Cisco Application Policy Infrastructure Controller Release Notes, Release 5.0(1)

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 supported hardware, no longer supported hardware (if any), features, issues, and limitations for the Cisco Nexus 9000 series switches in ACI mode, see the *Cisco Nexus 9000 ACI-Mode Switches Release Notes, Release 15.0(1)*.

Note: This release ends the support of the oldest generation of Cisco Nexus hardware. For the list of no longer supported hardware, see the *Cisco Nexus 9000 ACI-Mode Switches Release Notes, Release 15.0(1)*.

Note: The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

For more information about this product, see Related Content.

Date	Description
April 29, 2024	In the Miscellaneous Compatibility Information section, added: ■ 4.2(3j) CIMC HUU ISO (recommended) for UCS C220/C240 M5 (APIC-L3/M3) ■ 4.1(3m) CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3)
August 1, 2022	In the Miscellaneous Compatibility Information section, added: ■ 4.2(2a) CIMC HUU ISO (recommended) for UCS C220/C240 M5 (APIC-L3/M3) ■ 4.1(2k) CIMC HUU ISO (recommended) for UCS C220/C240 M4 (APIC-L2/M2)
June 30, 2022	In the section Miscellaneous Compatibility, added information about Cisco Nexus Dashboard Insights creating the cisco_SN_NI user.
March 21, 2022	In the Miscellaneous Compatibility Information section, added: ■ 4.1(3f) CIMC HUU ISO (recommended) for UCS C220/C240 M5 (APIC-L3/M3)
February 23, 2022	In the Miscellaneous Compatibility Information section, added: ■ 4.1(2g) CIMC HUU ISO (recommended) for UCS C220/C240 M4 (APIC-L2/M2)
November 15, 2021	In the Open Issues section, added bug CSCvy17504.

Date	Description
November 2, 2021	In the Miscellaneous Compatibility Information section, added: ■ 4.1(3d) CIMC HUU ISO (recommended) for UCS C220/C240 M5 (APIC-L3/M3)
July 26, 2021	In the Miscellaneous Compatibility Information section, the CIMC 4.1(3c) release is now recommended for UCS C220/C240 M5 (APIC-L3/M3).
March 11, 2021	In the Miscellaneous Compatibility Information section, for CIMC HUU ISO, added: ■ 4.1(3b) CIMC HUU ISO (recommended) for UCS C220/C240 M5 (APIC-L3/M3) Changed: ■ 4.1(2b) CIMC HUU ISO (recommended) for UCS C220/C240 M4 (APIC-L2/M2) and M5 (APIC-L3/M3) To: ■ 4.1(2b) CIMC HUU ISO (recommended) for UCS C220/C240 M4 (APIC-L2/M2
March 9, 2021	In the Hardware Compatibility Information section, added: In this release, the Cisco APIC M3/L3 server does not support the UCSC-PCIE-IQ10GC Intel X710 Quad Port 10GBase-T network interface card.
February 3, 2021	In the Miscellaneous Compatibility Information section, for CIMC HUU ISO, added: 4.1(2b) CIMC HUU ISO (recommended) for UCS C220/C240 M4 (APIC-L2/M2) and M5 (APIC-L3/M3)
September 29, 2020	In the Miscellaneous Compatibility Information section, specified that the 4.1(1f) CIMC release is deferred. The recommended release is now 4.1(1g).
September 16, 2020	In the Known Issues section, added the issue that begins with: Beginning in Cisco APIC release 4.1(1), the IP SLA monitor policy validates the IP SLA port value.
June 25, 2020	Release 5.0(1l) became available; there are no changes to this document for this release. See the *Cisco Nexus 9000 ACI-Mode Switches Release Notes, Release 15.0(1)* for the changes in this release.
May 14, 2020	Release 5.0(1k) became available.

Contents

New Software Features

Feature	Description	Guidelines and Restrictions
Active/Active Layer1/Layer2 symmetric policy-based redirect design	The Layer1/Layer 2 devices in the service chain can now operate in an active/active symmetric policy-based redirect (PBR) design. Symmetric PBR is used to load balance traffic to individual devices based on the hash. For more information, see *Cisco APIC Layer 4 to Layer 7 Services Deployment Guide, Release 5.0(x)*.	None.
Additional modes and auto-negotiation for FEC	Forwarding Error Correction (FEC) encodes data in a redundant way to obtain reliable data transmission over a noisy channel. This release adds more FEC modes, including auto-negotiation of FEC. For more information, see *Cisco ACI and Forward Error Correction*.	None.
Avoiding suboptimal traffic from Cisco ACI internal endpoints to a floating L3Out	Prior to Cisco APIC release 5.0(1), even if an external router is connected under a non-anchor leaf node, traffic from a Cisco ACI internal endpoint to a floating L3Out goes to an anchor leaf node and then goes to the external router through the non-anchor leaf node, which is not an optimal traffic path. Beginning in Cisco APIC release 5.0(1), you can avoid this suboptimal traffic path by using next-hop propagation. For more information, see *Using Floating L3Out to Simplify Outside Network Connections*.	None.
BFD multihop support	BFD multihop provides subsecond forwarding failure detection for a destination with more than one hop and up to 255 hops. Cisco APIC now supports BFD multihop for IPv4 and IPv6 in compliance with RFC5883. For more information, see *Cisco APIC Layer 3 Networking Configuration Guide, Release 5.0(x)*.	None.

Feature	Description	Guidelines and Restrictions
C-bit support for BFD	Cisco ACI now supports C-bit-aware bidirectional forwarding detection (BFD). The C-bit on incoming BFD packets determines whether BFD is dependent or independent of the control plane. For more information, see *Cisco APIC Layer 3 Networking Configuration Guide, Release 5.0(x)*.	None.
DUO two-factor authentication on Cisco APIC	Cisco APIC supports multi-factor authentication with DUO security. Cisco APIC offers second factor (2F) authentication on top of an organization's existing authentication, which could be on-premises or cloud-based. For more information, see *Cisco APIC Security Configuration Guide, Release 5.0(x)*.	None.
Endpoint security groups	An endpoint security groups (ESG) is a logical entity that contains a collection of physical or virtual network endpoints. The endpoints can classified based on attributes, such as an IPv4 or IPv6 address spanning across bridge domains in the VRF table. An ESG is a security construct that has certain match criteria for creating segmentation, and uses contracts or policies to define the security stance. An ESG separates forwarding from security. For more information, see *Cisco APIC Security Configuration Guide, Release 5.0(x)*.	■ Contracts between EPGs and ESGs or uSeg EPGs are not supported. ■ Cisco ACI Multi-Site is not supported. ■ The ESG selector is based on matching IP addresses and does not allow matching MAC addresses, VM tags, or other criteria. ■ An ESG can be applied only for routed traffic with IP as the selector. ■ To prevent Layer 2 traffic (that is, non-routed traffic) from bypassing ESG security, enable an intra EPG contract with the permit-all rule, such as the common default contractor. In addition, enable intra EPG isolation with proxy ARP enabled on all of the EPGs that provide VLAN-to-interface binding for the ESG endpoints. If the EPG is used only for VMM DVS integration, you can alternately

Feature	Description	Guidelines and Restrictions
		enable the "Allow Micro-Segmentation" option. Either feature forces all communication between ESG endpoints of an EPG to go through Layer 3 routing. ■ EPGs are still used to bind VLANs and interfaces. ■ Taboo contracts are not supported. ■ Inter-VRFs service graphs between ESGs are not supported. ■ OpenStack is not supported.
Link flap policies	You can create a link flap policy in interface policies, which sets the state of a port to "error-disable" after the port flaps for specified number of times during a specified interval of time. For more information, see the *Cisco APIC Basic Configuration Guide, Release 5.0(x)*.	This feature is not honored on fabric extender (FEX) host interface (HIF) ports nor on leaf switch models without -EX, -FX, -FX2, -GX, or later designations in the product ID.
Multicast filtering	Beginning with Cisco APIC release 5.0(1), you can use the multicast filtering feature to filter multicast traffic from two directions: source filtering at the first-hop route and receiver filtering at the last-hop route. For more information, see *Cisco APIC Layer 3 Networking Configuration Guide, Release 5.0(x)*.	■ Multicast filtering is supported only for IPv4. ■ If you attach an empty route map to a bridge domain, route maps assume a deny-all by default, so all sources and groups will be blocked on that bridge domain. ■ The multicast filtering feature is applied at the bridge domain level. ACI supports configuration of multiple EPGs in a single bridge domain. When this configuration is used with the bridge domain filtering features, the filter will be applied across all EPGs in the bridge

Feature	Description	Guidelines and Restrictions
		domain as it is a bridge domain level setting. Additional guidelines and restrictions are provided in the *Cisco APIC Layer 3 Networking Configuration Guide, Release 5.0(x)*.
Per-leaf switch RBAC	A fabric administrator can now assign a physical node, such as a leaf switch, to a security domain. Only a user with node management privileges within the security domain can configure nodes assigned to that domain. The user has no access to nodes outside of the security domain, and users in other security domains have no access to the node assigned to the security domain. For more information, see *Cisco APIC Security Configuration Guide, Release 5.0(x)*.	None.
Physical domains	Physical domains enable you to use the floating L3Out feature with virtual routers without VMM domain integration or to use a physical router without L3Out logical interface path configurations. For more information, see *Using Floating L3Out to Simplify Outside Network Connections*.	None.
Policy-based redirect with an L3Out service EPG	The unidirectional policy-based redirect is now supported with the other connector in an L3Out, regardless if the L3Out is the provider or consumer connector and regardless if the L3Out is last node or not. For more information, see *Cisco APIC Layer 4 to Layer 7 Services Deployment Guide, Release 5.0(x)*.	None.
Port bring-up delay	When you configure a link level policy, you can set the Port bring-up delay (milliseconds) parameter, which specifies a time in milliseconds that the decision feedback equalizer (DFE) tuning is delayed when a port is coming up. The delay begins when an incoming signal is detected, and can help avoid CRC errors in a specific circumstance. You should set the delay only as required; in most cases, you do not need to set a delay. For more information, see the *Cisco APIC Basic Configuration Guide, Release 5.0(x)*.	This feature is not honored on fabric extender (FEX) ports.
Restricting infra VLAN traffic	For stronger isolation between hypervisors in the fabric, you can now restrict infra VLAN traffic to only network paths specified by a set of infra security entry policies.	None.

Feature	Description	Guidelines and Restrictions
	For more information, see *Cisco APIC Security Configuration Guide, Release 5.0(x)*.	
Rewrite source MAC address when creating a Layer 4 to Layer 7 policy-based redirect	When the rewrite source MAC address feature is enabled and traffic is redirected through a policy-based redirect policy, the traffic will carry the redirected destination service bridge domain SVI MAC address instead of its original source MAC address. For more information, see *Cisco APIC Layer 4 to Layer 7 Services Deployment Guide, Release 5.0(x)*.	None.
Secondary IP address and floating secondary IP address	You can use a secondary IP address as a common IP address for anchor leaf nodes. A floating secondary IP address enables additional floating IP address subnets on the same floating switch virtual interface (SVI). For more information, see *Using Floating L3Out to Simplify Outside Network Connections*.	None.
SNMP and syslog configuration in the First Time Setup wizard	The First Time Setup wizard assists the user in configuring a Cisco APIC for the first time. This release adds initial configuration of Syslog monitoring destinations and of SNMP external management and trap destinations. For more information, see the *Cisco APIC Basic Configuration Guide, Release 5.0(x)*.	None.
Segment routing multiprotocol label switching handoff	Prior to Cisco APIC release 5.0(1), when setting up a Cisco ACI fabric connected to a data center provider edge (DC-PE) for a configuration with a multi-tenant network, you need multiple VRFs and a routing protocol for each VRF. You also need to dedicate an interface for each VRF, where the interface is either a physical interface or a logical interface. This configuration uses IP handoff and is typically called VRF-Lite. Beginning with Cisco APIC release 5.0(1), you can now set up a Cisco ACI fabric connection with a DC-PE using segment routing (SR) Multiprotocol Label Switching (MPLS) handoff. For more information, see *Cisco APIC Layer 3 Networking Configuration Guide, Release 5.0(x)*.	■ Even though a border leaf switch can be in multiple SR-MPLS infra L3Outs, a border leaf switch/provider edge router combination can only be in one SR-MPLS infra L3Out as there can be only one routing policy for a user VRF/border leaf switch/DC-PE combination. ■ If there is a requirement to have SR-MPLS connectivity from multiple pods and remote locations, ensure that you have a different SR-MPLS infra L3Out in each of those pods and remote leaf locations with SR-MPLS connectivity.

Feature	Description	Guidelines and Restrictions
		■ Within each SR-MPLS VRF L3Out, defining the outbound route map (export routing policy) is mandatory, but defining the inbound route map (import routing policy) is optional. ■ Routing policies associated with any SR-MPLS VRF L3Outs have to be a global type. In other words, you have to explicitly add all the routes, including bridge domain subnets. ■ Host-based routing is not supported with SR-MPLS. ■ Transit routing is supported for most configurations, but transit SR-MPLS traffic within the same VRF and on the same border leaf pair is not supported. Additional guidelines and restrictions are provided in the Cisco APIC Layer 3 Networking Configuration Guide, Release 5.0(x).
Upgrade enhancements	Various enhancements have been made to the upgrade process, including: ■ The restriction on the number of pods that you can upgrade in parallel has been relaxed so that you can upgrade multiple pods at the same time for pod nodes in Multi-Pod configurations. Switches in a Multi-Pod configuration that are part of the same maintenance group can now be upgraded in parallel. ■ Upgrades or downgrades might be blocked if certain issues are present. ■ Additional information is provided in the GUI for each stage of the APIC upgrade or downgrade	None.

Feature	Description	Guidelines and Restrictions
	process. ■ The default concurrency in a group has changed from 20 to unlimited (the default number of leaf or spine switches that can be upgraded at one time is unlimited). ■ When upgrading nodes in an upgrade group using the GUI, Download Progress field is available in the Work pane, which provides a status on the progress of the download of the firmware for the node upgrade. For more information, see *Cisco APIC Installation, Upgrade, and Downgrade Guide*.	

Changes in Behavior

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

No Longer Supported Software

- Beginning with Cisco APIC release 5.0(1), Cisco Application Virtual Switch (AVS) is no longer supported. If you use Cisco AVS and upgrade to Cisco APIC release 5.0(1), in case of issues, the fabric will not be supported. Also, a fault will be raised for the Cisco AVS domain. If you use Cisco AVS, we recommend that you migrate to Cisco ACI Virtual Edge. See the *Cisco ACI Virtual Edge Installation Guide, Release 3.0(x)*.

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 5.0(1) releases in which the bug exists. A bug might also exist in releases other than the 5.0(1) releases.

Bug ID	Description	Exists in
CSCvq81020	For strict security requirements, customers require custom certificates that have RSA key lengths of 3072 and 4096.	5.0(1k) and later
CSCvm56946	Support for local user (admin) maximum tries and login delay configuration.	5.0(1k) and later
CSCvq54761	The application EPG or the corresponding bridge domain's public subnet may be advertised out of an L3Out in another VRF instance without a contract with the L3Out under certain conditions.	5.0(1k) and later
CSCvs47602	A bridge domain route is not leaked on the service ToR switch after re-triggering the service graph.	5.0(1k) and later

Bug ID	Description	Exists in
CSCvs97029	All the external prefixes from VRF-A could be leaked to VRF-C even when an inter-VRF ESG leak route is configured for a specific prefix.	5.0(1k) and later
CSCvt18145	The routemap becomes missing in the shared service routemap.	5.0(1k) and later
CSCvt92062	The Cisco APIC CLI does not have commands for the following functionality: 1. ESG show commands 2. ESG inter-VRF route leak configuration	5.0(1k) and later
CSCvt98140	A custom QoS policy is not supported on the logical interface profile of non-anchor leaf nodes that are part of a floating L3Out.	5.0(1k) and later
CSCvt99928	An egress/ingress data plane policer policy is not supported on the logical interface profile of non-anchor nodes that are part of a floating L3Out.	5.0(1k) and later
CSCvt99966	A SPAN session with the source type set to "Routed-Outside" goes down. The SPAN configuration is pushed to the anchor or non-anchor nodes, but the interfaces are not pushed due to the following fault: "Failed to configure SPAN with source SpanFL3out due to Source fvIfConn not available".	5.0(1k) and later
CSCvu18502	The Layer 3 health group destination has both the old and new entry after a service bridge domain is moved from one VRF table to another VRF table.	5.0(1k) and later
CSCvu69651	VMM floating L3Out basic functionality does not work. The L3Out port group on a VMware vCenter does not match the configuration in the Cisco APIC. For example, there can be a VLAN mismatch. Cisco APIC visore will show missing compEpPConn, and the port-group's hvsExtPol managed object will not form hvsRsEpPD to the L3Out compEpPD.	5.0(1k) and later
CSCvw69692	If a service graph gets attached to the inter-VRF contract after it was already attached to the intra-VRF contract, the pctag for the shadow EPG gets reprogrammed with a global value. The zoning-rule entries that matched the previous pctag as the source and EPG1 and EPG2 as the destination do not get reprogrammed and they remain in a stale status in the table. Traffic between EPG1 and EPG2 gets broken as the packets flowing from the PBR get classified with the new global pctag.	5.0(1k) and later
CSCvx10921	A standby APIC disappears from the GUI after cluster convergence.	5.0(1k) and later
CSCvy17504	When the OpFlexAgent moved from one vPC pair leaf switches to a new vPC pair, it may take up to 20 minutes for the OpFlexAgent detected the movement, and reconnect the OpFlex channel. Ideally, this should be completed within a few seconds.	5.0(1k) and later

Bug ID	Description	Exists in
CSCwa58709	The GIPo address is only visible on APIC 1 when using the command "cat /data/data_admin/sam_exported.config". The command output from the other APICs outputs do not show the GIPo address.	5.0(1k) and later
CSCwh98712	When running "show running-config" from API CLI, the command takes several minutes to complete. Several thousand API requests are seen in access.log querying ptpRsProfile on every static path.	5.0(1k) and later
CSCwi01316	In the following topology: Tenant 1: VRF 1 > EPG A, EPG B. There is an any-to-any Intra VRF instance contract and EPG A and B are providers for an inter-VRF instance contract. VRF 2 > L3Out or EPG. The VRF instance consumes the inter-VRF instance contract. Traffic will unexpectedly get sent to the wrong rule when inter-VRF instance traffic is flowing.	5.0(1k) and later

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 whether the bug was resolved in the base release or a patch release.

Bug ID	Description	Fixed in
CSCvd66359	The Port ID LLDP Neighbors panel displays the port ID when the interface does not have a description. Example: Ethernet 1/5, but if the interface has description, the Port ID property shows the Interface description instead of the port ID.	5.0(1k)
CSCvf70362	This enhancement is to change the name of "Limit IP Learning To Subnet" under the bridge domains to be more self-explanatory. Original : Limit IP Learning To Subnet: [check box] Suggestion : Limit Local IP Learning To BD/EPG Subnet(s): [check box]	5.0(1k)
CSCvg00627	A tenant's flows/packets information cannot be exported.	5.0(1k)
CSCvg35344	Requesting an enhancement to allow exporting a contract by right clicking the contract itself and choosing "Export Contract" from the right click context menu. The current implementation of needing to right click the Contract folder hierarchy to export a contract is not intuitive.	5.0(1k)
CSCvh52046	This is an enhancement to allow for text-based banners for the Cisco APIC GUI login screen.	5.0(1k)

Bug ID	Description	Fixed in
CSCvi20535	When a VRF table is configured to receive leaked external routes from multiple VRF tables, the Shared Route Control scope to specify the external routes to leak will be applied to all VRF tables. This results in an unintended external route leaking. This is an enhancement to ensure the Shared Route Control scope in each VRF table should be used to leak external routes only from the given VRF table.	5.0(1k)
CSCvj56726	The connectivity filter configuration of an access policy group is deprecated and should be removed from GUI.	5.0(1k)
CSCvk18014	The action named 'Launch SSH' is disabled when a user with read-only access logs into the Cisco APIC.	5.0(1k)
CSCvm42914	This is an enhancement request to add policy group information to the properties page of physical interfaces.	5.0(1k)
CSCvn12839	Error "mac.add.ress not a valid MAC or IP address or VM name" is seen when searching the EP Tracker.	5.0(1k)
CSCvp26694	A leaf switch gets upgraded when a previously-configured maintenance policy is triggered.	5.0(1k)
CSCvp62048	New port groups in VMware vCenter may be delayed when pushed from the Cisco APIC.	5.0(1k)
CSCvq57942	In a RedHat OpenStack platform deployment running the Cisco ACI Unified Neutron ML2 Plugin and with the CompHosts running OVS in VLAN mode, when toggling the resolution immediacy on the EPG<->VMM domain association (fvRsDomAtt.resImedcy) from Pre-Provision to On-Demand, the encap VLANs (vlanCktEp mo's) are NOT programmed on the leaf switches. This problem surfaces sporadically, meaning that it might take several resImedcy toggles between PreProv and OnDemand to reproduce the issue.	5.0(1k)
CSCvq63415	Disabling dataplane learning is only required to support a policy-based redirect (PBR) use case on pre-"EX" leaf switches. There are few other reasons otherwise this feature should be disabled. There currently is no confirmation/warning of the potential impact that can be caused by disabling dataplane learning.	5.0(1k)
CSCvq80820	A previously-working traffic is policy dropped after the subject is modified to have the "no stats" directive.	5.0(1k)
CSCvq96516	There is an event manager process crash.	5.0(1k)
CSCvr10020	Fault alarms get generated at a higher rate with a lower threshold. There is no functional impact.	5.0(1k)

Bug ID	Description	Fixed in
CSCvr12971	The Cisco APIC GUI produces the following error messages when opening an EPG policy: Received Invalid Json String. The server returned an unintelligible response. This issue might affect backup/restore functionality.	5.0(1k)
CSCvr19693	When configuring local SPAN in access mode using the GUI or CLI and then running the "show running-config monitor access session<session>" command, the output does not include all source span interfaces.	5.0(1k)
CSCvr62453	When a Cisco ACI fabric upgrade is triggered and a scheduler is created and associated to the maintenance group, the scheduler will remain associated to the maintenance group. If the version is changed in the maintenance group, it will trigger the upgrade. This enhancement is to avoid unwanted fabric upgrades. Post-upgrade, the association of the scheduler should be removed from the maintenance group after the node upgrade reaches 100%.	5.0(1k)
CSCvr73902	The GUI allows the target version to be changed in an existing upgrade group even when an upgrade is in progress.	5.0(1k)
CSCvr85945	The description field does not appear in the subnet IP address tables.	5.0(1k)
CSCvr86018	Some endpoints in the Cisco APIC GUI endpoint tracker have no state transitions, even when they have moved. When using icurl to get data on the same endpoints, state transitions are shown.	5.0(1k)
CSCvs03055	While configuring a logical node profile in any L3Out, the static routes do not have a description.	5.0(1k)
CSCvs04899	When you run the 'show vpc map' command in the Cisco APIC CLI, it only prints the column headers, but none of the vPC information. If you go to the leaf switch CLI and run the 'show vpc extended' command, it will show the vPCs there.	5.0(1k)
CSCvs11202	After exiting Maintenance (GIR) mode, the switch reloads automatically after 5 minutes without warning.This enhancement will provide messaging in the GUI to indicate that the reload is expected.	5.0(1k)
CSCvs13857	L3Out encapsulated routed interfaces and routed interfaces do not have any monitoring policy attached to them. As a result, there is no option to change the threshold values of the faults that occur due to these interfaces.	5.0(1k)
CSCvs16317	An app does not get fully removed from all Cisco APICs.	5.0(1k)
CSCvs29556	When logging into the Cisco APIC using "apic#fallback\\user", the "Error: list index out of range" log message displays and the lastlogin command fails. There is no operational impact.	5.0(1k)
CSCvs31335	App techsupport collection does not work sometimes when triggered from the Cisco APIC GUI.	5.0(1k)

Bug ID	Description	Fixed in
CSCvs53247	OpenStack supports more named IP protocols for service graph rules than are supported in the Cisco APIC OpenStack Plug-in.	5.0(1k)
CSCvs56642	This is an enhancement request for schedule-based Tech Support for leaf and spine switches.	5.0(1k)
CSCvs62693	The Name column of the the output of the "show zoning-rule" CLI command that is executed on a leaf switch running a 14.x release does not populate all of the expected contracts names. This issue makes it difficult to identify which rule ID is associated to which contract from the "show zoning-rule" command that is executed on a given leaf switch.	5.0(1k)
CSCvs81421	It is difficult to configure interface selectors in the GUI, because "interface policy group" window is too narrow.	5.0(1k)
CSCvs81429	It is difficult to configure interface selectors, because there is no search option available for the interface policy group window.	5.0(1k)
CSCvs81944	The following example shows UNIX time in the subject header: Subject: Configuration import/export job 2020-01-27T09-00-16 finished with status: success Created: 1580144423366 ContentType: plain/text	5.0(1k)
CSCvs92682	OID "1.3.6.1.4.1.9.9.117.2.0.0.2" in v1 SNMP trap cefcPowerStatusChange by Cisco APIC is observed.	5.0(1k)
CSCvt39746	Cisco APIC interfaces e2/3 & 2/4 persist in the GUI and the MIT after disabling and enabling the port channel on the VIC.	5.0(1k)
CSCvt44854	- Leaf or spine switch is stuck in 'downloading-boot-script' status. The node never fully registers and does not become active in the fabric. - You can check the status by running 'cat /mit/sys/summary | grep state' on the CLI of the spine or leaf switch: If the state is set to 'downloading-boot-script' for a long period of time (> 5 minutes) you may be running into this issue. - Checking the policy element logs on the spine or leaf switch will confirm if the bootscript file cannot be found on the Cisco APIC: 1. Change directory to /var/log/dme/log. 2. Grep all svc_ifc_policyelem.log files for "downloadUrl - failed, error=HTTP response code said error" If you see this error message, check to make sure all Cisco APICs have the node bootscript files located in /firmware/fwrepos/fwrepo/boot.	5.0(1k)
CSCvt48790	There is a stale fvIfConn entry after physically removing the ESXi host after a host is removed from the datacenter or VMware vCenter.	5.0(1k)

Bug ID	Description	Fixed in
CSCvt49260	The 'Primary VLAN for Micro-Seg' field does not show without putting a check in the Allow Micro-Segmentation check box.	5.0(1k)
CSCvt55566	In the Cisco APIC GUI, after removing the Fabric Policy Group from "System > Controllers > Controller Policies > show usage", the option to select the policy disappears, and there is no way in the GUI to re-add the policy.	5.0(1k)
CSCvt67097	In the Cisco APIC GUI, external EPGs under L2Out and L3Out in tenants are called "External Network Instance Profile". This is the official name for object (l2extInstP and l3extInstP). However, these are typically referred to as external EPGs. This is an enhancement to update the GUI label from "External Network Instance Profile" to "External EPG".	5.0(1k)
CSCvt67279	After VMware vCenter generates a huge amount of events and after the eventId increments beyond 0xFFFFFFFF, the Cisco APIC VMM manager service may start ignoring the newest event if the eventId is lower than the last biggest event ID that Cisco APIC received. As a result, the changes to virtual distributed switch or AVE would not reflect to the Cisco APIC, causing required policies to not get pushed to the Cisco ACI leaf switch. For AVE, missing those events could put the port in the WAIT_ATTACH_ACK status.	5.0(1k)
CSCvt68786	A Cisco ACI Virtual Edge EPG is not programmed on a port channel toward the blade switch after it is deleted and recreated.	5.0(1k)
CSCvt70316	SNMP poll/walk to the Cisco APIC does not work . The error message "unknown username" is received.	5.0(1k)
CSCvt92961	A TEP endpoint can expire on the leaf switch if the host does not respond on a unicast ARP refresh packet initiated by the leaf switch.	5.0(1k)
CSCvu01818	There is a message in the Cisco APIC GUI saying that vleaf_elem has restarted several times and may not have recovered, and there are core files of the vleaf_elem process.	5.0(1k)
CSCvu12478	Fabric > Inventory > Topology > Topology shows wrong Cisco APIC counts (Active + Standby) in different pods.	5.0(1k)
CSCvu18072	The Cisco APIC setup script will not accept an ID outside of the range of 1 through 12, and the Cisco APIC cannot be added to that pod. This issue will be seen in a multi-pod setup when trying add a Cisco APIC to a pod ID that is not between 1 through 12.	5.0(1k)

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 5.0(1) releases in which the known behavior exists. A bug might also exist in releases other than the 5.0(1) releases.

Bug ID	Description	Exists in

Bug ID	Description	Exists in
CSCvj26666	The "show run leaf|spine <nodeId>" command might produce an error for scaled up configurations.	5.0(1k) and later
CSCvj90385	With a uniform distribution of EPs and traffic flows, a fabric module in slot 25 sometimes reports far less than 50% of the traffic compared to the traffic on fabric modules in non-FM25 slots.	5.0(1k) and later
CSCvq39764	When you click Restart for the Microsoft System Center Virtual Machine Manager (SCVMM) agent on a scaled-out setup, the service may stop. You can restart the agent by clicking Start.	5.0(1k) 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)	5.0(1k) and later
CSCvr89603	The CRC and stomped CRC error values do not match when seen from the APIC CLI compared to the APIC GUI. This is expected behavior. The GUI values are from the history data, whereas the CLI values are from the current data.	5.0(1k) and later
CSCvs19322	Upgrading Cisco APIC from a 3.x release to a 4.x release causes Smart Licensing to lose its registration. Registering Smart Licensing again will clear the fault.	5.0(1k) and later
CSCvs77929	In the 4.x and later releases, if a firmware policy is created with different name than the maintenance policy, the firmware policy will be deleted and a new firmware policy gets created with the same name, which causes the upgrade process to fail.	5.0(1k) and later
CSCvs92309	A custom QoS policy at the LifP-level configuration is not supported for an MPLS L3Out.	5.0(1k) and later
CSCvt56254	Stats that should update every 15 minutes instead get updated after between 15 minutes and 20 minutes.	5.0(1k) and later
CSCvt85167	A Service graph that has service EPGs with vzAny as the consumer and provider gets the Global PCTag with EPGs/ESGs.	5.0(1k) and later

Bug ID	Description	Exists in
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.	5.0(1k) 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.	5.0(1k) 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.	5.0(1k) 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.	5.0(1k) 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.	5.0(1k) and later
N/A	When there are silent hosts across sites, ARP glean messages might not be forwarded to remote sites if a leaf switch without -EX or a later designation in the product ID happens to be in the transit path and the VRF is deployed on that leaf switch, the switch does not forward the ARP glean packet back into the fabric to reach the remote site. This issue is specific to transit leaf switches without -EX or a later designation in the product ID and does not affect leaf switches that have -EX or a later designation in the product ID. This issue breaks the capability of discovering silent hosts.	5.0(1k) 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.	5.0(1k) and later
N/A	MPLS interface statistics shown in a switch's CLI get cleared after an admin or operational down event.	5.0(1k) and later

Bug ID	Description	Exists in
N/A	MPLS interface statistics in a switch's CLI are reported every 10 seconds. If, for example, an interface goes down 3 seconds after the collection of the statistics, the CLI reports only 3 seconds of the statistics and clears all of the other statistics.	5.0(1k) and later

Compatibility Information

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
VMM Integration and VMware Distributed Virtual Switch (DVS)	6.5.x	*Cisco ACI Virtualization Guide, Release 5.0(x)*

Hardware Compatibility Information

This release supports the following Cisco APIC servers:

Product ID	Description
APIC-L1	Cisco APIC with large CPU, hard drive, and memory configurations (more than 1000 edge ports)
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-M1	Cisco APIC with medium-size CPU, hard drive, and memory configurations (up to 1000 edge ports)
APIC-M2	Cisco APIC with medium-size CPU, hard drive, and memory configurations (up to 1000 edge ports)

Product ID	Description
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 15.0(1)*.
- 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:

Hardware	Information
Cisco UCS M3/L3-based Cisco APIC	In this release, the Cisco APIC M3/L3 server does not support the UCSC-PCIE-IQ10GC Intel X710 Quad Port 10GBase-T network interface card.
Cisco UCS M4-based Cisco APIC	The Cisco UCS M4-based Cisco APIC and previous versions support only the 10G interface. Connecting the Cisco APIC to the Cisco ACI fabric requires a same speed interface on the Cisco ACI leaf switch. You cannot connect the Cisco APIC directly to the Cisco N9332PQ ACI leaf switch, unless you use a 40G to 10G converter (part number CVR-QSFP-SFP10G), in which case the port on the Cisco N9332PQ switch auto-negotiates to 10G without requiring any manual configuration.
Cisco UCS M5-based Cisco APIC	The Cisco UCS M5-based Cisco APIC supports dual speed 10G and 25G interfaces. Connecting the Cisco APIC to the Cisco ACI fabric requires a same speed interface on the Cisco ACI leaf switch. You cannot connect the Cisco APIC directly to the Cisco N9332PQ ACI leaf switch, unless you use a 40G to 10G converter (part number CVR-QSFP-SFP10G), in which case the port on the Cisco N9332PQ switch auto-negotiates to 10G without requiring any manual configuration.
N2348UPQ	To connect the N2348UPQ to Cisco ACI leaf switches, the following options are available: ■ Directly connect the 40G FEX ports on the N2348UPQ to the 40G switch ports on the Cisco ACI leaf switches ■ Break out the 40G FEX ports on the N2348UPQ to 4x10G ports and connect to the 10G ports on all other Cisco ACI leaf switches. Note: A fabric uplink port cannot be used as a FEX fabric port.
N9K-C9348GC-FXP	This switch does not read SPROM information if the PSU is in a shut state. You might see an empty string in the Cisco APIC output.
N9K-C9364C-FX	Ports 49-64 do not support 1G SFPs with QSA.

Hardware	Information
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	15.0(1)
Cisco AVS	5.2(1)SV3(4.10) For more information about the supported AVS releases, see the AVS software compatibility information in the *Cisco AVS Release Notes, Release 5.2(1)SV3(4.10)*.
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

Product	Supported Release
CIMC HUU ISO	■ 4.2(3j) CIMC HUU ISO (recommended) for UCS C220/C240 M5 (APIC-L3/M3) ■ 4.2(3e) CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3) ■ 4.2(3b) CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3) ■ 4.2(2a) CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3) ■ 4.1(3m) CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3) ■ 4.1(3f) CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3) ■ 4.1(3d) CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3) ■ 4.1(3c) CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3) ■ 4.1(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(4l) CIMC HUU ISO (recommended) for UCS C220/C240 M3 (APIC-L1/M1) ■ 3.0(4d) CIMC HUU ISO for UCS C220/C240 M3 and M4 (APIC-L1/M1 and APIC-L2/M2) ■ 3.0(3f) CIMC HUU ISO for UCS C220/C240 M4 (APIC-L2/M2) ■ 3.0(3e) CIMC HUU ISO for UCS C220/C240 M3 (APIC-L1/M1) ■ 2.0(13i) CIMC HUU ISO ■ 2.0(9c) CIMC HUU ISO ■ 2.0(3i) CIMC HUU ISO

Product	Supported Release
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 Day-2 Operations Apps Support 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 5.0(x)*.
- For compatibility with Day-2 Operations apps, see the Cisco Day-2 Operations Apps Support 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.

You can watch videos that demonstrate how to perform specific tasks in the Cisco APIC on the Cisco ACI 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 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.

The following table provides links to the release notes, verified scalability documentation, and new documentation:

Document	Description
Cisco ACI Virtual Edge Release Notes, Release 3.0(1a)	The release notes for Cisco ACI Virtual Edge.
Cisco ACI Virtual Pod Release Notes, Release 5.0(1)	The release notes for Cisco ACI Virtual Pod.
Cisco Application Centric Infrastructure Simulator Release Notes, Release 5.0(1)	The release notes for the Cisco ACI Simulator.

Cisco Nexus 9000 ACI-Mode Switches Release Notes, Release 15.0(1)	The release notes for Cisco NX-OS for Cisco Nexus 9000 Series ACI-Mode Switches.
Verified Scalability Guide for Cisco APIC, Release 5.0(1), Multi-Site, Release 3.0(1), and Cisco Nexus 9000 Series ACI-Mode Switches, Release 15.0(1)	This guide contains the maximum verified scalability limits for Cisco Application Centric Infrastructure (ACI) parameters for Cisco APIC, Cisco ACI Multi-Site, and Cisco Nexus 9000 Series ACI-Mode Switches.

Documentation Feedback

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

Legal Information

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: 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.

© 2020-2024 Cisco Systems, Inc. All rights reserved.