Cisco Application Policy Infrastructure Controller Release Notes, Release 6.0(2)

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(2).

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

Date	Description
August 2, 2023	Release 6.0(2j) became available. Added the resolved bugs for this release.
July 5, 2023	In the Related Content section, added information about the APIC REST API Configuration Procedures document on developer.cisco.com.
June 21, 2023	In the Miscellaneous Compatibility Information section, added: • 4.2(3e) CIMC HUU ISO (recommended) for UCS C225 M6 (APIC-L4/M4)
March 1, 2023	Release 6.0(2h) became available.

New Software Features

Product Impact	Feature	Description
Base Functionality	Support for Cisco APIC-M4/L4 servers	This release adds support for the APIC-L4 and APIC-M4 servers. For more information, see the Cisco APIC M4/L4 Server Installation and Service Guide.
	Support for Cisco APIC virtual form factor in ESXi	You can deploy a Cisco APIC cluster wherein all the Cisco APICs in the cluster are virtual APICs. You can deploy a virtual APIC on an ESXi using the OVF template. For more information, see the Deploying Cisco Virtual APIC Using VMware vCenter document.
	Support for Cisco APIC cloud form factor using AWS	You can deploy a Cisco APIC cluster wherein all the Cisco APICs in the cluster are virtual APICs. You can deploy a virtual APIC on AWS using the CloudFormation template. For more information, see the Deploying Cisco Virtual APIC Using AWS document.
	BGP additional paths	The BGP speaker can propagate and receive multiple paths for the same prefix without the new paths replacing any previous paths. This feature allows BGP speaker peers to negotiate whether they support advertising and receiving multiple paths per prefix and advertising such paths. Cisco APIC supports only the receive functionality. For more information, see the Cisco APIC Layer 3 Networking Configuration Guide, Release 6.0(x).
	Proportional ECMP	You can use the next-hop propagate and redistribute attached host features to avoid sub-optimal routing in the Cisco ACI fabric. When

Product Impact	Feature	Description
		these features are enabled, packet flows from a non-border leaf switch are forwarded directly to the leaf switch connected to the next-hop address. All next-hops are now used for ECMP forwarding from the hardware. In addition, Cisco ACI now redistributes ECMP paths into BGP for both directly connected next-hops and recursive next-hops. For more information, see the [Cisco APIC Layer 3 Networking Configuration Guide, Release 6.0(x)](#).
	Support for config stripe winner policies	When you configure the Layer 3 IPv4 multicast, you can now configure the config stripe winner policy for a multicast group range within a pod. For more information, see the [Cisco APIC Layer 3 Networking Configuration Guide, Release 6.0(x)](#).
Security	First hop security (FHS) support for VMM	FHS is supported on the VMware DVS VMM domain. Ensure to enable intra EPG isolation for implementing FHS within an EPG. For more information, see the [Cisco APIC Security Configuration Guide, Release 6.0(x).](#)
	TACACS external logging for switches	You can enable TACACS external logging for switches. When enabled, the Cisco APIC collects the same types of AAA data from the switches in the chosen TACACS monitoring destination group. For more information, see the [Cisco ACI TACACS External Logging](#).
Performance and Scalability	Scale enhancements	10,000 VRF instances per fabric - Mis-Cabling Protocol (MCP): 2,000 VLANs per interface and 12,000 logical ports (port x VLAN) per leaf switch 200 IP SLA probes per leaf switch 24 leaf switches (12 pairs) in the same L3Out 2,000 sub-interfaces (BGP, OSPF, and static) 2,000 bidirectional forwarding detection (BFD) sessions
Upgrade/Downgrade	Auto firmware update for Cisco APIC on discovery	When you add a new Cisco APIC to the fabric either through Product Returns & Replacements (RMA), cluster expansion, or commission, it is automatically upgraded to the same version of the existing cluster. For more information, see the the [Cisco APIC Installation and ACI Upgrade and Downgrade Guide](#).
	Installing switch software maintenance upgrade patches without reloading	Some switch software maintenance upgrade (SMU) patches do not require you to reload the switch after you install those patches. For more information, see the [Cisco APIC Installation and ACI Upgrade and Downgrade Guide](#).
Interoperability	Cisco Nexus Cloud support	This release adds support for Cisco Nexus Cloud, which enables telemetry collection from the Cisco Nexus switches. For more information, see the [Cisco Nexus Cloud documentation](#).
Ease of Use	Troubleshooting Cisco APIC QoS Policies	You can view the QoS statistics by using the Cisco APIC GUI. For more information, see the [Cisco APIC and QoS](#) document.

New Hardware Features

For the new hardware features, see the [Cisco Nexus 9000 ACI-Mode Switches Release Notes, Release 16.0(2)](#).

Changes in Behavior

- Scale enhancements:

  ○ 10,000 VRF instances per fabric

  ○ Mis-Cabling Protocol (MCP): 2,000 VLANs per interface and 12,000 logical ports (port x VLAN) per leaf switch

  ○ 200 IP SLA probes per leaf switch

  ○ 24 leaf switches (12 pairs) in the same L3Out

  ○ 2,000 sub-interfaces (BGP, OSPF, and static)

  ○ 2,000 bidirectional forwarding detection (BFD) sessions

  ○ Longest Prefix Matches (LPM): 440,000 IPv4 and 100,000 IPv6 routes

- To upgrade to this release, you must perform the following procedure:

  1. Download the 6.0(2) Cisco APIC image and upgrade the APIC cluster to the 6.0(2) release. Before this step is completed, DO NOT download the Cisco ACI-mode switch images to the APIC. The 6.0(2) release has both 32-bit and 64-bit switch images, but releases prior to 6.0(2) do not support 64-bit images. As a result, downloading the 64-bit images at this time might cause errors or unexpected results.

  2. Download both the 32-bit and 64-bit images to the Cisco APIC. Downloading only one of the images may result in errors during the upgrade process.

  3. Create the maintenance groups and trigger the upgrade procedure as usual. Cisco APIC automatically deploys the correct image to the respective switch during the upgrade process.

  For more information, see the [Cisco APIC Installation and ACI Upgrade and Downgrade Guide](#).

- On the "Interface Configuration" GUI page (**Fabric > Access Policies > Interface Configuration**), the node table now contains the following columns:

  ○ Interface Description: The user-entered description of the interface. You can edit the description by clicking ... and choosing **Edit Interface Configuration**.

  ○ Port Direction: The direction of the port. Possible values are "uplink," "downlink," and "default." The default value is "default," which indicates that the port uses its default direction. The other values display if you converted the port from uplink to downlink or downlink to uplink.

- There is now a "Switch Configuration" GUI page (**Fabric > Access Policies > Switch Configuration**) that shows information about the leaf and spine switches controlled by the Cisco APIC. This page also enables you to modify a switch's configuration to create an access policy group and fabric policy group, or to remove the policy groups from 1 or more nodes. This page is similar to the "Interface Configuration" GUI page that existed previously, but is for switches.

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

- The "Images" GUI page (**Admin > Firmware > Images**) now includes a "Platform Type" column, which specifies whether a switch image is 64-bit or 32-bit. This column does not apply to Cisco APIC images.

- The initial cluster set up and bootstrapping procedure has been simplified with the introduction of the APIC Cluster Bringup GUI. The APIC Cluster Bringup GUI supports virtual and physical APIC platforms.

- When you configure a custom certificate for Cisco ACI HTTPS access, you can now choose the elliptic-curve cryptography (ECC) key type. Prior to this release, RSA was the only key type.

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(2) releases in which the bug exists. A bug might also exist in releases other than the 6.0(2) 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(2h) 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.	6.0(2h) and later
CSCwd81562	A Cisco APIC that was previously part of the Cisco APIC cluster will not rejoin the cluster after the reload, decommission, and commission process.	6.0(2h) and later
CSCwd82212	There is a login denied error while importing or exporting a configuration.	6.0(2h) and later
CSCwe01680	User is not allowed to configure static route for an inband EPG which is not deployed on the current APIC.	6.0(2h) and later
CSCwe13941	Following are some of the symptoms seen because of this issue : 1. Failure to verify APIC's CIMC credentials. 2. Failure to verify the power status. 3. Failure to verify the serial number of the APIC as seen in CIMC. These symptoms can be seen during the following workflows: 1. APIC Cluster Initial Bootstrap. 2. Adding a new APIC to the cluster - Expansion. 3. Replacing an APIC in the cluster - RMA operation. 4. Recommission of APIC following a decommission.	6.0(2h) and later
CSCwe39842	PXE boot for vmedia installation of the Cisco APIC 6.0(2) release does not work on APIC-SERVER-M2/M3/L2/L3.	6.0(2h) and later

Bug ID	Description	Exists in
CSCwe41446	When APICs are upgraded to the 6.0(2) release and switches are still on older releases, the upgraded standby Cisco APIC cannot join the cluster.	6.0(2h) and later
CSCwe46071	A leaf node gets stuck in bootstrap. Although bootstrap eventually gets forced completed, the node might not download the entire expected configuration, resulting in a node that is not fully functional.	6.0(2h) and later
CSCwe47966	SMU installation fails in the 6.0(2) release due to collecting the techsupport files prior to installing the SMU.	6.0(2h) and later
CSCwe50393	Using the back-to-back spine switch wizard will not display node IDs for the switch selection, and so the task in the wizard cannot be completed.	6.0(2h) and later
CSCwf54771	User configuration is missing on APICs and switches following an ungraceful reload or power outage.	6.0(2h) and later
CSCwf72015	vAPICs hosted on ESXi hosts directly connected to the fabric must see the leaf switch using LLDP. Hosts cannot be connected by an intermediate switch, including UCS Fabric Interconnects. This applies to vAPIC clusters and vAPICs used in ACI mini deployments.	6.0(2h) and later
CSCwf80352	Cisco APIC does not accept special characters "#" and ";" in then fabric name field when upgrading to the 6.0(2) release. For example, if the fabric name is "Test#03, it will be truncated to "Test", which causes prevents switches from joining the fabric after they are reloaded during the upgrade. In this example, the Cisco APIC expects the name "Test#03", but the switch is assigned the name "Test".	6.0(2h)
CSCwh01298	The SSHD daemon does not listen on the IPV6 address.	6.0(2h)

Resolved Issues

Bug ID	Description	Fixed in
CSCwf80352	Cisco APIC does not accept special characters "#" and ";" in then fabric name field when upgrading to the 6.0(2) release. For example, if the fabric name is "Test#03, it will be truncated to "Test", which causes prevents switches from joining the fabric after they are reloaded during the upgrade. In this example, the Cisco APIC expects the name "Test#03", but the switch is assigned the name "Test".	6.0(2j)
CSCwh01298	The SSHD daemon does not listen on the IPV6 address.	6.0(2j)
CSCvz72941	While performing ID recovery, id-import gets timed out. Due to this, ID recovery fails.	6.0(2h)
CSCwc66053	Preconfiguration validations for L3Outs that occur whenever a new configuration is pushed to the Cisco APIC might not get triggered.	6.0(2h)
CSCwe19885	The Nexus Insights application cannot stream the telemetry data to NDI, even though the Cisco ACI site is registered and active.	6.0(2h)

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(2) releases in which the bug exists. A bug might also exist in releases other than the 6.0(2) releases.

Bug ID	Description	Exists in
CSCvj26666	The "show run leaf|spine <nodeId>" command might produce an error for scaled up configurations.	6.0(2h) 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(2h) and later
CSCvm71833	Switch upgrades fail with the following error: Version not compatible.	6.0(2h) 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.	6.0(2h) 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(2h) 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(2h) 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(2h) 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(2h) 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(2h) 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(2h) 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(2h) 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(2h) and later
CSCvy34357	Starting with the 6.0(2) 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(2h) 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.	6.0(2h) and later
CSCvz06118	In the "Visibility and Troubleshooting Wizard," ERSPAN support for IPv6 traffic is not available.	6.0(2h) 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(2h) and later
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(2h) 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(2h) 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(2h) 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.	6.0(2h) 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(2h) 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(2h) 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(2h) 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(2h) 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(2h) 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(2h) 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(2h) and later
N/A	MPLS interface statistics shown in a switch's CLI get cleared after an admin or operational down event.	6.0(2h) 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(2h) 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.

- If you use Microsoft vSwitch and want to downgrade to Cisco APIC Release 2.3(1) from a later release, you first must delete any microsegment EPGs configured with the **Match All** filter.

- This release supports the following additional virtualization products:

Product	Supported Release	Information Location
Microsoft Hyper-V	2016 Update Rollup 1, 2, 2.1, and 3	N/A
VMM Integration and VMware	6.5, 6.7, and 7.0	Cisco ACI Virtualization Guide, Release

Product	Supported Release	Information Location
Distributed Virtual Switch (DVS)		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(2).

- 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.

Product ID	Description
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.

Adaptive Security Appliance (ASA) Compatibility Information

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

- This release supports Adaptive Security Appliance (ASA) device package version 1.2.5.5 or later.
- If you are running a Cisco Adaptive Security Virtual Appliance (ASA) version that is prior to version 9.3(2), you must configure SSL encryption as follows:
   (config)# ssl encryption aes128-sha1

Miscellaneous Compatibility Information

This release supports the following products:

Product	Supported Release
Cisco NX-OS	16.0(2)

Product	Supported Release
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	4.2(3e) CIMC HUU ISO (recommended) 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(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(2k) CIMC HUU ISO (recommended) 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.

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 16.0(2)	The release notes for Cisco NX-OS for Cisco Nexus 9000 Series ACI-Mode Switches.
Verified Scalability Guide for Cisco APIC, Release 6.0(2) and Cisco Nexus 9000 Series ACI-Mode Switches, Release 16.0(2)	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.