Release Notes for Cisco Nexus Dashboard, Release 4.3.1

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Introduction

From insight to impact, Cisco Nexus Dashboard 4.3.1 sets the stage for the next leap delivering unified visibility, smarter automation, and seamless integration empowering networks to do more, faster, and smarter!

Cisco Nexus Dashboard 4.3.1 integrates multiple capabilities such as visibility, orchestration and automation into a single, seamless platform for data center operations. The dashboard serves as the unified management pane for modern networks, enabling seamless operations across disparate architectures such as ACI, VXLAN EVPN, Classic LAN, AI, Routed, External and Inter-fabric, Media fabrics, SAN fabrics and more. It delivers real-time analytics, deep visibility, and robust assurance for networks, empowering organizations to optimize performance, and enhance reliability.

For more information, refer to the " Related Content" section of this document.

Table 1 New and changed information

Date	Description
August 22, 2026	Release 4.3.1.175 became available.

New software features

New Infrastructure features

Table 2 New Infrastructure Features

Product Impact	Feature	Description
Ease of Use	VMware ESXi 9.0.2 deployment support	Deploy Nexus Dashboard on the latest supported VMware infrastructure with added support for VMware ESXi 9.0.2, giving teams greater flexibility to align Nexus Dashboard with current virtualization standards. For more information, refer to the *Cisco Nexus Dashboard Deployment and Upgrade Guide*.
Ease of Use	Streamlined QCOW2 deployment for KVM environments	Deploy Nexus Dashboard more consistently across KVM-based environments, including RHEL and Nutanix. QCOW2 images now include a deployment validation and orchestration script that simplifies setup, validates compatibility, and promotes consistent deployment across supported platforms. For more information, refer to the *Cisco Nexus Dashboard Deployment and Upgrade Guide*.
Ease of Use	Faster support with expanded Connected TAC	Accelerate issue resolution across LAN and SAN environments with expanded Connected TAC. The experience no longer depends on active software telemetry, can be managed centrally from System Settings > Fabric Management, and supports targeted diagnostic collection and secure, read-only command execution on Cisco N9000 switches through the Nexus Dashboard proxy.

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Product Impact	Feature	Description
		For more information, refer to the Connected TAC section in *Working with Cisco Tech Support*.
Ease of Use	Deeper LLDP diagnostics for faster connectivity troubleshooting	Troubleshoot node connectivity issues faster with rescue-user access to LLDP neighbor, interface, configuration, and statistics data through the acs lldp show command. Tech-support collections now also include LLDP neighbor information from ND node management and data interfaces, providing more complete evidence for diagnosis. For more information, refer to the System and connectivity troubleshooting section in the *Cisco Nexus Dashboard Troubleshooting* article.
Ease of Setup	Delegated device-upgrade administration	Delegate fabric software upgrades without granting broader administrative access. Nexus Dashboard 4.3.1 reintroduces the Device Upgrade Administrator role, previously available as NDFC Device Upgrade Admin, for device-upgrade workflows. For more information, refer to the Roles and permissions in the unified releases section in the *Configuring Users, Roles, and Security* article.
Ease of Use	Reliable import of same-name policies in autonomous templates	Import orchestrator related autonomous-template policies with greater confidence when identical object names exist across fabrics. Nexus Dashboard resolves relationship references only within the source fabric, preventing same-name objects in other fabrics from being used incorrectly during import. For more information, refer to the *Schemas and Application Templates for ACI Fabrics* article.
Licensing Process	ACI license-tier reporting	Gain more reliable visibility into ACI license consumption. Nexus Dashboard now reports the onboarded switch count and the license tier in use—Essentials, Advantage, or Premier—for APICs that are onboarded on the ND. For more information, refer to the Support for ACI fabrics section in the *Configuring Licensing* article.
Ease of Use	Enterprise proxy authentication with Kerberos	Integrate Nexus Dashboard with enterprise-authenticated proxy environments. Nexus Dashboard can now act as a Kerberos client, obtain tickets from the configured Key Distribution Center (KDC), and authenticate outbound HTTP and HTTPS proxy traffic. The feature title also reflects NTLM-based proxy authentication support documented for this release. For more information, refer to the Proxy configuration section in the *Working with System Settings* article.
Ease of Use	Secure AI integration through the Nexus Dashboard MCP server	Connect Nexus Dashboard securely to Cisco Cloud Control and customer-managed large language models through native Model Context Protocol (MCP) server integration. This foundation enables AI-assisted network operations and custom AI workflows while allowing

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Product Impact	Feature	Description
		organizations to keep enterprise data and AI models within their own environment. For more information, refer to the *Model Context Protocol (MCP) Server Integration* article.
Ease of Use	Flexible first-login password policy	Give super administrators greater control over user onboarding workflows by allowing them to disable the mandatory password change at first login when organizational policy or automated account provisioning requires it. For more information, refer to the Violation action section in the *Configuring Users, Roles, and Security* article.

Automation functionality

Table 3 New LAN Automation functionality

Product Impact	Feature	Description
Ease of Use	Unified visibility and troubleshooting across VXLAN-ACI fabric groups	Operate VXLAN and ACI domains as one connected environment. VXLAN–ACI fabric groups now support EPG-to-ESG migration, centralized VXLAN EVPN multi-site peering using route servers, all security-group types, Connectivity Analysis, and Traffic Analytics. Search and Explore is also available across every fabric-group type, making it easier to investigate endpoints, policies, and connectivity across domains. For more information, refer to these articles: • *Analyzing and Troubleshooting Your Network* • *Editing Fabric Settings for Fabric Groups* • *Nexus Dashboard Search and Explore* • *Understanding Fabric Groups*
Ease of Use	Faster multicast source discovery for IP Fabric for Media	Accelerate multicast source discovery in IP Fabric for Media (IPFM) environments with PIM Flooding Mechanism-Source Discovery (PFM-SD). First-hop routers can announce active sources across the fabric without relying on a Rendezvous Point, MSDP, or BSR. Support includes single-site and multi-site deployments, default and non-default VRFs, and inter-fabric boundary control. For more information, refer to the PIM flooding mechanism for source discovery and PFM-SD policies for non-default VRFs and multi-site deployments sections in *Editing IP Fabric for Media (IPFM) Fabric Settings* article.

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Product Impact	Feature	Description
Ease of Use	Support for Smart Switches in VXLAN EVPN fabrics with Hypershield integration	Simplify distributed security for top-of-rack and zone-based segmentation deployments. Nexus Dashboard can onboard the Cisco Hypershield controller to automate security-policy enforcement, zone segmentation, and traffic steering on Cisco N9324C-SE1U and N9348Y2C6D Smart Switches. For more information, refer to the *Hypershield integration* section.
Ease of Use	Flexible ACI onboarding across multi-cluster deployments	Onboard and manage ACI fabrics from any Nexus Dashboard cluster of a multi-cluster deployment. This release adds secondary-cluster onboarding and deregistration for APICs in multi-cluster environments. This release adds secondary-cluster onboarding and deregistration for APICs in multi-cluster environments. For more information, refer to these sections in the *Connecting Clusters* article: • Understanding multi-cluster connectivity in Nexus Dashboard • Connect ACI clusters • Disconnect ACI clusters • Deregister a secondary cluster from an ACI fabric
Ease of Use	Automated remote fabric backups	Protect fabric configurations with scheduled backups to remote storage. Nexus Dashboard can now use configured remote storage locations for switch running-configuration backups, helping teams centralize recovery data and capture fabric state consistently. This functionality is supported in External and Classic LAN fabrics. For more information, refer to *Backing Up and Restoring Your Nexus Dashboard*.
Ease of Use	Fabric-agent updates for monitored NX-OS fabrics	Keep Connectivity Analysis ready without moving standalone NX-OS fabrics out of monitor mode. Nexus Dashboard can update fabric-agent packages when the required telemetry, licensing, metadata, and image-management prerequisites are met. For more information, refer to the Create connectivity analysis section in the *Analyzing and Troubleshooting Your Network* article.
Ease of Setup	Zero-touch in-band deployment in Campus fabrics with Layer-2 ToR support	VXLAN EVPN Campus fabrics can now be bootstrapped with inband Plug-n-Play (PnP). In addition, bootstrap and manage Catalyst 9200-CX switches as Layer-2 top-of-rack switches in an External fabric using in-band Plug and Play. This extends zero-touch deployment to

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Product Impact	Feature	Description
		access switches connected to the Catalyst 9000 leafs of an in-band-managed Campus fabric. For more information, refer to the Inband PnP for Catalyst 9200-CX ToR switches section in the *Configuring Inband Management and Out-of-Band PnP* article.
Ease of Setup	Hardware-accelerated OpenStack networking with the Nexus Dashboard ML2 plugin	Bring cloud orchestration and fabric automation together with enhanced OpenStack ML2 integration. The new Nexus Dashboard network type enables hardware-accelerated Layer-3 forwarding; Hierarchical Port Binding dynamically allocates VLAN segments; address scopes map to VRFs for granular isolation; and the nd-status extension provides automatic deployment retry and real-time status. Additional controls enable Layer-3 forwarding for VLAN networks and border leaf switches. For more information, refer to the *Cisco OpenStack Integration Installation Guide for Nexus Dashboard*.
Ease of Use	Expanded automation and assurance for Cisco Nexus E100 platforms	Manage additional Cisco Nexus E100-based platforms running NX-OS 10.6(4) with support for VLAN mapping on trunk-interface policies and selected Nexus Dashboard Insights capabilities. For these platforms, Nexus Dashboard supports Port VLAN Translation through VLAN Mapping on trunk interface policies. Nexus Dashboard Insights supports selected capabilities for these platforms, including topology, route telemetry, interface analytics, resource analytics, and assurance-related workflows. Traffic Analytics is supported only in compact mode on E100 platforms, while Flow Telemetry and Traffic Analytics full mode are not supported. **NOTE**: Cisco Nexus E100-based platforms running Cisco NX-OS Release 10.6(3) or earlier do not support QoS in AI fabrics. If one of these platforms is added to an AI fabric, the Recalculate operation fails, and the user sees an error.
Ease of Use	Cisco N9164E-NS4-O support for AI and External fabrics	Deploy the Cisco N9164E-NS4-O running NX-OS 10.6.2(N) in AI Routed, AI VXLAN, and External fabrics. On this platform, Dynamic Load Balancing is supported in per-packet mode only.
Ease of Use	Stronger fabric security and finer protocol control	Strengthen fabric operations with SHA-512 hashing, Type 8 and Type 9 password encryption in switch-user policies, AES-128-CMAC authentication for NTP, routing-protocol keychain management, and expanded OSPF and BFD timer controls. For more information, refer to the Authentication section in the *Editing Data Center VXLAN Fabric Settings* article.

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Product Impact	Feature	Description
Ease of Use	Scalable border connectivity and routing isolation for multi-tier VXLAN	Build larger, more resilient VXLAN fabrics with enhanced border and border-gateway connectivity for three-tier topologies with super spines. New capabilities include unique ASNs on applicable border switches, per-VRF and per-VTEP loopback auto-provisioning, and automatic EVPN overlay peering policies for Data Center and AI VXLAN eBGP fabrics. For more information, refer to the Fabric Management (for fabrics with eBGP overlay routing protocol) section in the *Editing Data Center VXLAN Fabric Settings* article.
Ease of Use	Expanded design flexibility for Campus VXLAN EVPN	Design Campus VXLAN EVPN fabrics with greater routing and topology flexibility. Enhancements include 4-byte BGP ASNs, BGP fast convergence, a larger loopback ID range, custom route distinguishers for IP VRFs, SVI-based IOS XE VRF-Lite connectivity, the Border Spine role, and enhanced border connectivity for three-tier topologies with border-gateway super spines. For more information, refer to the *Editing Campus VXLAN Fabric Settings* article.
Ease of Use	Fabric-group-wide analytics, advisories, and connectivity visibility	Monitor and troubleshoot connected fabrics from a single fabric-group context. Operators can view analytics and advisories, review connectivity and fabric bugs, launch Connectivity Analysis, explore endpoints across member fabrics, and monitor the health of inter-fabric connections for every supported fabric-group type. For more information, refer to these articles: • *Analyzing and Troubleshooting Your Network* • *Detecting Anomalies in Your Nexus Dashboard* • *Identifying Advisories in Your Nexus Dashboard* • *Understanding Fabric Groups*
Ease of Setup	Image management in monitor mode	Prepare and manage software images for External and Classic LAN fabrics while they remain in monitor mode, reducing mode changes and operational friction during upgrade planning. For more information, refer to the Image management in monitor mode section in the *Managing Your Fabric Software* article.
Ease of Use	Fabric-level NetFlow automation for Nexus H1 and H2 platforms	Extend flow visibility to Nexus H1 and H2 switches with fabric-level NetFlow configuration generation from Nexus Dashboard. For more information, refer to the Configuring Netflow support section in the *Creating Fabrics and Fabric Groups* article.
Ease of Use	Co-existence with Catalyst Center Assurance	Nexus Dashboard can be employed to provision VXLAN EVPN configurations on Catalyst 9000 based Campus fabrics while the switches can stream telemetry and assurance data to Catalyst Center. Assurance related configuration policies related to NetFlow and device-

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Product Impact	Feature	Description
		tracking can be pushed to the Catalyst 9000 switches from the Catalyst Center in these environments. Nexus Dashboard provides the ability to update the assurance policy related intent so that it remains in sync with the switch running configurations. This ensures wireless Assurance related features in Catalyst Center continue to co-exist with Nexus Dashboard managing the Campus EVPN fabrics. For more information, refer to the Edit interfaces section in the *Working with Connectivity in Your Nexus Dashboard LAN Fabrics* article and the Catalyst Center Assurance interface fields section in the *Editing Campus VXLAN Fabric Settings* article.

Automation functionality

Table 4 New SAN Automation functionality

Product Impact	Feature	Description
Ease of use	Centralized CyberArk credential management for SAN	Extend enterprise credential governance to SAN operations. Nexus Dashboard can retrieve Cisco MDS fabric-discovery and device credentials from CyberArk using credential-store keys, reducing locally stored credentials and simplifying credential rotation for SAN workflows. For more information, refer to the Edit device credentials for SAN switches section in the *Creating and Editing SAN Fabrics* article and the AAA remote authentication passthrough for SAN fabrics section in the *Working with System Settings* article.

New Orchestration functionality

Table 5 New Orchestration functionality

Product Impact	Feature	Description
Ease of use	Expanded configuration-drift detection and reconciliation Configuration drift support for application templates	Protect application intent across more Orchestrator template properties. Nexus Dashboard now detects and reconciles drift for EPG and bridge-domain subnets, bridge-domain DHCP labels, EPG static ports, contract relationships, and uSeg attributes. For more information, refer to the Configuration drifts and Reconcile configuration drift in application templates sections in the *Templates Overview and Operations for ACI Fabrics* article.
	Support import and deployment of same name policies and associated policies for autonomous templates	Find the right configuration policy template faster with category-based filtering, then review the resulting intent in a consolidated show running-config-like view. Related parent and child policies are presented together, making generated configuration easier to understand and validate before deployment. For more information, refer to the Simplified policy template selection and combined configuration view section in the *Working with Configuration Policies for Your Nexus Dashboard LAN or IPFM Fabrics* article.

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

New Monitoring and Observability functionality

Table 6 New Monitoring and Observability functionality

Product Impact	Feature	Description
Ease of Use	Actionable anomaly suppression and upgrade-aware correlation	Reduce alert fatigue and speed root-cause analysis. Suppress anomalies that are not relevant to your environment, apply rules across fabrics, and create a rule directly from an anomaly. During ACI software updates, correlation can identify controller or switch update events as the root event for related anomalies. For more information, refer to the Create an anomaly rule from an anomaly, Anomaly rules, and Understanding anomaly correlation sections in the *Detecting Anomalies in Your Nexus Dashboard* article.
Ease of Use	End-to-end multicast path visibility for VXLAN fabrics	Troubleshoot multicast delivery with a complete view from the first-hop router to the last-hop router. In VXLAN EVPN data center fabrics with Tenant Routed Multicast (TRM), Nexus Dashboard visualizes multicast routes and state from Cisco N9000 switches, provides source and receiver statistics, and identifies the top multicast groups by traffic and receiver count. For more information, refer to the Multicast traffic monitoring overview section in the Working with Connectivity in Your Nexus Dashboard LAN Fabrics article.
Ease of Use	Live Protect enhancements	See security posture and protection status in one place. The new Overview tab on the Device Security page brings together security advisories, Live Protect deployment status, hit counts, and historical trends so operators can identify exposure, verify protection, and prioritize action faster. For more information refer to the Overview section in *Managing Security Advisories and Protecting Devices Using Nexus Dashboard* article.
Ease of Use	Proactive scale-compliance monitoring	Identify capacity risk before it affects operations. Nexus Dashboard raises an anomaly when fabric telemetry resources approach or exceed the verified limits for the cluster profile and provides the affected resource, current use, verified limit, utilization percentage, impact, and recommended remediation. For more information, refer to the Scale compliance anomalies section in the *Reviewing System Status for Your Nexus Dashboard* article.
Ease of Use	End-to-end AI job visibility with server NIC telemetry	Correlate AI workload performance from the GPU and server NIC through the network fabric. AI job monitoring now supports External AI fabrics and adds server-NIC metrics such as CRC errors, discards, bandwidth, NACKs, CNPs, operational state, and link speed alongside GPU and switch-interface data.

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Product Impact	Feature	Description
		For more information, refer to *Understanding enhanced analytics for AI fabrics*.
Ease of Use	sFlow support for Traffic Analytics compatibility mode	Use sFlow, in addition to Netflow, when enabling Traffic Analytics compatibility mode on supported platforms, expanding traffic visibility across heterogeneous fabrics. For more information, refer to *Traffic analytics support for Silicon One (S1) platforms*.
Ease of Use	Traffic Analytics for Cisco Silicon One platforms	Extend traffic visibility to supported Cisco Silicon One platforms. Nexus Dashboard supports NetFlow compatibility mode on Silicon One based Cisco N9000 switches running NX-OS 10.6(3) or later and sFlow on Cisco N9000 -C9804, Cisco N9000 -C9808, and G200 switches. Supported mode depends on the switch platform; Cloud Scale-only traditional fabrics continue to use Netflow compatibility mode. For more information, refer to *Traffic analytics support for Silicon One (S1) platforms*.
Ease of Use	Accurate Traffic Analytics capability reporting for ACI switches	See the Traffic Analytics mode each ACI switch supports. The Telemetry status page now distinguishes full-mode-capable hardware from switches that support compatibility mode only, helping operators set correct expectations before enablement. For more information, refer to the Telemetry section in the *Reviewing System Status for Your Nexus Dashboard* article.

New hardware features

The following is the list of new hardware supported with this release.

Table 7 New hardware features

Product Impact	Feature	Description
Hardware support	Cisco N9164E-NS4-O support	Manage the Cisco Nexus N9164E-NS4-O running NX-OS 10.6(2n) release in AI Routed, External, and Classic LAN fabrics. Support is limited to Layer-3 operations; SVI, vPC, port channels, multicast, VLAN, PACL, VACL, VXLAN, Connectivity Analysis, NetFlow, sFlow, Traffic Analytics, and Flow Telemetry are not supported on this platform.
	SONiC support for Cisco Nexus platforms	Extend Nexus Dashboard operations to Cisco N9164E-NS4-O and Cisco N93108TC-FX3 switches running SONiC. These platforms are supported in Routed, AI Routed, and External fabrics. For more information, refer to these articles: • *Creating Fabrics and Fabric Groups* • *Editing AI Data Center Routed Fabric Settings* • *Editing Routed Fabric Settings* • *Editing External Fabric Settings*

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Product Impact	Feature	Description
	Expanded Catalyst platform support with integrated image management	Extend Campus VXLAN and External fabric operations to Catalyst C9300L-24P-4G, C9300L-48P-4G, C9200CX-12P-2X2G-E switches and Cisco Secure Router 8475-G2 and 8455-G2 platforms. Support includes Software Image Management (SWIM) and all supported Catalyst switch roles.
	Cisco Nexus N9348Y12C-SE1 support across LAN fabrics	Deploy and manage the Cisco Nexus N9348Y12C-SE1 running NX-OS 10.6(4) across all Nexus Dashboard LAN fabric types. For more information, refer to these articles: • *Editing AI Data Center Routed Fabric Settings* • *Editing AI Data Center VXLAN Fabric Settings* • *Editing Campus VXLAN Fabric Settings* • *Editing Classic LAN Fabric Settings* • *Editing Data Center VXLAN Fabric Settings* • *Editing External Fabric Settings* • *Editing IP Fabric for Media (IPFM) Fabric Settings* • *Editing Routed Fabric Settings*

NOTE: Cisco Nexus 9000 Series is now the Cisco N9000 Series:

- N9200 (previously known as Nexus 9200)
- N9300 (previously known as Nexus 9300)
- N9400 (previously known as Nexus 9400)
- N9500 (previously known as Nexus 9500)
- N9800 (previously known as Nexus 9800)
- N9300 Smart Switches

End of Support for 3-Node vND Large and 5-Node vND App Small/Large Deployments

These cluster types are not supported for greenfield deployments in Nexus Dashboard release 4.3.1 but are supported when upgrading to release 4.3.1:

- 3-node virtual cluster app large (app node with 1.5TB storage)
- 5-node virtual cluster app large (app node with 1.5TB storage)
- 5-node virtual cluster small (app node with 500G storage)

These cluster types will not be supported as an upgrade option in the next release. Migration to the new cluster type 3-node virtual cluster (data nodes) or the 3-node physical cluster using the procedures provided in the *Cisco Nexus Dashboard Deployment and Upgrade Guide* is recommended.

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Guidelines and limitations

- For Nexus Dashboard feature guidelines and limitations, refer to the feature article for details.
- For more information on compatibility, refer to the Compatibility Information.

Supported upgrade paths

The platform and its individual services have now been unified into a single product. As a result, you no longer need to deploy, configure, or upgrade services individually–all management is handled collectively through the unified platform.

For further details, refer to the Supported upgrade paths for upgrading ND from 3.2.2 or Supported upgrade paths for upgrading ND from 4.1.1 sections in the *Cisco Nexus Dashboard Deployment and Upgrade Guide*.

Changes in behavior

Changes in behavior for Nexus Dashboard 4.3.1

These sections describe the categories for the changes in behavior introduced in Cisco Nexus Dashboard 4.3.1 in comparison to Nexus Dashboard 4.2.1.

System level unified changes

Table 8 Behavior Change for System level unified features

Behavior Change Category	Description
System level unified features	Changes to Backup and Restore Cluster name changed when restoring a backup • In Nexus Dashboard release 4.2.1, the cluster names were not changed to match the backup. • In Nexus Dashboard release 4.3.1, for both federated clusters and standalone clusters, when restoring a backup, the local cluster name is now changed to match the backup. The name of the cluster where you took the backup is the name that will be used when the restore occurs. For more information, refer to the *Backing Up and Restoring Your Nexus Dashboard*.
	API schema validation Beginning with Nexus Dashboard (ND) release 4.3.1, the system validates all API requests against the published API schema before backend processing. Key changes and requirements include: • Validation behavior: Requests that do not conform to the schema are now rejected. In earlier releases, the system may have accepted, ignored, or normalized non-compliant data. • Validation scope: The schema validation applies to request payloads, query parameters, path parameters, field types, required fields, supported enum values, and object structure. • Upgrade impact: If your integrations or automation workflows send incorrect data types, missing required attributes, or non-schema-compliant values, you may receive validation errors after upgrading to release 4.3.1 or later. Recommended actions: Review your API clients and automation workflows to ensure all requests match the API schema for the target Nexus Dashboard release.

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Behavior Change Category	Description
	You must use only documented fields, provide required attributes, and ensure that values use the expected type and format.
	ACI onboarding and visibility support on secondary clusters • In Nexus Dashboard 4.2.1, in a federation, only the primary cluster could onboard new APIC clusters; only then will they become available on secondary clusters for enabling features such as orchestration or telemetry. • In Nexus Dashboard 4.3.1, in a federation, secondary clusters can now onboard APICs directly without requiring explicit onboarding on the primary cluster. This provides a more streamlined multi-cluster experience for ACI fabrics.
	Freeform interface configuration is blocked when Change Control is enabled • In Nexus Dashboard 4.2.1, the Freeform interface configuration was permitted while Change Control was enabled. Rollback and preview operations provided limited status details and supported a narrower set of roles. • In Nexus Dashboard 4.3.1, interface configuration is now blocked by default when Change Control is enabled, unless an override property is configured. This release introduces stricter validation to block overlapping or restricted edits earlier in the workflow. Additionally, rollback and preview operations now provide more explicit status information and updated role-based access control.
	Changes to LAN fabric templates, validation, and PTP configuration • In Nexus Dashboard 4.2.1, LAN fabric template workflows used older field names and enum values, left some omitted settings blank, and programmed PTP source IP and interface with a narrower model. • In Nexus Dashboard 4.3.1, LAN fabric template field names and values (enums) are normalized, templates automatically apply default values to ensure no settings are left blank, and automates PTP source IP derivation. You must review your existing templates, API payloads, and PTP settings to ensure consistency, as these changes may affect generated configurations and accepted input values. Switch selection and upgrade group creation in monitor mode • In Nexus Dashboard 4.2.1, the **Fabric Software Devices** tab disabled switch selection and blocked update-group creation when a device or fabric was in monitor or migration mode. • In Nexus Dashboard 4.3.1, switches remain selectable, and update groups can be created for fabrics in monitor mode.
	Changes to device upgrade admin role permissions • In Nexus Dashboard 4.2.1, remote TACACS users with the device-upgrade-admin role were mapped to the ND fabric-admin role. Accordingly, all fabric-admin related operations such as configuration changes were available to users with that role. • In Nexus Dashboard 4.3.1, remote TACACS users with the device-upgrade-admin role will be mapped to the newly introduced ND device-upgrade role which only allows switch upgrades to be performed. No configuration changes can be done by a user with this role.
	Tenant-Based RBAC for Orchestration templates • In Nexus Dashboard 4.2.1, you could delete, tag, submit for approval, or approve templates for tenants you were not allowed to modify despite the Role Based Access Control (RBAC) and user-to-tenant association rules. • In Nexus Dashboard 4.3.1, you cannot delete, tag, submit for approval, or approve templates for tenants you are not allowed to modify, unless you have permission for that tenant.

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Behavior Change Category	Description
	Upgrade support for tenants named “default” • In Nexus Dashboard release 4.2, tenancy became a platform-wide construct. The system-created default tenant contains policies for applications that did not previously support tenancy. An existing NDO tenant named default could conflict with the system-created tenant and cause an upgrade to release 4.2 to fail. • In Nexus Dashboard release 4.3, this conflict is resolved by migrating the existing Orchestrator tenant under one of these names: orch_default, ndo_default, tenant_default, or migrated_default. The tenant name on the APIC continues to be 'default' and all policies on templates associated with the newly named default tenant, for example, orch_default will be deployed on the tenant named 'default' on the APIC.
	Analyze proxy requires TLS certificate verification • In Nexus Dashboard 4.2.1, the DCNM ACI analyze-proxy could connect without enforcing TLS certificate verification. • In Nexus Dashboard 4.3.1, the DCNM ACI analyze-proxy connection path enforces certificate verification; deployments with untrusted or misconfigured certificates must correct trust settings. Certificate management requires RBAC permissions • In Nexus Dashboard 4.2.1, some authenticated users with broader roles could upload, modify, attach, or delete certificates. • In Nexus Dashboard 4.3.1, these certificate-management actions require more specific RBAC permissions. You may need to update user roles as needed to allow authorized users to continue managing certificates.
	Upgrade validation for SMTP email server host • In Nexus Dashboard 4.2.1, upgrade validation did not block SMTP email server configurations whose smtpHost value did not follow the OpenAPI hostname schema. Such configurations could proceed and fail later with hostname validation errors after upgrade. • In Nexus Dashboard 4.3.1, upgrade is blocked if any configured SMTP email server has an empty or invalid smtpHost. The host must be a valid RFC 1123 hostname or IP address before upgrade can proceed.
	vND OVF deployment configuration • In Nexus Dashboard 4.2.1, there is only one management network field that takes both IP and subnet mask. For example: 192.168.1.100/24. • In Nexus Dashboard 4.3.1, there are two separate fields, one for “Management Network IP address” and another one for " Management Network Mask" . This allows better handling of validation overcoming the limitations of the VMware OVF template.

Automation

Table 9 Behavior Change for Automation features

Behavior Change Category	Description
Automation	Changes to Nexus Dashboard GUI Fabric-management changes for monitored fabrics • In Nexus Dashboard 4.2.1, some actions were hidden or blocked for those fabrics, new fabrics used older monitor-mode defaults, and monitored fabrics could show managed-state success statuses.

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Behavior Change Category	Description
	• In Nexus Dashboard 4.3.1, new fabrics default to monitor mode, monitored status is shown as not applicable, and switch selection or update-group creation is available for monitor-mode or migration-mode fabrics. Pre-Change Validation reports and results Pre-Change Validation (PCV) submissions and results follow more stringent input and result rules resubmitting the request. • In Nexus Dashboard 4.2.1, some PCV submissions were accepted, and results were returned under less stringent rules. • In Nexus Dashboard 4.3.1, PCV submission requirements and result handling follow more stringent rules. Validate PCV inputs and correct every reported input error before resubmitting the request. OpenShift integration follows OpenShift-specific tooling Certificate setup generated by the OpenShift integration now follows OpenShift-specific tooling. • In Nexus Dashboard 4.2.1, adding an OpenShift integration generated certificate tooling and commands through Kubernetes-oriented endpoints. • In Nexus Dashboard 4.3.1, the generated workflow uses OpenShift-specific certificate endpoints and tooling. Use the generated OpenShift-specific certificate commands and procedures when adding an OpenShift integration. Manual time zone selection required before saving User Preferences The manual-time zone control in **User Preferences** now blocks saving until a value is selected. • In Nexus Dashboard 4.2.1, manual mode allowed **Save** without a selected time zone, and clearing the selection could reopen the list. • In Nexus Dashboard 4.3.1, **Save** remains disabled until a time zone is selected, and clearing the value resets the control without reopening it. Select a manual time zone before saving User Preferences Backup in progress warning to alert users Configuration attempts made while a backup is active, now triggers a warning banner. • In Nexus Dashboard 4.2.1, the configuration workflow did not display any backup-in-progress warning when a user attempted a change. • In Nexus Dashboard 4.3.1, users attempting configuration changes during an active backup receive an explicit warning banner Settings option added to Fabrics > General A new “Settings” option has been added to the General card for fabrics to display the fabric settings in a drawer. • In Nexus Dashboard 4.2.1, Settings option is not available. • In Nexus Dashboard 4.3.1, a new Settings option is added to the **General** card for fabrics to display the fabric settings in a drawer. This is for visibility only. Fully collapsible breakdown panels for filterable tables

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Behavior Change Category	Description
	The breakdown panels across all filterable tables with charts will now be fully collapsed and not expandable. • In Nexus Dashboard 4.2.1, the breakdown panels were not collapsible. • In Nexus Dashboard 4.3.1, the breakdown panels across all filterable tables with charts are now fully collapsible and not expandable. Journey implementation for fabric groups • In Nexus Dashboard 4.2.1, fabric group journey page is not available in the Nexus Dashboard UI. • In Nexus Dashboard 4.3.1, journey page is added to fabric group making it easier to follow the fabric group configuration process. Default credential error popup • In Nexus Dashboard 4.2.1, no warnings are displayed during login for users without default credentials. • In Nexus Dashboard 4.3.1, a warning is now displayed during login for users without default credentials, regardless of their tenant domain. This restores legacy behavior consistent with previous DCNM and NDFC releases. This validation check is bypassed for vND-app small when orchestration is enabled (Orchestrator-only) and all SAN fabric configurations.
	Nexus Data Broker (NDB) Support for Redirect_all option in Connection creation page • In Nexus Dashboard 4.2.1, there is no option to program redirect_all command in ACE programming. • In Nexus Dashboard 4.3.1, Redirect_all checkbox option is introduced in Connection creation page. By default this option is disabled. New CDP permit rules introduced on the Input and ISL ports • In Nexus Dashboard 4.2.1, there were no CDP permit rules programmed. • In Nexus Dashboard 4.3.1, CDP permit ACE rules will be programmed on the ISL ports and Input port by default. Change in PTP feature • In Nexus Dashboard 4.2.1, NDB controller programs the PTP feature, Source IP address, and the Interface configuration. • In Nexus Dashboard 4.3.1, NDB Controller programs PTP feature, Source IP address based on the device connection either External Grandmaster or Peer neighbor. Also provides the option to configure the domain. Support for LAN fabric as Production device in the NDB fabric • In Nexus Dashboard 4.2.1, only ACI fabric could be onboarded into data broker fabric. • In Nexus Dashboard 4.3.1, LAN fabrics (Classic Lan, Enhanced Classic Lan, VXLAN, Campus VXLAN, VXLANibgp) are supported and it can be onboarded into data broker fabric. In the Data Broker Fabric Overview page, the “Controller” tab is now renamed to “Production Fabrics.” These fabrics can be used to create SPAN destinations and sessions.

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Behavior Change Category	Description
	Legacy controller APIs no longer support CRUD operations on tenant-associated VXLAN fabrics and fabric groups • In Nexus Dashboard 4.2.1, legacy controller (NDFC) APIs should not be used to access (CRUD) VXLAN fabrics and fabric groups that have tenants associated with them. Use newly published open APIs for any access to tenant-associated fabrics. • In Nexus Dashboard 4.3.1, legacy controller (NDFC) APIs cannot access or perform CRUD operations on VXLAN fabrics and fabric groups that have tenants associated with them. Use newly published open APIs for any access to tenant-associated fabrics.
	Freeform Interface Configuration with Change Control The behavior for adding interface configurations to freeform policies when Change Control is enabled has changed. • In Nexus Dashboard 4.2.1, interface configurations could not be added to switch, fabric, or bootstrap freeform policies when Change Control was enabled. • In Nexus Dashboard 4.3.1, a new flag Allow interface configuration in freeform policies when Change Control is enabled is available under Admin > System Settings > Fabric Management > Advanced Setting > LAN-Fabric which can be enabled to allow the interface configurations in the freeform policies. This flag is disabled by default. The setting is available only when the Display advanced settings and options for TAC support option is enabled.
	Layer 4 (L4) to Layer 7 (L7) Route peerings after upgrade L4 to L7 route peering is reorganized during an upgrade when a static route has multiple next hops. • In Nexus Dashboard 4.2.1, the next hops could be represented together. • In Nexus Dashboard 4.3.1, after upgrading to Nexus Dashboard 4.3.1, a separate route-peering configuration is created for each next hop, and its tooltip identifies that next hop. Verify the generated route peerings after upgrade.
	Layer 4 (L4) to Layer 7 (L7) services for default-tenant resources L4-L7 services can now be configured for default-tenant resources in a tenancy-enabled fabric. • In Nexus Dashboard 4.2.1, L4-L7 services were unavailable for tenancy-enabled fabrics. • In Nexus Dashboard 4.3.1, the workflow is allowed when the resources belong to the default tenant and the account has all-tenant-domain access. Use default-tenant resources and an account with all-tenant-domain access.
	Switch status after Push Policy • In Nexus Dashboard 4.2.1, the switch configuration sync status could be incorrectly set to the success or failure result of a Push Policy deployment, even though that result did not represent the switch's complete configuration state. • In Nexus Dashboard 4.3.1, the existing configuration sync status is preserved after a Push Policy operation. The policy deployment result does not overwrite the sync status because the switch may already have other pending configuration changes. To evaluate the complete configuration and refresh the sync status: Run **Configuration Preview** or **Resync** after pushing the policy. The Push Policy functionality itself has not changed; only the handling of the configuration sync status has been corrected.
	AI Monitored is available as a fabric type • In Nexus Dashboard 4.2.1, AI monitored was not available as a fabric type.

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Behavior Change Category	Description
	• In Nexus Dashboard 4.3.1, AI monitored is available as a fabric type. No migration action is required.
	Border Gateway (BGW) loopback100 description • In Nexus Dashboard 4.2.1, the BGW loopback 100 descriptions were not available in greenfield deployments. • In Nexus Dashboard 4.3.1, the description is added automatically to the Border Gateway Loopback100 interface in greenfield deployments.
	ACI and NX-OS (Nexus One) Fabric Group Address, subnet, gateway, and switch-IP formats changed across fabric and network APIs Fabric subnet, gateway, SVI, and switch-IP fields use revised address formats. • In Nexus Dashboard 4.2.1, affected fields used IPv4-only, CIDR-only, or cidrv4 and cidrv6 formats. ◦ Subnet and gateway IP import accepted /32 and /128 Ips and later on these values were rejected during deploy. ◦ Only two types of port mode are supported, trunk and trunk native. ◦ Tenant name is not used to accurately identify networks. • In Nexus Dashboard 4.3.1, fields use ipv4WithSubnet, ipv6WithSubnet, or broader IP formats and can accept or return IPv6 values where only IPv4 was previously supported. Update validators and parsers for the affected fabric subnet, gateway, SVI, and switch-IP fields. ◦ Subnet and gateway IP import will not accept /32 and /128 Ips and these values are now flagged in a compatibility report. ◦ In addition to trunk and trunk native, a new port mode, “access” is added. ◦ Tenant name is used to accurately identify networks. Security-group and contract APIs enforce dependency checks and revised request and response rules. • In Nexus Dashboard 4.2.1, some security-group and contract operations proceeded without the newer dependency checks and used older delete-response fields or TCP flag constraints. • In Nexus Dashboard 4.3.1, affected APIs apply dependency checks, change delete-response fields, and revise TCP flag and status behavior. Update security-group and contract API calls to process dependency failures, revised delete fields, and the new TCP flag behavior. ACI attachment workflows now preserve and expose port mode explicitly The ACI attachment create, edit, and deploy workflows preserve port mode explicitly. • In Nexus Dashboard 4.2.1, affected attachments effectively assumed trunk mode and did not consistently preserve native or access intent. • In Nexus Dashboard 4.3.1, attachment mode is exposed explicitly, and trunk, trunk-native, and access behavior is preserved end to end. Validate the attachment mode during create and edit operations instead of relying on implicit trunk behavior. It changes stored/default MAX_PATHS from 1 to 64 and fixes upgrade/meta-device cases. normal effective config often remains 64/32, but erroneous maximum-paths 1 and pending diffs are removed. It does not affect links ACI-ISN links.

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Behavior Change Category	Description
	External fabric selection and host-port resync changes External-fabric attachment and host port resync now filters switch roles and recovers altered vPC state differently. • In Nexus Dashboard 4.2.1, spine switches could appear in multi-attach selection, and Host Port Resync could fail after out-of-band removal of vPC configuration. • In Nexus Dashboard 4.3.1, spine switches are filtered from selection and resync can automatically unpair affected vPC peers and render them as standalone switches.
	External service IP validation and IPv6 pool defaults are changed Management-pool reachability validation and IPv6 resource-pool sequencing now use stricter defaults. • In Nexus Dashboard 4.2.1, IP validation used five pings with a three-second timeout per address, and IPv6 auto-allocation could start at .0. • In Nexus Dashboard 4.3.1, validation uses two pings with a one-second timeout plus SIM reachability checks, and IPv6 auto-allocation starts at .1. Replace IPv6 pool assumptions that start at .0 and select addresses that pass the shorter ping and SIM reachability checks.
	SNMP validation and default behavior changes SNMP community and user-template workflows enforce stricter validation and revised privacy defaults. • In Nexus Dashboard 4.2.1, some community strings and template fields were validated loosely and authNoPriv could assign a concrete Privacy Protocol default. • In Nexus Dashboard 4.3.1, invalid community and template values are rejected earlier and authNoPriv no longer assigns that Privacy Protocol default. Correct invalid SNMP inputs and stop relying on an implicit Privacy Protocol value for authNoPriv.

Telemetry

Table 10 Behavior Change for Telemetry features

Behavior Change Category	Description
Telemetry	Change in Default Fabric Setting Parameter: AI QoS & Queueing – RoCEv2 • In Nexus Dashboard 4.2.1, the RoCEv2 DSCP default value: 26 • In Nexus Dashboard 4.3.1, RoCEv2 DSCP default value: 24-31 This change does not impact the upgrade scenarios. If Nexus Dashboard is upgraded from a previous release and a QoS policy is already configured, Nexus Dashboard 4.3 will preserve the existing RoCEv2 DSCP value.
	Traffic Analytics compatibility mode now requires NTP Traffic Analytics compatibility mode time synchronization prerequisite is changed • In Nexus Dashboard 4.2.1, Enabling PTP was required for Traffic Analytics Compatibility mode. • In Nexus Dashboard 4.3.1, NTP must be configured, and PTP is no longer needed. Configure and verify NTP before enabling Traffic Analytics compatibility mode.

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Behavior Change Category	Description
	Changes to Connected TAC • In Nexus Dashboard 4.2.1, you cannot disable Connected TAC (faststart) flows. Used admin user and Telemetry cluster was needed and claimed to Intersight. • In Nexus Dashboard 4.3.1, you can disable Connected TAC (faststart) flows in the Nexus Dashboard UI, you can set a Nexus Dashboard user (corresponding device credentials used to collect showtech), and (NXOS) controller cluster additionally needs to be connected and claimed in Intersight for Co-location deployments.
	Connected TAC actions now enforce enablement, permissions, and stricter command checks Connected TAC, callhome, and proxy actions enforce enablement, busy-state, role, command, and credential checks. • In Nexus Dashboard 4.2.1, these workflows were more flexible, broader role access, and less strict validation. • In Nexus Dashboard 4.3.1, disabled or busy requests can be rejected, Connected TAC endpoints require super-admin role, and commands and credentials are validated more strictly. Use a 'super-admin' account, enable Connected TAC, clear active operations, and correct command or credential failures before retrying the actions.
	Removed or deprecated System anomalies System anomaly and telemetry platform coverage is reduced. • In Nexus Dashboard 4.2.1, the affected system anomalies were generated, and C9200CX was supported for telemetry collection • In Nexus Dashboard 4.3.1, the affected system anomalies are removed or deprecated, and telemetry support for C9200CX is removed. We recommend removing monitoring dependencies on the retired anomalies and C9200CX telemetry data.
	Traffic Analytics compatibility skips unsupported switches Unsupported switches no longer make Traffic Analytics compatibility enablement appear failed. • In Nexus Dashboard 4.2.1, an unsupported switch could be represented as an enablement failure. • In Nexus Dashboard 4.3.1, unsupported switches are skipped instead of being marked as "failed" during compatibility enablement.
	Changes to Bug scan and Log collection on switches impacted by disruptive NX-OS or ACI bugs • In Nexus Dashboard 4.2.1, no warnings were provided when running on-demand Log collection or Bug scan jobs on impacted switches, and scheduled Bug scans were executed automatically. • In Nexus Dashboard 4.3.1, Scheduled Bug scan jobs are automatically skipped for affected switches. Before initiating an on-demand Bug scan or Log collection jobs for these switches, the system displays a warning and requires explicit user acknowledgement. Switches skipped during scheduled Bug scans are displayed with a "Skipped" status on the **System Status > Telemetry** page. **NOTE**: Nexus Dashboard can identify potential switches that could have disruption due to collection of show tech. This identification does not require running a show tech on those devices.

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Behavior Change Category	Description
	Unsupported hardware combinations are now blocked earlier in existing workflows PTP and device-admission workflows block unsupported hardware and image combinations earlier. • In Nexus Dashboard 4.2.1, some unsupported switch models or images could proceed through PTP enablement or device admission. • In Nexus Dashboard 4.3.1, the C9200CX campus additions and unsupported PTP model or version combinations are rejected with clearer validation guidance. Remove C9200CX from affected campus additions and upgrade unsupported switch images before enabling PTP or admitting the device.
	Legacy Classic LAN fabrics are excluded from policy-cam workflow Policy-cam eligibility now excludes Legacy Classic LAN fabrics from both manual and scheduled resync. • In Nexus Dashboard 4.2.1, fabrics could appear in policy-cam selections even though the workflow was not applicable to them. • In Nexus Dashboard 4.3.1, legacy Classic LAN fabrics are excluded from selection and periodic policy-cam resync is not attempted. Remove Legacy Classic LAN fabrics from policy-cam resync and scheduled-sync procedures.
	In AI fabrics, fleet collection script blocks collection if required services are not running • In Nexus Dashboard 4.2.1, If any of the required services (DCGM Exporter, NVIDIA DOCA Telemetry Service (DTS), or Fluent Bit) is not running, the script will not block the collection. • In Nexus Dashboard 4.3.1, If any of the required services (DCGM Exporter, NVIDIA DOCA Telemetry Service (DTS), or Fluent Bit) is not running, the script blocks the collection. Before you run the GPU/NIC Topology Fleet Collector script, verify that the following services are running on the target GPU servers: ◦ Data Center GPU Manager (DCGM) Exporter ◦ NVIDIA Data Center Infrastructure on a Chip Architecture (DOCA) Telemetry Service (DTS) ◦ Fluent Bit
	External anomaly events use correct acronym casing Acronyms in anomaly events exported to external syslog and Kafka now retain correct capitalization. • In Nexus Dashboard 4.2.1, acronym text was forced to lowercase before exporting to external syslog and Kafka destinations. • In Nexus Dashboard 4.3.1, acronym text is no longer converted to lowercase, preserving the correct acronym casing in exported events. Update case-sensitive syslog and Kafka parsers to accept the corrected acronym capitalization.

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Behavior Change Category	Description
	Topology import and views follow stricter fabric RBAC and updated link handling Topology import and topology views enforce fabric RBAC and return BGP-focused link data. • In Nexus Dashboard 4.2.1, imports could proceed without fabric-scoped authorization for every referenced fabric and topology results could include LLDP-based links. • In Nexus Dashboard 4.3.1, uploaded content is checked for fabric-level authorization before import and LLDP links are filtered from affected topology views. Use an account authorized for every referenced fabric and update topology consumers that depend on LLDP links in those views.
	EPL snapshot summary count interval changes for endpoints, VRFs, and networks • In Nexus Dashboard 4.1 and 4.2.1, EPL snapshot summary counts for endpoints, VRFs, and networks on virtual clusters were updated every hour. • In Nexus Dashboard 4.3.1, these counts are updated every six hours, and snapshot comparisons have six-hour granularity. For more information, refer to the Analyzing and Troubleshooting Your Network article.

Orchestration

Table 11 Behavior Change for Orchestration features

	Description
Orchestration	Tenant creation rejects empty descriptions The tenant-create request now rejects an explicitly empty description. • In Nexus Dashboard 4.2.1, a tenant could be created with an empty description field. • In Nexus Dashboard 4.3.1, an explicitly empty description is rejected, while an omitted description remains valid. Omit the tenant **description** field or provide a non-empty value in every create request.
	Tenant uplift handles tenants named default differently Uplifting tenant named “default” now assigns separate local and global names. • In Nexus Dashboard 4.2.1, tenants named “default” were not uplifted from 3.2.2. • In Nexus Dashboard 4.3.1, “default” is retained as the local name and a global tenant name is assigned during uplift. Update post-uplift procedures and automation to use the assigned global name while preserving the “default” as the local name.
	Fabric-policy template responses no longer expose sensitive keys to users Observer-visible fabric-policy template GET payloads now exclude NTP, MCP, and MACsec authentication keys. • In Nexus Dashboard 4.2.1, observer-role responses could include those authentication keys.

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

	Description
	• In Nexus Dashboard 4.3.1, users can no longer view the values of the NTP, MCP, and MACsec authentication keys in the response.
	Scale limits are enforced and scale limit anomalies are now reported Scale checks now cover policy objects, subnets, EPGs, and IP L3Outs. • In Nexus Dashboard 4.2.1, the supported scale numbers were not enforced. • In Nexus Dashboard 4.3.1, Nexus Dashboard reports limit violations at 500 policy objects per tenant, fabric, or monitoring template, 8000 subnets, 6000 EPGs, and 100 IP L3Outs per template. Reduce or redistribute policy objects, subnets, EPGs, and IP L3Outs that exceed the supported limits.
	Different-site migration now requires source-template deployment first Target deployment in a different-site migration now depends on prior source-template deployment. • In Nexus Dashboard 4.2.1, deployment order between the source and target templates was not enforced. • In Nexus Dashboard 4.3.1, deploying the target template first returns a validation error directing the user to deploy the source template. Deploy the source template before the target template in every different-site migration.
	Config drift detection now includes child policies Configuration-drift monitoring now includes children of Nexus Dashboard owned parent policies. • In Nexus Dashboard 4.2.1, direct APIC changes to existing child policies or newly created child policies were not detected as Config Drift when the parent was Nexus Dashboard-owned. • In Nexus Dashboard 4.3.1, direct APIC changes to existing child policies or newly created child policies are detected as Config Drift and are available for review and reconciliation.

Resolved issues

To see additional information about the caveats, click the bug ID to access the Bug Search Tool (BST). The “Fixed In” column of the table lists the specific patches in which the issue exists.

To search for a bug ID within Cisco’s product documentation, enter in the address bar of a web browser: <*bug_number*> site:cisco.com

For example: **CSCwo61222 site:cisco.com**

Table 12 Resolved issues for Nexus Dashboard

Bug ID	Description	Fixed in	Affected Functionality
CSCwt93725	When creating a Configuration Compliance rule using a Template, the preview may fail when attempting the " View Selected Objects" function.	4.3.1.175 and later	Monitoring/Observability

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Bug ID	Description	Fixed in	Affected Functionality
CSCws51848	In Nexus Dashboard GUI for ACI Fabric Inventory, navigating to **Fabric Summary > Connectivity > Interfaces > Sub-Interface Interfaces Details > Trends and Statistics > Errors > Errors Details** and clicking on **Error Details** shows no data on the GUI even though errors are present on the main Interface details page.	4.3.1.175 and later	Automation
CSCwu07730	In a Nexus Dashboard VXLAN-ACI Fabric Group deployment, traffic bridged across fabrics via Border Gateways (BGW) may encounter incorrect Security Group Tag (SGT) assignment. This issue occurs specifically when traffic traverses an NX-OS BGW that has the L2VNI-associated SVI in a shutdown state. In this configuration, the source SGT is incorrectly tagged as " 0," leading to inconsistent policy enforcement across the stretched network.	4.3.1.175 and later	Automation
CSCwv16926	In a co-located Nexus Dashboard deployment, when Live Protect is enabled, Live Protect shield policy updates cannot be applied to the affected switches, and the Monitor mode option does not appear in Nexus Dashboard. As a result, policy changes do not take effect, and monitoring cannot be configured or verified from the Nexus Dashboard UI. This issue does not occur in a co-hosted deployment.	4.3.1.175 and later	Monitoring/Observability
CSCwt08695	Slack integration configuration is missing after restoring the Nexus Dashboard (ND) cluster setup.	4.3.1.175 and later	General
CSCwt22977	Incorrect Endpoint Security Group (ESG) names are displayed on the Fabric Telemetry (FT) and Telemetry Analytics (TA) tables for ACI fabrics. This issue occurs when an ACI fabric with ESGs configured is onboarded to Nexus Dashboard (ND) and telemetry is enabled, the following sequence causes issues: • The user disables telemetry and then reconfigures Endpoint Groups (EPGs), ESGs, and Layer 3 Outs (L3OUTs). • After re-provisioning, the user enables telemetry again.	4.3.1.175 and later	Monitoring/Observability
CSCwt11065	When a user creates a protocol definition in Nexus Dashboard (ND) and pushes it to ACI with some DSCP value, ND pushes the value of DSCP property as “unspecified” by default. This issue requires changes to the model and database so that ND does not push unspecified value for DSCP property.	4.3.1.175 and later	General
CSCwt17198	Tenant deployment appears to progress sequentially across NX1, NX2, and ACI fabrics in the Nexus Dashboard UI. Status bars for each fabric move to completion one after another, rather than concurrently. Users may perceive deployments as taking longer due to the sequential visual feedback, despite backend deployments happening in parallel.	4.3.1.175 and later	Automation
CSCwt33814	Update groups with names longer than 128 characters are permitted when using the attach groups API to support backward compatibility during Nexus Dashboard upgrades. However, a validation is added on the UI to restrict update group names to a maximum of 128 characters during creation or edit.	4.3.1.175 and later	Automation

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Bug ID	Description	Fixed in	Affected Functionality
CSCwt52799	When attempting to perform Software Upgrade Analysis on an ACI fabric, the corresponding fabric shows a lock symbol. Please refer to Bug Search Tool details for workaround.	4.3.1.175 and later	Fabric Software Upgrades
CSCwt49667	Special characters are not allowed for security group names. In version 4.2, the system fails to process security group names that include any of the following special characters: !@#$^=+{}. This results in a failure during the update process and displays an error within the user interface.	4.3.1.175 and later	Automation
CSCwq78591	When Traffic Analytics Interface Filter Flow Rules are configured and a backup and restore is attempted, the interface filters are visible in the UI in the fabrics Telemetry settings, but the filter configuration is not pushed to devices after Nexus Dashboard configuration restore.	4.3.1.175 and later	Monitoring/Observability
CSCwt34011	A Kafka consumer can enter a stuck state during a rare Kafka rebalance event. When this occurs, on-demand/triggered Bug Scan requests are not processed, and subsequent requests are blocked. This results in a functional outage of on-demand/triggered workflows until manual recovery is performed.	4.3.1.175 and later	General
CSCwt40431	GPU memory utilization anomaly is showing wrong value for memory usage.	4.3.1.175 and later	General
CSCwt41931	Endpoint table displays internal fabric network links as EP (within the fabric) after restoring/reconfiguring a backup on the cluster or after Telemetry pause/resume.	4.3.1.175 and later	Monitoring/Observability
CSCwt42224	When you perform a clean reboot using “acs reboot clean” on a single node cluster, the node may fail to come back as active, causing the cluster to be broken.	4.3.1.175 and later	General
CSCwt42921	After upgrading from Nexus Dashboard 3.2 to 4.2 the endpoints vCenter enrichment information is not displayed in the Endpoints table.	4.3.1.175 and later	General
CSCwt43518	When VLAN is configured out-of-band on the device with sub-commands, then the VLAN is not included in the VLAN range CLI in diff view and pending config side-by-side view. It only shows the block for vlan line with sub-cmds but not the list of vlan cli even though it shows up in device show run	4.3.1.175 and later	Automation
CSCwt46057	After upgrading from v3.2x to v4.1 or v4.2, in a Multi Cluster Fabric Group (MCFG) with auto-created multisite underlay links, managed member fabrics on secondary clusters may appear as pending configurations related to BGP Max Paths on the border gateways. This occurs when the underlay links were not manually updated to use a non-default max path value prior to the upgrade.	4.3.1.175 and later	Automation
CSCwt52763	Switch Config-sync status displays as "Pending" even if the Tenant deploy was successful and there is no pending intent to be deployed.	4.3.1.175 and later	Automation
CSCwt46809	A network is detached from a host interface and the uplink access port-channel on a ToR switch after the ToR switch is added into a VxLAN fabric using brownfield import.	4.3.1.175 and later	Automation

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Bug ID	Description	Fixed in	Affected Functionality
CSCwt49616	If a multi-cluster fabric group had security groups enabled and security groups with network port selectors in ND 4.1 then once primary cluster is upgraded to ND 4.2, the network port selectors will be missing in ND 4.2. Also, the associated contract count for default security groups will not be populated.	4.3.1.175 and later	Automation
CSCwt51427	Following an upgrade from ND 3.2 or 4.1 to 4.2, associating a Security Group (SG) with a VM via Connectivity > Virtual Infrastructure may cause existing VM-derived selectors in other SGs within the same VRF to be negated during subsequent deployments.	4.3.1.175 and later	Automation
CSCws08868	BGP down anomaly is not generated when underlying VPC is made down.	4.3.1.175 and later	Automation
CSCws90654	Launching Splunk UI with native Splunk on a Nexus Dashboard cluster without IPv4 stack and using IPv6 only for Management and Data network addresses does not work.	4.3.1.175 and later	General
CSCwt07507	When telemetry is enabled from Nexus Dashboard, sensor path to query nxsecure policy remains present, even if the nxsecure feature is disabled on the switch.	4.3.1.175 and later	Monitoring/Observability
CSCws35228	A Search & Explorer query such as " Can security-group ESG1 talk to ESG2" may indicate that the two ESGs can communicate because they are part of the same preferred group, even if there is actually a direct deny contract between them that is blocking the traffic.	4.3.1.175 and later	Monitoring/Observability
CSCws98701	Tenant policy import from an ACI fabric into a VXLAN-ACI fabric group fails with network creation error.	4.3.1.175 and later	Automation
CSCwt25921	Loopback interface IP addresses are not streamed in telemetry data for Cisco IOS-XE Catalyst devices. As a result, these IPs are not displayed on the Nexus Dashboard.	4.3.1.175 and later	Monitoring/Observability
CSCwt25919	OSPF Router ID is not displayed on Nexus Dashboard for Cisco IOS-XE Catalyst devices.	4.3.1.175 and later	Automation
CSCwt04861	Import fails with the error message " Tenant <ND_TenantName> not found on fabric" when Nexus Dashboard tenant names do not match the corresponding ACI tenant names.	4.3.1.175 and later	Automation
CSCwt11065	When a user creates a protocol definition in Nexus Dashboard (ND) and pushes it to ACI with some DSCP value, ND pushes the value of DSCP property as "unspecified" by default. This issue requires changes to the model and database so that ND does not push unspecified value for DSCP property.	4.3.1.175 and later	General
CSCwt14341	Deployments to ACI sites using the VXLAN-ACI fabric-group are not displayed in the deployment history. Only audit-logs of the deployments are available, but no deployment history is displayed for the ACI deployments.	4.3.1.175 and later	Automation

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Bug ID	Description	Fixed in	Affected Functionality
CSCwt17198	Tenant deployment appears to progress sequentially across NX1, NX2, and ACI fabrics in the Nexus Dashboard UI. Status bars for each fabric move to completion one after another, rather than concurrently. Users may perceive deployments as taking longer due to the sequential visual feedback, despite backend deployments happening in parallel.	4.3.1.175 and later	Automation
CSCws26984	For objects in VXLAN-ACI, the "Config Sync" feature is unavailable for ACI fabrics in Release 4.2, and the status updates are not periodic. ACI objects transition from N/A (at creation) to PENDING (when attached or detached). To clear the PENDING state and return the status to N/A, a "deploy" action must be performed.	4.3.1.175 and later	Automation
CSCwt33814	Update groups with names longer than 128 characters are permitted when using the attach groups API to support backward compatibility during Nexus Dashboard upgrades. However, a validation is added on the UI to restrict update group names to a maximum of 128 characters during creation or edit.	4.3.1.175 and later	Automation
CSCwt52799	When attempting to perform Software Upgrade Analysis on an ACI fabric, the corresponding fabric shows a lock symbol. Please refer to Bug Search Tool details for workaround.	4.3.1.175 and later	Fabric Software Upgrades
CSCwt49667	Special characters are not allowed for security group names. In version 4.2, the system fails to process security group names that include any of the following special characters: !@#$^=+{}. This results in a failure during the update process and displays an error within the user interface.	4.3.1.175 and later	Automation

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Bug ID	Description	Fixed in	Affected Functionality
CSCwt29261	In a multi-cluster environment, if any member cluster is still running version 4.1, certain 4.2 features that are not backward-compatible will be unavailable for the Multi-Cluster Fabric Group (MCFG). The following limitations apply when clusters with mixed versions (4.2 and 4.1) are present: • Layer 2 Network with VRF – Not supported. An error message will be displayed in both the UI and the API response. • Fabric Group Backup and Restore – Not supported. An error message will be displayed in both the UI and the API response. • Security Policy Updates – Modifications to certain properties of Security Groups, Contracts, Associations, and Protocols will not be permitted. • MCFG Config Preview: Add/Remove Config Count – The Add/Remove Config Count will not be available for switches on 4.1 clusters, in both the UI and the API response. • MCFG Audit Records – Accessing MCFG Audit Records from the 4.1 All Clusters View is not supported. • MCFG Security Association creation is not supported if srcSecurityGroup or dstSecurityGroup is default UNWARE group, for example, SG_DEFAULT~GPO_UNAWARE, SG_DEFAULT~MyVRF_50001 • MCFG Security Association attach/detach in Edit flow is not supported. The attach/detach is available in the Actions Attach/Detach. • MCFG Add Fabric Group Member of 4.1.1g fabric is not supported if user has already created securityGroup/securityContract/securityAssociation/securityProtocol via swagger with description on MCFG. Network Attachments Performance -Network attachment query and update might exhibit some performance degradation	4.3.1.175 and later	Automation
CSCwr95624	After disassociating an ACI fabric from a tenant, the tenant is not deleted from the remote APIC.	4.3.1.175 and later	General
CSCwq78591	When Traffic Analytics Interface Filter Flow Rules are configured and a backup and restore is attempted, the interface filters are visible in the UI in the fabrics Telemetry settings, but the filter configuration is not pushed to devices after Nexus Dashboard configuration restore.	4.3.1.175 and later	Monitoring/Observability
CSCwt34011	A Kafka consumer can enter a stuck state during a rare Kafka rebalance event. When this occurs, on-demand/triggered Bug Scan requests are not processed, and subsequent requests are blocked. This results in a functional outage of on-demand/triggered workflows until manual recovery is performed.	4.3.1.175 and later	General
CSCwt40431	GPU memory utilization anomaly is showing wrong value for memory usage.	4.3.1.175 and later	General
CSCwt41931	Endpoint table displays internal fabric network links as EP (within the fabric) after restoring/reconfiguring a backup on the cluster or after Telemetry pause/resume.	4.3.1.175 and later	Monitoring/Observability
CSCwt42224	When you perform a clean reboot using “acs reboot clean” on a single node cluster, the node may fail to come back as active, causing the cluster to be broken.	4.3.1.175 and later	General
CSCwt42921	After upgrading from Nexus Dashboard 3.2 to 4.2 the endpoints vCenter enrichment information is not displayed in the Endpoints table.	4.3.1.175 and later	General

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Bug ID	Description	Fixed in	Affected Functionality
CSCwt43518	When VLAN is configured out-of-band on the device with sub-commands, then the VLAN is not included in the VLAN range CLI in diff view and pending config side-by-side view. It only shows the block for vlan line with sub-cmds but not the list of vlan cli even though it shows up in device show run	4.3.1.175 and later	Automation
CSCwt45228	Re-import of policies from an ACI fabric into an VXLAN-ACI fabric group results in a duplicate interface attachment error in cases where Bridge Domains with the same name are being re-imported in both the user tenant and common tenant.	4.3.1.175 and later	Automation
CSCwt46057	After upgrading from v3.2x to v4.1 or v4.2, in a Multi Cluster Fabric Group (MCFG) with auto-created multisite underlay links, managed member fabrics on secondary clusters may appear as pending configurations related to BGP Max Paths on the border gateways. This occurs when the underlay links were not manually updated to use a non-default max path value prior to the upgrade.	4.3.1.175 and later	Automation
CSCwt46630	For Colo Fabrics only, VM name and hypervisor redirection do not work from Endpoints table. • On NDFC Cluster, clicking the VM name or hypervisor link in the endpoint table for endpoints learned via vCenter integration fails with a 400 error. • On NDI Cluster, clicking the hypervisor link in the endpoint table fails with a 400 error when vCenter integration is not configured on the local cluster. Clicking the VM name in the Endpoint table redirects to a "No Data" page when the vCenter integration is configured on a remote cluster.	4.3.1.175 and later	Monitoring/Observability
CSCwt52763	Switch Config-sync status displays as "Pending" even if the Tenant deploy was successful and there is no pending intent to be deployed.	4.3.1.175 and later	Automation
CSCwt46809	A network is detached from a host interface and the uplink access port-channel on a ToR switch after the ToR switch is added into a VxLAN fabric using brownfield import.	4.3.1.175 and later	Automation
CSCwt49616	If a multi-cluster fabric group had security groups enabled and security groups with network port selectors in ND 4.1 then once primary cluster is upgraded to ND 4.2, the network port selectors will be missing in ND 4.2. Also, the associated contract count for default security groups will not be populated.	4.3.1.175 and later	Automation
CSCwt51427	Following an upgrade from ND 3.2 or 4.1 to 4.2, associating a Security Group (SG) with a VM via Connectivity > Virtual Infrastructure may cause existing VM-derived selectors in other SGs within the same VRF to be negated during subsequent deployments.	4.3.1.175 and later	Automation

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Bug ID	Description	Fixed in	Affected Functionality
CSCwt53079	Custom network template Issues with reference to L2 network creation and Fabric/Fabric Group addition. • In Multi-Cluster Fabric Group (MCFG), when a L2 network is created using a user-defined network template, the API response returns "layer" : "layer3" instead of "layer" : "layer2". • When attempting to add a fabric or fabric group that contains networks of type user defined to an MCFG , the add operation fails and the incoming fabric is rejected.	4.3.1.175 and later	Automation
CSCwt46375	Network creation fails with an error when initiated from the L4-L7 Services workflow. This occurs because the workflow is unable to resolve the target fabric group when its name does not match the parent Multi-Cluster fabric group name.	4.3.1.175 and later	Automation

Open issues

To see additional information about the caveats, click the bug ID to access the Bug Search Tool (BST). The “Exists In” column of the table lists the specific patches in which the issue exists.

To search for a bug ID within Cisco’s product documentation, enter in the address bar of a web browser: <*bug_number*> site:cisco.com

For example: **CSCwo61222 site:cisco.com**

Table 13 Open issues for Nexus Dashboard

Bug ID	Description	Exists in	Affected Functionality
CSCwt47732	When a restore is attempted from a NAS where configured storage quota threshold is exceeded, the Nexus Dashboard restore will be aborted before starting any actual restore.	4.3.1.175 and later	Automation
CSCwv82709	A Catalyst 9000 (Cat9k) switch becomes unreachable when it is provisioned as a Top-of-Rack (TOR) switch during bootstrap in an external fabric with an incorrect password (base64 format).	4.3.1.175 and later	Automation
CSCwv89975	When the number of displayed rows on the **Anomalies** page is increased from the default (10) to 100, the selection of the rows on the page degrades and it can lag up to 5 seconds. The lag is specifically observed on the Windows Virtual Desktop Infrastructure (VDI) environment.	4.3.1.175 and later	Monitoring/Observability
CSCww00810	After restoring a Nexus Dashboard (co-host or co-located) from a backup, the Live Protect Shield status displays inconsistently across Nexus Dashboard fabrics.	4.3.1.175 and later	General
CSCww05274	After an NX-OS upgrade and subsequent downgrade, the Live Protect shield status displayed in Nexus Dashboard does not match the actual shield mode on the switch. The shield policy is correctly restored on the switch in **Monitor** mode, but Nexus Dashboard incorrectly displays the advisory/shield status as “Active/Available”.	4.3.1.175 and later	Fabric Software Upgrades

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Bug ID	Description	Exists in	Affected Functionality
CSCwv75308	When the switch timezone is changed from a non-UTC timezone to UTC while its clock is recovering from a drift greater than 60 seconds, the switch may fail to send the required timezone-change notification. As a result, Nexus Dashboard Insights (NDI) retains the previous clock-offset state and continues to report the PTP clock as “OUT OF SYNC”, even though the switch has returned to synchronization.	4.3.1.175 and later	Monitoring/Observability
CSCww05954	After upgrading from Nexus Dashboard 3.2 to 4.3.1, existing fabrics may not automatically receive the configuration event required to create PolicyCAM schedules. This issue can occur when upgrading from a release without NX-OS PolicyCAM feature to a release with that feature, particularly when the Assurance Analysis settings are enabled before the upgrade.	4.3.1.175 and later	Fabric Software Upgrades
CSCwv73261	After upgrading a SONiC FX3 switch in a Routed fabric from Nexus Dashboard, the upgraded switches run into an “SSH Key Mismatch” error in the **Manage > Inventory > Discovery Status** column.	4.3.1.175 and later	Fabric Software Upgrades
CSCwv33170	Users with the fabric-admin role and security domain scoped to a specific fabric cannot see the alert rule configurations.	4.3.1.175 and later	Automation
CSCwv25969	Adding switches fails when multiple sessions to add switches are initiated in parallel across different fabrics. If REST API is used to add switches, it incorrectly returns HTTP 200 (Success) even when the switch addition operation fails.	4.3.1.175 and later	Automation
CSCwv81908	On Nexus Dashboard, saving an interface configuration fails with a generic request validation error when a valid IP address contains a leading or trailing whitespace. The interface is not created or updated, and the error message does not identify which field caused the failure.	4.3.1.175 and later	Automation
CSCww01224	Upgrade to 4.3.1 fails if Telemetry enabled cluster is expanded to add worker nodes after bootstrapping.	4.3.1.175 and later	Fabric Software Upgrades
CSCww14559	In VXLAN-ACI fabric groups, route-servers must source the overlay EVPN sessions from Loopback0, no other loopback IDs are supported in this release.	4.3.1.175 and later	Automation

Known issues

To see additional information about the caveats, click the bug ID to access the Bug Search Tool (BST). The “Exists In” column of the table lists the specific patches in which the issue exists.

To search for a bug ID within Cisco’s product documentation, enter in the address bar of a web browser: <*bug_number*> site:cisco.com

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

For example: **CSCwo61222 site:cisco.com**

Table 14 Known issues for Nexus Dashboard

Bug ID	Description	Exists in	Affected Functionality
CSCwv20271	In a brownfield fabric, Nexus Dashboard does not allow you to choose devices to deploy security advisories, even when Live Protect or NX-Secure is already enabled on the switches. This issue occurs when you configure Live Protect, NX-Secure, or the required shields directly on the switches before you onboard the fabric to Nexus Dashboard. Nexus Dashboard does not automatically discover or adopt the existing Live Protect configurations. To deploy security advisories, enable Live Protect or NX-Secure and deploy the required shields through Nexus Dashboard.	4.3.1.175 and later	Automation
CSCwv67802	Max Paths and Max BGP Paths appear as Pending Config after upgrade from 3.2.2m to Nexus Dashboard 4.3.1.	4.3.1.175 and later	Automation
CSCwv47593	25G links between FX3-SONiC and NX-OS devices fail to establish when using default Forward Error Correction (FEC) settings due to incompatibility. The issue occurs because the default FEC modes on SONiC and NX-OS do not match.	4.3.1.175 and later	Automation
CSCwv93995	After upgrading from Nexus Dashboard release 3.2.2m with custom templates in L4-L7 services configuration, any edit operations to the service function may result in an error, "An unexpected error occurred during template execution"	4.3.1.175 and later	Fabric Software Upgrades
CSCwv05468	During Nexus Dashboard upgrade validation, the upgrade may fail in the Validation state with an error similar to: "SMTP email server(s) missing a valid hostname: <server-name>. Please update the configuration before proceeding with the upgrade." This issue occurs when upgrading to Nexus Dashboard 4.3.1 and an SMTP email server is configured with an empty or invalid SMTP host value,	4.3.1.175 and later	Fabric Software Upgrades

Compatibility information

For Nexus Dashboard cluster sizing guidelines, refer to the Nexus Dashboard Capacity Planning tool.

Physical Nexus Dashboard nodes support these servers:

- Cisco UCS-220-M5 (SE-NODE-G2),
- Cisco UCS-225-M6 (ND-NODE-L4), and
- Cisco UCS-C225-M8 (ND-NODE-G5S and ND-NODE-G5L)

Physical Nexus Dashboard nodes must be running a supported version of UCS server firmware (which includes CIMC, BIOS, RAID controller, and disk and NIC adapter firmware).

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Table 15 Supported UCS server firmware

Product ID	Supported Releases
Cisco UCS-220-M5 (SE-NODE-G2)	• 4.2(3b) • 4.2(3e) • 4.3(2.230207) • 4.3(2.250037) • 4.3(2.250045) • 4.3(2.260007) • 4.3(2.260020)
Cisco UCS-225-M6 (ND-NODE-L4)	• 4.3(4.240152) • 4.3(4.242066) • 4.3(5.250001) • 4.3(5.250030) • 4.3(6.250040) • 4.3(6.250053) • 4.3(6.260017) • 4.3(6.260054)
Cisco UCS-C225-M8 (ND-NODE-G5S)	• 6.0(1.250127) • 6.0(1.250131) • 6.0(2.260143)
Cisco UCS-C225-M8 (ND-NODE-G5L)	• 6.0(1.250127) • 6.0(1.250131) • 6.0(2.260143)

Note:

- The 4.3(2.240009) and 4.3(2.240077) releases are no longer listed as supported releases on the Cisco UCS-220-M5 (SE-NODE-G2) and are not recommended due to the issues related to CSCwn56294.
- Though other firmware versions than those listed above may be supported on standard UCS C220/C225 servers, they are not supported on Nexus Dashboard appliances and could lead to issues.
- For more information on supported UCS server firmware, refer to:
  - Firmware Files for 4.3(2)
  - Firmware Files for 4.3(6)
  - Firmware Files for 6.0(2)

VMware vMotion is not supported for Nexus Dashboard virtual nodes deployed in VMware ESX.

Nexus Dashboard can be claimed in Intersight US regions ('us-east-1') or EU regions ('eu-central-1').

Browser compatibility

The Cisco Nexus Dashboard UI is intended to be compatible with the most recent desktop version of most common browsers, including Chrome, Firefox, Edge, and Safari. In most cases, compatibility will extend one version behind their most recent release.

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

While not designed for compatibility with mobile devices, most mobile browsers are still able to render the majority of Nexus Dashboard UI. However, using the above-listed browsers on a desktop or laptop is recommended. Mobile browsers aren't officially supported by Cisco Nexus Dashboard.

Verified scalability limits

For verified scalability limits, refer to the *Cisco Nexus Dashboard Verified Scalability Guide, Release 4.3.1*, which is available in the documentation is directly available on the CCO portal.

Related content

For release 4.3.1, all documentation content is provided directly in the product's GUI and accessible via the Help Center link.

To search and view all of the ND 4.3.1 user content, go to this URL:
https://www.cisco.com/c/en/us/td/docs/dcn/nd/4x/collections/nd-user-content-431.html

Documentation feedback

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

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.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

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: https://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)

Printed in USA Cxx-xxxxxx-xx 01/20

Cisco Confidential