Cisco Application Policy Infrastructure Controller Release Notes, Release 6.0(8)

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 16.0(8).

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

Date	Description
June 16, 2025	Release 6.0(8h) became available; CSCwn59662 was added to the list of Resolved Issues.
May 30, 2025	The Miscellaneous Compatibility Information table was updated to indicate support for 4.3.2.250016 CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3).
December 4, 2024	Release 6.0(8f) became available.
October 28, 2024	Release 6.0(8e) became available.

New Software Features

Product Impact	Feature	Description
N/A	N/A	There are no new software features in this release.

New Hardware Features

For the new hardware features, see the Cisco Nexus 9000 ACI-Mode Switches Release Notes, Release 16.0(8).

Changes in Behavior

For the changes in behavior, see Cisco ACI Releases Changes in Behavior.

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 6.0(8) releases in which the bug exists. A bug might also exist in releases other than the 6.0(8) releases.

Bug ID	Description	Exists 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 fvIfConn not available".	6.0(8e) and later

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.	6.0(8e) and later
CSCwa90084	- Traffic gets disrupted across a vPC pair on a given encapsulation. OR - EPG flood in encapsulation gets blackholed 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.	6.0(8e) and later
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.	6.0(8e) and later
CSCwf78521	A GOLF spine switch advertises the bridge domain prefixes to a GOLF peer in multiple VRF instances.	6.0(8e) and later
CSCwf99067	Deleting and re-adding RedirectDest with a different IP address, but the same MAC address, generates the following error: "Same virtual MAC is provided for different RedirectDest".	6.0(8e) and later
CSCwh63412	Audit logs under System > History > Audit Logs are limited to the current logged in user. Only the user with the username admin can see the audit logs from all users, but other users despite having admin privileges cannot see the audit logs from other users. The audit logs under Tenants are visible to every user.	6.0(8e) and later
CSCwi28712	Additional entries of svcredirRsBackupDestAttMo and svcredirRsDestAttMo are created in a leaf switch. This can impact the traffic hash and can lead to traffic drop.	6.0(8e) and later
CSCwk35279	The second vPC pair switch was stuck in the "Queued" state.	6.0(8e) and later
CSCwc50398	Licensemgr process crashes on node-1, with Smart license mode being "Direct connection to CSSM" under smart license settings.	6.0(8e) and later
CSCwn59662	After upgrading an ACI leaf, the GBP cache may miss some contracts, which can cause traffic disruptions for the affected EPGs. On the OSP/compute node, this issue may manifest as policy miss drops in OVS, specifically indicated by POL_TABLE MISS.	6.0(8e), 6.0(8f)

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 6.0(8) release in which the bug was first fixed.

Bug ID	Description	Fixed in
CSCwn59662	After upgrading an ACI leaf, the GBP cache may miss some contracts, which can cause traffic disruptions for the affected EPGs. On the OSP/compute node, this issue may manifest as policy miss drops in OVS, specifically indicated by POL_TABLE MISS.	6.0(8h)

Bug ID	Description	Fixed in
CSCwf17013	Trigger inventory sync- Failed.	6.0(8e)
CSCwh08862	In a configuration that has IPv4 disabled, the replace operation performed from the GUI fails.	6.0(8e)
CSCwh56468	"No data stats to display" in stats tab for some L3out profile, while for others it works fine.	6.0(8e)
CSCwh82544	This is a modification on the product to adopt new secure code best practices to enhance the security posture and resiliency of the product.	6.0(8e)
CSCwh92412	DELETE Queries from Kubernetes CNI causing tracebacks on the APIC.	6.0(8e)

CSCwh96100	Login to apic in the following way works:
	
	`C:\Users\>ssh admin@`
	`Application Policy Infrastructure Controller`
	`admin@10.48.22.94's password:`
	`Last login: 2023-10-24T10:38:34.000+02:00 UTC`
	`bdsol-aci13-apic1#`
	
	When we add for example, show endpoint we get the following error:
	
	`C:\Users\>ssh admin@ show endpoint`
	`Application Policy Infrastructure Controller`
	`admin@10.48.22.94's password:`
	`Unknown scope: endpoint`
	
	This command is being deprecated on APIC controller, please use NXOS-style equivalent command.
		6.0(8e)

CSCwi17652	Service-ep flag get enabled for service device with no redirect policy (no PBR).	6.0(8e)
CSCwi78265	Operational tab shows useg EPGs under ESG column of the base EPG.	6.0(8e)
CSCwi97447	Leaf took a longer time to push add/delete of config, Seen so far with the acc-provision tool while adding/removing an opflex integration.	6.0(8e)
CSCwj03122	Leaf connected to ESXi hosts with VMM integration may crash due to OOM.	6.0(8e)
CSCwj05269	Endpoints were in down state after node is restarted.	6.0(8e)
CSCwj11115	When executing an API call, APIC responds to an xml query with the server name for a virtual machine (VM) with the name "GK R&D Server". Therefore, the automation tool, cannot interpret the data because of the "&" character in the response.	6.0(8e)
CSCwj11163	++ Leaf reset due to kernel-panic. ++ High memory due to SCVMM partially update	6.0(8e)
CSCwj71077	ntpd_logs to is not part of switch policy techsupport. It is only available on local techsupport.	6.0(8e)
CSCwj88821	Cannot delete static node mgmt address.	6.0(8e)

Bug ID	Description	Fixed in
CSCwj94500	Syslog messages generated by ACI mode switches or APIC's may not be received by syslog destinations, including local syslog files and remote syslog destination. Stack trace or core file information is required to generated to confirm signature of issue.	6.0(8e)
CSCwk15849	The leaf crashed in continue due out of memory. ptplc_sdk invoked oom-killer opflexp dme crashed as well due to oom.	6.0(8e)
CSCwk19612	In the UI, go to Tenant->application profile and select an application profile. The number of EPG in the summary includes shadow objects regardless the option "show hidden policy" selected in settings. The list of EPG under the application profile on the panel on the left reflect the option selected.	6.0(8e)
CSCwk28521	If l3out pbr Ipv4 prefix is leaked using "Shared Route Control Subnet" knob, and then remove "Shared Route Control Subnet" in the prefix, the actual route won't get removed in the provider vrf until the last prefix in the instp removes advertising the prefix.	6.0(8e)
CSCwm03003	Fault F4388 is raised, indicating a warning for high inode usage on APIC.	6.0(8e)
CSCwm30830	GPB policy where Pod EPG/BD missed under VRF <sample JSON> ,if you look at the children part of the JSON, you should see all EPG / BDs within this VRF. We see only node network and service network, which is used for PBR. The Pod's EPG is missingAs result, OVS gets misprogrammed, that leads to wrong communication flows.For example: traffic from the node network to the pod network get snat in OSP OVS and send out to L3OUT.	6.0(8e)
CSCwm32859	Vmotion/Live Migration (LM) leads to connectivity failure for virtual machines as they are not registered on new location in a timely manner. Opflex Proxy is unable to send disconnect to Opflex Agent after Vmotion/LM.	6.0(8e)
CSCwm61087	opflex-agent connected to the source leaf pair after migration to destination leaf pair. MAC address entry did not disappear, new ODev on destination leafs was not created, source leaf did not send platform config delete.	6.0(8e)
CSCwk42626	After the following OS transition, gipoPool settings disappeared when APIC Replace with 6.0(2h).	6.0(8e)

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 6.0(8) releases in which the bug exists. A bug might also exist in releases other than the 6.0(8) releases.

Bug ID	Description	Exists in
CSCvj26666	The "show run leaf|spine <nodeId>" command might produce an error for scaled up configurations.	6.0(8e) 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.	6.0(8e) and later

Bug ID	Description	Exists in
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.	6.0(8e) 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 acidiag scheduler logs members command contains the following error: Error querying node status: Unexpected response code: 500 (rpc error: No cluster leader)	6.0(8e) 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.	6.0(8e) 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.	6.0(8e) 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.	6.0(8e) 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.	6.0(8e) 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.	6.0(8e) 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.	6.0(8e) 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.	6.0(8e) and later
CSCvy34357	Starting with the 6.0(7) release, the following apps built with the following non-compliant Docker versions cannot be installed nor run: • ConnectivityCompliance 1.2 • SevOneAciMonitor 1.0	6.0(8e) and later
CSCvy45358	The file size mentioned in the status managed object for techsupport "dbgexpTechSupStatus" is wrong if the file size is larger than 4GB.	6.0(8e) and later
CSCvz06118	In the "Visibility and Troubleshooting Wizard," ERSPAN support for IPv6 traffic is not available.	6.0(8e) 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.	6.0(8e) and later

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.)	6.0(8e) and later
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.	6.0(8e) and later
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.	6.0(8e) and later
CSCwf71934	Multiple duplicate subnets are created on Nutanix for the same EPG.	6.0(8e) and later
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.	6.0(8e) and later
CSCwh92539	After upgrading a Cisco APIC from a release before 5.2(8) to release 6.0(7) 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.	6.0(8e) and later
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.	6.0(8e) 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.	6.0(8e) 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.	6.0(8e) 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.	6.0(8e) 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.	6.0(8e) 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.	6.0(8e) 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.	6.0(8e) and later
N/A	MPLS interface statistics shown in a switch's CLI get cleared after an admin or operational down event.	6.0(8e) 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.	6.0(8e) 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	• 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, 7.0 and 8.0. **Note**: vSphere 8.0 does not support the vCenter Plug-in and Cisco ACI Virtual Edge (AVE). If you need to continue to use the vCenter Plug-in and Cisco AVE, use vSphere 7.0.	[Cisco ACI Virtualization Guide, Release 6.0(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-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)

The following list includes general hardware compatibility information:

- For the supported hardware, see the [Cisco Nexus 9000 ACI-Mode Switches Release Notes, Release 16.0(8)](#).

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

Product ID	Description
Cisco APIC	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 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	16.0(8)
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	**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.

Product	Supported Release
	• 4.3.4.241063 (recommended) CIMC HUU ISO for UCS C225 M6 (APIC-L4/M4)
	• 4.3.2.240077 (recommended) 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)
	• 4.3.2.240009 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)
	• 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	For the release information, documentation, and download links, see the Cisco Network Insights for Data Center page. For the supported releases, see the Cisco Data Center Networking Applications Compatibility Matrix.

- 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 6.0(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.

- Cisco APIC uses an SSL library called CiscoSSL, which is a customized version of the OpenSSL library to support CVE fixes and FIPS compliance. Cisco maintains an extended support contract with OpenSSL. CVE fixes from OpenSSL upstream is regularly incorporated in the older versions of CiscoSSL library as well.

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 16.0(8)	The release notes for Cisco NX-OS for Cisco Nexus 9000 Series ACI-Mode Switches.
Verified Scalability Guide for Cisco APIC, Releases 6.0(4) through 6.0(8) and Cisco Nexus 9000 Series ACI-Mode Switches, Releases 16.0(4) through 16.0(8)	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.