



# Cisco Application Policy Infrastructure Controller Release Notes, Release 5.2(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 15.2\(8\)](#).

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

Date	Description
June 18, 2025	In the Miscellaneous Compatibility Information section, added support for 4.3.2.250016 CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3).
September 24, 2024	In the Miscellaneous Compatibility Information section, added: <ul style="list-style-type: none"><li>4.3.2.240077 CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3)</li></ul>
May 1, 2024	In the Miscellaneous Compatibility Information section, added: <ul style="list-style-type: none"><li>4.3.2.240009* CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3)</li></ul>
March 19, 2024	The 4.1(2m) CIMC HUU ISO is now recommended for UCS C220/C240 M4 (APIC-L2/M2).
March 1, 2024	Release 5.2(8i) became available. Added the resolved issues for this release.
December 15, 2023	Release 5.2(8h) became available. Added the resolved issues for this release.
October 30, 2023	Release 5.2(8g) became available. Added the resolved issues for this release.
September 11, 2023	Release 5.2(8f) became available. Added the resolved issues for this release.
August 9, 2023	Release 5.2(8e) became available; there are no changes to this document for this release. See the <a href="#">Cisco Nexus 9000 ACI-Mode Switches Release Notes, Release 15.2(8)</a> for the changes in this release.
June 29, 2023	Release 5.2(8d) became available.

## New Software Features

Product Impact	Feature	Description
Base Functionality	Source IP address in the audit log messages	The audit log messages now include the IP address of the source of the configuration change.
Base Functionality	Enhanced timestamp for UDP transport syslog messages	Cisco APIC supports a new enhanced timestamp mode for syslog to include the year in the timestamp for UDP transport.
Interoperability	Support for VMware vSphere 8.0	VMM domains now support VMware vSphere 8.0. For more information, see the <a href="#">Cisco ACI vCenter Plug-in chapter in the Cisco ACI Virtualization Guide, 5.2(x)</a> and <a href="#">Cisco ACI Virtual Edge Release Notes, Release 3.2(4)</a> .

## New Hardware Features

For the new hardware features, see the [Cisco Nexus 9000 ACI-Mode Switches Release Notes, Release 5.2\(8\)](#).

## 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(8) releases in which the bug exists. A bug might also exist in releases other than the 5.2(8) releases.

Bug ID	Description	Exists in
<a href="#">CSCwk13546</a>	There are stale hvExtPI objects due to the hvsExtPol managed object not being cleaned up when an EPG is deleted.  Fault F1606 is raised, but has no operational impact:  desc :Fault delegate: Operational issues detected on portgroup error: Cannot find an EPG policy in the domain for the port group.	5.2(8i) and later
<a href="#">CSCwj23752</a>	Changing in the name of the remote-destination group stops the sending of syslog messages to the remote destination. Changing the port number or forwarding facility does not affect the sending of the messages. Only when the name is changed does the leaf switch stop sending the syslog messages. Enabling and disabling the policy does not resume the sending of the messages.	5.2(8h) and later
<a href="#">CSCwj43407</a>	Altering the IP SLA policy for an IP SLA track member led to the crashing of switches.	5.2(8h) and later
<a href="#">CSCwj42027</a>	F1527, F1528 faults raised for /var/log/dme/log crossing 75% usage and cleared over and over.	5.2(8g) and later
<a href="#">CSCwj71324</a>	F3083 is not generated for two endpoints in the same EPG having the same IP address.	5.2(8g) and later
<a href="#">CSCwi71834</a>	Interface Configuration Migration created unexpected infra/access node profile and interface profile for a fabric port. The unexpected infra profile causes a fault.	5.2(8g) and later
<a href="#">CSCwi83667</a>	The Interface Configuration Migration created Leaf profile and interface profile Access with the Spine interface	5.2(8g) and later
<a href="#">CSCwi97842</a>	After upgrading, the Cisco APIC cluster is diverged and policymgr is down and repeatedly crashing on one Cisco APIC.	5.2(8g) and later
<a href="#">CSCwj55258</a>	Fault F4144 will not clear from the Cisco APIC even with matching dhcpPool and Fabric Node Vector information.	5.2(8g) and later
<a href="#">CSCwh56468</a>	"No data stats to display" in stats tab for some L3out profile, while for others it works fine. Failed L3Outs doesn't have I2EgrBytesAgHist15min MO created on APIC.	5.2(8f) and later
<a href="#">CSCwh53727</a>	The API call /mqapi2/deployment.query.json?mode=getvmmCapInfo that is done against the Cisco APICs by an external management system takes too long to process.	5.2(8f) and later

Bug ID	Description	Exists in
<a href="#">CSCwi03663</a>	Recent upgraded versions of SCP servers do not support some of the old ciphers or host key algorithms causing SCP to/from APIC to break.	5.2(8f) and later
<a href="#">CSCwh05135</a>	Override vpc interface policy doesnot consistently take precedence over regular vpc interface policy. Upon a leaf reload, its quite random which policy takes precedence, and accordingly the VLANs get programmed. If the override or regular AEP is missing, the relevant domain association/VLANs, then those VLANs are not programmed causing outages.	5.2(8e) and later
<a href="#">CSCwi12992</a>	After upgrading to ACI 5.2(8), the custom SSL certificate is not installed in the Cisco APICs and the default self-signed SSL certificate is used instead.	5.2(8e) through 5.2(8h)
<a href="#">CSCwi40019</a>	The description of an interface is configured but not pushed to a spine switch.	5.2(8e) through 5.2(8h)
<a href="#">CSCwh05135</a>	Override vpc interface policy doesnot consistently take precedence over regular vpc interface policy.Upon a leaf reload, its quite random which policy takes precedence, and accordingly the vlans get programmed.If the override or regular AEP is missing the relevant domain association/vlans, then those vlans are not programmed causing outages.	5.2(8e) and later
<a href="#">CSCwh07037</a>	An outage occurred because traffic coming from the TEPs was dropped by the receiving leaf switches with INFRA_ENCAP_SRC_TEP_MISS.	5.2(8e) and later
<a href="#">CSCwi17652</a>	Service-ep flag get enabled for service device with no redirect policy (no PBR). In ELAM "Don't learn" bit get set when packet sent from service leaf to destination leaf.	5.2(8e) and later
<a href="#">CSCwh96100</a>	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#	5.2(8d) and later
<a href="#">CSCwj03122</a>	Leaf connected to ESXi hosts with VMM integration may crash due to OOM.	5.2(8g) and later
<a href="#">CSCwj05269</a>	Endpoints were in down state after node is restarted.	5.2(8f) and later
<a href="#">CSCwk19612</a>	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.	5.2(8d) and later
<a href="#">CSCwf20254</a>	There is a delay in downloading and programming of policies on the node.	5.2(8d) through

Bug ID	Description	Exists in
		5.2(8h)
<a href="#">CSCwf92312</a>	Whenever the 'server monitoring' feature is enabled on Cisco APIC and there is a complex password that includes more than one special character, all the RADIUS users that have access to the APICs cannot log in. Users receive the following error: 'Failed to populate authentication data snapshot - AAA Servers are unreachable'. Fault F0021 is raised on all Cisco APICs of the cluster, which says that 'the RADIUS provider is not reachable anymore'.	5.2(8d) through 5.2(8h)
<a href="#">CSCwh36670</a>	During an upgrade, at times it is not known if a DME has completed all the necessary steps to run in the new version. To assess reliably that information, it must be known for which DME and for which managed object the postUpgrade and postClusterUpgrade phases has been executed.	5.2(8d) through 5.2(8h)
<a href="#">CSCwf54771</a>	User configuration is missing on APICs and switches following an ungraceful reload or power outage.	5.2(8d) through 5.2(8g)
<a href="#">CSCwh77285</a>	OpFlex OOM crashes in leaf switches.	5.2(8d) through 5.2(8g)
<a href="#">CSCwh47921</a>	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(8d) through 5.2(8f)
<a href="#">CSCwf61646</a>	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(8d) through 5.2(8e)
<a href="#">CSCvg81020</a>	For strict security requirements, customers require custom certificates that have RSA key lengths of 3072 and 4096.	5.2(8d) and later
<a href="#">CSCvm56946</a>	Support for local user (admin) maximum tries and login delay configuration.	5.2(8d) and later
<a href="#">CSCvt99966</a>	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(8d) and later
<a href="#">CSCvy40511</a>	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(8d) and later
<a href="#">CSCvz72941</a>	While performing ID recovery, id-import gets timed out. Due to this, ID recovery fails.	5.2(8d) and later
<a href="#">CSCvz83636</a>	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(8d) and later
<a href="#">CSCwa58709</a>	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(8d) and later

Bug ID	Description	Exists in
<a href="#">CSCwa90058</a>	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(8d) and later
<a href="#">CSCwa90084</a>	<ul style="list-style-type: none"> <li>- Traffic disruption across a vPC pair on a given encapsulation.</li> </ul> OR <ul style="list-style-type: none"> <li>- EPG flood in encap blackholing on a given encapsulation.</li> </ul> OR <ul style="list-style-type: none"> <li>- 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.</li> </ul>	5.2(8d) and later
<a href="#">CSCwd26277</a>	When deploying a service graph, the dialog does not list all bridge domains for the provider connector. This issue is observed when you enter or edit the bridge domain name in the consumer connector field. After this, the provider connector will only list the bridge domain that is selected by the consumer connector field.	5.2(8d) and later
<a href="#">CSCwe39988</a>	The Cisco APIC GUI becomes unresponsive when there is large configuration for given tenant and VRF instance.	5.2(8d) and later
<a href="#">CSCwe52465</a>	The NICC app image fails to load.	5.2(8d) and later
<a href="#">CSCwe58398</a>	<p>This is added functionality for upgrade show command.</p> <ol style="list-style-type: none"> <li>1. aci diag show postupgrade -service &lt;dme&gt; -&gt; This gives details for dmes and which shard still have pending postUpgradeCb.</li> <li>2. aci diag show postupgrade -service &lt;dme&gt; -shard &lt;shard_id&gt; -&gt; This gives the details of log path for the dmes and shard for which postUpgradeCb has been completed.</li> </ol>	5.2(8d) and later
<a href="#">CSCwe66712</a>	For a customer using America/Mexico_City time, the DST time change will still happen on APIC in the year 2023.	5.2(8d) and later
<a href="#">CSCwe92155</a>	After configuring syslog using TCP on port 59500, the logit was sent out normally and netstat showed that it was established. However, after aborting the connection from the syslog server side, the TCP connection went from ESTABLISHED to CLOSE_WAIT and disappeared from the APIC side.	5.2(8d) and later
<a href="#">CSCwe93045</a>	There is general slowness when an application contacts the Cisco APIC cluster through the REST API. The same slowness is experienced when accessing using the Cisco APIC GUI.	5.2(8d) and later
<a href="#">CSCwf04318</a>	In a Cisco APIC 5.2 release, a user in a restricted security domain is allowed to create a VRF instance, but that same restricted mode user is not allowed to delete that VRF instance.	5.2(8d) and later
<a href="#">CSCwf16927</a>	The system time does not reflect the daylight saving adjustments done in Egypt for releases prior to 5.3.1 and 6.0.4	5.2(8d) and later
<a href="#">CSCwf55317</a>	<ol style="list-style-type: none"> <li>1. Go to <b>Tenant &gt; Application Profile &gt; Topology</b>.</li> <li>2. Drag and drop a contract. Problem 1: No pop up displays.</li> </ol> <p>Drag and drop an EPG icon, then cancel the create view. Problem 2: The pop up remains open.</p>	5.2(8d) and later

Bug ID	Description	Exists in
<a href="#">CSCwf59938</a>	Fault code F1414 is triggered and cleared manually. After certain time, the fault is triggered again. This issue occurs when using the syslog server FQDN.	5.2(8d) and later
<a href="#">CSCwf92856</a>	During upgrade "deserialization error" is seen on APIC 1 PD.	5.2(8d) and later
<a href="#">CSCwh17898</a>	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(8d) and later
<a href="#">CSCwh18649</a>	Inter-pod/Inter-site BGP peer is incorrectly marked as "manual,wan" under the BGP for the peer managed object of a spine switch.	5.2(8d) and later
<a href="#">CSCwh28834</a>	The "show running config" command does not work in the APIC CLI and generates the following errors:  Error while processing mode: interface  Error while processing mode: leaf  Error while processing mode: configure  Error: ERROR occurred: <class 'xml.etree.ElementTree.ParseError'>, not well-formed (invalid token): line 1, column 51242, File "/mgmt/opt/controller/yaci/yaci/_cfg.py", line 18, in _execute_func  subCmd.runningConfig(ctx, **kwargs)	5.2(8d) and later
<a href="#">CSCwh41632</a>	Enhancement - show apic upgrade complete only after postUpgradeCb is done	5.2(8d) and later
<a href="#">CSCwh41865</a>	When upgrading an APIC, the "from" version is displayed as "to" version in the event record.	5.2(8d) and later
<a href="#">CSCwh44987</a>	When a non-default OOB management EPG is configured and a default one is removed from the configuration, the default EPG will be recreated automatically after a fabric upgrade. This is causes fault F0523 "Configuration failed for EPG default due to Not Associated With Management Zone".	5.2(8d) and later
<a href="#">CSCwh47794</a>	The ACI VMM Tags tab returns "the server returned unintelligible response" message even though the tag is retrievable using the CLI.	5.2(8d) and later
<a href="#">CSCwh53706</a>	In scale setups, when there are more than the usual number of objects and if the user tries to load the Capacity Dashboard page, the page times out. A few queries that are hit from the browser and the page become stuck for few seconds.	5.2(8d) and later
<a href="#">CSCwh56716</a>	When the Cisco APICs use Direct Connect to CSSM, running the "show license usage" command on APIC 1, 2, or 3 shows ACI_LEAF_ESS_10G 6 in use. When APICs 2 and 3 are restarted, this output is unchanged. When APIC 1 is restarted, the output becomes "No Licenses in use" on APICs 1, 2, and 3. The "Registering for Smart Licensing with Direct Connect to CSSM Using the GUI" process has to be done again. This was tested in the lab with Cisco APIC releases 5.2(6g), 5.2(7g), and 6.0(2j)	5.2(8d) and later
<a href="#">CSCwh67428</a>	The GUI does not display maxSpeed and direction information in the equipment view.	5.2(8d) and later
<a href="#">CSCwh74484</a>	ACI pushes the VLANs from the old VLAN pool after changing the vNIC template in the UCSM	5.2(8d) and later
<a href="#">CSCwh75348</a>	Decommission an APIC causes the message "the node configuration will be wiped out from controller" to display even though the controllers still retain the user	5.2(8d) and later

Bug ID	Description	Exists in
	configuration.	later
<a href="#">CSCwh77285</a>	OpFlex OOM crashes in leaf switches.	5.2(8d) and later
<a href="#">CSCwh78409</a>	The SNMPD service failed on all Cisco APICs after configuring SNMPv3.	5.2(8d) and later
<a href="#">CSCwh81272</a>	The system resets due to a policyelem high availability policy reset.	5.2(8d) and later
<a href="#">CSCwh83273</a>	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(8d) and later
<a href="#">CSCwh84052</a>	When using the OpenStack integration, the Cisco APIC VMM Manager process may consume more memory than is available and then end.	5.2(8d) and later
<a href="#">CSCwh87245</a>	An edmManagedNic or compManagedNic object may be mapped to the wrong server (compHv).	5.2(8d) and later
<a href="#">CSCwh87458</a>	Search Filters in Endpoint - Operational - Client Endpoints do not show up in the endpoint learning filter.	5.2(8d) and later
<a href="#">CSCwh95573</a>	Fault " F4142" is raised when there is inconsistency in FNV and the idmgr database. Even though the addrAssigner in FNV is set to 0 and the corresponding "identContextElement" managed object is missing from the idmgr database, the fault gets raised.	5.2(8d) and later
<a href="#">CSCwh98712</a>	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(8d) and later
<a href="#">CSCwi01316</a>	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(8d) and later
<a href="#">CSCwi06427</a>	Navigating to FABRIC -> Inventory -> Pod1 -> Operational -> Routes -> IPv6 learned routes results in the following error message:Value is not specified for the argument 'undefined'	5.2(8d) and later
<a href="#">CSCwi09894</a>	In a mini ACI fabric, the physical APIC does not join the cluster after power cycling the entire setup.	5.2(8d) and later
<a href="#">CSCwi34095</a>	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(8d) and later
<a href="#">CSCwi40671</a>	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(8d) and later



Bug ID	Description	Exists in
<a href="#">CSCWi52324</a>	The fault F3227 "ACI failed processing an already accepted configuration change" continuously gets raised	5.2(8d) and later
<a href="#">CSCWi66348</a>	A Cisco ACI switch can spend hours to complete the bootstrap process. At the worst, the expected completion time should be about 90 minutes.	5.2(8d) and later
<a href="#">CSCWi78474</a>	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(8d) and later
<a href="#">CSCWi99378</a>	There are packet drops between the pods.	5.2(8d) and later
<a href="#">CSCWj08117</a>	After a reboot is triggered, any of the Cisco APICs take around 1 hour to reach the cluster fully fit status and the affected DME is ifc_observer. During the issue, there is non-optimal leader for some shards for the service ifc_observer, which it clears after 30 minutes.	5.2(8d) and later
<a href="#">CSCWj13396</a>	<p>ACI switches show in maintenance with the CLI command "acdiag fnvread" on Cisco APIC, but they show "normal" in vsh and even top. System also shows In service.</p> <ul style="list-style-type: none"> <li>- Switches do not show up in the GUI nor API for configurations, as APIC vectors it as in maintenance. This severely impacts the ability to make changes.</li> <li>- Switches may continue to work normally even though no new configurations can be made on them.</li> </ul>	5.2(8d) and later
<a href="#">CSCWj17966</a>	The Cisco APIC bootmgr or appliance director allows an incorrect attribute/value update to be received in LLDP TLV due to miscabling.	5.2(8d) and later
<a href="#">CSCWj38953</a>	log_bin_decode crashes on distinguished name decoding failures.	5.2(8d) and later
<a href="#">CSCWj42913</a>	REST API can be used to configure static ports for nodes that are restricted in by a node rule.	5.2(8d) and later
<a href="#">CSCWj57993</a>	The F0413 PSU fault is not reported by SMART callhome. The tcpdump command on the leaf switch does not show SMTP messages being sent for this fault for which the PSU was removed.	5.2(8d) and later
<a href="#">CSCWj69046</a>	SAML authentication fails when using the HTTPS Proxy 5.2 image.	5.2(8d) and later
<a href="#">CSCWh01347</a>	If customer configures some ACI policies from cli, these objects are created as __ui_<name>. However, these objects are hidden by default in the GUI.	5.2(8d)
<a href="#">CSCWf17013</a>	<p>Trigger inventory sync- Failed.</p> <p>re-associated (removed/re-add) portgroup bindings to VMs interface on the vcenter side, did not helped.</p> <p>checking hvs.ExtPol MO, shows operIssues &gt; invalid-extpol</p>	5.2(8d) and later
<a href="#">CSCWc50398</a>	Licensemgr process crashes on node-1, with Smart license mode being "Direct connection to CSSM" under smart license settings.	5.2(8d) and later

## Resolved Issues

Bug ID	Description	Fixed in
<a href="#">CSCwf20254</a>	There is a delay in downloading and programming of policies on the node.	5.2(8i)
<a href="#">CSCwf92312</a>	Whenever the 'server monitoring' feature is enabled on Cisco APIC and there is a complex password that includes more than one special character, all the RADIUS users that have access to the APICs cannot log in. Users receive the following error: 'Failed to populate authentication data snapshot - AAA Servers are unreachable'. Fault F0021 is raised on all Cisco APICs of the cluster, which says that 'the RADIUS provider is not reachable anymore'.	5.2(8i)
<a href="#">CSCwh36670</a>	During an upgrade, at times it is not known if a DME has completed all the necessary steps to run in the new version. To assess reliably that information, it must be known for which DME and for which managed object the postUpgrade and postClusterUpgrade phases has been executed.	5.2(8i)
<a href="#">CSCwi12992</a>	After upgrading to ACI 5.2(8), the custom SSL certificate is not installed in the Cisco APICs and the default self-signed SSL certificate is used instead.	5.2(8i)
<a href="#">CSCwi40019</a>	The description of an interface is configured but not pushed to a spine switch.	5.2(8i)
<a href="#">CSCwf54771</a>	User configuration is missing on APICs and switches following an ungraceful reload or power outage.	5.2(8h)
<a href="#">CSCwh77285</a>	OpFlex OOM crashes in leaf switches.	5.2(8h)
<a href="#">CSCwh47921</a>	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(8g)
<a href="#">CSCwf61646</a>	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(8f)
<a href="#">CSCwh01347</a>	If customer configures some ACI policies from cli, these objects are created as __ui_<name>. However, these objects are hidden by default in the GUI.	5.2(8f)
<a href="#">CSCwc11570</a>	In certain configuration sequences, bridge domain routes (and consequently, host routes) are not advertised out of GOLF and ACI Anywhere L3Outs.	5.2(8d)
<a href="#">CSCwc66053</a>	Preconfiguration validations for L3Outs that occur whenever a new configuration is pushed to the Cisco APIC might not get triggered.	5.2(8d)
<a href="#">CSCwd44827</a>	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:polcymgr:FabricCtrlrConfigPUpdatePodConnPDef)	5.2(8d)
<a href="#">CSCwd88076</a>	This issue is seen when Syslog is configured with CA signed certificates.The TLS connection was terminated due to certificate validation failure. This is not correct behavior and TLS connection should be established for CA signed certificates too.	5.2(8d)
<a href="#">CSCwd90130</a>	After performing an interface migration from the old selector-based style to the new per-port configuration, an interface with an active override might not work as before the migration.	5.2(8d)

Bug ID	Description	Fixed in
<a href="#">CSCwe09859</a>	The OpFlex agent on a hypervisor randomly disconnects, impacting VM traffic.	5.2(8d)
<a href="#">CSCwe19885</a>	The Nexus Insights application cannot stream the telemetry data to NDI, even though the Cisco ACI site is registered and active.	5.2(8d)
<a href="#">CSCwe25534</a>	When an IPv6 address is added as the BGP peer address, the APIC does not validate the IPv6 address if the address contains any letters.	5.2(8d)
<a href="#">CSCwe64159</a>	Podman is unstable, and gets restarted every 5 seconds, even after running the podman_cleanup.py script. The scheduler services show all the services are running on all the Cisco APICs.	5.2(8d)
<a href="#">CSCwe96230</a>	The Appliance Element (AE) service gets restarted several times by the cgroup process (oom-killer).	5.2(8d)
<a href="#">CSCwf11826</a>	Endpoints are moved from a Tag-based ESG to the base EPG. Tag-to-VM associations are lost and not refreshed for Tags used in ESG selectors.	5.2(8d)
<a href="#">CSCwf19660</a>	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(8d)
<a href="#">CSCwf29094</a>	The error "Error:Server did not return JSON response" occurs in Nexus Cloud Connectivity in any of the Cisco APICs.	5.2(8d)

## 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(8) releases in which the bug exists. A bug might also exist in releases other than the 5.2(8) releases.

Bug ID	Description	Exists in
<a href="#">CSCuu11416</a>	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(8d) and later
<a href="#">CSCvj26666</a>	The "show run leaf spine <nodeld>" command might produce an error for scaled up configurations.	5.2(8d) and later
<a href="#">CSCvj90385</a>	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(8d) and later
<a href="#">CSCvq39764</a>	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(8d) and later
<a href="#">CSCvq58953</a>	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(8d) and later

Bug ID	Description	Exists in
<a href="#">CSCvr89603</a>	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(8d) and later
<a href="#">CSCvs19322</a>	Upgrading Cisco APIC from a 3.x release to a 4.x or later release causes Smart Licensing to lose its registration. Registering Smart Licensing again will clear the fault.	5.2(8d) and later
<a href="#">CSCvs77929</a>	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(8d) and later
<a href="#">CSCvx75380</a>	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(8d) and later
<a href="#">CSCvx78018</a>	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(8d) and later
<a href="#">CSCvy07935</a>	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(8d) and later
<a href="#">CSCvy10946</a>	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(8d) and later
<a href="#">CSCvy34357</a>	Starting with the 5.2(8) release, the following apps built with the following non-compliant Docker versions cannot be installed nor run: <ul style="list-style-type: none"> <li>ConnectivityCompliance 1.2</li> <li>SevOneAciMonitor 1.0</li> </ul>	5.2(8d) and later
<a href="#">CSCvy45358</a>	The file size mentioned in the status managed object for techsupport "dbgexpTechSupStatus" is wrong if the file size is larger than 4GB.	5.2(8d) and later
<a href="#">CSCvz06118</a>	In the "Visibility and Troubleshooting Wizard," ERSPAN support for IPv6 traffic is not available.	5.2(8d) and later
<a href="#">CSCvz84444</a>	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(8d) and later
<a href="#">CSCvz85579</a>	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.)	5.2(8d) and later

Bug ID	Description	Exists in
<a href="#">CSCwa78573</a>	<p>When the "BGP" branch is expanded in the Fabric &gt; Inventory &gt; POD 1 &gt; Leaf &gt; Protocols &gt; 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(8d) and later
<a href="#">CSCwd45200</a>	Hosting server details for AVE endpoints at the operational tab under the EPG is not updated after VM migration.	5.2(8d) and later
<a href="#">CSCwd51537</a>	After changing a VM's name, the name does not get updated for endpoints in the Operational tab of an EPG.	5.2(8d) 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(8d) 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(8d) 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(8d) 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(8d) and later
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(8d) 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(8d) and later

Bug ID	Description	Exists in
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(8d) 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(8d) and later
N/A	MPLS interface statistics shown in a switch's CLI get cleared after an admin or operational down event.	5.2(8d) 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(8d) 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"> <li>SCVMM 2019 RTM (Build 10.19.1013.0) or newer</li> <li>SCVMM 2016 RTM (Build 4.0.1662.0) or newer</li> <li>SCVMM 2012 R2 with Update Rollup 9 (Build 3.2.8145.0) or newer</li> </ul>	N/A
VMM Integration and VMware Distributed Virtual Switch (DVS)	6.5, 6.7, 7.0, and 8.0	<a href="#">Cisco ACI Virtualization Guide, Release 5.2(x)</a>

## Hardware Compatibility Information

This release supports the following Cisco APIC servers:

Product ID	Description
APIC-L2	Cisco APIC with large CPU, hard drive, and memory configurations (more than 1000 edge ports)
APIC-L3	Cisco APIC with large CPU, hard drive, and memory configurations (more than 1200 edge

Product ID	Description
	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\(8\)](#).
- 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 Cisco APIC	The Cisco UCS M4-based Cisco APIC and previous versions support only the 10G interface. Connecting the Cisco APIC to the Cisco ACI fabric requires a same speed interface on the Cisco ACI leaf switch. You cannot connect the Cisco APIC directly to the Cisco N9332PQ ACI leaf switch, unless you use a 40G to 10G converter (part number CVR-QSFP-SFP10G), in which case the port on the Cisco N9332PQ switch auto-negotiates to 10G without requiring any manual configuration.
Cisco UCS M5-based Cisco APIC	The Cisco UCS M5-based Cisco APIC supports dual speed 10G and 25G interfaces. Connecting the Cisco APIC to the Cisco ACI fabric requires a same speed interface on the Cisco ACI leaf switch. You cannot connect the Cisco APIC directly to the Cisco N9332PQ ACI leaf switch, unless you use a 40G to 10G converter (part number CVR-QSFP-SFP10G), in which case the port on the Cisco N9332PQ switch auto-negotiates to 10G without requiring any manual configuration.
N2348UPQ	To connect the N2348UPQ to Cisco ACI leaf switches, the following options are available:  Directly connect the 40G FEX ports on the N2348UPQ to the 40G switch ports on the Cisco ACI leaf switches  Break out the 40G FEX ports on the N2348UPQ to 4x10G ports and connect to the 10G ports on all other Cisco ACI leaf switches.  <b>Note:</b> 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.



Product ID	Description
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	15.2(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	<ul style="list-style-type: none"> <li>• 4.3.2.240077 CIMC HUU ISO (recommended) for UCS C220/C240 M5 (APIC-L3/M3)</li> <li>• 4.3.2.250016 CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3)</li> <li>• 4.3.2.240009 CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3)</li> <li>• 4.3.2.230207 CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3)</li> <li>• 4.2(3e) CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3)</li> <li>• 4.2(3b) CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3)</li> <li>• 4.2(2a) CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3)</li> <li>• 4.1(3m) CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3)</li> <li>• 4.1(3f) CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3)</li> <li>• 4.1(3d) CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3)</li> <li>• 4.1(3c) CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3)</li> <li>• 4.1(2m) CIMC HUU ISO (recommended) for UCS C220/C240 M4 (APIC-L2/M2)</li> <li>• 4.1(2k) CIMC HUU ISO for UCS C220/C240 M4 (APIC-L2/M2)</li> <li>• 4.1(2g) CIMC HUU ISO for UCS C220/C240 M4 (APIC-L2/M2)</li> <li>• 4.1(2b) CIMC HUU ISO for UCS C220/C240 M4 (APIC-L2/M2)</li> <li>• 4.1(1g) CIMC HUU ISO for UCS C220/C240 M4 (APIC-L2/M2) and M5 (APIC-L3/M3)</li> <li>• 4.1(1f) CIMC HUU ISO for UCS C220 M4 (APIC-L2/M2) (deferred release)</li> <li>• 4.1(1d) CIMC HUU ISO for UCS C220 M5 (APIC-L3/M3)</li> <li>• 4.1(1c) CIMC HUU ISO for UCS C220 M4 (APIC-L2/M2)</li> <li>• 4.0(4e) CIMC HUU ISO for UCS C220 M5 (APIC-L3/M3)</li> <li>• 4.0(2g) CIMC HUU ISO for UCS C220/C240 M4 and M5 (APIC-L2/M2 and APIC-L3/M3)</li> </ul>



Product	Supported Release
	<ul style="list-style-type: none"> <li>• 4.0(1a) CIMC HUU ISO for UCS C220 M5 (APIC-L3/M3)</li> <li>• 3.0(4d) CIMC HUU ISO for UCS C220/C240 M3 and M4 (APIC-L2/M2)</li> <li>• 3.0(3f) CIMC HUU ISO for UCS C220/C240 M4 (APIC-L2/M2)</li> <li>• 2.0(13i) CIMC HUU ISO</li> <li>• 2.0(9c) CIMC HUU ISO</li> <li>• 2.0(3i) CIMC HUU ISO</li> </ul>
Network Insights Base, Network Insights Advisor, and Network Insights for Resources	<p>For the release information, documentation, and download links, see the <a href="#">Cisco Network Insights for Data Center</a> page.</p> <p>For the supported releases, see the <a href="#">Cisco Data Center Networking Applications Compatibility Matrix</a>.</p>

- 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.
- 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
<a href="#">Cisco Nexus 9000 ACI-Mode Switches Release Notes, Release 15.2(8)</a>	The release notes for Cisco NX-OS for Cisco Nexus 9000 Series ACI-Mode Switches.
Verified Scalability Guide for Cisco APIC, Release 5.2(8) and Cisco Nexus 9000 Series ACI-Mode Switches, Release 15.2(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.

## Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, send your comments to [apic-docfeedback@cisco.com](mailto:apic-docfeedback@cisco.com). We appreciate your feedback.

## Legal Information

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2025 Cisco Systems, Inc. All rights reserved.