Release Notes for Cisco Nexus Dashboard, Release 4.2.1

Introduction

From insight to impact, Cisco Nexus Dashboard 4.2.1 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 4.2.1 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, see the " Related Content" section of this document.

Table 1 New and changed information

Date	Description
March 12, 2026	Release 4.2.1.10 became available.

New software features

New Infrastructure features

Table 2 New Infrastructure Features

Product Impact	Feature	Description
Ease of use	vND (Virtual Appliance) Support on Nutanix	Beginning with this release, you can now deploy virtual Nexus Dashboard (vNDs) on Nutanix Hyperconverged Infrastructure (HCI). For more information, see the “Deploying vNDs in Nutanix” section in the *Cisco Nexus Dashboard Deployment Guide*
	vND (Virtual Appliance) Support on AWS for ACI	Beginning with release 4.2.1, Nexus Dashboard adds support for deploying virtual Nexus Dashboard on AWS for managing ACI fabrics for Orchestration and Telemetry. Telemetry for ACI fabrics is supported for out-of-band (OOB) only with Traffic Analytics. For more information, see the “Deploying a Virtual Nexus Dashboard (vND) in Amazon Web Services (AWS)” section in the *Cisco Nexus Dashboard Deployment Guide.*
	Open API support for unified Nexus Dashboard	This release adds complete support for Open APIs across all features of the unified Nexus Dashboard. For more information, see *Nexus Dashboard Unified APIs*.
	Microsoft Entra ID (MFA) Integration	Beginning in this release, user authentication using Microsoft Azure multi-factor authentication (Entra ID) domain is now supported. For more information, see the “Microsoft Entra ID multi-factor authentication (MFA)” section in the *Configuring Users, Roles, and Security* article.

	Slackbot Integration	Beginning with release 4.2.1, Nexus Dashboard adds support for Slack integration. You can now send alerts and notifications directly to your specified Slack channels. To ensure secure and efficient communication between Nexus Dashboard and your Slack workspace, configure your Slack application credentials and set up channel authorizations within Nexus Dashboard. For more information, see the “Slack integration” section in the *Working with Integrations in Your Nexus Dashboard* article.
	Resolve Streaming Anomalies on Switches	Beginning with Nexus Dashboard 4.2.1, Nexus Dashboard introduces the capability to detect and resolve streaming telemetry anomalies on both Cisco ACI and standalone NX-OS switches. For more information, see the “Resolve streaming anomalies on switches” section in the *Detecting Anomalies and Identifying Advisories in Your Nexus Dashboard* article.
	Backup and Restore with Operational Data and NFS Support	Previously, when performing a **Backup and Restore** of Nexus Dashboard, telemetry operational data was not included. Starting in this release, you can perform a ‘Full’ backup and restore, where telemetry operational data is backed up and restored, along with telemetry configuration data. For more information, see the “Backing up and restoring telemetry operational data” section in the *Backing Up and Restoring your Nexus Dashboard* article.
	UI Dark Mode Support	With this release, Nexus Dashboard provides additional options to toggle the UI display to **Classic dark** and **Midnight dark** color themes for easier viewing in low-light environments such as Network Operations Centers (NOCs). For more information, see “Customize color themes” section in the *Exploring Your Nexus Dashboard* article.
	UI Table Enhancements	Continuing the effort started with ND 4.1, this release will complete the migration of remaining table to the standardized look and function. This will provide consistent functionality including sorting, data download, and user adjustments.
	System Software Notifications	Nexus Dashboard now provides automated alerts to notify you when a new recommended software version is available. For more information, see the “System update notifications” section in the in *Exploring Your Nexus Dashboard* article.
	Native Splunk Support	Beginning with 4.2.1, Splunk is now an embedded application within the Nexus Dashboard Analysis Hub, providing you with robust capabilities to build personalized dashboards, generate insightful reports, and configure critical alerts. For more information, see the “Integrating Splunk for advanced monitoring and compliance” section in the *Analyzing and Troubleshooting Your Network* article.
	SNMP Export Support for System Anomalies	System Anomalies can now be exported to an external SNMP trap receiver. For more information, see the “SNMP” section in the *Working with System Settings* article.
	Anomaly Streaming via Webhooks	Starting with Nexus Dashboard Release 4.2.1, Nexus Dashboard supports streaming event data to external webhook servers, in addition to existing options such as **Syslog**, **SNMP**, and **Splunk**.

		The **Webhook** export feature enables network operations to seamlessly integrate Nexus Dashboard anomaly data to remote Webhook endpoints. This allows for centralized anomaly collection, simplifies monitoring, and helps meet compliance policies. For more information, see the "Webhooks" section in the *Working with System Settings* article.
	Software Maintenance Updates (SMU) Support for Nexus Dashboard Platform	Beginning in this release, you can now apply SMU (Software Maintenance Upgrade) released images on top of your Nexus Dashboard software. For more information, see the "Applying SMU packages on your Nexus Dashboard" section in the *Managing Your System Software* article.
	Upgrade Process Enhancements	With this release, the following enhancements are added to the software upgrade process: • Retry Failed Software Installation or Upgrade: You can now retry a failed software installation or upgrade. If a failure occurs during system software installation, upgrade, or during the Cluster bring up stage as part of the Journey process, a window will appear describing the issue. This window now includes a **Retry** option, allowing you to repeat the software installation or upgrade process. For more information, see the "Retry software installation" section in the *Managing Your System Software* article. • View Update History for Cluster Software - The update history for your cluster software is now accessible. You can view a record of past updates for your cluster directly from the interface. For more information, see the "View update history" section in the *Managing Your System Software* article.
	Customizable UI Login Banner	With this release, a 'super-admin' user can modify the text that appears in the lower left corner on the login page in the Nexus Dashboard. For more information, see the "Login banner" section in the *Configuring Users, Roles, and Security* article.
	Enhanced Password Security Features	With this release, when a new user is created, they will be prompted to reset their password at first login. The password management security features are also enhanced, allowing you to make modifications to ensure stronger password security for your Nexus Dashboard passwords. For more information, see the "Violation action" section in the *Configuring Users, Roles, and Security* article.
	Platform Security and Hardening Enhancements	Beginning with Nexus Dashboard 4.2.1, security enhancements have been added for Nexus Dashboard. For more information, see the "Webserver security configuration", "SSH configuration", and "*Platform security and hardening enhancements"* sections in the *Configuring Users, Roles, and Security* article.
	Certificate Signing Request (CSR) Enhancements	Starting with Nexus Dashboard 4.2.1, you can create a Certificate Signing Request (CSR) for a System or Fabric certificate role. For more information, see the "Certificate signing request (CSR)" section in the *Managing Certificates* article.

	Certificate Expiry Alert Notifications	With this release, you can view certificate expiry date anomalies in Nexus Dashboard. The **CA certificates** page displays the **Expires on** date for certificates. For certificates that are due to expire in 90 days or less, the system generates an alarm notification or anomaly every 24 hours. For more information, see the “Viewing certificate expiry date anomalies” section in the *Managing Certificates* article.

New LAN Automation functionality

Table 3 New LAN Automation functionality

Product Impact	Feature	Description
Ease of use	Multi-Tenancy Support	Beginning with this release, you can now use tenants and tenant domains in Nexus Dashboard to unify the configuration of networking policies that are applied to fabrics, regardless of whether that fabric is an NX-OS or an ACI fabric. For more information, see the *Configuring Tenants and Tenant Domains* article.
	Fabric Designer Support	With this release, Nexus Dashboard introduces the Fabric Designer feature, enabling you to virtually plan and design your network fabric before you purchase or deploy any physical equipment. For more information, see the *Working with Fabric Designer in Nexus Dashboard* article.
	Brownfield ToR Support	Beginning with Nexus Dashboard 4.2.1, you can use this feature to seamlessly integrate existing Top-of-Rack (ToR) switches into the existing leaf-tor functional fabrics, providing centralized management and preserving current configurations, thereby simplifying operations and enhancing network control. For more information, see the “Brownfield Top-of-Rack (ToR) Integration” in *Editing Data Center VXLAN Fabric Settings* article.
	AI Fabric Default Settings Enhancements	Beginning with Nexus Dashboard 4.2.1, enhanced AI fabric settings simplify network setup and optimize performance for AI VXLAN EVPN - iBGP/AI VXLAN EVPN - eBGP and AI Routed fabrics. These settings include updated default routing protocols and centralized configuration for advanced QoS and Dynamic Load Balancing (DLB). For more information, see the “AI fabric management” section in *Editing AI Data Center VXLAN Fabric Settings* article.
	Nexus Data Broker Integration	Beginning in this release, Nexus Dashboard will support a new fabric type for Data broker networks. This will allow users to manage SPAN configurations for Data broker switches from Nexus Dashboard. For more information, see the *Understanding NDB Fabrics and Switches*, *Editing NDB Fabric Settings* and *Working with Connectivity in your Nexus Dashboard NDB Fabrics* articles.
	Config Profile to CLI Conversion	With this release, Nexus Dashboard introduces the ability to migrate overlay mode from config-profile to CLI, even with active attachments, provided all switches run the same NX-OS version and are in sync. If the NX-OS image is 10.5(x), the feature is supported on 10.5(5) or later. If the NX-OS image is 10.6(x), the feature is supported on 10.6(2) or later. For more information, see the “Overlay mode” section in the *Editing AI Data Center VXLAN Fabric Settings* article.

	Automatic Reconciliation of Local Operation Switch Changes (Reconcile Switch Config with ND)	Beginning with this release, Nexus Dashboard supports the detection and reconciliation of operational (local) configuration changes made directly on managed Nexus switches. This enhancement enables automatic identification of configuration drift, detailed diff review, and user-driven reconciliation actions, ensuring the dashboard remains the single source of truth. For more information, see the “Reconciliation of local operational switch changes” in *Configuration Compliance* article.
	LLDP Handshake to Enable Adaptive Routing with NVIDIA NICS	With this release, Nexus Dashboard enables Adaptive Routing for NVIDIA SmartNICs by automating the LLDP handshake and 'hardware profile spectrum-x' command. This optimizes packet reordering and enhances performance for AI/ML workloads. For more information, see the “LLDP handshake to enable Adaptive Routing with NVIDIA” section in the *Working with Integrations in Your Nexus Dashboard* article.
	Advanced DLB Feature Support on Silicon One (S1) Platforms	Beginning with Nexus Dashboard 4.2.1, you can apply Dynamic Load Balancing (DLB) configuration at fabric level using the **Apply Fabric Level Setting** option. Nexus Dashboard now supports Dynamic_Load_Balancing_S1 policy templates for Silicon One (S1) switches, in addition to the Dynamic_Load_Balancing_CS policy template for the CloudScale platform. For more information, see the “Add a Dynamic Load Balancing (DLB) policy template” section in the *Working with Configuration Policies for Your Nexus Dashboard LAN or IPFM Fabrics* article.
	Fabric Software Image Management Workflow Enhancements	Beginning with Nexus Dashboard 4.2.1, the workflow to update switch software as well as running both basic and custom update checks has been enhanced. The Fabric Software workflow significantly simplifies managing the software lifecycle for multiple switches by leveraging update groups, role-based grouping and comprehensive validation, and reporting features. For more information, see the “Upgrade or downgrade switches in a fabric under Overview tab” section in the see *Managing Your Fabric Software* article.
	Inband Plug and Play (PnP) Support for Catalyst switches (9200/9300/9500)	Beginning with Nexus Dashboard release 4.2.1, inband PnP in Campus VXLAN EVPN fabrics streamlines zero-touch deployment for Cisco Catalyst 9000 Series switches, automating onboarding and integrating critical network infrastructure configurations for seamless operation. For more information, see the “Inband PnP in Campus VXLAN EVPN fabrics” in *Configuring Inband Management and Out-of-Band PnP* article.
	Granular Flow Priority Enablement	With this release, the granular priority-based flow feature provides multiple levels of priorities to the IPFM flow and allows you to prioritize the critical flows. You can choose additional priorities to match switch priorities. For more information, see the “Create a flow policy” section in *Working with Connectivity in Your Nexus Dashboard IPFM Fabrics* article.
	Increased Max Rate for PMN Policers for IPFM Fabrics	With Nexus Dashboard 4.2.1, IPFM fabrics allow a bandwidth up to 100 Gbps to support 8k and 16k video resolutions. For more information, see the “Create a flow policy” section in the *Working with Connectivity in Your Nexus Dashboard LAN Fabrics*

		article.
	Image Management Support for Cisco Catalyst 8000 Switches (Cat8k)	Beginning with Nexus Dashboard 4.2.1, Nexus Dashboard supports software upgrade for Cisco Catalyst 8000 switches. For more information, see the "Understand the information provided in the Fabric Software page for NX-OS and IOS-XE fabrics" section in the *Managing Your Fabric Software* article.
	Live Protect Support for NX-OS	Beginning with this release, you can protect your network from active threats by deploying compensating-control policies directly to switches, without requiring a maintenance window or immediate software upgrade. For more information, see the *Managing Security Advisories and Protecting Devices Using Nexus Dashboard* article.
	ACI interoperability with VXLAN Border Gateway	Beginning with Nexus Dashboard 4.2.1, introduces the Nexus One architecture, which is an architectural framework rather than a standalone product. Nexus Dashboard unifies the management and operations of Application Centric Infrastructure (ACI) and Cisco NX-OS fabrics to provide control, policy enforcement, and operational workflows across domains. For more information, see the "Understanding Nexus One" section in the *Creating Fabrics and Fabric Groups* article.
	Nexus One – Importing Tenant Policies Ability to import tenant policies from ACI fabrics	Beginning with this release, you can now import tenant policies from ACI fabrics, which provides the ability to migrate endpoint groups (EPGs) on APIC to endpoint security groups (ESGs) using the ESG Migration Assistant script, and import those ESGs, as well as VRFs, BDs, and so on, into Nexus Dashboard. For more information, see *Importing Tenant Policies from ACI Fabrics* article.
	Increase in Scale Support for VXLAN and IPFM Fabrics	With this release, scale support for mixed fabrics has been qualified for this release to support 50 IPFM fabric switches and 50 VXLAN switches. For more information, see the "Controller scale limits" section in the *Cisco Nexus Dashboard Verified Scalability Guide, Release 4.2.1* document.
	Increase in Scale Limits to Accommodate Larger Fabrics, Higher Telemetry Ingests, and Support for All Services Within a Cluster	With this release, Nexus Dashboard supports increased scale limits to accommodate larger fabrics, higher telemetry ingests, and support for all services within a cluster. For more information, see the "Telemetry scale limits" and "Orchestration scale limits" sections in the *Cisco Nexus Dashboard Verified Scalability Guide, Release 4.2.1* document.

New SAN Automation functionality

Table 4 New SAN Automation functionality

Product Impact	Feature	Description
Ease of use	Exclude Switches from Discovery (Discovery Mute)	With this release, Nexus Dashboard provides administrators greater control and flexibility when managing SAN fabric discovery by excluding certain devices from discovery. Nexus Dashboard automatically discovers and maps connected devices, hosts, and fabrics to ensure comprehensive visibility. However, in some environments, there may be devices that administrators wish to exclude from this process, which will now be possible.

		For more information, see the “Exclude from discovery” section in the *Working with Inventory in Your Nexus Dashboard SAN Fabrics* article
	Support for Manual IP Addresses Assignment to NPV Switches	With this release, Nexus Dashboard provides an option to manually assign IP addresses to NPV switches in the SAN fabric inventory. Unlike traditional Fibre Channel switches, NPV switches do not participate in the full control plane. Manual IP assignment helps when NPV switches are not automatically discovered. For more information, see the “Assign discovery IP address” section in the *Working with Inventory in Your Nexus Dashboard SAN Fabrics* article.

New Monitoring and Observability functionality

Table 5 New Monitoring and Observability functionality

Product Impact	Feature	Description
Ease of use	Traffic Analytics Support for L2 and Transit Conversations	Beginning with 4.2.1, Traffic analytics full mode will support tracking L2 and transit L3 conversations (L3out to L3out). Transit L3 conversations include flows where neither the client nor the service endpoint resides within the managed fabric. For more information, see the “Traffic analytics transit conversations” section in the *Analyzing and Troubleshooting Your Network* article.
	Connectivity analysis for L4-L7 Service Devices and Cisco Silicon One switches	Beginning with 4.2.1, connectivity analysis supports path visualization for traffic through Layer 4 to Layer 7 (L4-L7) service nodes (such as firewalls) in VXLAN EVPN fabrics. The feature uses Cisco Silicon One Packet Tracer for inspection at network processing unit (NPU) and external network boundaries. Enable telemetry for end-to-end visualization. For more information, see the “Connectivity Analysis support for Layer 4 to Layer 7 services” section in the *Analyzing and Troubleshooting Your Network* article.
	AI Fabric Visibility Enhancements	Enhanced analytics is available for workloads in AI routed and VXLAN fabrics within Nexus Dashboard. This enhancement provides end-to-end visibility and actionable insights for AI infrastructures by integrating job completion and GPU statistics with network statistics, providing a detailed overview of network topologies along with GPUs. For more information, see the “Understanding enhanced analytics for AI fabrics” section in the *Editing AI Data Center VXLAN Fabric Settings* and *Editing AI Data Center Routed Fabric Settings* articles.
	ESG and GPO Visibility Enhancements	Beginning with Nexus Dashboard 4.2.1, Search and Explore supports 'Can' queries for security groups, including Group Policy Objects (GPOs) in NX-OS and Endpoint Security Groups (ESGs) in ACI. For more information, see the “Supported query types” section in the *Nexus Dashboard Search and Explore* article.
	Bug Scan Active Classification and Metadata Support	With this release, Nexus Dashboard Bug scan feature is enhanced to classify bugs as Active (in addition to Known) based on device software version, running configurations, and log or service analysis. The enhanced Bug scan functionality provides Active bugs only after you download the complete metadata package, which includes comprehensive bug data, signatures, Field Notices, PSIRT information, and Known bug details. For more information, see the “Enhancements to Bug scan” section in

		the *Analyzing and Troubleshooting Your Network* article.
	AI Topology Enhancements for GPU Servers	Beginning with release 4.2.1, Nexus Dashboard introduces enhanced discovery capabilities to provide visibility into AI workloads. This feature extends traditional network device discovery in Nexus Dashboard to include detailed host-level information, offering a foundational understanding of your AI infrastructure, from network fabric to individual GPU servers. For more information, see the “AI endpoint and topology discovery” in the *Editing AI Data Center VXLAN Fabric Settings* article.
	Basic Telemetry for Catalyst Devices	Beginning with Nexus Dashboard 4.2.1, basic telemetry data is now collected from Cisco Catalyst 9000 series devices. This data includes inventory, hardware statistics, essential-level anomalies, including correlation, L3 neighbors, and traffic analytics compatibility mode. For more information, see the “Telemetry” section in the *Editing Campus VXLAN Fabric Settings*, and the “Telemetry”, “Enable telemetry on Cisco Cat9k switch”, and “Support for Traffic Analytics” sections in the *Reviewing System Status for Your Nexus Dashboard* articles.
	Real Time Telemetry Support for ACI	Beginning in this release, Nexus Dashboard will now be able to “subscribe” to real-time event updates for ACI telemetry. This will include expedited statistical updates for Interfaces, Small Form-factor Pluggable / Digital Optical Monitoring (SFP/DOM), Link Aggregation Control Protocol (LACP), Environmental metrics, Capacity, and Quality of Service Monitoring (QOSM). ACI will also stream routing table updates as part of this enhancement. This feature requires ACI version 6.2(1) or later. For more information, see the “Real-time telemetry and UI enhancements for ACI fabrics” section in the *Working with Connectivity in Your Nexus Dashboard ACI Fabrics* article.
	Search and Explore Support for Security Groups	Beginning with Nexus Dashboard 4.2.1, Search and Explore supports 'Can' queries for security groups, including Security Groups (SGs) in NX-OS and Endpoint Security Groups (ESGs) in ACI. For more information, see the “Supported query types” section in the *Nexus Dashboard Search and Explore* article.
	ACI Microsegmentation (uSeg) Support with PBR and Assurance	Starting with Nexus Dashboard 4.2.1, Search and Explore 'Can' queries are supported for microsegmentation endpoint groups (uSeg EPG), including those in PBR deployments. This feature provides visibility for uSeg EPGs in analytics features such as traffic analytics, connectivity analysis, Policy CAM, compliance, and delta analysis. You can identify misconfigurations, such as missing classifications or static leaf configurations, and view enriched flow records and endpoint details. For more information, see the “Microsegmentation endpoint groups (uSeg EPG) and PBR assurance” section in the *Analyzing and Troubleshooting Your Network* article.
	ACI Route Telemetry Streaming	Beginning with Nexus Dashboard 4.2.1, Nexus Dashboard introduces ACI route telemetry streaming. This feature provides near real-time and historical visibility into unicast routing tables within ACI fabrics through Nexus Dashboard. For more information, see the “ACI route telemetry streaming” section in *Working with Inventory in Your Nexus Dashboard ACI Fabrics* article.
	Anomaly Rules Enhancements	Beginning with Nexus Dashboard 4.2.1, Nexus Dashboard supports

		rules to override the default severity of anomalies, enhanced match criteria to include only anomaly-relevant criteria, and system anomalies for use with anomaly rules. For more information, see the “Analyze anomalies” and “Anomaly rules” sections in the *Detecting Anomalies and Identifying Advisories in Your Nexus Dashboard* article.
	In-band Telemetry Support for Enhanced Classic LAN (ECL) Fabrics	Starting with Nexus Dashboard 4.2.1, Nexus Dashboard added support for In-band telemetry for Enhanced Classic LAN fabrics. For more information, see the *Editing Classic LAN Fabric Settings* article.

New hardware support

Table 6 New hardware support

Product Impact	Feature	Description
Hardware support	Support for Nexus platforms and Linecards	This release of the Nexus Dashboard expands support for the following Nexus hardware. These devices are supported on both ACI and NX-OS operating systems. For any specific limitations on the hardware, see the Guidelines and limitations section. • Nexus 9396Y12C-SE1 platform • Nexus 9396T12C-SE1 platform • Nexus N9K-C9800-SUP-B supervisor
	Support for M8-based Large Appliance	Beginning with Nexus Dashboard 4.2.1, support has been introduced for the ND-NODE-G5L large-size appliance powered by Cisco UCS M8 technology, available in 3-node cluster deployments for higher density scale and performance. For more information, see: • *Cisco Nexus Dashboard Deployment and Upgrade Guide* • *Cisco Nexus Dashboard Verified Scalability Guide*

New hardware features

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

New Switch Hardware support

- Nexus 9348Y2C6D-SE1
- Nexus 9396Y12C-SE1
- Nexus 9396T12C-SE1
- Nexus N9K-C9800-SUP-B supervisor
- Catalyst 8500-12x
- Catalyst C8300-1N1S-6T

New hardware appliance

The following new hardware appliance is supported in this release.

- Nexus Dashboard M8-based large appliance (ND-NODE-G5L)

Guidelines and limitations

- For Nexus Dashboard feature guidelines and limitations, see the feature article for details.
- For more information on compatibility, see 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 4.2.1

These sections describe the categories for the changes in behavior introduced in Cisco Nexus Dashboard 4.2.1 in comparison to Nexus Dashboard 4.1.1g.

System level unified changes

Table 7 Behavior Change for System-level unified features

Behavior Change Category	Description
System level unified features	Changes to **Backup and Restore** • Changes to backup filenames • In Nexus Dashboard 4.1.1, backups are saved as `backupname.tar.gz`. • In Nexus Dashboard 4.2.1, for backup files that are saved to an SCP location, the cluster name is now prefixed to the name that you enter in the **Create backup** page in the Nexus Dashboard GUI. For example, if you enter `backup1` as the backup name in the **Create backup** page in the Nexus Dashboard GUI, the filename in the SCP location will show as `<cluster-name>_backup1`. • Downloading a backup file The download action on a full backup with telemetry will download a backup file without the telemetry data. You can restore this backup file, but the telemetry data will not be restored. • Backup schedules • In Nexus Dashboard 4.1.1, you can run 2 full backup schedules with no additional restrictions. • In Nexus Dashboard 4.2.1, you can only run 1 full backup. Full backup with telemetry schedules cannot be configured to run every day. • Save and restore backups on NFS-based NAS In Nexus Dashboard 4.2.1, you can save and restore backups on Network File System (NFS)-based Network Attached Storage (NAS) On NAS, backups are saved in a directory named `clustername_backupname`. You can restore backups on NAS after specifying the path to the `clustername_backupname` directory. You can only restore backups containing telemetry stored on a NAS from a NAS.
	Changes to Nexus Dashboard versioning • In Nexus Dashboard 4.2.1, versioning has been updated to introduce two types of

Behavior Change Category	Description
	versions: product Version and Build version. The product version indicates the release version and remains unchanged throughout the release cycle. For example, 4.2.1 is the product version for Nexus Dashboard release 4.2.1. • The Build version indicates the actual build of the software. There are no changes to the ACS version command; it continues to display the build version.
	Login and Password Management Nexus Dashboard 4.2.1 has various changes and enhancements to manage login and user passwords. In some cases, these controls are new, but they are adjacent to existing functionality and must be understood for the holistic picture of how things work. Changes to login and passwords • As per NIST 800-53 recommendations, Nexus Dashboard no longer allows 1 million commonly known passwords. Note that on an upgraded system, existing passwords are honored. • Nexus Dashboard has implemented a complex password since day 1, however, the following additional complex rules may be enabled by a "super-admin": ◦ You cannot use the same English alphabet or numbers 4 or more times consecutively. ◦ On a QWERTY keyboard, you can also not use 4 or more keys left-to-right or right-to-left consecutively. Enforce password change if the current password was configured by a different user, including cases where a new user was created, or another user's password was reset. • Nexus Dashboard 4.1.1, as well as earlier versions, did not require a first-time login password change. • In Nexus Dashboard 4.2.1, login is blocked if a password is configured by a different user. This happens when a "super-admin" created a new user, or a password was reset by a "super-admin". After the password is set by another user, the login of that user is blocked with a return code 403, and a password change screen is presented to force a new password. Note that a password change by a user for his own login doesn't go through this mechanism. Reuse an old password • In Nexus Dashboard 4.1.1 and earlier releases, you could reuse passwords. In Nexus Dashboard 4.2.1, you cannot reuse passwords for the same username. • The number of password resets prior to password reuse is configurable by a "super-admin" user under the Admin > Users and Security menu. Passwords have a validity time interval • In Nexus Dashboard 4.1.1 and earlier releases, passwords are valid indefinitely. • In Nexus Dashboard 4.2.1, Nexus Dashboard enforces a configurable password expiration period and provides advance warnings before passwords expire. Password expiry feature is a configurable option. Login using wrong password • In Nexus Dashboard 4.1.1 and earlier releases, users could try a login indefinitely, as there was no limit on how many times a login could fail. • In Nexus Dashboard 4.2.1, a configurable option is available which can lock a user account after "N" number of failed login attempts. You can configure the number of failed attempts allowed for user login. Unlocking of users follows a paradigm and rules which are explained in the *Cisco Nexus Dashboard Deployment and Upgrade Guide*. Allowed Host list to access webserver and SSH using rescue-user • In Nexus Dashboard 4.1.1 and earlier releases, there was no control over who could

Behavior Change Category	Description
	access the system; anyone could use it, and unlimited attempts were allowed. • On Nexus Dashboard 4.2.1, a “super-admin” can configure an Allowed Host list to restrict who can access the webserver on management interface port 443 and who can SSH as “rescue-user” on management interface port 22. The Allowed Host list supports a subnet. NOTE: While configuring an Allowed Host list, ensure that the machines from which the system is accessed are included. Otherwise, you may lock yourself out, and you cannot unlock your account without assistance from Cisco TAC.
	Onboarding an ND cluster into federation or multi-cluster connectivity setup, if using a Fully Qualified Domain Name (FQDN) • In ND 4.1.1 release, any FQDN or hostname is accepted to onboard another ND cluster if it resolves to a ND node IP address. • In ND 4.2.1 release, hostnames are no longer allowed to onboard ND clusters unless they are fully qualified. • If a DNS name is used to onboard ND, it must be a full FQDN, for example, `node1: invalid, node1.cisco.com: valid` • If an FQDN is used to onboard ND cluster to a federation, it must be a valid FQDN: • Must follow the format, `(node-name).(domain)` for one master node name in the cluster (case insensitive) • Equivalent FQDNs using the same domain must exist for all other master nodes in the respective cluster. • If using `node1.cisco.com: node2.cisco.com` corresponding to the first ND master node, `node2.cisco.com`, and `node3.cisco.com` for the other 2 masters must also exist and resolve to the nodes management IP(s) • If using FQDN to onboard another ND cluster, the local primary cluster is also validated. The primary cluster must have a search domain configured (Admin > System Settings > DNS) that creates valid FQDNs for each of the primary cluster’s nodes. This will be validated only at onboarding or re-registration time.
	Multi Cluster connectivity (aka federation) backup and restore • In Nexus Dashboard 4.1.1 release, on restore, the state of the secondary clusters in the federation does not change. On restore of a primary cluster, it deletes and restores the local state of all federation members. However, post restore, you must re-register all secondary ND clusters on the primary ND cluster. • In Nexus Dashboard 4.2.1 release, secondary deletes and restores federation members in an unregistered state. You must re-register secondary ND clusters on the primary cluster. • In Nexus Dashboard 4.1.1 release, federation is only allowed between clusters running version 4.1.1. • In Nexus Dashboard 4.2.1 release, federation is allowed between 4.1.1 and 4.2 clusters. If a federation is already in place, the primary cluster must be the first cluster to be upgraded to 4.2.1. • When an ND cluster hosting telemetry function for a fabric is separate from the ND cluster that is hosting the controller functionality for that fabric, it is recommended to first upgrade the controller cluster to 4.2.1. • Clusters upgrading from ND release 3.2.2m are automatically disconnected from the federation and must be re-registered by the primary cluster once all clusters are running 4.2. 1. • In ND 4.1.1 release, management connectivity routes were required for reachability between members of a multi-cluster aka federation setup for some features, for example, Topology, One Search. In ND 4.2.1 release, management connectivity routes are no longer required.
	Audit Lucene filter • In Nexus Dashboard 4.1.1, filter parameters were following a proprietary syntax format. • In Nexus Dashboard 4.2.1, filter parameters are now following Lucene syntax.

Automation

Table 8 Behavior Change for Automation features

Behavior Change Category	Description
Automation	Interface Manager changes to listing, creation, and modification The **Policies** column, which displayed the template in use, has been removed and replaced with **Intended configuration mode**, and **Policy**. These two new fields are consistently present in the openAPI, CSV import/export, create, and edit pages. • The Intended configuration mode may be options like trunk, access, and routed. • The Policy may have options like Host, virtual port-channel (vPC) Member, or port-channel Member • The mode column has been renamed Discovered configuration mode By default, template names are no longer shown unless User defined templates have been used.
	Links changes to listing, creation, and modification The Policy column no longer displays the template in use except when a User defined template is being used. The field has moved to a model-based approach for listing, csv import/export, create, and modify. This behavior is consistently represented in the UI and openAPI.
	VRF creation and modification Create and Modify workflows will no longer display the template in use, except when a User defined template is being used. The option for User defined will not be present unless the system has User defined VRF templates. A **Tenant** field is now displayed when at least one tenant is associated with the fabric.
	VRF attachment changes In Nexus Dashboard UI, the extension table has been moved above other options on border device attachment.
	Network creation and modification • Create and Modify will no longer display the template in use, except when a User defined template is being used. The option for User defined will not be present unless the system has User defined Network templates. • Networks previously supported a Boolean option for Layer 2 only. This has been changed to an option to set the Network mode with three options: Layer 2 only, Layer 2 with VRF, and Layer 3. • A Tenant field is now displayed when at least one tenant is associated with the fabric.
	Network attachment changes • Interface attachment has been changed and the UI displays only the attached interfaces, and there are explicit add/edit/delete options to choose. • Interface attachment options for setting the native VLAN or customer VLAN have been added. • Network attachment on ToR switches are now done on the ToR switch rather than the Leaf, with implicit Leaf attachment. • Network attachment on Access switches are now done on the Access switch rather than the Aggregation switch, with implicit Aggregation attachment.
	Security Group related changes Security group: Creating a security group requires a mandatory " VRF" selection. • For upgraded 4.1.1 data, this will be auto populated. The selectors can be chosen only for the VRFs that were selected.

Behavior Change Category	Description
	• You can edit the VRF list for default tenant. • Status displays only the following " deployed" , " pending" , and " notApplicable" . The " outOfSync" status is removed. • The " Any" group will show VRFs as empty because it is VRF agnostic, and it can be applied to a contract under any VRF. • Security group name length is increased from 40 characters to 63. Security contract A new Direction field is introduced at the contract level during contract creation, in addition to the existing Direction field at the rule level. For the default tenant, the contract-level Direction is set to Custom. For data upgraded from Nexus Dashboard 4.1.1 release, the contract-level Direction field is automatically populated based on the existing configuration. Protocol definition The Name field is now mandatory for each protocol filter entry created within a protocol definition. For data upgraded from Nexus Dashboard 4.1.1 release, the Name field is automatically populated. Security association • A new Name field is introduced for security associations. • The Source VRF selection is now restricted to the VRFs associated with the selected source security group. • The Action, Protocol definition, and Policy name columns are removed from the Monitoring page.
	Security protocol and contract names are case sensitive • In Nexus Dashboard 4.1.1, case sensitive names were allowed for security protocol definition names and security contract names. • In Nexus Dashboard 4.2.1, case insensitive names are enforced for security protocol definition names and security contract names. This change is introduced because NX-OS platforms do not support case insensitive names for class-maps (protocol definitions) and policy-maps (security contracts). • Upgrade from Nexus Dashboard 4.1.1 or Nexus Dashboard 3.2.2m to Nexus Dashboard 4.2.1 is handled gracefully, the existing data is retained, and no change of intent. • Any new protocol definitions or security contracts created in Nexus Dashboard 4.2.1 are handled as case insensitive. • If you update an existing protocol definition or security contract for which a case insensitive duplicate name exists, an error message will be displayed indicating and asking you to retain only one of them. You can delete existing case sensitive names for protocol definitions or security contracts.
	Changes to Advance Settings These are some changes to the Nexus Dashboard **Admin > System settings > Fabric management > Advanced settings**: • The Enable config compliance optimization for config-profile overlay mode is enabled by default. • LAN discovery now initiates scale-in after reaching the configured number of idle cycles. Default is 30. • The SSH Host Key verification is enabled by default. • A new setting is introduced to specify the maximum number of days of PM data is retained in the Elastic Search database. The default value is 90. • The configurable value range for Background Resync Timer (minutes) is updated from 60 to 600 minutes. • Template in-Use Override (only available when the Admin > System Settings > General > Display advanced settings and options for TAC support setting are enabled) is automatically Enabled after every 12 hours.

Behavior Change Category	Description
	Image Policy removed from bootstrap, pre-provision, and RMA • The Image Policies feature is removed from Fabric Software, as such UIs and APIs which previously referenced this are no longer valid. For any API including Legacy APIs there are no longer functional references to an Image Policy which are possible. The user may specify the image directly instead of the policy. • During bootstrap a new option to select the image to set as the boot image has been added as a replacement.
	Image management image upload • Local file upload is no longer a two-step process. You can now select the image file and the Save action will do both the upload and validation. • Remote storage location SCP or SFTP upload now requires definition of the remote location under the Admin tab prior to use. The API and UI no longer provide an ad-hoc option to specify the URL.
	Fabric Software • Fabric Image Policies, and Device Image policies have been removed. The fabric software update plan, as well as individual device granular actions, have been removed. All update actions have been normalized whether starting from a fabric, or a device to use update groups. For more information, see the Managing Your Fabric Software article. • Update groups have two actions: Prepare and Install Update. • Update Analysis, pre-upgrade reports, post-upgrade reports, and snapshot have all been combined into new Update Reports with customizable update checks. • Previous APIs involving Image Management are obsolete. The underlying features involving Image policies have been removed. Any automation must be migrated to new openAPIs. API options for bootstrap, pre-provision, and RMA involving selection of an image policy will no longer function as there are no image policies.
	Changes to Rollback • Rollback functionality is now strictly limited to the following entities: Policies (Regular and Shared), Networks, VRFs, and Interfaces and Links. • You can now rollback the last action, this is allowed only if the action involves one of the supported entities. • You cannot rollback full ticket if the rollback ticket has any actions besides the ones listed above. Support for Interface Groups Nexus Dashboard 4.2.1 introduces support for Interface Groups. Change Control changes to Interface Groups are tracked using standard Change Control procedures via tickets. Rollback is not supported for Interface Group configurations. The "Change System Mode" and "ticketId" functions are not supported in Nexus Dashboard 4.2.1. For these operations, the LAN fabric will internally set the "ticket bypass" parameter to “true” to ensure system processing continues without requiring a manual ticket ID.
	Changes to SAN backup migration SAN switch backups are purged during an upgrade from Nexus Dashboard 3.2.2m or ND 4.1.1g. Ensure that you save switch backups offline before starting the ND upgrade.
	Change in Dynamic Load Balancing (DLB) template deletion workflow The template type for *Dynamic_Load_Balancing_CS*.template has been changed from PYTHON (used in ND 4.1) to PYTHON_CLI. As a result, the policy deletion workflow has changed: • In Nexus Dashboard 4.1.1, policy instances could be deleted directly. • In Nexus Dashboard 4.2.1, policy deletion requires a two-step process:

Behavior Change Category	Description
	1. Mark the policy for deletion 2. Invoke the delete API
	Separate banner parameters for switch types • In Nexus Dashboard 4.1.1, there is only one " Banner" parameter for both IOS XE and NX-OS switches. • In Nexus Dashboard 4.2.1, a new " IOS XE Banner" parameter is introduced for IOS XE switches in Campus VXLAN EVPN fabric. The old " Banner" parameter is used for NX-OS switches. You must provide banner configurations separately for IOS XE and NX-OS switches.
	AI VXLAN fabric security group status • In Nexus Dashboard 4.1.1, security group status was not visible in fabric overview or Fabric group list. • In Nexus Dashboard 4.2.1, security group status is visible in fabric overview and Fabric group list for AI VXLAN iBGP fabrics.
	Routing configuration changes for license server reachability • In Nexus Dashboard 4.1.1, Management route is required for Cisco Smart Software Manager (CSSM) server reachability, and issues arise when the DNS IP changes • In Nexus Dashboard 4.2.1, Management route is no longer required. You must manually add the Data routes to reach CSSM via the Data network
	Changes to VMM and vCenter • VMM background resync timer settings • The VMM Background Resync Timer in minutes has changed. In Nexus Dashboard 4.2.1, the minimum VMM Background Resync Timer is changed from one minute to 60 minutes. The range is now 60–600 minutes, with a default of 60. On upgrade to Nexus Dashboard 4.2.1, this value will be set to the default value of 60 minutes. • This setting is only visible when the “Display advanced settings and options for TAC support” feature is enabled via the **Admin > System Settings > General > Advanced Settings** menu. Once enabled, you can configure the value under **Admin > System Settings > Fabric Management > Advanced Settings > VMM** in the Nexus Dashboard GUI. • Resync vCenters action The **Resync vCenters** action is no longer available as an option when you right click on the vCenter node in the topology view. Instead, it is now available as an option in all fabrics **Topology > Actions** drop-down list and under the Virtual Machines VMs > Actions if security groups are enabled.
	Push Configuration (config) case normalization In Nexus Dashboard 4.2.1, config is converted to lowercase during both Push config preview and Push actions, following the **Manage > Template Library > compliance_case_insensitive_clis** template.

Telemetry

Table 9 Behavior Change for Telemetry features

Behavior Change Category	Description

Telemetry	Traffic Analytics multi fabric cluster property is deprecated • In Nexus Dashboard 4.1.1, you can configure the Traffic Analytics multi fabric cluster property. Admin > System Settings > Flow Collection > Multifabric Enable/Disable • In Nexus Dashboard 4.2.1, the Traffic Analytics multi fabric cluster property is deprecated and moved at a per fabric level. Manage > Fabrics > <*fabric*> > Edit Fabric Settings > Telemetry> Traffic Analytics Scope.
	Change in error code for ACI telemetry manage objects (MO) • In Nexus Dashboard 4.1.1, system throws a 500-error code when user attempts to enable telemetry on an APIC where it's already enabled by another ND. • In Nexus Dashboard 4.2.1, system throws a 400-error code when user attempts to enable telemetry on an APIC where it's already enabled by another ND.
	Changes to Flow anomalies in Flow Telemetry • In Nexus Dashboard 4.1.1, Flow Telemetry anomalies were raised at 5 tuple (Source IP, Destination IP, Source Port, Destination Port, and Protocol), • In Nexus Dashboard 4.2.1, the flow anomalies are changed to IP address-level anomalies. If an IP address is learned in an Endpoint, this will be reflected in the Endpoint Score. Change to Flow Telemetry Events (FTE) • In Nexus Dashboard 4.1.1, the Flow Telemetry Events were raised at the node level. • In Nexus Dashboard 4.2.1, Flow Telemetry Events are raised at the IP address-level, like the Flow Telemetry anomalies. For a known Endpoint, will be reflected in the Endpoint Score.
	Changes to Bug scan Bug scans are executed only when the network device is either: • Connected to Intersight with metadata successfully downloaded, or • Operating in air-gapped mode with the latest metadata obtained from an Intersight account and applied. • Active Bugs are generated only after a Bug scan is successfully run. • PSIRTs are detected and reported only when the network device is either: • Connected to Intersight with metadata successfully downloaded, or • Operating in air-gapped mode with the latest metadata obtained from an Intersight account and applied. • Known Bugs are displayed only when the network device is either: • Connected to Intersight with metadata successfully downloaded, or • Operating in air-gapped mode with the latest metadata obtained from an Intersight account and applied.
	Changes to Fabric Software Management • Pre-Upgrade Analysis reports forecast clearing of Active Bugs and Advisories only when: • The network device is connected to Intersight with metadata downloaded, or • The latest air-gapped metadata from an Intersight account is applied, and a Bug scan has been run to identify any Active Bugs, if present. • Post-Upgrade Analysis reports clear Active Bugs and Advisories only when: • The network device is connected to Intersight with metadata downloaded, or • The latest air-gapped metadata from an Intersight account is applied, and a Bug scan has been run to identify any Active Bugs, if present.

	Changes to ACI connectivity interface summary and filtering The behavior of the **Summary** pane (including Anomaly level, Admin/Operational status, and Type) in the **Connectivity > Interfaces** page has been changed. • In Nexus Dashboard 4.1.1, when filters were applied to the interface list, the Summary pane only reflected the filtered results. • In Nexus Dashboard 4.2.1, the Summary pane appears above the Filter by attributes field and displays the total interface summary for the ACI fabric.
	System Stream Anomalies • In Nexus Dashboard 4.1.1, single object with field names remoteStreamingServer- array of strings anomalies -array of strings • In Nexus Dashboard 4.2.1, array of objects with field names remoteStreamingServers- strings anomalies -array of strings servertype - string.

Orchestration

Table 10 Behavior Change for Orchestration features

	Description
Orchestration	The behavior changes described in the Orchestration (NDO) section of the *Nexus Dashboard Release Notes for Release 4.1.1* are also applicable when upgrading to Nexus Dashboard Release 4.2.1. No additional changes are introduced beyond those previously documented changes.
	Changes to tenant management In Nexus Dashboard Release 4.2.1, tenant management is moved from Orchestration to Nexus Dashboard. For details, see the *Configuring Tenants and Tenant Domains* article.

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 11 New hardware support

Bug ID	Description	Fixed in	Affected Functionality
CSCwq86832	Connectivity Analysis does not function correctly for ACI endpoints if the corresponding bridge domain is advertising host routes.	4.2.1.10 and later	General
CSCwq56045	1) On 3.2, prior to starting an upgrade there is a fault in the System Settings page that tells user there is a NAS storage that is currently not healthy. In this case, please fix the nas server before starting upgrade. NO further WA required post upgrade starts. 2) If CU missed the error above and went ahead with 4.1 iso upload and start of Installation, you would see that after the nodes reboot, the UI throws an error that mentions the nas with the issue, and a recovery command for the upgrade.	4.2.1.10 and later	General

Bug ID	Description	Fixed in	Affected Functionality
CSCwq57884	Fabric is a member of Fabric Group and the networks are exported to be imported again to create new networks or update existing networks. Export includes internal variables and only if the user changes it and imports the networks, there are some unintended side effects.	4.2.1.10 and later	General
CSCwq59171	OpenSearch cluster may have shards stuck in INITIALIZING or UNASSIGNED state. The output of: esctl --name <namespace> get health may return: status: yellow or red initializing_shards >0 for hours unassigned_shards >0 for hours	4.2.1.10 and later	General
CSCwq60404	Home Overview: Active Endpoints Not Updating with Refresh Active endpoints are not updated while clicking on UI refresh button	4.2.1.10 and later	General
CSCwq68038	Some audit logs missing in the streaming server and logs /logs/k8_infra/streaming/fluentbit.stderr.log has logs saying failed to terminate continuously.	4.2.1.10 and later	General
CSCwo67502	A new knob has been introduced on the switch preview side-by-side page for viewing Expected/Generated configurations in Nexus Dashboard Fabric Controller (NDFC) for LAN Classic and External Fabric. The Pending Config option, which is meant to display the same order of commands for the same operation, does not consistently show the correct order in some scenarios. Specifically: Incorrect Command Ordering: When there is a config diff (i.e., differences in configurations that need to be pushed), the Generated Config displays the commands in the wrong order. This is especially noticeable when comparing the configuration to the running config output in the same screen. The ordering mismatch can lead to confusion, even though there is no functional impact on the system. Display Gaps Between Configs: In some cases, there are visible gaps between configuration entries in the display, which further contributes to the confusion. These gaps may appear when comparing the Expected vs. Generated configurations, making it unclear whether there are missing configurations or misalignment in the data. While the issue does not affect the functionality of the system (i.e., the configuration will still be pushed and applied correctly), it could cause confusion for users who are relying on the previewed config order to verify changes before applying them.	4.2.1.10 and later	Automation
CSCwq01290	The issue is observed in the onesearch feature on a scale setup. It takes 30 seconds to generate recommendations.	4.2.1.10 and later	Automation

Bug ID	Description	Fixed in	Affected Functionality
CSCwq15975	1. Security Groups are enabled in the fabric. 2. VRF is updated to modify the Default Security Action from 'Unenforced' to 'Enforced permit/deny'. 3a. Network(s) within the VRF is attached to anycast BGWs. or 3b. Network(s) within the VRF has enableL3OnBorder disabled and is attached to borders or vpc BGWs.	4.2.1.10 and later	Automation
CSCwq71238	The additional options displayed while user navigates into All cluster Topology are non-functional and when clicked will provide an error that it is not permissible from this level(All clusters). Additionally, the nodes VRFs and Networks when clicked gives 'Failed to load' error specifically in the case of upgrade.	4.2.1.10 and later	Automation
CSCwq71655	External Fabric allows neighbor switches to be added to the fabric. These switches are expected to appear only in the inventory with the role of " Neighbor." However, the switches are clickable, and ND does not support Switch Overview for neighbor switches.	4.2.1.10 and later	Automation
CSCwp33209	Shadow ESGs/EPGs are missing after migrating consumer ESG/EPG from site1 to site2 while provider ESG/EPG is still present on site1.	4.2.1.10 and later	Orchestration
CSCwq14237	While importing into an L3out template on NDO, an L3out which has static routes containing next hop configuration with a reference to an IPSLA monitoring policy users may be blocked for selection. On hovering over the L3out, users may see the error message " L3out reference to IPSLA Monitoring Policy 'foo' on IPSLA next-hop with address 'bar' on static route 'baz' cannot be imported into NDO. Please remove the IPSLA monitoring policy reference on the next hop to import the L3out. The import is blocked both through NDO UI and via API due to above error.	4.2.1.10 and later	Orchestration
CSCwp19272	In Segmentation and Security view of the fabric, global contracts imported as interface contracts which are consumed or provided by ESGs are not shown.	4.2.1.10 and later	Monitoring/Observability
CSCwp79955	When the fabric is in Traffic Analytics Compatibility mode (traffic Analytics at cluster level) Admin->System Status->Telemetry->Switches tab, Flow collections column will show " failed" for N9K model - N9K-C9364D-GX2A and version -10.3(2) and Expected configuration will show " !Netflow is not supported in this switch"	4.2.1.10 and later	Monitoring/Observability
CSCwp87489	After RMA of a border node in NXOS VxLAN fabric, the user cannot edit or delete Traffic Analytics Interface Filtering rules that have been configured before swapping the device. These rules are associated with the previous switch serial number. New rules can be created and associated with the new switch serialnumber and configurations are correctly pushed to the new switch.	4.2.1.10 and later	Monitoring/Observability
CSCwp95109	Fabric state in fabric overview page and one or more switches in the Inventory page show out-of-sync state.	4.2.1.10 and later	Monitoring/Observability

Bug ID	Description	Fixed in	Affected Functionality
CSCwq54557	Anomaly levels don't match between the Switch overview screen and Manage > Inventory and also Topology switches view.	4.2.1.10 and later	Monitoring/Observability
CSCwq56023	After an upgrade following a fabric re-register, the ACI fabric is in Add failed state with respect to its software telemetry status.	4.2.1.10 and later	Monitoring/Observability
CSCwq59448	Traffic analytics and flow troubleshooting jobs are reporting a higher latency than the actual packet latency for traffic passing through Cisco Nexus 9000 H1 and H2 series switches.	4.2.1.10 and later	Monitoring/Observability
CSCwq65103	The flow path may have unknown nodes in place of the super-spines. Or in the scenario where the correct path cannot be determined, the nodes from which flow records were received will be listed under " Uncertain Paths" .	4.2.1.10 and later	Monitoring/Observability
CSCwq66676	Navigation to basic inventory pages and topology gets stuck on the UI.	4.2.1.10 and later	Monitoring/Observability
CSCwq67934	In TA compatibility mode, Analysis Hub -> Traffic Analytics Page -> no traffic is seen.	4.2.1.10 and later	Monitoring/Observability
CSCwq71639	When telemetry is configured to stream over IPv6 with TA enabled at conversions in moderate scale, not all the conversations will be seen on Analysis hub -> Traffic Analytics page.	4.2.1.10 and later	Monitoring/Observability
CSCwq73546	Cannot enable TA Compat mode on the fabric if its running TA full.	4.2.1.10 and later	Monitoring/Observability
CSCwt24408	After restoring a backup in the 4.1.1g release on a freshly installed Nexus Dashboard (ND) where Nexus Dashboard Insights (NDI) is in the base tier, NDI integrations such as NAS, PDU, and others may not function as expected.	4.2.1.10 and later	General
CSCws00401	VRFs count data is displayed incorrectly on these pages: • Navigate to **Manage > Inventory** and select a switch from the **Overview** page, the VRFs count from security and segmentation card are displayed incorrectly. • Navigate to **Manage > Inventory** and select a switch and click the **Security Segmentation** tab, the VRFs table might display partial data or stale data.	4.2.1.10 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 12 Open issues for Nexus Dashboard

Bug ID	Description	Exists in	Affected Functionality
CSCws93719	In environments where Nexus Dashboard workflows require Fabric TechSupport collection, users may experience intermittent network instability. Specifically, control plane micro-outages and Port-Channel (LACP) flaps can occur, potentially causing brief disruptions in fabric connectivity.	4.2.1.10 and later	General
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.	4.2.1.10 and later	Automation
CSCwt20453	The “in-progress” status of **Reports** is missing from the **Analysis** columns under the **Devices** tab, **Update groups** tab, and **Group > Analysis** section. Ensure that when a **Rerun** is triggered, the user can still select switches and perform other actions from the **Devices** tab without being blocked by the in-progress status display. This means the in-progress indicator should not disable or prevent user interaction with other controls or actions on the Devices tab.	4.2.1.10 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

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

Table 13 Known issues for Nexus Dashboard

Bug ID	Description	Exists in	Affected Functionality
CSCws93719	When Telemetry is enabled, the Bug Scan feature may automatically trigger tech-support collection or retrieve diagnostic data from fabric switches as part of its scheduled operation. This behavior is automatic and cannot be disabled. Under certain scale and configuration conditions, tech-support collection can cause issues such as protocol flaps or switch reloads, leading to unexpected service impacts. These issues may also occur independently when tech-support collection is triggered manually or by other means Depending on the fabric characteristics you may observe one or more of the following: • Transient LACP port-channel flaps, causing brief traffic interruption, as described in CSCwj73031. • Switch instability or node reload during diagnostic data collection, resulting in an outage, as described in	4.2.1.10 and later	Automation

	CSCwp15375.		
CSCwt08695	Slack integration configuration is missing after restoring the Nexus Dashboard (ND) cluster setup.	4.2.1.10 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.	4.2.1.10 and later	Monitoring/Observability
CSCwt23223	Common Vulnerability Scoring System (CVSS) scores and advisory ID information for Third Party Software (TPS) CVEs are not displayed in advisory details. Cisco Bug Search Tool may show advisory links for such bug IDs, but the Cisco Security API does not provide corresponding advisory details.	4.2.1.10 and later	General
CSCws08868	BGP down anomaly is not generated when underlying VPC is made down.	4.2.1.10 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.	4.2.1.10 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.	4.2.1.10 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.	4.2.1.10 and later	Monitoring/Observability
CSCws98701	Tenant policy import from an ACI fabric into a VXLAN-ACI fabric group fails with network creation error.	4.2.1.10 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.	4.2.1.10 and later	Monitoring/Observability
CSCwt25919	OSPF Router ID is not displayed on Nexus Dashboard for Cisco IOS-XE Catalyst devices.	4.2.1.10 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.	4.2.1.10 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.	4.2.1.10 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.	4.2.1.10 and later	Automation
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.	4.2.1.10 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.	4.2.1.10 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.	4.2.1.10 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.	4.2.1.10 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.	4.2.1.10 and later	Automation
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	4.2.1.10 and later	Automation

	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		
CSCwr95624	After disassociating an ACI fabric from a tenant, the tenant is not deleted from the remote APIC.	4.2.1.10 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.	4.2.1.10 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.	4.2.1.10 and later	General
CSCwt40431	GPU memory utilization anomaly is showing wrong value for memory usage.	4.2.1.10 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.	4.2.1.10 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.	4.2.1.10 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.	4.2.1.10 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	4.2.1.10 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.	4.2.1.10 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.	4.2.1.10 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	4.2.1.10 and later	Monitoring/Observability

	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.		
CSCwt52763	Switch Config-sync status displays as "Pending" even if the Tenant deploy was successful and there is no pending intent to be deployed.	4.2.1.10 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.	4.2.1.10 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.	4.2.1.10 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.	4.2.1.10 and later	Automation
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.	4.2.1.10 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.	4.2.1.10 and later	Automation

Compatibility information

For Nexus Dashboard cluster sizing guidelines, see 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).

Table 14 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(2.240009)* • 4.3(2.240077)* • 4.3(2.250037) • 4.3(2.250045) • 4.3(2.260007)
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)
Cisco UCS-C225-M8 (ND-NODE-G5S)	• 4.3(6.250040) • 4.3(6.250053) • 6.0(1.250127)
Cisco UCS-C225-M8 (ND-NODE-G5L)	• 6.0(1.250127)

Note: The asterisk (*) indicates that releases 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 related known bug CSCwn56294.

Note: 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.

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 and services 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.

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

Verified scalability limits

For verified scalability limits, see the *Cisco Nexus Dashboard Verified Scalability Guide, Release 4.2.1*, which is available in the documentation is directly available on the CCO portal.

Related content

For release 4.2.1, 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 4.2.1 user content, go to this URL:
https://www.cisco.com/c/en/us/td/docs/dcn/nd/4x/collections/nd-user-content-421.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.

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**.

Printed in USA Cxx-xxxxxx-xx 01/20