Cisco Catalyst Center Banner Messages

© 2025 Cisco and/or its affiliates. All rights reserved.

Overview of banners 3
Explanation of each banner 3
Related resources 4
Legal information 24

© 2025 Cisco and/or its affiliates. All rights reserved.

Overview of banners

To ensure your network always benefits from the latest best practices, Catalyst Center automatically refines feature configurations with each release.

When an upgrade includes improved settings, you'll see a clear banner notification. Apply the update instantly with a click. There's no need to reconfigure features or perform any manual steps. Catalyst Center handles the process for you.

Some banner notifications depend on specific IOS-XE versions. These banners remain inactive and do not count toward the 180-day timer until your network devices are running the required IOS-XE versions.

Not all banner notifications apply to every customer. You only see banners for updates introduced based on your feature usage. This ensures that you are notified only about configuration changes relevant to your deployment.

See the individual Catalyst Center Release Notes for any additional caveats.

Workflow

1. Banner messages notify you of required CLI changes after a release upgrade.
2. You have 180 days to apply the changes.
3. All fabric provisioning operations are blocked after 180 days if the banner changes are not applied.

Note: Existing fabric continues to work unaffected. Only new fabric provisioning is blocked.

Explanation of each banner

This section describes each Catalyst Center banner and its impact.

Cluster IP change

Table 1. Banner title: Cluster IP change

Value	Description
Release introduced	3.1.3
Full text of banner	The Catalyst Center IP address has changed. The Supplicant-Based Extended Node onboarding ACL must be updated to allow the new IP address. This update is necessary before onboarding new supplicant-based extended nodes. The update should not impact production network traffic.
Summary	After a backup and restore operation, if the Catalyst Center IP address changes and supplicant-based extended node (SBEN) onboarding is enabled in the fabric, this banner is shown. This banner alerts you that the SBEN ACL configuration must be updated with the new Catalyst Center IP address.

© 2025 Cisco and/or its affiliates. All rights reserved.

Value	Description
Configuration details	ip access-list extended SBEN_MAB_ACL no 10 permit ip any host <IP_address> no 20 permit tcp any host <IP_address> eq www no 30 permit tcp any host <IP_address> eq 443 10 permit ip any host <IP_address> 20 permit tcp any host <IP_address> eq www 30 permit tcp any host <IP_address> eq 443 exit
Impact	Supplicant-based extended node onboarding doesn't work until this banner is applied. There is no impact to production network traffic.

Remove automated iBGP within the fabric

Table 2. Banner title: Remove automated iBGP within the fabric

Value	Description
Release introduced	2.3.7.9
Full text of banner	Automated iBGP sessions between Border Nodes and Control Plane Nodes will be removed as part of a configuration simplification, as they are no longer needed for fabric operations. This change does not affect Layer 3 Handoff automated eBGP neighbors or any manually configured or templated BGP neighbors.
Summary	This banner removes iBGP configurations within the fabric on LISP/PubSub sites. This banner ensures routes imported from LISP to BGP (on internal borders) are redistributed back to BGP on other borders, including other borders on other sites that are connected using SDA-Transit.

© 2025 Cisco and/or its affiliates. All rights reserved.

Value	Description
Configuration details	Sample configuration of external collocated border (CP + B) with SDA transit: no ip community-list 84 no ip community-list 84 permit 844888 route-map LISP_TO_BGP permit 10 match tag 955999 route-map LISP_TO_BGP permit 15 description Set the BGP AS Path to AS Number of BGP Handoff Neighbor set as-path tag router bgp 64001 address-family ipv4 no neighbor <IP_address> route-map DENY_0_FABRIC_PREFIX out no neighbor <IP_address> send-community both no neighbor <IP_address> route-map DENY_0_FABRIC_PREFIX out no neighbor <IP_address> send-community both exit address-family vpnv4 no neighbor <IP_address> route-map DENY_0_FABRIC_PREFIX out no neighbor <IP_address> send-community both no neighbor <*IP_address*> route-map DENY_0_FABRIC_PREFIX out no neighbor <*IP_address*> send-community both exit address-family ipv6 no neighbor <IP_address> route-map DENY_0_FABRIC_PREFIX_V6 out no neighbor <IP_address> send-community both no neighbor <IP_address> route-map DENY_0_FABRIC_PREFIX_V6 out no neighbor <IP_address> send-community both exit address-family vpnv6 no neighbor <IP_address> route-map DENY_0_FABRIC_PREFIX_V6 out no neighbor <IP_address> send-community both no neighbor <IP_address> route-map DENY_0_FABRIC_PREFIX_V6 out no neighbor <IP_address> send-community both exit no neighbor <IP_address> remote-as 64001 no neighbor <IP_address> remote-as 64001 router lisp instance-id 4097 service ipv4 database-mapping <IP_address>/24 locator-set rloc_537529e3-d852-4475-861a-468c66d0ec25 route-tag 955999 proxy instance-id 4098

Value	Description
Impact	There is impact to traffic forwarding when the banner is executed. It is recommended to execute this banner only during a maintenance window.

Group-based policy enforcement update for supplicant-based extended nodes

Table 3. Banner title: Group-based policy enforcement update for supplicant-based extended nodes

Value	Description
Release introduced	2.3.7.6
Full text of banner	The configuration standards for supplicant-based extended nodes have been revised to explicitly disable group-based policy enforcement on the uplink interfaces. This modification will improve the reliability of the onboarding process for these nodes.
Summary	Improves onboarding reliability for supplicant-based extended nodes (SBENs) by ensuring group-based policy enforcement is explicitly disabled on uplink interfaces for SBENs and APs.
Configuration details	Fabric Edge or Authenticated Extended node in daisy chained deployment: template SWITCH_SBEN_FULL_ACCESS_TEMPLATE no cts role-based enforcement exit Authenticated Extended Node: interface GigabitEthernet1/0/1 no cts role-based enforcement exit
Impact	Adds to the interface template for onboarding supplicant-based extended nodes.

Client not reauthenticated with Open Auth when AAA server comes back online

Table 4. Banner title: Client not reauthenticated with Open Auth when AAA server comes back online

Value	Description
Release introduced	2.3.5.4
Full text of banner	When AAA servers become unreachable, some endpoints cannot authenticate with the SD-Access fabric. When the AAA servers become reachable, the endpoints that failed authentication cannot reauthenticate. To enable reauthentication, a new authentication template must be applied to all edge nodes and extended nodes. Applying a new authentication template may reset the active client sessions.
Summary	If the AAA server becomes unreachable or the device loses connection to it, the device enters critical voice and critical VLAN mode. When the AAA server comes back online, only the service templates for the critical voice VLAN are activated for the critical authentication class map. To allow data clients to reauthenticate, the critical VLAN for data must also be configured. This banner appears when the fabric site includes an edge or extended node device.

© 2025 Cisco and/or its affiliates. All rights reserved.

Value	Description
Configuration details	Before: class-map type control subscriber match-any IN_CRITICAL_AUTH match activated-service-template DefaultCriticalVoice_SRV_TEMPLATE ! class-map type control subscriber match-none NOT_IN_CRITICAL_AUTH match activated-service-template DefaultCriticalVoice_SRV_TEMPLATE After: class-map type control subscriber match-any IN_CRITICAL_AUTH match activated-service-template DefaultCriticalVoice_SRV_TEMPLATE match activated-service-template DefaultCriticalAuthVlan_SRV_TEMPLATE <<<< After banner application class-map type control subscriber match-any IN_CRITICAL_AUTH_CLOSED_MODE match activated-service-template DefaultCriticalAuthVlan_SRV_TEMPLATE <<<< After banner application match activated-service-template DefaultCriticalVoice_SRV_TEMPLATE
Impact	Applying this banner might reset the active client sessions.

Explicit device provisioning capability online card addition event for edge nodes and extended nodes

Table 5. Banner title: Explicit device provisioning capability online card addition event for edge nodes and extended nodes

Value	Description
Release introduced	2.3.4.3
Full text of banner	One or more stack members or linecards have been added to existing switches. The Site Authentication Template must be configured on these new stack members/linecards.
Summary	This banner appears when a new member stack or line card is added to a fabric edge or extended node, requiring explicit provisioning. You must manually apply this banner to initiate device provisioning for the added ports. This applies when fabric authentication is set to Closed, Open, or Low Impact. This banner also appears when a line card is detected with ports previously used for port assignment or port channels, but whose interfaces are set to dynamic auto, instead of the expected access mode. This banner may reappear if additional new ports are detected.

© 2025 Cisco and/or its affiliates. All rights reserved.

Value	Description
Configuration details	If the authentication template is Closed Auth: interface Forty1/1/1 no load-interval no switchport voice vlan no switchport access vlan switchport mode access source template DefaultWiredDot1xClosedAuth spanning-tree portfast spanning-tree bpduguard enable dot1x timeout tx-period 7 dot1x max-reauth-req 3 If the authentication template is Open Auth: interface Forty1/1/1 no load-interval no switchport voice vlan no switchport access vlan switchport mode access source template DefaultWiredDot1xOpenAuth spanning-tree portfast spanning-tree bpduguard enable dot1x timeout tx-period 7 dot1x max-reauth-req 3 If Authentication Template is Low Impact: interface Forty1/1/1 no load-interval no switchport voice vlan no switchport access vlan switchport mode access source template DefaultWiredDot1xLowImpactAuth spanning-tree portfast spanning-tree bpduguard enable ipv6 traffic-filter IPV6_PRE_AUTH_ACL in ip access-group IPV4_PRE_AUTH_ACL in dot1x timeout tx-period 7 dot1x max-reauth-req 3
Impact	This configuration change impacts newly added line cards or stack members and their ports.

© 2025 Cisco and/or its affiliates. All rights reserved.

Extended nodes daisy chaining enhancements

Table 6. Banner title: Extended nodes daisy chaining enhancements

Value	Description
Release introduced	2.3.3.0
Full text of banner	This release introduces the capability to daisy chain Supplicant-Based Extended Nodes and Catalyst 9000 Series Switches operating as Policy Extended Nodes. To support this feature, new Access-Control Lists and interface templates will be provisioned on existing Policy Extended Node devices.
Summary	This banner enables Catalyst 9000 series supplicant-based extended nodes to be onboarded in a daisy chain topology. The banner is available when upgrading to 2.3.3.0 with supplicant-based extended node enabled and existing policy extended nodes in the fabric.

© 2025 Cisco and/or its affiliates. All rights reserved.

Value	Description

Configuration details	template SWITCH_AEN_MAB_TEMPLATE
	  switchport access vlan {en_vlan}
	  switchport mode access
	
	template SWITCH_AEN_FULL_ACCESS_TEMPLATE
	  cts manual
	  policy static sgt 8000 trusted
	  switchport mode trunk
	  access-session host-mode multi-host peer
	
	template SWITCH_AEN_BPDU_TEMPLATE
	  spanning-tree bpduguard enable
	
	ip access-list extended AEN_DHCP_ACL
	  permit udp any any eq 67
	  permit udp any any eq 68
	  deny ip any any
	
	ip access-list extended AEN_MAB_ACL
	  permit ip any host {DNAC_IP}
	  permit ip any host {EN_Subnet_Gateway}
	  permit ip any host {DHCP_Server}
	  permit ip any host {DNS_Server}
	  permit tcp any host {DNAC_IP} eq 80
	  permit tcp any host {DNAC_IP} eq 443
	  permit tcp any host {DNAC_IP} eq 2222
	  permit udp any any eq 67
	  permit udp any any eq 68
	  deny ip any any

Impact	No impact. New functionality.

TCP adjust-MSS feature

Table 7. Banner title: TCP Adjust-MSS Feature

Value	Description
Release introduced	2.3.3.x

© 2025 Cisco and/or its affiliates. All rights reserved.

Value	Description
Full text of banner	In a Fabric Site, Edge Nodes and Border Nodes with a Layer 2 Handoff are provisioned with the same Anycast Gateways. An Anycast Gateway is instantiated on these devices as a Switched Virtual Interface (SVI). When connecting to an IP-based transit, a Border Node can be provisioned with a Layer 3 Handoff which designates one or more physical interfaces that connect to the transit. This Layer 3 handoff is instantiated with SVIs on switching platforms and sub-interfaces on routing platforms. This release provides an enhancement to the instantiated interfaces by configuring the maximum segment size (MSS) value of the TCP segments traversing them. If there is disparity in the MTU (maximum transmission unit) value in the path between devices forming a TCP session, packets may be dropped, and the TCP session may be terminated. To address this potential MTU disparity, this enhancement adjusts the TCP MSS value to 1250 bytes on these interfaces. This provides an optimized value to accommodate common MTU overhead used by encapsulation protocols. If there are existing TCP MSS values on these interfaces, those values will not be overridden by this enhancement
Summary	SD-Access uses VxLAN encapsulation for transporting endpoint data which cannot be fragmented in fabric sites or fabric transits. Today DNAC LAN automation pushes 9100 MTU to fabric nodes. To support VXLAN traffic over links with a lower MTU, configure TCP MSS adjustment at the SD-Access fabric ingress using either templates or the device CLI. Applying this banner will enable the automation of wired TCP adjust MSS settings.
Configuration details	Interface VLAN ## / Interface Gig0/0/0.xxx ip tcp adjust-mss 1250 <--- if ipv4 address is configured on the interface ipv6 tcp adjust-mss 1250 <--- if ipv6 address is configured on the interface If there are existing tcp adjust-mss configuration on the interfaces, the above CLIs will not be pushed.
Impact	Enhancement

SD-Access Assurance banner to call out the NETCONF requirements for streaming telemetry

Table 8. Banner title: SD-Access Assurance banner to call out the NETCONF requirements for streaming telemetry

Value	Description
Release introduced	2.3.3.x
Full text of banner	SD-Access Assurance subscribes to telemetry subscriptions from the fabric nodes to gather real-time assurance data. This requires network devices to be configured with NETCONF and telemetry enabled for Key Performance Indicators to be provisioned. Note: To enable NETCONF, navigate to Provision > Network Devices > Inventory > FOCUS: Inventory, select devices and choose Actions > Inventory > Edit Device the network device to configure netconf. To provision telemetry subscription, navigate to Provision > Network Devices > Inventory > FOCUS: Inventory, select devices and choose Actions > Telemetry > Update Telemetry Settings.

© 2025 Cisco and/or its affiliates. All rights reserved.

Value	Description
Summary	SD-Access Assurance requires fabric nodes to be provisioned with NETCONF to subscribe to steaming telemetry. This banner alerts network administrators to enable NETCONF and streaming telemetry for all fabric nodes to get data in fabric Assurance.
Configuration details	None because this banner is only a read-only banner.
Impact	None because this banner is only a read-only banner.

Route map TAG_LOCAL_EIDS update

Table 9. Banner title: Route map TAG_LOCAL_EIDS update

Value	Description
Release introduced	2.3.2.0
Full text of banner	In certain deployment topologies, a flap in the reachability between the Border Node and the Site-Local Control Plane Node or Border Nodes and the Transit Control Plane Node can create routing loops. To address this potentiality, the additive keyword is applied to an existing route-map provisioned on Border Nodes and Site-Local Control Plane Nodes. When the additive keyword is used, BGP community values are appended to existing community values rather than simply replacing them. For deployments using the SD-Access Fabric as a transit for BGP between two or more external BGP domains, this keyword may alter the existing routing policy behavior between those domains using fabric as a transit.
Summary	In a fabric site with a standalone control plane, the site border learns routes from the transit CP with a BGP community tag. The same routes are also learned from the local CP without a BGP community tag. This can create routing loops and cause traffic drops when the remote site border becomes unreachable and then reachable again.
Configuration details	route-map tag_local_eids permit 5 set community 655370 additive
Impact	This change impacts traffic.

Supplicant-based extended node feature

Table 10. Banner title: Supplicant-based extended node feature

Value	Description
Release introduced	2.3.2.0
Full text of banner	This release provides an enhancement to optionally authenticate Catalyst 9000 Series Switches operating as Policy Extended Nodes. To use this feature, the Policy Extended Nodes and their associated Edge Nodes must be upgraded to IOS XE 17.7.1 or later. The Identity Service Engine (ISE) must be upgraded to version 3.1.0 or later. This release provides further enhancements through an update to the configuration on Extended Nodes which assists in sending attributes to ISE in order to profile connected endpoints.
Summary	A more secure option is now available for supplicant-based extended node onboarding, which authenticates and authorizes the extended node through Cisco ISE.

© 2025 Cisco and/or its affiliates. All rights reserved.

Value	Description
Configuration details	Edge nodes: device-sensor filter-list dhcp list iseDHCP option name v-i-vendor-class <----------new config ! <if AP pool is provisioned in fabric> template ApAutzTemplate access-session interface-template sticky timer 60 <----updated from 10 to 60 On existing extended nodes: ip dhcp snooping <----------new config ip dhcp snooping vlan <vlan-list> <-------new config ip dhcp snooping glean <----------new config ! <interface connected to Edge Node or other Extended Nodes> ip dhcp snooping trust <----------new config device-sensor filter-list dhcp list iseDHCP option name v-i-vendor-class <----------new config ! <if AP pool is provisioned in fabric> template ApAutzTemplate access-session interface-template sticky timer 60 <-- updated from 10 to 60
Impact	No impact. New functionality.

Support for CLI 'bgp nopeerup-delay nsf-switchover 1' on SVL borders

Table 11. Banner title: Support for CLI 'bgp nopeerup-delay nsf-switchover 1' on SVL borders

Value	Description
Release introduced	2.3.2.0
Full text of banner	This release provides an update to the BGP configuration to improve convergence time during switchover of a StackWise Virtual member switch. This change applies to Border Nodes operating in StackWise Virtual that have been configured using the Layer 3 handoff automation.
Summary	When an SVL switchover occurs, convergence for south-to-north traffic takes 31 seconds. However, if you add the command " bgp nopeerup-delay nsf-switchover 1" under " router bgp <ASN>" , convergence for south-to-north traffic after a switchover is reduced to well within 250 milliseconds.
Configuration details	router bgp <bgp-as> bgp nopeerup-delay nsf-switchover 1

© 2025 Cisco and/or its affiliates. All rights reserved.

Value	Description
Impact	This banner appears when you upgrade to 2.3.2.0 on fabric with SVL configured on borders. This configuration change impacts traffic forwarding. It is recommended to execute this banner only during a maintenance window.

Anycast Gateway MAC address update

Table 12. Banner title: Anycast Gateway MAC address update

Value	Description
Release introduced	2.2.3.x
Full text of banner	In a fabric site, Edge Nodes and Border Nodes with a Layer 2 Handoff are provisioned with the same Anycast Gateways. An Anycast Gateway is instantiated on these devices as a Switched Virtual Interface (SVI). For correct operations within the fabric site, the SVI used as a Anycast Gateway must have the same IP address and MAC addresses across devices provisioned with this gateway. Catalyst Center detects that some of the Anycast Gateways for a given subnet within this fabric site have different MAC addresses. These Anycast Gateways must be updated to have the same MAC address. When this change is applied, active client sessions associated with the relevant Anycast Gateways are interrupted.
Summary	This issue was introduced in version 2.1.x due to changes in how Anycast MAC addresses are generated. The problem is triggered when a wireless flow updates a specific L2 Virtual Network (VN) segment. Generally, this impacts any Edge Nodes added to the network after the issue becomes active. To address the migration scenario, we added this banner and when you choose to apply the fix, some of the Anycast Gateways Mac addresses update. to make it consistent for all Anycast Gateways. of given IP Pool.
Configuration details	The mac address under the respective SVI will changeinterface Vlan 1023 mac address <<<
Impact	This change impacts client sessions on impacted Anycast Gateways.

Closed Authentication mode template update (IBNS_PMAP_AAA_SVR_DOWN)

Table 13. Banner title: Closed Authentication mode template update (IBNS_PMAP_AAA_SVR_DOWN)

Value	Description
Release introduced	2.2.3.x
Full text of banner	When AAA servers become unreachable, some endpoints cannot authenticate with the SD-Access fabric. When the AAA servers become reachable, the endpoints that failed authentication cannot reauthenticate. To enable reauthentication, a new authentication template must be applied to all Fabric Edge Nodes and Extended Nodes. Applying a new authentication template may reset the active client sessions
Summary	In earlier releases for closed authentication templates, we only configure it when critical VLAN is present. Add this configuration to all templates all the times.

© 2025 Cisco and/or its affiliates. All rights reserved.

Value	Description
Configuration details	10 class AAA_SVR_DOWN_UNAUTHD_HOST do-until-failure 10 activate service-template DefaultCriticalAuthVlan_SRV_TEMPLATE >>> this is now configured 20 activate service-template DefaultCriticalVoice_SRV_TEMPLATE >>> this is now configured 30 authorize 40 pause reauthentication This migration impacts all policy map Authentication template with following names: PMAP_DefaultWiredDot1xClosedAuth_1X_MAB, PMAP_DefaultWiredDot1xClosedAuth_MAB_1X PMAP_DefaultWiredDot1xLowImpactAuth_1X_MAB PMAP_DefaultWiredDot1xLowImpactAuth_MAB_1X PMAP_DefaultWiredDot1xOpenAuth_1X_MAB PMAP_DefaultWiredDot1xOpenAuth_MAB_1X
Impact	This migration workflow updates the Authentication policy maps. There can be client session resets on impacted devices.

Bridge-Network Virtual Machine feature onboarding

Table 14. Banner title: Bridge-Network Virtual Machine feature onboarding

Value	Description
Release introduced	2.2.3.x
Full text of banner	This release introduces segmentation capabilities within the Bridged-Network Virtual Machine feature. To enable these capabilities, switches that operate with the Edge Node functionality must be upgraded to IOS XE 17.8.x or later. After these changes are incorporated, you will not be able to add new switches with the Edge Node functionality that do not meet this minimum IOS XE version requirement.
Summary	Earlier releases supported only bridge-network virtual machine onboarding for wireless clients. Current releases support bridge-network virtual machine authentication, VN assignment, and SGT-based policy enforcement for microsegmentation.

© 2025 Cisco and/or its affiliates. All rights reserved.

Value	Description
Configuration details	On any existing Edge devices: if Bridge Network Virtual Machine is enabled: dynamic-eid detection multiple-addr bridged-vm regardless of if bridge vm is enabled or not: access-session bridge-mode vm-policy PMAP_DefaultBridgeModeVM_MAB policy-map type control subscriber PMAP_DefaultBridgeModeVM_MAB event session-started match-all 10 class always do-until-failure 10 authenticate using mab event authentication-failure match-first 10 class AAA_SVR_DOWN_UNAUTHD_HOST do-until-failure 10 activate service-template DefaultCriticalBridgeVM_SRV_TEMPLATE 30 authorize 20 class AAA_SVR_DOWN_AUTHD_HOST do-until-failure 10 pause reauthentication 20 authorize 60 class always do-until-failure 20 terminate mab 30 authentication-restart 60 event aaa-available match-all 10 class IN_CRITICAL_BRIDGE_MODE_VM do-until-failure 10 authenticate using mab 20 class NOT_IN_CRITICAL_BRIDGE_MODE_VM do-until-failure 10 resume reauthentication event authorization-failure match-all 10 class AUTHC_SUCCESS-AUTHZ_FAIL do-until-failure 10 authentication-restart 60

© 2025 Cisco and/or its affiliates. All rights reserved.

Value	Description
Impact	By acknowledging and accepting the banner, a customer agrees that any devices before 17.8 won't be allowed to be added to the fabric.

Layer 2 flooding access control list

Table 15. Banner title: Layer 2 flooding access control list

Value	Description
Release introduced	2.2.3.x
Full text of banner	This release provides an updated Layer 2 Flooding behavior in Cisco SD-Access for IOS XE-based switches by enabling an Access Control List (ACL) on the Layer 2 LISP sub-interfaces. This ACL is provisioned if Layer 2 Flooding is enabled, and it is applied on all devices operating with the Edge Node function and Border Nodes that have a Layer 2 Handoff. To enable this ACL support, switches operating in fabric roles must be upgraded to IOS XE 17.6.x or later. After these changes are incorporated, you will not be able to add new switches in fabric roles which do not meet this minimum IOS XE version requirement.
Summary	Starting in 2.2.3.x, we are pushing a l2lisp0 interface on devices 17.6 or older and attaching the following ACLs to it. By acknowledging and accepting the banner, you agree that any devices before 17.6 won't be allowed to be added to the fabric. **Note**: This banner would be shown for greenfield deployments as well irrespective of the version of devices on the fabric. This banner acts like a notification letting you know that devices before 17.6 won't be supported after the banner is applied.
Configuration details	ip access-list extended SDA-FABRIC-LISP 10 deny ip any host 224.0.0.22 20 deny ip any host 224.0.0.13 30 deny ip any host 224.0.0.1 40 permit ip any any interface l2lisp0.xxxx ip access-group SDA-FABRIC-LISP in ip access-group SDA-FABRIC-LISP out
Impact	By acknowledging and accepting the banner, you agree that any devices before 17.6 won't be allowed to be added to the fabric.

Message to configure on devices without NETCONF

Table 16. Banner title: Message to configure on devices without NETCONF

Value	Description
Release introduced	2.2.2.x
Full text of banner	To provision subscriptions on devices that have not been discovered with NETCONF, rediscover the devices with NETCONF, and update the Telemetry Settings with the Force Configuration Push option.

© 2025 Cisco and/or its affiliates. All rights reserved.

Value	Description
Summary	This banner alerts you that some devices assigned to sites do not have NETCONF configured, which prevents the configuration of all required streaming telemetry subscriptions. When the banner is applied, Catalyst Center enables the necessary telemetry subscriptions on these devices. These subscriptions are essential for providing assurance insights.
Configuration details	Sample configuration for a single subscription to push to the Catalyst 9500: telemetry ietf subscription 550 encoding encode-tdl filter tdl-uri /services;serviceName=smevent/sessionevent receiver-type protocol source-address <IP_address> stream native update-policy on-change receiver name DNAC_ASSURANCE_RECEIVER
Impact	This banner configures all relevant streaming telemetry subscriptions on the applicable devices. These subscriptions are necessary to provide assurance insights.

RADIUS server liveliness tester

Table 17. Banner title: RADIUS server liveliness tester

Value	Description
Release introduced	2.2.2.x
Full text of banner	To determine RADIUS server liveliness and availability to process transactions, the RADIUS automated tester sends a request periodically to the server using a test user ID. This release adds support for this automated testing feature. With this configuration, the devices send periodic test authentication messages to the RADIUS server to test for liveliness. This configuration will be applied to policy extended nodes and all devices operating with the edge node function. Applying this change updates RADIUS server configurations which may reset the active client sessions.
Summary	This banner appears when you upgrade from a release earlier than 2.2.2.x with RADIUS server provisioned on fabric devices.
Configuration details	radius server dnac-radius_2.2.2.2 address ipv4 2.2.2.2 auth-port 1812 acct-port 1813 timeout 2 retransmit 1 automate-tester username dummy ignore-acct-port probe-on pac key 7 0011100F
Impact	Applying the banner may reset active client sessions.

© 2025 Cisco and/or its affiliates. All rights reserved.

Switched virtual interface fabric DHCP update

Table 18. Banner title: Switched virtual interface fabric DHCP update

Value	Description
Release introduced	2.1.2.3
Full text of banner	Switched Virtual Interfaces (SVIs) on switches remain in a ‘down’ state if there are no associated clients on the Layer 2 ports assigned to the VLAN. For Fabric DHCP functionality to operate correctly when deploying a Fabric in a Box and/or a colocated Border Node | Edge Node, the SVI must always remain in the ‘Up’ state. This release enables this capability through the ‘no autostate’ command applied under the SVI that have been automated as part of the fabric. These changes will not create downtime or impact the network or clients.
Summary	In a FiAB + FE deployment, DHCP packets don’t reach clients located behind the FE because the SVI on the FiAB is down (because there are no clients connected to it). To resolve this, Catalyst Center configures the "no autostate" command on the FiAB/Border+Edge device, which brings up the SVI and enables it to forward DHCP packets.
Configuration details	interface Vlan1021 no autostate
Impact	No impact

Self-ping IPv6-enabled switched virtual interfaces on edge nodes

Table 19. Banner title: Self-ping IPv6-enabled switched virtual interfaces on edge nodes

Value	Description
Release introduced	2.1.2.3
Full text of banner	This release provides the ability for edge node to self-ping their IPv6-enabled Switched Virtual Interfaces (SVIs) that have been automated as part of the fabric.
Summary	The same IPv6 address is assigned to the anycast gateways on different edge nodes. Because of duplicate address detection, Catalyst Center can’t ping the anycast gateway’s IPv6 address. Applying this banner allows Catalyst Center to ping the IPv6 anycast gateway.
Configuration details	interface vlan <vlan> ipv6 nd dad attempts 0
Impact	No impact

Telemetry subscription configuration on upgrades

Table 20. Banner title: Telemetry subscription configuration on upgrades

Value	Description
Release introduced	1.3.3.x

© 2025 Cisco and/or its affiliates. All rights reserved.

Value	Description
Full text of banner	We detected IOS-XE device(s) in your network where new telemetry subscription for assurance data needs to be enabled and some of the existing subscription needs to be optimized for performance. Please note that these devices will receive a new subscription for group based policy monitoring telemetry. Do you want to take action to provision these subscriptions?
Summary	This banner prompts you to apply any missing telemetry updates to devices when new telemetry features are introduced in a Catalyst Center release. If there is a mismatch between the telemetry subscriptions on the device and those required for the current Catalyst Center release, this banner appears. After the correct telemetry is applied, the banner disappears.
Configuration details	<mdt-config-data xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-mdt-cfg" > <mdt-named-protocol-rcvrs> <mdt-named-protocol-rcvr> <name>ASSURANCE_RECEIVER</name> <host> <address> <IP_address></address> </host> <protocol>tls-native</protocol> <profile>sdn-network-infra-iwan</profile> <port>25103</port> </mdt-named-protocol-rcvr> </mdt-named-protocol-rcvrs> </mdt-config-data>
Impact	This banner updates the telemetry subscription of the devices.

Layer 2 flooding update (FLOODING_BEHAVIOR)

Table 21. Banner title: Layer 2 flooding update (FLOODING_BEHAVIOR)

Value	Description
Release introduced	1.3.3.1
Full text of banner	When Layer 2 Flooding is enabled for a given address pool, broadcast, link-local multicast, and ARP frames are flooded. This release provides an updated Layer 2 Flooding behavior in Cisco SD-Access for IOS XE-based switches to further enable support for 'silent hosts.' This is provided by flooding unknown-unicast and IPv6 Neighbor Discovery frames. To enable this updated flooding behavior, switches operating in fabric roles must be upgraded to IOS XE 16.12.2 or later. After these changes are incorporated, you will not be able to add new switches in fabric roles which do not meet this minimum IOS XE version requirement.

© 2025 Cisco and/or its affiliates. All rights reserved.

Value	Description
Summary	Catalyst Center pushes flood arp-nd and flood unknown-unicast CLI commands for Layer 2 flooding-enabled pools. For these CLIs, the IOS version should be newer than 16.12.2. If the banner has not been applied, you are able to add devices earlier than 16.12.2 to the fabric. CLIs pushed are to devices 16.12.2 and earlier. For other devices these won't be pushed. By acknowledging and accepting the banner, a customer agrees that any devices before 16.12.2 won't be allowed to be added to the fabric. **Note**: This banner would be shown for greenfield deployments as well irrespective of the version of devices on the fabric. This banner acts like a notification to let you know that devices before16.12.2 won't be supported after the banner is applied.
Configuration details	flood arp-nd" and " flood unknown-unicast clis are configured for l2 flooding enabled pools
Impact	This change impacts client sessions on impacted Anycast Gateways and the Fabric won't support switches that don't meet the IOS version criteria.

Edge node multicast stub routing (MULTICAST_PIM)

Table 22. Banner title: Edge node multicast stub routing (MULTICAST_PIM)

Value	Description
Release introduced	1.3.3.1
Full text of banner	This release provides an enhancement to the multicast configuration on Edge Nodes by enabling multicast stub routing on Switched Virtual Interfaces (SVIs) that have been automated as part of the fabric. Implementing multicast stub routing between an Edge Node and interested receivers provides efficiency by reducing the overall processing of PIM control traffic while still passing and forwarding IGMP traffic.
Summary	When upgrading from a Catalyst Center release earlier than 1.3.3.1 to a later release, this banner appears if multicast is enabled on a VN in the fabric and Layer 2 flooding is active on a subnet within the same VN. Before 1.3.3.1, Protocol Independent Multicast – Sparse Mode (PIM-SM) was used on edge nodes. After applying this banner, edge nodes are configured with PIM-Passive instead. With PIM-Passive configured on a routed interface, the interface doesn't process or forward PIM control traffic, only IGMP traffic. This reduces unnecessary PIM control processing on edge nodes, as they are directly connected to the receivers.
Configuration details	interface Vlan101 no ip pim sparse-mode ip pim passive
Impact	This configuration change impacts multicast traffic.

Classic extended nodes as 802.1x authenticator switches and critical VLAN authentication template update

Table 23. Banner title: Classic extended nodes as 802.1x authenticator switches and critical VLAN authentication template update

Value	Description
Release introduced	1.3.3.1

© 2025 Cisco and/or its affiliates. All rights reserved.

Value	Description
Full text of banner	This release provides an update to the authentication template on edge nodes for the critical VLAN. As a part of this enhancement, the SGT value 3999 which was previously provisioned is removed from the authentication templates. If the deployment currently uses SGT value 3999 for the critical VLAN, this value will need to be assigned to the critical VLAN segment during host onboarding workflows. This release provides further enhancements through an update to the configuration on classic extended nodes which provides the ability to perform as an 802.1x authenticator for connected endpoints. Once these reconfiguration processes are started, downtime will occur for wired and wireless endpoints until it is completed. Client sessions will be interrupted, and devices will need to reauthenticate with the AAA server.
Summary	In Catalyst Center 1.3.3.1, enhancements have been made to the authentication profile (IBNS) for critical VLANs and to authentication on extended nodes. If you are upgrading to this or a later release, these enhancements are not enabled by default. You must manually enable them through the banner. Catalyst Center will update the critical VLAN settings in the authentication templates for both fabric edge and extended node devices. Catalyst Center will also update the authentication configuration on extended nodes, including the relevant authentication templates. As a result, client devices will now be authenticated directly at the extended node.
Configuration details	SWITCH_INTERFACE_TEMPLATE no switchport mode trunk no access-session host-mode multi-host LAP_INTERFACE_TEMPLATE no switchport mode trunk no access-session host-mode multi-host ApAutzTemplate no switchport mode trunk no access-session host-mode multi-host service-template DefaultCriticalAuthVlan_SRV_TEMPLATE vlan <critical_vlan_id>
Impact	Due to an update in the authentication templates, network traffic is impacted. The change might reset the client sessions, and those clients must be reauthenticated on Cisco ISE.

Fabric authentication key - retry

Table 24. Banner title: Fabric authentication key - retry

Value	Description
Release introduced	1.3.1.7
Full text of banner	The fabric authentication key update did not complete successfully. This update must complete successfully before any other operations can occur in the fabric site.
Summary	If the fabric authentication key fails to update, this banner notifies you to retry the operation.

© 2025 Cisco and/or its affiliates. All rights reserved.

Value	Description
Configuration details	service ipv4 . . etr map-server <IP_address> key 7 0357020E030C2715175D41554F46595E02 <--- modified key . . exit-service-ipv4 ! service ethernet . . etr map-server <IP_address> key 7 0357020E030C2715175D41554F46595E02 <--- modified key . exit-service-ethernet !
Impact	This reconfiguration process causes downtime for wired and wireless endpoints until the process completes. After completion, reboot any AireOS-based WLC devices operating in a fabric role.

Fabric authentication key update

Table 25. Banner title: Fabric authentication key update

Value	Description
Release introduced	1.3.0
Full text of banner	When border nodes, edge nodes, and wireless LAN controllers (WLCs) register prefixes with the control plane node(s), that registration process uses an authentication key. This fabric authentication key must be updated. Once this reconfiguration process is started, downtime will occur for wired and wireless endpoints until it is completed. After the process is completed, please reboot your AireOS-based WLC device(s) if they are operating in a fabric role. Please make sure to reprovision all WLCs in this fabric at device level and fabric level individually to make sure there are no errors in WLC provisioning before attempting the banner push to avoid wireless outage.
Summary	This banner prompts you to update to the fabric authentication key. Previously, the key was set as a constant string; applying this banner ensures a unique, randomly generated key for each fabric. This banner appears during any migration from 1.2.x to 1.3.x or later.

© 2025 Cisco and/or its affiliates. All rights reserved.

Value	Description
Configuration details	service ipv4 . . etr map-server <IP_address> key 7 0357020E030C2715175D41554F46595E02 <--- modified key . . exit-service-ipv4 ! service ethernet . . etr map-server <IP_address> key 7 0357020E030C2715175D41554F46595E02 <--- modified key . exit-service-ethernet !
Impact	Wired and wireless endpoints undergo downtime during this operation.

Related resources

See Cisco Catalyst Center Documentation for additional documents relating to Catalyst Center.

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.

© 2026 Cisco Systems, Inc. All rights reserved.