



Cisco Application Policy Infrastructure Controller Release Notes, Release 6.1(4)

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 16.1\(4\)](#).

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

Date	Description
August 26, 2025	Updated the Miscellaneous Compatibility Information table with the recommended CIMC versions for M3/L3 and M4/L4.
August 13, 2025	Release 6.1(4h) became available.

New Software Features

Product Impact	Feature	Description
Base Functionality	Virtual APIC deployment on Nutanix	You can deploy a virtual APIC on an AHV (Acropolis Hypervisor) host using the OVA template in Nutanix. For more information, see the Deploying Cisco Virtual APIC Using Nutanix document.
	OSPF max-metric support on L3Out	OSPF max-metric feature controls the flow of routing information within a network. This feature lets a router advertise its locally generated link-state advertisements (LSAs) with the maximum metric. This makes the router less preferable as a transit path for data traffic. This approach is especially useful during switch reloads, as it prevents the device from being selected for transit traffic until it is operational. For more information, see the Cisco APIC Layer 3 Networking Configuration Guide, Release 6.1(x) .
	Border gateway enhancements	With the Cisco ACI border gateway (BGW) solution, support for normalized (asymmetric) VNI functionality has been enabled. A new Security Group Tag (SGT) has also been introduced to map all endpoints that belong to an SGT from the remote EVPN fabric to a particular ESG. Enhanced support for inter-VRF traffic flows (shared services) across domains. For more information, see the Cisco APIC Layer 3 Networking Configuration Guide, Release 6.1(x) .
Security	Micro-segmentation support for Nutanix	Micro-segmentation support for the Nutanix VMM domain. Support for intra-ESG isolation and enhancements to intra-EPG isolation. For more information, see the Cisco ACI and Nutanix AHV Integration document.
	TACACS+ authentication over TLS	You can configure TACACS+ providers over Transport Layer Security (TLS). TACACS+ over TLS uses certificate-based authentication and supports TLS version 1.3. For more information, see the Cisco APIC Security Configuration Guide, Release 6.1(x) .

Product Impact	Feature	Description
	ESG to classify L3Out traffic	<p>Endpoint Security Groups now offer an alternate way to handle segmentation with an added flexibility of decoupling this from the earlier concepts of forwarding and security associated with Endpoint Groups. Endpoints can now be classified into ESGs by using the <i>Selectors</i> constructs.</p> <p>For more information, see the Cisco APIC Security Configuration Guide, Release 6.1(x).</p>
Interoperability	Multi-site ESG fit and finish	<p>Beginning with Cisco APIC 6.1(4) and Nexus Dashboard (ND) 4.1(1), Endpoint Security Group (ESG) can be configured through ND for Multi-Site use cases. With this, ESGs can be stretched across multiple sites that are connected through ND.</p> <p>For more information see the <i>ESG for ACI, Nexus Dashboard Release 4.1(1)</i> document.</p>
	Cross-launch to Nexus Dashboard cluster from APIC	<p>You can directly navigate to a registered Nexus Dashboard cluster from the APIC GUI without the need for a separate login. The navigation is supported only for Nexus Dashboard release 4.1 or later, and the APIC release 6.1(4) or later.</p> <p>For more information, see the Cisco APIC Getting Started Guide, Release 6.1(x).</p>
	Support for Cisco Nexus Dashboard Insights interface-based filter for ACI traffic analytics	<p>The Traffic Analytics (TA) for Cisco Nexus Dashboard Insights (NDI) feature was introduced in Cisco APIC release 6.1(1). TA automatically discovers services and visualizes flows by matching well-known TCP layer 4 ports to their corresponding service endpoint categories, and identifies congestion, latency, and traffic drops. Traffic analytics provides detailed information about which services are running on the data center switches and the clients that are connected to these services.</p> <p>Beginning with Cisco APIC release, 6.1(4), targeted monitoring is possible at the interface-level. When traffic analytics is enabled on Nexus Dashboard, a REST API call is made to APIC to enable the traffic analytics mode on select interfaces of the switches in the ACI fabric. The switches then export the flow records directly to Nexus Dashboard Insights. You can select the subnets on the L3Out ports to be monitored. Similarly, on spine switches, you can select subnets to be recorded on the ISN/IPN ports. Note that, SPAN and interface-level TA on spines are not supported together.</p> <p>To confirm the configurations on the switch, use the show flow monitor and show flow exporter commands.</p> <p>See the <i>Analyzing and Troubleshooting the Network, Nexus Dashboard, Release 4.1(1)</i> document for more details.</p>
Ease of use	Support for DSCP-based PFC	<p>Support for DSCP-based PFC for host ports and for spine ports facing the IPN. A new global configuration has been introduced at the QoS class level to impose a <i>no drop</i> packet handling in case of congestion of traffic.</p> <p>For more information, see the Cisco APIC and QoS document.</p>
	Simplified admin password recovery	<p>The admin password can be recovered through a simplified procedure involving the root user, with minimal TAC assistance.</p> <p>For more information, see Cisco APIC Security Configuration Guide, Release 6.1(x).</p>
	APIC GUI enhancements	<p>Faster response and display time for the Capacity Dashboard tabs. Details of more entries are now available in the Fabric Capacity and Leaf switch capacity sub-tabs.</p> <p>For more information, see the Cisco APIC Getting Started Guide, Release 6.1(x).</p>
Scale enhancements	SPAN session scale mode	<p>SPAN session support in scale mode for FX2 and newer switches. In scale mode, there is no limit to the number of source interfaces per switch, and filter groups are not supported. The filter mode supports a maximum of 63 source interfaces per switch. Prior to the 6.1(4) release, the filter mode was implicitly used as the</p>

Product Impact	Feature	Description
		only mode for all SPAN sessions. For details, see the Cisco APIC Basic Configuration Guide, Release 6.1(x) and the Verified Scalability Guide for Cisco APIC, Release 6.1(4) and Cisco Nexus 9000 Series ACI-Mode Switches, Release 16.1(4) .

New Hardware Features

This release adds support for the APIC-G5 servers. For more information, see the [Cisco APIC G5 Server Installation and Service Guide](#).

For the new ACI-mode switch hardware features, see the [Cisco Nexus 9000 ACI-Mode Switches Release Notes, Release 16.1\(4\)](#).

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 "Fixed In" column of the table specifies the 6.1(4) release in which the bug was first fixed.

Bug ID	Description	Fixed in
CSCvt99966	A SPAN session with the source type set to "Routed-Outside" goes down. The SPAN configuration is pushed to the anchor or non-anchor nodes, but the interfaces are not pushed due to the following fault: "Failed to configure SPAN with source SpanFL3out due to Source fvlConn not available".	6.1(4h)
CSCwo08936	After DR promotion with Inband, it is seen that, even though the APIC Connectivity is set to OOB, the MO is updated, but the default route still points to Inband, making it unable to reach any external nw following this action.	6.1(4h)
CSCwo27162	When non-default https port is configured and user is trying to do RMA or Add node workflow from the incoming new node, the workflow might not be able to reach the cluster to fetch details.	6.1(4h)
CSCwp14876	Return PBR traffic dropped on Service Leaf after APIC upgrade due to actrlRule missing to allow traffic.	6.1(4h)
CSCwn54329	Capacity Dashboard page load throws "server is temporarily busy" error when there are high-volume requests on nginx especially in bigger scale setups.	6.1(4h)

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 6.1(4) releases in which the bug exists. A bug might also exist in releases other than the 6.1(4) releases.

Bug ID	Description	Exists in
CSCwm38976	EP behind a Remote Leaf accessing the server behind a non anchor node in floating L3out in the main pod. It fails because the BL in the main pod uses PTEP for non anchor nodes instead of Routable TEP. We do not allocate a Routable TEP for a leaf if it is configured as a nonanchor node in floating L3out and does not have a regular L3out. This is a baseline issue.	6.1(4h)
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.	6.1(4h)
CSCwg33306	ESG is in on-demand mode and no zoning rules are deployed for the ESG after contract is configured and DEC feature is being used to set pcTag to ESG pcTag. This can lead to traffic drop despite contracts being configured with SECURITY_GROUP_DENY.	6.1(4h)
CSCwg54652	Shared service pervasive subnets were advertised to vxlan sites in both cons/prov VRFs in ACI BGW. In Vxlan BGW solution, When pervasive subnets are leaked from source to destination VRF, ACI is expected to advertise the pervasive subnets only in source VRF to remote side. Here the pervasive routes are getting advertised on both source and destination VRF. (consumer and provider VRFs).	6.1(4h)

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 6.1(4) releases in which the bug exists. A bug might also exist in releases other than the 6.1(4) releases.

Bug ID	Description	Exists in
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.	6.1(4h)
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.	6.1(4h)
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.	6.1(4h)
CSCwj60150	The configuration (EPGs, Contracts, External EPGs etc) is out-of-sync between APIC and ISE.	6.1(4h)
CSCwi86409	SGT bindings missing on ACI.	6.1(4h)
CSCwf78521	A GOLF spine switch advertises the bridge domain prefixes to a GOLF peer in multiple VRF instances.	6.1(4h)
CSCwn30213	If user configures a ongoing atomic counter policy, they may see faults related to packet loss (F1545 and F1547) raised against nodeToVpc paths involving Border Gateways.	6.1(4h)

Bug ID	Description	Exists in
CSCvj26666	The " show run leaf spine <nodeld>" command might produce an error for scaled up configurations.	6.1(4h)
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.	6.1(4h)
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.	6.1(4h)
CSCvs19322	Upgrading Cisco APIC from a 3.x release to a 4.x release causes Smart Licensing to lose its registration. Registering Smart Licensing again will clear the fault.	6.1(4h)
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.	6.1(4h)
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.	6.1(4h)
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.	6.1(4h)
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.	6.1(4h)
CSCvy45358	The file size mentioned in the status managed object for techsupport "dbgexpTechSupStatus" is wrong if the file size is larger than 4GB.	6.1(4h)
CSCvz06118	In the "Visibility and Troubleshooting Wizard," ERSPAN support for IPv6 traffic is not available.	6.1(4h)
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.	6.1(4h)
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.)	6.1(4h)
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.	6.1(4h)

Bug ID	Description	Exists in
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.	6.1(4h)
CSCwf71934	Multiple duplicate subnets are created on Nutanix for the same EPG.	6.1(4h)
CSCwh74888	With the addressing of CSCwe64407, a release that integrates that bug fix can the 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.	6.1(4h)
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.	6.1(4h)
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.	6.1(4h)
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.	6.1(4h)
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.	6.1(4h)
N/A	When there are silent hosts across sites, ARP glean messages might not be forwarded to remote sites if a leaf switch without -EX or a later designation in the product ID happens to be in the transit path and the VRF is deployed on that leaf switch, the switch does not forward the ARP glean packet back into the fabric to reach the remote site. This issue is specific to transit leaf switches without -EX or a later designation in the product ID and does not affect leaf switches that have -EX or a later designation in the product ID. This issue breaks the capability of discovering silent hosts.	6.1(4h)
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.	6.1(4h)
N/A	MPLS interface statistics shown in a switch's CLI get cleared after an admin or operational down event.	6.1(4h)

Bug ID	Description	Exists in
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.	6.1(4h)

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	Information Location
VMM Integration and VMware Distributed Virtual Switch (DVS)	6.5, 6.7, 7.0 and 8.0.	Cisco ACI Virtualization Guide, Release 6.1(x)
Nutanix	<ul style="list-style-type: none"> Prism Central (PC) version: 2022.6.0.4; AOS version 6.5.x Prism Central (PC) version: 2023.1.0.1; AOS version 6.6.x Prism Central (PC) version: 2024.2.0.1; AOS version – 6.10.x 	N/A

Hardware Compatibility Information

This release supports the following Cisco APIC servers:

Product ID	Description
APIC-L2	Cisco APIC with large CPU, hard drive, and memory configurations (more than 1000 edge ports).
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-M2	Cisco APIC with medium-size CPU, hard drive, and memory configurations (up to 1000 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 16.1\(4\)](#).
- 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."
- First generation switches (switches without -EX, -FX, -GX, or a later suffix in the product ID) do not support Contract filters with match type "IPv4" or "IPv6." Only match type "IP" is supported. Because of this, a contract will match both IPv4 and IPv6 traffic when the match type of "IP" is used.

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 M4-based Cisco APIC	The Cisco UCS M4-based Cisco APIC and previous versions support only the 10G interface. 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.
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

Product ID	Description
	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.
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	16.1(4)
CIMC HUU ISO	<p>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.</p> <ul style="list-style-type: none"> • 4.3.6.250044 CIMC HUU ISO for UCS C225 M8 (APIC-G5) • 4.3.4.252002 (recommended) CIMC HUU ISO for UCS C225 M6 (APIC-L4/M4) • 4.3.2.250016 (recommended) CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3) • 4.3.4.241063 CIMC HUU ISO for UCS C225 M6 (APIC-L4/M4) • 4.3.2.240077 CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3) • 4.3.2.240009 CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3) and UCS C225 M6 (APIC-L4/M4) • 4.3.2.230207 CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3) and UCS C225 M6 (APIC-L4/M4) • 4.2(3e) CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3) and UCS C225 M6 (APIC-L4/M4) • 4.2(3b) CIMC HUU ISO for UCS C225 M6 (APIC-L4/M4) • 4.2(3b) CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3) • 4.2(2a) CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3) • 4.1(3m) CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3) • 4.1(3f) CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3) • 4.1(3d) CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3) • 4.1(3c) CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3) • 4.1(2m) CIMC HUU ISO (recommended) for UCS C220/C240 M4 (APIC-L2/M2) • 4.1(2k) CIMC HUU ISO for UCS C220/C240 M4 (APIC-L2/M2) • 4.1(2g) CIMC HUU ISO for UCS C220/C240 M4 (APIC-L2/M2) • 4.1(2b) CIMC HUU ISO for UCS C220/C240 M4 (APIC-L2/M2)

Product	Supported Release
	<ul style="list-style-type: none"> • 4.1(1g) CIMC HUU ISO for UCS C220/C240 M4 (APIC-L2/M2) and M5 (APIC-L3/M3) • 4.1(2a) CIMC HUU ISO for UCS C220 M4 (APIC-L2/M2) (deferred release) • 4.1(1d) CIMC HUU ISO for UCS C220 M5 (APIC-L3/M3) • 4.1(1c) CIMC HUU ISO for UCS C220 M4 (APIC-L2/M2) • 4.0(4e) CIMC HUU ISO for UCS C220 M5 (APIC-L3/M3) • 4.0(2g) CIMC HUU ISO for UCS C220/C240 M4 and M5 (APIC-L2/M2 and APIC-L3/M3) • 4.0(1a) CIMC HUU ISO for UCS C220 M5 (APIC-L3/M3) • 3.0(4d) CIMC HUU ISO for UCS C220/C240 M3 and M4 (APIC-L2/M2) • 3.0(3f) CIMC HUU ISO for UCS C220/C240 M4 (APIC-L2/M2) • 2.0(13i) CIMC HUU ISO • 2.0(9c) CIMC HUU ISO • 2.0(3i) CIMC HUU ISO
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 16.1(4)	The release notes for Cisco NX-OS for Cisco Nexus 9000 Series ACI-Mode Switches.

Document	Description
<i>Verified scalability guide, Release 6.1(4)</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.

© 2025 Cisco Systems, Inc. All rights reserved.