



Cisco Application Policy Infrastructure Controller Release Notes, Release 6.2(3)

Introduction

The Cisco Application Centric Infrastructure (ACI) is an architecture that allows the application to define the networking requirements in a programmatic way. This architecture simplifies, optimizes, and accelerates the entire application deployment lifecycle. Cisco Application Policy Infrastructure Controller (APIC) is the software, or operating system, that acts as the controller.

This document describes the features, issues, and limitations for the Cisco APIC software. For the features, issues, and limitations for the Cisco NX-OS software for the Cisco Nexus 9000 series switches, see the [Cisco Nexus 9000 ACI-Mode Switches Release Notes, Release 16.2\(3\)](#).

For more information about this product, see "Related Content."

Date	Description
August 28, 2026	Release 6.2(3g) became available.

New software features

Product Impact	Feature	Description
Base Functionality	PBR 5-tuple service node balancing	This feature introduces support for 5-tuple hashing in policy-based redirect (PBR) destination groups. Previously, hashing was limited to Layer 3 fields. It allows the Cisco ACI fabric to compute hash values using the source IP address, source port, destination IP address, destination port, and protocol number. It provides more granular traffic distribution across service nodes. For more information, see the Cisco Layer 4 to Layer 7 Services Deployment Guide, Release 6.2(x).
	SHA2 support in BGP Neighborship within ACI	This feature introduces support for the SHA-256 algorithm for Border Gateway Protocol (BGP) authentication. It supports for TCP Authentication Option (TCP-AO for BGP peers). Now, administrators can configure BGP neighbors to use SHA-256 for enhanced cryptographic security. It strengthens control plane security by providing a more robust, modern cryptographic alternative to legacy MD5-based authentication. For more information, see the Cisco APIC Layer 3 Networking Configuration Guide, Release 6.2(x).
	BGP Local ECMP scale increase to 64-way ECMP	This enhancement enables more granular load balancing and increases the effective capacity for transit routing. By allowing up to 64 next-hops when redistributing local routes (such as Static or OSPF) into MP-BGP, this update improves traffic distribution efficiency and fabric scalability in large-scale network designs. For more information, see the Cisco APIC Layer 3 Networking Configuration Guide, Release 6.2(x).
	Bridge Domain-Level Local Proxy ARP for Layer 3 Policy Enforcement	Support for local proxy ARP. Enable local proxy ARP on a bridge domain to force Layer 2 traffic within a subnet to be routed so that the fabric applies security policies based on IP addresses. Local proxy ARP can also be extended to ACI border gateways for one-fabric (VXLAN EVPN) deployments. For more information, see the Cisco APIC Layer 3 Networking Configuration Guide, Release 6.2(x) and the Cisco APIC Security Configuration Guide, Release 6.2(x).

Product Impact	Feature	Description
	MCP PDU Per VLAN blocking Enhancement	The MCP Support: Per-VLAN Disable Loop Protection Action feature is an enhancement to the ACI Miscabling Protocol (MCP), designed to prevent broad service outages caused by loop-detection actions. Previously, MCP loop protection only supported a "Port Disable" action, which shut down the entire physical port and affected all traffic, regardless of which VLAN was actually causing the loop. This new feature allows the fabric to selectively suspend only the specific VLAN where a loop is detected, ensuring that unaffected VLANs on the same port remain operational. For more information, see the Cisco APIC Basic Configuration Guide, Release 6.2(x).
	Support for auto firmware update on APIC discovery	When you add a new Cisco APIC to the fabric through a return merchandise authorization (RMA), cluster expansion, or commission, the Cisco APIC is automatically upgraded to the same release as the existing cluster. For more information see, the Cisco APIC Installation and ACI Upgrade and Downgrade Guide.
Security	Support for Duo as an Identity Provider (IdP) for SAML	This feature enables official support for Duo Security as an Identity Provider (IdP) for remote SAML 2.0 authentication, addressing the current limitation where the APIC GUI is restricted to Okta, ADFS, and Ping Identity. For more information, see the Cisco APIC Security Configuration Guide, Release 6.2(x).
	CoPP support for HSRP	The HSRP PPPI (Per-Interface Per-Protocol) CoPP feature introduces HSRP support to the ACI per-interface CoPP framework. Users can now define specific rate and burst limits for HSRP control packets at the individual interface level, rather than relying solely on global defaults. This feature is designed to improve fabric stability and provide better observability for HSRP control traffic in environments where fine-tuned per-interface protection is required. For more information, see the Cisco APIC Security Configuration Guide, Release 6.2(x).
Interoperability	Support for Nutanix AOS 7.5	Support for Nutanix AOS 7.5 integration. For AOS 7.5, the tilde (~) character replaces the pipe () character as the delimiter in category values. For more information, see the Cisco ACI and Nutanix Integration document. You may also refer to the <i>Virtualization compatibility information</i> table (available in this document).
Ease of use	Support for running commands on multiple fabric nodes	Use the <code>acidiag run fabriccmd</code> command to run show commands on a single node, a list or range of nodes, all nodes in a pod, or all leaf or spine nodes, directly from the APIC. You can also run multiple commands in one operation by using a YAML input file. For more information, see the Cisco APIC Basic Configuration Guide, Release 6.2(x).
	DHCP Request-ACK timeout Enhancement	This feature introduces a new global configuration knob to mitigate switch startup delays caused by DHCP timeouts when the APIC is unavailable. By allowing switches to bypass the wait for a DHCP ACK, this feature improves convergence time while ensuring existing default behaviors remain unchanged. For more information, see the Cisco APIC REST API Configuration Guide.

Changes in behavior

For the changes in behavior, see [Cisco ACI Releases Changes in Behavior](#).

Resolved issues

Click the bug ID to access the Bug Search tool and see additional information about the bug. The "Exists In" column of the table specifies the 6.2(3) releases in which the bug exists. A bug might also exist in releases other than the 6.2(3) releases.

Bug ID	Description	Fixed in
CSCwu25374	Unnecessary entries in RIB leak route-map on NBL when VRF is not stretched using BGW.	6.2(3g)
CSCwu34390	This is a request to disable Fabric-BFD (BFD on ISIS) feature.	6.2(3g)

Open issues

Click the bug ID to access the Bug Search tool and see additional information about the bug. The "Exists In" column of the table specifies the 6.2(3) releases in which the bug exists. A bug might also exist in releases other than the 6.2(3) releases.

Bug ID	Description	Exists in
CSCwt67826	Temporary fault is raised on the node for missing ctx where the ctx segment id has changed and EPG is not deployed on the node.	6.2(3g)
CSCwv18952	APIC firmware upgrade is not starting when initiated from APIC GUI. When APIC 1 CIMC is upgraded from APIC UI, the status is shown as pending even if the upgrade is successful.	6.2(3g)
CSCwv74044	Auto upgrade feature on Nutanix vAPIC does not work. version: 6.2.3	6.2(3g)

Known issues

Click the bug ID to access the Bug Search tool and see additional information about the bug. The "Exists In" column of the table specifies the 6.2(3) releases in which the bug exists. A bug might also exist in releases other than the 6.2(3) releases.

Bug ID	Description	Exists in
CSCwr65747	CIMC upgrade failure for APIC-L3.	6.2(3g)
CSCwf48875	When using two different host profiles (for example UCS C-Series and UCS B-Series) to deploy NSX, the uplink policy will be different for the host profiles. In this case, using one uplink profile with two policies might cause traffic disruption for a non-default teaming policy.	6.2(3g)
CSCwk37514	An external EPG in an L3Out that is used to connect to the campus is missing even though the corresponding service graph in the outbound filter still exists.	6.2(3g)
CSCwn21313	snmptrapd service runs only on the leader APIC. If snmp is not enabled in snmp policy attached to pod containing leader apic, snmp traps will not get forwarded to the external server.	6.2(3g)

Bug ID	Description	Exists in
CSCvy40511	Traffic from an endpoint under a remote leaf switch to an external node and its attached external networks is dropped. This occurs if the external node is attached to an L3Out with a vPC and there is a redistribution configuration on the L3Out to advertise the reachability of the external nodes as direct-attached hosts.	6.2(3g)
CSCwj60150	The configuration (EPGs, Contracts, External EPGs etc) is out-of-sync between APIC and ISE.	6.2(3g)
CSCwi86409	SGT bindings missing on ACI.	6.2(3g)
CSCwf78521	A GOLF spine switch advertises the bridge domain prefixes to a GOLF peer in multiple VRF instances.	6.2(3g)
CSCvj26666	The "show run leaf spine <nodeld>" command might produce an error for scaled up configurations.	6.2(3g)
CSCvj90385	With a uniform distribution of EPs and traffic flows, a fabric module in slot 25 sometimes reports far less than 50% of the traffic compared to the traffic on fabric modules in non-FM25 slots.	6.2(3g)
CSCvr89603	The CRC and stomped CRC error values do not match when seen from the APIC CLI compared to the APIC GUI. This is expected behavior. The GUI values are from the history data, whereas the CLI values are from the current data.	6.2(3g)
CSCvx75380	svcredirDestmon objects get programmed in all of the leaf switches where the service L3Out is deployed, even though the service node may not be connected to some of the leaf switch. There is no impact to traffic.	6.2(3g)
CSCvx78018	A remote leaf switch has momentary traffic loss for flushed endpoints as the traffic goes through the tglean path and does not directly go through the spine switch proxy path.	6.2(3g)
CSCvy07935	xR IP flush for all endpoints under the bridge domain subnets of the EPG being migrated to ESG. This will lead to a temporary traffic loss on remote leaf switch for all EPGs in the bridge domain. Traffic is expected to recover.	6.2(3g)
CSCvy10946	With the floating L3Out multipath recursive feature, if a static route with multipath is configured, not all paths are installed at the non-border leaf switch/non-anchor nodes.	6.2(3g)
CSCvy45358	The file size mentioned in the status managed object for techsupport "dbgexpTechSupStatus" is wrong if the file size is larger than 4GB.	6.2(3g)
CSCvz06118	In the "Visibility and Troubleshooting Wizard," ERSPAN support for IPv6 traffic is not available.	6.2(3g)
CSCvz84444	While navigating to the last records in the various History sub tabs, it is possible to not see any results. The first, previous, next, and last buttons will then stop working too.	6.2(3g)

Bug ID	Description	Exists in
CSCvz85579	VMMmgr process experiences a very high load for an extended period of time that impacts other operations that involve it. The process may consume excessive amount of memory and get aborted. This can be confirmed with the command "dmesg -T grep oom_reaper" if messages such as the following are reported: oom_reaper: reaped process 5578 (svc_ifc_vmmmgr.)	6.2(3g)
CSCwa78573	When the "BGP" branch is expanded in the Fabric > Inventory > POD 1 > Leaf > Protocols > BGP navigation path, the GUI freezes and you cannot navigate to any other page. This occurs because the APIC gets large set of data in response, which cannot be handled by the browser for parts of the GUI that do not have the pagination.	6.2(3g)
CSCwe18213	The logical switch created for the EPG remains in the NSX-T manager after the EPG is disassociated from the domain, or the logical switch does not get created when the EPG is associated with the domain.	6.2(3g)
CSCwf71934	Multiple duplicate subnets are created on Nutanix for the same EPG.	6.2(3g)
CSCwh74888	With the addressing of CSCwe64407, a release that integrates that bug fix can reference of a static VLAN pool in a VMM domain, which before was not possible. However, if the VMM domain is used by Layer 4 to Layer 7 virtual services and the VMM domain is referencing a static VLAN pool, the services do not work and a fault is raised.	6.2(3g)
CSCwh92539	After upgrading a Cisco APIC from a release before 5.2(8) to release 6.1(1) or later, there is a loss of out-of-band management connectivity over IPv6 if the APIC has dual stack out-of-band management. However, IPv4 connectivity remains intact. This issue does not occur if the out-of-band management is only IPv4 or only IPv6.	6.2(3g)
N/A	Beginning in Cisco APIC release 4.1(1), the IP SLA monitor policy validates the IP SLA port value. Because of the validation, when TCP is configured as the IP SLA type, Cisco APIC no longer accepts an IP SLA port value of 0, which was allowed in previous releases. An IP SLA monitor policy from a previous release that has an IP SLA port value of 0 becomes invalid if the Cisco APIC is upgraded to release 4.1(1) or later. This results in a failure for the configuration import or snapshot rollback. The workaround is to configure a non-zero IP SLA port value before upgrading the Cisco APIC, and use the snapshot and configuration export that was taken after the IP SLA port change.	6.2(3g)
N/A	In a multipod configuration, before you make any changes to a spine switch, ensure that there is at least one operationally "up" external link that is participating in the multipod topology. Failure to do so could bring down the multipod connectivity. For more information about multipod, see the Cisco Application Centric Infrastructure Fundamentals document and the Cisco APIC Getting Started Guide.	6.2(3g)
N/A	A query of a configurable policy that does not have a subscription goes to the policy distributor. However, a query of a configurable policy that has a subscription goes to the policy manager. As a result, if the policy propagation from the policy distributor to the policy manager takes a prolonged amount of time, then in such cases the query with the subscription might not return the policy simply because it has not reached policy manager yet.	6.2(3g)
N/A	Typically, faults are generally raised based on the presence of the BGP route target profile under the VRF table. However, if a BGP route target profile is configured without actual route targets (that is, the profile has empty policies), a fault will not be raised in this situation.	6.2(3g)

Bug ID	Description	Exists in
N/A	MPLS interface statistics shown in a switch's CLI get cleared after an admin or operational down event.	6.2(3g)
N/A	MPLS interface statistics in a switch's CLI are reported every 10 seconds. If, for example, an interface goes down 3 seconds after the collection of the statistics, the CLI reports only 3 seconds of the statistics and clears all of the other statistics.	6.2(3g)

Virtualization compatibility information

This section lists virtualization compatibility information for the Cisco APIC software.

- For a table that shows the supported virtualization products, see the [ACI Virtualization Compatibility Matrix](#).
- For information about Cisco APIC compatibility with Cisco UCS Director, see the appropriate [Cisco UCS Director Compatibility Matrix](#) document.
- This release supports the following additional virtualization products:

Product	Supported Release
VMM Integration and VMware Distributed Virtual Switch (DVS)	6.5, 6.7, 7.0, 8.0, 9.0. Note: VCF 9.0 integration is supported only on vSphere and not the SDDC manager.
Nutanix	- Prism Central (PC) version: 2022.6.0.4; AOS version 6.5.x - PC version: 2023.1.0.1; AOS version 6.6.x - PC version: 2024.2.0.1; AOS version 6.10.x - PC version: 2024.3.x; AOS version 7.0.x - PC version: 7.3.0.x; AOS version 7.3.0.x - PC version: 7.5.0.x; AOS version 7.5.0.x

Hardware compatibility information

This release supports the following Cisco APIC servers:

Product ID	Description
APIC-L3	Cisco APIC with large CPU, hard drive, and memory configurations (more than 1200 edge ports).
APIC-L4	Cisco APIC with large CPU, hard drive, and memory configurations (more than 1200 edge ports).
APIC-M3	Cisco APIC with medium-size CPU, hard drive, and memory configurations (up to 1200 edge ports).
APIC-M4	Cisco APIC with medium-size CPU, hard drive, and memory configurations (up to 1200 edge ports).
APIC-G5	Cisco APIC with CPU, hard drive, and memory configurations.

The following list includes general hardware compatibility information:

- For the supported hardware, see the [Cisco Nexus 9000 ACI-Mode Switches Release Notes, Release 16.2\(3\)](#).
- Contracts using matchDscp filters are only supported on switches with "EX" on the end of the switch name. For example, N9K-93108TC-EX.
- When the fabric node switch (spine or leaf) is out-of-fabric, the environmental sensor values, such as Current Temperature, Power Draw, and Power Consumption, might be reported as "N/A." A status might be reported as "Normal" even when the Current Temperature is "N/A."

The following table provides compatibility information for specific hardware:

Product ID	Description
Cisco UCS M8-based Cisco APIC	The following PCIe NICs are supported: APIC-O-ID10GC-D, APIC-P-V5Q50G-D (same Cisco VIC 15425). All ports must have the same speed. 10/25G connectivity between the Cisco ACI leaf and Cisco APIC G5 can use either copper or fiber cables with APIC-P-V5Q50G-D/Cisco VIC 15425 network interface card.
Cisco UCS M6-based Cisco APIC	The following PCIe NICs are supported: APIC-P-I8D25GF, APIC-P-ID10GC, APIC-PCIE-C25Q-04 (same Cisco VIC 1455) 10/25GbE ports on APIC-P-I8D25GF can be used as either 10G or 25G ports. All ports must have the same speed. 25G connectivity between Cisco Application Centric Infrastructure (ACI) leaf and Cisco APIC M4/L4 must use copper cable when APIC-P-I8D25GF network interface cards are used. For example, Cisco SFP-H25G-CU1M. 25G connectivity between the Cisco ACI leaf and Cisco APIC M4/L4 can use either copper or fiber cables when APIC-PCIE-C25Q-04/Cisco VIC 1455 network interface cards are used.
Cisco UCS M5-based Cisco APIC	The Cisco UCS M5-based Cisco APIC supports dual speed 10G and 25G interfaces. Connecting the Cisco APIC to the Cisco ACI fabric requires a same speed interface on the Cisco ACI leaf switch. You cannot connect the Cisco APIC directly to the Cisco N9332PQ ACI leaf switch, unless you use a 40G to 10G converter (part number CVR-QSFP-SFP10G), in which case the port on the Cisco N9332PQ switch auto-negotiates to 10G without requiring any manual configuration.
N2348UPQ	To connect the N2348UPQ to Cisco ACI leaf switches, the following options are available: Directly connect the 40G FEX ports on the N2348UPQ to the 40G switch ports on the Cisco ACI leaf switches Break out the 40G FEX ports on the N2348UPQ to 4x10G ports and connect to the 10G ports on all other Cisco ACI leaf switches. Note: A fabric uplink port cannot be used as a FEX fabric port.
N9K-C9348GC-FXP	This switch does not read SPROM information if the PSU is in a shut state. You might see an empty string in the Cisco APIC output.
N9K-C9364C-FX	Ports 49-64 do not support 1G SFPs with QSA.
N9K-C9508-FM-E	The Cisco N9K-C9508-FM-E2 and N9K-C9508-FM-E fabric modules in the mixed mode configuration are not supported on the same spine switch.
N9K-C9508-FM-E2	The Cisco N9K-C9508-FM-E2 and N9K-C9508-FM-E fabric modules in the mixed mode configuration are not supported on the same spine switch. The locator LED enable/disable feature is supported in the GUI and not supported in the Cisco ACI NX-OS switch CLI.

Product ID	Description
N9K-C9508-FM-E2	This fabric module must be physically removed before downgrading to releases earlier than Cisco APIC 3.0(1).
N9K-X9736C-FX	The locator LED enable/disable feature is supported in the GUI and not supported in the Cisco ACI NX-OS Switch CLI.
N9K-X9736C-FX	Ports 29 to 36 do not support 1G SFPs with QSA.

Miscellaneous compatibility information

This release supports the following products:

Product	Supported Release
Cisco NX-OS	16.2(3)
CIMC HUU ISO	Note: Install only the CIMC versions mentioned here in this table. Though other firmware versions may be supported on standard UCS C220/C225 servers, they are not supported on APIC and could lead to issues, including failure to boot. 6.0.2.260143 (recommended) CIMC HUU ISO for UCS C225 M8 (APIC-G5) 6.0.2.260044 CIMC HUU ISO for UCS C225 M8 (APIC-G5) 6.0.1.250192 CIMC HUU ISO for UCS C225 M8 (APIC-G5) 6.0.1.250131 CIMC HUU ISO for UCS C225 M8 (APIC-G5) 6.0.2.260143 (recommended) CIMC HUU ISO for UCS C225 M6 (APIC-L4/M4) (See the related CSCwo74485 software advisory notice before upgrading) 6.0.2.260044 CIMC HUU ISO for UCS C225 M6 (APIC-L4/M4) (See the related CSCwo74485 software advisory notice before upgrading) 6.0.1.250192 CIMC HUU ISO for UCS C225 M6 (APIC-L4/M4) (See the related CSCwo74485 software advisory notice before upgrading) 6.0.1.250131 CIMC HUU ISO for UCS C225 M6 (APIC-L4/M4) (See the related CSCwo74485 software advisory notice before upgrading) 4.3.6.250053 CIMC HUU ISO for UCS C225 M6 (APIC-L4/M4) (See the related CSCwo74485 software advisory notice before upgrading) 4.3.4.252002 CIMC HUU ISO for UCS C225 M6 (APIC-L4/M4) 4.3.2.260020 (recommended) CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3) 4.3.2.260007 CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3) 4.3.2.250016 CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3) 4.3.2.250063 CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3) 4.3.2.240077 CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3)
Nexus Dashboard (ND)	See the ND and Services Compatibility Matrix .

- A known issue exists with the Safari browser and unsigned certificates, which applies when connecting to the Cisco APIC GUI. For more information, see the *Cisco APIC Getting Started Guide*.
- Cisco Nexus Dashboard Insights creates a user in Cisco APIC called cisco_SN_NI. This user is used when Nexus Dashboard Insights needs to make any changes or query any information from the Cisco APIC. In the Cisco APIC, navigate to the **Audit Logs** tab of the **System > History** page. The cisco_SN_NI user is displayed in the User column.

Related content

See the [Cisco Application Policy Infrastructure Controller \(APIC\)](#) page for the documentation.

The documentation includes installation, upgrade, configuration, programming, and troubleshooting guides, technical references, release notes, and knowledge base (KB) articles, as well as other documentation. KB articles provide information about a specific use case or a specific topic.

By using the "Choose a topic" and "Choose a document type" fields of the APIC documentation website, you can narrow down the displayed documentation list to make it easier to find the desired document.

You can watch videos that demonstrate how to perform specific tasks in the Cisco APIC on the [Cisco Cloud Networking](#) YouTube channel.

Temporary licenses with an expiry date are available for evaluation and lab use purposes. They are strictly not allowed to be used in production. Use a permanent or subscription license that has been purchased through Cisco for production purposes. For more information, go to [Cisco Data Center Networking Software Subscriptions](#).

The following table provides links to the release notes, verified scalability documentation, and new documentation:

Document	Description
Cisco Nexus 9000 ACI-Mode Switches Release Notes, Release 16.2(3)	The release notes for Cisco NX-OS for Cisco Nexus 9000 Series ACI-Mode Switches.
<i>Verified scalability guide, Release 6.2(3)</i>	This guide contains the maximum verified scalability limits for Cisco Application Centric Infrastructure (ACI) parameters for Cisco APIC and Cisco Nexus 9000 Series ACI-Mode Switches.
APIC REST API Configuration Procedures	This document resides on developer.cisco.com and provides information about and procedures for using the Cisco APIC REST APIs. The new REST API procedures for this release reside only here and not in the configuration guides. However, older REST API procedures are still in the relevant configuration guides.

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.

© 2026 Cisco Systems, Inc. All rights reserved.