade group, click the **x** in the corner of the field to clear out the field, then enter a name for the new upgrade group.

Note that if you select an existing POD maintenance group, fields associated with that maintenance group are automatically filled in.

d) Determine if you want to perform a silent roll package upgrade.

> **Note**   Choose **Manual Silent Roll Package Upgrade** (SR package upgrade) only when you need to perform an internal package upgrade for ACI switch hardware SDK, drivers, and so on, instead of a normal switch software upgrade. When performing an SR package upgrade, the maintenance group is dedicated for SR package upgrade and a normal switch software upgrade cannot be performed. Refer to Silent Roll Package Upgrade, on page 133 for details.

e) In the **Target Firmware Version** field, from the drop-down list, choose the desired image version to which you want to upgrade the switches.

f) In the **Ignore Compatibility Check** field, leave the setting in the default **off** (unchecked) setting, unless you are specifically told to disable the compatibility check feature.

> **Note**   If you choose to disable the compatibility check feature by entering a check mark in the box next to the Ignore Compatibility Check field, you run the risk of making an unsupported upgrade to your system, which could result in your system going to an unavailable state.

g) Check the **Graceful Maintenance** check box if you want to isolate the node from the fabric prior to the reboot that occurs during the upgrade operation so that traffic is pro-actively diverted to other available switches.

h) In the **Run Mode** field, choose the run mode to proceed automatically to the next set of nodes once the set of nodes has gone through the maintenance process successfully.

The options are:

- **Do not pause on failure and do not wait on cluster health**

- **Pause upon upgrade failure**

The default is **Pause only Upon Upgrade Failure**.

i) In the **Upgrade Start Time** field, select either **Now** or **Schedule for Later**.

The number of switches that can be upgraded at a time varies depending on release:

- For releases prior to Release 4.2(5), the default concurrency in a group is set at 20. Therefore, up to 20 switches at a time will get upgraded, and then the next set of 20 switches are upgraded.

- For Release 4.2(5) and forward, the default concurrency in a group has changed from 20 to unlimited (the default number of leaf or spine switches that can be upgraded at one time is unlimited).

The values above apply for both **Now** and **Schedule for Later**.

If you select **Schedule for Later**, either select an existing trigger scheduler, or click Create Trigger Scheduler to create a new trigger scheduler.

j) For Release 4.1(2) or later, click the + icon at the right of the All Nodes area.

The **Add Nodes to Upgrade Group** page appears.

k) In the **Add Nodes to Upgrade Group** page (Release 4.1(2) or later), or in the **Node Selection** field (for releases prior to 4.1(2)), select either **Range** or **Manual**.

- If you select **Range**, enter the range in the **Group Node Ids** field.

- If you select **Manual**, a list of available leaf switches and spine switches appears in the All Nodes area. Select the nodes that you want to include in this upgrade.

  Note that the nodes displayed are physical leaf switches and spine switches if you selected **Switch** in the **Group Type** field, or virtual leaf switches or virtual spine switches if you selected **Vpod**.

l) Click **Submit**.

You are then returned to the main **Firmware** page.

Beginning with Cisco APIC release 4.2(5), a **Download Progress** field is available in the **Work** pane, which provides a status on the progress of the download of the firmware for the node upgrade.

- If the firmware download fails for any reason, the status in the **Download Progress** field will show as red. An error popup will be displayed when you hover your cursor over the status bar in this case, with the message **Download Status: download-failed** displayed.

- If the firmware download is successful, the status bar in the **Download Progress** field will change to green and will display **100%**. If you hover your cursor over the status bar in this case, the message **Download Status: downloaded** is displayed.

You might also get a notification in this screen if you do not have enough space in the `/firmware` partition for the image to download. Confirm that the `/firmware` partition is not filled beyond 75%. If the partition is filled beyond 75%, you might have to remove some unused firmware files from the repository. This accommodates the compressed image and provides adequate space to extract the image.

In the table under **Admin** > **Firmware** > **Infrastructure** > **Nodes**, there is a column for **Upgrade Group** (formerly displayed as POD maintenance group) to show which upgrade group each node belongs to. You can see the following options by right-clicking this column for a specific node.

- Edit Upgrade Group (releases prior to 4.1(2))

- View Upgrade Group (For Release 4.1(2) or later)

- Delete Upgrade Group

Prior to release 4.1(2), you can edit the upgrade group using this option to change the target version and trigger the upgrade of nodes. For release 4.1(2) or later, this column can only be used to view the existing upgrade group details. You can delete a selected upgrade group in any release.

Step 5 For release 4.1(2) or later, to remove nodes from the upgrade group:

a) Select the nodes in the table that you want to remove from the upgrade group.

b) Click the trashcan icon at the right of the All Nodes area.

c) Click **Submit**.

Upgrading or Downgrading with APIC Release 5.1 or Later Using the GUI

Note Ensure that you check and follow these guidelines:

- Starting from release 5.1, ACI firmware upgrade using the GUI does not provide an option to set a scheduler for the upgrade. Instead, the benefits from using a scheduler such as image pre-download on switches are all built-in the native workflow.

- You must decommission an unsupported leaf switch that is connected to the Cisco APIC and move the cables to the other leaf switch that is part of the fabric before you upgrade the image.

Accessing the Dashboard

You can access the dashboard, which shows you the firmware status of the APIC nodes and switches in your fabric, by navigating to **Admin** > **Firmware** > **Dashboard**.

The dashboard also shows the usage of firmware repository on each APICs.

Downloading APIC and Switch Images on APICs

This procedure downloads firmware images of the Cisco Application Policy Infrastructure Controllers (APICs) and Cisco Application Centric Infrastructure (ACI)-mode switches into the Cisco APIC's firmware repository from an external file server or from your local machine.

If you are downgrading the software on the Cisco APICs, the process is identical to the process for upgrading the software, except that the target release that you choose will be earlier than the currently installed release. The text for dialogs, fields, buttons, and other controls in the Cisco APIC GUI specify "upgrade" even though you are downgrading the software.

Note In the Cisco APIC release 6.0(2) and later, download both the 32-bit and 64-bit Cisco ACI-mode switch images to the Cisco APIC. Downloading only one of the images may result in errors during the upgrade process. For more information, see Guidelines and Limitations for Upgrading or Downgrading, on page 55.

In the Cisco ACI-mode switch 16.0(3d), 16.0(3e), 16.0(4c), and 16.0(5h) releases, the 64-bit switch software has the same image name as the 32-bit software when installed on the switch. To verify which version is running on the switch, use the **md5sum** command against the image file on switch. Compare this md5sum hash to the switch image contained in the `/firmware/fwrepos/fwrepo` directory of the Cisco APIC. On subsequent upgrades, the 64-bit and 32-bit image names are differentiated on the switch.

Procedure

Step 1 Download the desired target version from the Cisco Software Download site (for example, 5.2(1g) release) to your file server or local machine.

Step 2 On the menu bar, choose **Admin** > **Firmware**.
The **Dashboard** window appears, which provides general information one the controllers and the leaf and spine switches (nodes).

Step 3 Click **Images** in the left navigation bar.
The **Image** window appears, which shows the images that you downloaded previously.

Step 4 Click the **Actions** icon and select **Add Firmware** from the scrolldown menu.
The **Add Firmware Image** popup window appears.

Step 5 Determine if you want to import the firmware image from a local or a remote location.

- If you want to import the firmware image from your computer, in the **Location** field, click the **Local** radio button. Click the **Choose File** button, then navigate to the folder on your local system with the firmware image that you want to import. Go to Step 6, on page 91.

- If you want to import the firmware image from a remote location, click either **Secure copy** or **HTTP**, depending on the method that you want to use to import the firmware image from the remote location:

    - If you selected the **Secure copy** radio button, enter the Secure Copy Protocol (SCP) source that you want to use to download the software image:

        a. In the **URL** field, enter the URL from where the image will be downloaded.

        The format for the SCP source is:

        ```
        <SCP server IP or FQDN>:/<path>/<filename>
        ```

An example URL is `10.1.2.3:/path/to/the/image/aci-apic-dk9.5.0.1a.iso`.

b. In the **Username** field, enter your username for secure copy.

c. In the **Authentication Type** field, select the type of authentication for the download. The type can be:

- **Password**

- **Ssh Public Private Files**

The default is **Password**.

- If you selected **Password**, in the **Password** field, enter your password for secure copy.

- If you selected **Ssh Public Private Files**, enter the following information:

  - **Ssh Key Contents**: The SSH private key content.

  - **Ssh Key Passphrase**: The SSH key passphrase that is used for generating the SSH private key.

    Note Based on the provided SSH private key, the Cisco APIC internally creates a temporary SSH public key just for this transaction to establish a connection with the remote server. You must ensure that the remote server has the corresponding public key as one of the "authorized_keys". After the authentication check is performed, the temporary public key on the Cisco APIC is deleted.

    You can generate an SSH private key (`~/.ssh/id_rsa`) and a corresponding SSH public key (`~/.ssh/id_rsa.pub`) on one of the Cisco APICs by entering the following:

    ```
    ssh-keygen -t rsa -b 2048 -C "<username>@<apic_name>"
    ```

    Or you can generate them on another machine. For either method, you need to provide the generated private key for each download configuration.

- If you selected the **HTTP** radio button, enter the http source that you want to use to download the software image.

  The format for the HTTP source is:

  ```
  <HTTP server IP or FQDN>:/<path>/<filename>
  ```

  An example URL is `10.1.2.3:/path/to/the/image/aci-apic-dk9.5.0.1a.iso`.

Step 6 Click **Submit**.

The Cisco APICs begins downloading the specified firmware images from the configured source. The download progress is shown in the **Download Status** column

Upgrading or Downgrading the Cisco APIC From Releases 5.1x or Later

Use these GUI-based upgrade or downgrade procedures to upgrade the software on the Cisco APICs in your fabric.

If you are not able to upgrade the software on the Cisco APICs in your fabric using these GUI-based upgrade procedures for some reason (such as if you received a Cisco APIC through a new order or Product Returns & Replacements (RMA), and the version is old and not able to join the fabric to perform an upgrade using the GUI), you can perform a clean installation of the software on the Cisco APICs through the CIMC instead to upgrade your Cisco APIC software. See Installing Cisco APIC Software Using Virtual Media for those procedures. Or, if your Cisco APIC cluster is running the Cisco APIC 6.0(2) release or newer, the new Cisco APIC is automatically upgraded or downgraded to the same version of the existing cluster using Auto Firmware Update on APIC Discovery.

If you are downgrading the software on the Cisco APICs, the process is identical to the process for upgrading the software, except that the target release that you choose will be earlier than the currently installed release. The text for dialogs, fields, buttons, and other controls in the Cisco APIC GUI specify "upgrade" even though you are downgrading the software.

Before you begin

Ensure that you check and follow these guidelines:

- If you are upgrading from a Cisco APIC release earlier than 5.0 to a 5.0 or later release and you have an IPv4 host route (/32) or IPv6 host route (/128) that is learned using MP-BGP, if those host routes overlap with a local attached non-pervasive subnet, such as an L3Out SVI subnet, the forwarding information base (FIB) process skips the hardware programming for those host routes. This behavior is intentional. You can avoid this situation by using one of the following workarounds:

  - Do not advertise in the /32 or /128 host route that overlaps with an L3Out interface subnet.
  - Advertise using any subnet other than /32 or /128.
  - Peer directly from the border leaf switches to the same peers as the original nodes where there is peering.

Procedure

Step 1   On the menu bar, choose **Admin** > **Firmware**.
The **Dashboard** window appears, which provides general information one the controllers and the leaf and spine switches (nodes).

Step 2   In the left navigation window, click **Controllers**.
The **Controllers** window appears, which provides firmware information for the controllers.

Step 3   Click the **Setup Update** button.

The **Version Selection** step of the **Setup Controller Firmware Upgrade** window appears, showing all of the software images that you have downloaded onto your system.

Note   If you see the following error message instead:

```
No firmware images available. Please check the Images tab.
```

Then you do not have a image available to use for the upgrade. Add an image to use for the upgrade using the procedures provided in Downloading APIC and Switch Images on APICs, on page 90.

Step 4   Select an image that you want to use for the firmware update, then click **Next**.

The **Validation** step appears.

Step 5   Review the information provided in the **Validation** screen.

Beginning with release 5.1(1), certain validation checks are performed and displayed in the **Validation** screen, with a message showing whether each validation check passed or failed.

For any validation check that has failed, we recommend that you address those faults or issues before proceeding with the upgrade.

Once you have addressed the faults or issues raised in the **Validation** window, click **Next** to go to the **Confirmation** window.

Step 6   In the **Confirmation** window, verify that the information is correct, then click **Begin Install**.

The **Controllers** window appears again, and the status of the upgrade or downgrade is displayed.

The Cisco APICs are upgraded or downgraded serially so that the controller cluster is available during the upgrade or downgrade. Once a controller image is upgraded or downgraded, it drops from the cluster, and it reboots with the newer version while the other Cisco APICs in the cluster are still operational. Once the controller reboots, it joins the cluster again. Then the cluster converges, and the next controller image starts to upgrade or downgrade. If the cluster does not immediately converge and is not fully fit, the upgrade or downgrade waits until the cluster converges and is fully fit. During this period, a **Waiting for Cluster Convergence** message is displayed in the **Update Status** column for each Cisco APIC as it upgrades or downgrades.

When the Cisco APIC that the browser is connected to is upgraded or downgraded and it reboots, the browser first displays an error message, then you will not be able to see anything in the browser that you used to log into this Cisco APIC. However, you can log into any of the remaining Cisco APICs in the cluster to continue to monitor the progress of the upgrade or downgrade process, if you want.

Additional information may be provided on the status of the upgrade process for the controllers. See **Understanding APIC Upgrade and Downgrade Stages** for a complete description of the different stages for Cisco APIC upgrades or downgrades.

Note   The actual upgrade or downgrade process remains the same with release 5.1(1) as it was with previous releases. However, starting with release 5.1(1), additional information is now provided that shows you the stage that you are in during the upgrade or downgrade process.

Step 7   In the browser URL field, enter the URL for the Cisco APIC that has already been upgraded, and sign in to the Cisco APIC as prompted.

Step 8   Wait for all the Cisco APICs to complete the upgrade or downgrade and become **Fully Fit**.

Upgrading or Downgrading the Leaf and Spine Switches Through APIC Running Release 5.1x or Later

Pre-Download Images to the Leaf and Spine Switches

This procedure describes how to download switch images to leaf and spine switches from APIC's firmware repository at your own timing without starting the actual upgrade (i.e. software installation) or downgrade. This is called pre-download. Prior to APIC release 5.1(1), this operation had to be triggered through a scheduler. But starting from APIC release 5.1(1), the native GUI workflow allows you to create switches update groups and perform pre-download.

During this operation, switches will remain up and no reboot will be performed.

> **Note** When you upgrade a switch from one release to the next release, the fault code F1821 is displayed as the bootflash memory increases. Ignore this fault as it is auto cleared after the switch upgrade.

If you are downgrading the software on the Cisco APICs, the process is identical to the process for upgrading the software, except that the target release that you choose will be earlier than the currently installed release. The text for dialogs, fields, buttons, and other controls in the Cisco APIC GUI specify "upgrade" even though you are downgrading the software.

Before you begin

Ensure that you check and follow these guidelines:

- Wait until all the controllers are upgraded or downgraded to the new firmware version before proceeding to upgrade or downgrade the switch firmware.

- Workflow to Upgrade or Downgrade the Cisco ACI Fabric, on page 34

- Pre-Upgrade/Downgrade Checklists, on page 63

- Guidelines and Limitations for Upgrading or Downgrading, on page 55

Procedure

Step 1 On the menu bar, choose **Admin** > **Firmware**.
The **Dashboard** window appears, which provides general information one the controllers and the leaf and spine switches (nodes).

Step 2 In the left navigation window, click **Switches**.
The **Switches** window appears, which provides firmware information for the upgrade groups of leaf and spine switches.

Step 3 Click the **Actions** icon and select **Create Update Group** from the scroll down menu.

Step 4 In the **Setup Switch Update Group** window appears, enter a name for the **Upgrade Group Name**.

Step 5   In the **Switch Selection** step, click the **Add Switches** button, then select the switches that need to be upgraded / downgraded and then click **OK**, then click **Next**.

Step 6   In the **Version Selection** step, select an **Update Type**, then in the **Select Firmware** section select an image that you want to upgrade/downgrade.

Step 7   (Optional) If you need any of the advanced options listed below, click **Advanced Settings** to bring up the **Advanced Settings** window.

Note that typically there is no need to set these advanced options. We recommend that you disable the options or use the default values.

In the **Advanced Settings** window, perform any of the following actions if needed:

- In the **Compatibility Check** field, leave the setting in the default **Enforced** setting, unless you are specifically told to disable the compatibility check feature.

  Note   A compatibility check verifies if an upgrade path from the currently running version of the system to a specific newer version is supported or not based on catalog that is embedded in Cisco APIC image. If you choose to disable the compatibility check feature by entering a check mark in the box next to the **Compatibility Check** field, you run the risk of making an unsupported upgrade to your system, which could result in your system going to an unavailable state.

- **Graceful Upgrade (Graceful Check)**

  Enable this option to perform a **Graceful Upgrade** when the firmware installation is triggered. By default, this setting is **Unenforced**.

  See Graceful Upgrade or Downgrade of ACI Switches, on page 39 for details and make sure to follow the guidelines when enabling this option. Otherwise, your upgrade may fail.

- In the **Run Mode** field, choose the run mode to proceed automatically to the next set of nodes after the set of nodes has gone through the maintenance process successfully.

  The options are:

  - **Pause Upon Upgrade Failure**: The update group does not approve further switch upgrades if there is an upgrade failure in one of the switches, or if the APIC cluster status becomes not Fully Fit, which may happen (for example, when all APIC-connected leaf switches are upgraded at the same time, which is not recommended in Guidelines for ACI Switch Upgrades and Downgrades, on page 36).

  - **Do not pause on failure and do not wait on cluster health**: The update group does not stop switch upgrades of the entire group just because one of the switches had an upgrade failure or a temporary APIC cluster issue.

  We recommend that you choose **Do not pause on failure and do not wait on cluster health** because it is recommended to group switches that should be upgraded at the same time in one update group instead of letting each update group to dynamically decide which set of switches within the same group to be upgraded (for instance, with the concurrent capacity setting). When following such best practices, **Pause Upon Upgrade Failure** does not provide much value.

Click **Done** when you have finished performing any of the actions in the **Advanced Settings** window. You are then returned to the main **Firmware** page.

Step 8   When you have verified that everything in the **Version Selection** step is correct, click **Next**.
The **Validation** step appears.

Step 9   Review the information provided in the **Validation** step.

Any faults or issues that might affect your upgrade are displayed in this page. We recommend that you address any faults or issues that you see displayed before proceeding with the upgrade.

See the Pre-Upgrade/Downgrade Checklists, on page 63 for items that are checked by the APIC pre-upgrade validator in your version and other items you should check through the AppCenter pre-upgrade validator, either using a script or manually.

After you have addressed the faults or issues raised in the **Validation** step, click **Next** to go to the **Confirmation** step.

Step 10   In the **Confirmation** step, verify that the information is correct, then click **Begin Download**.

The system begins downloading the software to all of the nodes that you selected in the previous screen, and displays the download status for each node.

Note   If you are upgrading from a release prior to Cisco APIC release 4.2(6), the download status will show as `downloading` but will not progress to the next stage showing that the download has completed. This is a known issue when upgrading from a release prior to Cisco APIC release 4.2(6) and is expected behavior. Follow the instructions in Installing Images to the Leaf and Spine Switches, on page 97 so that the software installation process will begin after the download is completed.

Note   If you are upgrading nodes in different upgrade groups from a pre-5.1x release using the instructions provided in Upgrading or Downgrading the Leaf and Spine Switches Through a Cisco APIC Running Releases 4.x or 5.0, on page 84 and you made the following selections previously:

- **Now** in the **Upgrade Start Time** field

- **unlimited** in the **Maximum Running Time** field

Then you might see the following behavior:

- **First upgrade group**: When you click on **Begin Download** in these procedures, the software begins the image download and then automatically installs the software on the nodes in the first upgrade group after the image download is complete. This is unexpected behavior.

- **Second upgrade group**: When you click on **Begin Download** in these procedures, the software begins the image download but does not automatically install the software on the nodes in the second upgrade group after the image download is complete. This is expected behavior - you will install the software using the information in Installing Images to the Leaf and Spine Switches, on page 97 in these procedures.

While the behavior for the first upgrade group is unexpected, it is not harmful. Be aware that the nodes in the first upgrade group will reboot as part of the software installation process that happens automatically in this scenario.

Step 11   Verify that the download was completed successfully for all of the nodes that you want to upgrade in the group.

If any nodes are shown as **Failed** in the Status column, you have several options:

- Click **Retry All** at the bottom of the page to retry the download for all the nodes in the upgrade group.

- Click **Cancel All** at the bottom of the page to cancel the downloads for the nodes in the upgrade group.

- If you want to manually remove the failed nodes from this upgrade group so that you can move forward with the upgrade for the nodes that were successful in the download phase, click the pencil icon next to any node that you want to manually remove from this upgrade group and click **Remove**.

See Common Reasons for Download Failure, on page 122 for troubleshooting.

When you see the status of **Download Complete** for all the nodes in your group, you will see **Ready to Install** at the top of the screen.

Installing Images to the Leaf and Spine Switches

After the pre-download on all switches is done and their upgrade status show **Ready to Install**, you can perform the procedure to trigger the upgrade, which will install the firmware and reboot the switches.

Typically, you would perform a pre-download hours or days before this procedure. Make sure that you did not violate any validations since the pre-upgrade validations were performed at the time of pre-download. If you want to perform pre-upgrade validations again at this point, use the App Center Pre-Upgrade Validator or the script because the APIC built-in pre-upgrade validator will result in the re-downloading of the switch image.

Before you begin

Ensure that you check and follow these guidelines:

- Workflow to Upgrade or Downgrade the Cisco ACI Fabric, on page 34

- Pre-Upgrade/Downgrade Checklists, on page 63

- Guidelines and Limitations for Upgrading or Downgrading, on page 55

You must first finish the pre-download procedures in Pre-Download Images to the Leaf and Spine Switches, on page 94.

Procedure

Step 1   When you have a maintenance window where you are able to have the nodes reboot as part of the upgrade process, click **Actions**, then **Begin Install** to begin the software installation.

You can monitor the progress of the upgrade for the nodes in the upgrade group in the **Node Firmware Update** window. You can also close this window and click **Nodes** in the left navigation window to check the overall status of the upgrade group in the **Status** column in the table.

Step 2   When all of the nodes are shown with a status of **Completed**, click **Done** and proceed with the next update group.

Understanding App Installation Behavior

Certain Apps are available to install on APICs and are available to download through the App Center (https://dcappcenter.cisco.com/). These Apps fall into two categories:

- **User-installed Apps**: Apps that you download manually from the App Center and then upload to the APIC.

- **Pre-packaged Apps**: Apps that are installed on an APIC automatically by the plugin-handler.

You can install an App using the REST API or the APIC GUI:

- To install an App using the REST API, send a post with XML such as the following examples. The protocol that you choose while triggering a download task depends on the file server hosting the App image. The following post shows an example where the protocol is SCP:

```
POST {{apic-url}}/api/policymgr/mo/.xml

<polUni>
    <fabricInst>
        <firmwareRepoP>
            <firmwareOSource name="MY-APP" proto="scp" url="URL:PATH-TO-APP-IMAGE"
user="MY-USER-NAME" password="MY-PASSWORD"/>
        </firmwareRepoP>
    </fabricInst>
</polUni>
```

The following example shows a similar post where the protocol is HTTP:

```
POST {{apic-url}}/api/policymgr/mo/.xml

<polUni>
    <fabricInst>
        <firmwareRepoP>
            <firmwareOSource name="httpuploadapp" proto="http"
url="{{downloadserver}}/{{filename}}" status="created,modified"/>
        </firmwareRepoP>
    </fabricInst>
</polUni>
```

- To install an App using the APIC GUI:

    - For APIC releases prior to 5.2:

        1. Click **Admin** > **Downloads**.

           The **Downloads** screen appears.

        2. Click the **Task** icon (✖▾) on the far-right side of the **Downloads** work pane and select **Add File to APIC**.

           The **Add File to APIC** dialog appears.

        3. Enter the name of the download file in the **Download Name** field.

        4. In the **Protocol** field, choose **Secure Copy**.

        5. In the **URL** field, enter the path to the download file image location.

6. Enter your username and password in the **Username** and **Password** field and click **Submit**.

7. Click the **Operational** tab and then click the **Refresh** icon (⟳) on the far-right side of the **Downloads** work pane to check the status.

   The application will automatically install after downloaded. This could take approximately five minutes to complete.

   • For APIC release 5.2 or later:

   1. Click **Apps** > **Downloads**.

      The **Downloads** screen appears.

   2. Click the **Task** icon (✕▾) on the far-right side of the **Downloads** work pane and select **Add File to APIC**.

      The **Add File to APIC** dialog appears.

   3. Enter the name of the download file in the **Download Name** field.

   4. In the **Protocol** field, choose **Secure Copy**.

   5. In the **URL** field, enter the path to the download file image location.

   6. Enter your username and password in the **Username** and **Password** field and click **Submit**.

   7. Click the **Operational** tab and then click the **Refresh** icon (⟳) on the far-right side of the **Downloads** work pane to check the status.

      The application will automatically install after downloaded. This could take approximately five minutes to complete.

When you install an App from App Center on an APIC, the behavior around that App installation varies, depending on several factors:

   • Whether the App is a **user-installed App** or a **pre-packaged App**

   • Whether this is a fresh installation, an upgrade, or a downgrade for the App on the APIC

User-Installed Apps

If you are manually installing an App that doesn't normally come pre-installed on an APIC, the behavior around that installation varies, depending on the following situations:

   • If you do not already have this App installed on your APIC, then this is considered a fresh installation and the App is installed on your APIC in the normal fashion.

   • If you already have this App installed on your APIC and the App currently installed on your APIC is an **earlier** version of the App, then the upload of this later version of the App to your APIC triggers an upgrade of the App on your APIC.

   • If you already have this App installed on your APIC and the App currently installed on your APIC is a **later** version of the App, then the upload of this earlier version of the App to your APIC triggers a downgrade of the App on your APIC.

Pre-Packaged Apps

When you upgrade or downgrade all of the APICs in a cluster to a new APIC image, the plugin-handler checks for pre-packaged Apps images that come with that new APIC image.

- If the plugin-handler finds that an App is available in the new APIC image but that App is not currently installed on your APICs, then the plugin-handler triggers the installation of that App on your APICs.

- If the plugin-handler finds that an App is available in the new APIC image and that App is already installed on your APICs, the plugin-handler then checks if the App that is available in the new APIC image is an earlier or later release than the App currently installed on your APICs:

    - If the version of the App in the new APIC image is a **later** release than the App currently installed in your APICs, then the plugin-handler triggers an upgrade or downgrade for that App on your APICs. Beginning with release 5.2(3), pre-packaged Apps get upgraded or downgraded to whatever App images are bundled in the APIC image after all of the APICs are upgraded or downgraded in a setup, regardless of what version of those Apps were running on that setup before the APICs got upgraded or downgraded.

    - If the version of the App in the new APIC image is an **earlier** release than the App currently installed in your APICs, then the plugin-handler takes no action with the App on your APICs. The plugin-handler does not downgrade the App on your APICs to that earlier version that is available in the new APIC image. This is done so that you can install newer versions of an App, where the version of an App that you install might be later than the version that comes pre-packaged with an APIC image, and the plugin-handler won't automatically overwrite the later version of that App currently on your APICs with an earlier version.

For example, assume the APICs in a cluster are running on release version 1.2(3), and the pre-packaged App **AcmeApp** is available for APIC release 1.2(3), where 4.5(6) is the version of AcmeApp that is normally pre-packaged on APICs running on release 1.2(3).

Assume that you want to upgrade the AcmeApp at some later date and the latest version of AcmeApp, the 4.6(1) version of AcmeApp, is available at the App Center. You then manually download and install that latest version of AcmeApp so that the APICs and the AcmeApp are at the following versions:

- The APICs in the cluster are still running on APIC release 1.2(3)

- The AcmeApp on these APICs is now updated to AcmeApp version 4.6(1)

Now assume that you decide to upgrade the APIC from release 1.2(3) to release 1.2(4) at another date later on. However, for APICs running on 1.2(4), the version of AcmeApp that is normally pre-packaged is version 4.5(7). In that case, the plugin-handler would not make any changes to the version of AcmeApp running on your APIC, because your APIC already has a version of AcmeApp running on it [version 4.6(1)] that is later than the 4.5.(7) version that would normally come pre-packaged with APIC release 1.2(4).

Note that you can change the Apps policy for pre-packaged Apps:

- Through the REST API, you can change the Apps policy for pre-packaged Apps by modifying the `apPrepackagedPlugins` MO using one of the following three options:

    - **install-all**: This is the default value. This option installs or upgrades pre-packaged Apps in the manner that is described above.

    ```
    POST {{apic-url}}/api/policymgr/mo/.xml

    <polUni>
    ```

```
    <apPluginPolContainer>
        <apPrepackagedPlugins PrepackagedAppsAction="install-all"/>
    </apPluginPolContainer>
</polUni>
```

- **remove-all**: This option removes all pre-packaged Apps from APIC.

```
POST {{apic-url}}/api/policymgr/mo/.xml

<polUni>
  <apPluginPolContainer>
      <apPrepackagedPlugins PrepackagedAppsAction="remove-all"/>
  </apPluginPolContainer>
</polUni>
```

- **skip-installation**: This option disables the plugin-handler from automatically installing or upgrading pre-packaged Apps in future APIC image upgrades.

```
POST {{apic-url}}/api/policymgr/mo/.xml

<polUni>
  <apPluginPolContainer>
      <apPrepackagedPlugins PrepackagedAppsAction="skip-installation"/>
  </apPluginPolContainer>
</polUni>
```

- Through the APIC GUI:

  1. Navigate to **Apps** > **Installed Apps**.

     The **Apps** page is displayed.

  2. Click on the **Settings** icon (⚒▾), then choose **Change Prepackaged Apps Policy**.

     The **Change Prepackaged Apps Policy** page appears.

  3. Choose one of the following options (see the options descriptions above in the REST API information):

     - Install All

     - Remove All

     - Skip Installation

Working with Hidden Pre-Packaged Apps

For any App that you install, whether it is a user-installed App or a pre-packaged App, you can usually see that App displayed in the **Apps** window in the APIC GUI, which you can view by navigating to **Apps** > **Installed Apps**.
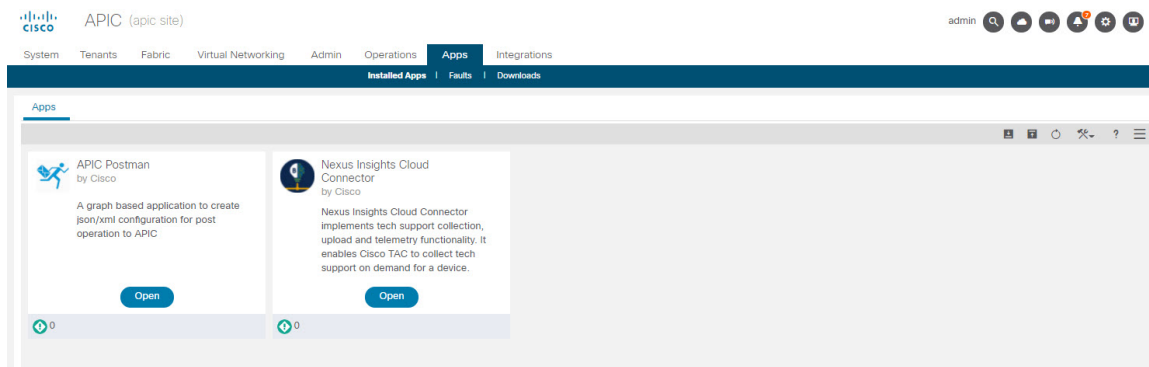
You can perform certain actions for Apps displayed in this window, such as opening, enabling, or deleting those Apps.

However, there are certain pre-packaged Apps that might be installed on your APICs but are not displayed in the **Apps** window in the APIC GUI, such as the ApicVision App that became available beginning with release 5.2(1). While these hidden Apps won't appear in the **Apps** window, they might appear in the **Faults** window if there is an issue with that App (**Apps** > **Faults**).

> **Note** The pre-packaged ApicVision App that became available with release 5.2(1) is not available for download through the App store, so do not make changes to or delete the ApicVision App. Contact Cisco TAC support if you have any issues or faults with the pre-packaged ApicVision App.

You can locate and work with these hidden pre-packaged Apps through Visore, the APIC Object Store Browser that you can use to directly query Managed Objects (MOs). For more information on Visore, see *Application Policy Infrastructure Controller Visore Tool Introduction*.

You can access Visore by appending `/visore.html` to the URL that you would normally use to log into your APIC GUI:

```
https://<APIC or Switch IP ADDRESS>/visore.html
```

After you have logged into Visore, the Object Store window is displayed.
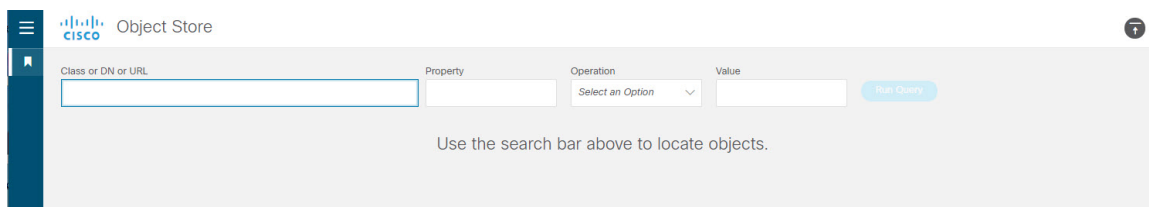
From there, you can query the MO for any Apps installed on your APICs by entering `apPlugin` in the **Class or DN or URL** field and clicking **Run Query**. Visore returns output showing the number of objects found for this MO, which is the total number of Apps that are installed on your APICs, including hidden Apps that aren't displayed in the **Apps** window in the normal APIC GUI.

Object Store

Class or DN or URL		Property	Operation	Value	
apPlugin	×		Select an Option		Run Query

3 objects found   Show URL and response of last query

☑ Empty Properties

apPlugin

dn	‹ pluginContr/plugin-Cisco_ApicVision ›
annotation	
apicMode	Apic
appCtxRoot	Cisco_ApicVision
appId	ApicVision
appType	infra
cert	-----BEGIN CERTIFICATE----- MIIDoTCCAomgAwIBAgIJANuUZW17M35PMA0GCSqGSIb3DQEBCwUAMGcxCzAJBgNV BAYTAlVTMQswCQYDVQQIDAJDQTEQMA4GA1UEBwwHU0FOSk9TRTENMAsGA1UECgwE QVBJQzEPMA0GA1UECwwGUExVR0lOMRkwFwYDVQQDDBBDaXNjb19BcGljVmlzaW9u MB4XDTIxMDUyMTAwMzkyNVoXDTMxMDUxOTAwMzkyNVowZzELMAkGA1UEBhMCVVMx CzAJBgNVBAgMAkNBMRAwDgYDVQQHDAdTQU5KT1NFMQ0wCwYDVQQKDARBUEIDMQ8w DQYDVQQLDAZQTFVHSU4xGTAXBgNVBAMMEENpc2NvX0FwaWNWaXNpb24wggEiMA0G CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCRM/tIejSz/a6KIX//R3ycR43eWrKr sxAgyFnSq3/kQvcL7zYI4OE1blcbniyj5DdaAoyJP+1bCy4b+r2C/ZPFjAq8Fvpb vTVc6ZBg2xMeiKWhtvdBDrzp6bcxkcGqqbo9inNl0AVuiOPm0c+WwDDGGpVQ9KLL iAg5xQrA1qlhaMi6RIW2DDnfQF4bp7N+x3Zvn7kkUm2tf6DkpNp6LiEupwGaqAy6 oJ0Azctmiapj0THM3RIvxjZtvlj3ZDuOzIekW4rHY3TkngfujXfEcCDn/byonF3L 4p3Xs9MA5EcojJHYWY7nyNIVTMItE8Atdpc0wcaG4tr6394nuUpDhM69AgMBAAGj UDBOMB0GA1UdDgQWBBQRIIutaVq3BrbRqCUbscQvQje9/jAfBgNVHSMEGDAWgBQR IIutaVq3BrbRqCUbscQvQje9/jAMBgNVHRMEBTADAQH/MA0GCSqGSIb3DQEBCwUA A4IBAQA7pYolc8BedbKte3i3Xtszao4WmWktLME+xWVKSGGXZVRsOg9chwFyOxPE C6ClJUha0Tzyw333IQ5/QkGCPbG8bOR+0rhucGPs02J9lsehq512Aszv3Oc6DjVc ws0cyeY2b0mDWpxLXkAwSSsaCmwsuCo0js2x13jR0bKPixdG1/cxSIYG2/JpX/UI g+wn1Ufk+qMz2tjo/8Pck9M16ds8NRHqN1kdi68dSm1eru7iASvYshPmiL8OzWxw 1OVCqqlqpQSLcB70MpmJST1wj+HCeY1g3BwSezIQshw4K2O+7DRa+U8roWUe8Mjj mALYQonhEHNBODvtqnxICXSmt7FI ----- END CERTIFICATE-----
childAction	
clusterManagerType	kron
configInfo	
configIssues	
configSt	none
ctrlrVersion	5.1(1a)
description	ApicVision
dockerImage	
extMngdBy	
highPrivilege	no
isInstalledAllApics	yes

For example, the information provided in the **Apps** window in the example above shows two Apps installed, whereas the information returned from the `apPlugin` query in Visore shows three objects found for the Apps MO. Comparing the two lists of Apps, you can see that the ApicVision App is not shown in the **Apps** window in the normal APIC GUI but is displayed in the Visore output, so that means that the ApicVision App is a hidden pre-packaged App.

You can now get more information on this hidden pre-packaged App through certain fields displayed in the Visore output, such as the **pluginSt** field that shows your desired state for the App and the **operSt** field that shows the operational state for the App.

For example, you could verify that an App is up and running if you see the following for an App:

- No faults are shown for this App in the **Faults** window (**Apps** > **Faults**)

- The state in the **operSt** field is shown as `active`

- The state in the **pluginSt** field is shown as `active`

In addition, you should pick a security domain when you enable an App, and the **securityDomains** field is populated with that value when you enable an App as described below (when you set the **pluginSt** field to `active` for an instance of an apPlugin MO). Note that the plugin-handler selects `all` as the security domain for infra Apps (for Apps that are set to `infra` in the **appType** field in the apPlugin MO instance).

Because you can't view these hidden Apps in the **Apps** window in the normal APIC GUI, you are not able to perform certain actions such as opening, enabling, or deleting the hidden Apps through the APIC GUI. However, you can perform these actions on a hidden App through the REST API:

- To enable a hidden App, send a post with XML such as the following example:

```xml
<?xml version="1.0" encoding="UTF-8"?>
<!-- /api/plgnhandler/mo/.xml -->
<apPluginContr>
    <apPlugin appCtxRoot="{{vendordomain}}_{{appid}}" pluginSt="active"
securityDomains="{{security-domains}}"/>
</apPluginContr>
```

Where the `pluginSt` is `active`.

- To disable a hidden App, send a post with XML such as the following example:

```xml
<?xml version="1.0" encoding="UTF-8"?>
<!-- /api/plgnhandler/mo/.xml -->
<apPluginContr>
    <apPlugin appCtxRoot="{{vendordomain}}_{{appid}}" pluginSt="inactive"/>
</apPluginContr>
```

Where the `pluginSt` is `inactive`.

Note the following:

- The security domain is not needed when disabling a hidden App.

- To find the `appCtxRoot` value for an App for either of the posts shown above, query for instances of the apPlugin MO and use the entry in the `appCtxRoot` field in the instance of the apPlugin MO that corresponds to your App of interest.

  To get this information, log in to your APIC through ssh as an admin user and enter the `moquery -c apPlugin | grep appCtxRoot` command:

  ```
  # moquery -c apPlugin | grep appCtxRoot
  appCtxRoot              : Cisco_NIBASE
  appCtxRoot              : Cisco_ApicVision
  ```

- To delete a hidden App, send a post with XML such as the following example:

  ```
  <?xml version="1.0" encoding="UTF-8"?>
  <!-- /api/node/mo/.xml -->
  <firmwareRepo>
      <firmwareFirmware name="{{vendordomain}}_{{appid}}" deleteIt="true"/>
  </firmwareRepo>
  ```

CHAPTER 11

Upgrading or Downgrading the Software Using the REST API

You can upgrade the software using the REST API.

Upgrading or Downgrading the Cisco APIC Software Using the REST API

Procedure

Step 1   Download the Cisco APIC image into the repository.

Example:
```
POST URL: https://<ip address>/api/node/mo/uni/fabric.xml
<firmwareRepoP>
 <firmwareOSource name="APIC_Image_download" proto="http" url="http://<ip address>/<ver-no>"/>
</firmwareRepoP>
```

Step 2   Post the following policy to set the desired version for controllers:

Example:
```
POST URL: https://<ip address>/api/node/mo/uni/controller.xml
<firmwareCtrlrFwP
    version="<ver-no>"
    ignoreCompat="true">
</firmwareCtrlrFwP>
```

Step 3   Post the following policy to trigger the controller upgrade immediately:

Example:

```
POST URL : https://<ip address>/api/node/mo/uni/controller.xml
<maintCtrlrMaintP
    adminState="up" adminSt="triggered">
</maintCtrlrMaintP>
```

Upgrading or Downgrading Switches Software Using the REST API

Procedure

Step 1   Download the switch image into the repository.

Example:

```
POST URL: https://<ip address>/api/node/mo/uni/fabric.xml
<firmwareRepoP>
 <firmwareOSource name="Switch_Image_download" proto="http" url="http://<ip
address>/<ver-no>"/>
</firmwareRepoP>
```

Step 2   Post the appropriate policies to create a firmware group and a maintenance group with the necessary node IDs, depending on your software release:

- For releases prior to Release 4.0(1), post the following policies to create a firmware group that consists of your switches with node IDs 101, 102, 103, 104, and to create a maintenance group with node IDs 101, 102, 103, 104:

```
POST URL : https://<ip address>/api/node/mo/uni/fabric.xml
<fabricInst>
<firmwareFwP
    name="AllswitchesFwP"
    version="<ver-no>"
    ignoreCompat="true">
</firmwareFwP>

<firmwareFwGrp
    name="AllswitchesFwGrp" >
        <fabricNodeBlk name="Blk101"
            from_="101" to_="101">
        </fabricNodeBlk>
        <fabricNodeBlk name="Blk102"
            from_="102" to_="102">
        </fabricNodeBlk>
        <fabricNodeBlk name="Blk103"
            from_="103" to_="103">
        </fabricNodeBlk>
        <fabricNodeBlk name="Blk104"
            from_="104" to_="104">
        </fabricNodeBlk>
<firmwareRsFwgrpp
    tnFirmwareFwPName="AllswitchesFwP">
</firmwareRsFwgrpp>
</firmwareFwGrp>

<maintMaintP
```

```
        name="AllswitchesMaintP"
        runMode="pauseOnlyOnFailures" >
    </maintMaintP>

    <maintMaintGrp
        name="AllswitchesMaintGrp">
            <fabricNodeBlk name="Blk101"
                from_="101" to_="101">
            </fabricNodeBlk>
            <fabricNodeBlk name="Blk102"
                from_="102" to_="102">
            </fabricNodeBlk>
            <fabricNodeBlk name="Blk103"
                from_="103" to_="103">
            </fabricNodeBlk>
            <fabricNodeBlk name="Blk104"
                from_="104" to_="104">
            </fabricNodeBlk>
    <maintRsMgrpp
        tnMaintMaintPName="AllswitchesMaintP">
    </maintRsMgrpp>
    </maintMaintGrp>
    </fabricInst>
```

- For Release 4.0(1) and later, post the following policies to create a firmware group that consists of your switches with node IDs 101, 102, 103, 104, and to create a maintenance group with node IDs 101, 102, 103, 104:

```
POST URL : https://<ip address>/api/node/mo/uni/fabric.xml
<fabricInst>
        <maintMaintP
                version="<ver-no>"
                name="AllswitchesFwP"
                runMode="pauseOnlyOnFailures">
        </maintMaintP>
        <maintMaintGrp name="AllswitchesMaintGrp">
                <fabricNodeBlk name="Blk101" from_="101" to_="101">
                </fabricNodeBlk>
                <fabricNodeBlk name="Blk102" from_="102" to_="102">
                </fabricNodeBlk>
                <fabricNodeBlk name="Blk103" from_="103" to_="103">
                </fabricNodeBlk>
                <fabricNodeBlk name="Blk104" from_="104" to_="104">
                </fabricNodeBlk>
                <maintRsMgrpp tnMaintMaintPName="AllswitchesMaintGrp">
                </maintRsMgrpp>
        </maintMaintGrp>
</fabricInst>
```

- For Release 5.1(1) and later, post the following policies to create a firmware group that consists of your switches with node IDs 101, 102, 103, 104, and to create a maintenance group with node IDs 101, 102, 103, 104:

  - Pre-upgrade validator (APIC)

    For APIC pre-validation

    ```
    GET URL - https://<ip
    address>/mqapi2/deployment.query.json?mode=validateCtrlrMaintP&targetVersion=
    b.
    ```

    For Switch pre-validation

```
                        POST URL - https://<ip
                        address>/mqapi2/deployment.query.xml?mode=validateSwitchMaintPAsync
                        <syntheticMaintPSwitchDetails maintPName="
```

• Pre-Download Images to the Leaf and Spine Switches

```
POST URL - https://<ip address>/api/node/mo/uni/fabric.xml
                        <fabricInst>
                <maintMaintP downloadSt="triggered" name="
                </maintMaintP>
                <maintMaintGrp name="
                        <fabricNodeBlk name="blk102" from_="102" to_="102">
                        </fabricNodeBlk>
                        <maintRsMgrpp  tnMaintMaintPName="
                        </maintRsMgrpp>
                </maintMaintGrp>
        </fabricInst>
```

• Graceful Upgrade

```
POST URL - https://<ip address>/api/node/mo/uni/fabric.xml
                        <fabricInst>
                <maintMaintP downloadSt="triggered" name="
                </maintMaintP>
                <maintMaintGrp name="
                        <fabricNodeBlk name="blk102" from_="102" to_="102">
                        </fabricNodeBlk>
                        <maintRsMgrpp  tnMaintMaintPName="
                        </maintRsMgrpp>
                </maintMaintGrp>
        </fabricInst>
```

Step 3   Post the following policy to trigger the upgrade of all switches immediately:

Example:

```
POST URL : https://<ip address>/api/node/mo/uni/fabric.xml
<maintMaintP
    name="AllswitchesMaintP" adminSt="triggered">
</maintMaintP>
```

The Cisco APICs are upgraded serially so that the controller cluster is available during the upgrade.

Upgrading or Downgrading the Catalog Software Version Using the REST API

Typically, the catalog image is upgraded or downgraded when an Cisco APIC image is upgraded or downgraded. However occasionally, a catalog image must be upgraded by the administrator.

Procedure

Upgrade the catalog image.

Example:

```
http://trunk6-ifc1/api/node/mo/uni/fabric.xml
<firmwareCatFwP
    version="catalog-1.0(1e)"  ignoreCompat="yes" />
</firmwareCatFwP>
```

Verifying the Firmware Version and the Upgrade Status Using the API

Verification Description	Example URL
For the current running firmware version on controllers	GET URL: https://<ip address>/api/node/class/firmwareCtrlrRunning.xml
For the currently operating firmware version on switches	GET URL: https://<ip address>/api/node/class/firmwareRunning.xml
For the upgrade status of controllers and switches	GET URL: https://<ip address>/api/node/class/maintUpgJob.xml

Upgrade Examples

Controller Upgrade Examples

Download Cisco APIC image into repository

```
POST URL: http://trunk6-ifc1/api/node/mo/uni/fabric.xml
<firmwareRepoP>
 <firmwareOSource name="APIC_Image_download" proto="http"
url="http://172.21.158.190/aci-apic-dk9.1.0.0.72.iso"/>
</firmwareRepoP>
```

Download switch image into repository

```
POST URL: http://trunk6-ifc1/api/node/mo/uni/fabric.xml
<firmwareRepoP>
 <firmwareOSource name="Switch_Image_download" proto="http"
url="http://172.21.158.190/aci-n9000-dk9.11.0.0.775.bin"/>
</firmwareRepoP>
```

Controller Firmware Policy - set the desired version for controllers

```
POST URL: http://trunk6-ifc1/api/node/mo/uni/controller.xml
<firmwareCtrlrFwP
    version="apic-1.0(0.72)"
    ignoreCompat="true">
</firmwareCtrlrFwP>
```

Controller Maintenance Policy – trigger upgrade on controllers starting now

```
POST URL: http://trunk6-ifc1/api/node/mo/uni/controller.xml
<maintCtrlrMaintP
 adminState="up" adminSt="triggered">
</maintCtrlrMaintP>
```

Get current running version on controllers

```
(all controllers) GET URL :
http://trunk6-ifc1.insieme.local/api/node/class/firmwareCtrlrRunning.xml
(a controller) GET URL :
http://trunk6-ifc1.insieme.local/api/node/mo/topology/pod-1/node-1/sys/ctrlrfwstatuscont/ctrlrrunning.xml
```

Get upgrade status of controllers

```
(all controllers) GET URL : http://trunk6-ifc1.insieme.local/api/node/class/maintUpgJob.xml
(a controllers) GET URL :
http://trunk6-ifc1.insieme.local/api/node/mo/topology/pod-1/node-1/sys/ctrlrfwstatuscont/upgjob.xml
```

Switch Upgrade Examples

Switch Firmware Group – Group of switches with same firmware policy

```
POST URL: http://trunk6-ifc1/api/node/mo/uni/fabric.xml
<firmwareFwGrp name="AllswitchesFwGrp" >
        <fabricNodeBlk name="Blk101to104" from_="101" to_="104" />
      <firmwareRsFwgrpp tnFirmwareFwPName="AllswitchesFwP" />
</firmwareFwGrp>
```

Switch Firmware Firmware Policy – Set desired version

```
POST URL: http://trunk6-ifc1/api/node/mo/uni/fabric.xml
<firmwareFwP name="AllswitchesFwP" version="n9000-11.0(0.775)" ignoreCompat="true">
</firmwareFwP>
```

Switch Maintenance Group – Group of switches with same maintenance policy

```
POST URL: http://trunk6-ifc1/api/node/mo/uni/fabric.xml
<maintMaintGrp name="AllswitchesMaintGrp">
        <fabricNodeBlk name="Blk101to104" from_="101" to_="104" />
        <maintRsMgrpp tnMaintMaintPName="AllswitchesMaintP" />
</maintMaintGrp>
```

Switch Maintenance Policy – Setup schedule for maitenance

```
POST URL: http://trunk6-ifc1/api/node/mo/uni/fabric.xml
<maintMaintP name="AllswitchesMaintP" runMode="pauseOnlyOnFailures" >
</maintMaintP>
```

Trigger upgrade on Maintenance Group – starting now

```
POST URL: http://trunk6-ifc1/api/node/mo/uni/fabric.xml
<maintMaintP name="AllswitchesMaintP" adminSt="triggered">
</maintMaintP>
```

Get current running version on switches

```
(all switches) GET UR : http://trunk6-ifc1.insieme.local/api/node/class/firmwareRunning.xml
(a switch) GET URL:
http://trunk6-ifc1.insieme.local/api/node/mo/topology/pod-1/node-101/sys/fwstatuscont/running.xml
```

Get upgrade status of switches

```
(all switches) GET URL: http://trunk6-ifc1.insieme.local/api/node/class/maintUpgJob.xml
(a switch) GET URL:
http://trunk6-ifc1.insieme.local/api/node/mo/topology/pod-1/node-101/sys/fwstatuscont/upgjob.xml
```

C H A P T E R **12**

Upgrading or Downgrading the Software Using the CLI

You can upgrade the software using the CLI.

Note
• Ensure that you check and follow these guidelines:

  • Workflow to Upgrade or Downgrade the Cisco ACI Fabric, on page 34

  • Pre-Upgrade/Downgrade Checklists, on page 63

  • Guidelines and Limitations for Upgrading or Downgrading, on page 55

• If you create policies for upgrade through the GUI, you cannot change that same policy through the CLI, and vice versa.

Upgrading or Downgrading the Cisco APIC Software Using the NX-OS Style CLI

Procedure

Step 1 Download the image from the source into the controller.

Example:
```
admin@ifc1:~> scp <username>@<Host IP address that has the image>:/<absolute path to the
image including image file name>  .
admin@ifc1:~> pwd
/home/admin
admin@ifc1:~> ls
<ver-no>.bin
```

Step 2 Display the repository information.

Example:

```
apic1# show firmware repository
```

Step 3 Add the firmware image to the repository.

```
apic1# firmware repository add <name of the image file>
```

Example:

```
apic1# firmware repository add aci-apic-dk9.2.0.1r.iso
```

Step 4 Configure the controllers for upgrade or downgrade.

```
apic# configure
apic1(config)# firmware
apic1(config-firmware)# controller-group
apic1(config-firmware-controller)# firmware-version <name of the image file>
```

Example:

```
apic# configure
apic1(config)# firmware
apic1(config-firmware)# controller-group
apic1(config-firmware-controller)# firmware-version aci-apic-dk9.2.2.2e.bin
```

Step 5 Upgrade or downgrade the controller.

Example:

```
apic1(config-firmware-controller)# exit
apic1(config-firmware)# exit
apic1(config)# exit
apic1# firmware upgrade controller-group
```

The Cisco APICs are upgraded or downgraded serially so that the controller cluster is available during the upgrade or downgrade. The upgrade or downgrade occurs in the background.

Step 6 Verify the upgrade or downgrade for the controller.

Example:

```
apic1# show firmware upgrade status
 Pod        Node      Current-Firmware    Target-Firmware      Status
     Upgrade-Progress(%)
 ---------- --------- ------------------- -------------------- ------------------------
   --------------------
 1        1         apic-2.3(0.376a)                         success
     100
 1        2         apic-2.3(0.376a)                         success
     100
 1        3         apic-2.3(0.376a)                         success
     100
 1        101       n9000-12.3(0.102)   n9000-12.3(0.102)    success
     100
 1        102       n9000-12.3(0.102)   n9000-12.3(0.102)    success
     100
 1        103       n9000-12.3(0.100)   n9000-12.3(0.102)    upgrade in progress
     5
 1        104       n9000-12.3(0.102)   n9000-12.3(0.102)    success
     100
 1        201       n9000-12.3(0.102)   n9000-12.3(0.102)    success
     100
 1        202       n9000-12.3(0.100)   n9000-12.3(0.102)    upgrade in progress
```

```
      5
apic1#
```

Upgrading or Downgrading the Switches Using the NX-OS Style CLI

Procedure

Step 1 Download the image from the source into the controller.

Example:

```
admin@ifc1:~> scp <username>@<image_host_IP>:/<filename_and_image_absolute_path>  .
admin@ifc1:~> pwd
/home/admin
admin@ifc1:~> ls
<ver-no>.bin
```

Step 2 Display repository information.

Example:

```
apic1# show firmware repository
```

Note When you migrate to 6.0 (2) by using the CLI mode to upgrade the firmware, the maintenance group displays two target firmware versions. It displays both these images because their base version is the same. Both the firmware versions belong to the same release, where one version has the 64 bit extension and the other version does not have the 64 bit extension as shown below:

```
apic1(config-firmware-switch)# show running-config
# Command: show running-config firmware switch-group 64bit
# Time: Thu Jan 19 05:23:15 2023
  firmware
    switch-group 64bit
      switch 102
      switch 103
      switch 104
      switch 105
      switch 152
      firmware-version aci-n9000-dk9.16.0.2.bin
      firmware-version aci-n9000-dk9.16.0.2-cs_64.bin
      exit
    exit
```

The `firmware-version aci-n9000-dk9.16.0.2.bin` and `firmware-version aci-n9000-dk9.16.0.2-cs_64.bin` firmware statements in the above output shows 2 firmware versions are present even though 1 is configured.

Step 3 Add the firmware image to the repository.

```
apic1# firmware repository add <image_filename>
```

Example:

```
apic1# firmware repository add aci-apic-dk9.2.0.1r.iso
```

Step 4 Configure the switch group for upgrade.

```
apic1# configure
apic1(config)# firmware
apic1(config-firmware)# switch-group <switch_group>
apic1(config-firmware-switch)# switch <switches_to_add_to_group>
apic1(config-firmware-switch)# firmware-version <image_filename>
```

Example:

```
apic1# configure
apic1(config)# firmware
apic1(config-firmware)# switch-group group1
apic1(config-firmware-switch)# switch 101-104,201,202
apic1(config-firmware-switch)# firmware-version aci-n9000-dk9.12.2.2e.bin
```

Note You can also use the **no** argument with the **switch** command above to remove switches from the group:

Example:

```
apic1(config-firmware-switch)# no switch 203,204
```

Step 5 Specify whether to proceed to the next set of nodes if the upgrade fails on the current set of nodes.

```
apic1(config-firmware-switch)# [no] run-mode {pause-never | pause-on-failure}
```

Example:

```
apic1(config-firmware-switch)# run-mode pause-on-failure
```

Step 6 Determine if you want to assign a scheduler for the upgrade or if you want to upgrade immediately.

- If you want to assign a scheduler for the upgrade, a scheduler must exist to specify when the upgrade will be executed.

  See About Upgrading or Downgrading with the Scheduler, on page 43 for more information about the scheduler.

  To assign that existing scheduler for the upgrade:

  ```
  apic1(config-firmware-switch)# schedule <scheduler_name>
  ```

  For example:

  ```
  apic1(config-firmware-switch)# schedule myNextSunday
  ```

- If you want to upgrade immediately, return to EXEC mode and type the command **firmware upgrade switch-group**.

  Note The **firmware upgrade switch-group** command performs the upgrade immediately in this situation.

  This takes priority over any configured scheduled upgrades.

  ```
  apic1(config-firmware-switch)# exit
  apic1(config-firmware)# exit
  apic1(config)# exit
  apic1# firmware upgrade switch-group <switch_group>
  ```

  For example:

  ```
  apic1(config-firmware-switch)# exit
  apic1(config-firmware)# exit
  apic1(config)# exit
  apic1# firmware upgrade switch-group group1
  ```

Step 7   Verify the upgrade status for the switch group.

```
apic1# show firmware upgrade status switch-group <switch_group>
```

The output that is produced from this command will vary, depending on the release:

- For releases prior to Release 4.2(5), output similar to the following appears:

```
Pod   Node  Current-Firmware    Target-Firmware     Status                Upgrade-Progress(%)
---   ----  ------------------  ------------------  --------------------  --------------------
1     1     apic-2.3(0.376a)                        success               100
1     2     apic-2.3(0.376a)                        success               100
1     3     apic-2.3(0.376a)                        success               100
1     101   n9000-12.3(0.102)   n9000-12.3(0.102)   success               100
1     102   n9000-12.3(0.102)   n9000-12.3(0.102)   success               100
1     103   n9000-12.3(0.100)   n9000-12.3(0.102)   upgrade in progress   5
1     104   n9000-12.3(0.102)   n9000-12.3(0.102)   success               100
1     201   n9000-12.3(0.102)   n9000-12.3(0.102)   success               100
1     202   n9000-12.3(0.100)   n9000-12.3(0.102)   upgrade in progress   5
apic1#
```

- For Release 4.2(5) and later, output similar to the following appears, where the **Download-Status** and **Download-Progress(%)** columns are now available to provide additional information:

```
Pod   Node  Current-Firmware    Target-Firmware     Status                Upgrade-      Download-    Download-
                                                                          Progress(%)   Status       Progress(%)
----  ----  ------------------  ------------------  --------------------  -----------   ----------   -----------
1     101   n9000-15.0(0.138)   n9000-15.0(0.144)   upgrade in progress   45            downloaded   100
1     107   n9000-15.0(0.138)   n9000-15.0(0.144)   waiting in queue      0             downloaded   100
1     108   n9000-15.0(0.138)   n9000-15.0(0.144)   upgrade in progress   45            downloaded   100
1     112   n9000-15.0(0.138)   n9000-15.0(0.144)   upgrade in progress   45            downloaded   100
1     113   n9000-15.0(0.138)   n9000-15.0(0.144)   upgrade in progress   45            downloaded   100
1     121   n9000-15.0(0.138)   n9000-15.0(0.144)   upgrade in progress   45            downloaded   100
1     122   n9000-15.0(0.138)   n9000-15.0(0.144)   waiting in queue      0             downloaded   100
1     123   n9000-15.0(0.138)   n9000-15.0(0.144)   waiting in queue      0             downloaded   100
1     124   n9000-15.0(0.138)   n9000-15.0(0.144)   upgrade in progress   45            downloaded   100
1     126   n9000-15.0(0.138)   n9000-15.0(0.144)   upgrade in progress   45            downloaded   100
1     127   n9000-15.0(0.138)   n9000-15.0(0.144)   upgrade in progress   45            downloaded   100
1     128   n9000-15.0(0.138)   n9000-15.0(0.144)   upgrade in progress   45            downloaded   100
1     130   n9000-15.0(0.138)   n9000-15.0(0.144)   upgrade in progress   45            downloaded   100
2     171   n9000-15.0(0.138)   n9000-15.0(0.144)   upgrade in progress   45            downloaded   100
2     172   n9000-15.0(0.138)   n9000-15.0(0.144)   upgrade in progress   45            downloaded   100
2     173   n9000-15.0(0.138)   n9000-15.0(0.144)   upgrade in progress   45            downloaded   100
2     174   n9000-15.0(0.138)   n9000-15.0(0.144)   upgrade in progress   45            downloaded   100
2     175   n9000-15.0(0.138)   n9000-15.0(0.144)   upgrade in progress   45            downloaded   100
2     196   n9000-15.0(0.138)   n9000-15.0(0.144)   upgrade in progress   45            downloaded   100
2     197   n9000-15.0(0.138)   n9000-15.0(0.144)   upgrade in progress   45            downloaded   100
1     201   n9000-15.0(0.138)   n9000-15.0(0.144)   upgrade in progress   45            downloaded   100
2     303   n9000-15.0(0.138)   n9000-15.0(0.144)   upgrade in progress   45            downloaded   100
1     501   n9000-15.0(0.138)   n9000-15.0(0.144)   upgrade in progress   45            downloaded   100
1     502   n9000-15.0(0.138)   n9000-15.0(0.144)   waiting in queue      0             downloaded   100
1     1001  n9000-15.0(0.138)   n9000-15.0(0.144)   upgrade in progress   45            downloaded   100
1     1002  n9000-15.0(0.138)   n9000-15.0(0.144)   waiting in queue      0             downloaded   100
1     1901  n9000-15.0(0.138)   n9000-15.0(0.144)   upgrade in progress   45            downloaded   100
1     1902  n9000-15.0(0.138)   n9000-15.0(0.144)   upgrade in progress   45            downloaded   100
1     1903  n9000-15.0(0.138)   n9000-15.0(0.144)   upgrade in progress   45            downloaded   100
1     3999  n9000-15.0(0.138)   n9000-15.0(0.144)   waiting in queue      0             downloaded   100
apic1#
```

Upgrading or Downgrading the Catalog Software Version Using the NX-OS Style CLI

By default, upgrading or downgrading the controllers automatically upgrades or downgrades the catalog that corresponds to the controller version. That is, adding a controller image to the repository adds a catalog image into the repository as well.

You can also copy a separate catalog image and add that to the repository.

Procedure

Step 1   Add the catalog image to the repository.

Example:

```
apic1(config)# firmware
apic1(config-firmware)# catalog-version aci-catalog-dk9.2.2.2e.bin
```

Step 2   Verify the catalog upgrade status.

Example:

```
apic1# show catalog
Catalog-version : 2.2(2e)
apic1#
```

Troubleshooting Failures During the Upgrade and Downgrade Process

General Failure Considerations

Note Before proceeding, review the list of operations to avoid in Guidelines and Limitations for Upgrading or Downgrading, on page 55 to ensure stability of the system when troubleshooting an upgrade failure.

For ACI switch upgrades, there is one scheduler per maintenance policy. By default, when an upgrade or downgrade failure is detected, the scheduler pauses, and no more nodes in that group begin to upgrade. The scheduler expects manual intervention to debug any upgrade failures. After manual intervention is complete, you must resume the paused scheduler.

If you notice that switches are in "queued" state, then check the following:

- Is the controller cluster healthy? The APIC controller cluster needs to be healthy. If you see "waitingForClusterHealth = yes" in the API or "Waiting for Cluster Convergence" showing "Yes" in the GUI, that means the controller cluster is not healthy. And until it is healthy, switches which have not already started their upgrade will be in the "queued" state.

- Is the switch maintenance group paused? The group will be paused if any switch fails its upgrade.

- Navigate to **Admin** > **Firmware** > **History** > **Events** > **Schedulers** to check the event logs for each maintenance group. The event logs will provide more detailed information as to why the state of the upgrade is not progressing

Common Reasons for Download Failure

Some common reasons for download failure are as follows:

- Insufficient permissions for the remote server

- Directory or file not found on the remote server

- Directory full on APIC

- Request timeout / download did not complete in acceptable amount of time

- Remote server error / unknown server error

- Invalid Ack

- Username / password authentication issues

After the issue has been resolved, you can restart the download task to re-trigger the download

Verifying Cluster Convergence

As described in , the APIC controller cluster must be healthy in order to upgrade the ACI switch nodes successfully. You can verify the cluster convergence using the GUI.

Furthermore, you can monitor the progress of the cluster convergence after a scheduled maintenance. You view the **Controller Firmware** screen on the GUI, which presents you with a series of messages during the process of one cluster converging and then the next cluster. These messages are displayed in the **Status** field.

This may take a while. When all the clusters have converged successfully, you will see **No** in the **Waiting for Cluster Convergence** field of the **Controller Firmware** screen.

Verifying Scheduler Status

Verifying That the Controller Upgrade Paused

You can verify that the controller upgrade or downgrade paused using either the GUI or the REST API.

Using the GUI to Verify Whether a Controller Upgrade or Downgrade Scheduler Paused

Procedure

Step 1   On the menu bar, choose **ADMIN** > **Firmware**.

Step 2   In the **Navigation** pane, expand **Fabric Node Firmware** > **Controller Firmware**.

Step 3   If the scheduled maintenance policy is paused, you will see **Upgrade failed** in the **Status** column in the **Work** pane for the specific Cisco APIC.

When things are proceeding correctly, you see **Firmware upgrade queued, waiting for cluster convergence** in the Status column in the **Work** pane for the specific Cisco APIC.

Step 4   Identify the problem and fix this problem.

Step 5   Click the **Actions** tab, and click **Upgrade Controller Firmware Policy**.

Using the REST API to Verify Whether a Controller Upgrade or Downgrade Scheduler Paused

Procedure

Post the following API to verify that a scheduler is paused for a controller maintenance policy.

Example:

```
https://<ip address>/api/node/class/maintUpgStatus.xml
```

You will see a return similar to the following:

Example:

```
https://<ip address>/api/node/class/maintUpgStatus.xml

ConstCtrlrMaintP ==> controller group
Nowgrp ===> A switch group

<?xml version="1.0" encoding="UTF-8"?>
<imdata totalCount="2">
    <maintUpgStatus childAction="" dn="maintupgstatuscont/maintupgstatus-ConstCtrlrMaintP"
 faultDelegateKey="uni/fabric/
maintpol-ConstCtrlrMaintP" lcOwn="local" maxConcurrent="0"
modTs="2014-08-28T14:45:24.232-07:00" polName="
ConstCtrlrMaintP" runStatus="paused" status="" uid="0" waitOnClusterHealth="no"
windowName=""/>
    <maintUpgStatus childAction="" dn="maintupgstatuscont/maintupgstatus-nowgrp"
faultDelegateKey="" lcOwn="local"
maxConcurrent="0" modTs="2014-08-28T08:05:15.148-07:00" polName="nowgrp" runStatus="running"
 status="" uid="0"
waitOnClusterHealth="no" windowName=""/>
</imdata>
```

Verifying That the Switch Upgrade or Downgrade Paused

You can verify that the switches upgrade or downgrade paused using either the GUI or the REST API.

Using the GUI to Verify Whether a Switch Upgrade Scheduler Paused

Procedure

Step 1   On the menu bar, choose **ADMIN** > **Firmware**.

Step 2   In the Navigation pane, expand **Fabric Node Firmware** > **Maintenance Groups**.

Step 3	Expand the **Maintenance Groups**, and click on **All Switches**.
Step 4	In the **Work** pane, look to see if the **Scheduler Status** reads **Paused**.

> **Note** If the **Scheduler Status** reads **Running**, and the nodes in the group are proceeding in their upgrades or have completed their upgrades, the device is running and the upgrade is proceeding or has completed.

Step 5	Go and fix the device, and repeat Step 1 through Step 4.
	At this point the **Scheduler Status** will read **Running**.
Step 6	Using the **Actions** drop-down list on the top right, choose **Resume Upgrade Schedule**.
Step 7	Using the **Actions** drop-down list on the top right, choose **Upgrade Now**.

Using the REST API to Verify Whether a Switch Upgrade Scheduler Paused

Procedure

Post the following API to verify that a scheduler is paused for a switch maintenance policy.

Example:

```
https://<ip address>/api/node/class/maintUpgStatus.xml
```

You will see a return similar to the following:

Example:

```
https://<ip address>/api/node/class/maintUpgStatus.xml

ConstCtrlrMaintP ==> controller group
Nowgrp ===> A switch group

<?xml version="1.0" encoding="UTF-8"?>
<imdata totalCount="2">
    <maintUpgStatus childAction="" dn="maintupgstatuscont/maintupgstatus-ConstCtrlrMaintP"
 faultDelegateKey="uni/
fabric/maintpol-ConstCtrlrMaintP" lcOwn="local" maxConcurrent="0"
modTs="2014-08-28T14:45:24.232-07:00"
polName="ConstCtrlrMaintP" runStatus="paused" status="" uid="0" waitOnClusterHealth="no"
windowName=""/>
    <maintUpgStatus childAction="" dn="maintupgstatuscont/maintupgstatus-nowgrp"
faultDelegateKey="" lcOwn="
local" maxConcurrent="0" modTs="2014-08-28T08:05:15.148-07:00" polName="nowgrp"
runStatus="running" status=""
uid="0" waitOnClusterHealth="no" windowName=""/>
</imdata>
```

Resuming a Paused Scheduler for a Controller Maintenance Policy

You can resume the paused scheduler for a controller maintenance policy using either GUI or REST API.

Using the GUI to Resume Paused Controller Upgrade Scheduler

Procedure

Step 1	On the menu bar, choose **ADMIN** > **Firmware**.
Step 2	In the **Navigation** pane, expand **Fabric Node Firmware** > **Controller Firmware**.
Step 3	In the **Work** pane, click the **Policy** tab.
Step 4	In the **Controller Maintenance Policy** area, verify that the **Running Status** field displays **Paused**.
Step 5	Click the **Actions** tab, and click **Resume Upgrade Scheduler**.
Step 6	Click the **Actions** tab, and choose **Upgrade Controller Firmware Policy** from the drop-down list.
Step 7	Click the **Actions** tab, and choose **Apply Now** from the drop-down list.

Using the REST API to Resume Paused Controller Upgrade Scheduler

Procedure

Step 1 Post the following API to resume a paused scheduler for a controller maintenance policy.

In this example, the maintenance policy is ConstCtrlrMaintP.

Example:

```
URL: https://<ip address>/api/node/mo.xml
<maintUpgStatusCont>
<maintUpgStatus polName="ConstCtrlrMaintP" status="deleted" />
</maintUpgStatusCont>
```

Step 2 Use the REST API that you used initially to upgrade the Cisco APIC controller software.

Resuming a Paused Scheduler for a Switch Maintenance Policy

Using the GUI to Resume Paused Switch Upgrade Scheduler

Procedure

Step 1	On the menu bar, choose **ADMIN** > **Firmware**.
Step 2	In the **Navigation** pane, expand **Fabric Node Firmware** > **Maintenance Groups** > *maintenance_group_name*.
Step 3	In the **Work** pane, click the **Policy** tab.
Step 4	In the **Maintenance Policy** area, verify that the **Running Status** field displays **Paused**.
Step 5	In the **Maintenance Policy** area, verify that the **Scheduler Status** field displays **Paused** and that the **Waiting for Cluster Convergence** field displays **No**.

Step 6	Click the **Actions** tab, and click **Resume Upgrade Scheduler**.
Step 7	Click the **Actions** tab, and choose **Upgrade Now** from the drop-down list.

Using the REST API to Resume Paused Switch Upgrade Scheduler

Procedure

Step 1	Post the following API to resume a paused scheduler for a switch maintenance policy.

In this example, the maintenance policy is swmaintp.

Example:
```
URL: https://<ip address>/api/node/mo.xml
<maintUpgStatusCont>
<maintUpgStatus polName="swmaintp" status="deleted" />
</maintUpgStatusCont>
```

Step 2	Use the REST API that you used initially to upgrade the switches software.

Checking Firmware Log Files

APIC Installer Log Files

Beginning in software release 4.0, the upgrade logs (installer logs) for the APICs have been moved to a user accessible location to allow for live consumption. They can be opened or tailed to determine if the APIC upgrade is proceeding as expected. Depending on the upgrade jump, there will be either one or two log files to encompass the entire upgrade process.

The file that is always expected will have a name similar to *insieme_*_installer.log*, and for upgrades starting with 4.x there will be an additional *atom_installer.log*. In all version scenarios, the *insieme_*_installer.log* should be checked first, as this log will have a message indicating when it has invoked the atom_installer which then logs to the *atom_installer.log*.

The log files are stored in the */firmware/logs/YYYY-MM-DDTHH-MM-SS-MS* directory on each APIC, where the timestamp of the folder corresponds to the timestamp where that specific upgrade was triggered.

```
admin@apic1:logs> pwd
/firmware/logs

admin@apic1:logs> ls -l
2021-04-15T07:42:57-50
2021-05-28T10:18:33-50

admin@apic1:logs> ls -l ./2021-05-28T10:18:33-50
atom_installer.log
insieme_4x_installer.log
```

In the example above, a recent upgrade was triggered on May 28, 2021 around 10:18. The corresponding log files are contained within that directory. The individual log files can be opened with your linux file viewer of

choice for content viewing. If instead the goal is to watch the logs live to ensure an upgrade is still in-progress, issue a *tail –f insieme_zx_installer.log* to view the content as its being written to the log file in real time.

ACI Switch Installer Log Files

Any ACI switch version supports viewing the installer log file. The installer log for ACI switches is located in the `/mnt/pss` directory. You can open the file, or issue a *tail –f installer_detail.log* in order to view the current content being printed to the log file in real time.

```
leaf101# pwd
/mnt/pss

leaf101# ls -asl installer_detail.log
142 -rw-rw-rw- 1 root root 144722 Apr 29 07:58 installer_detail.log
```

Collecting Tech-Support Files

The preferred method for collecting tech-support files is using the "On-Demand TechSupport" feature. Try using this method first, as documented in the following guide: Collecting ACI show tech from APIC UI

However, if the APIC upgrade has failed, the overall health of the cluster may be degraded, meaning that the cluster status may be in a "Data Layer Partially Diverged / Data Layer Partially Degraded Leadership" state. If this is the case, it is unlikely that you will be able to collect tech-support files using the On-Demand Tech Support Policy. If this is the case, you can collect local tech-support files on each APIC node individually. This method is documented in the following guide: Collecting Local show tech from CLI of individual ACI nodes

CIMC/BIOS Settings Post-HUU upgrade

In general, an APIC should be pre-configured with the required CIMC and BIOS settings required for it to function properly as an APIC. However, there are some scenarios or actions which can result in the CIMC and BIOS settings deviating from the expected values.

Note   Performing an HUU upgrade may result in BIOS TPM Settings becoming disabled. If the APIC exhibits issues booting back into the APIC OS post-HUU, reset the APIC and validate the BIOS settings.

Expected CIMC Values

Management - Dedicated

Default admin password - password

LLDP - disabled

Expected BIOS Values

TPM – Enabled

TPM State – Owned

Validation

The CIMC of an APIC can be ssh'd into to validate these settings using the following set of commands:

```
C220-FCH1838V001# scope bios

C220-FCH1838V001 /bios # show main detail
Set-up parameters:
    Power ON Password Support: Disabled
    TPM Support: Enabled <<<<<<<<<<<<

C220-FCH1838V001# scope cimc

C220-FCH1838V001 /cimc # show network detail
Network Setting:
    ...
    NIC Mode: dedicated <<<<<<<<<<<<
    NIC Redundancy: none
    ...

C220-FCH1838V001# scope chassis

C220-FCH1838V001 /chassis # show adapter detail
PCI Slot 1:
    Product Name: UCS VIC 1225
    Product ID: UCSC-PCIE-CSC-02
    ...
    VNTAG: Disabled
    FIP: Enabled
    LLDP: Disabled <<<<<<<<<<<<
    PORT CHANNEL: N/A      <<<<<<<<<<<<   Validate for Gen 3 APICs
    Configuration Pending: no
    Cisco IMC Management Enabled: no
    ...
```

Auto Firmware Update on Discovery

Auto Firmware Update on APIC Discovery

Beginning with the Cisco Application Policy Infrastructure Controller (APIC) 6.0(2) release, when you add a new Cisco APIC to the fabric either through product a return merchandise authorization (RMA), cluster expansion, or commission, the Cisco APIC is automatically upgraded to the same release as the existing cluster. As the new Cisco APIC goes through the upgrade process, the Cisco APIC may take additional time to be upgraded and join the cluster. If the auto upgrade fails, the Cisco APIC raises a fault and you will be alerted.

Prerequisites and conditions for the automatic Cisco APIC firmware update on discovery feature:

- All the commissioned Cisco APICs in the cluster must be running the same release, which must be 6.0(2) or later.

- The Cisco APIC image of the same release as the commissioned Cisco APICs in the cluster must be available in the firmware repository of the commissioned Cisco APICs in the cluster.

- The CIMC IP address of the new Cisco APIC must be configured and reachable from the commissioned Cisco APICs in the cluster.

- You must complete using the Initial Setup Utility using the Cisco APIC console that sets the fabric name, Cisco APIC ID and so on, on the new Cisco APIC if the new Cisco APIC is running a release earlier than 6.0(2). If the new Cisco APIC is also running release 6.0(2) or later, you do not no need to use the Initial Setup Utility.

- Auto firmware update on APIC discovery is supported only on Cisco APIC release 4.2(1) and later.

Auto Firmware Update on Switch Discovery

When you enable Auto Firmware Update on Switch Discovery, the Cisco Application Policy Infrastructure Controller (APIC) automatically updates the firmware of the new switch in the following scenarios:

- A new switch discovery with a new node ID

- A switch replacement with an existing node ID

- An initialization and rediscovering of an existing node

Prior to Cisco APIC release 5.1(1), this feature was named **Enforce Bootscript Version Validation** and was located at **Admin > Firmware > Infrastructure > Nodes**. In release 5.1(1), the feature is renamed and moved to its current location.

Procedure

Step 1	On the menu bar, navigate to **Fabric > Inventory > Fabric Membership > Auto Firmware Update**.
Step 2	Check the **Auto Firmware Update on Switch Discovery** checkbox to enable the feature.
Step 3	Select the target firmware version for updating new switches in the **Default Firmware Version** drop-down list.

> **Note** If the node ID of the new switch is part of a firmware update group under **Admin > Firmware**, such as a replacement scenario, the new switch is updated to the target version specified by the update group. Otherwise, it's updated to the default firmware version specified in this procedure.
>
> When the selected **Default Firmware Version** is "any," this feature will not update the firmware of a new switch that has an ID that is not part of a firmware update group. A new switch that has a node ID that is part of a firmware update group will be updated to the target version specified by the update group.

Step 4	Click **Submit**.

Auto Firmware Update on Switch Discovery Limitations

The following limitation applies to auto firmware update on switch discovery:

- Auto firmware update on switch discovery is not supported when the target switch release is 16.0(3) or later while the current release running on the switch is 15.2(7) or earlier or 16.0(1) or 16.0(2). If auto firmware update on switch discovery was attempted under this condition, the switch may get stuck indefinitely. To add the switch into the fabric from that state, you must perform a clean reboot after you disable auto firmware update on switch discovery on the Cisco Application Policy Infrastructure Controller (APIC).

Managing FPGA/EPLD/BIOS Firmware

About Managing FPGA/EPLD/BIOS Firmware

Cisco switches contain several programmable logical devices (PLDs) that provide hardware functionalities in all modules. PLDs include electronic programmable logic devices (EPLDs) and field programmable gate arrays (FPGAs). Cisco provides periodic PLD image upgrades to enhance hardware functionality or to resolve known issues.

In Cisco ACI, there is no need for you to manually manage FPGA/EPLD/BIOS firmware individually or explicitly. Instead, when ACI switches are managed by APICs and the regular firmware upgrade is performed for switches through the APICs, the appropriate FPGA/EPLD/BIOS firmware that is included in the ACI switch image itself (such as aci-n9000-dk9.14.2.1i.bin) will be automatically applied.

However, when a switch boots up with an ACI switch image without going through the upgrade triggered through the APICs, the FPGA/EPLD/BIOS firmware running in the ACI switch will not be upgraded with the appropriate versions from the ACI switch image. This may result in a mismatched FPGA/EPLD/BIOS version. This may occur on a switch if you received it through a new order, Product Returns & Replacements (RMA), or when you convert the switch from standalone NX-OS software to ACI switch software.

Prior to Cisco APIC release 5.2(1) and ACI switch release 15.2(1), at such times, you had to downgrade the switch once and then perform the upgrade to the desired version through the APICs in order to upgrade FPGA/EPLD/BIOS versions to the appropriate ones.

Starting from Cisco APIC release 5.2(1) and ACI switch release 15.2(1), ACI switches will automatically upgrade the FPGA/EPLD/BIOS based on the booting ACI switch image during a normal boot up sequence for the following components, even if it's not an upgrade operation performed through the APICs:

- **Leaf switches and box-type spine switches**: EPLD/FPGA/BIOS is automatically upgraded on the switch itself

- **Modular-type spine switches**: EPLD/FPGA/BIOS is automatically upgraded on these components:

  - Supervisor module

  - Linecard module

  - Fabric module

When one of the supported components listed above boots up, the system automatically performs the following actions to determine if the EPLD/FPGA/BIOS image is in sync with the Cisco ACI or NX-OS image:

1. The system compares the BIOS versions and performs an upgrade at the BIOS level if it finds that the images are out of sync.

2. The system compares the EPLD/FPGA versions and performs an upgrade at the EPLD/FPGA level if it finds that the images are out of sync.

3. If the system has to perform an upgrade at any of the levels (at the BIOS level or at the EPLD/FPGA level), the system then performs a power cycle on that component (the switch, supervisor module, linecard module, or fabric module).

These automatic FPGA/EPLD/BIOS upgrades during a normal boot up sequence is performed per component. For instance, when a new linecard module is inserted and boots up with the base ACI switch image downloaded from the supervisor module, only the new linecard module is power-cycled to apply the FPGA/EPLD/BIOS from the base ACI switch image. Other modules will not be impacted.

Guidelines and Restrictions When Managing FPGA/EPLD/BIOS Firmware

- Note the following component-specific considerations:

  - **For supervisor modules**: Because ACI switches operate in cold-standby, when the active supervisor module is reloaded, the entire box is reloaded. Therefore, when the FPGA/EPLD/BIOS upgrade during a normal boot up sequence is required for both active and standby supervisor modules or only for the active module, a power cycle will be performed on both the active and the standby supervisor module at the same time. If the FPGA/EPLD/BIOS upgrade is required only on the standby module, a power cycle will be performed only on the standby module and the active module will remain up and running.

  - **For system controllers**: The FPGA/EPLD/BIOS on the system controllers (SCs) on modular switches are not upgraded during the normal boot up sequence. If the EPLD/FPGA/BIOS version on the system controllers does not match with the base ACI switch image, you still need to perform an upgrade of the switch itself through the APICs.

- There are known Memory Technology Device (MTD) intermittent mount issues, where the automatic FPGA/EPLD/BIOS upgrades are not triggered on some linecard modules and fabric modules on certain MTD-based boards. If the Embedded MultiMediaCard (EMMC) or MTD has gone bad, the automatic FPGA/EPLD/BIOS upgrades will not get triggered.

- Entering the command `show system reset-reason` at the upper board level provides information on the reason for the reset when the automatic FPGA/EPLD/BIOS upgrades are triggered. However, entering the command at the linecard or fabric module level (for example, `show system reset-reason module 3`) does not produce any information.

C H A P T E R **16**

Silent Roll Package Upgrade

About the Silent Roll Package Upgrade or Downgrade

Cisco APIC release 4.1(2) introduces the silent roll package upgrade (SR upgrade) feature. An SR upgrade enables you to manually perform an internal package upgrade for ACI switch hardware SDK, drivers, and so on, without upgrading the entire ACI switch software OS. Typically, you do not need to perform an SR upgrade because upgrading the ACI switch software OS takes care of internal packages as well.

As of Cisco APIC release 4.1(2), the SR upgrade feature supports the following two switches:

- N9K-C93216TC-FX2

- N9K-C93360YC-FX2

Configuring a Silent Roll Package Upgrade or Downgrade Using the Cisco APIC GUI

Before you begin

- Wait until all the controllers are upgraded to the new firmware version before proceeding to upgrade or downgrade the switch firmware.

- Download a SR package (ex. aci-srpkg-dk9.1.0.0.bin) to use for the SR package upgrade, if necessary, using the procedures provided in Downloading APIC and Switch Images on APICs, on page 79.

- Review the information in Workflow to Upgrade or Downgrade the Cisco ACI Fabric, on page 34 for the recommended steps for a successful upgrade with minimum disruption.

Procedure

Step 1   Verify that all the controllers are upgraded to the new firmware version before proceeding.
Do not upgrade the switch firmware until all the controllers are upgraded to the new firmware version first.

Step 2   On the menu bar, choose **Admin** > **Firmware**.

Step 3   From the Work pane, click **Infrastructure** > **Nodes**.

Step 4   Click **Actions**, choose **Schedule Node Upgrade**, and perform the following actions:

a) In the **Group Type** field, choose **Switch**.

b) In the **Upgrade Group** field, choose either **Existing** or **New**, if this field is available.

- **Existing**—Enables you to schedule the node upgrade on an existing upgrade group.

- **New**—Enables you to create a new upgrade group.

c) In the **Upgrade Group Name** field, either choose an existing upgrade group using the options provided in the drop-down menu, or enter a name to create a new upgrade group.

For releases prior to 4.1(2), to create a new upgrade group, click the **x** in the corner of the field to clear out the field then enter a name for the new upgrade group.

Note that if you choose an existing POD maintenance group, fields associated with that maintenance group are automatically filled in.

d) Click to place a check mark in the **Manual Silent Roll Package Upgrade** check box.

Note   When **Manual Silent Roll Package Upgrade** is chosen:

- The **Silent Roll Package Version** drop-down list appears with a list of SR upgrade package versions.

- The following fields are disabled:

- **Target Firmware Version**

- **Ignore Compatibility Check**

- **Graceful Maintenance**

e) Click the **Silent Roll Package Version** drop-down list to choose the package for the SR package upgrade.

f) In the **Run Mode** field, choose the run mode to proceed automatically to the next set of nodes once the set of nodes has gone through the maintenance process successfully.

The options are:

- **Do not pause on failure and do not wait on cluster health**

- **Pause only Upon Upgrade Failure**

The default is **Pause only Upon Upgrade Failure**.

g) In the **Upgrade Start Time** field, select either **Now** or **Schedule for Later**.

If you select **Schedule for Later**, select the trigger value using the Scheduler scroll-down menu.

h) Click the plus icon at the right of the **All Nodes** table.

The **Add Nodes to Upgrade Group** page appears.

i) In the **Add Nodes to Upgrade Group** page , choose one of the following:

  • **Range**—Enter the range in the **Group Node Ids** field.

  • **Manual**—When chosen, a list of available leaf switches and spine switches appears in the All Nodes area. Select the nodes that you want to include in this upgrade.

    Note that the nodes displayed are physical leaf switches and spine switches.

j) Click **Submit**.

Step 5   To remove nodes from the upgrade group:

a) Choose the nodes in the table that you want to remove from the upgrade group.
b) Click the trashcan icon at the right of the **All Nodes** table.
c) Click **Submit**.

Configuring a Silent Roll Package Upgrade or Downgrade Using the CLI

This section demonstrates how to configure and unconfigure an SR package upgrade or downgrade and how to trigger the upgrade or downgrade after configuring the SR package upgrade or downgrade and SR package version using the CLI.

For more information about SR package upgrades or downgrades, see About the Silent Roll Package Upgrade or Downgrade , on page 133.

Procedure

Step 1   To configure the SR package upgrade:

```
Switch# configure
Switch(config)# firmware
Switch(config-firmware)# switch-group new
Switch(config-firmware-switch)# sr-version aci-srpkg-dk9.1.0.0.bin
Switch(config-firmware-switch)# sr-upgrade
Switch(config-firmware-switch)# show running-config
# Command: show running-config firmware switch-group new
# Time: Wed Mar 13 15:55:59 2019
  firmware
    switch-group new
      sr-version aci-srpkg-dk9.1.0.0.bin
      sr-upgrade
      exit
    exit
```

Step 2   To unconfigure the SR package upgrade:

```
Switch# configure
Switch(config)# firmware
Switch(config-firmware)# switch-group new
Switch(config-firmware-switch)# no sr-upgrade
Switch(config-firmware-switch)# show running-config
# Command: show running-config firmware switch-group new
# Time: Wed Mar 13 16:17:01 2019
  firmware
    switch-group new
      sr-version aci-srpkg-dk9.1.0.0.bin
      exit
    exit
```

Step 3   To trigger the upgrade after configuring the SR package version and SR package upgrade:

Note   When the SR package upgrade is configured, the SR package version should not be empty for triggering the upgrade. And if the SR package upgrade is not configured, the firmware version (switch version) should not be empty.

```
Switch# firmware upgrade switch-group new
```

Configuring a Silent Roll Package Upgrade or Downgrade Using the REST API

This section demonstrates how to configure an SR package upgrade or downgrade using the REST API.

For more information about SR package upgrades, see About the Silent Roll Package Upgrade or Downgrade , on page 133.

Procedure

To configure the SR package upgrade:

```
<fabricInst>
            <maintMaintP
            srVersion="srpkg-1.0(1)"
            srUpgrade="yes"
            name="m1"
            runMode="pauseOnlyOnFailures">
            </maintMaintP>
            <maintMaintGrp name="m1">
          <fabricNodeBlk name="Blk101"
          from_="101" to_="101">
          </fabricNodeBlk>
            <maintRsMgrpp
            tnMaintMaintPName="m1">
            </maintRsMgrpp>
            </maintMaintGrp>
</fabricInst>
```

Software Maintenance Upgrade Patches

About Software Maintenance Upgrade Patches

Beginning with the Cisco Application Policy Infrastructure Controller (APIC) release 5.2(1), you can install software maintenance upgrade (SMU) patches that contain fixes for specific defects. Because SMU patches can be released much more quickly than a more traditional patch release, you can resolve specific issues in a more timely manner. SMU patches are available for download from Cisco.com and generally include the ID number of the resolved defect in the filename to enable you to identify easily which issue the patch will resolve. SMU patches do not include new features.

SMU patches are available for the Cisco APIC and Cisco ACI-mode switches. When patching a Cisco APIC, the patch gets installed on all Cisco APICs in the cluster, and the Cisco APICs are automatically rebooted to complete the patch installation. When patching a switch, the switch must also be rebooted to complete the installation, but you can delay the reboot until after you have initiated the installation of multiple SMU patches.

If necessary, you can uninstall an SMU patch. As with patch installation, the Cisco APIC or switch must be rebooted to complete the uninstallation.

Guidelines and Limitations for Software Maintenance Upgrade Patches

The following guidelines and limitations apply for software maintenance upgrade (SMU) patches:

- The **Graceful Upgrade** feature is not supported for SMU patch installation and uninstallation.

- The **Auto Firmware Update on Switch Discovery** feature is not performed for switches that belong to an update group for SMU patch installation or uninstallation.

- In releases earlier than 5.2(8) and in the 6.0(1) and 6.0(2) releases, an SMU patch cannot modify the Cisco Application Policy Infrastructure Controller (APIC) GUI. Beginning with the 5.2(8) and 6.0(3) releases, an SMU patch can modify the Cisco APIC GUI.

- Upgrading or downgrading the software on a switch removes any SMU patches that you previously installed on that switch.

Installing a Cisco APIC Software Maintenance Upgrade Patch Using the GUI

In the Cisco Application Policy Infrastructure Controller (APIC) 5.2(1) release or later, you can use the following procedure to install a software maintenance upgrade (SMU) patch on a Cisco Application Policy Infrastructure Controller (APIC).

Procedure

Step 1   Add the firmware image that corresponds to the SMU patch to the Cisco APIC. The patch will be listed along with any other firmware images (SMU patches and otherwise).

For the procedure, see Upgrading or Downgrading with APIC Release 5.1 or Later Using the GUI, on page 89.

Step 2   Set up a controller firmware update. On the **Version Selection** screen, for the **Update Type**, choose **Software Maintenance Upgrade (Install)**, then choose the SMU patch in the **Select Firmware** section.

For the procedure, see Upgrading or Downgrading with APIC Release 5.1 or Later Using the GUI, on page 89.

Installing a Switch Software Maintenance Upgrade Patch Using the GUI

In the Cisco Application Policy Infrastructure Controller (APIC) 5.2(1) release or later, you can use the following procedure to install a software maintenance upgrade (SMU) patch on a Cisco Application Centric Infrastructure (ACI)-mode switch.

SMU patch installation or uninstallation uses the same update group as a regular firmware upgrade. Because one node can belong to only one update group, when you apply a SMU patch to a specific node, remove that node from the existing group and create a new group that is dedicated for the node so that other nodes are not impacted. In the future when you must perform a regular firmware upgrade for the entire fabric, you can delete the dedicated update group that is used for the SMU patch installation and add the node back to one of the original groups. If all the nodes in the existing group need the SMU patch, you can simply reuse the same update group without creating a new update group.

Procedure

Step 1 Add the firmware image that corresponds to the SMU patch to the Cisco Application Policy Infrastructure Controller (APIC). The Cisco APIC lists the patch along with any other firmware images (SMU patches and otherwise).

In the Cisco APIC release 6.0(2) and later, download both the 32-bit and 64-bit SMU images to the Cisco APIC. Downloading only one of the images may result in errors during the upgrade process.

For the procedure, see .

Step 2 Set up a node firmware update. On the **Version Selection** screen, for the **Update Type**, choose **Software Maintenance Upgrade (Install)**, then choose the SMU patch in the **Select Firmware** section.

For the procedure, see .

After you click **Begin Download** in the **Confirmation** screen, the patch gets downloaded to the selected switches. The **Firmware Updates** tab in the Work pane displays.

Step 3 In the Work pane, click the upgrade group that you created.

The **Node Firmware Update** dialog displays with information for the upgrade group.

Step 4 When the status for the switches is `Ready to Install`, click **Actions**.

Before the 6.0(2) release, or if the **Switch Restart Type** property is set to **Reload** in the 6.0(2) release and later, choose one of the following actions:

- **Install and Reload**: The switches reboot after the SMU patch gets installed. Choose this action if you want to install only one SMU patch, or if you are installing the final patch of multiple patches.

- **Install and Skip Reload**: The switches do not reboot after the SMU patch gets installed. Choose this action if you want to install multiple SMU patches and this patch is not the final patch. In this case, repeat this entire procedure for each additional patch and continue to choose **Install and Skip Reload** until you install the final patch. For the final patch, choose **Install and Reload**. Optionally, you can choose **Install and Skip Reload** and manually reboot the switch after the patch gets installed.

In the 6.0(2) release and later and if the **Switch Restart Type** property is set to **Restart**, choose **Install**. For SMUs that you can apply to a switch without rebooting the switch, after choosing **Install**, the SMU will be installed while the switch remains operational. Whether or not the SMU installation impacts the traffic going through the switch depends on the fixes that the SMU applies.

Uninstalling a Cisco APIC Software Maintenance Upgrade Patch Using the GUI

In the Cisco Application Policy Infrastructure Controller (APIC) 5.2(1) release or later, you can use the following procedure to uninstall a software maintenance upgrade (SMU) patch from a Cisco APIC.

Procedure

Set up a controller firmware update. On the **Version Selection** screen, for the **Update Type**, choose **Software Maintenance Upgrade (Uninstall)**, then choose the SMU patch to uninstall in the **Select Firmware** section.

For the procedure, see Upgrading or Downgrading with APIC Release 5.1 or Later Using the GUI, on page 89. Even though the procedure is intended for upgrading, uninstalling the patch uses the same steps, except as specified here.

Uninstalling a Switch Software Maintenance Upgrade Patch Using the GUI

In the Cisco Application Policy Infrastructure Controller (APIC) 5.2(1) release or later, you can use the following procedure to uninstall a software maintenance upgrade (SMU) patch from a Cisco Application Centric Infrastructure (ACI)-mode switch. The process for uninstalling includes creating an upgrade group and using that group to uninstall the SMU patch.

SMU patch installation or uninstallation uses the same update group as a regular firmware upgrade. Because one node can belong to only one update group, when you apply a SMU patch to a specific node, remove that node from the existing group and create a new group dedicated for the node so that other nodes are not impacted. In the future when you need to perform a regular firmware upgrade for the entire fabric, you can delete the dedicated update group used for the SMU patch installation and add the node back to one of the original groups. If all the nodes in the existing group need the SMU patch, you can simply reuse the same update group without creating a new update group.

Procedure

Step 1 Set up a node firmware update. On the **Version Selection** screen, for the **Update Type**, choose **Software Maintenance Upgrade (Uninstall)**, then choose the SMU patch to uninstall in the **Select Firmware** section.

For the procedure, see Upgrading or Downgrading with APIC Release 5.1 or Later Using the GUI, on page 89. Even though you are uninstalling the patch, the procedure is almost the same as the upgrade procedure.

When you get to the **Confirmation** screen, continue with the next step.

Step 2 If the information that displays is correct, then click **Uninstall and Skip Reload** or **Begin Uninstall**. Otherwise, return to any of the previous screens and change the configuration as appropriate.

- **Uninstall and Skip Reload**: The switches are not rebooted after the SMU patch gets uninstalled. Choose this action if you want to uninstall multiple SMU patches and this patch is not the final patch. In this case, repeat this entire procedure for each additional patch and continue to choose **Uninstall and Skip Reload** until you are uninstalling the final patch. For the final patch, choose **Begin Uninstall**. Optionally, you can choose this action and manually reboot the switch after the final patch gets uninstalled.

- **Begin Uninstall**: The switches are rebooted after the SMU patch gets uninstalled. Choose this action if you want to uninstall only one SMU patch, or if you are uninstalling the final patch of multiple patches.

Installing or Uninstalling a Cisco APIC Software Maintenance Upgrade Patch Using the REST API

The following example REST API XML installs a software maintenance upgrade (SMU) patch on a Cisco Application Policy Infrastructure Controller (APIC) and reboots the Cisco APIC after the installation completes:

```
<polUni>
    <ctrlrInst>
        <firmwareCtrlrFwP
          version="apicpatch-CSCab12345-9.0.0-5.2.0.155d.x86_64">
        </firmwareCtrlrFwP>
        <maintCtrlrMaintP
          adminState="up" smuOperation="smuInstall" adminSt="triggered" >
        </maintCtrlrMaintP>
    </ctrlrInst>
</polUni>
```

The following table explains the elements and parameters that are specific to SMU patches:

Element	Parameter	Descripiton
`firmwareCtrlrFwP`	`version`	Specifies the filename of the SMU patch.
`maintCtrlrMaintP`	`smuOperation`	Specifies whether to install or uninstall the patch. The possible values are: • `smuInstall`: Install the patch. • `smuUninstall`: Uninstall the patch.

Installing or Uninstalling a Switch Software Maintenance Upgrade Patch Using the REST API

The following example REST API XML installs a software maintenance upgrade (SMU) patch on a switch and reboots the switch after the installation completes:

```
<polUni>
    <fabricInst>
        <maintMaintP
          version="n9000-patch-CSCsysinfo12-15.2.0.151-S1.1.1.x86_64"
          smuOperation="smuInstall"
          smuOperationFlags="smuReloadImmediate"
          name="Leaf202"
```

```
            adminSt="triggered">
        </maintMaintP>

        <maintMaintGrp name="Leaf202">
            <fabricNodeBlk name="blk202" from_="202" to_="202">
            </fabricNodeBlk>
            <maintRsMgrpp tnMaintMaintPName="Leaf202">
            </maintRsMgrpp>
        </maintMaintGrp>
    </fabricInst>
</polUni>
```

The following table explains the elements and parameters that are specific to SMU patches:

Element	Parameter	Descripiton
maintMaintP	version	Specifies the filename of the SMU patch.
maintMaintP	smuOperation	Specifies whether to install or uninstall the patch. The possible values are: • smuInstall: Install the patch. • smuUninstall: Uninstall the patch.

Element	Parameter	Descripiton
`maintMaintP`	`smuOperationFlags`	Specifies whether to reboot the switch after the patch is installed. The possible values are: • `smuReloadImmediate`: The switches are rebooted after the SMU patch gets installed. Specify this value if you want to install only one SMU patch, or if you are installing the final patch of multiple patches. • `smuReloadSkip`: The switches are not rebooted after the SMU patch gets installed. Specify this value if you want to install multiple SMU patches and this patch is not the final patch. In this case, post the appropriate XML for each additional patch and continue to specify `smuReloadSkip` until you are installing the final patch. For the final patch, specify `smuReloadImmediate`. Optionally, you can specify `smuReloadSkip` and manually reboot the switch after the patch gets installed.
`maintMaintP`	`name`	Specifies the name of the maintenance group.
`fabricNodeBlk`	`from_` and `to_`	Specifies the range of switch node IDs on which to install or from which to uninstall the patch.
`maintRsMgrpp`	`tnMaintMaintPName`	Specifies the name of the maintenance group. The value must match the value of the `name` parameter of the `maintMaintP` element.

By changing some of the parameter values as specified in the table, you can specify whether to install or uninstall a patch, and you can specify not to reboot the switches after a patch is installed or uninstalled.

Upgrading the Switch Hardware

Introduction

When upgrading a switch hardware in the ACI fabric, there are multiple scenarios to consider:

- **Scenario 1** - Upgrade the hardware of spine switches.

- **Scenario 2** - Upgrade the hardware of leaf switches without vPC.

- **Scenario 3** - Upgrade the hardware of leaf switches with vPC.

Each scenario has two variations depending on the supported software versions of the old and new switch hardware.

Variation 1 - Old and new switches can run the same ACI software version.

Variation 2 - Old and new switches cannot run the same ACI software versions.

Whenever possible, it is recommended to run the same software version on both old and new switches (Variation 1). Variation 2 is for a specific situation when the old switch hardware is no longer supported by the software versions that support the new switch hardware.

An Example of Variation 2 - Old and new switches cannot run the same ACI software versions

As mentioned above, Variation 2 is for specific situations when the old switch hardware is no longer supported by the software versions that support the new switch hardware.

The most common scenario is when migrating from the first-generation Cisco Nexus 9000 series switches to newer generation Cisco Nexus 9000 series switches. The first-generation switches are no longer supported starting on Cisco ACI switch software 15.0(1) or later releases while some of the newer generation switches are supported only from 15.0(1) or later.

Note

- The first-generation Cisco Nexus 9000 switches are equipped with Cisco Application Leaf Engine (ALE) ASICs. The product ID of those switches do not contain -EX, -FX or -GX. Examples are N9K-C9372PX, N9K-C9372PX-E and so on.

- The newer generation Cisco Nexus 9000 Switches are equipped with Cisco Cloud Scale ASICs. The product ID of those switches have the -EX, -FX, -GX or later suffix. Examples are N9K-C93180YC-EX, N9K-C93180YC-FX, N9K-C93180YC-FX3 and so on.

General Guidelines

- To determine which transceivers, adapters, and cables support this switch, see the Cisco Transceiver Modules Compatibility Information document.

- To see the transceiver specifications and installation information, see Transceiver Module Installation Guides.

- Due to potential traffic loss, it is recommended that you perform the hardware replacement during a maintenance window.

- It is recommended to move any Cisco Application Policy Infrastructure Controllers (APICs) that are connected to the switches that you are replacing to any other switches in the fabric and wait for the Cisco APIC cluster to become "Fully Fit".

- When the Auto Firmware Update feature is used, make sure to set the Default Firmware Version to your target version. If the node ID is part of an upgrade group, make sure that the upgrade group is set with your target version, or delete the upgrade group. See Auto Firmware Update for details.

- The number of ports and port types of the new switches must match the old switch that you are replacing. If the number does not match, then you must change the configuration to accommodate the new ports or port types.

Spine Switches

Old and New Switches Cannot Run the Same ACI Software Version

1. Upgrade the APIC cluster to the software version that can run the new switch hardware.

2. Upgrade switches that are not to be replaced to the same version as the APIC cluster.

3. Follow the same procedure as RMA with the existing switch running the old version and the new switch running the new version.

   See "Procedures and verification" in "Troubleshoot ACI Fabric Discovery - Device Replacement" for details.

Old and New Switches Can Run the Same ACI Software Version

The procedure is the same as Return Material Authorization (RMA).

See "Procedures and verification" in "Troubleshoot ACI Fabric Discovery - Device Replacement" for details.

Leaf Switches Without vPC

Old and New Switches Cannot Run the Same ACI Software Version

Same as Spine Switches above.

Old and New Switches Can Run the Same ACI Software Version

Same as Spine Switches above.

Leaf Switches with vPC

As documented in Cisco APIC Layer 2 Networking Configuration Guide, mixing a first-generation switch and newer generation switch in the same vPC pair is not supported. However, it is supported temporarily during the migration with a limitation where the secondary vPC switch will keep its vPC legs down.

Old and New Switches Cannot Run the Same ACI Software Version

Before you begin

Complete the following steps:

- The Auto Firmware Update policy must be disabled.

- Upgrade the Cisco APIC cluster to the 4.2(7v) release if the cluster is running an older release. Also upgrade all the switches to the 14.2(7v) release. Wait for the fabric to converge.

- Upgrade the Cisco APIC cluster to 5.2(7f) release and wait for the cluster to become "Fully Fit."

- Upgrade switches that are not to be replaced to 15.2(7f).

- Ensure that the new switches are preloaded and running the equivalent release as the Cisco APICs, that is 15.2(7f) release. Other than source and target version software releases 4.2(7v)/14.2(7v) and 5.2(7f)/15.2(7f), no other software releases are supported for this migration procedure.

Note The procedure below is not supported when the minimum software version requirement for the new switches is newer than 15.2(7f). In such a case, you need to remove both of the old switches in the vPC pair at once, and add the new switches in one shot.

Procedure

Step 1 From the Cisco APIC GUI, perform the **Remove From Controller** operation for the operational secondary vPC switch node.

The Cisco APIC clean reboots the switch. Wait for about 10 minutes for this operation to finish. This action prompts all traffic to use the other first generation switch for data traffic.

Note There will be a loss of traffic for a few seconds for the operational secondary vPC when you perform the **Remove From Controller** operation.

Step 2 Disconnect the cabling from the first generation switch that you just removed.

Step 3 Uninstall the old switch by reversing the order of the steps in the "Installing the Switch Chassis" section of the switch-specific *Hardware Installation Guide*

Step 4 Install the new switch by following the steps in the "Installing the Switch Chassis" section of the switch-specific *Hardware Installation Guide*.

Step 5 Connect the loose cabling that you removed from the old switch to the same ports on the new switch.

Step 6 Register the new second generation switch with the Cisco APIC.

Register the new node with the same node name and node ID. This switch becomes part of the fabric. The Cisco APIC pushes the policies to the new switch and keeps down the vPC legs because there is a mismatch of the generation of switches. At this point, the vPC primary continues to send the data traffic.

Step 7 Before you proceed to Step 8, on page 148, wait for 10 to 15 minutes for the new switch to download the configurations.

Step 8 From the Cisco APIC GUI, perform the **Remove From Controller** operation for the vPC primary. The Cisco APIC clean reboots the switch.

Wait for about 10 minutes for this operation to finish. The vPC leg on the new switch, which the Cisco APIC kept down earlier, comes up. This action prompts all traffic to move to the new switch. The vPC ports on the new switch can take a few minutes to come up, during which time there will be traffic drops. The duration of traffic drops varies by the scale and flows in the fabric.

Step 9 Disconnect the cabling from the first generation switch.

Step 10 Uninstall the first generation switch as you did in Step 3, on page 148.

Step 11 Install the second generation switch as you did in Step 4, on page 148.

Step 12 Connect the loose cabling as you did in Step 5, on page 148.

Step 13 Register the new second generation switch with the Cisco APIC.

Register the new node with the same node name and node ID. This switch becomes part of the fabric. The Cisco APIC pushes policies to the new switch and the vPC legs comes up and starts passing traffic.

Old and New Switches Can Run the Same ACI Software Version

Follow the same steps as the Old and new switches cannot run the same ACI software version section of "Leaf Switches with vPC" below. It is the same procedure without the additional requirements such as specific source and target version requirements mentioned in Before you begin section in the Old and new switches cannot run the same ACI software version section.