Cisco Application Policy Infrastructure Controller Release Notes, Release 5.1(4)

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 15.1(4).

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

Date	Description
May 6, 2024	In the Miscellaneous Compatibility Information section, added: • 4.3.2.240009 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)
July 1, 2022	In the Open Issues section, added bug CSCwb93239.
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.
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 18, 2021	Release 5.1(4c) became available.

New Software Features

Feature	Description
Applying a route map to interleak redistribution from direct subnets	You can apply a route map to interleak redistribution from direct subnets (L3Out interfaces). You can also configure the deny action in the route-map for interleak redistribution for static routes and direct subnets. For more information, see the Cisco APIC Layer 3 Networking Configuration Guide, Release 5.1(x).
Deny action in the route	You can configure the deny action in the route-map for interleak redistribution for static

Feature	Description
map for interleak redistribution for static routes and direct subnets	routes and direct subnets. For more information, see the Cisco APIC Layer 3 Networking Configuration Guide, Release 5.1(x).

New Hardware Features

For the new hardware features, see the Cisco Nexus 9000 ACI-Mode Switches Release Notes, Release 15.1(4).

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 5.1(4) releases in which the bug exists. A bug might also exist in releases other than the 5.1(4) releases.

Bug ID	Description	Exists in
CSCvq81020	For strict security requirements, customers require custom certificates that have RSA key lengths of 3072 and 4096.	5.1(4c) and later
CSCvm56946	Support for local user (admin) maximum tries and login delay configuration.	5.1(4c) and later
CSCvs47602	A bridge domain route is not leaked on the service ToR switch after re-triggering the service graph.	5.1(4c) and later
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.	5.1(4c) 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".	5.1(4c) and later
CSCvw12766	In a setup where there is already existing MDP confguration (spine and leaf nodes), after having deleted an MDP spine node, MDP tunnels and traffic might still be directed to that spine node. In the case of a new MDP spine node, the traffic might not get directed to the new spine node.	5.1(4c) 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.	5.1(4c) and later
CSCvw84947	The BGP loop prevention feature for the inter-VRF shared service case does function as expected upon upgradeing to the 5.1(4) release with existing contracts for a brownfield environment. There is no impact if new contracts are used.	5.1(4c) and later

Bug ID	Description	Exists in
CSCvx10921	A standby APIC disappears from the GUI after cluster convergence.	5.1(4c) 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.	5.1(4c) and later
CSCwa58709	The GIPo address is only visible on APIC 1 when using the command " cat /data/data_admin/sam_exported.config" . The command output from the other APICs outputs do not show the GIPo address.	5.1(4c) and later
CSCwb93239	The GUI displays the following error: Failed, Local Upload Failure Msg (Request failed with status code 413).	5.1(4c) and later
CSCwe58398	This is added functionality for upgrade show command. 1. acidiag show postupgrade -service <dme> -> This gives details for dmes and which shard still have pending postUpgradeCb. 2.acidiag show postupgrade -service <dme> -shard <shard_id> -> This gives the details of log path for the dmes and shard for which postUpgradeCb has been completed.	5.1(4c) and later
CSCwh84052	When using the OpenStack integration, the Cisco APIC VMM Manager process may consume more memory than is available and then end.	5.1(4c) 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.	5.1(4c) 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.	5.1(4c) and later

Resolved Issues

Bug ID	Description	Fixed in
CSCvw62384	After upgrading the switch nodes, the policy manager crashes on all Cisco APICs in a cluster and all replicas are down for the policy manager data management engine.	5.1(4c)
CSCvx12522	When adding or deleting a static route to an L3Out, it may trigger an update to the contracts to which its VRF is related, even if the contract is not modified.	5.1(4c)
CSCvx45585	The urlToken is not returned after logging in to the Cisco APIC.	5.1(4c)

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 5.1(4) releases in which the bug exists. A bug might also exist in releases other than the 5.1(4) releases.

Bug ID	Description	Exists in
CSCvj26666	The "show run leaf|spine <nodeId>" command might produce an error for scaled up configurations.	5.1(4c) 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.	5.1(4c) 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.	5.1(4c) 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)	5.1(4c) 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.	5.1(4c) 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.	5.1(4c) 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.	5.1(4c) and later
N/A	Beginning in Cisco APIC release 4.1(1), the IP SLA monitor policy validates the IP SLA port value. Because of the validation, when TCP is configured as the IP SLA type, Cisco APIC no longer accepts an IP SLA port value of 0, which was allowed in previous releases. An IP SLA monitor policy from a previous release that has an IP SLA port value of 0 becomes invalid if the Cisco APIC is upgraded to release 4.1(1) or later. This results in a failure for the configuration import or snapshot rollback. The workaround is to configure a non-zero IP SLA port value before upgrading the Cisco APIC, and use the snapshot and configuration export that was taken after the IP SLA port change.	5.1(4c) 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.	5.1(4c) 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.	5.1(4c) and later

Bug ID	Description	Exists in
N/A	With a non-english SCVMM 2012 R2 or SCVMM 2016 setup and where the virtual machine names are specified in non-english characters, if the host is removed and re-added to the host group, the GUID for all the virtual machines under that host changes. Therefore, if a user has created a micro segmentation endpoint group using "VM name" attribute specifying the GUID of respective virtual machine, then that micro segmentation endpoint group will not work if the host (hosting the virtual machines) is removed and re-added to the host group, as the GUID for all the virtual machines would have changed. This does not happen if the virtual name has name specified in all english characters.	5.1(4c) 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.	5.1(4c) 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.	5.1(4c) 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.	5.1(4c) and later
N/A	MPLS interface statistics shown in a switch's CLI get cleared after an admin or operational down event.	5.1(4c) 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.	5.1(4c) and later

Virtualization Compatibility Information

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

- For a table that shows the supported virtualization products, see the ACI Virtualization Compatibility Matrix.
- For information about Cisco APIC compatibility with Cisco UCS Director, see the appropriate Cisco UCS Director Compatibility Matrix document.
- This release supports the following additional virtualization products:

Product	Supported Release	Information Location
Microsoft Hyper-V	• SCVMM 2019 RTM (Build 10.19.1013.0) or newer • SCVMM 2016 RTM (Build 4.0.1662.0) or newer • SCVMM 2012 R2 with Update Rollup 9 (Build 3.2.8145.0) or newer	N/A

Product	Supported Release	Information Location
VMM Integration and VMware Distributed Virtual Switch (DVS)	6.5, 6.7, and 7.0	Cisco ACI Virtualization Guide, Release 5.1(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)
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 15.1(4).
- 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

Product ID	Description
	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 supporFut 1G SFPs with QSA.
N9K-C9508-FM-E	The Cisco N9K-C9508-FM-E2 and N9K-C9508-FM-E fabric modules in the mixed mode configuration are not supported on the same spine switch.
N9K-C9508-FM-E2	The Cisco N9K-C9508-FM-E2 and N9K-C9508-FM-E fabric modules in the mixed mode configuration are not supported on the same spine switch. The locator LED enable/disable feature is supported in the GUI and not supported in the Cisco ACI NX-OS switch CLI.
N9K-C9508-FM-E2	This fabric module must be physically removed before downgrading to releases earlier than Cisco APIC 3.0(1).
N9K-X9736C-FX	The locator LED enable/disable feature is supported in the GUI and not supported in the Cisco ACI NX-OS Switch CLI.
N9K-X9736C-FX	Ports 29 to 36 do not support 1G SFPs with QSA.

Adaptive Security Appliance (ASA) Compatibility Information

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

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

  (config)# ssl encryption aes128-sha1

Miscellaneous Compatibility Information

This release supports the following products:

Product	Supported Release
Cisco NX-OS	15.1(4)
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 Application Virtual Switch Release Notes, Release 5.2(1)SV3(4.11).
Cisco UCS Manager	2.2(1c) or later is required for the Cisco UCS Fabric Interconnect and other components, including the BIOS, CIMC, and the adapter.
CIMC HUU ISO	• 4.3.2.240009 CIMC HUU ISO (recommended) for UCS C220/C240 M5 (APIC-L3/M3) • 4.2(3e) CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3) • 4.2(3b) CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3) • 4.2(2a) CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3) • 4.1(3m) CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3) • 4.1(3f) CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3) • 4.1(3d) CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3) • 4.1(3c) CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3) • 4.1(2m) CIMC HUU ISO (recommended) for UCS C220/C240 M4 (APIC-L2/M2) • 4.1(2k) CIMC HUU ISO for UCS C220/C240 M4 (APIC-L2/M2) • 4.1(2g) CIMC HUU ISO for UCS C220/C240 M4 (APIC-L2/M2) • 4.1(2b) CIMC HUU ISO for UCS C220/C240 M4 (APIC-L2/M2) • 4.1(1g) CIMC HUU ISO for UCS C220/C240 M4 (APIC-L2/M2) and M5 (APIC-L3/M3) • 4.1(1f) CIMC HUU ISO for UCS C220 M4 (APIC-L2/M2) (deferred release) • 4.1(1d) CIMC HUU ISO for UCS C220 M5 (APIC-L3/M3) • 4.1(1c) CIMC HUU ISO for UCS C220 M4 (APIC-L2/M2) • 4.0(4e) CIMC HUU ISO for UCS C220 M5 (APIC-L3/M3) • 4.0(2g) CIMC HUU ISO for UCS C220/C240 M4 and M5 (APIC-L2/M2 and APIC-L3/M3) • 4.0(1a) CIMC HUU ISO for UCS C220 M5 (APIC-L3/M3) • 3.0(4d) CIMC HUU ISO for UCS C220/C240 M3 and M4 (APIC-L2/M2) • 3.0(3f) CIMC HUU ISO for UCS C220/C240 M4 (APIC-L2/M2) • 2.0(13i) CIMC HUU ISO • 2.0(9c) CIMC HUU ISO • 2.0(3i) CIMC HUU ISO
Network Insights Base, Network Insights Advisor, and Network Insights for Resources	For the release information, documentation, and download links, see the Cisco Network Insights for Data Center page. For the supported releases, see the Cisco Data Center Networking Applications Compatibility Matrix.

- This release supports the partner packages specified in the L4-L7 Compatibility List Solution Overview document.
- A known issue exists with the Safari browser and unsigned certificates, which applies when connecting to the Cisco APIC GUI. For more information, see the Cisco APIC Getting Started Guide, Release 5.1(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 Data Center Networking YouTube channel.

Temporary licenses with an expiry date are available for evaluation and lab use purposes. They are strictly not allowed to be used in production. Use a permanent or subscription license that has been purchased through Cisco for production purposes. For more information, go to Cisco Data Center Networking Software Subscriptions.

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

Document	Description
Cisco Nexus 9000 ACI-Mode Switches Release Notes, Release 15.1(4)	The release notes for Cisco NX-OS for Cisco Nexus 9000 Series ACI-Mode Switches.
Verified Scalability Guide for Cisco APIC, Release 5.1(3) and Cisco Nexus 9000 Series ACI-Mode Switches, Release 15.1(3)	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. **Note:** The 5.1(3) release document applies to the 5.1(4) release.

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