Cisco ACI Releases Changes in Behavior

Introduction

This document describes the changes in behavior for the Cisco Application Policy Infrastructure Controller (APIC) and Cisco Nexus 9000 ACI-Mode Switches software for all active releases.

Date	Description
August 13, 2025	Added the ACI 6.1(4) release.
April 4, 2025	Added the ACI 6.1(3) release.
December 13, 2024	For the ACI 6.1(2) release, added a change related to the SNMP daemon functionality.
December 4, 2024	Added the ACI 6.1(2) release.
November 4, 2024	Added the "ACI release post-6.1(1) deprecated features" section. This section was later renamed to "ACI release 6.1(2) deprecated features".
October 29, 2024	Added the ACI 6.0(8) release.
September 24, 2024	For the ACI 6.1(1) release, added that the **Security** object is no longer in a tenant's navigation pane.
August 29, 2024	Added the ACI 6.0(7) release.
August 1, 2024	Added the ACI 6.1(1) release.
June 28, 2024	Added the ACI 6.0(6) release.
June 14, 2024	For the ACI 6.0(3) release, added a change related to the **show interface** command.
May 21, 2024	For the ACI 5.2(3) release, added an upgrade/downgrade change.
March 11, 2024	This document was created.

ACI release 6.1(4)

Table 1 Cisco APIC release 6.1(4) changes in behavior

Product Impact	Description
N/A	There are no changes in behavior.

Table 2 Cisco Nexus 9000 ACI-Mode Switches release 16.1(4) changes in behavior

Product Impact	Description
N/A	There are no changes in behavior.

ACI release 6.1(3)

Table 3 Cisco APIC release 6.1(3) changes in behavior

Product Impact	Description
Security	While configuring a local user using the GUI, the password must meet additional requirements. You can configure the password strength parameters by either creating Custom Conditions or by selecting the Default Three Conditions, which include lowercase letters, digits, and special characters. For more information, see the Cisco APIC Basic Configuration Guide, Release 6.1(x).
Security	ACI-mode switches will support rsa-sha2 only (512 or 256). Upgrade the SSH client to a version above OpenSSH 7.2.

Table 4 Cisco Nexus 9000 ACI-Mode Switches release 16.1(3) changes in behavior

Product Impact	Description
Base Functionality	Switch hardware ID information has been modified, earlier N9K-C9400-SW-GX2A represented the N9K-C9408 switch. It has now been corrected to represent the actual switch ID information, which is the N9K-C9408 switch. If a N9K-C9400-SW-GX2A chassis is already registered with an ACI Fabric, complete the following steps after upgrading to release 6.1(3): (After the switch upgrade to 6.1(3), the node is displayed as inactive and the existing N9K-C9408 switch (which was earlier indicated as N9K-C9400-SW-GX2A) will appear as a new node pending registration.) 1. Decommission the old node. 2. Register the new node. If the node ID is the same as before, the existing configuration is applied. 3. After the node is registered, it will become *active* with the expected model and serial number.

ACI release 6.1(2)

Table 5 Cisco APIC release 6.1(2) changes in behavior

Product Impact	Description
Base Functionality	SNMP daemon will not start during the APIC bring up. It will start when the user attaches the SNMP policy to the pod profile policy and configures `adminSt` as "Enabled" . Similarly, it will stop when the user either configures `adminSt` as "Disabled" or removes the SNMP policy from the pod-profile policy. This behaviour is also applicable to the SNMP trap daemon. Hence, the SNMP trap aggregation feature relies on the SNMP policy admin state. For SNMP trap aggregation to work, add all the APICs as the trap forwarding destinations.
Base Functionality	The **show running config** command is not available for all operations. Use relevant show commands and debug commands.
Upgrade/Downgrade	Enable the global AES encryption check-box before you upgrade to the latest image. This includes a pre-validation check to ensure that Global AES encryption is enabled prior to proceeding with the upgrade.

Product Impact	Description
	See the [Cisco APIC Installation and ACI Upgrade and Downgrade Guide](#) for details.

Deprecated Features	Deprecated features for Cisco APIC release 6.1(2):
	
	• Atomic counters and latency: For information about atomic counters, see the [Cisco Application Centric Infrastructure Fundamentals, Release 6.1(x)](#)
	
	• Cisco ACI App Center: Cisco ACI App Center [applications](#) are no longer supported in Cisco APIC. These Cisco-authored apps are native functionality of Cisco APIC in this release:
	  ◦ Upgrade Validator
	  ◦ DC Connector
	  ◦ ELAM Assistant
	For information about the Cisco ACI App Center, see the [Cisco ACI App Center User Guide](#).
	
	• Cisco APIC NX-OS-style configuration mode CLI: The configuration mode of the Cisco APIC NX-OS-style CLI is no longer supported. Other functionality on the APIC CLI such as the EXEC mode and UNIX CLI are still available.
	For information about the NX-OS-style CLI, see the [Cisco APIC NX-OS Style CLI Configuration Guide, Release 4.2(x) and Later](#).
	
	• Cisco UCS Manager integration with the External Switch app: Due to the deprecation of Cisco ACI App Center, the integration of Cisco UCS Manager (UCSM) with the External Switch app, which is an App Center application, is also deprecated.
	For information about the integration, see the [Cisco ACI Virtualization Guide, Release 6.1(x)](#).
	
	• VMM integration for Cloud Foundry: For information about VMM integration for Cloud Foundry, see the [Cisco ACI and Cloud Foundry Integration](#)
	
	• VMM integration for Microsoft Windows Azure Pack: For information about VMM integration for Microsoft Windows Azure Pack, see the [Cisco ACI Virtualization Guide, Release 6.1(x)](#).
	
	• VMM integration for Red Hat Virtualization: For information about VMM integration for Red Hat Virtualization, see the [Cisco ACI and Red Hat Virtualization](#).
	
	• VMM integration for SCVMM: For information about VMM integration for SCVMM, see the [Cisco ACI Virtualization Guide, Release 6.1(x)](#).
	
	• ACI and SD-WAN Integration: For information about VMM integration for SDWAN, see the [Cisco ACI and SDWAN Integration](#)

Table 6 Cisco Nexus 9000 ACI-Mode Switches release 16.1(2) changes in behavior

Product Impact	Description
N/A	There are no changes in behavior.

ACI release 6.1(1)

Table 7 Cisco APIC release 6.1(1) changes in behavior

Product Impact	Description
Base Functionality	Custom BGP timers are now applied to infra L3Outs.
Base Functionality	On the **Fabric > Access Policies > Interface Configuration** screen, the table now has a **Port Type** column that specifies whether the node is a leaf or spine, and whether the ports are access or fabric. In previous releases, the **Port Mode** column included this information.
Base Functionality	On the **Fabric > Access Policies > Interface Configuration** screen, when you try to edit a multi-node interface, the GUI displays following warning: Unable to edit the configuration of interface {id} on Node {node} since the interface is currently configured via a user-configured switch profile which contains multiple nodes ({nodes}). Please migrate the configuration of interface {id} on all nodes that are part of the switch profile to the new configuration method with this table first by selecting interface {id} on all the corresponding nodes ({nodes}), clicking on Actions -> Configure Interfaces, then Save with the same parameters. In previous releases, the warning was not as informative.
Base Functionality	Ongoing atomic counters are now disabled by default.
Base Functionality	Tag matching is now supported in tenant common and in endpoint security groups in user-created tenants.
Base Functionality	The "Enforce Subnet Check" feature is now enabled by default for new Cisco APIC deployments and clean reloads of an APIC.
Base Functionality	You can configure vzAny as a shared service provider only for contracts with the scope "shared service." In previous releases, you could configure vzAny as a shared service provider for contracts with policy-based redirect.
Security	The Cisco APIC cluster's default security mode is now "strict."
Upgrade/Downgrade	The Cisco APIC upgrade is shown as completed only after the post upgrade activities are completed. The upgrade status is shown as "Post Upgrade Pending" when the post upgrade activities are either pending or in progress and will change to "Completed" after the post upgrade activities are done. Prior to Cisco APIC 6.1(1), the Cisco APIC cluster upgrade or downgrade time was in the range of 90 to 130 minutes. Beginning with Cisco APIC 6.1(1), the APIC cluster upgrade or downgrade takes 40 to 60 minutes longer.
Deprecated feature(s)	Deprecated feature(s) for Cisco APIC release 6.1(1): Security tab: This is the **System > Security** page in the Cisco APIC GUI, which shows the detailed contract resolutions.

Table 8 Cisco Nexus 9000 ACI-Mode Switches release 16.1(1) changes in behavior

Product Impact	Description
Base Functionality	The global MSS configuration is now applied only to leaf switches. Spine switches will always have the default configuration and be disabled. In previous releases, the global MSS configuration was applied on both leaf and spine switches.

Product Impact	Description
Base Functionality	The N9K-C93180LC-EX leaf switch is no longer supported. These fabric extenders are no longer supported: • N2K-C2332TQ-10GT • N2K-C2348TQ-10GE • N2K-C2232PP-10GE • N2K-C2232TM-E-10GE • N2K-C2348TQ-10G-E These supervisors are no longer supported: • N9K-SUP-A • N9K-SUP-B
Base Functionality	When a leaf switch receives multiple adjacencies over the same port, a fabricLooseNode entry is created for each adjacency. In previous releases, a fabricLooseNode entry was created for only one of the adjacencies.
Base Functionality	When NTP is disabled, the "show ntp" commands now display "NTP is already disabled". In previous releases, the commands displayed peer information.

ACI release 6.0(9)

Table 9 Cisco APIC release 6.0(9) changes in behavior

Product Impact	Description
N/A	There are no changes in behavior.

Table 10 Cisco Nexus 9000 ACI-Mode Switches release 16.0(9) changes in behavior

Product Impact	Description
N/A	There are no changes in behavior.

ACI release 6.0(8)

Table 11 Cisco APIC release 6.0(8) changes in behavior

Product Impact	Description
N/A	There are no changes in behavior.

Table 12 Cisco Nexus 9000 ACI-Mode Switches release 16.0(8) changes in behavior

Product Impact	Description
N/A	There are no changes in behavior.

ACI release 6.0(7)

Table 13 Cisco APIC release 6.0(7) changes in behavior

Product Impact	Description
N/A	There are no changes in behavior.

Table 14 Cisco Nexus 9000 ACI-Mode Switches release 16.0(7) changes in behavior

Product Impact	Description
N/A	There are no changes in behavior.

ACI release 6.0(6)

Table 15 Cisco APIC release 6.0(6) changes in behavior

Product Impact	Description
Deprecated feature(s)	Deprecated features for Cisco APIC release 6.0(6): • CloudSec Encryption: For information about CloudSec encryption, see the Nexus Dashboard Orchestrator CloudSec Encryption for ACI Fabrics, Release 4.3.x • Cisco ACI vRealize 8 plug-in; For information about the Cisco ACI vRealize 8 plug-in, see the Cisco ACI vRealize 8 Plug-in Guide

Table 16 Cisco Nexus 9000 ACI-Mode Switches release 16.0(6) changes in behavior

Product Impact	Description
Upgrade/Downgrade	When you upgrade to the 16.0(6) release or later, the upgrade process loads the 32-bit image onto SUP-A, SUP-A+, and SUP-B. In previous releases, the upgrade process loaded the 64-bit image. If you upgrade the switches to ACI-mode switch release 16.0(6) before upgrading your Cisco APICs to the 6.0(6) release, then the Cisco APIC downloads the 32-bit ACI-mode switch image for all 4 of the supervisor types (A, B, A+, and B+). This is not the desired behavior for the 16.0(6) ACI-mode switch release, because you need the 64-bit image for SUP-B+. Therefore, upgrade the Cisco APIC to release 6.0(6) before you upgrade the switches to release 16.0(6).

ACI release 6.0(5)

Table 17 Cisco APIC release 6.0(5) changes in behavior

Product Impact	Description
N/A	There are no changes in behavior.

Table 18 Cisco Nexus 9000 ACI-Mode Switches release 16.0(5) changes in behavior

Product Impact	Description
N/A	There are no changes in behavior.

ACI release 6.0(4)

Table 29 Cisco APIC release 6.0(4) changes in behavior

Product Impact	Description
Base functionality	In case of failed login attempts, a detailed description of the reasons for failure are displayed under **System > History > Session Logs** in the Cisco APIC GUI. These details, along with the username, are also available on external servers, such as TACACS accounting or syslog servers (if external logging is configured).
Base functionality	The "#" character is not supported for SNMPv3 authentication and privacy keys.

Table 20 Cisco Nexus 9000 ACI-Mode Switches release 16.0(4) changes in behavior

Product Impact	Description
N/A	There are no changes in behavior.

ACI release 6.0(3)

Table 35 Cisco APIC release 6.0(3) changes in behavior

Product Impact	Description
Security	This release uses the rsa-sha2-256 and rsa-sha2-512 SSH keys instead of ssh-rsa. If you are using a Microsoft Windows terminal software such as Teraterm, PuTTY, or WinSCP, upgrade the terminal software to the latest release. If you do not upgrade the terminal software, you might not be able to log into the Cisco APIC.
Upgrade/Downgrade	To upgrade to this release, you must perform the following procedure: 1. Download the 6.0(3) Cisco APIC image and upgrade the APIC cluster to the 6.0(3) release. If you are upgrading from a release prior to 6.0(2), before this step is completed, DO NOT download the Cisco ACI-mode switch images to the APIC. 6.0(2) and later releases have both 32-bit and 64-bit switch images, but releases prior to 6.0(2) do not support 64-bit images. As a result, downloading the 64-bit images at this time might cause errors or unexpected results. 2. Download both the 32-bit and 64-bit images to the Cisco APIC. Downloading only one of the images may result in errors during the upgrade process. 3. Create the maintenance groups and trigger the upgrade procedure as usual. Cisco APIC automatically deploys the correct image to the respective switch during the upgrade process. For more information, see the *Cisco APIC Installation and ACI Upgrade and Downgrade Guide*.

Table 46 Cisco Nexus 9000 ACI-Mode Switches release 16.0(3) changes in behavior

Product Impact	Description
Upgrade/Downgrade	A switch now determines which image to install (32-bit or 64-bit) from the Cisco APIC based on the available memory of the switch instead of based on a static mapping. If the available memory of the switch is less than or equal to 24 GB, the switch installs the 32-bit image. If the available memory of the switch is greater than or equal to 32 GB, the switch may be upgraded to the 32-bit image first, then upgrade again to the 64-bit image, which results in two reboots during the upgrade process. Modular spine switches install the 64-bit image regardless of the switch's available memory. You must download both the 32-bit and 64-bit Cisco ACI-mode switch images to the Cisco APIC.

Base Functionality	The **show interface** command no longer displays the "30 seconds input" and "30 seconds output" counters. Example:
	
	`30 seconds input rate 0 bits/sec, 0 packets/sec`
	
	`30 seconds output rate 0 bits/sec, 0 packets/sec`
	
	These counters were never supported and displayed with incorrect values.

ACI release 6.0(2)

Table 17 Cisco APIC release 6.0(2) changes in behavior

Product Impact	Description
Base Functionality	The service BD default configuration is converted to "routing" for all IP traffic; this is true for new and existing service BDs. This can change how ACI forwards the existing Layer 2 traffic exchanged between L4-L7 devices. If this Layer 2 traffic uses an IP address that is not defined in the service BD subnet, this traffic may be routed instead of switched, and as a result, it may be forwarded according to the default route. This could potentially interrupt the cluster communication between L4-L7 HA pairs, such as, firewall pairs. In order to avoid this interruption, ensure that the subnet for the IP addresses that the firewalls use to communicate among each other is included in the service BD subnet configuration. For more information, see the section titled "Service BD configuration option" in the [Cisco Application Centric Infrastructure Policy-Based Redirect Service Graph Design White Paper]().
Base Functionality	The "Images" GUI page (**Admin > Firmware > Images**) now includes a "Platform Type" column, which specifies whether a switch image is 64-bit or 32-bit. This column does not apply to Cisco APIC images.
Ease of Use	On the "Interface Configuration" GUI page (**Fabric > Access Policies > Interface Configuration**), the node table now contains the following columns: • Interface Description: The user-entered description of the interface. You can edit the description by clicking ... and choosing **Edit Interface Configuration**. • Port Direction: The direction of the port. Possible values are "uplink," "downlink," and "default." The default value is "default," which indicates that the port uses its default direction. The other values display if you converted the port from uplink to downlink or downlink to uplink.
Ease of Use	The initial cluster set up and bootstrapping procedure has been simplified with the introduction of the APIC Cluster Bringup GUI. The APIC Cluster Bringup GUI supports virtual and physical APIC platforms.
Ease of Use	There is now a "Switch Configuration" GUI page (**Fabric > Access Policies > Switch Configuration**) that shows information about the leaf and spine switches controlled by the Cisco APIC. This page also enables you to modify a switch's configuration to create an access policy group and fabric policy group, or to remove the policy groups from 1 or more nodes. This page is similar to the "Interface Configuration" GUI page that existed previously, but is for switches.

Product Impact	Description
Security	The Diffie-Hellman (DH) parameters are now dynamically determined during the communication handshake between the devices in the fabric.
Security	When you configure a custom certificate for Cisco ACI HTTPS access, you can now choose the elliptic-curve cryptography (ECC) key type. Prior to this release, RSA was the only key type.
Security	You can no longer use telnet to connect to the management IP address of a Cisco APIC or Cisco ACI-mode switch.
Upgrade/Downgrade	To upgrade to this release, you must perform the following procedure: 1. Download the 6.0(2) Cisco APIC image and upgrade the APIC cluster to the 6.0(2) release. Before this step is completed, DO NOT download the Cisco ACI-mode switch images to the APIC. The 6.0(2) release has both 32-bit and 64-bit switch images, but releases prior to 6.0(2) do not support 64-bit images. As a result, downloading the 64-bit images at this time might cause errors or unexpected results. 2. Download both the 32-bit and 64-bit images to the Cisco APIC. Downloading only one of the images may result in errors during the upgrade process. 3. Create the maintenance groups and trigger the upgrade procedure as usual. Cisco APIC automatically deploys the correct image to the respective switch during the upgrade process. For more information, see the *Cisco APIC Installation and ACI Upgrade and Downgrade Guide*.

Table 18 Cisco Nexus 9000 ACI-Mode Switches release 16.0(2) changes in behavior

Product Impact	Description
Base Functionality	You can now convert the Cisco N9K-C93180YC-FX3 and N9K-C93108TC-FX3P switches to be used as FEXes.

ACI release 6.0(1)

Table 19 Cisco APIC release 6.0(1) changes in behavior

Product Impact	Description
Base Functionality	Beginning with this release, the online help has been removed from the GUI. You can instead view the documentation by clicking the ? in the upper right of any GUI screen and choosing Help. The Help Center dialog that appears contains links to various Cisco APIC documentation.
Base Functionality	In the Cisco APIC GUI, On the "Welcome to Access Policies" page (**Fabric > Access Policies > Quick Start**), the work pane now contains the following choices: • Configure Interfaces: Used to configure the interfaces on a node. • Breakout: Used to configure breakout ports on a node. • Create a SPAN Source and Destination: Used to create a SPAN source group. • Convert Interfaces: Used to convert interfaces on a node to uplink or downlink ports. • Fabric Extender: Used to connect a node to a fabric extender (FEX).
Ease of Use	In the Cisco APIC GUI, on the "Interface Configuration" page (**Fabric > Access Policies >**

Product Impact	Description
	Interface Configuration), the node table now contains the following columns:
	• Pod: The ID of the pod to which the node belongs.
	• Interface: The ID of interface.
	• Node: The ID of the node.
	• Port Type: The type of the port on the node (access or fabric).
	• Admin State: The administrative state of the node.
	• Port Mode: The mode of the port on the node (individual, port channel, or virtual port channel, fabric leaf port, fabric spine port, spine port, or FEX connected).
	• Policy Group: The policy group to which the node belongs.
	• Interface Description: An optional description of the interface.
Performance and Scalability	A leaf switch now supports only up to 56 uplinks. Prior to the 16.0(1) release, a leaf switch supported more than 56 uplinks. If your configuration has more than 56 uplinks, before you upgrade to the 16.0(1) release, reduce the number of uplinks to 56 or less otherwise you will lose any uplinks that are more than 56. If you upgrade to the 16.0(1) release and have more than 56 uplinks, Cisco APIC raises a fault similar to the following example: [F2981][raised][portp-policy-limit-exceeded][warning][sys/ops/slot-lcslot-1/portpol-21/fault-F2981] PortP policy limit exceeded
Performance and Scalability	The hash result of symmetric EtherChannel could be different because of the fix for issue CSCwb93059. This change could cause asymmetric flow. For example, if the ingress leaf switch for the incoming traffic uses a prior release and the ingress leaf switch for the return traffic uses this release or later, the switches get different hash results for the incoming and return traffic.
Security	In the Cisco APIC GUI, the **Admin > AAA** pages have been modified. The Work panes of **Authentication**, **Security**, and **Users** have been enhanced for better functionality and ease of use.
Security	Transport Layer Security (TLS) version 1.0 and 1.1 are no longer supported.
Deprecated feature(s)	Deprecated features for Cisco APIC release 6.0(1): • Cisco ACI Virtual Edge Switch: For information about Cisco ACI Virtual Edge, see the Cisco ACI Virtual Edge Release Notes, Release 3.2(4). • Cisco ACI Virtual Pod: For information about Cisco ACI Virtual Pod, see the Cisco ACI Virtual Pod Release Notes, Release 5.1(3).

Table 20 Cisco Nexus 9000 ACI-Mode Switches release 16.0(1) changes in behavior

Product Impact	Description
Base Functionality	The Cisco N9K-C93120TX switch is no longer supported.
Performance and Scalability	A leaf switch now supports only up to 56 uplinks. Prior to the 16.0(1) release, a leaf switch supported more than 56 uplinks. If your configuration has more than 56 uplinks, before you upgrade to the 16.0(1) release, reduce the number of uplinks to 56 or less otherwise you will lose any uplinks that are more than 56. If you upgrade to the 16.0(1) release and have more than 56 uplinks, Cisco APIC raises a fault similar to the following example: [F2981][raised][portp-policy-limit-exceeded][warning][sys/ops/slot-lcslot-1/portpol-21/fault-F2981] PortP policy limit exceeded

ACI release 5.3(2)

Table 5 Cisco APIC release 5.3(2) changes in behavior

Product Impact	Description
Base Functionality	In case of failed login attempts, a detailed description of the reasons for failure are displayed under System > History > Session Logs in the Cisco APIC GUI. These details, along with the username, are also available on external servers, such as syslog servers (if external logging is configured).

Table 6 Cisco Nexus 9000 ACI-Mode Switches release 15.3(2) changes in behavior

Product Impact	Description
N/A	There are no changes in behavior.

ACI release 5.3(1)

Table 7 Cisco APIC release 5.3(1) changes in behavior

Product Impact	Description
Security	You can no longer use telnet to connect to the management IP address of a Cisco APIC or Cisco ACI-mode switch.

Table 8 Cisco Nexus 9000 ACI-Mode Switches release 15.3(1) changes in behavior

Product Impact	Description
N/A	There are no changes in behavior.

ACI release 5.2(8)

Table 9 Cisco APIC release 5.2(8) changes in behavior

Product Impact	Description
N/A	There are no changes in behavior.

Table 10 Cisco Nexus 9000 ACI-Mode Switches release 15.2(8) changes in behavior

Product Impact	Description
N/A	There are no changes in behavior.

ACI release 5.2(7)

Table 11 Cisco APIC release 5.2(7) changes in behavior

Product Impact	Description
Base Functionality	On the "Interface Configuration" GUI page (**Fabric > Access Policies > Interface Configuration**), the node table now contains the following columns: • Interface Description: The user-entered description of the interface. You can edit the description by clicking **...** and choosing **Edit Interface Configuration**. • Port Direction: The direction of the port. Possible values are "uplink," "downlink," and "default." The default value is "default," which indicates that the port uses its default direction. The other values display if you converted the port from uplink to downlink or downlink to uplink.
Base Functionality	On the "Welcome to Access Policies" GUI page (**Fabric > Access Policies > Quick Start**), work pane now contains the following choices: • Configure Interfaces: Used to configure the interfaces on a node. • Breakout: Used to configure breakout ports on a node. • Create a SPAN Source and Destination: Used to create a SPAN source group. • Convert Interfaces: Used to convert interfaces on a node to uplink or downlink ports. • Fabric Extender: Used to connect a node to a fabric extender (FEX).
Ease of Use	On the "Interface Configuration" GUI page (**Fabric > Access Policies > Interface Configuration**) and "Switch Configuration" page (**Fabric > Access Policies > Switch Configuration**), if you configured your switches in the Cisco APIC 5.2(5) release or earlier, the following warning message displays near the top of the page: Some of the switches are still configured the old way. We can help you migrate them. If you click "migrate them" and use the dialog that appears, the Cisco APIC converts the selected switches' configuration from the method used in the 4.2 and earlier releases to the newer method used in the 5.2 and later releases. The newer configuration is simplified. For example, the configurations no longer have policy selectors. After the conversion, each switch will have an access policy group and fabric policy group. You can expect to have a short duration of traffic loss during the migration.
Ease of Use	There is now a "Switch Configuration" GUI page (**Fabric > Access Policies > Switch Configuration**) that shows information about the leaf and spine switches controlled by the Cisco APIC. This page also enables you to modify a switch's configuration to create an access policy group and fabric policy group, or to remove the policy groups from 1 or more nodes. This page is similar to the "Interface Configuration" GUI page that existed previously, but is for switches.

Table 12 Cisco Nexus 9000 ACI-Mode Switches release 15.2(7) changes in behavior

Product Impact	Description
N/A	There are no changes in behavior.

ACI release 5.2(6)

Table 13 Cisco APIC release 5.2(6) changes in behavior

Product Impact	Description
Base Functionality	Beginning with this release, the online help has been removed from the GUI. You can instead view the documentation by clicking the **?** in the upper right of any GUI screen and choosing **Help**. The Help Center dialog that appears contains links to various Cisco APIC documentation. After you view any desired documentation, if you are unable to close the Help Center dialog, reload the Cisco APIC GUI page.
Base Functionality	The hash result of symmetric EtherChannel could be different because of the fix for issue CSCwb93059. This change could cause asymmetric flow. For example, if the ingress leaf switch for the incoming traffic uses a prior release and the ingress leaf switch for the return traffic uses this release or later, the switches get different hash results for the incoming and return traffic.

Table 14 Cisco Nexus 9000 ACI-Mode Switches release 15.2(6) changes in behavior

Product Impact	Description
N/A	There are no changes in behavior.

ACI release 5.2(5)

Table 15 Cisco APIC release 5.2(5) changes in behavior

Product Impact	Description
Security	• Transport Layer Security (TLS) version 1.0 and 1.1 are no longer supported. • Beginning with APIC version 5.2(5c) and switch version 15.2(5c), regardless of the fabric secure mode setting (permissive mode or strict mode), the switch will continue to function and remain *active* within the fabric even if the switch certificate has expired.

Table 16 Cisco Nexus 9000 ACI-Mode Switches release 15.2(5) changes in behavior

Product Impact	Description
Base Functionality	The default timer value and minimum timer value for bidirectional forwarding detection (BFD) over IS-IS are both now 250ms.

ACI release 5.2(4)

Table 17 Cisco APIC release 5.2(4) changes in behavior

Product Impact	Description
Base Functionality	The " Interfaces and Policies" GUI screen is now titled " Interface Configuration" (Fabric > Access Policies > Interface Configuration). On the screen, the node table now contains the following columns: • Name • Speed

Product Impact	Description
	• Admin State • Operational State • Port Mode • Policy Group For more information, see the online help page for this screen.

Upgrade/Downgrade	When you upgrade to the 5.2(4) release, the Cisco APIC now creates the following interface policies automatically:
	• CDP (cdpIfPol)
	  ◦ system-cdp-disabled
	  ◦ system-cdp-enabled
	• LLDP (lldpIfPol)
	  ◦ system-lldp-disabled
	  ◦ system-lldp-enabled
	• LACP (lacpLagPol)
	  ◦ system-static-on
	  ◦ system-lacp-passive
	  ◦ system-lacp-active
	• Link Level (fabricHIfPol)
	  ◦ system-link-level-100M-auto
	  ◦ system-link-level-1G-auto
	  ◦ system-link-level-10G-auto
	  ◦ system-link-level-25G-auto
	  ◦ system-link-level-40G-auto
	  ◦ system-link-level-100G-auto
	  ◦ system-link-level-400G-auto
	• Breakout Port Group Map (infraBrkoutPortGrp)
	  ◦ system-breakout-10g-4x
	  ◦ system-breakout-25g-4x
	  ◦ system-breakout-100g-4x
	For caveats about these default policies if you upgrade to this release or downgrade from this release, see the *Cisco APIC Installation and ACI Upgrade and Downgrade Guide*.

Table 18 Cisco Nexus 9000 ACI-Mode Switches release 15.2(4) changes in behavior

Product Impact	Description
N/A	There are no changes in behavior.

ACI release 5.2(3)

Table 19 Cisco APIC release 5.2(3) changes in behavior

Product Impact	Description
Security	For increased security, the random key for an encrypting user-specific configuration and operational data in the SSD on both Cisco APIC and switch nodes is now generated in the

Product Impact	Description
	hardware using a true random number generator (TRNG) instead of in the software.
Upgrade/Downgrade	When you upgrade or downgrade the leaf and spine switches using the **Setup Switch Update Group** wizard in the Cisco APIC GUI, the following GUI elements have been renamed: • The **Add Nodes** button is now named **Add Switches**. • The **Node Selection** step is now named **Versions**. • The **Advanced Options** dialog is now named **Advanced Settings**. • The **Ignore Compatibility Check** setting in the **Advanced Settings** dialog is now named **Compatibility Check** and the default value is **Enforced**. The overall procedure has changed, including the order of some of the steps. In the Cisco APIC Installation and ACI Upgrade and Downgrade Guide, Upgrading or Downgrading with APIC Release 5.1 or Later Using the GUI chapter, see the Pre-Download Images to the Leaf and Spine Switches section.

Table 20 Cisco Nexus 9000 ACI-Mode Switches release 15.2(3) changes in behavior

Product Impact	Description
Security	For increased security, the random key for an encrypting user-specific configuration and operational data in the SSD on both Cisco APIC and switch nodes is now generated in the hardware using a true random number generator (TRNG) instead of in the software.

ACI release 5.2(2)

Table 21 Cisco APIC release 5.2(2) changes in behavior

Product Impact	Description
N/A	There are no changes in behavior.

Table 22 Cisco Nexus 9000 ACI-Mode Switches release 15.2(2) changes in behavior

Product Impact	Description
N/A	There are no changes in behavior.

ACI release 5.2(1)

Table 23 Cisco APIC release 5.2(1) changes in behavior

Product Impact	Description
Base Functionality	A minor fault is now raised if a line card or fabric module has the "err-pwr-down" or "failure" status, as shown by the show module command. This fault is cleared if the status changes to "ok" after the line card or fabric module is rebooted.
Base Functionality	A minor fault is now raised when you remove a line card or fabric module from the chassis. In previous releases, the Cisco APIC had an event notification, but no fault was raised. This same fault is cleared when you reinsert the line card or fabric module.

Product Impact	Description
Base Functionality	When a line card or fabric module slot is empty on boot up, there is a fault raised for the missing slots, and the fault is cleared only on insertion. That is, in addition to physically removing the card scenario, there will be a fault raised if the box boots up with empty line card or fabric module slots.
Base Functionality	You can no longer create a new SNMP policy user with authType:MD5 and privType:DES. However, you can still import a SNMP policy user that has authType:MD5 and privType:DES.
Deprecated Feature(s)	Deprecated features for Cisco APIC release 5.2(1): Layer 4 to Layer 7 services device packages (service graph managed mode): Device packages are no longer supported. There is no longer a managed mode for devices; all devices are effectively unmanaged. For information about device packages, see the Cisco APIC Layer 4 to Layer 7 Services Deployment Guide, Release 5.1(x)

Table 24 Cisco Nexus 9000 ACI-Mode Switches release 15.2(1) changes in behavior

Product Impact	Description
Base Functionality	You now must specify a VRF instance with when using the nslookup command: nslookup vrf <vrf_id> [-option] [name	-] [server]

ACI release 5.1(4)

Table 25 Cisco APIC release 5.1(4) changes in behavior

Product Impact	Description
N/A	There are no changes in behavior.

Table 26 Cisco Nexus 9000 ACI-Mode Switches release 15.1(4) changes in behavior

Product Impact	Description
N/A	There are no changes in behavior.

ACI release 5.1(3)

Table 27 Cisco APIC release 5.1(3) changes in behavior

Product Impact	Description
Base Functionality	ICMP now replies with the same Class of Service (CoS) value that was sent in the request.

Table 28 Cisco Nexus 9000 ACI-Mode Switches release 15.1(3) changes in behavior

Product Impact	Description
N/A	There are no changes in behavior.

ACI release 5.1(2)

Table 29 Cisco APIC release 5.1(2) changes in behavior

Product Impact	Description
N/A	There are no changes in behavior.

Table 30 Cisco Nexus 9000 ACI-Mode Switches release 15.1(2) changes in behavior

Product Impact	Description
N/A	There are no changes in behavior.

ACI release 5.1(1)

Table 31 Cisco APIC release 5.1(1) changes in behavior

Product Impact	Description
Base Functionality	The SQL database is no longer persistent during ungraceful reloads of the switches. Examples of ungraceful reload include kernel panics and forced power cycles. In the event of an ungraceful reload, the switch will reboot as stateless and must re-download its policies from the Cisco APIC. Graceful reloads, such as manual reloads and hap-resets, are still stateful and the switch will maintain its database across the reload.
Base Functionality	When the same subnet is configured under both a bridge domain and an EPG, the scope such as "Advertised Externally" and "Shared between VRFs" must match. Configurations with a mismatched scope are rejected beginning in releases 4.2(6d) and 5.1(1).
Performance and Scalability	The "ip" attribute of the fvCEp class has been deprecated. IP addresses are now represented as fvIp children of fvCEp. This change provides better support for having multiple IP addresses on the same MAC address.

Table 32 Cisco Nexus 9000 ACI-Mode Switches release 15.1(1) changes in behavior

Product Impact	Description
N/A	There are no changes in behavior.

ACI release 5.0(2)

Table 33 Cisco APIC release 5.0(2) changes in behavior

Product Impact	Description
N/A	There are no changes in behavior.

Table 34 Cisco Nexus 9000 ACI-Mode Switches release 15.0(2) changes in behavior

Product Impact	Description
N/A	There are no changes in behavior.

ACI release 5.0(1)

Table 35 Cisco APIC release 5.0(1) changes in behavior

Product Impact	Description
Base Functionality	A service endpoint group (EPG) in a service graph that has vzAny as the consumer and provider now has the PCTag get changed to the Global PCTag with EPGs and endpoint security groups. If you have such a service graph with Cisco APIC running a pre-5.0 release (such as 4.2(8)) and you are upgrading to 5.0 or a later release, the change takes place during the Cisco APIC upgrade. There may be transient disruption to the traffic going through the service graph because the pcTag along with the relevant contracts are re-programmed. See CSCwh75475 for more information.
Base Functionality	The hypervisor topology view has changed in this release. Leaf switches no longer appear in the topology diagram in the work pane when you choose a particular hypervisor in a virtual machine manager (VMM) domain. Also, virtual machines (VMs) attached to the hypervisor now appear as circles instead of squares.

Table 36 Cisco Nexus 9000 ACI-Mode Switches release 15.0(1) changes in behavior

Product Impact	Description
Security	The implicit deny rules on a leaf switch are reordered and will prevent route leak traffic flows if the "Shared Security Import Subnet" option is not configured on the related L3Out external EPG subnet. For more information, see the "Scope and Aggregate Controls for Subnets" section in the *Cisco APIC Layer 3 Networking Configuration Guide, Release 5.0(x)*.

ACI release 4.2(7)

Table 37 Cisco APIC release 4.2(7) changes in behavior

Product Impact	Description
Base Functionality	A minor fault is now raised if a line card or fabric module has the "err-pwr-down" or "failure" status, as shown by the show module command. This fault is cleared if the status changes to "ok" after the line card or fabric module is rebooted.

Product Impact	Description
Base Functionality	A minor fault is now raised when you remove a line card or fabric module from the chassis. In previous releases, the Cisco APIC had an event notification, but no fault was raised. This same fault is cleared when you reinsert the line card or fabric module.
Base Functionality	When a line card or fabric module slot is empty on boot up, there is a fault raised for the missing slots, and the fault is cleared only on insertion. That is, in addition to physically removing the card scenario, there will be a fault raised if the box boots up with empty line card or fabric module slots.

Table 38 Cisco Nexus 9000 ACI-Mode Switches release 14.2(7) changes in behavior

Product Impact	Description
Reliability	Cisco ACI uses a TCP session-based messaging queue (referred to as vPC ZMQ) to represent the peer-link status. Under rare circumstances, leaf nodes of a vPC pair may experience a vPC ZMQ down symptom, where the nodes fail to establish the vPC peer-link even though there is route reachability between the vPC nodes through the Cisco ACI infra. Unless explicitly mentioned about route reachability, the state of vPC ZMQ down in below context should be seen as one with valid route reachability. This release strengthens the handling of the following scenarios: • If the vPC role of the node is still None Established when vPC ZMQ is down, the node remains None Established. This poses a problem when both leaf nodes of a vPC pair are in the None Established role, because neither of the vPC nodes will bring up its vPC ports. This could happen in a rare case of all spine nodes rebooting at once while a problem with the vPC ZMQ is present. The Cisco ACI 14.2(7) release enhances the internal handling mechanism for this condition by automatically flapping the fabric links on one of the nodes up to 5 times. Flapping the fabric links of a leaf node breaks the incomplete state in which vPC ZMQ is down while the vPC nodes have route reachability, which allows the other node to promote itself to the vPC primary role. If the problem with vPC ZMQ is still present after the fabric links of the to-be-secondary node comes back up, the node will flap its fabric links 4 more times (for 5 times total) to try to re-establish the vPC peer-link status while the other node handles user traffic as the primary. After the 5th flap, if the vPC peer-link status is not yet established, the Cisco APIC raises a critical fault for the given node. As a side effect, the flapping also impacts non-vPC traffic on the node because fabric links are used for any type of traffic. • Prior to the Cisco ACI 14.2(7) release, you could try manually to flap the fabric links or reboot one of the vPC nodes to attempt to re-establish the vPC peer-link. However, the other vPC node did not bring up its vPC ports even after the node promoted itself to the primary from None Established if it had a problem with vPC ZMQ. This was fixed along with the change in behavior explained here.
Reliability	Under rare circumstances, a leaf node of a vPC pair may lose COOP database connectivity with spine nodes. Starting in this release, a vPC node brings down its vPC ports if it lost the COOP database connectivity due to the risk of inconsistent endpoint learning information.

ACI release 4.2(6)

Table 39 Cisco APIC release 4.2(6) changes in behavior

Product Impact	Description
Base Functionality	The SQL database is no longer persistent during ungraceful reloads of the switches. Examples of ungraceful reload include kernel panics and forced power cycles. In the event of an ungraceful reload, the switch will reboot as stateless and must re-download its policies from the Cisco APIC. Graceful reloads, such as manual reloads and hap-resets, are still stateful and the switch will main-tain its database across the reload.
Base Functionality	The storm policer is now enforced for all forwarded control traffic in the leaf switch for the DHCP, ARP, ND, ICMP, HSRP, PIM, IGMP, and EIGRP protocols. This behavior change applies

Product Impact	Description
	only to EX and later leaf switch switches.

In Cisco N9K-C93180LC-EX, N9K-93180YC-EX, and N9K-C93108TC-EX switches, you can configure both the supervisor policer and storm policer for one of the protocols. In this case, if the incoming traffic rate is greater than the supervisor policer rate, the switch will allow more storm traffic than the configured storm policer rate. If the incoming traffic rate is equal to or less than supervisor policer rate, then the switch will correctly allow the configured storm traffic rate. This behavior is applicable irrespective of the configured supervisor policer and storm policer rates.

One side effect of this change is that control traffic that gets forwarded in the leaf switch will now get subjected to storm policer drops. In previous releases, no such storm policer drops occur for the protocols that are affected by this change. |
| Base Functionality | When the same subnet is configured under both a bridge domain and an EPG, the scope such as "Advertised Externally" and "Shared between VRFs" must match. Configurations with a mismatched scope are rejected beginning in releases 4.2(6d) and 5.1(1). |
| Base Functionality | You can configure a vzAny shared services provider only for contracts with the shared services scope. In previous release, you could configure a vzAny shared services provider for any policy-based redirect contract. |

Table 40 Cisco Nexus 9000 ACI-Mode Switches release 14.2(6) changes in behavior

Product Impact	Description
N/A	There are no changes in behavior.

ACI release 4.2(5)

Table 41 Cisco APIC release 4.2(5) changes in behavior

Product Impact	Description
Base Functionality	For the Intersight Device Connector, the **Auto Update** option is now enabled by default. For more information, see the _Cisco APIC and Intersight Device Connector_ document.

Table 42 Cisco Nexus 9000 ACI-Mode Switches release 14.2(5) changes in behavior

Product Impact	Description
N/A	There are no changes in behavior.

ACI release 4.2(4)

Table 43 Cisco APIC release 4.2(4) changes in behavior

Product Impact	Description
N/A	There are no changes in behavior.

Table 44 Cisco Nexus 9000 ACI-Mode Switches release 14.2(4) changes in behavior

Product Impact	Description
N/A	There are no changes in behavior.

ACI release 4.2(3)

Table 45 Cisco APIC release 4.2(3) changes in behavior

Product Impact	Description
Base Functionality	The hypervisor topology view has changed in this release. Leaf switches no longer appear in the topology diagram in the work pane when you choose a particular hypervisor in a virtual machine manager (VMM) domain. Also, virtual machines (VMs) attached to the hypervisor now appear as circles instead of squares.

Table 46 Cisco Nexus 9000 ACI-Mode Switches release 14.2(3) changes in behavior

Product Impact	Description
N/A	There are no changes in behavior.

ACI release 4.2(2)

Table 47 Cisco APIC release 4.2(2) changes in behavior

Product Impact	Description
N/A	There are no changes in behavior.

Table 48 Cisco Nexus 9000 ACI-Mode Switches release 14.2(2) changes in behavior

Product Impact	Description
N/A	There are no changes in behavior.

ACI release 4.2(1)

Table 49 Cisco APIC release 4.2(1) changes in behavior

Product Impact	Description
Base Functionality	IPv6 multicast is now enabled with PIMv6 protocol settings.
Base Functionality	The tech support file size is reduced by up to 25%, depending on the switch type and the configured features.
Base Functionality	When you create a bridge domain using the Cisco APIC GUI, the ARP flooding option is now enabled by default. The ARP flooding option is still disabled by default when you use the create a bridge domain using the CLI or REST API.

Product Impact	Description
Base Functionality	You can now configure the Cisco Discovery Protocol (CDP) and Link Layer Discovery Protocol (LLDP) in the leaf and spine switch management interfaces.
Ease of Use	The default behavior of the Callhome email received by a user has been modified for clarity.
Performance and Scalability	Multi-node policy-based redirect now supports up to 5 nodes in a single service graph.
Security	When installing the Cisco ACI simulator virtual machine, you no longer need a challenge key nor an activation token. You still need the challenge key and activation token for earlier releases.
Upgrade/Downgrade	Cisco APIC and switch upgrades are now stopped if the scheduled time and date has already passed.

Table 50 Cisco Nexus 9000 ACI-Mode Switches release 14.2(1) changes in behavior

Product Impact	Description
N/A	There are no changes in behavior.

ACI release 4.1(2)

Table 51 Cisco APIC release 4.1(2) changes in behavior

Product Impact	Description
Base Functionality	Cisco APIC-X is deprecated.

Table 52 Cisco Nexus 9000 ACI-Mode Switches release 14.1(2) changes in behavior

Product Impact	Description
N/A	There are no changes in behavior.

ACI release 4.1(1)

Table 53 Cisco APIC release 4.1(1) changes in behavior

Product Impact	Description
Base Functionality	You no longer need to include the IP prefix of the Layer 3 interface when configuring source SPAN with Layer 3 interface filtering. For more information, see the *Cisco APIC Troubleshooting Guide, Release 4.1(x)*.

Table 54 Cisco Nexus 9000 ACI-Mode Switches release 14.1(1) changes in behavior

Product Impact	Description
N/A	There are no changes in behavior.

ACI release 4.0(3)

Table 55 Cisco APIC release 4.0(3) changes in behavior

Product Impact	Description
N/A	There are no changes in behavior.

Table 56 Cisco Nexus 9000 ACI-Mode Switches release 14.0(3) changes in behavior

Product Impact	Description
N/A	There are no changes in behavior.

ACI release 4.0(2)

Table 57 Cisco APIC release 4.0(2) changes in behavior

Product Impact	Description
N/A	There are no changes in behavior.

Table 58 Cisco Nexus 9000 ACI-Mode Switches release 14.0(2) changes in behavior

Product Impact	Description
N/A	There are no changes in behavior.

ACI release 4.0(1)

Table 59 Cisco APIC release 4.0(1) changes in behavior

Product Impact	Description
Base Functionality	The Capacity Dashboard (**Operations > Capacity Dashboard**) has been reorganized. In previous releases, the dashboard displayed all of its information on one screen. In this release, the information is split between the new **Fabric Capacity** tab and **Leaf Capacity** tab. In addition, the leaf switches listed in the **Leaf Capacity** tab have a **Configure Profile** link, which opens the **Forward Scale Profile** form. The form enables you to configure the scale profile of the switch, if the switch model supports multiple profiles.
Ease of Use	In the **Apps** tab, if you open an app, navigate to another menu tab, then navigate back to the **Apps** menu tab, the app now remains open. The app also continues to perform the operation that it was doing before you navigated away. In previous releases, the app would close if you navigated to a different menu tab, which also stopped the app's current operation.

Product Impact	Description
Performance and Scalability	The data plane forwarding impact to endpoints is decreased because the front panel port bring up is delayed during reload scenarios. This enhancement allows the upstream protocols (VXLAN, MP-BGP, and COOP) to converge.
Upgrade/Downgrade	The procedures for upgrading the software using the GUI has changed. For more information, see the *Cisco APIC Management, Installation, Upgrade, and Downgrade Guide*.
Upgrade/Downgrade	You can no longer 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. For more information, see the *Cisco APIC Management, Installation, Upgrade, and Downgrade Guide*.

Table 60 Cisco Nexus 9000 ACI-Mode Switches release 14.0(1) changes in behavior

Product Impact	Description
Base Functionality	All dynamic packet prioritization (DPP)-prioritized traffic is now marked Class of Service (CoS) 3 regardless of a custom Quality of Service (QoS) configuration. When these packets ingress and egress the same leaf switch, the CoS value is retained, causing the frames to leave the fabric with the CoS 3 marking.

ACI release 3.2(10)

Table 61 Cisco APIC release 3.2(10) changes in behavior

Product Impact	Description
N/A	There are no changes in behavior.

Table 62 Cisco Nexus 9000 ACI-Mode Switches release 13.2(10) changes in behavior

Product Impact	Description
N/A	There are no changes in behavior.

ACI release 3.2(9)

Table 63 Cisco APIC release 3.2(9) changes in behavior

Product Impact	Description
N/A	There are no changes in behavior.

Table 64 Cisco Nexus 9000 ACI-Mode Switches release 13.2(9) changes in behavior

Product Impact	Description
N/A	There are no changes in behavior.

ACI release 3.2(7)

Table 65 Cisco APIC release 3.2(7) changes in behavior

Product Impact	Description
Base Functionality	The EIGRP metric is now carried over the BGP VPNv4 address family using extended communities.

Table 66 Cisco Nexus 9000 ACI-Mode Switches release 13.2(7) changes in behavior

Product Impact	Description
N/A	There are no changes in behavior.

ACI release 3.2(6)

Table 67 Cisco APIC release 3.2(6) changes in behavior

Product Impact	Description
Base Functionality	The rogue endpoint control policy no longer drops traffic to and from the rogue endpoint.

Table 68 Cisco Nexus 9000 ACI-Mode Switches release 13.2(6) changes in behavior

Product Impact	Description
N/A	There are no changes in behavior.

ACI release 3.2(5)

Table 69 Cisco APIC release 3.2(5) changes in behavior

Product Impact	Description
N/A	There are no changes in behavior.

Table 70 Cisco Nexus 9000 ACI-Mode Switches release 13.2(5) changes in behavior

Product Impact	Description
N/A	There are no changes in behavior.

ACI release 3.2(4)

Table 71 Cisco APIC release 3.2(4) changes in behavior

Product Impact	Description
N/A	There are no changes in behavior.

Table 72 Cisco Nexus 9000 ACI-Mode Switches release 13.2(4) changes in behavior

Product Impact	Description
N/A	There are no changes in behavior.

ACI release 3.2(3)

Table 73 Cisco APIC release 3.2(3) changes in behavior

Product Impact	Description
N/A	There are no changes in behavior.

Table 74 Cisco Nexus 9000 ACI-Mode Switches release 13.2(3) changes in behavior

Product Impact	Description
N/A	There are no changes in behavior.

ACI release 3.2(2)

Table 75 Cisco APIC release 3.2(2) changes in behavior

Product Impact	Description
Base Functionality	The catalog version no longer matches with the Cisco APIC version. The catalog uses a different versioning scheme beginning in this release.
Base Functionality	The EP tracker can now locate L3Out endpoints. The tracker results now have fields that are specific to L3Out endpoints. For more information, see the EP tracker online help.

Table 76 Cisco Nexus 9000 ACI-Mode Switches release 13.2(2) changes in behavior

Product Impact	Description
N/A	There are no changes in behavior.

ACI release 3.2(1)

Table 77 Cisco APIC release 3.2(1) changes in behavior

Product Impact	Description
Base Functionality	The units of measure for bidirectional forwarding detection intervals are now in milliseconds.

Table 78 Cisco Nexus 9000 ACI-Mode Switches release 13.2(1) changes in behavior

Product Impact	Description
N/A	There are no changes in behavior.

Documentation Feedback

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

Legal Information

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: http://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. (1110R)

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.