

Detecting Anomalies and Identifying Advisories in Your Nexus Dashboard, Release 4.2.1

Table of Contents

New and changed information . . . 1
Anomalies . . . 2
- Understanding anomaly correlation . . . 2
  - Root cause anomalies . . . 2
  - Correlated anomalies . . . 2
  - Uncorrelated anomalies . . . 3
  - Anomaly levels . . . 3
  - Anomaly properties . . . 4
- Navigate to Anomalies . . . 4
  - View all anomalies across all fabrics . . . 4
  - View anomalies for a single fabric . . . 4
  - View anomalies for a single switch . . . 5
  - View system anomalies . . . 5
- Analyze anomalies . . . 5
  - Resolve streaming anomalies on switches . . . 8
  - Resolve telemetry configuration anomalies on switches . . . 10
- View platform and system alerts in global anomalies table . . . 12
  - System anomaly notification . . . 13
- Guidelines and limitations for anomalies . . . 13
- Configure anomaly properties . . . 14
- Anomaly filters . . . 16
  - Filtering for acknowledged or unacknowledged anomalies . . . 17
  - Filtering for root cause and uncorrelated anomalies . . . 17
  - Determine the primary affected object for an anomaly . . . 17
- Global rules . . . 17
  - Customize anomaly level thresholds . . . 18
- Anomaly rules . . . 22
  - Guidelines and limitations . . . 24
  - Create anomaly rules . . . 25
  - Manage anomaly rules . . . 26

Advisories . . . 27
- Navigate to Advisories . . . 28
  - View all advisories across all fabrics . . . 28
  - View advisories for a single fabric . . . 28
  - View security advisories . . . 28
  - View advisories for a single switch . . . 29
  - View system advisories . . . 29
- Analyze advisories . . . 29
- View platform and system alerts in global advisories table . . . 30
  - System advisory notification . . . 31
- Advisory filters . . . 31

Metadata support 32
Metadata support for air-gapped environment 32
Update metadata version 32
Copyright 34

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 4.2.1	Route event correlation for ACI fabric.	Beginning with Nexus Dashboard 4.2.1, Nexus Dashboard correlates route events for both NX-OS switches and ACI fabric environments, enabling more comprehensive root cause analysis. For more information, see Correlated anomalies.
Nexus Dashboard 4.2.1	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: * Analyze anomalies * Anomaly rules
Nexus Dashboard 4.2.1	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 Resolve streaming anomalies on switches.

Anomalies

Nexus Dashboard proactively detects different types of anomalies across the network, analyzes the anomalies, and identifies remediation methods.

Nexus Dashboard collects and analyzes data from all nodes within the fabric, establishing a baseline to define "normal" behavior. Deviations from this baseline are flagged as anomalies. This allows you to focus on resolving issues rather than tracking them. Furthermore, Nexus Dashboard can assess the anomaly's impact and provide tailored recommendations based on its nature, thereby reducing the mean time to troubleshooting and resolution (MTTR). This helps in accelerated troubleshooting, enhanced operational efficiency, and effective remediation.

The **Anomalies** page displays the anomalies by level and category for your fabrics, based on the chosen time range.

- The **Anomaly level** donut chart displays the total number of anomalies of Critical, Major, Minor, and Warning severities.
- The **Category** list displays the number of anomalies grouped by various categories, such as Hardware, Capacity, Compliance, Connectivity, Configuration, GPU, Integrations, Active bugs, Telemetry configuration, and System.

About CRC Anomalies

CRC anomalies are raised based on the error count with respect to total packets received within 60 mins interval. If the number of CRC Error counter reached 5% of Total Packets Received - the anomaly severity is set to Warning. If the error rate crosses 7% the severity becomes Major. If the error rate crosses 10% the severity becomes Critical.

Understanding anomaly correlation

The anomaly correlation functionality identifies cause-and-effect relationships between various anomalies within a specific time frame. It examines attributes such as device, interface, and protocols to pinpoint the root cause anomaly. This root cause anomaly acts as the primary issue that triggers the secondary anomalies, known as correlated anomalies. This approach helps in pinpointing the root cause, enabling efficient resolution of related issues.

Root cause anomalies

A root cause anomaly is an anomaly that causes other anomalies, which are referred to as correlated anomalies. Resolving the root cause anomaly should resolve the correlated anomalies.

Correlated anomalies

When a root cause anomaly occurs, it can trigger additional issues within Nexus Dashboard, known as correlated anomalies. These correlated anomalies arise specifically because the root cause anomaly creates effects or disruptions. As a result, you must identify and address the root cause anomaly to prevent or resolve the correlated anomalies that may follow.

With Nexus Dashboard 4.2.1, anomaly correlation now supports route events for both NX-OS switches and ACI fabric environments, providing more comprehensive root cause analysis across

your network infrastructure. For each correlated anomaly, Nexus Dashboard assigns a confidence score between 50% and 100% to indicate how certain it is about the root cause relationship. Higher scores reflect stronger evidence of correlation.

When you investigate correlated anomalies, you can use the new analysis filters to focus on specific event types. Nexus Dashboard also displays the last seen time for each anomaly, providing you with helpful context about issue persistence.

The following are common examples of parent (root cause) and child (correlated) anomaly relationships:

- Admin shut event (Parent) and AM Route Delete event (Child)
- Interface Down (Parent) and AM Route Delete event (Child)
- OSPF Neighbor Lost (Parent) and OSPF Route Delete event (Child)
- AM/OSPF Route Delete event (Parent) and BGP Neighbor Down (Child)
- BGP Neighbor Down (Parent) and BGP Route Delete event (Child)
- Route Delete event (Parent) to Service Endpoint Traffic Score Unhealthy (Forward drop)
- Route Delete event (Parent) to Endpoint Traffic Score Unhealthy (Forward drop)



- **AM route** refers to a route learned through the Adjacency Manager.
- In ACI fabrics, the auto-state feature controls the Switch Virtual Interface (SVI) down behavior and is disabled by default. When Nexus Dashboard disables auto-state, the SVI stays up even if the underlying interface goes down. This behavior can impact anomaly correlation and root cause analysis because the SVI status may not accurately reflect the actual state of the underlying interfaces. To improve accuracy in anomaly correlation and root cause analysis, enable the auto-state feature on the L3Out SVIs.

Uncorrelated anomalies

An uncorrelated anomaly neither causes correlated anomalies nor results from a root cause anomaly. Therefore, it does not affect any other anomalies. You must resolve each uncorrelated anomaly individually.

An uncorrelated anomaly can also be an anomaly that Nexus Dashboard does not yet evaluate for correlated anomalies. Nexus Dashboard will be able to evaluate these anomalies for correlated anomalies in a future release.

Anomaly levels

Anomalies are classified into the following levels based on their severity and impact.

- **Critical**—Anomalies are shown as critical when the network is down. Some of the examples include:
  - When connectivity to a given prefix or endpoint is lost
  - When a fabric or switch is not operational.
- **Major**—Anomalies are shown as major when connectivity to a given prefix or endpoint could be

compromised. An example includes:

  - Overlapping IP addresses or subnets

- **Minor**—Anomalies are classified as minor when they represent less severe issues that do not immediately impact network connectivity but may require attention. Examples include:
  - Interface errors or packet drops below threshold
  - Non-critical hardware component warnings
- **Warning**—Anomalies are shown as warnings when there are best practice violations or when components such as power supply units (PSUs) are non-redundant.

Anomaly properties

You can configure these properties on an anomaly:

- Assign a user
- Add tags
- Add a comment
- Set verification status
- Acknowledge an anomaly so that the acknowledged anomalies are not displayed in the **Anomalies** table

For more information, see Configure anomaly properties.

You can acknowledge anomalies in these ways.

- Manually acknowledge an anomaly. See Configure anomaly properties.
- Manually acknowledge multiple anomalies. See Analyze anomalies.
- Use anomaly rules to automatically acknowledge anomalies matching anomaly rules. See Create anomaly rules.

Navigate to Anomalies

You can efficiently monitor and investigate anomalies in Nexus Dashboard at different levels such as across all fabrics, for a specific fabric, for a specific switch, or for system-wide anomalies. Use the following methods to access anomaly details.

View all anomalies across all fabrics

Follow these steps to view all anomalies across all fabrics.

1. Navigate to **Analyze** > **Anomalies**.

   This displays all anomalies detected across all fabrics in your environment.

View anomalies for a single fabric

Follow these steps to view the anomalies for a single fabric.

1. Navigate to **Home** > **Overview**.
2. Choose online fabrics or snapshot fabrics from the drop-down list.
3. Click the **Anomaly level** card.
4. In the **Anomalies** page, click **Analyze Anomalies** to view detailed information for the selected fabric.
5. You can also view the anomalies for a single fabric in the **Fabrics Overview** page.
   a. Navigate to **Manage** > **Fabrics**.
   b. Choose an appropriate fabric.

      The **Fabrics Overview** page displays.

   c. Click the **Anomalies** tab to view anomalies specific to that fabric.

View anomalies for a single switch

Follow these steps to view the anomalies for a single switch in the **Inventory** page.

1. Navigate to **Manage** > **Inventory**.
2. Choose online fabrics or snapshot fabrics from the drop-down list.
3. Choose a switch.

   The **Switch Overview** page displays.

4. Click the **Anomalies** tab.

View system anomalies

Follow these steps to view the system anomalies.

1. Navigate to **Admin** > **System Status**.
2. Click the **Anomalies** tab.

   See Reviewing System Status for Your Nexus Dashboard for more information.

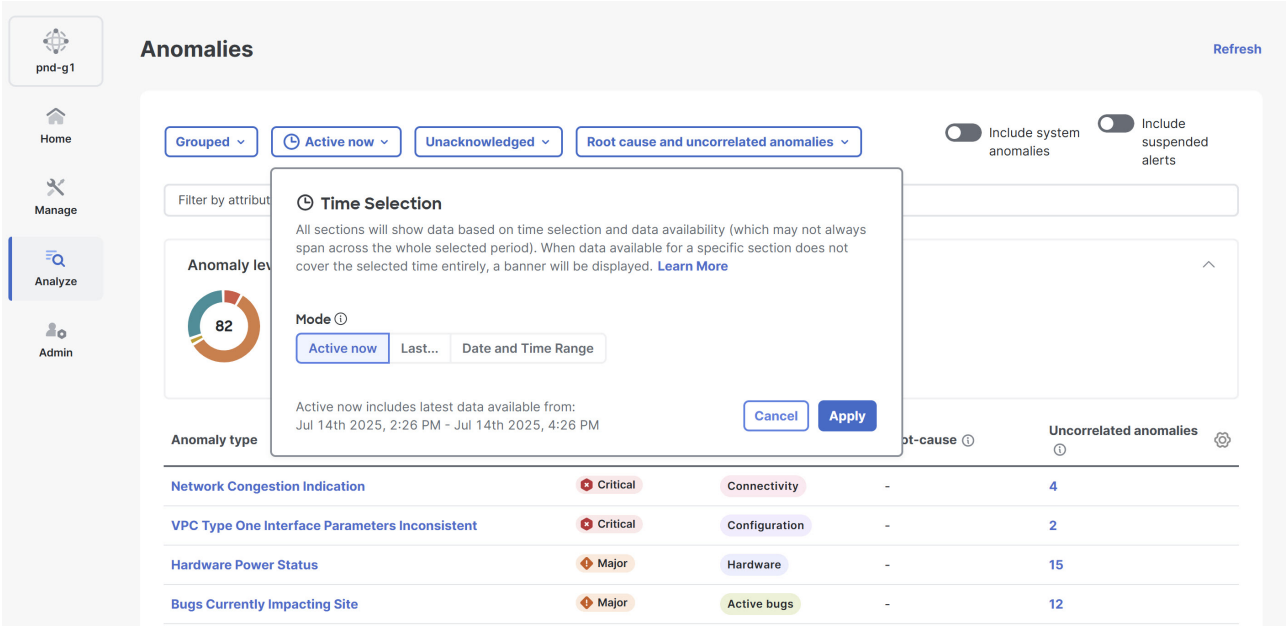
Analyze anomalies

Follow these steps to analyze anomalies.

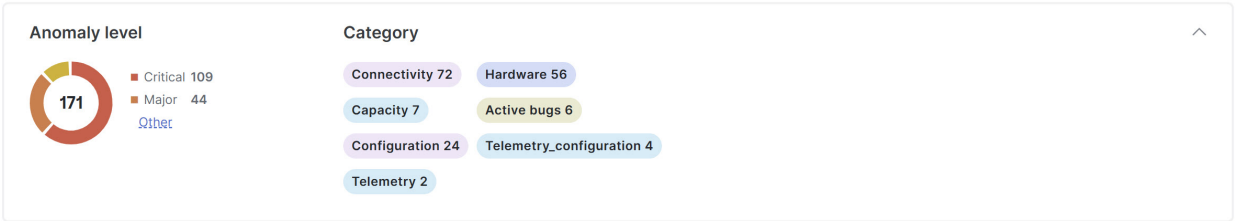
1. Navigate to Anomalies.
2. From the drop-down list, choose **Grouped**, **Ungrouped**, or **Root events**.
   - The **Ungrouped** view displays the individual anomalies raised for your fabrics.
   - The **Grouped** view displays the aggregated view of the anomalies based on the anomaly type.
   - The **Root events** table displays root events that cause dependent anomalies. You can view root events until Nexus Dashboard deletes them, which happens only after it deletes all the associated dependent anomalies.
3. Go to **Active now > Time Selection** to choose the date and time range. By default, **Active now** is

chosen. You can customize the date and time range to determine the data displayed in the **Anomalies** table.

The **Anomalies** page displays the anomalies by level and category for your fabrics, based on the chosen time range.



- The **Anomaly level** donut chart displays the total number of anomalies of Critical, Major, Minor, and Warning severities.
- The **Category** list displays the number of anomalies grouped by various categories, such as Hardware, Capacity, Compliance, Connectivity, Configuration, GPU, Integrations, Active bugs, Telemetry configuration, and System.



- For snapshot fabrics, the anomalies shown represent all detected anomalies across all snapshots, not just those from the latest snapshot.

4. If you want to include system anomalies in the **Anomalies** table, click the **Include system anomalies** toggle button. Note that the **System** category appears in the **Category** list only when you enable the **Include system anomalies** toggle button.

   For more information, see View platform and system alerts in global anomalies table.

5. If you want to include suspended alerts, click the **Include suspended alerts** toggle button.

   For more information, see Alerts suspend mode for anomalies and advisories.

6. Use the filter field to filter the anomalies. You can filter affected objects such as interface, VRF instance, EPG, or BD and view the associated anomalies.

   a. When you view the ungrouped anomalies, you can use the drop-down list next to the filter field to filter for unacknowledged or acknowledged anomalies. The default is

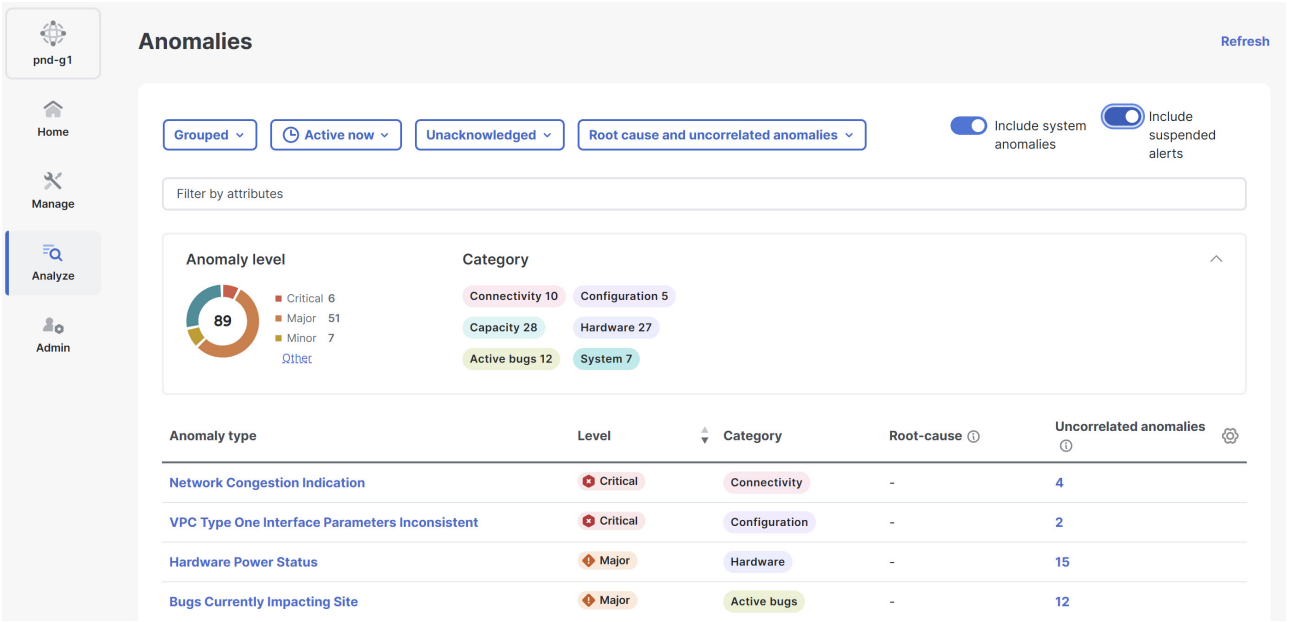
Unacknowledged.

b. You can use the drop-down list next to the unacknowledged and acknowledged anomalies drop-down list to filter by root cause and uncorrelated anomalies, root cause anomalies only, uncorrelated anomalies only, or all anomaly types. The default is **All anomaly types**.

   For more information about the filters, see Anomaly filters.

7. The **Anomalies** table displays the filtered anomalies. By default, the anomalies are sorted by level. Click the column heading to sort the anomalies in the table.

   When you view the ungrouped anomalies and configure the table to display the **Status** column, the status appears as either **Active** or **Cleared**. An **Active** status means the anomaly is present in your network, while a **Cleared** status means the anomaly is no longer present.



8. Click the gear icon to configure which columns display in the **Anomalies** table.

   By default, the columns **Anomaly type**, **Level**, **Category**, **Root-cause**, and **Uncorrelated anomalies** are displayed for grouped anomalies. The **Root-cause** column shows how many anomalies in that group are root cause anomalies.

   By default, the columns **What's wrong**, **Level**, **Category**, **Fabric**, **Detection time**, and **Correlated anomalies/events** are displayed for ungrouped anomalies.

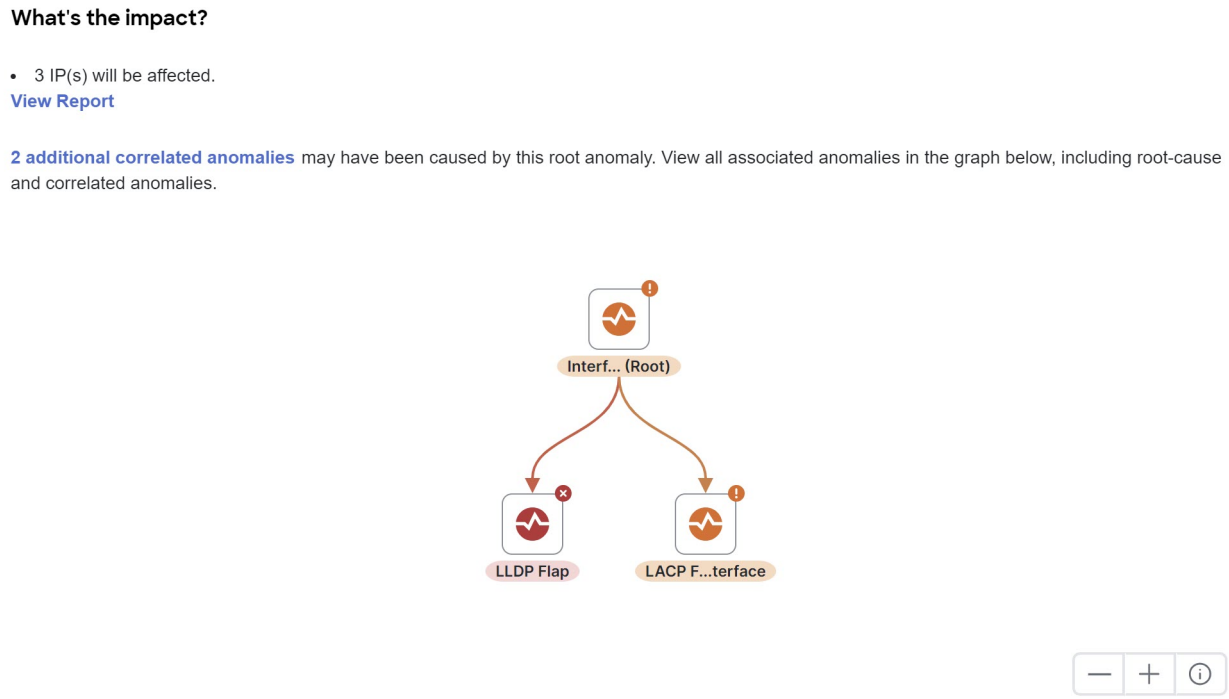
9. Click an anomaly to view more information.

   The *Anomaly Name* page displays these details.

   - **What's wrong?**—provides a problem description with the specific affected objects.
   - **What triggered this anomaly?**—provides the primary source of the anomaly, including a link that you can click to see information about it. This area includes a graph that shows the root cause anomaly and all correlated anomalies. You can click an anomaly in the graph to get more information about that anomaly. The controls at the lower right of the area enable you to zoom the graph in or out and view the topology legend. This area appears only for correlated anomalies.

- **What's the impact?**—explains the potential impact if the problem is not fixed. If the anomaly is a root cause, it also shows the number of correlated anomalies. You can click this number to view a table listing those correlated anomalies.

  For root cause anomalies, this area includes a graph that shows the root cause anomaly and all correlated anomalies. You can click an anomaly in the graph to get more information about that anomaly. The controls at the lower right of the area enable you to zoom the graph in or out and view the topology legend.

  When you view the correlated anomalies page and you configure the table to display the **Status** column, the status can be **Active**, **Cleared**, or **Deleted**. The **Active** status indicates that the anomaly is present in your network. The **Cleared** status indicates that the anomaly is not present in your network anymore. The **Deleted** status indicates that the system deleted the anomaly from the anomalies database due to being aged out, but the anomaly is not yet deleted from this page because some of its correlated anomalies still exist.

- **How do I fix it?**—provides prescriptive recommendations.

10. From the drop-down list in the **Anomalies** page, choose **Ungrouped**.
    a. Choose anomalies from the **Anomalies** table and click **Acknowledge anomalies** to acknowledge the anomalies.
    b. You can also click an anomaly, then click the ellipses (...) next to each anomaly, and choose **Acknowledge anomaly** from the drop-down list.

       By default, all the unacknowledged anomalies are displayed in the **Anomalies** table. After you acknowledge an anomaly, choose **Acknowledged** from the drop-down list to view all the acknowledged anomalies.

Resolve streaming anomalies on switches

When telemetry streaming from switches stops for more than five minutes, you can use Nexus Dashboard to identify the root cause and restore telemetry data flow. Restoring telemetry enables you

to regain critical visibility into switch health and performance metrics for both ACI and NX-OS switches.

Switch anomaly for ACI

In ACI fabrics, streaming telemetry anomalies occur when Nexus Dashboard does not receive telemetry data from a switch for more than five minutes. This interruption causes a loss of visibility into the switch's operational status, interfaces, capacity, hardware resources, and endpoints.

Some symptoms include:
* The switch does not send telemetry data for over five minutes.
* Nexus Dashboard loses visibility of the affected switch.
* Telemetry data, such as interface status, capacity, and hardware resources are not updated.

Follow these steps to resolve streaming anomalies on ACI switches.

1. Verify that telemetry is enabled on the fabric and not paused. Use the management interface or relevant configuration settings to confirm.
2. Use CLI or management tools to ensure the switch is operating without errors and all necessary processes are running.
3. Check connectivity between the switch inband or out-of-band (OOB) interfaces and the data interfaces. If a firewall exists in the network path, verify that all required ports are open and accessible.
4. Confirm that all services within the Nexus Dashboard cluster are operational and that no system anomalies or errors affect telemetry data collection.
5. Determine whether other switches in the fabric are experiencing similar issues to help identify common causes or patterns.
6. Briefly pause telemetry streaming, wait a few seconds, and then re-enable it to reset data flow and resolve transient issues using Nexus Dashboard.
7. If the issue persists after completing these steps, contact Cisco Technical Assistance Center (TAC) for further troubleshooting and support.

Switch anomaly for NX-OS

Streaming telemetry anomalies on standalone NX-OS switches occur when Nexus Dashboard does not receive telemetry data for more than five minutes, similar to ACI fabrics. As a result, Nexus Dashboard loses visibility into the switch status and telemetry information. Some symptoms include:

- The switch does not send telemetry data for over five minutes
- Nexus Dashboard loses visibility of the affected switch
- Telemetry data, such as interface status, capacity, and hardware resources, does not update

Follow these steps to resolve streaming anomalies on NX-OS switches.

1. On the affected NX-OS switch, run the **show telemetry transport** command to identify the receiver IP address.
2. Confirm that the receiver IP address is reachable from the switch.
3. Check network connectivity between the switch and Nexus Dashboard cluster nodes.

4. Verify that telemetry is enabled and active on the switch using the command 'show running-config telemetry'.
5. In the Nexus Dashboard, navigate to **Admin** > **System Status** > **Telemetry** > **Switches** and confirm the telemetry configuration status.
6. On the switch CLI, use the **show running telemetry** and **show telemetry transport** commands to verify the configuration.
7. Use CLI or management tools to ensure the switch is operating without errors and all necessary processes are running.
8. Confirm connectivity between the switch inband or out-of-band (OOB) interfaces and Nexus Dashboard data interfaces. Ensure firewall rules allow required ports as per Cisco guidelines.
9. Confirm that all Nexus Dashboard cluster services are operational and that no system anomalies or errors affect telemetry data collection.
10. Check whether other NX-OS switches in the fabric are experiencing the same issue to identify common causes or patterns.
11. Briefly pause telemetry streaming, wait a few seconds, and then re-enable it to reset data flow and resolve transient issues.
12. If the issue persists after completing these steps, contact Cisco Technical Assistance Center (TAC) for further troubleshooting and support.

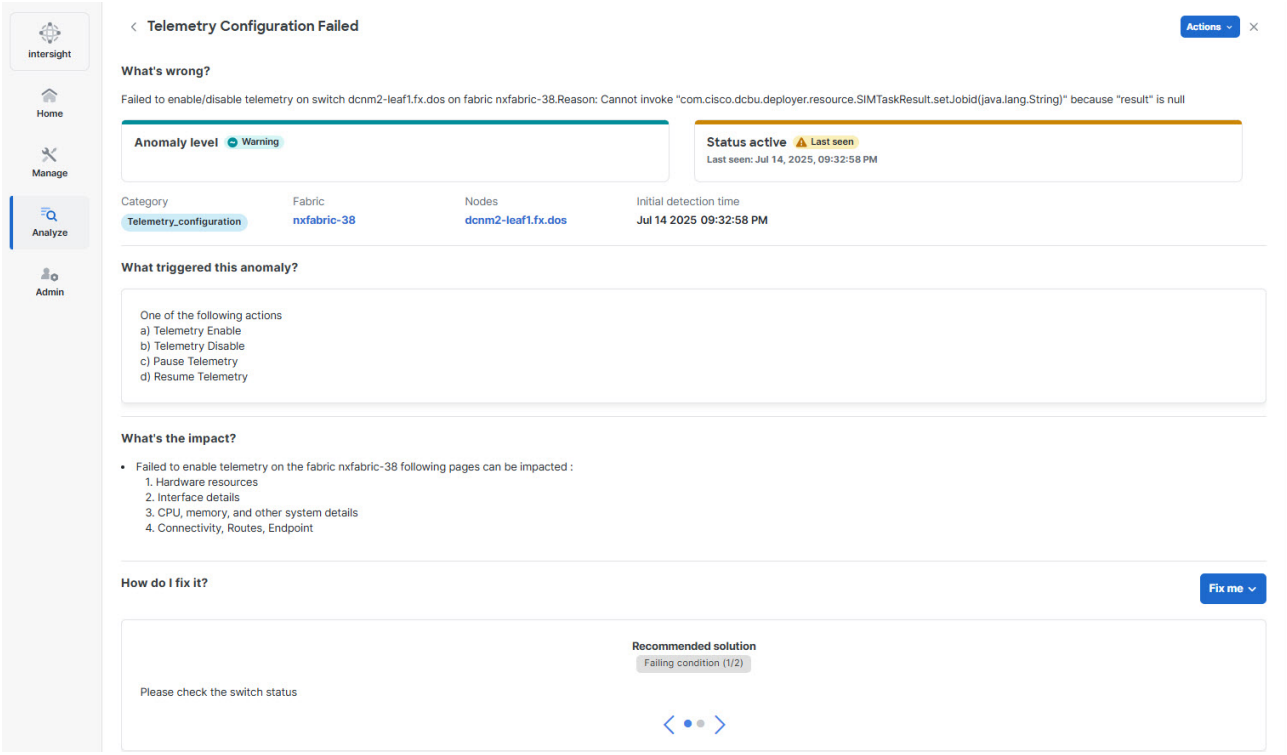
Resolve telemetry configuration anomalies on switches

Policy gateway anomalies are categorized under **Telemetry configuration**. If telemetry configuration fails on a switch, you can resolve the issue using the **Fix me** option available in the **How do I fix it?** section in the **Telemetry Configuration Failed** page. This option helps to systematically resolve telemetry configuration anomalies and restore normal telemetry operations on affected switches.

Follow these steps to resolve the telemetry configuration anomalies.

1. In the **Anomalies** table, click a **Telemetry configuration** anomaly.

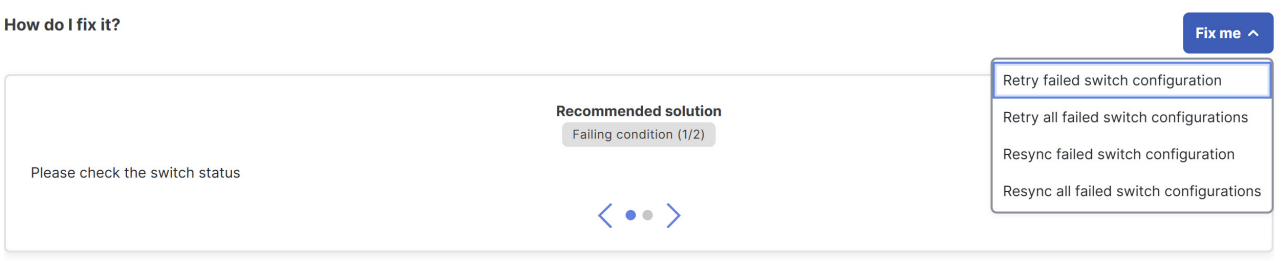
   The **Telemetry Configuration Failed** page displays.



2. In the **How do I fix it?** section, click the **Fix me** drop-down list.

   You can view these options.

Field	Description
Retry failed switch configuration	Attempts to re-apply the configuration only on the switch associated with the anomaly that the user is interacting with.
Retry all failed switch configuration	Attempts to re-apply the configuration on all switches that have failed telemetry configuration. This option does not remove any stale or failed configurations on the affected switches, it only attempts to reconfigure the telemetry configurations on the failed switches.
Resync failed switch configuration	Synchronizes and re-applies the configuration exclusively on the switch associated with the anomaly that the user is interacting with.
Resync all failed switch configuration	Synchronizes and re-applies telemetry configurations on all switches with any failed telemetry configuration.



3. Choose one of these options from the **Fix me** drop-down list to resolve telemetry configuration anomalies.

View platform and system alerts in global anomalies table

Anomalies that affect a Nexus Dashboard cluster but are not necessarily associated with a fabric are referred to as system anomalies. These anomalies can include issues such as hardware malfunctions, capacity constraints, compliance violations, connectivity disruptions, configuration errors, and active bugs. Enabling system anomalies allows you to identify the root cause, improve network health, and enhance operational efficiency.

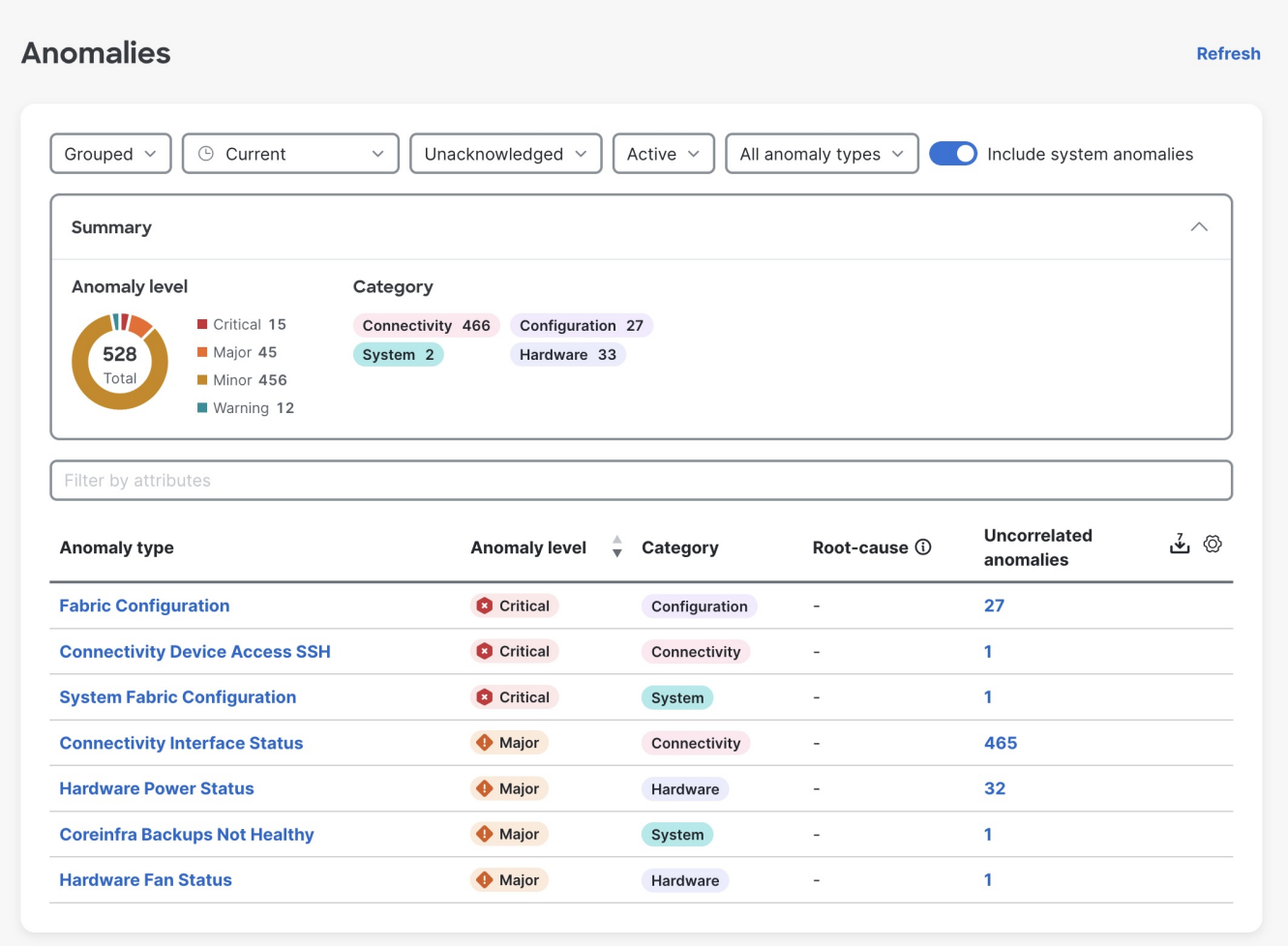
Follow these steps to view platform and system alerts in global anomalies table.

1. Navigate to **Analyze > Anomalies**.

   The **Anomalies** page displays.

2. Click the **Include system anomalies** toggle button in the top-right corner, to include system-related anomalies in the **Anomalies** table.

   Once enabled, the **System** category appears under anomalies by category in the **Anomalies** page.



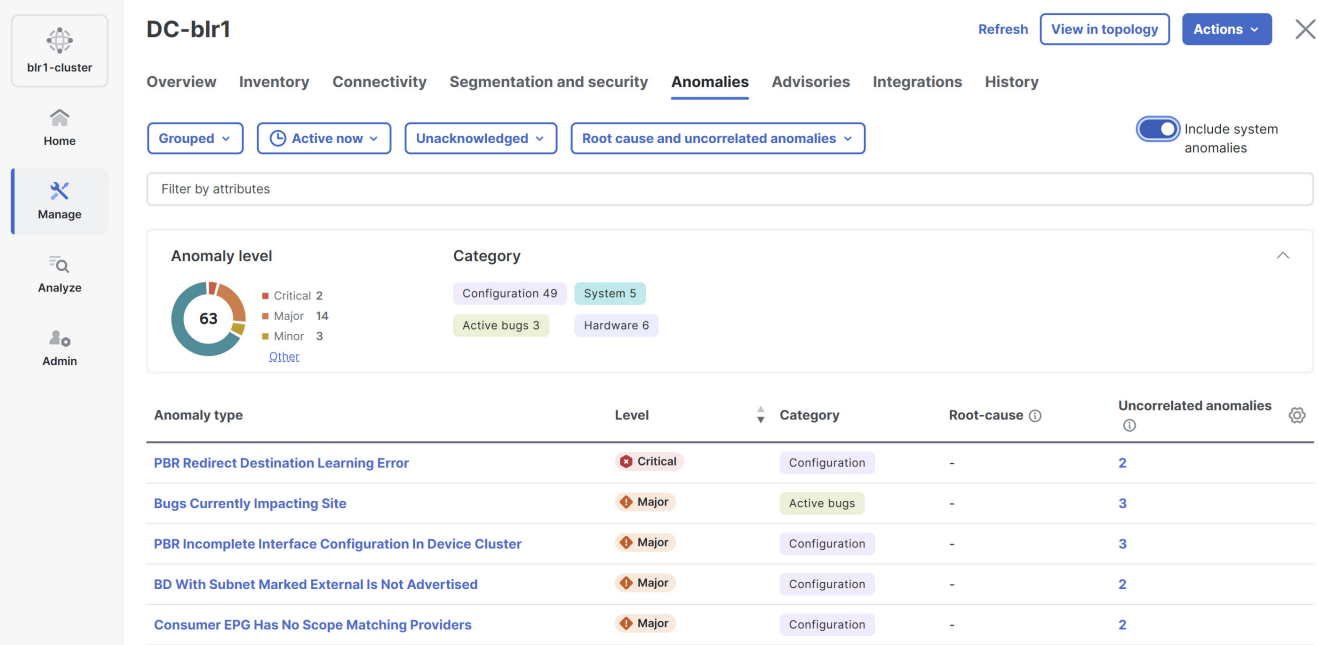
Follow these steps to include system-related anomalies at fabric level.

1. Navigate to **Manage > Fabrics**.
2. In the **Fabrics** page, choose the appropriate fabric.

The **Fabric Overview** page displays.

3. In the **Fabric Overview** page, click the **Anomalies** tab.
4. Click the **Include system anomalies** toggle button in the top-right corner, to include system-related anomalies in the **Anomalies** table.

   Once enabled, the **System** category appears in the anomalies by category card in the **Anomalies** page.



System anomaly notification

When an active system anomaly impacts the cluster health, a notification alert appears on the **Notifications** bell icon located in the common navigation bar at the top of the page. Click the notification bell icon to open the **Notifications** pane. In the **Notifications** pane, click **View system anomalies**. Nexus Dashboard redirects you to the **System Status** page, where you can review the full list of current and past system anomalies in the **Anomalies** table.

Nexus Dashboard will not display a notification alert if the cluster health is not affected.

Guidelines and limitations for anomalies

- Nexus Dashboard does not display certain anomalies in the **Anomalies** page by default in the following scenarios.
  - Nexus Dashboard does not display anomalies that belong to the **System** category in the **Anomalies** page by default.
  - If there is a collection or login failure:
    - When you navigate to **Admin > System Settings > System Status Details**, the **Assurance** status diplays as **Healthy**.
    - When you navigate to **Admin > System Settings > System Issues**, Nexus Dashboard does not display anomalies related to collection or login failures.

Follow these steps to view system anomalies.

1. Navigate to **Analyze** > **Anomalies**.
2. Select **Online Fabrics** from the drop-down list.
3. Select **Ungrouped** from the All Anomalies drop-down list.
4. Use the search bar to filter on category == system. All system anomalies are displayed in the anomalies table.

- For any fabric, the data is purged in either of the following scenarios:
  - After the thirty day retention period
  - When the storage threshold is reached

    As a result, the anomalies and advisories for that fabric are not displayed. You have to rerun the analysis to view the anomalies and advisories.
- In Nexus Dashboard, invalid and stale alarms are periodically cleared every 24 hours.
- When you upgrade a device, there may be instances where traps are not sent or received by the Nexus Dashboard, resulting in anomalies not being raised or cleared."

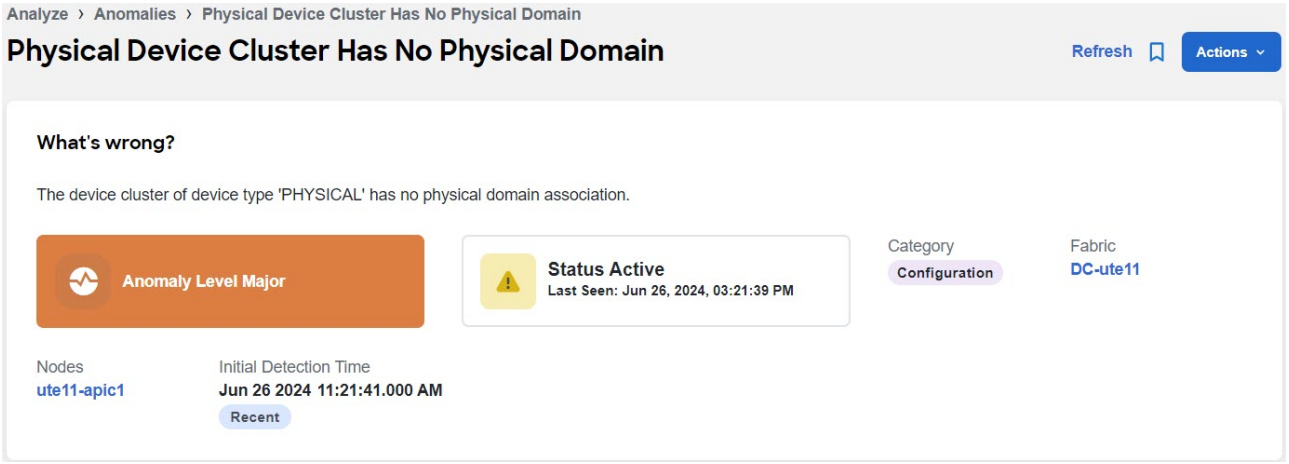
Configure anomaly properties

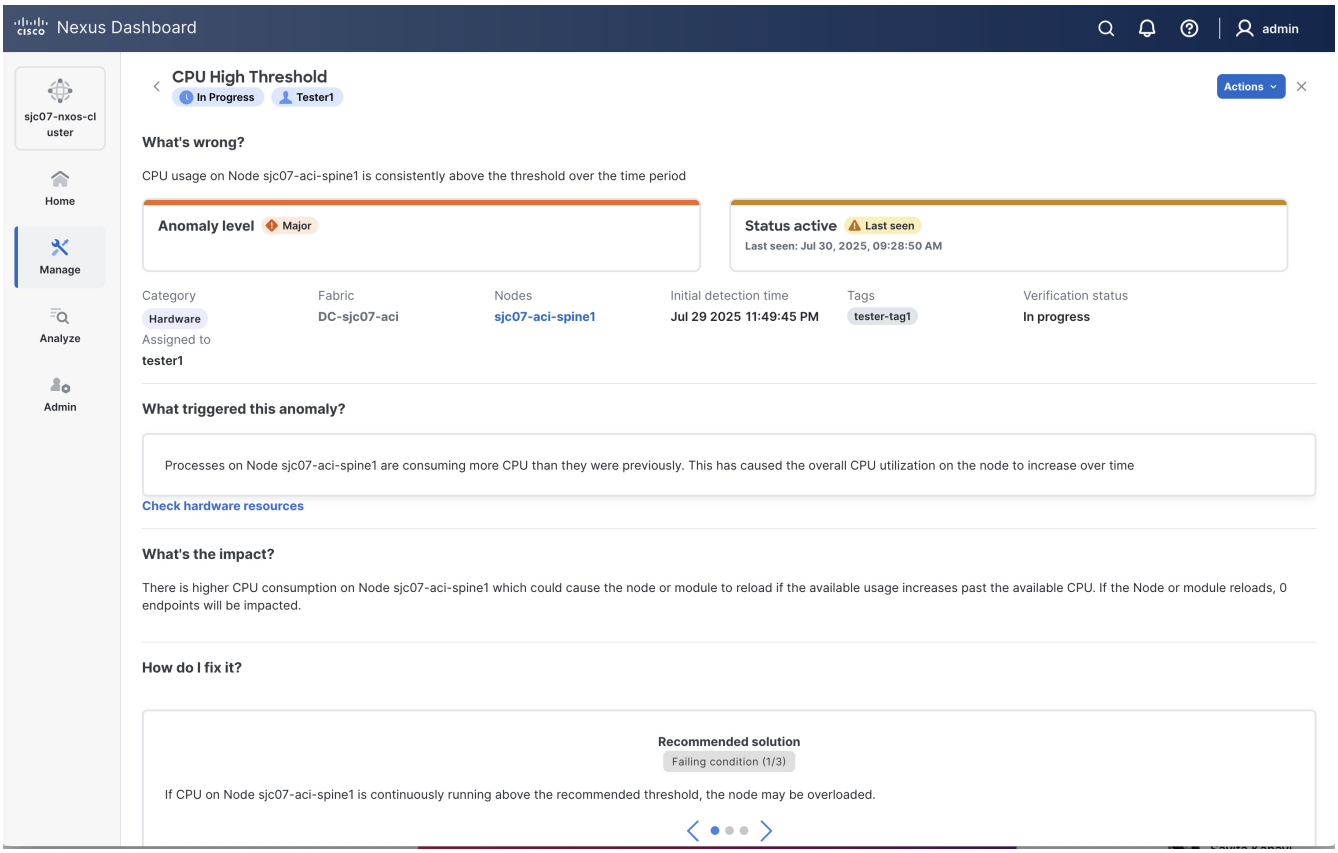
Follow these steps to configure properties for an anomaly.

1. Navigate to **Analyze** > **Anomalies**.
2. Choose **Online fabrics** or **Snapshot fabrics** from the drop-down list.
3. From the Anomalies drop-down list, choose **Ungrouped**.

   The Ungrouped view displays the individual anomalies raised for your fabrics.
4. From the **Time Selection** dialog, choose the desired mode, then click **Apply**. The default is **Active Now**.
   - For **Last...**, you must also choose a period.
   - For **Date and Time Range**, you must also choose the range.
5. Click an anomaly from the table and then choose a property from the **Actions** drop-down list.
   a. Choose **Acknowledge Anomaly** to acknowledge an anomaly. By default all the unacknowledged anomalies are displayed in the anomalies table. After you acknowledge an anomaly, choose Acknowledged from the drop-down list to view all the acknowledged anomalies.
   b. Choose **Verification Status** to set a user defined status such a New, In Progress, or Closed to an anomaly. Choose a status from the drop-down list and click **Save**.
   c. Choose **Assigned To** to assign an anomaly to an user. Enter the username and click **Save**.
   d. Choose **Comment** to assign a comment to an anomaly. Enter a comment and click **Save**.
   e. Choose **Manage Tags** to add user-defined tags to an anomaly. Enter the tag name and click **Save**. You can enter multiple tags. After entering the tag name, press Enter.
6. To acknowledge multiple anomalies, select the anomalies. Click **Acknowledge anomalies**.

7. To view the the properties assigned to an anomaly, click an anomaly to view the Anomaly page. In the Anomaly page, properties such as **Verification Status**, **Acknowledge**, and **Assigned To** are displayed. To view comments and tags assigned to an anomaly, from the **Actions** menu, choose **Comment** or **Manage Tags**.





- When you acknowledge an anomaly using the **Actions** menu, it will override any of the properties you have configured on an individual anomaly using the ellipsis icon in the **Anomalies** table.
- You must refresh the timeline range to view the configured properties on an anomaly.
- All the properties configured on an anomaly are only applicable to future analysis.
- To view an active anomaly for snapshot fabric analysis, you must select the time range when the analysis was created.

Anomaly filters

The filter field allows you to filter the table of anomalies when viewing the ungrouped anomalies, or filter the table of anomaly types when viewing the grouped anomalies.

In the Anomalies page, you can use the following filters to refine entries in the table:

- Anomaly Type – Display anomalies with a specific type.
- Assigned To – (Ungrouped, only) Display anomalies assigned to a specific user.
- BD – Display anomalies with a specific bridge domain.
- Category – Display anomalies from a specific category.
- Check code – (Ungrouped, only) Display anomalies with a specific check code.
- Cleared Time – (Ungrouped, only) Display anomalies with a specific cleared time.
- Comment – (Ungrouped, only) Display anomalies with a specific comment.
- Detection Time – (Ungrouped, only) Display anomalies with a specific detection time.
- EPG – Display anomalies with a specific EPG.
- Fabric – (Ungrouped, only) Display anomalies for a specific fabric.
- Interface – Display anomalies with a specific interface.
- IP address – (Ungrouped, only) Display anomalies with a specific IP address.
- Last Seen Time – (Ungrouped, only) Display anomalies with a specific last seen time. Last Seen Time indicates the time the anomaly was updated while under active status. If the status of the anomaly is not cleared, then the anomaly is active.
- Level – Display anomalies of a specific level.
- MAC address – Display anomalies with a MAC address.
- Nodes – Display anomalies for specific nodes.
- Status – Displays anomalies that have the specified status.
- Tags – (Ungrouped, only) Display anomalies with a specific tag.
- VPC – Display anomalies with a specific virtual port channel (vPC).
- VRF – (Ungrouped, only) Display anomalies with a specific virtual routing and forwarding (VRF) instance.
- Verification Status – (Ungrouped, only) Display anomalies with a specific verification status.
- What's Wrong – (Ungrouped, only) Displays anomalies of a specific affected object.

As a secondary filter refinement, use the following operators:

- == – With the initial filter type, this operator, and a subsequent value, returns an exact match. This operator is available for all filters.
- != – With the initial filter type, this operator, and a subsequent value, returns all that do not have the same value. This operator is available for most filters.
- contains – With the initial filter type, this operator, and a subsequent value, returns all that contain the value. This operator is available for some filters.

- !contains – With the initial filter type, this operator, and a subsequent value, returns all that do not contain the value. This operator is available for some filters.

Filtering for acknowledged or unacknowledged anomalies

This drop-down menu next to the filter field enables you to filter the anomalies the unackowledged or ackowledged status. Choose **Acknowledged** to filter out unackowledged anomalies. Choose **Unacknowledged** to filter out ackowledged anomalies.

Filtering for root cause and uncorrelated anomalies

This drop-down menu near to the filter field enables you to filter for root cause and uncorrelated anomalies, which filters the table of anomalies accordingly.

You can choose the following filters:

- **Root Cause and Uncorrelated Anomalies** – The table displays root cause anomalies and uncorrelated anomalies, but not correlated anomalies. This is the default value because it shows only the anomalies that you must manually resolve. If you resolve the root cause anomalies, then the correlated anomalies also get resolved. Because of this, it is not as important for you to see the correlated anomalies.
- **Root Cause Anomalies Only** – The table displays only root cause anomalies.
- **Uncorrelated Anomalies** – The table displays only uncorrelated anomalies.
- **All Anomaly Types** – The table displays all anomalies.

Determine the primary affected object for an anomaly

To filter for anomalies using a combination of affected object filters, such as IP address, MAC address, interface, VPC, EPG, and VRF, all the provided filter objects should be a primary affected object for any given anomaly. The filter will not return results if the query contains non-primary affected objects.

Follow these steps to determine the primary affected object for a particular anomaly.

1. To determine the primary affected object for a particular anomaly, navigate to **Analyze > Anomalies**.
   a. To determine the object from the ungrouped anomalies, choose **Ungrouped** from the drop-down menu.
   b. To determine the object from the grouped anomalies, choose **Grouped** from the drop-down menu, then click the desired anomaly type in the table.
2. Choose an anomaly from the **Anomalies** table.
3. In the **What's the impact?** area, the primary affected objects are highlighted in bold.

Global rules

Global rules page enables you to see which anomaly levels are enabled for the different anomaly categories. You can also customize the thresholds that determine whether an anomaly is assigned the warning, major, or critical level.

Customize anomaly level thresholds

Follow these steps to customize anomaly level thresholds.

1. Navigate to **Manage** > **Anomaly and Compliance Rules** > **Global Rules**.
2. Locate the row with the anomaly category that you want to customize, then click the entry in the **Status** column on that row.

   These are the anomaly categories that you can customize in **Global Rules** - the threshold customizations that are available differ for each of the anomaly categories:

   - Capacity
   - Hardware
   - Connectivity
   - GPU

Capacity

This information applies if **Capacity** is the entry in the **Anomaly Category** column and you click the entry in the **Status** column on that row.

1. In the **Customize thresholds for capacity anomalies** table, find the anomaly whose thresholds you want to customize and click the edit (pencil) icon.

   The **Customize thresholds for capacity anomalies** table can have multiple pages. If necessary, use the page controls at the bottom of the table to find the desired anomaly.

2. Enter the desired percent for each anomaly level, then click the green check mark.

   After you customize the thresholds, Nexus Dashboard recalculates the anomaly levels of existing anomalies, which takes approximately 30 minutes to complete.

   You can click **Reset** to reset the values to their default or **X** to cancel the edit.

   - The values can be from 0 to 100. A value of 0 indicates Nexus Dashboard will not raise any anomalies for that severity. If you enter 0 for all of the severities, Nexus Dashboard suppresses the anomaly completely.
   - The value for **Warning** must be lower than the value for **Major**, and the value for **Major** must be lower than the value for **Critical**.
   - The value defined for **Major** sets the upper end limit of the range defined for **Warning**, and the value defined for **Critical** sets the upper end limit of the range defined for **Major**.

Hardware

This information applies if **Hardware** is the entry in the **Anomaly Category** column and you click the entry in the **Status** column on that row.

In the **Customize Hardware** page, choose the appropriate category:

- Fabric Management
- Telemetry

Fabric Management

The **Fabric Management Anomaly Thresholds** option under **Hardware** is available for NX-OS fabrics only.

1. In the **Fabric Management Anomaly Thresholds** table, find the anomaly whose thresholds you want to customize and click the edit (pencil) icon.

   The **Fabric Management Anomaly Thresholds** table can have multiple pages. If necessary, use the page controls at the bottom of the table to find the desired anomaly.

2. In the **Warning**, **Minor**, **Major**, and **Critical** columns, enter the desired percent for each anomaly level, then click the green check mark.
   - The values can be from 0 to 100. A value of 0 indicates Nexus Dashboard will not raise any anomalies for that severity. If you enter 0 for all of the severities, Nexus Dashboard suppresses the anomaly completely.
   - The value for **Warning** must be lower than the value for **Minor**, the value for **Minor** must be lower than the value for **Major**, and the value for **Major** must be lower than the value for **Critical**.
   - The value defined for **Minor** sets the upper end limit of the range defined for **Warning**, the value defined for **Major** sets the upper end limit of the range defined for **Minor**, and the value defined for **Critical** sets the upper end limit of the range defined for **Major**.
3. In the **Forwarding** column, determine if you want to enable forwarding using email, SNMP, or all, or leave the option set at **None** if you do not want to enable forwarding.

   After you customize the thresholds, Nexus Dashboard recalculates the anomaly levels of existing anomalies, which takes approximately 30 minutes to complete.

   You can click **Reset** to reset the values to their default or **X** to cancel the edit.

4. To enable notifications for the CPU, memory, power usage, or temperature anomaly types, locate the appropriate row and toggle the button in the **Enable** column to the on position.

   Toggle the button in the **Enable** column back to the off position to disable the appropriate notification.

Telemetry

1. In the **Customize thresholds for capacity anomalies** table, find the anomaly whose thresholds you want to customize and click the edit (pencil) icon.

   The **Customize thresholds for capacity anomalies** table can have multiple pages. If necessary, use the page controls at the bottom of the table to find the desired anomaly.

2. Enter the desired percent for each anomaly level, then click the green check mark.

   After you customize the thresholds, Nexus Dashboard recalculates the anomaly levels of existing anomalies, which takes approximately 30 minutes to complete.

   You can click **Reset** to reset the values to their default or **X** to cancel the edit.

   - The values can be from 0 to 100. A value of 0 indicates Nexus Dashboard will not raise any

anomalies for that severity. If you enter 0 for all of the severities, Nexus Dashboard suppresses the anomaly completely.

- The value for **Warning** must be lower than the value for **Major**, and the value for **Major** must be lower than the value for **Critical**.
- The value defined for **Major** sets the upper end limit of the range defined for **Warning**, and the value defined for **Critical** sets the upper end limit of the range defined for **Major**.

Connectivity

These areas are available under **Connectivity**:

- Fabric Management Anomaly Thresholds
- Interface Anomaly Option
- Syslog Rules

Fabric Management Anomaly Thresholds

The **Fabric Management Anomaly Thresholds** option under **Connectivity** is available for NX-OS fabrics only.

Follow these steps to customize anomaly thresholds and notification settings for NX-OS fabrics.

1. In the **Fabric Management Anomaly Thresholds** table, find the anomaly whose thresholds you want to customize and click the edit (pencil) icon.

   The **Fabric Management Anomaly Thresholds** table can have multiple pages. If necessary, use the page controls at the bottom of the table to find the desired anomaly.

2. In the **Warning**, **Minor**, **Major**, and **Critical** columns, enter the desired percent for each anomaly level, then click the green check mark.
   - The values can be from 0 to 100. A value of 0 indicates Nexus Dashboard will not raise any anomalies for that severity. If you enter 0 for all of the severities, Nexus Dashboard suppresses the anomaly completely.
   - The value for **Warning** must be lower than the value for **Minor**, the value for **Minor** must be lower than the value for **Major**, and the value for **Major** must be lower than the value for **Critical**.
   - The value defined for **Minor** sets the upper end limit of the range defined for **Warning**, the value defined for **Major** sets the upper end limit of the range defined for **Minor**, and the value defined for **Critical** sets the upper end limit of the range defined for **Major**.
3. In the **Forwarding** column, determine if you want to enable forwarding using email, SNMP, or all, or leave the option set at **None** if you do not want to enable forwarding.

   After you customize the thresholds, Nexus Dashboard recalculates the anomaly levels of existing anomalies, which takes approximately 30 minutes to complete.

   You can click **Reset** to reset the values to their default or **X** to cancel the edit.

4. To enable notifications for any of the anomaly types available under **Fabric Management Anomaly Thresholds**, locate the appropriate row and toggle the button in the **Enable** column to the on position.

Toggle the button in the **Enable** column back to the off position to disable the appropriate notification.

Interface Anomaly Option

Follow these steps to customize thresholds and notification settings for interface anomalies.

1. In the **Interface Anomaly Option** table, find the anomaly whose thresholds you want to customize and click the edit (pencil) icon.

   The **Interface Anomaly Option** table can have multiple pages. If necessary, use the page controls at the bottom of the table to find the desired anomaly.

   The **Edit Interface Anomaly Option** page appears.

2. In the **Edit Interface Anomaly Option** page, make the appropriate choices for the interface anomaly option:

   a. Toggle the button in the **Enable** field to the on position to enable this option, or in the off position to disable this option.

   b. In the **Forwarding** field, determine if you want to enable forwarding using email, SNMP, or all, or leave the option set at **None** if you do not want to enable forwarding.

   c. In the **Severity** field, determine if you want to set the severity threshold at **Minor**, **Major**, **Warning**, or **Critical**.

   d. Click **Save** to save the configured interface anomaly option.

   After you customize the thresholds, Nexus Dashboard recalculates the anomaly levels of existing anomalies, which takes approximately 30 minutes to complete.

Syslog Rules

Syslog Alarm Policy defines a pair of Syslog messages formats; one which raises the alarm, and one which clears the alarm.

Follow these steps to add a syslog rule.

1. Click **Add Syslog Rule**.

   The **Add Syslog Rule** page appears.

2. Enter the necessary information to add a syslog rule.

Field	Description
Identifier	Specify the identifier portions of the raise and clear messages.
Syslog Raise	Define the format of a syslog raise message. The syntax is as follows: Facility-Severity-Type: Message
Syslog Clear	Define the format of a syslog clear message. The syntax is as follows: Facility-Severity-Type: Message
Policy Name	Specify the name for this policy. It must be unique.
Policy Details	Specify a brief description for this policy.

Field	Description
Forwarding	Determine if you want to enable forwarding using email, SNMP, or all, or leave the option set at **None** if you do not want to enable forwarding
Severity	Determine if you want to set the severity threshold at **Minor**, **Major**, **Warning**, or **Critical**.
What is wrong	Enter text that describes what went wrong.
What triggered it	Enter text that describes what went triggered the alarm.
What's the impact	Enter text that describes what the impact is.
How do I fix it?	Enter text that describes how to fix the issue.

3. Determine how you want to proceed after entering the information for the syslog rule.
    - Click **Save and Add New** to save the information for this syslog rule and to add another syslog rule
    - Click **Save** to save the information for this syslog rule and exit the page
    - Click **Cancel** to exit out of the page without saving

GPU

To customize GPU anomaly thresholds, locate a row with "GPU" in the **Anomaly Category** column and click the entry in the **Status** column.

Follow these steps to customize thresholds for GPU anomalies.

1. In the **Customize thresholds for GPU anomalies** table, find the anomaly whose thresholds you want to customize and click the edit (pencil) icon.

   The **Customize thresholds for GPU anomalies** table can have multiple pages. If necessary, use the page controls at the bottom of the table to find the desired anomaly.

2. Specify the desired percentage for each anomaly level, and click the green check mark.

   After you customize the thresholds, Nexus Dashboard recalculates the anomaly levels of existing anomalies, which takes approximately 30 minutes to complete.

   Click **Reset** to reset the values to their defaults or **X** to cancel the edit.

    - The values range from 0 to 100. A value of 0 indicates Nexus Dashboard will not raise any anomalies for that severity. If you enter 0 for all of the severities, Nexus Dashboard suppresses the anomaly completely.
    - The value for **Warning** must be lower than the value for **Major**, and the value for **Major** must be lower than the value for **Critical**.
    - The value defined for **Major** sets the upper limit of the range defined for **Warning**, and the value defined for **Critical** sets the upper limit of the range defined for **Major**.

Anomaly rules

Anomaly rules act on raised anomalies (even those based on global rules) to change properties of the

anomaly such as severity, acknowledge, and custom recommendation. These rules allow for wider match criteria options to control the properties of all supported anomaly types. You can also match an alert against an anomaly rule using the match criteria.

Anomaly rules also allow you to customize an anomaly by adding a custom message that will be displayed when an anomaly is raised based on the anomaly rule.

- An anomaly rule contains the match criteria required to match an anomaly against the rule and the action that should be applied on the matched anomaly.
- An anomaly rule can contain multiple match criteria.
- You can use attributes such as severity, category, anomaly title, and affected object match, to define the match criteria for the anomaly rule.



Affected object match is not available for all scopes including system.

- A match criteria can contain either single or multiple attributes. When there are multiple attributes, the **AND** operator is applied to all the attribute match conditions within a match criteria entry including the object matches.
- If an anomaly rule contains multiple match criteria, then the anomaly matching any of the match criteria will be seen as matching the rule and all the actions of the rule get applied on that anomaly. The **OR** operator will apply to the criteria.
- Anomaly rules using **Match Criteria** with **Object Match Rule** will only support the **Equals to** criteria.
- An Anomaly rule can be enabled only if it contains at least one match criteria.
- Anomaly rules are not supported for advisories.
- If you create multiple anomaly rules, an anomaly with actions of only the first rule that matches the criteria is applied. No further rules are considered once a rule is matched. The order of rules are listed in the **Anomaly rules** tab.
- If you specify multiple attributes in the match criteria entry of a rule, the conditions of each attribute must be met for the rule to be applied.
- If you specify multiple conditions for an attribute, any of the conditions must be met for the attribute to evaluate as true.
- If you specify multiple match criteria within an affected object, each criteria must be met.

In Nexus Dashboard 4.2.1, all matching options like fabric, category, title and relevant object matches for rule creation continue to be supported. Also, system anomaly titles have been added to allow users to create rules for system anomalies.

Additionally, the following new rule actions have been added:

- Override the default severity level of an anomaly based on specific match criteria, with support for applying changes to existing anomalies.
- Include the ability to apply changes to existing anomalies for all the supported actions. Instead of per-action option to apply changes to existing anomalies, this option will be per-rule and applies all actions of the rule to existing active anomalies.
- Rules are applied and validated while adhering to the hiding behavior when Alert Suspend is

enabled on a fabric.

- Centralized management of alert rules for all use cases improves extensibility for more match options and actions in a unified way.
- Support for alert rules based on system category.

Guidelines and limitations

- When you delete or disable an anomaly rule containing either the **Acknowledge** or **Customize Anomaly** action, all actions applied to active anomalies are reverted. This includes custom messages.
- Deleting or disabling an anomaly rule that includes the **Override Severity** action reverts the actions applied to active anomalies that were matched by that rule. Also, the anomaly severity is reset to the default highest severity applicable to that anomaly.
- The **Severity Override** action cannot be applied when severity is selected as a match criteria.
- When an anomaly rule is created or modified and the **Apply all actions to existing active anomalies** option is unchecked, the updates will not affect currently active anomalies. The updated rule will apply only to new anomalies or to existing anomalies when they receive further updates.
- When overlapping rules are created, the newest rule that is created takes precedence.
- Manual updates on an anomaly do not pass the alert rule match check and actions.
- Auto clear from source of an anomaly does pass the alert rule match check and action
- Any update of an anomaly caused by user-created **Anomaly alert rule** is not captured in the audit log.
- When you delete or disable an anomaly rule containing the **Customize Anomaly** action, the recommendations are still displayed in the **How do I fix it** area.
- You can only manually unacknowledge anomalies, including those that are automatically acknowledged by an anomaly rule. You cannot automatically unacknowledge these anomalies by disabling or deleting the anomaly rules.
- If you manually unacknowledge an anomaly that was previously acknowledged by an anomaly rule, re-applying the same anomaly rule (even with the **Apply to existing active anomalies** option checked) may not re-acknowledge that specific anomaly. In such cases, you need to manually acknowledge the anomaly.
- When you configure an anomaly rule with both **Acknowledge** and **Customize anomaly actions**, and check the **Apply to existing active anomalies** check box, the rule may not acknowledge active anomalies that were previously manually unacknowledged. However, the custom message action is applied to all existing active anomalies.

  For example, if you set a rule to acknowledge and add a custom message to *L3 QoS TCAM Threshold Exceeded* anomalies, the custom message appears on all the 8 existing anomalies. However, the rule acknowledges only 2 out of 8 anomalies, if the other 6 anomalies are unacknowledged manually earlier.

- Maximum anomaly rules supported across all fabrics is 500.
- In the following scenario, you cannot use an alert rule to automatically acknowledge existing active anomalies matching the match criteria by selecting the **Apply to existing active anomalies** check box in the **Create Anomaly Rule** page.

- An anomaly is raised before the alert rule is created and there are no further updates to the anomaly after the alert rule is created.

  In this scenario, you can manually acknowledge the anomalies. See Configure anomaly properties.

- After upgrading to this release, some anomaly rules may be updated or deleted. You can manually add these rules after the upgrade based on the new categories and severity.
- Anomaly rules using match criteria with an object match rule or code rule does not apply to anomalies with the one of the following categories: Active Bugs, Capacity, Hardware, Integrations, or Connectivity.

Create anomaly rules

Follow these steps to create custom anomaly rules.

1. Navigate to **Manage** > **Anomaly and Compliance Rules** > **Anomaly Rules**.
2. Click **Create Anomaly Rule**.
3. Complete the following fields for **General**.
   a. In the **Name** field, enter the name.
   b. In the **Description** field, enter the description.
   c. Choose the state to enable the rule to be active.

      If the state is enabled, the rule will be applied in the next analysis. If the state is disabled, the rule will not be applied during the next analysis.

   d. Click **Next**.
4. Complete the following fields for **Settings**.
   a. Click **Add Criteria** to define the match criteria for the anomaly rule.
   b. From the **Scope** drop-down list, select the fabric. Only the match criteria for the fabric running the analysis will be selected and matched with the alerts to perform the action.
   c. Select the attributes for the match criteria. You can use category, event title, object match rule, code rule, and severity to define the attribute for the match criteria. Select category and event title from the drop-down list.
   d. Click **Add Object Match Rule** to define the primary affected objects for the match criteria.

      To determine the primary affected objects, see Determine the primary affected object for an anomaly.

      If multiple affected objects are included in the match criteria, then the anomalies containing all the affected objects will be matched. If an anomaly rule contains multiple match criteria, then the anomalies containing the union of the match criteria will be matched.

e. Select severity from the drop-down list.

f. Click **Save**.

5. Complete the following fields for **Actions**.

   a. Use the toggle to choose **Acknowledge**.

   > Acknowledge enables you to acknowledge all new detected anomalies that match the criteria and adjust the anomaly score accordingly.

      i. Check **Apply to existing active anomalies** check-box to apply the anomaly rule to existing instance of the anomalies matching the alert anomaly. Uncheck the check-box to apply the anomaly rule to match to new instance of anomalies.

   b. Use the toggle to choose **Security level override**.

   > Customize Anomaly allows you to customize an anomaly by adding a custom message that will be displayed when an anomaly is raised based on the anomaly rule.

      i. Enter the recommendations to be displayed in the anomaly rule. You can create multiple rules based on different matching criteria to have more than one customized recommendation displayed in the anomaly rule. In the Anomaly page, the recommendations are displayed in the **How do I fix it?** area.

      ii. Check **Apply to existing active anomalies** check-box to apply the anomaly rule to existing instance of the anomalies matching the anomaly rule. Uncheck the check-box to apply the anomaly rule to match the new instance of anomalies.

   c. Use the toggle to choose **Severity level override**.

   d. If needed, you may **Add Custom Message**.

6. In the **Summary**, review your selections and click **Add Anomaly Rule**. The new anomaly rule is displayed in the **Anomaly Rule** table.

Manage anomaly rules

Follow these steps to manage anomaly rules in Nexus Dashboard.

1. Navigate to **Manage** > **Anomaly and Compliance Rules** > **Anomaly Rules**. The anomaly rules are displayed in the **Anomaly Rule** table.
2. Use the search bar to filter the rules based on Name, Actions, and State.
3. Select an anomaly rule and click **Edit Rule** to edit.
4. Select an anomaly rule and click **Delete Rule** to delete the rule from the system.
5. Select an anomaly rule and click ellipsis icon. Click **Enable** to enable the rule. If the state is enabled, the rule will be applied in the next analysis. Before enabling an anomaly rule make sure that at least one match criteria is present in the anomaly rule.
6. Select an anomaly rule and click ellipsis icon. Click **Disable** to disable the rule. If the state is disabled, the rule will not be applied during the next analysis.

Advisories

Nexus Dashboard identifies field notices, software and hardware end-of-life and end-of-sale announcements, as well as security advisories that can potentially impact the network fabrics that it is monitoring, and generate advisories. Advisories provides recommendations to keep your network under support and running in optimal conditions.

Advisories in Nexus Dashboard provide details of relevant impact from field notices, security advisories, EoL/EoS of hardware and software, and best practices. You can view the advisories by level and category for a particular fabric based on the selected time range.

Comprehensive security advisories that evaluate a range of device configurations, including specific product IDs (PIDs), SSH configurations, Bash configurations, and so on, require the **Advantage** tier subscription. **Essentials** tier subscribers receive security advisories based only on device software versions, such as a security advisory for an affected software version. For more information about bug scan, refer to the section "Collecting information on bugs that might affect your network using Bug scan" in Analyzing and Troubleshooting Your Network.

When Advisories identifies field notices that can potentially impact the network fabrics that it is monitoring, Nexus Dashboard validates the serial number of the devices in the fabrics against a list of affected device serial numbers in each field notice. If a serial number is not included in a field notice, Nexus Dashboard excludes that field notice. For Advisories to validate the device serial numbers, Nexus Dashboard must have an Internet connection and be connected to and registered to Cisco Intersight. Without such connectivity, Advisories cannot validate the serial numbers, which can result in Advisories incorrectly including field notices that do not apply. Not all field notices include serial number validation.

Click a particular advisory to view information such as What's wrong, What's the impact, and How do I fix it.

- What's wrong? provides problem description with the specific affected objects.
- What's the impact? explains what will happen if the problem is not fixed and includes end-of-sale key dates.
- How do I fix it? provides prescriptive recommendations.

Advisories enable you to stay current with

- new software and hardware availability
- hardware and software EoS and EoL announcements and lead time for upgrades
- security advisories and field notices, which helps you stay secure and compliant, and
- instant visibility into applicable bugs.

Advisories are classified into three levels: critical, major, and warning.

- **Critical**: Advisories are shown as critical when there are unsupported infrastructure and the severity of the bugs associated with notices is Severity1. Some of the examples include:
  - When switches in a fabric are running under End-of-Life conditions. When a critical (Severity1) field notice or security advisory has been issued for a switch or software version

currently running in your network.

- **Major**: Advisories are shown as major when the severity of the bugs associated with notices is Severity2. Some of the examples include:
  - When a critical (Severity2) field notice or security advisory has been issued for a switch or software version currently running in your network.
- **Warning**: Advisories are shown as warning when there is support for potentially at risk infrastructure and the severity of the bugs associated with notices is Severity3. Some of the examples include:
  - When switches in a fabric are approaching end-of-life conditions. When a Severity3 field notice or security advisory has been issued for a switch or software version currently running in your network.

Navigate to Advisories

You can view advisories in Nexus Dashboard at different levels such as across all fabrics, for a specific fabric, for a specific switch, or for system-wide advisories. Use the following methods to access advisory details.

View all advisories across all fabrics

Follow these steps to view all advisories across all fabrics.

1. Navigate to **Analyze** > **Advisories**.

   This displays all advisories detected across all fabrics in your environment.

View advisories for a single fabric

Follow these steps to view the advisories for a single fabric.

1. Navigate to **Home** > **Overview**.
2. Choose online fabrics or snapshot fabrics from the drop-down list.
3. Click the **Advisory level** card.
4. In the **Advisories** page, click **Analyze Advisories** to view detailed information for the selected fabric.
5. You can also view the advisories for a single fabric in the **Fabrics Overview** page.
   a. Navigate to **Manage** > **Fabrics**.
   b. Choose an appropriate fabric.

      The **Fabrics Overview** page displays.

   c. Click the **Advisories** tab to view advisories specific to that fabric.

View security advisories

Follow these steps to view the security advisories.

1. Navigate to **Home** > **Overview**.
2. Choose online fabrics or snapshot fabrics from the drop-down list.
3. Click **Security advisories** in the **Advisory level** card.
4. Click **Active advisories**.

View advisories for a single switch

Follow these steps to view the advisories for a single switch in the **Inventory** page.

1. Navigate to **Manage** > **Inventory**.
2. Choose online fabrics or snapshot fabrics from the drop-down list.
3. Choose a switch.

   The **Switch Overview** page displays.
4. Click the **Advisories** tab.

View system advisories

Follow these steps to view the system advisories.

1. Navigate to **Admin** > **System Status**.
2. Click the **Advisories** tab.

Analyze advisories

Follow these steps to analyze advisories.

1. Navigate to Advisories.
2. Click the **Date and Time selector** to choose the time range.

   The Advisories page displays the advisories by Level and Category for your account based on the selected time range.

   - The Level donut chart displays the total number of advisories of Critical,Major, and Warning severity.
   - The category displays a list of categories with number of anomalies against each category.
   - For the advisories displayed for a snapshot fabric, the advisory levels are across all snapshots and not just the latest snapshot.
3. Use the search bar to filter the advisories.
4. The Advisories table displays the filtered advisories. The advisories are sorted by Level by default. Click the column heading to sort the advisories in the table.

   The advisory status include Active and Cleared. An active state indicates that the advisory is

present on your network. A cleared state indicates that the advisory is not present on your network anymore and therefore the advisory is marked cleared.

5. Click the gear icon to configure the columns in the Advisories table. By default, the columns Title, Level, Category, and Fabric are displayed.
6. Click an advisory to view the additional details such as What's wrong?, What's the impact?, and How do I fix it?.

   - What's wrong? provides problem description with the specific affected objects.
   - What's the impact? explains what will happen if the problem is not fixed and includes End-of-Sale key dates.
   - How do I fix it? provides prescriptive recommendations.

7. Choose advisories from the **Advisories** table and click **Acknowledge Advisories** to acknowledge advisories.

   You can also click an advisory in the **Advisory** page and choose **Acknowledge Advisory** from the **Actions** drop-down list.

   By default all the unacknowledged **Advisories** are displayed in the advisories table. Once you acknowledge an advisory, choose **Acknowledged** from the drop-down list to view all the acknowledged advisories.

View platform and system alerts in global advisories table

System advisories allow you to view information about updates, issues, or required actions related to a system, application, or network. These advisories ensure that you are aware of critical information that might impact the system's performance, security, or operation.

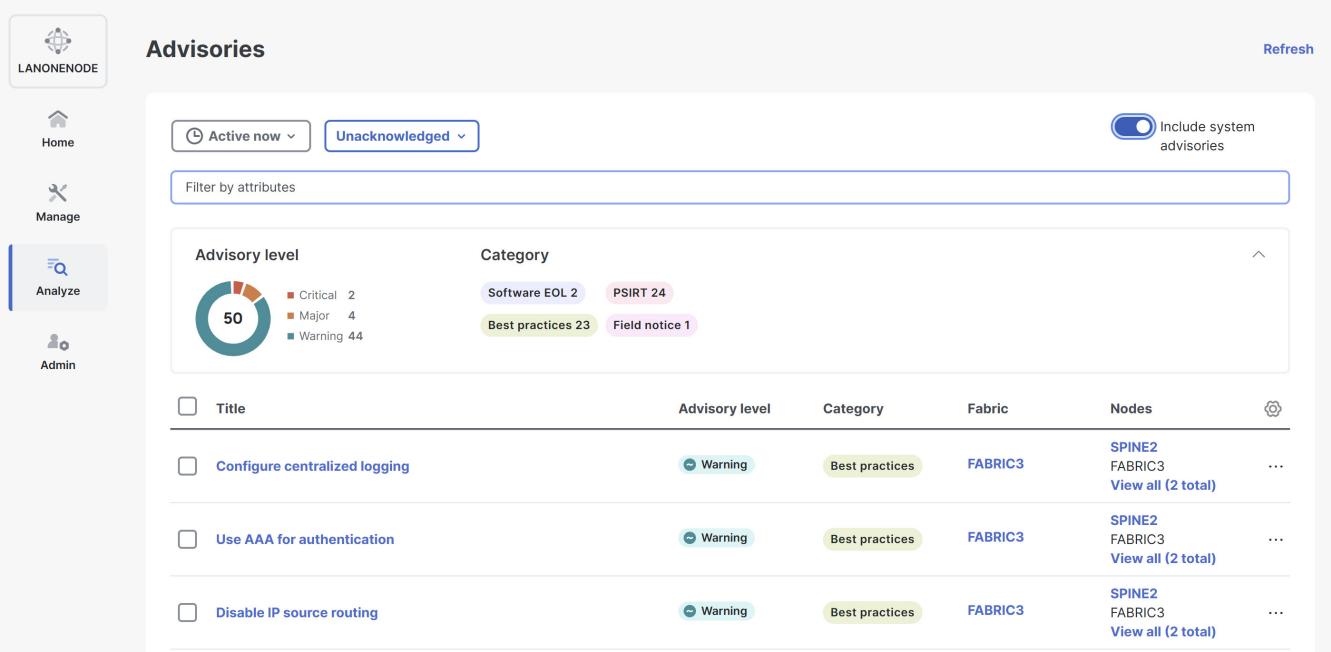
Follow these steps to include system-related advisories.

1. Navigate to **Analyze > Advisories**.

   The **Advisories** page displays.

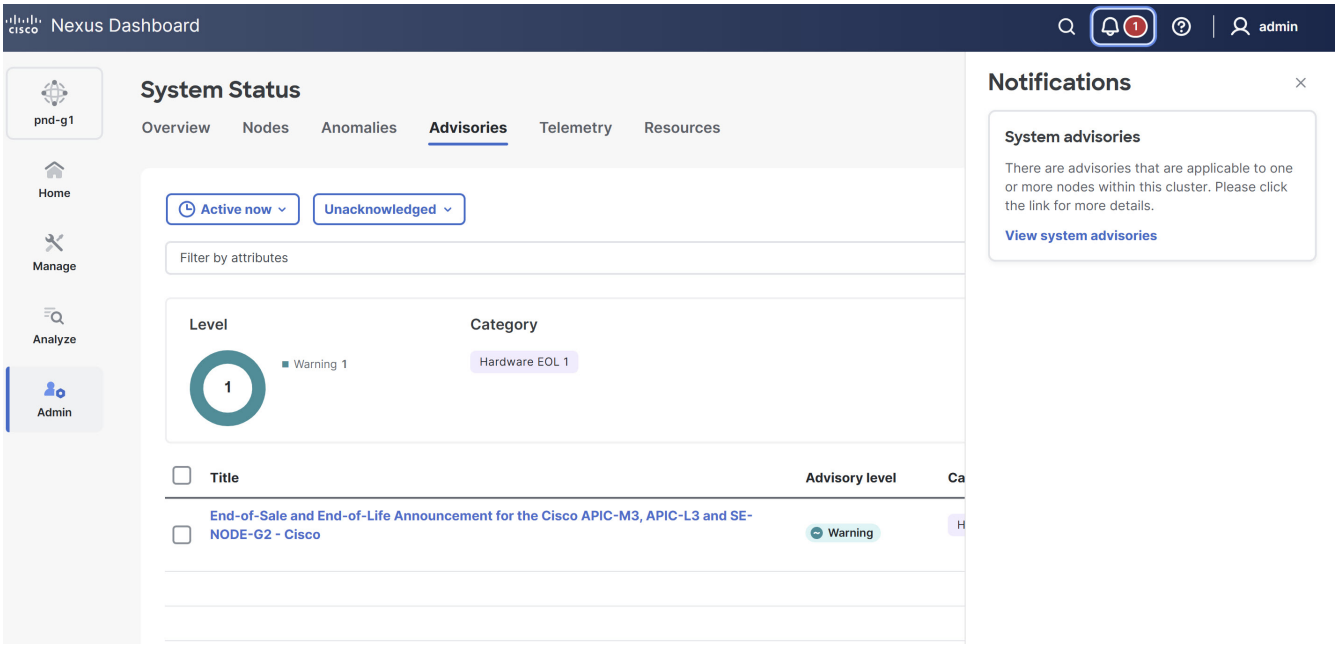
2. Click the **Include system advisories** toggle button in the top-right corner, to include system-related advisories in the **Advisories** table.

   Once enabled, the **System** category appears under advisories by category in the **Advisories** page.



System advisory notification

When there is an active system advisory, a notification alert appears on the **Notifications** bell icon located in the common navigation bar at the top of the page. Click the notification bell icon to open the **Notifications** pane. In the **Notifications** pane, click **View system advisories**. Nexus Dashboard redirects you to the **System Status** page, where you can review the full list of current and past system advisories in the **Advisories** table.



Advisory filters

The search bar allows you to filters the advisories. In the Advisories page, you can use the following filters to refine the displayed advisories:

- Title - Display advisories with a specific title.
- Advisory Level - Display advisories of a specific level.

- Detection Time – Display advisories with a specific detection time.
- Last Seen time – Display only advisories with a specific last seen time. Last Seen Time indicates the time advisory was updated while under active status. If the status of the advisory is not cleared, then the advisory is active.
- Category – Display advisories from a specific category.
- Fabric – Display advisories for a specific fabric.
- Nodes – Display advisories for specific nodes.
- What's wrong? – Display advisories of a specific affected object.

As a secondary filter refinement, use the following operators:

- == – with the initial filter type, this operator, and a subsequent value, returns an exact match.
- != – with the initial filter type, this operator, and a subsequent value, returns all that do not have the same value.
- contains – with the initial filter type, this operator, and a subsequent value, returns all that contain the value.
- !contains – with the initial filter type, this operator, and a subsequent value, returns all that do not contain the value.

Metadata support

Nexus Dashboard uses metadata bundles to detect new bugs, security advisories, Field Notices, and End of Life Notices. Metadata packages are constantly updated by us and posted to the Cisco Intersight Cloud after validation. Nexus Dashboard connects to the Cisco Intersight Cloud through a device connector that is embedded in the Nexus Dashboard platform and that pulls periodically updated metadata packages. With metadata support for air-gapped environment, if Nexus Dashboard is not connected to Cisco Intersight Cloud, you can manually upload the latest metadata to Nexus Dashboard in a secure and trusted way. You can download the bundle updates from the Cisco DC App Center.

Navigate to **Admin** > **System Settings** > **Metadata** to view the metadata version.

- In the General area, the Metadata Version is displayed.
- In the Update Metadata Version area, you can upload metadata for air-gapped environments.

Metadata support for air-gapped environment

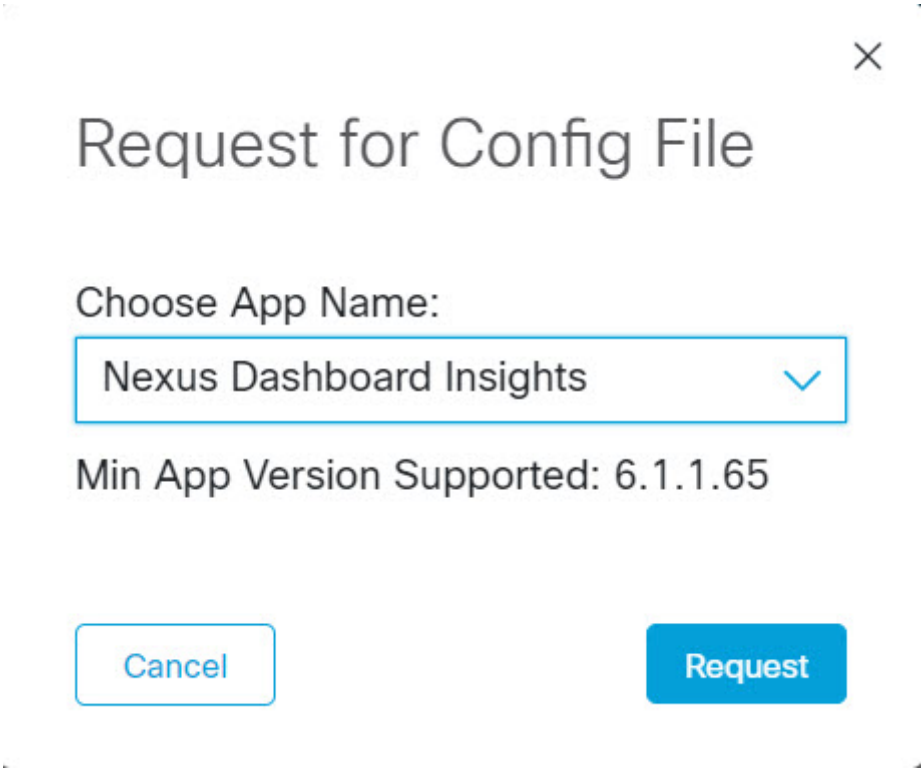
With metadata support for air-gapped environment, if Nexus Dashboard is not connected to Cisco secure cloud, you can upload the latest metadata to Nexus Dashboard periodically in a secure and trusted way.

You can download the encrypted metadata file from the Cisco DC App Center and upload it to Nexus Dashboard to get decrypted updates on exposure to Bugs, security advisories, Defects, Field Notices, and End of Life Notices.

Update metadata version

Follow these steps to update the latest metadata version in an air-gapped or offline environment.

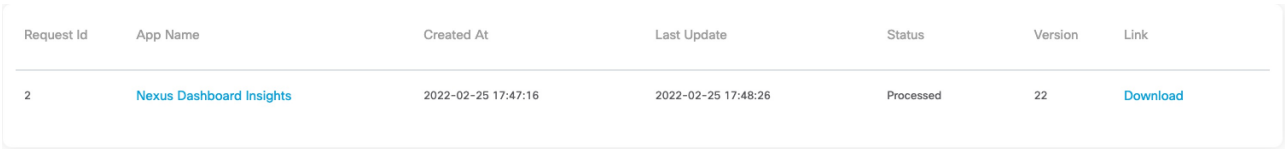
1. Log in to Cisco DC App Center.
2. From the User drop-down list, choose **My Account**.
3. Click **Config Files Requests** tab.
4. Click **Request Config File**.
5. From the **Choose App ID** drop-down list, select Nexus Dashboard.



6. Verify the minimum supported app version and click **Request**.

   It takes approximately 15 minutes for the request to be completed. In the Config Files Request page, the generated file is displayed in the table below.

7. Select the file and click **Download** to download the file locally.



Request Id	App Name	Created At	Last Update	Status	Version	Link
2	Nexus Dashboard Insights	2022-02-25 17:47:16	2022-02-25 17:48:26	Processed	22	Download

8. Log in to Nexus Dashboard.
9. Navigate to **Admin** > **System Settings** > **Metadata** to view the metadata version.
10. In the Update Metadata Version area, upload the file you have downloaded from the Cisco DC App Center.
11. Click **Begin Upload** to upload the latest metadata.

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