The specifications and information regarding the products in this manual are subject to change without notice. All statements, information, and recommendations in this manual are believed to be accurate but are presented without warranty of any kind, express or implied. Users must take full responsibility for their application of any products.

The software license and limited warranty for the accompanying product are set forth in the information packet that shipped with the product and are incorporated herein by this reference. If you are unable to locate the software license or limited warranty, contact your Cisco representative for a copy.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

Notwithstanding any other warranty herein, all document files and software of these suppliers are provided “as is” with all faults. Cisco and the above-named suppliers disclaim all warranties, expressed or implied, including, without limitation, those of merchantability, fitness for a particular purpose and noninfringement or arising from a course of dealing, usage, or trade practice.

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 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.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

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

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)

© 2016–2019 Cisco Systems, Inc. All rights reserved.
CONTENTS

PREFACE
Preface vii
  Audience vii
  Document Conventions vii
  Related Documentation ix
  Documentation Feedback x
  Obtaining Documentation and Submitting a Service Request x

CHAPTER 1
New and Changed Information 1
  New and Changed Information 1

CHAPTER 2
Installing or Recovering Cisco APIC Images 3
  Installation Notes 3
  Usage Guidelines 5
  Conditions for Recovering or Installing Cisco APIC Software Image 7
  Installing Cisco APIC Software Using a PXE Server 8
  Installing Cisco APIC Software Using Virtual Media 9
    Installing Software Using Virtual Media (Releases Prior to Release 4.x) 9
    Installing Cisco APIC Software Using Virtual Media 9
    Installing Cisco APIC Software Using Virtual Media Through KVM Console 9
    Installing Software Using Virtual Media (Release 4.x and Later) 10
    Installing Cisco APIC Software Using CIMC Virtual Media 10
  Cleanly Installing a Single Cisco APIC Using the Debug CLI 12
  Cleanly Installing the Entire Cisco APIC Cluster and Clean the Cisco ACI Fabric Using the Debug CLI 13
  Statefully Installing a Cisco APIC Cluster Using the Debug CLI 14
Contents

CHAPTER 3 Upgrading and Downgrading the Cisco APIC and Switch Software

   About Firmware Management 15
   Firmware Upgrade Modes 17
   Workflow to Upgrade or Downgrade the Cisco ACI Fabric 19
   About Upgrading the Cisco APIC and the Switch Software 21
   Supported Upgrade Paths for the Cisco APIC and Switch Software 23
   Cisco APIC Long-Lived Release 23
   About Downgrading the Cisco APIC and Switch Software 24
   Stateless Downgrade Procedure 25
   Supported Downgrade Paths for the Cisco APIC and Switch Software 26
   About Upgrading with the Scheduler 26
   About Disabling LLDP Back to Back Connections Before Upgrading 27
   Upgrading the Software Using the GUI (Releases Prior to Release 4.x) 27
      Upgrading the Cisco APIC Software Version Using the GUI (Releases Prior to Release 4.x) 27
      Upgrading the Leaf and Spine Switch Software Version Using the GUI (Releases Prior to Release 4.x) 29
      Upgrading the Catalog Software Version Using the GUI (Releases Prior to Release 4.x) 31
   Changing the Ignore Compatibility Checks Setting (Releases Prior to Release 4.x) 31
   Upgrading the Software Using the GUI (Release 4.x and Later) 32
      Downloading an Image (Release 4.x and Later) 32
      Upgrading the Cisco APIC Software Version Using the GUI (Release 4.x and Later) 34
      Upgrading the Leaf and Spine Switch Software Version Using the GUI (Release 4.x and Later) 35
      Upgrading the Nodes in the Upgrade Groups Using the GUI (Release 4.x and Later) 37
      Changing the Ignore Compatibility Checks Setting (Release 4.x and Later) 38
   Upgrading the Software Using the REST API 39
      Upgrading the Cisco APIC Software Using the REST API 39
      Upgrading Switches Software Using the REST API 40
      Upgrading the Catalog Software Version Using the REST API 41
   Upgrading the Software Using the CLI 41
      Upgrading the Cisco APIC Software Using the NX-OS Style CLI 41
      Upgrading the Switches Using the NX-OS Style CLI 43
      Upgrading the Catalog Software Version Using the NX-OS Style CLI 44
   Upgrading the Controller Using the Debug CLI 44
Upgrading the Controller Using the Debug CLI in Three Steps 45
Verifying the Firmware Version and the Upgrade Status Using the API 45
Verifying SSD Installation Status 45
Troubleshooting Failures During the Upgrade Process 46
  Common Reasons for Download Failure 46
Verifying Cluster Convergence 47
Verifying That the Controller Upgrade Paused 47
  Using the GUI to Verify Whether a Controller Upgrade Scheduler Paused 47
  Using the REST API to Verify Whether a Controller Upgrade Scheduler Paused 48
Verifying That the Switch Upgrade Paused 48
  Using the GUI to Verify Whether a Switch Upgrade Scheduler Paused 48
  Using the REST API to Verify Whether a Switch Upgrade Scheduler Paused 49
Resuming a Paused Scheduler for a Controller Maintenance Policy 49
  Using the GUI to Resume Paused Controller Upgrade Scheduler 50
  Using the REST API to Resume Paused Controller Upgrade Scheduler 50
Resuming a Paused Scheduler for a Switch Maintenance Policy 50
  Using the GUI to Resume Paused Switch Upgrade Scheduler 50
  Using the REST API to Resume Paused Switch Upgrade Scheduler 51
Performing a Clean Reboot 51
Upgrading with Shared Layer 3 Out 52
  Upgrading the Cisco APIC before the Leaf Switches 52
  Upgrading the Leaf Switches Before the Cisco APIC 52
  After the Cisco APIC and Leaf Switches are Upgraded 53
Downgrading with Shared Layer 3 Out 53
  Downgrading the Cisco APIC Before the Leaf Switches 53
  Downgrading the Leaf Switches Before the Cisco APIC 53
  Recommended Downgrade 53
Network Configuration Capabilities and Changes During Mixed OS Operation 53
About the Silent Roll Package Upgrade 57
  Configuring an Silent Roll Package Upgrade Using the Cisco APIC GUI 58
  Configuring an Silent Roll Package Upgrade Using the CLI 59
  Configuring an Silent Roll Package Upgrade Using the REST API 60
Cisco Nexus 9300 Platform Switches to Cisco Nexus 9300-EX Platform Switches Migration 61
Upgrade Examples 62
Controller Upgrade Examples  62
Switch Upgrade Examples  62
Preface

This preface includes the following sections:

- Audience, on page vii
- Document Conventions, on page vii
- Related Documentation, on page ix
- Documentation Feedback, on page x
- Obtaining Documentation and Submitting a Service Request, on page x

Audience

This guide is intended primarily for data center administrators with responsibilities and expertise in one or more of the following:

- Virtual machine installation and administration
- Server administration
- Switch and network administration
- Cloud administration

Document Conventions

Command descriptions use the following conventions:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>bold</strong></td>
<td>Bold text indicates the commands and keywords that you enter literally as shown.</td>
</tr>
<tr>
<td><em>Italic</em></td>
<td>Italic text indicates arguments for which the user supplies the values.</td>
</tr>
<tr>
<td>[x]</td>
<td>Square brackets enclose an optional element (keyword or argument).</td>
</tr>
<tr>
<td>[x</td>
<td>y]</td>
</tr>
<tr>
<td>Convention</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>{x \mid y}</td>
<td>Braces enclosing keywords or arguments separated by a vertical bar indicate a required choice.</td>
</tr>
<tr>
<td>[x {y \mid z}]</td>
<td>Nested set of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical bar within square brackets indicate a required choice within an optional element.</td>
</tr>
<tr>
<td><code>variable</code></td>
<td>Indicates a variable for which you supply values, in context where italics cannot be used.</td>
</tr>
<tr>
<td><code>string</code></td>
<td>A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.</td>
</tr>
</tbody>
</table>

Examples use the following conventions:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>screen font</code></td>
<td>Terminal sessions and information the switch displays are in screen font.</td>
</tr>
<tr>
<td><code>boldface screen font</code></td>
<td>Information you must enter is in boldface screen font.</td>
</tr>
<tr>
<td><code>italic screen font</code></td>
<td>Arguments for which you supply values are in italic screen font.</td>
</tr>
<tr>
<td><code>&lt; &gt;</code></td>
<td>Nonprinting characters, such as passwords, are in angle brackets.</td>
</tr>
<tr>
<td><code>[]</code></td>
<td>Default responses to system prompts are in square brackets.</td>
</tr>
<tr>
<td><code>!, #</code></td>
<td>An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.</td>
</tr>
</tbody>
</table>

This document uses the following conventions:

- **Note**
  - Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

- **Caution**
  - Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

- **Warning**
  - **IMPORTANT SAFETY INSTRUCTIONS**
    - This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.
    - **SAVE THESE INSTRUCTIONS**
Related Documentation

Cisco Application Policy Infrastructure Controller (APIC) Documentation

The following companion guides provide documentation for Cisco APIC:

- Cisco APIC Getting Started Guide
- Cisco APIC Basic Configuration Guide
- Cisco ACI Fundamentals
- Cisco APIC Layer 2 Networking Configuration Guide
- Cisco APIC Layer 3 Networking Configuration Guide
- Cisco APIC NX-OS Style Command-Line Interface Configuration Guide
- Cisco APIC REST API Configuration Guide
- Cisco APIC Layer 4 to Layer 7 Services Deployment Guide
- Cisco ACI Virtualization Guide
- Cisco Application Centric Infrastructure Best Practices Guide

All these documents are available at the following URL: http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html

Cisco Application Centric Infrastructure (ACI) Documentation


Cisco Application Centric Infrastructure (ACI) Simulator Documentation


Cisco Nexus 9000 Series Switches Documentation


Cisco Application Virtual Switch Documentation

Cisco ACI Virtual Edge Documentation


Cisco ACI Virtual Pod Documentation


Cisco Application Centric Infrastructure (ACI) Integration with OpenStack Documentation


Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, please send your comments to apic-docfeedback@cisco.com. We appreciate your feedback.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What's New in Cisco Product Documentation at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html

Subscribe to What’s New in Cisco Product Documentation, which lists all new and revised Cisco technical documentation as an RSS feed and delivers content directly to your desktop using a reader application. The RSS feeds are a free service.
New and Changed Information

- New and Changed Information, on page 1

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

<table>
<thead>
<tr>
<th>Cisco APIC Release Version</th>
<th>Feature</th>
<th>Description</th>
<th>Where Documented</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>APIC upgrade and downgrade paths removed from document</td>
<td>The APIC upgrade and downgrade paths have been removed from this document. Refer to the Cisco APIC Upgrade/Downgrade Support Matrix for APIC upgrade and downgrade paths, available here: <a href="https://www.cisco.com/c/dam/en/us/td/docs/Website/datacenter/apicmatrix/index.html">https://www.cisco.com/c/dam/en/us/td/docs/Website/datacenter/apicmatrix/index.html</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Silent Roll Package Upgrade</td>
<td>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.</td>
<td>About the Silent Roll Package Upgrade, on page 57</td>
</tr>
<tr>
<td>Cisco APIC Release Version</td>
<td>Feature</td>
<td>Description</td>
<td>Where Documented</td>
</tr>
<tr>
<td>----------------------------</td>
<td>---------</td>
<td>-------------</td>
<td>------------------</td>
</tr>
<tr>
<td></td>
<td>The <em>Cisco APIC Installation, Upgrade, and Downgrade Guide, Release 4.0(1)</em> document is no longer available</td>
<td>The <em>Cisco APIC Installation, Upgrade, and Downgrade Guide, Release 4.0(1)</em> 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.</td>
<td></td>
</tr>
<tr>
<td>Release 4.0(1)</td>
<td>Bash no longer supported as upgrade method</td>
<td>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.</td>
<td>Upgrading and Downgrading the Cisco APIC and Switch Software, on page 15</td>
</tr>
<tr>
<td>Release 4.0(1)</td>
<td>Changes to upgrade procedure using the GUI</td>
<td>The procedures for upgrading the software using the GUI has changed starting with Cisco APIC release 4.0(1).</td>
<td>Upgrading and Downgrading the Cisco APIC and Switch Software, on page 15</td>
</tr>
<tr>
<td>Release 3.2(1m)</td>
<td>Cisco APIC long-lived release</td>
<td></td>
<td>Cisco APIC Long-Lived Release, on page 23</td>
</tr>
<tr>
<td>Release 2.3(1e)</td>
<td>Network Configuration Capabilities and Changes During Mixed OS Operation</td>
<td>Support for additional features was added.</td>
<td>Network Configuration Capabilities and Changes During Mixed OS Operation, on page 53</td>
</tr>
<tr>
<td>Release 2.2(2e)</td>
<td>Network Configuration Capabilities and Changes During Mixed OS Operation</td>
<td>This feature was introduced.</td>
<td>Network Configuration Capabilities and Changes During Mixed OS Operation, on page 53</td>
</tr>
<tr>
<td>Release 2.2(2e)</td>
<td>--</td>
<td>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 <em>Cisco APIC Getting Started Guide, Release 2.x</em>.</td>
<td>--</td>
</tr>
<tr>
<td>Release 2.2(1n)</td>
<td>High Availability for APIC Cluster</td>
<td>The High Availability functionality for an APIC cluster enables you to operate the APICs in a cluster in an Active/Standby mode.</td>
<td>This content is available in the <em>Cisco APIC Getting Started Guide, Release 2.x</em></td>
</tr>
<tr>
<td>Release 1.3(1g)</td>
<td>The title of this document has been changed.</td>
<td>The old name was Cisco APIC Firmware Management Guide.</td>
<td></td>
</tr>
</tbody>
</table>
Installing or Recovering Cisco APIC Images

- Installation Notes, on page 3
- Usage Guidelines, on page 5
- Conditions for Recovering or Installing Cisco APIC Software Image, on page 7
- Installing Cisco APIC Software Using a PXE Server, on page 8
- Installing Cisco APIC Software Using Virtual Media, on page 9
- Cleanly Installing a Single Cisco APIC Using the Debug CLI, on page 12
- Cleanly Installing the Entire Cisco APIC Cluster and Clean the Cisco ACI Fabric Using the Debug CLI, on page 13
- Statefully Installing a Cisco APIC Cluster Using the Debug CLI, on page 14

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 (see Release Table below):

    acicobra-2.1_1X-py2.7.egg

    "X" is the letter of the release. For example, "2.1_1h".
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.

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

Table 2: Release Table

<table>
<thead>
<tr>
<th>Release Version</th>
<th>SDK egg file name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.1(2g)</td>
<td>acicobra-4.1_2g-py2.7.egg</td>
</tr>
<tr>
<td>Release 4.1(1i)</td>
<td>acicobra-4.1_1i-py2.7.egg</td>
</tr>
<tr>
<td>Release 4.0(3d)</td>
<td>acicobra-4.0_3d-py2.7.egg</td>
</tr>
<tr>
<td>Release 4.0(2c)</td>
<td>acicobra-4.0_2c-py2.7.egg</td>
</tr>
<tr>
<td>Release 4.0(1h)</td>
<td>acicobra-4.0_1h-py2.7.egg</td>
</tr>
<tr>
<td>Release 3.2(6i)</td>
<td>acicobra-3.2_6i-py2.7.egg</td>
</tr>
<tr>
<td>Release 3.2(5d)</td>
<td>acicobra-3.2_5d-py2.7.egg</td>
</tr>
<tr>
<td>Release 3.2(4d)</td>
<td>acicobra-3.2_4d-py2.7.egg</td>
</tr>
<tr>
<td>Release 3.2(3i)</td>
<td>acicobra-3.2_3i-py2.7.egg</td>
</tr>
<tr>
<td>Release 3.2(2l)</td>
<td>acicobra-3.2_2l-py2.7.egg</td>
</tr>
<tr>
<td>Release 3.2(1m)</td>
<td>acicobra-3.2_1m-py2.7.egg</td>
</tr>
<tr>
<td>Release 3.1(2m)</td>
<td>acicobra-3.1_2m-py2.7.egg</td>
</tr>
<tr>
<td>Release 3.1(1i)</td>
<td>acicobra-3.1_1i-py2.7.egg</td>
</tr>
<tr>
<td>Release 3.0(2h)</td>
<td>acicobra-3.0_2h-py2.7.egg</td>
</tr>
<tr>
<td>Release 3.0(1k)</td>
<td>acicobra-3.0_1k-py2.7.egg</td>
</tr>
<tr>
<td>Release 2.3(1e)</td>
<td>acicobra-2.3_1e-py2.7.egg</td>
</tr>
<tr>
<td>Release 2.2(2e)</td>
<td>acicobra-2.2_2e-py2.7.egg</td>
</tr>
<tr>
<td>Release 2.2(1n)</td>
<td>acicobra-2.2_1n-py2.7.egg</td>
</tr>
<tr>
<td>Release 2.1(1h)</td>
<td>acicobra-2.1_1h-py2.7.egg</td>
</tr>
<tr>
<td>Release 2.0(2f)</td>
<td>acicobra-2.0_2f-py2.7.egg</td>
</tr>
<tr>
<td>Release 2.0(1m)</td>
<td>acicobra-2.0_1m-py2.7.egg</td>
</tr>
<tr>
<td>Release Version</td>
<td>SDK egg file name</td>
</tr>
<tr>
<td>-----------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>Release 1.3(2f)</td>
<td>acicobra-1.3_2f-py2.7.egg</td>
</tr>
<tr>
<td>Release 1.3(1i)</td>
<td>acicobra-1.3_1i-py2.7.egg</td>
</tr>
<tr>
<td>Release 1.3(1h)</td>
<td>acicobra-1.3_1h-py2.7.egg</td>
</tr>
<tr>
<td>Release 1.3(1g)</td>
<td>acicobra-1.3_1g-py2.7.egg</td>
</tr>
</tbody>
</table>

For information about previous releases, see Cisco Application Policy Infrastructure Controller (APIC) Release Notes

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 max 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

Note
Use the procedures in this section ONLY with the assistance of the Cisco Technical Assistance Center (TAC).

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 Cisco APIC Software Using a PXE Server

Follow these steps to install the Cisco APIC software using a Preboot Execution Environment (PXE) server:

Procedure

Step 1  Configure the PXE server as follows:

a) Configure the PXE server with a standard configuration for Linux.
b) Mount the ISO image.

Example:

$ mount -t iso9660 -o loop aci-apic-dk9.1.0.0.200v.iso myisomount

c) Inspect the contents of the file.

Example:

$ ls -n myisomount
...  drwxrwxr-x 6 76989 2000 4096 May 30 14:56 insieme
    drwxrwxr-x 3 76989 2000 4096 May 30 14:56 images
...
$ ls myisomount/images/pxeboot/
   initrd.img vmlinuz

d) PXE Menu entry: <pxe-dir>/tftpboot/boot_msg
e) PXE Menu entry images: <pxe-dir>/tftpboot/pxelinux.cfg/default

Example:

$ cat tftpboot/pxelinux.cfg/default
...  label 10
      kernel ifcimages/vmlinuz
                       ksdevice=eth0 loglevel=0 console=tty9
  ...
$ ls myisomount/images/pxeboot/
   initrd.img vmlinuz

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

f) Add the kickstart file: <pxe-dir>/kickstart/<mykickstartfile>

Example:

$ cat kickstart/ifc-stable

# IFC Kickstart script for UCS C200
install
url --url=http://172.21.157.10/myisomount
lang en_US.UTF-8
Installing Cisco APIC Software Using Virtual Media

The method that you use to install Cisco APIC software using virtual media varies slightly, depending on the release of the software.

Installing Software Using Virtual Media (Releases Prior to Release 4.x)

Installing Cisco APIC Software Using Virtual Media

Installing or Upgrading the Cisco APIC software using vMedia requires the following high-level process:

• Obtain the relevant Cisco APIC .iso image from CCO.

• Access the Cisco Integrated Management Controller (IMC) web interface for the controller.

Note

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

• Mount the .iso image using the Integrated Management Controller vMedia functionality.

• Boot or power cycle the controller.

• During the boot process press F6 to select the Cisco vKVM-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

Due to the slower transfer rate of vMedia, you can optionally install the main image from the network. When prompted, press Enter within 30 seconds during the IMC vMedia installation process. The installer will switch from vMedia installation to the network image location. Answer the prompts by entering the relevant host networking configuration details, such as the IP address, subnet, gateway, and image path.

Installing Cisco APIC Software Using Virtual Media Through KVM Console

Use this procedure to install or upgrade the Cisco APIC software using vMedia through the KVM console.
Procedure

**Step 1** Update the Java security.
   a) Open the Java Control Panel.
   b) In the **Security** tab, click **High Security** radio button.
   c) Add the IMC IP address in the **Exception Site List**.
   d) Click **OK**.

**Step 2** Log in to the Cisco Integrated Management Controller (IMC) using the IMC credentials.
   The IMC credentials may be different from the Cisco APIC credentials.

**Step 3** Access the KVM console.
   a) Choose **Server > Summary > Launch KVM Console**.
   b) Open the downloaded file using the **Java Web Start Launcher**.
   c) Map the file to the viewer located at `C:/user/Program Files/Java/bin/name of the java viewer`.

   **Note** Ensure that the downloaded file has the extension `.jnlp`.

**Step 4** Map the Cisco APIC `.iso` image.
   a) Download the Cisco APIC `.iso` image from `Cisco.com`.
   b) On the KVM console, choose **Virtual Media > Activate Virtual Devices** and then choose **Virtual Media > Map CD/DVD**.
   c) Click **Browse** to select the Cisco APIC `.iso` image.
   d) Click **Map Device**.

**Step 5** Boot or power cycle the controller.
   a) On the IMC page, choose **Server > Server Summary > Power Cycle Server**.
   b) Press F6 to select the boot device.
   c) Enter the BIOS password if required. The default password is 'password'.
   d) Choose **Cisco vKVM-Mapped vDVD1.22** to load the image.

   After this process is completed, the Cisco APIC setup script is displayed.

   e) To verify, choose **KVM Console > Tools > Stats**.

**Step 6** In the Cisco APIC console, enter the options for the initial setup such as fabric name, number of controllers, tunnel endpoint address pool, infra VLAN ID.

   **Note** When setting up Cisco APIC in an active-standby mode, ensure that the Cisco APIC information for all the Cisco APICs in the cluster is the same.

---

**Installing Software Using Virtual Media (Release 4.x and Later)**

**Installing Cisco APIC Software Using CIMC Virtual Media**

Use this procedure to install the Cisco APIC software using CIMC Virtual Media.
Procedure

Step 1 Obtain the relevant Cisco APIC .iso image from CCO.
Step 2 Copy the .iso image to the HTTP server.
Step 3 Open the Cisco Integrated Management Controller GUI for the controller.
Step 4 From the CIMC GUI, choose Server > Summary > Launch KVM Console to access the KVM console.
Step 5 Log in to the CIMC console:

```bash
# ssh admin@cimc_ip
```

Step 6 Change the scope to virtual media:

```bash
# scope vmedia
```

Step 7 Map the .iso image to the HTTP server:

```bash
# map-www volume_name http://http_server_ip iso_file_name
```

Where:

- `volume_name` is the name of the volume.
- `http_server_ip` is the IP address of the HTTP server.
- `iso_file_name` is the name of the .iso file.

Step 8 Check the mapping status:

```bash
# show mappings detail
```

The status should be shown as `ok`.

Step 9 Connect to SOL (Serial over LAN) to monitor the installation process:

```bash
# connect host
```

Step 10 From the KVM console, choose Power > Reset System to power cycle the controller.

Step 11 During the boot process, press F6 to select the Cisco vCIMC-Mapped vDVD as the one-time boot device.

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

Step 12 Determine if you want to enter the ISO URL to speed up the installation process.

During the boot-up process, you will 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**: We recommend this option, as this will make the installation process go faster. If you choose this option, you will be asked to provide the protocol type:

  - **static**: If you choose this option, you will be asked to enter the interface name, management IP address and gateway.
• dhcp

• Do not enter the ISO URL: If you do not want to enter the ISO URL, the installation process starts after ten minutes.

The system starts fetching the ISO at this point.

Step 13 Wait until you see the message poweroff from SOL, then perform the following:
   a) Exit from SOL by pressing Ctrl+x.
   b) Unmap the .iso image:
      ```bash
      # unmap volume_name
      ``
   c) Connect back to SOL again:
      ```bash
      # connect host
      ```

Step 14 From the KVM console, choose Power > Power on System to power on the controller.

Step 15 During the boot process, press F6 to select the PCI RAID Adapter as the one-time boot device.

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

Step 16 From SOL, 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.

---

Cleanly Installing a Single Cisco APIC Using the Debug CLI

Use this procedure to install a single Cisco APIC; this does not install the entire cluster.

Procedure

Step 1 Decommission the Cisco APIC using either the GUI or the REST API.
Step 2 Log in as root to the Cisco APIC.
Step 3 Obtain the image you want to use by completing one of the following steps.
   a) Locate an existing image in the repository.
      Example:
      ```bash
      root@apic1:~> ls /firmware/fwrepos/fwrepo
      ``
   b) If the image you are looking for is not already present in the repository, you need to copy over your own image from outside the Cisco APIC. Please note that you should not copy your image into the repository (/firmware/fwrepos/fwrepo). Instead, copy to /firmware.
      Example:
      ```bash
      root@apic1:~> scp <username>@<external-server-ip-address>:/<path-to-image>/firmware/
      ``
Step 4 Install the copied image statelessly.
Cleanly Installing the Entire Cisco APIC Cluster and Clean the Cisco ACI Fabric Using the Debug CLI

Procedure

Step 1 Export the configuration.
Step 2 For each Cisco APIC in the Cisco APIC cluster, take the following steps.
   a) Log in as root.
   b) Obtain the image you want to use by completing one of the following steps.
      • Locate an existing image in the repository:
        root@apic1:~> ls /firmware/fwrepos/fwrepo
      • Copy your own image outside the repository.
        root@apic1:~> scp <username>@<external-server-ip-address>:/<path-to-image>/firmware/
   c) Perform the clean install.
      Example:
      root@apic1:~>/mgmt/support/insieme/installer.py full -f /firmware/<image-name>
   d) Reboot.
      Example:
      root@apic1:~> sync && reboot
Step 3 For each switch in the Cisco ACI fabric, take the following steps.
   a) Log in as root.
   b) Mark for clean data.
      Example:
      root@apic1:~> touch/mnt/pss/.clean
   c) Reboot.
      Example:
Statefully Installing a Cisco APIC Cluster Using the Debug CLI

Repeat this procedure for each Cisco APIC in the cluster.

Procedure

Step 1 Log in as root to the Cisco APIC.
Step 2 Obtain the image you want to use by completing one of the following steps.
  a) Locate an existing image in the repository.
     Example: 
     root@apic1:~> ls /firmware/fwrepos/fwrepo
  b) Copy your own image outside the repository.
     Example: 
     root@apic1:~> scp <username>@<external-server-ip-address>:/<path-to-image>/firmware/
Step 3 Perform the stateful installation of the Cisco APIC.
     Example: 
     root@apic1:~>/mgmt/support/insieme/installer.py full -f /firmware/<image-name> --dataconvertandreboot
Step 4 Wait for the Cisco APIC to resume processing and for the cluster to converge.
Step 5 Repeat the procedure with the next Cisco APIC.
CHAPTER 3

Upgrading and Downgrading the Cisco APIC and Switch Software

- About Firmware Management, on page 15
- Workflow to Upgrade or Downgrade the Cisco ACI Fabric, on page 19
- About Upgrading the Cisco APIC and the Switch Software, on page 21
- Supported Upgrade Paths for the Cisco APIC and Switch Software, on page 23
- Cisco APIC Long-Lived Release, on page 23
- About Downgrading the Cisco APIC and Switch Software, on page 24
- Stateless Downgrade Procedure, on page 25
- Supported Downgrade Paths for the Cisco APIC and Switch Software, on page 26
- About Upgrading with the Scheduler, on page 26
- About Disabling LLDP Back to Back Connections Before Upgrading, on page 27
- Upgrading the Software Using the GUI (Releases Prior to Release 4.x), on page 27
- Upgrading the Software Using the GUI (Release 4.x and Later), on page 32
- Upgrading the Software Using the REST API, on page 39
- Upgrading the Software Using the CLI, on page 41
- Upgrading the Controller Using the Debug CLI, on page 44
- Upgrading the Controller Using the Debug CLI in Three Steps, on page 45
- Verifying the Firmware Version and the Upgrade Status Using the API, on page 45
- Verifying SSD Installation Status, on page 45
- Troubleshooting Failures During the Upgrade Process, on page 46
- Upgrading with Shared Layer 3 Out, on page 52
- Downgrading with Shared Layer 3 Out, on page 53
- Network Configuration Capabilities and Changes During Mixed OS Operation, on page 53
- About the Silent Roll Package Upgrade, on page 57
- Cisco Nexus 9300 Platform Switches to Cisco Nexus 9300-EX Platform Switches Migration, on page 61
- Upgrade Examples, on page 62

About Firmware Management

The term "firmware" used in this guide refers to the Cisco APIC's appliance firmware, which can be upgraded in the Cisco APIC GUI on the menu bar under ADMIN > Firmware and, in APIC releases prior to 4.x, in
the Navigation pane under **Controller Firmware**. This term should not to be confused with the Cisco APIC’s component firmware such as the CIMC, BIOS, LOM, and RAID controllers, and NIC/VIC PCI adapters.

**Version Nomenclature**

The following information is necessary to manage the firmware:

- **Firmware Repository** — Firmware repository is a distributed store that stores firmware images required to upgrade Cisco ACI fabric. Firmware repository is synced to every controller in the cluster. A firmware image is downloaded into the firmware repository from an external server (HTTP or SCP) when you configure a firmware source policy. There are three types of firmware images that can be stored in the repository:
  - **Cisco APIC image** — This image consists of software that runs on Cisco Application Policy Infrastructure Controllers (Cisco APICs).
  - **Switch image** — This image consists of software that runs on Cisco ACI switches.
  - **Catalog image** — This image consists of Cisco-created internal policies. These internal policies contain information about the capabilities of different models of hardware, the compatibility across different versions of software, and the hardware and diagnostic tests. This image is usually bundled and upgraded along with the controller image. Unless specifically instructed by release notes of a specific release, an administrator should never have to individually upgrade a catalog image.

- **Firmware Group and Firmware Policy** — A Firmware Group is a group of switches on which you configure a firmware policy. A Firmware Policy specifies the desired firmware version for switches in the group.

- **Controller Firmware Policy and Controller Maintenance Policy** — Applies for APIC releases prior to 4.x. The Controller Firmware Policy specifies the desired version for controllers. The Controller Maintenance Policy specifies when the upgrade of controllers should start. The Controller Firmware Policy and the Controller Maintenance Policy apply to all the controllers in the cluster.

- **Maintenance Group and Maintenance Policy** — Applies for APIC releases prior to 4.x. A Maintenance Group is a group of switches on which you would configure a Maintenance Policy. A Maintenance Policy specifies a schedule for upgrade.

**Important Notes**

- **If you are running apps from** [https://aciappcenter.cisco.com/](https://aciappcenter.cisco.com/) **on your Cisco APIC nodes, you must disable those apps before upgrading or downgrading the APIC software on those APIC nodes. After you have completed the upgrade or downgrade process for the entire fabric (the APIC nodes and switches), re-enable the apps again.**

- **In 4.1 or later, a software check has been added to identify Fiber Channel (FC) and Ethernet transceivers. Before ACI 4.1, this check was not present in the software. This check is required to make sure FC ports and Ethernet ports are properly identified. All transceivers that have the correct SPROM programming should continue to work post-upgrade. If any transceivers have an incorrectly programmed SPROM which does not correctly identify them as an FC or Ethernet transceivers, they will fail transceiver validation and fail to come up on 4.1. In this scenario, contact your respective vendors to update and address the programmed SPROM values.**

- **Do not upgrade a Cisco ACI fabric if any node in the fabric is in the Graceful Insertion and Removal (GIR) mode, or maintenance mode. If any node on the fabric is in the GIR mode and the fabric is upgraded, then that node becomes inaccessible after all other connected nodes are reloaded, even if that node is not part of the current upgrade group.**
• If you are upgrading several leaf switches at once, and you are selecting the Graceful Maintenance option in the Schedule Node Upgrade screen for each switch, Cisco Application Policy Infrastructure Controller (Cisco APIC)-connected leaf switches must be put into different maintenance groups such that the Cisco APIC-connected switches get upgraded one at a time.

• Similarly, for multipod configurations, if you are upgrading several spine switches at once, and you are selecting the Graceful Maintenance option in the Schedule Node Upgrade screen for each switch, the spine switches must be put into different maintenance groups such that the switches get upgraded one at a time. In addition, for multipod, do not use Graceful Maintenance if only one spine switch is available in the pod.

• If a recurring or one-time upgrade schedule is set with a date in the past, the scheduler triggers the upgrade immediately. See Firmware Upgrade Modes, on page 17 for more information.

• You should have serial console access when upgrading or downgrading in the unlikely event that switch access through the Ethernet in-band or out-of-band access is no longer possible.

• When you upload the firmware using the Cisco APIC GUI, if the transfer time exceeds the web token time out value, the web token will time out and the upload will fail. Before you upload the firmware using the Cisco APIC GUI, you must increase the web token time out value to a time greater than the expected upload time.

**Firmware Upgrade Modes**

The method to upgrade the firmware using Cisco APIC varies, depending on the release:

- **Cisco APIC Releases Prior to 4.x, on page 17**
- **Cisco APIC Releases 4.x and Later, on page 18**

**Cisco APIC Releases Prior to 4.x**

In the Cisco APIC GUI, you can upgrade the firmware by navigating to **Admin > Firmware > Fabric Node Firmware > Maintenance Groups**. Select a maintenance group and from the Actions menu, select **Create One Time Window Trigger** or **Create Recurring Window Trigger** to schedule an upgrade.

There are two modes to upgrade the firmware using Cisco APIC.

- **Upgrade immediately**— In this mode, the firmware upgrade process is started immediately.
- **Schedule an upgrade**— In this mode you can schedule the firmware upgrade for a later date and time. The following parameters must be specified to schedule upgrade.
  
  • **Name**— Specifies the name.
  
  • **Date**— Specifies the start date and time for the upgrade to begin.
  
  • **Maximum Concurrent Nodes**— Specifies the concurrent nodes to upgrade. The default value for Cisco APIC is 1. The default value for switches is 20.
  
  • **Maximum Running Time**— Specifies the duration window for the upgrade. The default value is unlimited.

When you schedule a firmware upgrade, the following scenarios can occur.
Firmware Upgrade Modes

- Scenario 1— Maximum Running Time is set, and the Date is set to a date later than the current date and time. In this scenario, the upgrade will start at the scheduled start date.

- Scenario 2— Maximum Running Time is not set, and the Date is set to a date later than the current date and time. In this scenario, the upgrade will start at the scheduled start date.

- Scenario 3— The upgrade is scheduled to a Date earlier than the current date and time and the Maximum Running Time is also set to an earlier time than the current time. In this scenario, the upgrade will not start.

- Scenario 4— The upgrade is scheduled to a Date earlier than the current date and time and the Maximum Running Time is set to a later time than the current time. In this scenario, the upgrade will start immediately.

- Scenario 5— The upgrade is scheduled to a Date earlier than the current date and time and the Maximum Running Time is not set. In this scenario, the upgrade will start immediately.

Cisco APIC Releases 4.x and Later

In the Cisco APIC GUI, you can upgrade the firmware by navigating to Admin > Firmware. Click the Infrastructure tab, then click the Nodes sub-tab. Click Actions, then click Schedule Node Upgrade. Select an existing group or create a new one in the Upgrade Group Name area.

There are two modes to upgrade the firmware using Cisco APIC.

- Now— In this mode, the firmware upgrade process is started immediately.

- Schedule for Later— In this mode you can schedule the firmware upgrade for a later date and time. The following parameters must be specified to schedule upgrade.
  
  - Name— Specifies the name.
  
  - Date— Specifies the start date and time for the upgrade to begin.

- Maximum Concurrent Nodes—Specifies the concurrent nodes to upgrade. The default value for Cisco APIC is 1. The default value for switches is 20.

- Maximum Running Time—Specifies the duration window for the upgrade. The default value is unlimited.

When you schedule a firmware upgrade, the following scenarios can occur.

- Scenario 1— Maximum Running Time is set, and the Date is set to a date later than the current date and time. In this scenario, the upgrade will start at the scheduled start date.

- Scenario 2— Maximum Running Time is not set, and the Date is set to a date later than the current date and time. In this scenario, the upgrade will start at the scheduled start date.

- Scenario 3— The upgrade is scheduled to a Date earlier than the current date and time and the Maximum Running Time is also set to an earlier time than the current time. In this scenario, the upgrade will not start.

- Scenario 4— The upgrade is scheduled to a Date earlier than the current date and time and the Maximum Running Time is set to a later time than the current time. In this scenario, the upgrade will start immediately.
Scenario 5—The upgrade is scheduled to a **Date** earlier than the current date and time and the **Maximum Running Time** is not set. In this scenario, the upgrade will start immediately.

**Workflow to Upgrade or Downgrade the Cisco ACI Fabric**

Cisco APIC simplifies upgrading the fabric because it allows you to manage centrally the upgrade for the entire fabric. The Cisco APIC acts as the repository of the image and as the booting server. Leaf switches and spine switches have in-band connectivity to the Cisco APIC, and when upgrading, the switches download the firmware from the Cisco APIC. To complete an upgrade successfully, you must have connectivity from the leaf switches and spine switches that you are upgrading to the Cisco APIC. To maintain connectivity, you should define a minimum of two maintenance groups and upgrade one group at a time. Wait until the first group has successfully completed the upgrade before upgrading the second group. This section provides the recommended steps for a successful upgrade with minimum disruption.

**Note**

- The Cisco APIC-X is upgraded after the Cisco APIC.
- The Cisco APIC-X is supported starting with Cisco APIC Release 4.0(1) and should be decommissioned and shut down (or disconnected from the cluster) before downgrading to an older version.

At a high level, steps to upgrade or downgrade the Cisco ACI fabric are as follows:

- The procedure or steps for upgrade and downgrade are the same unless stated otherwise in the release notes of a specific release.
- Ensure that you have the required CIMC version required for Cisco APIC upgrade. See the Cisco APIC Release Notes for the supported CIMC versions.
- Download the Cisco ACI Controller image (Cisco APIC image) into the repository.
- Download the Cisco ACI switch image into the repository.
- Upgrade the cluster of Application Policy Infrastructure Controllers (Cisco APICs).
- Verify that the fabric is operational and the APIC cluster is "Fully Fit" before proceeding.
- Divide the switches into multiple groups, and upgrade the switches by group, verifying that the fabric is operational between switch group upgrades. For example, assume that you divided the switches into two groups – red and blue. You could then go through the following upgrade process:

1. Upgrade the red group of switches.
2. Verify that the fabric is operational.
3. Upgrade the blue group of switches.
4. Verify that the fabric is operational.
If the Cisco ACI fabric deployment includes Cisco AVS, upgrade the Cisco AVS to the version compatible with the Cisco APIC. To upgrade Cisco AVS, see the section **Recommended Upgrade Sequence for Cisco APIC, the Fabric Switches, and the Cisco AVS** in the *Cisco Application Virtual Switch Installation Guide*.

---

**Guidelines**

Additionally, here are some general guidelines regarding Cisco ACI fabric upgrade or downgrade:

- Divide switches into two or more groups. Upgrade one group at a time. That way you will not lose fabric bandwidth entirely during the upgrade window.

- Do not upgrade or downgrade nodes that are part of a disabled configuration zone.

- A specific release, or a combination of releases, may have some limitations and recommendations for the upgrade or downgrade procedure. Double check the release notes for the release before upgrading or downgrading your Cisco ACI fabric.

- Before an upgrade or downgrade is triggered, any faults on the fabric should be investigated and resolved. It is possible for the fabric to have benign faults that will not affect the upgrade, which might include unused or unfinished configurations. All faults should be evaluated before the upgrade or downgrade operation. Any disk usage related faults should be addressed before the upgrade as overcapacity can cause issues while unpacking new software.

- Before triggering an upgrade or downgrade operation, it is required that the fabric is in a **Fully Fit** state. All Cisco APICs should be in **Fully Fit** state before moving between Cisco APIC image versions or before initiating switch upgrade or downgrade. Initiating a controller or switch upgrade or downgrade while the controllers are not in a **Fully Fit** operational state can lead to unexpected results.

When you perform an upgrade or downgrade operation across multiple versions, you must ensure that the fabric is in a **Fully Fit** state. For example, if upgrading from version A to B to C, after upgrading from A to B, you must wait for all controllers and switches to be in a **Fully Fit** state and operational on version B before initiating the upgrade from version B to C.

- It is recommended to collect a configuration backup before upgrading or downgrading the fabric.

- For multipod configurations, it is recommended that you put the leaf switches and the spine switches into different maintenance groups when upgrading or downgrading. Also, it is recommended that you divide the leaf switches and spine switches using the method described in *Four-group method, on page 21*.

---

**Note**

It is recommended to divide your switches into two or more groups for upgrading or downgrading. Below are examples of dividing switches into two groups and four groups respectively.

---

**Two-group method**

1. Divide your switches into two groups: a red group and a blue group. Put one half of the spine switches in the red group, and the other half in the blue group. Also, put one half of the leaf switches in the red group and the other half in the blue group.
2. Upgrade the red group.
3. After the red group upgrade is complete, confirm that the fabric is healthy.
4. Upgrade the blue group.

Four-group method

1. Divide your switches into four groups: a red spine switches group, a blue spine switches group, a red leaf switches group, and a blue leaf switches group. Put one half of the spine switches in the red spine switches group, and the other half of the spine switches in the blue spine switches group. Then, place half the leaf switches in the red leaf switches group, and the other half in the blue leaf switches group.
2. Upgrade the red leaf switches group.
3. After the red leaf switches group upgrade is complete, confirm that the fabric is healthy.
4. Upgrade the blue leaf switches group.
5. After the blue leaf switches group upgrade is complete, confirm that the fabric is healthy.
6. Upgrade the red spine switches group.
7. After the red spine switches group upgrade is complete, confirm that the fabric is healthy.
8. Upgrade the blue spine switches group.

About Upgrading the Cisco APIC and the Switch Software

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

Possible Issue When Upgrading Leaf Switches in Different Maintenance Groups

Cisco has identified a defect, which is documented in the bug CSCvi76161, where a version mismatch between Cisco ACI leaf switches may cause an unexpected EP announce message to be received by the EPM process on the leaf switch, resulting in an EPM crash. You are impacted by this issue only if you are upgrading from one of the affected software releases to a 13.2(2) release or later, or are downgrading from a 13.2(2) release or later to one of the affected software releases.

You may experience this issue when upgrading leaf switches that belong to two different maintenance groups. As an example, Leaf 101 is in Maintenance Group "Odds" and Leaf 102 is in Maintenance Group "Evens." If you upgrade Maintenance Group "Odds" (thus upgrading Leaf 101), after the "Odds" upgrade completes, Leaf 102 may continuously HAP reset and reload.

There are two possible workaround options for this issue:

- Perform a Two-Step Upgrade: Perform one of the following procedures, depending on your current Cisco NX-OS release:
  - For fabrics running a pre-12.2(4p) Cisco NX-OS release, upgrade to 12.2(4r) and then upgrade to the desired destination release.
  - For fabrics running a 12.3(1) Cisco NX-OS release, upgrade to 13.1(2t) and then upgrade to the desired destination release.
• **Use the testapi Binary:** Use the testapi binary to disable the endpoint announce feature temporarily during the upgrade. You must use the testapi binary after the Cisco APIC is upgraded to a 3.2(2) or later release, but before the leaf switches are upgraded. To use this method, contact Cisco TAC.

**Important Notes**

• When you are upgrading the ACI switches, at the point when the upgrade process reaches 80%, the upgrade process that is shown in the GUI might freeze at 80-90%, although the switches have actually completed their upgrades and are in the process of reloading. Click the Refresh button at the top right corner of the table to get the latest status on the switches so that you can verify that the upgrade process was completed successfully.

• Starting with Cisco APIC release 4.0(1), you cannot use Bash to upgrade the Cisco APIC and the switch software. Use the NX-OS style CLI to upgrade the Cisco APIC and the switch software instead, as described in Upgrading the Software Using the CLI, on page 41.

• With mixed operating system operation, you can have at most two different releases in the fabric at any given time. If you upgrade the fabric, you can only upgrade to a release for which there is a direct upgrade path. When upgrading to a release that does not have a direct upgrade path from your current release, you must upgrade all the Cisco APICs and switches to an intermediate supported release to which there is a direct upgrade path, then upgrade from that release to your desired release. Sometimes, you must upgrade to multiple intermediate releases before being able to upgrade to your desired release, upgrading both the Cisco APICs and switches to the same release each time.

For example, if you upgrade from a Cisco APIC 2.3(1) release and Cisco NX-OS 12.3(1) release to a 3.2(3)/13.2(3) release, you cannot directly upgrade to the 3.2(3)/13.2(3) release. One supported direct upgrade path is to upgrade to the 3.1(2)/13.1(2) release. Thus, you must upgrade the Cisco APICs to the 3.1(2) release and the switches to the 13.1(2) release. Next, you can upgrade to the Cisco APIC 3.2(3) release and Cisco NX-OS 13.2(3) release.

• Starting with Cisco APIC release 1.2(2), when a contract is provided on an Out-of-band node management EPG, the default Cisco APIC Out-of-band contract source address is the local subnet that is configured on the Out-of-band node management address. Previously, any address was allowed to be the default Cisco APIC Out-of-band contract source address.

• Ensure that a contract is provided under the OOB EPG that it is properly configured before upgrading. When upgrading to the 1.2(2) release, a nondefault Out-of-band contract that is applied to the Out-of-band node management endpoint group can cause unexpected connectivity issues to the Cisco APICs. If an incorrectly configured Out-of-band contract is present that had no impact in prior Cisco APIC releases, upgrading to the 1.2(2) release can cause Out-of-band management EPGs that use such incorrectly configured Out-of-band contracts to lose access to the cluster of Cisco APICs.

• A minimum subnet mask of /19 is recommended.

• Cisco ACI Multipod deployment requires 239.255.255.240 system GIPO to be configured on the interpod network as a PIM BIDIR range. This 239.255.255.240 PIM BIDIR range configuration on the IPN devices can be avoided using the Infra GIPO as System GIPO feature. The Infra GIPO as System GIPO feature must be enabled, only after upgrading all the switches in the Cisco ACI fabric including the leaf switch and spine switch to the latest Cisco APIC release.

---

**Note**

Switches in different pods can only be upgraded serially, regardless if they are in the same maintenance group. The switches cannot be upgraded in parallel.
• Starting in the 2.2(1) release, the Cisco APICs must have 1 SSD and 2 HDD, and both RAID volumes must be healthy before upgrading to this release. An SSD is required to boot a Cisco APIC, and the Cisco APIC will not boot if the SSD is not installed. See Verifying SSD Installation Status, on page 45.

• Starting from Cisco APIC release 3.0(1), during a Cisco APIC upgrade if a switch upgrade is triggered, the switch is upgraded after all the Cisco APICs have been successfully upgraded. During the Cisco APIC upgrade process, the switches are in an IN Queue state.

• When performing a multistep upgrade, you should use an intermediate version of Cisco APIC release 2.1 if supported, or later to prevent issues that are related to CSCvb94260.

• In APIC, there is a compatibility check feature that verifies if an upgrade path from the currently running version of the system to a specific newer version is supported or not. There is an "Ignore Compatibility Checks" setting that is set to off by default, so the system automatically checks the compatibility for possible upgrades by default. See Changing the Ignore Compatibility Checks Setting (Releases Prior to Release 4.x), on page 31 or Changing the Ignore Compatibility Checks Setting (Release 4.x and Later), on page 38 if you wish to change the "Ignore Compatibility Checks" setting to on for any reason so that the compatibility check feature is disabled.

## Supported Upgrade Paths for the Cisco APIC and Switch Software

Supported upgrade paths for the Cisco APIC and switch software is no longer provided in this document. For the latest supported upgrade paths for Cisco APIC and the switch software, see the Cisco APIC Upgrade/Downgrade Support Matrix, available here:


## Cisco APIC Long-Lived Release

Cisco APIC 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 primarily be focused 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.

### 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.

### Long-Lived Release Life Cycle

• 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:

<table>
<thead>
<tr>
<th>Long-Lived Cisco APIC Release Version</th>
<th>Long-Lived Cisco Switch Release Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.2(x)</td>
<td>13.2(x)</td>
</tr>
<tr>
<td>2.2(x)</td>
<td>12.2(x)</td>
</tr>
</tbody>
</table>

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.

### About Downgrading the Cisco APIC and Switch Software

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

### Important Notes

- The following guidelines and limitations apply when downgrading the Cisco APIC and switch software:
  - Switches can be downgraded to a 1.0(1x) version if the imported configuration consists of a firmware policy with a desired version set to 1.0(1x).
  - 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.
  - Downgrading a Cisco APIC configured with Intra-EPG deny configuration from the 1.2(2) release to an earlier release is not supported. The Intra-EPG deny configuration must be manually cleaned up before downgrading.
  - When performing a Cisco APIC software downgrade, you must disable Federal Information Processing Standards (FIPS) first. See the *Cisco APIC and Federal Information Processing Standards (FIPS)* document for more information.
  - 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.
• When downgrading from Cisco APIC 1.2(1x) to 1.0(4q) or earlier or from 1.1(1x), 1.1(2x), 1.1(3x), or 1.1(4x) to 1.0(4h) or earlier, follow the stateless downgrade instructions below. You must plan for a fabric outage, as this procedure rebuilds the fabric.

• Cisco N9K-C9508-FM-E2 fabric modules must be physically removed before downgrading to releases earlier than Cisco APIC 3.0(1).

• If you have remote leaf switches deployed, if 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.

• When you enable or disable Federal Information Processing Standards (FIPS) on a Cisco ACI fabric, you must reload each of the switches in the fabric for the change to take effect. The configured scale profile setting is lost when you issue the first reload after changing the FIPS configuration. The switch remains operational, but it uses the default port scale profile. This issue does not happen on subsequent reloads if the FIPS configuration has not changed. FIPS is supported on Cisco NX-OS release 13.1(1) or later.

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.

### Stateless Downgrade Procedure

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Export the fabric configuration.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Run the <code>eraseconfig</code> command on the Cisco APICs. This will reboot the controllers. Ensure that the controllers have been rebooted before moving on to step 3.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Rediscover the fabric.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Downgrade the fabric to the desired release.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Run the <code>eraseconfig setup</code> command on the Cisco APICs. This step is required so that the script can run additional commands that might be required for the version that is being used. The <code>eraseconfig setup</code> command will reload the Cisco APICs.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Run the <code>setup-clean-config.sh</code> script on the switch nodes and reload them.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Complete the initial setup script on the Cisco APICs.</td>
</tr>
<tr>
<td>Step 8</td>
<td>Import the fabric configuration using the import “merge” mode.</td>
</tr>
</tbody>
</table>
Supported Downgrade Paths for the Cisco APIC and Switch Software

Supported downgrade paths for the Cisco APIC and switch software is no longer provided in this document. For the latest supported downgrade paths for the Cisco APIC and switch software, see the Cisco APIC Upgrade/Downgrade Support Matrix, available here:


About Upgrading with the Scheduler

The scheduler enables you to specify a window of time for operations such as upgrading 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. 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.
About Disabling LLDP Back to Back Connections Before Upgrading

Before you upgrade a Cisco ACI fabric to Cisco APIC 2.x, if the upgrade target has LLDP over back-to-back leaf switch connections that join two different Cisco ACI fabrics with different infrastructure VLAN configurations, you must first disable those LLDP Connections.

If you do not disable LLDP on those connections, the upgrade will overwrite and disrupt Cisco ACI connections between the spine and leaf switches.

- One way to disable LLDP on the target connections is by policy; include the associated interfaces in a common leaf switch interface profile, associate the interface profile with a common interface policy group. Then include in that policy group a special LLDP interface policy in which the Received State and Transmit State are disabled.

- You can also apply to the target interface, the CLI NX-OS style CLI commands no lldp receive and no lldp transmit.

- You can also disable through a REST API POST:

```json
POST https://<apic>/api/node/mo/uni/infra/lldpIfP-LLDP-Disabled.json
{
  "lldpIfPol":{
    "attributes":{
      "dn":"uni/infra/lldpIfP-LLDP-Disabled",
      "name":"LLDP-Disabled",
      "adminRxSt":"disabled",
      "adminTxSt":"disabled",
      "status":"created"
    },"children":[]
  }
}
```

Upgrading the Software Using the GUI (Releases Prior to Release 4.x)

You can upgrade the software using the GUI. The procedures in this section apply for Cisco APIC releases prior to release 4.x.

Upgrading the Cisco APIC Software Version Using the GUI (Releases Prior to Release 4.x)

Note Please see About Upgrading the Cisco APIC and the Switch Software, on page 21 and the Release Notes for the version to which you are upgrading in order to determine the correct upgrade sequence of the Cisco APIC and the switches.
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.

Step 2
In the **Navigation** pane, click **Controller Firmware**. The current firmware version of the Cisco APIC is displayed in the **Work** pane under **Current Firmware**.

Step 3
Choose **ADMIN > Firmware**, and in the **Navigation** pane, click **Download Tasks**.

Step 4
In the **Work** pane, choose **General > Actions**, and click **Create Outside Firmware source**.

Step 5
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 6
In the **Navigation** pane, click **Download Tasks**. In the **Work** pane, click **Operational** to view the download status of the images.

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

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

Step 7
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.

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 process begins.

   The Cisco APICs are upgraded serially so that the controller cluster is available during the upgrade.

Step 8
Verify the status of the upgrade in the **Work** pane by clicking **Controller Firmware** in the **Navigation** pane.

   **Note**

   The controllers upgrade in random order. Each Cisco APIC takes about ten minutes to upgrade.

   Once a controller image is upgraded, 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. If the cluster does not immediately converge and is not fully fit, the upgrade 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.

   **Note**

   When the Cisco APIC that the browser is connected to is upgraded and it reboots, the browser displays an error message.
Step 9
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 the Leaf and Spine Switch Software Version Using the GUI (Releases Prior to Release 4.x)

Before you begin

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

Procedure

Step 1
On the menu bar, choose ADMIN > Firmware, and in the Navigation pane, click Fabric Node Firmware. In the Work pane, the list of all switches in the fabric are displayed. Also displayed is a status of when the firmware was last upgraded.

Step 2
In the Navigation pane, click Download Tasks.

Step 3
In the Work pane, choose General > Actions, click Create Outside Firmware source, and perform the following actions:

a) In the Source Name field, enter a name for the switch image, for example switch_image.

b) In the Protocol field, click the Secure copy radio button.

Note Depending upon whether you wish to download the software image from an http source or a Secure Copy Protocol (SCP) source, choose the appropriate radio button.

c) In the Url field, enter the URL from where the image must be downloaded.
d) In the Username field, enter your username for secure copy.
e) In the Password field, enter your password for secure copy. Click Submit.

Wait for the switch firmware images to download.

Step 4
In the Navigation pane, click Download Tasks. In the Work pane, click Operational to view the download status of the images.

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

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

Step 5
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 6
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, check the check box.

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

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. 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 to bring down the node to the Graceful Insertion and Removal (GIR) mode before performing the upgrade. See the *Cisco APIC Getting Started Guide, Release 3.x* for information about Graceful Insertion and Removal (GIR) Mode.
j) Click **Submit**.
k) Click **Finish**.

Step 7

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.

Step 8

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 9

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

Step 10

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 simultaneously. 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. In case of any failures, the scheduler pauses and manual intervention is required by the Cisco APIC administrator. The switch upgrade takes up to 12 minutes for each group. The switches will reboot when they upgrade, connectivity drops, and the controllers in the cluster will not communicate for some time with the switches in the group. Once the switches rejoin the cluster after rebooting, you will see all the switches listed under the controller node. If there are any virtual port channel (vPC) configurations in the cluster, the upgrade process will upgrade only one switch at a time out of the two switches in a vPC domain.

Step 11

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 to the new image.
Upgrading the Catalog Software Version Using the GUI (Releases Prior to Release 4.x)

Typically, the catalog image is upgraded when an Cisco APIC image is upgraded. However occasionally, a catalog image must be upgraded by the administrator.

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 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.

Changing the Ignore Compatibility Checks Setting (Releases Prior to Release 4.x)

In APIC, there is a compatibility check feature that verifies if an upgrade path from the currently-running version of the system to a specific newer version is supported or not. There is an "Ignore Compatibility Checks" setting that is set to off by default, so the system automatically checks the compatibility for possible upgrades by default. Follow these procedures if you wish to change the "Ignore Compatibility Checks" setting to on for any reason so that the compatibility check feature is disabled.

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.

Procedure

Step 1
On the menu bar, choose Admin > Firmware.

Step 2
Access the screen that contains the Ignore Compatibility Check feature. For example:

- Under Firmware Management in the left panel, choose Fabric Node Firmware, then right-click on Firmware Groups and choose Create Firmware Group.

- Under Firmware Management in the left panel, right-click on Controller Firmware and choose Controller Upgrade.
Step 3 Make the appropriate selection in the Ignore Compatibility Check field:

- Enter a check mark in the box to enable the Ignore Compatibility Check option (to disable the compatibility check feature so that the system does not check the compatibility for possible upgrades), or
- Remove the check mark from the box (leave the box empty) to disable the Ignore Compatibility Check option (to enable the compatibility check feature so that the system does check the compatibility for possible upgrades).

---

Upgrading the Software Using the GUI (Release 4.x and Later)

You can upgrade the software using the GUI. The procedures in this section apply for Cisco APIC release 4.x and later.

Downloading an Image (Release 4.x and Later)

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 scrollbar 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.
- 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 scrollbar menu, or enter a name for the Cisco APIC image file to create a new download (for example, apic_image).
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. An example URL is
     10.67.82.87:/home/<username>/ACI/aci-apic-dk9.1.0.2j.iso.

   • 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, using the format <SCP 
     server>:/<path>. An example URL is
     10.67.82.87:/home/<username>/ACI/aci-apic-dk9.1.0.2j.iso.

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 User Password.

f) If you selected Use Password, in the Password field, enter your password for secure copy.

g) If you selected Use SSH Public/Private Key Files, enter the following information:

   • SSH Key Contents — The SSH Key Contents is used to create the SSH Key File which is required 
     when creating a Remote location for the download.

     Note The public key is generated at the time of the transfer. After the transfer the key files that 
     were generated in the background are deleted. The temporary key files are stored in 
     dataexport directory of the APIC.

   • SSH Key Passphrase — The SSH Key Passphrase is used to create the SSH Key File which is 
     required when creating a Remote location for the download.

     Note The Passphrase field can remain empty.

h) Click Submit.

   Wait for the Cisco APIC firmware images to download.

Step 4

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

Once 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 the Cisco APIC Software Version Using the GUI (Release 4.x and Later)

See About Upgrading the Cisco APIC and the Switch Software, on page 21 and the Release Notes for the version to which you are upgrading in order to determine the correct upgrade sequence of the Cisco APIC and the switches.

Before you begin

Download an image to use for the upgrade, if necessary, using the procedures provided in Downloading an Image (Release 4.x and Later), on page 32.

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. 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.

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 to occur.

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

Step 4

Verify the status of the upgrade by clicking the Controllers sub-tab again, if necessary, in the Infrastructure pane.
The controllers upgrade in a random order. Each Cisco APIC takes about ten minutes to upgrade. Once a controller image is upgraded, 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. If the cluster does not immediately converge and is not fully fit, the upgrade 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.

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

Step 5
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 the Leaf and Spine Switch Software Version Using the GUI (Release 4.x and Later)

Before you begin

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

- Download an image to use for the upgrade, if necessary, using the procedures provided in Downloading an Image (Release 4.x and Later), on page 32.

- Review the information in Workflow to Upgrade or Downgrade the Cisco ACI Fabric, on page 19 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.

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 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:

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 scroll-down 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 scroll-down 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. Please refer to the **Configuring an Silent Roll Package Upgrade Using the Cisco APIC GUI**, on page 58 section 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, check the check box.

g) Check the **Graceful Maintenance** check box to bring down the node to the Graceful Insertion and Removal (GIR) mode before performing the upgrade.

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 only 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**.

If you select **Schedule for Later**, select the trigger value using the Scheduler scroll-down menu.

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**.

**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 the Nodes in the Upgrade Groups Using the GUI (Release 4.x and Later)

Use these procedures to upgrade the nodes in the firmware upgrade groups. The firmware can be managed for each group separately.

**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 **Infrastructure** tab, then click the **Nodes** sub-tab.

The list of all switches in the fabric are displayed. Also displayed is a status of when the firmware was last upgraded.

**Step 3**

Right-click on a row listed in the **Upgrade Group** column (formerly displayed as POD maintenance group) for the firmware upgrade group that you want to upgrade, then select the appropriate option from the pop-up menu.

- For Release 4.1(2) or later, select **View Upgrade Group** to view or edit an upgrade group.
- For releases prior to 4.1(2), select **Edit Upgrade Group** to view or edit an upgrade group.

**Note** You can also select **Delete Upgrade Group** from the pop-up menu to delete an upgrade group.
A window appears with information on that upgrade group, such as the list of nodes associated with this maintenance group and the maintenance windows for this maintenance group.

**Step 4**

Click **Actions**, then make the appropriate selection from the scroll-down menu:

- **Create One Time Window Trigger**
- **Create Recurring Window Trigger**
- **Upgrade Now**

**Note**

In the **Work** pane, the **Status** displays that all the switches in the group are being upgraded simultaneously. 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. In case of any failures, the scheduler pauses and manual intervention is required by the Cisco APIC administrator. The switch upgrade takes up to 12 minutes for each group. The switches will reboot when they upgrade, connectivity drops, and the controllers in the cluster will not communicate for some time with the switches in the group. Once the switches rejoin the cluster after rebooting, you will see all the switches listed under the controller node. If there are any virtual port channel (vPC) configurations in the cluster, the upgrade process will upgrade only one switch at a time out of the two switches in a vPC domain.

- **Delete Upgrade Group**

---

**Changing the Ignore Compatibility Checks Setting (Release 4.x and Later)**

In APIC, there is a compatibility check feature that verifies if an upgrade path from the currently-running version of the system to a specific newer version is supported or not. There is an "Ignore Compatibility Checks" setting that is set to **off** by default, so the system automatically checks the compatibility for possible upgrades by default. Follow these procedures if you wish to change the "Ignore Compatibility Checks" setting to **on** for any reason so that the compatibility check feature is disabled.

**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.

**Procedure**

**Step 1**
On the menu bar, choose **Admin > Firmware**.

**Step 2**
Access the screen that contains the Ignore Compatibility Check feature. For example:

- Click the **Infrastructure** tab, then click the **Controllers** sub-tab, then click **Action > Schedule Controller Upgrade**.
- Click the **Infrastructure** tab, then click the **Nodes** sub-tab, then click **Action > Schedule Node Upgrade**.

**Step 3**
Make the appropriate selection in the **Ignore Compatibility Check** field:
• Enter a check mark in the box to enable the **Ignore Compatibility Check** option (to disable the compatibility check feature so that the system does not check the compatibility for possible upgrades), or

• Remove the check mark from the box (leave the box empty) to disable the **Ignore Compatibility Check** option (to enable the compatibility check feature so that the system does check the compatibility for possible upgrades).

---

**Upgrading the Software Using the REST API**

You can upgrade the software using the REST API.

**Upgrading 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>
  <firmwareOSourcename="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 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 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>
  </firmwareFwGrp>
  <firmwareRsFwgrpp
    tnFirmwareFwPName="AllswitchesFwP"> 
    </firmwareRsFwgrpp>
  </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>
  </firmwareFwGrp>
  <maintenanceMaintP
    name="AllswitchesMaintP"
    runMode="pauseOnlyOnFailures">
  </maintenanceMaintP>
  <maintenanceMaintGrp
    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>
  </maintenanceMaintGrp>
</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

```xml
<maintMaintP
    name="AllswitchesMaintP" adminSt="triggered"> 
</maintMaintP>
```

The Cisco APICs are upgraded serially so that the controller cluster is available during the upgrade.

---

**Upgrading the Catalog Software Version Using the REST API**

Typically, the catalog image is upgraded when an Cisco APIC image is upgraded. 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

```xml
<firmwareCatFwP
    version="catalog-1.0(1e)" ignoreCompat="yes" />
```

---

**Upgrading the Software Using the CLI**

You can upgrade the software using the CLI.

**Upgrading 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> ./
```
Step 2 Display the repository information.

Example:
```
show firmware repository
```

Step 3 Add the firmware image to the repository.

Example:
```
firmware repository add <name of the image file>
firmware repository add aci-apic-dk9.2.0.1r.iso
```

Step 4 Configure the controllers for upgrade.

Example:
```
apic1(config)# firmware
apic1(config-firmware)# controller-group
apic1(config-firmware-controller)# firmware-version <name of the image file>
apic1(config-firmware-controller)# firmware-version aci-apic-dk9.2.2.2e.bin
```

Step 5 Upgrade the controller.

Example:
```
apic1# firmware upgrade controller-group
```

The Cisco APICs are upgraded serially so that the controller cluster is available during the upgrade. The upgrade occurs in the background.

Step 6 Verify the upgrade for the controller.

Example:
```
apic1# show firmware upgrade status
Pod   Node   Current-Firmware     Target-Firmware   Status
      Upgradable-Progress(%)  
---------- ---------- ------------------- ------------ ---------------
1         1         apic-2.3(0.376a)         n9000-12.3(0.102)          upgrade in progress
1         2         apic-2.3(0.376a)         n9000-12.3(0.102)          success
1         3         apic-2.3(0.376a)         n9000-12.3(0.102)          success
1         101      n9000-12.3(0.100)         n9000-12.3(0.102)          success
1         102      n9000-12.3(0.100)         n9000-12.3(0.102)          success
1         103      n9000-12.3(0.100)         n9000-12.3(0.102)          upgrade in progress
1         104      n9000-12.3(0.100)         n9000-12.3(0.102)          success
1         201      n9000-12.3(0.100)         n9000-12.3(0.102)          success
1         202      n9000-12.3(0.100)         n9000-12.3(0.102)          success
```

apic1#
Upgrading 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>@<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 repository information.

**Example:**

```
show firmware repository
```

**Step 3** Add the firmware image to the repository.

**Example:**

```
firmware repository add <name of the image file>
firmware repository add aci-apic-dk9.2.0.1r.iso
```

**Step 4** Configure the switch group for upgrade.

**Example:**

```
apic1(config)# firmware
apic1(config-firmware)# switch-group <name of the switch group>
apic1(config-firmware-switch)# switch 101-104,201,202
apic1(config-firmware-switch)# firmware-version aci-n9000-dk9.12.2.2e.bin
```

**Step 5** Upgrade the switch group.

**Example:**

```
apic1# firmware upgrade switch-group <name of the switch group>
```

**Step 6** Verify the upgrade status for the switch group.

**Example:**

```
apic1# show firmware upgrade status
            Pod  Node  Current-Firmware  Target-Firmware  Status
            Upgrad-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
```
Upgrading the Catalog Software Version Using the NX-OS Style CLI

By default, upgrading the controllers automatically upgrades 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#

Upgrading the Controller Using the Debug CLI

If you want to install a new Cisco APIC firmware image that is not compatible with the running firmware image, you can upgrade using the debug CLI.

**Note**  
These procedures remove all previous user data from this Cisco APIC. The controller may retrieve data from other controllers in the cluster, if it is part of a cluster.
Upgrading the Controller Using the Debug CLI in Three Steps

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Log in to the Cisco APIC as admin.</td>
</tr>
</tbody>
</table>
| **Step 2** | Clear the user data from the Cisco APIC.  
**Example:**
admin@apic1:~> acidiag touch clean |
| **Step 3** | Install the image on the Cisco APIC.  
**Example:**
admin@apic1:~> acidiag install http://<ip>/<ver-no> |
| **Step 4** | Reboot the Cisco APIC.  
**Example:**
admin@apic1:~> acidiag reboot |

Verifying the Firmware Version and the Upgrade Status Using the API

<table>
<thead>
<tr>
<th>Verification Description</th>
<th>Example URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>For the current running firmware version on controllers</td>
<td>GET URL: https://&lt;ip address&gt;/api/node/class/firmwareCtrlrRunning.xml</td>
</tr>
<tr>
<td>For the currently operating firmware version on switches</td>
<td>GET URL: https://&lt;ip address&gt;/api/node/class/firmwareRunning.xml</td>
</tr>
<tr>
<td>For the upgrade status of controllers and switches</td>
<td>GET URL: https://&lt;ip address&gt;/api/node/class/maintUpgJob.xml</td>
</tr>
</tbody>
</table>

Verifying SSD Installation Status

Use this procedure to verify if the Cisco APIC has SSD installed.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Log in to the Cisco APIC as an admin user.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enter the command **acidiag hwcheck</td>
</tr>
</tbody>
</table>
admin@APIC1:~> acidiag hwcheck | grep -A 6 "Physical Disk /dev devices".

Disk /dev/sda: 999.0 GB, 998999326720 bytes, 1951170560 sectors
Disk /dev/sdb: 119.5 GB, 119453777920 bytes, 233308160 sectors
Disk /dev/sdc: 4009 MB, 4009754624 bytes, 7831552 sectors
Disk /dev/mapper/vg_ifc0_ssd-data: 113.8 GB, 113816633344 bytes, 222298112 sectors

admin@APIC1:~>

Step 3 Log in to CIMC.
Step 4 Choose Storage > Physical Drive Info.
Step 5 Verify if the SSD is installed.

Troubleshooting Failures During the Upgrade Process

There is one scheduler per maintenance policy. By default, when an upgrade 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. Once manual intervention is complete, you must resume the paused scheduler.

If you notice that switches are in “queued” state, then check the following:

• Is controller cluster healthy? 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 “queued” state.

• Is the switch maintenance group paused? The group will be paused if any switch fails its upgrade.

If the system takes longer than about 60 minutes for switch to display “waitingForClusterHealth = no” in the API or "Waiting for Cluster Convergence" showing "No" in the GUI, you should work through the steps about verifying a pause in the scheduler.

Common Reasons for Download Failure

Some common reasons for download failure are as follows:

• Insufficient permissions
• Directory or file not found
• Directory full on destination
• Request timeout / download did not complete in acceptable amount of time
• Server error / unknown server error
• Invalid Ack
• Username / password authentication issues

Follow one of the procedures for resuming the download.
Verifying Cluster Convergence

You verify the cluster convergence using the GUI.

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.

Note

You must have divided your switches into two groups for the upgrades to be successful. By default, the system upgrades 20 switches at a time; you can change this number.

As the controller and switches move through the upgrade, you will see messages about the number of nodes queued and the number in the process of upgrading, as well as how many have upgraded successfully.

The following are the possible upgrade states for a node:

• NotScheduled: No upgrade is currently scheduled for this node.
• Scheduled: Upgrade is scheduled for this node.
• Queued: There is a currently active window (schedule) and the node is requesting permission to upgrade.
• Inprogress: Upgrade is currently in progress on this node.
• CompleteOK: Upgrade completed successfully.
• CompleteNOK: Upgrade failed on this node.
• Inretryqueue: Node is queued again for upgrade retry (five attempts are made before declaring failure).

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 That the Controller Upgrade Paused

You can verify that the controller upgrade paused using either the GUI or the REST API.

Using the GUI to Verify Whether a Controller Upgrade Scheduler Paused

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>On the menu bar, choose ADMIN &gt; Firmware.</td>
</tr>
<tr>
<td>Step 2</td>
<td>In the Navigation pane, expand Fabric Node Firmware &gt; Controller Firmware.</td>
</tr>
<tr>
<td>Step 3</td>
<td>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.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Identify the problem and fix this problem.</td>
</tr>
</tbody>
</table>
**Using the REST API to Verify Whether a Controller Upgrade 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
<?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="2014-08-28T14:45:24.232-07:00"
        polName="nowgrp" runStatus="running" status="" uid="0"
        waitOnClusterHealth="no" windowName=""/>
</imdata>
```

**Verifying That the Switch Upgrade Paused**

You can verify that the switches upgrade paused using either the GUI or the REST API.

**Using the GUI to Verify Whether a Switch Upgrade Scheduler Paused**

**Procedure**

1. **Step 1** On the menu bar, choose **ADMIN > Firmware**.
2. **Step 2** In the Navigation pane, expand **Fabric Node Firmware > Maintenance Groups**.
3. **Step 3** Expand the **Maintenance Groups**, and click on **All Switches**.
4. **Step 4** In the **Work** pane, look to see if the **Scheduler Status** reads **Paused**.
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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>On the menu bar, choose <strong>ADMIN &gt; Firmware</strong>.</td>
</tr>
<tr>
<td>2</td>
<td>In the <strong>Navigation</strong> pane, expand <strong>Fabric Node Firmware &gt; Controller Firmware</strong>.</td>
</tr>
<tr>
<td>3</td>
<td>In the <strong>Work</strong> pane, click the <strong>Policy</strong> tab.</td>
</tr>
<tr>
<td>4</td>
<td>In the <strong>Controller Maintenance Policy</strong> area, verify that the <strong>Running Status</strong> field displays <strong>Paused</strong>.</td>
</tr>
<tr>
<td>5</td>
<td>Click the <strong>Actions</strong> tab, and click <strong>Resume Upgrade Scheduler</strong>.</td>
</tr>
<tr>
<td>6</td>
<td>Click the <strong>Actions</strong> tab, and choose <strong>Upgrade Controller Firmware Policy</strong> from the drop-down list.</td>
</tr>
<tr>
<td>7</td>
<td>Click the <strong>Actions</strong> tab, and choose <strong>Apply Now</strong> from the drop-down list.</td>
</tr>
</tbody>
</table>

Using the REST API to Resume Paused Controller Upgrade Scheduler

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Post the following API to resume a paused scheduler for a controller maintenance policy.</td>
</tr>
<tr>
<td></td>
<td>In this example, the maintenance policy is ConstCtrlrMaintP.</td>
</tr>
</tbody>
</table>

**Example:**

```xml
URL: https://<ip address>/api/node/mo.xml
<maintUpgStatusCont>
   <maintUpgStatus polName="ConstCtrlrMaintP" status="deleted" />  
</maintUpgStatusCont>
```

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Use the REST API that you used initially to upgrade the Cisco APIC controller software.</td>
</tr>
</tbody>
</table>

Resuming a Paused Scheduler for a Switch Maintenance Policy

Using the GUI to Resume Paused Switch Upgrade Scheduler

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>On the menu bar, choose <strong>ADMIN &gt; Firmware</strong>.</td>
</tr>
<tr>
<td>2</td>
<td>In the <strong>Navigation</strong> pane, expand <strong>Fabric Node Firmware &gt; Maintenance Groups &gt; maintenance_group_name</strong>.</td>
</tr>
<tr>
<td>3</td>
<td>In the <strong>Work</strong> pane, click the <strong>Policy</strong> tab.</td>
</tr>
<tr>
<td>4</td>
<td>In the <strong>Maintenance Policy</strong> area, verify that the <strong>Running Status</strong> field displays <strong>Paused</strong>.</td>
</tr>
</tbody>
</table>
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.

Performing a Clean Reboot

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.

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 using the following commands:

**Example:**

```
/bin/setup-clean-config.sh
vsh-c reload
```

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

**Example:**

```
acidiag touch clean
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 or register the switches using the UI.

---

**Upgrading with Shared Layer 3 Out**

The shared Layer 3 Out feature was introduced in the 1.2(1i) release. This section provides limitations and behaviors encountered when upgrading from an unsupported release.

**Upgrading the Cisco APIC before the Leaf Switches**

The shared Layer 3 Out feature is not enabled automatically after upgrading, so upgrading the Cisco APIC first should be harmless and will not cause a change in behavior. Because the leaf switches are still running the old image, the leaf switches will not program external prefixes in the other VRF. Shared Layer 3 Out traffic will not work unless the leaf switches are upgraded to a new image and external prefixes are properly marked as shared.

Below is a list of scenarios and expected behaviors when upgrading the leaf switches after the Cisco APIC:

- In a scenario where the Provider leaf switch is an Application EPG and the Consumer leaf switch is an L3Out, the order the leaf switches are upgraded does not matter. The shared Layer 3 Out feature will not work because the L3Out prefixes are marked as shared and no prefix entries are created in the Provider's VRF. After both leaf switches are upgraded, you must mark the prefixes to be shared with appropriate "scope" flags. This will leak external prefixes in the Provider VRF and also create acctl:PfxEntry. The shared Layer 3 Out feature should start working.

- In a scenario where the Provider leaf switch is an L3Out and the Consumer leaf switch is an Application EPG, the order the leaf switches are upgraded does not matter. The shared Layer 3 Out feature will not work because the L3Out prefixes are marked as shared and no prefix entries are created in the Provider's VRF. After both leaf switches are upgraded, you must mark the prefixes to be shared with appropriate "scope" flags. This will leak external prefixes in the Provider VRF and also create acctl:PfxEntry. The shared Layer 3 Out feature should start working.

- In a scenario where the Provider and Consumer are both L3Outs, the order the leaf switches are upgraded does not matter. The shared Layer 3 Out feature will not work because no L3Out prefixes are marked as shared in either the Provider or Consumer L3Outs. No prefix entries are created in the Provider's VRF for the Consumer's external prefixes, and no prefix entries are created in the Consumer's VRF for the Provider's external prefixes. After both leaf switches are upgraded, you must mark the prefixes to be shared with appropriate "scope" flags. This will leak external prefixes in the Provider VRF and also create acctl:PfxEntry. The shared Layer 3 Out feature should start working.

**Upgrading the Leaf Switches Before the Cisco APIC**

The shared Layer 3 Out feature is not enabled automatically after upgrading, so upgrading the leaf switches first should be harmless and will not cause a change in behavior.
After the Cisco APIC and Leaf Switches are Upgraded

All the leaf switches and Cisco APICs involved in the shared service with Layer 3 Outside must be upgraded to the release supporting the shared Layer 3 Out feature. After upgrading, for the subnets you want to share across private networks, put the following flags on the external subnet (represented by model class l3ext:Subnet) will leak subnets:

- For leaking the route in the other private network, add the "shared-rtctrl" bit to the "scope" property of the subnet.
- For enabling security on the route in the other private network, add the "shared-security" bit in the "scope" property of the subnet.

Downgrading with Shared Layer 3 Out

The shared Layer 3 Out feature was introduced in the 1.2(1i) release. This section provides limitations and behaviors encountered when downgrading to an unsupported release.

Downgrading the Cisco APIC Before the Leaf Switches

After downgrading the Cisco APIC, the system will automatically remove the bits used for enabling shared service from the external subnet's "scope" property. Leaf switches running the new image will get this change notification and will stop sharing those subnets. External network instance profiles (represented by model class l3ext:InstP), which are acting as contract consumers of a cross VRF contract, will get a local class Id. This will result in traffic flap for its existing communications.

Downgrading the Leaf Switches Before the Cisco APIC

Once the leaf switch is downgraded, it will stop getting external subnets that are only marked with "shared-rtctrl" or "shared-security." If the scope property also has other bits set, then the old behavior corresponding to those bits will follow. External network instance profiles (represented by model class l3ext:InstP), which are acting as contract consumers of a cross VRF contract, will get a local class Id. This will result in traffic flap for its existing communications.

Recommended Downgrade

Before a leaf switch is downgraded to an image that does not support the shared Layer 3 Out feature, it is recommended that you uncheck the bits used for shared service from the eternal subnets deployed on that leaf switch. However, even this recommended approach cannot avoid the traffic flap for the External Instance Profiles, which are acting as contract consumers of a cross VRF contract.

Network Configuration Capabilities and Changes During Mixed OS Operation

Starting from Release 2.2(1n), Cisco Application Policy Infrastructure Controller supports the following features for network configuration capabilities and changes during mixed OS operation.
Starting from Release 2.3(1), Cisco Application Policy Infrastructure Controller supports the following features in addition to the ones listed above for network configuration capabilities and changes during mixed OS operation.

Table 4: Supported Features for Network Configuration Capabilities and Changes During Mixed OS Operation

<table>
<thead>
<tr>
<th>Features</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contracts</td>
<td>• Create, update, and delete filters, subjects, and contracts.</td>
</tr>
<tr>
<td></td>
<td>• Export and import contracts.</td>
</tr>
<tr>
<td>Endpoint group</td>
<td>• Add and delete provided and consumed contracts in relationship with EPGs.</td>
</tr>
<tr>
<td>Microsegmentation</td>
<td>• Add and delete EPGs.</td>
</tr>
<tr>
<td>vMotion</td>
<td>• Add and delete VMM, physical, L2 external, and L3 external domain association.</td>
</tr>
<tr>
<td>VM operation</td>
<td>• Add, delete, and update static port assignment and statically link with the node.</td>
</tr>
<tr>
<td>Bridge domain</td>
<td>• Create an end point from one EPG to another EPG.</td>
</tr>
<tr>
<td></td>
<td>• Move an end point from uSeg EPG to base EPG.</td>
</tr>
<tr>
<td></td>
<td>Add and update uSeg EPG.</td>
</tr>
</tbody>
</table>

vMotion across leaf switch.
On and Off of virtual machines.
Create, update, and delete bridge domains.
<table>
<thead>
<tr>
<th>Features</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMM Domain</td>
<td>The following operations are supported only in VMware vDS and Cisco AVS.</td>
</tr>
<tr>
<td></td>
<td>• Create and delete VMM domains.</td>
</tr>
<tr>
<td></td>
<td>• Add and update VLAN pools.</td>
</tr>
<tr>
<td></td>
<td>• Add and delete multicast pools.</td>
</tr>
<tr>
<td></td>
<td>• Add and update VMware vCenter.</td>
</tr>
<tr>
<td></td>
<td>• Add and update vSwitch policies.</td>
</tr>
<tr>
<td>Layer 2 or Layer 3 Out</td>
<td>Add, update, and delete L2 external and L3 external domains.</td>
</tr>
<tr>
<td>Access Policy</td>
<td>• Add, update, and delete switch policies, interface policies, policy group, Attached Entity Profiles (AEP).</td>
</tr>
<tr>
<td>Troubleshooting</td>
<td>• Add, update, and delete SPAN configuration.</td>
</tr>
<tr>
<td></td>
<td>• Add, update, and delete syslog server.</td>
</tr>
<tr>
<td>Physical network</td>
<td>• Enable and disable port status.</td>
</tr>
<tr>
<td></td>
<td>• ON and OFF of a physical server.</td>
</tr>
<tr>
<td></td>
<td>• Move physical server within and across leaf switches.</td>
</tr>
<tr>
<td></td>
<td>• Reloading spine switches and leaf switches.</td>
</tr>
<tr>
<td></td>
<td>• Reloading spine switch LC card, FC card, CS card, and SUP card.</td>
</tr>
<tr>
<td></td>
<td>• Decommissioning spine switches and leaf switches.</td>
</tr>
<tr>
<td></td>
<td>• Adding and deleting virtual port channel (vP) domain.</td>
</tr>
<tr>
<td></td>
<td>• Flap primary link, secondary link, and all the links in the virtual port channel (vPC).</td>
</tr>
<tr>
<td></td>
<td>• Flap all the port channel links, flap one link in the port channel, flap NIF ports on FEX, and flap front panel ports on Top of Rack.</td>
</tr>
<tr>
<td>Fabric Policy</td>
<td>• Add, update, and delete NTP server, SNMP, BGP route reflector, L2 MTU policy.</td>
</tr>
<tr>
<td></td>
<td>• Update Cisco APIC connectivity preferences.</td>
</tr>
</tbody>
</table>
Prior to the 3.0 release, mixed OS operation displays a red banner warning, informing you that mixed OS is present in the fabric. After the 3.0 release, this warning banner has been removed.

**Important Notes**

- It is required that all the Cisco APICs must be first upgraded to the newer version and after the upgrade is completed, the supported network configuration operations may be performed. The supported network configuration operations cannot be performed during an upgrade of an Cisco APIC.

- Network configuration capabilities and changes during an upgrade are only supported at the node level. For a vPC pair, both of the switches participating in the vPC pair must have the same version.

- All physical network device related triggers such as changing the port status, connecting disconnecting servers to an existing fabric switch or a Cisco APIC on a fabric is supported.

- For the supported network triggers starting from Release 2.3(1), see Table 4: Supported Features for Network Configuration Capabilities and Changes During Mixed OS Operation, on page 54.

**Compatibility Information**

**Table 5: Compatibility Information**

<table>
<thead>
<tr>
<th>Description</th>
<th>Cisco APIC Release</th>
</tr>
</thead>
</table>
| The supported modifications mentioned in Important Notes, on page 56 during an upgrade to Release 2.2(1n) is supported for the following Cisco APIC releases: | • Release 2.1(1h)  
  • Release 2.0(2m) |
| The supported modifications mentioned in the table Table 4: Supported Features for Network Configuration Capabilities and Changes During Mixed OS Operation, on page 54 during an upgrade to Release 2.3(1) is supported for the following Cisco APIC releases: | • Release 2.2(2k) |
| **Note** The network configuration capabilities and changes during mixed OS operation support is only applicable for features available till release 2.1(1h). | |
| The supported modifications mentioned in the table Table 4: Supported Features for Network Configuration Capabilities and Changes During Mixed OS Operation, on page 54 during an upgrade to Release 3.0(1) is supported for the following Cisco APIC releases: | • Release 2.3(1f)  
  • Release 2.2(2k) |
| **Note** The network configuration capabilities and changes during mixed OS operation support is only applicable for features available till release 2.2(2k). | |
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 release 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 release include 2.0(1m) and 2.0(2f).
- A Cisco APIC patch release contains fixes for specific defects. Examples of patch release include 2.1(1h) and 2.1(1i).

The following table lists the network configuration capabilities and changes supported during an upgrade.

<table>
<thead>
<tr>
<th>Upgrade Path</th>
<th>Example</th>
<th>Supported Network Configuration Capabilities and Changes</th>
</tr>
</thead>
</table>
| Upgrade from one major release to another major release | Release 2.0(1) to Release 2.2(1) | • Physical network configuration change is supported.  
                                          |                          | • Policy change is not supported.                     |
| Upgrade from one major release to another minor or maintenance release | Release 2.0(1) to Release 2.0(2)  
                                          | Release 2.1(1) to Release 2.1(2) | • Physical network configuration change is supported.  
                                          |                          | • Policy change is not supported.                     |
| Upgrade from one major release to another major patch release | Release 2.0(1m) to Release 2.0(1n) | • Physical network configuration change is supported.  
                                          |                          | • Policy change is supported for features introduced prior to the major release. |

**About the Silent Roll Package Upgrade**

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 2 switches:

- N9K-C93216TC-FX2
- N9K-C93360YC-FX2
Configuring an Silent Roll Package Upgrade Using the Cisco APIC GUI

Before you begin

• Wait until all the controllers are upgraded to the new firmware version before proceeding to upgrade 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 an Image (Release 4.x and Later), on page 32.

• Review the information in Workflow to Upgrade or Downgrade the Cisco ACI Fabric, on page 19 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 an Silent Roll Package Upgrade Using the CLI

This section demonstrates how to configure and unconfigure an SR package upgrade and how to trigger the upgrade after configuring the SR package upgrade and SR package version using the CLI.

For more information about SR package upgrades, see *About the Silent Roll Package Upgrade, on page 57.*

#### 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
```
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
```

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 an Silent Roll Package Upgrade Using the REST API

This section demonstrates how to configure an SR package upgrade using the REST API.

For more information about SR package upgrades, see [About the Silent Roll Package Upgrade, on page 57](#).

#### 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>
```
Cisco Nexus 9300 Platform Switches to Cisco Nexus 9300-EX Platform Switches Migration

Use this procedure to migrate Cisco Nexus 9300 platform switches in virtual port channel (vPC) to Cisco Nexus 9300-EX platform switches.

**Procedure**

**Step 1** Remove the cables from Cisco Nexus 9300 platform switch. Power off the switch.

**Step 2** Log in to Cisco APIC.

**Step 3** Choose Fabric > Inventory > Unreachable Nodes.

Ensure that the node is unreachable. Make a note of the Node Name and Node ID.

**Step 4** Select the node. From the Actions menu, choose Remove From Controller.

Wait for 5-10 minutes for the node to be removed from the Cisco APIC.

**Step 5** Monitor the traffic on Cisco Nexus 9300 platform switch. All the traffic should be handled by the other Cisco Nexus 9300 platform switch and there should be minimal or no impact to traffic.

**Step 6** Replace Cisco Nexus 9300 platform switch with Cisco Nexus 9300-EX platform switch.

**Step 7** Power on Cisco Nexus 9300-EX platform switch and connect the cables.

**Step 8** Load the Cisco APIC Release 3.0(1) software on Cisco Nexus 9300-EX platform switch. Boot the switch.

**Step 9** Log in to Cisco APIC.

**Step 10** Choose Fabric > Inventory > Fabric Membership.

Verify if the switch is displayed.

**Step 11** Assign the Node Name and Node ID from step 3 to Cisco Nexus 9300-EX platform switch.

**Step 12** Wait for a few minutes for all the relevant policies to be pushed to the Cisco Nexus 9300-EX platform switch and for the end point synchronization to complete. To verify, choose Operations > Capacity Dashboard. Port channel on this switch is not activated.

**Step 13** Remove the cables from the other Cisco Nexus 9300 platform switch. Power off the switch.

**Step 14** Repeat the steps 1-12 for the other Cisco Nexus 9300 platform switch.
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
(aall 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
(aall 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" />
<firmwareRsFwGrp tnFirmwareFwPName="AllswitchesFwP" />
</firmwareFwGrp>

**Switch Firmware Firmware Policy – Set desired version**

POST URL: http://trunk6-ifc1/api/node/mo/uni/fabric.xml
<br/>&lt;firmwareFwP name="AllswitchesFwP" version="n9000-11.0(0.775)" ignoreCompat="true"&gt;

</firmwareFwP>

**Switch Maintenance Group – Group of switches with same maintenance policy**

POST URL: http://trunk6-ifc1/api/node/mo/uni/fabric.xml
<br/>&lt;maintMaintGrp name="AllswitchesMaintGrp"&gt;
<br/>&lt;fabricNodeBlk name="Blk101to104" from_="101" to_="104" /&gt;
<br/>&lt;maintRsMgrpp tnMaintMaintPName="AllswitchesMaintP" /&gt;

</maintMaintGrp>

**Switch Maintenance Policy – Setup schedule for maintenance**

POST URL: http://trunk6-ifc1/api/node/mo/uni/fabric.xml
<br/>&lt;maintMaintP name="AllswitchesMaintP" runMode="pauseOnlyOnFailures"&gt;

</maintMaintP>

**Trigger upgrade on Maintenance Group – starting now**

POST URL: http://trunk6-ifc1/api/node/mo/uni/fabric.xml
<br/>&lt;maintMaintP name="AllswitchesMaintP" adminSt="triggered"&gt;

</maintMaintP>

**Get current running version on switches**

(all switches) GET URL: http://trunk6-ifc1.insieme.local/api/node/class/firmwareRunning.xml
<br/>(a switch) GET URL: http://trunk6-ifc1.insieme.local/api/node/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
<br/>(a switch) GET URL: http://trunk6-ifc1.insieme.local/api/node/topology/pod-1/node-101/sys/fwstatuscont/upgjob.xml