



Cisco Application Policy Infrastructure Controller Release Notes, Release 5.2(5)

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 15.2\(5\)](#).

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

Date	Description
May 6, 2024	In the Miscellaneous Compatibility Information section, added: <ul style="list-style-type: none">4.3.2.240009 CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3)
April 29, 2024	In the Miscellaneous Compatibility Information section, added: <ul style="list-style-type: none">4.1(2m) CIMC HUU ISO (recommended) for UCS C220/C240 M4 (APIC-L2/M2)
January 11, 2023	In the Hardware Compatibility Information section, removed APIC-M1 and APIC-L1. The last date of support was October 31, 2021.
November 29, 2022	In the Known Issues section, added: <ul style="list-style-type: none">If you are upgrading to Cisco APIC release 4.2(6o), 4.2(7l), 5.2(1g), or later, ensure that any VLAN encapsulation blocks that you are explicitly using for leaf switch front panel VLAN programming are set as "external (on the wire)." If these VLAN encapsulation blocks are instead set to "internal," the upgrade causes the front panel port VLAN to be removed, which can result in a datapath outage.
November 18, 2022	In the Open Issues section, added bug CSCwc66053.
September 27, 2022	In the Open Issues section, added bug CSCwc49449.
August 1, 2022	In the Miscellaneous Compatibility Information section, added: <ul style="list-style-type: none">4.2(2a) CIMC HUU ISO (recommended) for UCS C220/C240 M5 (APIC-L3/M3)4.1(2k) CIMC HUU ISO (recommended) for UCS C220/C240 M4 (APIC-L2/M2)
July 29, 2022	Release 5.2(5e) became available; there are no changes to this document for this release. See the Cisco Nexus 9000 ACI-Mode Switches Release Notes, Release 15.2(5) for the changes in this release.
July 1, 2022	Release 5.2(5d) became available. Added a resolved bug for this release.
June 30, 2022	In the section Miscellaneous Compatibility, added information about Cisco Nexus Dashboard Insights creating the cisco_SN_NI user.
May 26, 2022	In the Open Issues section, added bug CSCwa90084.
May 15, 2022	Release 5.2(5c) became available.

New Software Features

Feature	Description
Transport Layer Security version 1.3 support	Transport Layer Security (TLS) version 1.3 is now supported.

New Hardware Features

For the new hardware features, see the [Cisco Nexus 9000 ACI-Mode Switches Release Notes, Release 5.2\(5\)](#).

Changes in Behavior

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

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 5.2(5) releases in which the bug exists. A bug might also exist in releases other than the 5.2(5) releases.

Bug ID	Description	Exists in
CSCwf61646	Adding wildcard entry (entry with etherType=unspecified) to a filter that has more specific entries (specific ethertype/protocol/etc) can cause SDKHAL to crashSwitch will crash constantly and eventually may come up with either a different image (golden image)	5.2(8c) and later
CSCwh41865	When upgrading an APIC, the "from" version is displayed as "to" version in the event record.	5.2(5e) and later
CSCvg81020	For strict security requirements, customers require custom certificates that have RSA key lengths of 3072 and 4096.	5.2(5c) and later
CSCvm56946	Support for local user (admin) maximum tries and login delay configuration.	5.2(5c) and later
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".	5.2(5c) and later
CSCvy00746	A breakout parent port shows in the drop-down list for the SPAN source even after the port is broken out.	5.2(5c) and later
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.	5.2(5c) and later
CSCvz72941	While performing ID recovery, id-import gets timed out. Due to this, ID recovery fails.	5.2(5c) and later
CSCvz83636	For a health record query using the last page and a time range, the GUI displays some health records with a creation time that is beyond the time range (such as 24h).	5.2(5c) and later

Bug ID	Description	Exists in
CSCwa53478	After migrating a VM between two hosts using VMware vMotion, EPG does not get deployed on the target leaf node. When affected, the fvIfConn managed object corresponding to the missing EPG can be seen on APIC, but it would be missing from the target leaf node when queried.	5.2(5c) and later
CSCwa58709	The GIPo address is only visible on APIC 1 when using the command "cat /data/data_admin/sam_exported.config". The command output from the other APICs outputs do not show the GIPo address.	5.2(5c) and later
CSCwa90058	When a VRF-level subnet <fvRtSummSubnet> and instP-level subnet <l3extSubnet> with a summary policy is configured for an overlapping subnet, the routes will get summarized by the configuration that was added first. But, the fault on the configuration that was added last will not be shown in the Cisco APIC GUI.	5.2(5c) and later
CSCwa90084	<ul style="list-style-type: none"> - Traffic disruption across a vPC pair on a given encapsulation. OR - EPG flood in encap blackholing on a given encapsulation. OR - STP packets received on an encapsulation on a given port are not forwarded on all the leaf switches where the same EPG/same encapsulation is deployed. 	5.2(5c) and later
CSCwc49449	When a maintenance policy has multiple switch nodes, such as vPC pair nodes, an SMU's uninstallation gets stuck in the "queued" state for one of the nodes.	5.2(5c) and later
CSCwc66053	Preconfiguration validations for L3Outs that occur whenever a new configuration is pushed to the Cisco APIC might not get triggered.	5.2(5c) and later
CSCwd44827	APIC fails to update standalone Layer3 controller subnet on its fabric. The following fault is raised. F609478 - [FSM:FAILED]: Update Standalone Controller Subnet(TASK:ifc:polycmgr:FabricCtrlrConfigPUUpdatePodConnPDef)	5.2(5c) and later
CSCwe09859	The OpFlex agent on a hypervisor randomly disconnects, impacting VM traffic.	5.2(5c) and later
CSCwe52465	The NICC app image fails to load.	5.2(5c) and later
CSCwe58398	<p>This is added functionality for upgrade show command.</p> <ol style="list-style-type: none"> 1. aci diag show postupgrade -service <dme> -> This gives details for dmes and which shard still have pending postUpgradeCb. 2. aci diag show postupgrade -service <dme> -shard <shard_id> -> This gives the details of log path for the dmes and shard for which postUpgradeCb has been completed. 	5.2(5c) and later
CSCwe66712	For a customer using America/Mexico_City time, the DST time change will still happen on APIC in the year 2023.	5.2(5c) and later
CSCwf19660	Major fault F3083 ("IP detected on multiple MACs") is raised under a uEPG and ESG when an EPG selector is configured in the ESG.	5.2(5c) and later
CSCwf54771	User configuration is missing on APICs and switches following an ungraceful reload or power outage.	5.2(5c) and later

Bug ID	Description	Exists in
CSCwf92856	During upgrade "deserialization error" is seen on APIC 1 PD.	5.2(5c) and later
CSCwh17898	The "panic: runtime error: invalid memory address or nil pointer dereference." Error occurred and then F1419 (Service kron failed on apic) was raised.	5.2(5c) and later
CSCwh47921	Numerous files that are in the deleted state, but are still being used by multiple processes, are not allowing the files to be removed from the file system. This causes the Cisco APIC storage to surpass the 90% threshold of log rotation.	5.2(5c) and later
CSCwh81272	The system resets due to a policyelem high availability policy reset.	5.2(5c) and later
CSCwh83273	A Cisco APIC cannot be added to the cluster because the GUI rejects the ID if is not within the range of 1-7.The Initial Setup Configuration states that the fabric ID valid range is 1-128.	5.2(5c) and later
CSCwh84052	When using the OpenStack integration, the Cisco APIC VMM Manager process may consume more memory than is available and then end.	5.2(5c) and later
CSCwh98712	When running "show running-config" from API CLI, the command takes several minutes to complete. Several thousand API requests are seen in access.log querying ptpRsProfile on every static path.	5.2(5c) and later
CSCwi01316	In the following topology: Tenant 1: VRF 1 > EPG A, EPG B. There is an any-to-any Intra VRF instance contract and EPG A and B are providers for an inter-VRF instance contract. VRF 2 > L3Out or EPG. The VRF instance consumes the inter-VRF instance contract. Traffic will unexpectedly get sent to the wrong rule when inter-VRF instance traffic is flowing.	5.2(5c) and later
CSCwi34095	App installation fails on the Cisco APIC with the error "Unable to add elasticsearch credentials" . This is seen for any app making use of Elasticsearch, such as Nexus Insight Cloud Connector.	5.2(5c) and later
CSCwi40671	In a remote leaf switch, when the initial policy download happens, nginx generates a core. The process recovers by itself after a restart. This issue does not have any major functionality impact.	5.2(5c) and later
CSCwi52324	The fault F3227 "ACI failed processing an already accepted configuration change" continuously gets raised	5.2(5c) and later
CSCwi78474	An upgraded Cisco APIC may attempt the second upgrade to same version and assume itself as APIC 1, which can cause all Cisco APICs to stop the postUpgradeCb process, which stops the upgrade.	5.2(5c) and later
CSCwj17966	The Cisco APIC bootmgr or appliance director allows an incorrect attribute/value update to be received in LLDP TLV due to miscabling.	5.2(5c) and later
CSCwj69046	SAML authentication fails when using the HTTPS Proxy 5.2 image.	5.2(5c) and later

Bug ID	Description	Exists in
CSCwb93239	The GUI displays the following error: Failed, Local Upload Failure Msg (Request failed with status code 413).	5.2(5c)

Resolved Issues

Bug ID	Description	Fixed in
CSCwb93239	The GUI displays the following error: Failed, Local Upload Failure Msg (Request failed with status code 413).	5.2(5d)
CSCwa99045	VMM domain attachments of floating SVIs configured for dual stack with the same encapsulation and the same VMM domain attachments are not being cleaned up after downgrading from 5.2(5) to an earlier release.	5.2(5c)
CSCwa58061	When there are more than 40 objects in the tree and you double click on an object in the BGP Peer table, then the tree does not expand because the tree does not have pagination. The APIC tries to load all objects in one query, which is drastically slows the GUI.	5.2(5c)
CSCwa78740	When HBR is enabled on a source EPG's bridge domain and the subnet is configured with the private scope (advertise externally = FALSE), if there is a shared service EPG contract with an L3Out, the L3Out will not publish the subnet or the corresponding /32 host routes because of this private scope. In this scenario, if there is also an explicit ESG leakRoute configured for the same subnet across those VRF instances, the leakRoute is faulted because the route is already shared with an EPG contract, and the leakRoute is installed in the hardware along with a pcTag, then the leakRoute should not be processed and any flags under it should not be considered. But, if this explicit leakRoute has a public scope, the /32 host routes are still published externally out of the L3Out, which should not happen as the leakRoute itself is faulted and bridge domain subnet scope is private.	5.2(5c)
CSCwa95297	When a VRF-level subnet, fvRtSummSubnet, exists with a summary policy and an instP level subnet, <l3extSubnet>, with the same subnet as the VRF-level subnet is associated with summary policy, then there won't be any fault seen on the Cisco APIC. The summarization will be done according to the VRF-level subnet <fvRtSummSubnet>.	5.2(5c)
CSCwb00781	Importing the routing table of a remote site carries the wrong autonomous system number (ASN).	5.2(5c)
CSCwb56853	Spine switches repeatedly reload, many services are tainted, and the stack trace of the kernel contains messages that state "out of memory" and "Page fault."	5.2(5c)
CSCwb73716	When the Nexus Insights Cloud Connector comes up the first time in APIC, there is a possibility the TAC Assist jobs might take longer or fail.	5.2(5c)

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 5.2(5) releases in which the bug exists. A bug might also exist in releases other than the 5.2(5) releases.

Bug ID	Description	Exists in
CSCuu11416	An endpoint-to-endpoint ACI policy that uses Layer 2 traffic with an IPv6 header does not get counted within or across ESGs/EPGs.	5.2(5c) and later
CSCvj26666	The "show run leaf spine <nodeld>" command might produce an error for scaled up configurations.	5.2(5c) and later
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.	5.2(5c) and later
CSCvq39764	When you click Restart for the Microsoft System Center Virtual Machine Manager (SCVMM) agent on a scaled-out setup, the service may stop. You can restart the agent by clicking Start.	5.2(5c) and later
CSCvq58953	One of the following symptoms occurs: App installation/enable/disable takes a long time and does not complete. Nomad leadership is lost. The output of the aci diag scheduler logs members command contains the following error: Error querying node status: Unexpected response code: 500 (rpc error: No cluster leader)	5.2(5c) and later
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.	5.2(5c) and later
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.	5.2(5c) and later
CSCvs77929	In the 4.x and later releases, if a firmware policy is created with different name than the maintenance policy, the firmware policy will be deleted and a new firmware policy gets created with the same name, which causes the upgrade process to fail.	5.2(5c) and later
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.	5.2(5c) and later
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.	5.2(5c) and later
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.	5.2(5c) and later
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.	5.2(5c) and later
CSCvy34357	Starting with the 5.2(5) release, the following apps built with the following non-compliant Docker versions cannot be installed nor run: <ul style="list-style-type: none"> ConnectivityCompliance 1.2 SevOneAciMonitor 1.0 	5.2(5c) and later

Bug ID	Description	Exists in
CSCvy45358	The file size mentioned in the status managed object for techsupport "dbgexpTechSupStatus" is wrong if the file size is larger than 4GB.	5.2(5c) and later
CSCvz06118	In the "Visibility and Troubleshooting Wizard," ERSPAN support for IPv6 traffic is not available.	5.2(5c) and later
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.	5.2(5c) and later
CSCvz85579	<p>VMMmgr process experiences a very high load for an extended period of time that impacts other operations that involve it.</p> <p>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:</p> <p style="padding-left: 40px;">oom_reaper: reaped process 5578 (svc_ifc_vmmmgr.)</p>	5.2(5c) and later
CSCwa78573	<p>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.</p> <p>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.</p>	5.2(5c) and later
CSCwk21572	License manager occasionally cores after image upgrade.	5.2(5c) and later
N/A	If you are upgrading to Cisco APIC release 4.2(6o), 4.2(7l), 5.2(1g), or later, ensure that any VLAN encapsulation blocks that you are explicitly using for leaf switch front panel VLAN programming are set as "external (on the wire)." If these VLAN encapsulation blocks are instead set to "internal," the upgrade causes the front panel port VLAN to be removed, which can result in a datapath outage.	5.2(5c) and later
N/A	<p>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.</p> <p>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.</p>	5.2(5c) and later
N/A	If you use the REST API to upgrade an app, you must create a new firmware.OSource to be able to download a new app image.	5.2(5c) and later
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.	5.2(5c) and later

Bug ID	Description	Exists in
N/A	With a non-english SCVMM 2012 R2 or SCVMM 2016 setup and where the virtual machine names are specified in non-english characters, if the host is removed and re-added to the host group, the GUID for all the virtual machines under that host changes. Therefore, if a user has created a micro segmentation endpoint group using "VM name" attribute specifying the GUID of respective virtual machine, then that micro segmentation endpoint group will not work if the host (hosting the virtual machines) is removed and re-added to the host group, as the GUID for all the virtual machines would have changed. This does not happen if the virtual name has name specified in all english characters.	5.2(5c) and later
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.	5.2(5c) and later
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.	5.2(5c) and later
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.	5.2(5c) and later
N/A	MPLS interface statistics shown in a switch's CLI get cleared after an admin or operational down event.	5.2(5c) and later
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.	5.2(5c) and later

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
Microsoft Hyper-V	<ul style="list-style-type: none"> SCVMM 2019 RTM (Build 10.19.1013.0) or newer SCVMM 2016 RTM (Build 4.0.1662.0) or newer SCVMM 2012 R2 with Update Rollup 9 (Build 3.2.8145.0) or newer 	N/A

Product	Supported Release	Information Location
VMM Integration and VMware Distributed Virtual Switch (DVS)	6.5, 6.7, and 7.0	Cisco ACI Virtualization Guide, Release 5.2(x)

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-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)

The following list includes general hardware compatibility information:

- For the supported hardware, see the [Cisco Nexus 9000 ACI-Mode Switches Release Notes, Release 15.2\(5\)](#).
- 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 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

Product ID	Description
	which case the port on the Cisco N9332PQ switch auto-negotiates to 10G without requiring any manual configuration.
N2348UPQ	<p>To connect the N2348UPQ to Cisco ACI leaf switches, the following options are available:</p> <p>Directly connect the 40G FEX ports on the N2348UPQ to the 40G switch ports on the Cisco ACI leaf switches</p> <p>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.</p> <p>Note: A fabric uplink port cannot be used as a FEX fabric port.</p>
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	<p>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.</p> <p>The locator LED enable/disable feature is supported in the GUI and not supported in the Cisco ACI NX-OS switch CLI.</p>
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	15.2(5)
Cisco UCS Manager	2.2(1c) or later is required for the Cisco UCS Fabric Interconnect and other components, including the BIOS, CIMC, and the adapter.
CIMC HUU ISO	<ul style="list-style-type: none"> 4.3.2.240009 CIMC HUU ISO (recommended) for UCS C220/C240 M5 (APIC-L3/M3) 4.2(3e) CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3) 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)

Product	Supported Release
	<ul style="list-style-type: none"> • 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) • 4.1(1g) CIMC HUU ISO for UCS C220/C240 M4 (APIC-L2/M2) and M5 (APIC-L3/M3) • 4.1(1f) 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
Network Insights Base, Network Insights Advisor, and Network Insights for Resources	<p>For the release information, documentation, and download links, see the Cisco Network Insights for Data Center page.</p> <p>For the supported releases, see the Cisco Data Center Networking Applications Compatibility Matrix.</p>

- This release supports the partner packages specified in the [L4-L7 Compatibility List Solution Overview](#) document.
- 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, Release 5.2\(x\)](#).
- For compatibility with Day-2 Operations apps, see the [Cisco Data Center Networking Applications Compatibility Matrix](#).
- 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 Data Center 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 15.2(5)	The release notes for Cisco NX-OS for Cisco Nexus 9000 Series ACI-Mode Switches.
Verified Scalability Guide for Cisco APIC, Release 5.2(5) and Cisco Nexus 9000 Series ACI-Mode Switches, Release 15.2(5)	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.

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.

© 2022–2024 Cisco Systems, Inc. All rights reserved.