

Reviewing History and Logs in Your Nexus Dashboard, Release 4.3.1

Table of Contents

New and changed information . . . 1
Understanding history and logs . . . 2
  Enable history and log settings . . . 2
Review history and logs for your Nexus Dashboard . . . 3
  View audit logs at the Nexus Dashboard level . . . 3
  View Anomaly and Advisory Audit Logs . . . 4
  Download Audit Logs . . . 4
Review history and logs for a fabric . . . 6
  View audit logs at the fabric level . . . 6
  View deployment history . . . 7
  View policy change history . . . 8
  View recent Tasks . . . 9
Add remote streaming servers . . . 10
  Splunk . . . 10
  Syslog . . . 11
  SNMP . . . 11
  Webhook . . . 12
  Enable Webhook as a remote streaming server . . . 13
  Add Webhook streaming for a fabric . . . 13
Copyright . . . 14

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	Anomaly and advisory audit logs	Beginning with Nexus Dashboard 4.3.1, audit log records for anomaly and advisory updates include a hyperlink that identifies the specific records affected by the audited action. For more information, see View Anomaly and Advisory Audit Logs.

Understanding history and logs

You can review history and log information in your Nexus Dashboard at several levels:

- At the upper Nexus Dashboard level: The **History and Logs** page allows you to see the system-wide list of events and alerts in your Nexus Dashboard cluster. See Review history and logs for your Nexus Dashboard for more information.
- At the lower fabric levels: The **History** tab within a configured fabric provides audit logs, deployment history, and policy change history information for that specific fabric. See Review history and logs for a fabric for more information.

Enable history and log settings

To enable history and log setting and set the maximum audit record retention duration for your Nexus Dashboard:

1. Go to **Admin > System Settings > General**.
2. Under **History and logs settings**, click **Edit**.

   The **History and logs settings** dialog box opens.

3. Check the box in the **Enable audit logs streaming** field to enable that feature, then choose a remote streaming server from the drop-down list.

   See Add remote streaming servers for more information on adding remote streaming servers.

4. In the **Maximum Number Record Retention duration** field, enter the number of months as the duration that you want to have the records retained.

   Valid entries are from 1-12. The default duration is 12 months.

5. In the **Maximum Number of Audit Records** field, enter the maximum number of audit records that you want to retain.

   Valid entries are from 0-2147483647. The default value for maximum number of audit records is 100K for virtual cluster setup and 500K for a physical cluster.

Review history and logs for your Nexus Dashboard

The **History and Logs** page allows you to see the system-wide list of audits in your Nexus Dashboard cluster.

View audit logs at the Nexus Dashboard level

Nexus Dashboard audit logging, which is automatically enabled when you first deploy the cluster, captures the operational changes made by the users in the environment.

You can view the History and logs by selecting **Admin > History and Logs** from the main navigation menu. You can also view History and Logs from the **Home** section of the main navigation menu. To view History and Logs, click **View All** under **Recent Activity**.

History and Logs provides this information for the audit logs in your Nexus Dashboard.

Field	Description
Creation time	Shows the date and time that the audit log was created.
User	Shows the user who was logged into the Nexus Dashboard when the audit log was created.
Affected object	Shows the object that was affected when the audit log was created.
Action performed	Shows the action that was performed when the audit log was created.
Description	Shows a description of the audit log. Click the entry in the **Description** column to display a drawer with additional information.
Fabric name	Shows the fabric that is associated with the audit log, if applicable.



The logs are not sorted by default. You can sort the list by clicking on any of the column headings. You can also sort data by choosing time modes like **Current**, **Last**, and **Date and Time Range**.

To filter the list by attribute, provide a specific attribute and value pair in the **Filter by attributes** field. For any entry in the table, click the funnel icon that appears to the right of that entry to automatically enter the filter attributes for that specific entry.

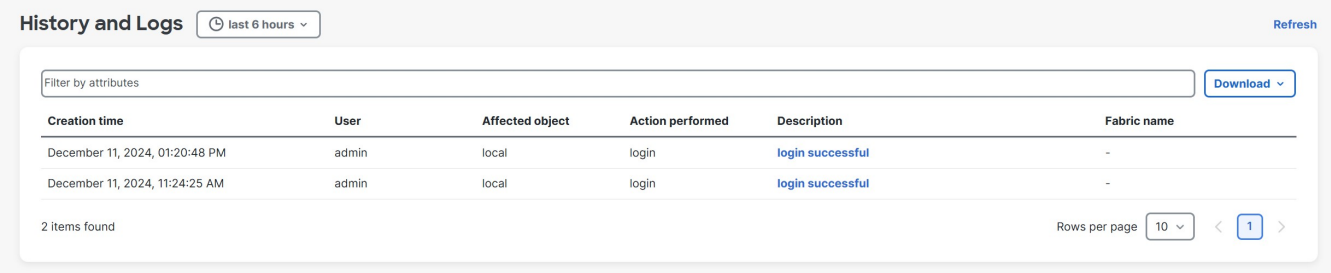
To filter the list based on time selection, click the clock icon next to **History and Logs**. Make the appropriate choice in the **Mode** area that appears:

- **Current**: Shows the latest available data.
- **Last...**: Choose from these options in the **Period** area:
  - last 15 minutes
  - last hour
  - last 2 hours
  - last 6 hours

- last day
- last week

- **Date and Time Range**: Choose the date and time range to use to filter the list.

Click **Apply** after you have made the appropriate choice in this page. The entries in the table are updated based on the choice the you made in the **Mode** area. The figure below shows example output where **last 6 hours** is chosen in the **Mode** area.



History and Logs

To view detailed information about a specific entry, click the link in the **Description** column to open the **Details** page for that entry.

View Anomaly and Advisory Audit Logs

When you update anomalies or advisories, Nexus Dashboard creates an audit log entry for each change. For these entries, the **Affected object** field includes a **View** link. Click **View** to open the **Anomalies** or **Advisories** page, which lists the anomalies or advisories affected by the action.

The page is read-only and provides limited table functionality. You cannot perform any actions on anomalies or advisories from this page.

In co-located fabrics, you can update anomalies or advisories on a remote cluster. Nexus Dashboard creates the audit log record on the cluster where the anomaly or advisory resides.

When a bulk update includes anomalies or advisories from multiple fabrics, Nexus Dashboard creates one audit log record per fabric. Each record includes only the affected items from that fabric.



- The page might show fewer records than the audit log entry indicates if some records were suppressed or aged out before you opened the audit log. Cleared records still appear in audit logs, and the audit log retains the identifiers for all affected anomaly or advisory records.
- Audit log records created before the upgrade to this release do not include the **View** link and continue to display identifiers as before. During the upgrade, existing anomalies and advisories are enhanced to support the **View** link for future updates. The **View** link is also supported for cleared anomalies and advisories.

Download Audit Logs

In the **History and Logs** page, click the **Download** button and choose either **Download as CSV** or **Download as JSON** to download audit logs.

The **Download as CSV** option downloads all audit log data, irrespective of the time selection in the **Mode** area and attributes filter in the **Filter by attributes** field.

Review history and logs for a fabric

You can review these history and logs at the fabric level:

- View audit logs at the fabric level
- View deployment history
- View policy change history

View audit logs at the fabric level

Nexus Dashboard audit logging is automatically enabled when you first deploy the cluster, and captures the operational changes made by the users in the environment.

To view the audit logs for a fabric:

1. Navigate to the fabric where you want to view the audit logs:
   a. Navigate to the main **Fabrics** page:

      Manage > Fabrics

   b. Single-click on the fabric where you want to view the audit logs.

      The Overview page for that fabric appears.
2. Click the **History** tab.
3. Click the **Audit Logs** subtab.

   These fields appear in the **Audit Logs** page.

   - The logs are not sorted by default; you can sort the list by clicking on any of the column headings.
   - You can choose to filter the list using the **Filter by attributes** field and providing a specific attribute and value pair.

Field	Description
Creation Time	Provides the date and time when an action was performed.
User	Provides information on the user who performed an action.
Resource	Provides information on the resource where an action was performed.
Action Performed	Describes what action was performed.
Description	Provides a description of the action that was performed.
Fabric Name	Provides information on the fabric name where an action was performed.

   You can also perform these actions in this page.

Action	Description
Download > Download as CSV	Click to download the audit log information to a CSV file.
Download > Download as JSON	Click to download the audit log information to a JSON file.

When you create anomaly alert rules, any updates to anomalies will not be recorded in the audit logs.

View deployment history

Deployment history of the switches and networks that are involved in the selected service policy or route peering are displayed in the **Deployment History** tab. The deployment history captures the changes that are pushed or deployed from Nexus Dashboard to the switches. The deployment history captures the changes that are pushed or deployed from Nexus Dashboard to the switches.

To view the deployment history for a fabric:

1. Navigate to the fabric where you want to view the deployment history:
   a. Navigate to the main **Fabrics** window:

      Manage > Fabrics

   b. Single-click on the fabric where you want to view the deployment history.

      The Overview window for that fabric appears.
2. Click the **History** tab.
3. Click the **Deployment History** subtab.

   This table describes the fields that appear on this page.

Field	Description
Hostname	Specifies the host name of the entity.
Entity Name	Specifies the entity name.
Entity Type	Specifies the entity type.
Source	Specifies the source of the deployment on the entity.
Commands	Click the link in the **Commands** column to bring up a window that displays the command execution details for the entity.
Status	Specifies the status of the host.
Serial Number	Specifies the serial number of the entity.
Status Description	Specifies the deployment status on the entity.
User	Specifies the user who performed the deployment on the entity.
Time of Completion	Specifies the timestamp of the deployment.

In certain scenarios after deploying configurations on a switch, the **Status** column displays the following error indicating a failure:

> Deployment Failed to execute job for this device with " Reason: dcnm-sim-agent-xx expired.

However, the **Config Status** in **Manage > Inventory > Switches** page displays **In-Sync**. The reason for a conflicting status is due to inter-node connectivity issue that causes the keep alives between the sim-agent and the sim-master to fail, resulting in an agent expiry event, whereas the sim-agent is alive and deploying the configuration on the switch. No further action is required from you for this error.

View policy change history

Different users can simultaneously change expected configuration of switches in the Nexus Dashboard. You can view the history of policy changes in the **Policy Change History** tab.

To view the policy change history for a fabric:

1. Navigate to the fabric where you want to view the policy change history:
   a. Navigate to the main **Fabrics** window:

      Manage > Fabrics

   b. Single-click on the fabric where you want to view the policy change history.

      The **Overview** page for that fabric appears.
2. Click the **History** tab.
3. Click the **Policy Change History** subtab.

   This table describes the fields that appear on this page.

Field	Description
Template	Specifies the template that was used in the policy change.
Description	Specifies the description of the policy change.
Content Type	Specifies the content type for the policy change.
Operations	Specifies the Policy Template Instances (PTIs).
Generated Config	Specifies the configuration history for the policy change. Click **Detailed History**, if available, to view the configuration history for the policy change.
Entity Name	Specifies the entity name where the policy change was performed.
Entity Type	Specifies the entity type where the policy change was performed.
Source	Specifies the source of the policy change.
Priority	Specifies the priority value of the policy change.

Field	Description
Policy ID	Specifies the policy ID of the policy change.
Host Name	Specifies the host name where the policy change was performed.
Created On	Specifies that date on which the policy was created.
Serial Number	Specifies the serial number where the policy change was performed.
User	Specifies the user who performed the policy change.

View recent Tasks

On the **Recent Tasks** tab, you can view the changes made for the event analytics.



When the device is rebooted, the recent task details are erased.

1. Navigate to the fabric where you want to view the policy change history:
   a. Navigate to the main **Fabrics** window:

      Manage > Fabrics

   b. Single-click on the fabric where you want to view the policy change history.

      The **Overview** page for that fabric appears.
2. Click the **History** tab.
3. Click the **Recent tasks** subtab.

   This table describes the fields that appear on this page.

Field	Description
Fabric	Specifies the name of the fabric.
Task Name	Specifies the name of operation done on fabric recently.
Task Description	Specifies the description of task done on fabric.
Duration	Specifies the time duration of the task.
Completed/Progress	Specifies the progress details, whether the task is completed 100% or still in progress.

Add remote streaming servers

You might need remote streaming servers to be configured when you deal with various areas in Nexus Dashboard, such as tech support, anomalies, and history and logs.

Follow these steps to add remote streaming servers.

1. Choose **Admin > System Settings**.

   The **General** tab is chosen by default.

2. Locate the **Remote streaming servers** tile and click **Edit**.

   A table showing any already-configured remote streaming servers appears.

3. Click **Add Server**.

   The **Add Server** dialog box opens.

4. Determine the service where you want to add remote streaming servers.
   - Splunk
   - Syslog
   - SNMP
   - Webhook

Splunk

1. In the **Protocol** field, choose **HTTP** or **HTTPS** based on the Splunk URL that you use.

   For example:

   - Choose **HTTP**, if your login URL is http://splunk.mycompany.com:8000.
   - Choose HTTPS, if your login URL is https://mycompany.splunkcloud.com/, https://mycompany.splunkcloud.com:443, or https://splunk.mycompany.com.

   Before enabling HTTP or HTTPS, you must upload the CA certificate for the Splunk destination host to Nexus Dashboard.

2. Enter a name for the Splunk remote streaming server in the **Name** field.
3. In the **Hostname/IP Address**, enter the hostname or IP address.
4. In the **Port** field, enter the HTTP event collector (HEC) port number.

   The HEC port number for Splunk deployments over HTTP or HTTPS protocols can be one of the following:

   - 8088 on Splunk Cloud free trials
   - 443 by default on Splunk Cloud Platform instances

5. In the **Token** field, enter the HEC token.

For more information on Splunk deployment guidelines, see the Set up and use HTTP Event Collector in Splunk Web.

6. In the **Index** field, enter the necessary index information for the Splunk remote streaming server.

   The index details on the Nexus Dashboard should match with the Splunk index.

7. Click **Save** in the **Add Server** page.

   You are returned to the **Remote streaming server** page.

8. In the **Remote streaming server** page, click **Add Server** to add another remote streaming server or click **Save** to save the configured remote streaming servers.

Syslog

1. In the **Protocol** field, choose either **TCP** or **UDP**.
2. Enter a name for the Syslog remote streaming server in the **Name** field.
3. In the **Hostname/IP Address** and **Port** fields, enter the hostname or IP address and port details.
4. Check the box next to the **TLS** field to enable this option.

   Before enabling TLS, you must upload the CA certificate for the Syslog destination host to Nexus Dashboard. See Managing Certificates in your Nexus Dashboard for more information.

5. Click **Save** in the **Add Server** page.

   You are returned to the **Remote streaming server** page.

6. In the **Remote streaming server** page, click **Add Server** to add another remote streaming server or click **Save** to save the configured remote streaming servers.

   The CA certificate you upload is used to sign the certificate that Splunk and Syslog uses. The certificate for Splunk and Syslog should contain the IP address or DNS name in the Subject Alternative Name (SAN) section.

SNMP

Previously, Nexus Dashboard anomaly notifications were limited to Kafka or syslog exports. Beginning with Nexus Dashboard 4.3.1, the SNMP anomaly export feature enables network operations to seamlessly integrate Nexus Dashboard anomaly data into the existing SNMP trap collectors and Network Management Systems (NMS). This allows for centralized anomaly collection, simplifies monitoring, and helps meet compliance policies. You can selectively export system anomalies based on severity (Critical, Major, Minor, and Warning), ensuring focus on the most relevant alerts. This provides a more versatile and compliant method for consuming Nexus Dashboard anomaly data, especially for environments heavily reliant on SNMP.

1. Enter a name for the SNMP remote streaming server in the **Name** field.
2. In the **Hostname/IP Address** and **Port** fields, enter the SNMP server's hostname or IP address and port details.

3. Choose the SNMP **Version**:
    - **v2c**: Choose **v2c**.
        - In the **Community string** field, enter the community string name.
    - **v3**: Choose **v3**.
        - Enter the SNMPv3 engine ID if it is different from the SNMP server engine ID.
        - Choose your option from the **Authentication / Privacy** drop-down list. If you choose **Authentication / No privacy** from the drop-down list, then choose from **Authentication algorithm** drop-down list for the authentication protocol (MD5, SHA, SHA2-224, SHA2-256, SHA2-384, SHA2-512), enter the **Password** and **Username**.
        - If you choose **Authentication / privacy** from the drop-down list, then choose from **Authentication algorithm** drop-down list for the authentication protocol (MD5, SHA, SHA2-224, SHA2-256, SHA2-384, SHA2-512), enter the **Password**. Choose from **Encryption algorithm** drop-down list, enter the **Password** and **Username**.
        - If you choose **No authentication / No privacy** from the drop-down list, enter the **Username**.
4. Click **Save** in the **Add Server** page.

    You are returned to the **Remote streaming server** page.

5. In the **Remote streaming server** page, click **Add Server** to add another remote streaming server or click **Save** to save the configured remote streaming servers.



- Multiple SNMP servers of different versions (SNMPv2c and SNMPv3) can be configured and coexist simultaneously.
- To stream anomalies to an external destination, configure Nexus Dashboard for system anomaly streaming. For more information, refer to Stream system anomalies.

Webhook

Starting with Nexus Dashboard 4.2.1, Nexus Dashboard supports streaming event data to external webhook servers, in addition to existing options such as **Syslog**, **SNMP**, and **Splunk**. 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.

You can selectively export fabric-level anomalies and advisories based on severity (Critical, Major, Minor, Warning), ensuring focus on the most relevant alerts. This provides a more versatile and compliant method for consuming Nexus Dashboard anomaly data.

This feature adds **Remote Streaming capability** via webhook endpoints, allowing administrators to receive real-time event notifications.



- In Nexus Dashboard 4.2.1, this feature supports exporting only Fabric anomalies and advisories. System anomalies are not supported for Webhook streaming in this release.
- Webhook streaming is supported only for IPv4. IPv6 support is not available in

this release.

Enable Webhook as a remote streaming server

You can enable Webhook as a remote streaming server and configure Webhook endpoints to receive real-time event notifications.

Follow these steps to enable Webhook remote streaming.

1. Follow the steps described in the Add remote streaming servers section, and click on **Webhook**.
2. Enter a name for the **Webhook remote streaming server** in the **Name** field.
3. (Optional) Enter a description for the Webhook remote streaming server in the **Description** field.
4. Enter the URL in the URL field using the format **http://{hostname/IP}:{port}/{endpoint}.**

   (Optional) Choose **Proxy**. If enabled, the URL will follow the Nexus Dashboard proxy.
5. (Optional) Enter the header name in the **Header name** field.
6. (Optional) Enter the header value in the **Header value** field.

   Click **Add** to add more headers.
7. Click **Save** in the **Add Server** page.

Add Webhook streaming for a fabric

After adding the **Webhook** configuration in **Admin > System Settings > General > Remote streaming servers**, you can enable Webhook streaming for fabric-level anomalies and advisories.

Follow these steps to add Webhook streaming for a fabric.

1. Navigate to **Manage > Fabrics**.
2. Click the radio button next to the fabric that you want to edit, then click **Actions > Edit fabric settings**.

   The **Edit *fabric_name* settings** page appears.
3. Click the **External streaming** tab and then choose **Webhook**.
4. In the **Destination** drop-down list, choose the Webhooks you want to configure for your fabric.
5. Choose the **Severity of Anomalies** and **Severity of Advisories**.

   You can check the check box for each severity type (Critical, Major, Minor, Warning) or click **Select all** to choose all severity types.
6. Click **Save**.

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