



Working with Cisco Tech Support, Release 4.3.1

Table of Contents

New and changed information	1
Working with tech support	2
Connected TAC	3
Connected TAC settings	3
Guidelines and limitations	4
Prerequisites	4
Connected TAC capabilities	5
Tech support collection	5
Targeted tech support collection	5
Nexus Dashboard proxy for diagnostic switch commands	6
Copyright	7

New and changed information

The following table provides an overview of the significant changes up to this current release. The table does not provide an exhaustive list of all changes or of the new features up to this release.

Release Version	Feature	Description
Nexus Dashboard 4.3.1	Connected TAC enhancements	Connected TAC now supports both LAN and SAN personas and no longer requires active software telemetry. Capabilities include targeted diagnostic collection and approved read-only remote diagnostic command execution on NX switches through the Nexus Dashboard proxy. For more information, refer to Connected TAC.
Nexus Dashboard 4.3.1	LLDP information in tech support	Beginning with Nexus Dashboard 4.3.1, tech support collections now include LLDP neighbor information gathered from the management and fabric interfaces of Nexus Dashboard nodes for additional troubleshooting. For more information, refer to Working with tech support.
Nexus Dashboard 4.3.1	Cisco Nexus 9000 Series name change	Cisco Nexus 9000 Series is now the Cisco N9000 Series.

Working with tech support

Tech support enables you to collect logs and activities in the system for further troubleshooting by Cisco TAC. Cisco Nexus Dashboard provides tech support collection and gives ability to download tech support for the whole cluster. Tech support files are hosted on the Cisco Nexus Dashboard and can be downloaded at any time.

These are the maximum number of tech supports that can be generated:

- 10 for a physical appliance, and
- 3 for virtual appliance.

To collect Tech Support information:

1. Collect Tech Support.
 - a. From the main navigation menu, select **Admin > Tech support**.
 - b. In the main pane, click **Collect Tech Support Files**.
2. In the **Collect Tech Support** page that opens, provide a name.
3. (Optional) Check the box next to the **Tech Support for the last 24 hours** field.
4. Click **Collect**.

After you begin the tech support collection, you can see the progress in the same screen.

If for any reason the tech support collection process fails, you can also obtain the same information by logging into each node as the **rescue-user** and running one of the **acs techsupport collect** commands. For more information about specific **techsupport collect** command options, see [Useful Commands](#).

Tech support collections also include LLDP neighbor information gathered from the management and fabric interfaces of Nexus Dashboard nodes for additional troubleshooting.

5. Download the tech support archive.

After the collection is finished, you can download the archive by clicking the ellipsis (...) on an entry and choosing **Download all**. You can also download the archive by clicking on the entry in the **Nodes** column and clicking **Download all** in the drawer that appears.

If you want to delete an existing tech support package, click the ellipsis (...) on an entry and choose **Delete tech support**. You can also delete a tech support package by clicking the box next to an entry and clicking **Delete Selected Tech Support**.

Connected TAC

Connected TAC now allows Cisco TAC to remotely collect and analyze technical support data from ACI and NX devices onboarded to Nexus Dashboard through Cisco Intersight.

In previous releases, Connected TAC required the Nexus Dashboard cluster to be in LAN persona with active software telemetry enabled for the target devices. These requirements have been relaxed for ND-managed fabrics, but ACI fabrics still require telemetry to be enabled.

Connected TAC now supports both LAN and SAN personas for ND-managed environments and can operate without software telemetry in those deployments, including on clusters configured with controller-only functionality. These changes expand TAC remote diagnostic support across a broader range of Nexus Dashboard deployments.

All Connected TAC operations are initiated by Cisco TAC through Cisco Intersight. After your Nexus Dashboard cluster is connected to Cisco Intersight, Connected TAC is available for supported TAC operations, and customers can manage the feature by using the Connected TAC settings.

Connected TAC settings

Nexus Dashboard provides Connected TAC settings in **Admin > System Settings > Fabric Management**.

This area includes a **Connected TAC** card that allows authorized users to view and manage how Connected TAC operates on the cluster.

Only users with the **super-admin** role can modify these settings.

Configure the Connected TAC settings on the Nexus Dashboard cluster where controller functionality is enabled for the target fabric.

The **Connected TAC** card includes the following settings:

- **Connected TAC enabled**—Controls whether Cisco TAC can use Connected TAC through Cisco Intersight for supported diagnostic operations.
- **Connected TAC username**—Specifies the Nexus Dashboard user whose configured device credentials are used for Connected TAC operations on supported LAN or SAN devices.

By default, Connected TAC is enabled and no username is configured. If a Connected TAC username is configured, Nexus Dashboard uses the device credentials associated with that user for supported operations.

If no username is configured, Connected TAC uses the discovery credentials of the target switch for supported operations.

For SAN deployments, fabric credentials are configured on a per-fabric basis. A Nexus Dashboard user can be selected for Connected TAC if that user has SAN fabric credentials configured for at least one fabric.

If Connected TAC is disabled, Cisco TAC cannot use Connected TAC through Intersight to collect show tech data or run supported diagnostic commands.

Guidelines and limitations

- Your Nexus Dashboard cluster must be connected to Cisco Intersight. If Intersight connectivity is not established, Connected TAC operations are not available.
- Both LAN and SAN personas are supported for all Connected TAC operations.
- For ACI deployments, software telemetry must be enabled to support Connected TAC operations. For ND-managed deployments, Connected TAC is supported without requiring locally enabled software telemetry, including on clusters with controller-only functionality.
- Connected TAC operations are initiated by Cisco TAC through Cisco Intersight. Customers cannot initiate Connected TAC jobs from the Nexus Dashboard GUI, but **super-admin** users can manage Connected TAC availability and username selection in **Admin > System Settings > Fabric Management**.
- If Connected TAC is disabled in **Admin > System Settings > Fabric Management**, Cisco TAC cannot use Connected TAC through Intersight to collect show tech data or run supported diagnostic commands.
- The Nexus Dashboard UI does not display progress for Connected TAC jobs in the following scenarios:
 - SAN persona deployments
 - NDFC LAN deployments where telemetry is not enabled locally

This is expected behavior and does not indicate a problem with the collection. TAC monitors job progress through Intersight.

- Remote command execution on NX switches through the Nexus Dashboard proxy is restricted to a system-enforced allowlist of commands. Commands not on the allowlist are rejected. The allowlist is dynamically maintained through metadata updates and is not configurable by Nexus Dashboard administrators.
- Only one Connected TAC collection job can be in progress at a time. If a collection is already running, additional requests are rejected until the current job completes and the data is uploaded to Intersight.
- To optimize storage on smaller form factor deployments, tech support data collected through Connected TAC is purged after the upload to Intersight completes. This differs from manual tech support collections, which remain on the cluster and can be downloaded later.
- On smaller form factor deployments, if a Connected TAC upload fails after data is collected, the collected data is purged and TAC must reinitiate the collection job. There is no option to retry the upload without recollecting the data.

Prerequisites

The following requirements must be met to support Connected TAC operations on your cluster:

- **Intersight connectivity**—Your Nexus Dashboard cluster must be connected to Cisco Intersight. To verify connectivity:
 - Log in to the Nexus Dashboard GUI.
 - Navigate to **Admin > Intersight**.

- Confirm that the Device Connector status shows **Claimed**.

If the Device Connector is not claimed, configure Intersight connectivity before Connected TAC operations can be used.

- **Connected TAC username**—If a Connected TAC username is configured, the selected Nexus Dashboard user must have valid LAN or SAN device credentials configured for the target environment.
- **SAN deployments**—For SAN deployments, fabric credentials are configured on a per-fabric basis. A user can be selected for Connected TAC if SAN fabric credentials are configured for at least one fabric.
- **Disk space**—For smaller form factor deployments, make sure the cluster has at least 15 GB of available storage for Connected TAC tech support collection. Larger form factor deployments that support telemetry already have the required persistent volume allocated.
- **TAC permissions**—Cisco TAC engineers require an open service request against your network device to use Connected TAC capabilities. These permissions are managed through Cisco's case management system and do not require any configuration on the Nexus Dashboard.
- **Nexus Dashboard configuration**—Beyond establishing Intersight connectivity, no additional configuration is required to make Connected TAC available.
- **Super-admin users**—Optionally, **super-admin** users can manage Connected TAC availability and username selection in **System Settings > Fabric Management**.

Connected TAC capabilities

When your Nexus Dashboard cluster is connected to Cisco Intersight, the following remote support capabilities are available to Cisco TAC.

Tech support collection

TAC can remotely initiate a full tech support bundle collection for any device onboarded to your Nexus Dashboard cluster. When TAC triggers a collection through Intersight, Nexus Dashboard collects the data from the target device, compresses it, and uploads it to Intersight for TAC analysis.

For devices on clusters without telemetry enabled, Nexus Dashboard uses the discovery VRF and the source interface that was used to discover the device to transfer the tech support file to the cluster before uploading it to Intersight. On the Nexus Dashboard side, this is the interface used for switch management, configured as **LAN Device Management Connectivity** in **Admin > System Settings > Fabric Management > Advanced settings > Admin**. Check that network policies permit traffic on the discovery VRF between Nexus Dashboard and the target device.

This process does not require customer action. After Intersight connectivity is established, tech support collection is available to TAC at any time.

Targeted tech support collection

Instead of collecting a full tech support bundle, TAC can initiate targeted diagnostic collection by using approved show tech options for specific troubleshooting scenarios. Targeted collection reduces the volume of data collected, decreases upload time, and allows TAC to focus analysis on a specific

subsystem or protocol.

Targeted collection uses an approved set of diagnostic show tech commands to collect only the data needed for a specific troubleshooting workflow.

The following show tech commands are supported for targeted collection:

Category	Supported Commands
Time-optimized	<code>show tech time-optimized</code>
Common protocols	<code>show tech ospf</code> , <code>show tech bgp</code> , <code>show tech forwarding</code> , <code>show tech multicast</code> , <code>show tech l2</code> , <code>show tech ethpm</code> , <code>show tech details</code> , <code>show tech vxlan</code> , <code>show tech vxlan-evpn</code> , <code>show tech vpc</code> , <code>show tech l2fm l2dbg</code> , <code>show tech port-channel</code> , <code>show tech lacp all</code> , <code>show tech license</code> , <code>show tech interfaces all</code> , <code>show tech transceiver</code> , <code>show tech ip multicast</code> , <code>show tech memory</code>
Install and configuration troubleshooting	<code>show tech install</code> , <code>show tech dme</code> , <code>show tech cli</code>

The set of supported commands is limited to approved diagnostic commands maintained by the system. This set may be updated in future releases or metadata updates.

Nexus Dashboard proxy for diagnostic switch commands

TAC can execute approved diagnostic commands directly on NX switches through Cisco Intersight using the Nexus Dashboard proxy.

These commands are limited to approved read-only diagnostic commands and cannot be used to modify switch configuration.

When TAC submits an approved diagnostic command through Intersight, Nexus Dashboard forwards the request to the target switch and returns the resulting output to Intersight. This allows TAC to gather real-time diagnostic information without requiring customer intervention or direct switch access.

Command execution through the proxy is subject to the following controls:

- **Allowlist enforcement**—Only approved read-only commands included in the system-enforced allowlist can be executed. Commands not on the allowlist are rejected. The allowlist is dynamically maintained through metadata updates and is not configurable by Nexus Dashboard administrators.

Copyright

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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.

The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

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)

© 2017–2026 Cisco Systems, Inc. All rights reserved.

Americas Headquarters

Cisco Systems, Inc.

170 West Tasman Drive

San Jose, CA 95134-1706

USA

<https://www.cisco.com>

Tel: 408 526-4000

800 553-NETS (6387)

Fax: 408 527-0883