



Cisco Application Policy Infrastructure Controller Release Notes, Release 5.1(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 15.1\(1\)](#).

For more information about this product, see [Related Content](#).

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.

Date	Description
December 15, 2020	In the Changes in Behavior section, added the following text: The "ip" attribute of the fvCEp class has been deprecated. IP addresses are now represented as fvlp children of fvCEp.
October 22, 2020	Release 5.1(1h) became available.

Contents

- New Software Features
- Changes in Behavior
- Open Issues
- Resolved Issues
- Known Issues
- Compatibility Information
- Related Content
- Documentation Feedback
- Legal Information

New Software Features

Feature	Description	Guidelines and Restrictions
Enhancements to the upgrade process through the GUI when upgrading the APIC or switch software.	The upgrade process for the APIC and switch software through the GUI has been enhanced. For more information, see the Cisco APIC Installation, Upgrade, and Downgrade Guide .	None.
IGMP snooping querier version 2 support	IGMP snooping querier version 2 is now supported. For information about the IGMP snooping querier, see the Cisco APIC Layer 3 Networking Configuration Guide, Release 5.1(x) .	None.
SSD write optimization	The SSD write strategy is optimized for improved performance and longer SSD life.	None.
Support for associating a Layer 3 EPG from the in-band management tenant with a NetFlow exporter	You can now associate an EPG or L3Out from the in-band VRF under the management tenant with a NetFlow exporter. For information about NetFlow, see the Cisco APIC and NetFlow document.	None.
Support for SNMPv3 and SHA-2	SNMPv3 trap aggregation and forwarding is now supported. SNMPv3 supports the Secure Hash Algorithm-2 (SHA-2) authentication type. For information about SNMP, see the Cisco APIC Basic Configuration Guide, Release 5.1(x) .	None.
VMware NSX-T data center integration with Cisco ACI	You can integrate VMware NSX-T Data Center with Cisco ACI. Integration enables you to use Cisco APIC to create and work with VMware NSX-T Data Center network constructs. For more information, see the Cisco ACI and VMware	None.

Changes in Behavior

Feature	Description	Guidelines and Restrictions
	NSX-T Data Center Integration document.	

Changes in Behavior

- The "ip" attribute of the fvCEp class has been deprecated. IP addresses are now represented as fvlp children of fvCEp. This change provides better support for having multiple IP addresses on the same MAC address.

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(1) releases in which the bug exists. A bug might also exist in releases other than the 5.1(1) releases.

Bug ID	Description	Exists in
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.	5.1(1h) and later
CSCvs47602	A bridge domain route is not leaked on the service ToR switch after re-triggering the service graph.	5.1(1h) 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(1h) 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 fvlfConn not available".	5.1(1h) and later
CSCvw69041	There is traffic loss on SDA after deleting an overlapping subnet.	5.1(1h) and later
CSCww12766	In a setup where there is already existing MDP configuration (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(1h) 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
--------	-------------	----------

Known Issues

Bug ID	Description	Fixed in
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.	5.1(1h) and later
CSCvu76494	User is logged into one tab and is trying to log in to another one using same credentials. Login page will show for less than a minute and then user will get redirected to main page.	5.1(1h) and later
CSCvt18145	The routemap becomes missing in the shared service routemap.	5.1(1h)
CSCvt92062	The Cisco APIC CLI does not have commands for the following functionality: <ul style="list-style-type: none"> 1. ESG show commands 2. ESG inter-VRF route leak configuration 	5.1(1h)
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.	5.1(1h)
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.	5.1(1h)

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(1) releases in which the known behavior exists. A bug might also exist in releases other than the 5.1(1) releases.

Bug ID	Description	Exists in
CSCvj26666	The "show run leaf spine <nodeId>" command might produce an error for scaled up configurations.	5.1(1h) 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(1h) and later
CSCvm71833	Switch upgrades fail with the following error: Version not compatible.	5.1(1h) 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(1h) and later

Known Issues

Bug ID	Description	Exists in
CSCvq58953	<p>One of the following symptoms occurs:</p> <ul style="list-style-type: none"> ■ 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: <p>Error querying node status: Unexpected response code: 500 (rpc error: No cluster leader)</p>	5.1(1h) 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(1h) 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(1h) 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(1h) and later
CSCvs92309	A custom QoS policy at the LifP-level configuration is not supported for an MPLS L3Out.	5.1(1h) and later
CSCvt56254	Stats that should update every 15 minutes instead get updated after between 15 minutes and 20 minutes.	5.1(1h) and later
CSCvt85167	A Service graph that has service EPGs with vzAny as the consumer and provider gets the Global PCTag with EPGs/ESGs.	5.1(1h) 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>	5.1(1h) 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(1h) and later

Bug ID	Description	Exists in
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(1h) 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.	5.1(1h) 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(1h) 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(1h) 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(1h) and later
N/A	MPLS interface statistics shown in a switch's CLI get cleared after an admin or operational down event.	5.1(1h) 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(1h) 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](#).

Compatibility Information

- For information about Cisco APIC compatibility with Cisco UCS Director, see the appropriate [Cisco UCS Director Compatibility Matrix](#) document.
- If you use Microsoft vSwitch and want to downgrade to Cisco APIC Release 2.3(1) from a later release, you first must delete any microsegment EPGs configured with the Match All filter.
- This release supports the following additional virtualization products:

Product	Supported Release	Information Location
Microsoft Hyper-V	2016 Update Rollup 1, 2, 2.1, and 3	N/A
VMM Integration and VMware 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)
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\(1\)](#).
- 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."
- Switches without -EX or a later designation 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
----------	-------------

Hardware	Information
M4 Cisco APIC	The M4 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.
M5 Cisco APIC	The M5 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: <ul style="list-style-type: none"> ■ 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. <p>Note: A fabric uplink port cannot be used as a FEX fabric port.</p>
N9K-C9348GC-FXP	This switch does not read SPROM information if the PSU is in a shut state. You might see an empty string in the Cisco APIC output.
N9K-C9364C-FX	Ports 49-64 do not support 1G SFPs with QSA.
N9K-C9508-FM-E	The Cisco N9K-C9508-FM-E2 and N9K-C9508-FM-E fabric modules in the mixed mode configuration are not supported on the same spine switch.
N9K-C9508-FM-E2	The Cisco N9K-C9508-FM-E2 and N9K-C9508-FM-E fabric modules in the mixed mode configuration are not supported on the same spine switch. The locator LED enable/disable feature is supported in the GUI and not supported in the Cisco ACI NX-OS switch CLI.
N9K-C9508-FM-E2	This fabric module must be physically removed before downgrading to releases earlier than Cisco APIC 3.0(2).
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(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
CIMC HUU ISO	<ul style="list-style-type: none"> ■ 4.1(1g) CIMC HUU ISO (recommended) 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 C240 M4 and M5 (APIC-L2/M2 and APIC-L3/M3) ■ 4.0(2g) CIMC HUU ISO for UCS C220 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

Related Content

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 5.1\(x\)](#).
- For compatibility with Day-2 Operations apps, see the [Cisco Day-2 Operations Apps Support Matrix](#).

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 3.1(1)	The release notes for Cisco ACI Virtual Edge.
Cisco Application Centric Infrastructure Simulator Release Notes, Release 5.1(1)	The release notes for the Cisco ACI Simulator.
Cisco Nexus 9000 ACI-Mode Switches Release Notes, Release 15.1(1)	The release notes for Cisco NX-OS for Cisco Nexus 9000 Series ACI-Mode Switches.
<i>Verified Scalability Guide for Cisco APIC, Release 5.1(1), Multi-Site, Release 3.1(1), and Cisco Nexus 9000 Series ACI-Mode Switches, Release 15.1(1)</i>	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. Note: This document is not yet available, but will be soon.

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 Cisco Systems, Inc. All rights reserved.