Cisco Nexus Dashboard Insights Anomalies and Advisories, Release 6.5.1 - For Cisco NDFC or Standalone NX-OS

Table of Contents

First Published: 2024-06-28

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

New and changed information

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

New features and changed behavior in the Cisco Nexus Dashboard Insights

Feature	Description	Release	Where Documented
Anomaly correlation	The Anomalies functionality now correlates anomalies that cause or are caused by other anomalies. An anomaly that causes other anomalies is known as a root cause anomaly, while an anomaly that is caused by a root cause anomaly is known as a correlated anomaly. An anomaly that is neither a root cause nor a correlated anomaly is known as an uncorrelated anomaly. There is now a drop-down menu that enables you to filter for root cause and uncorrelated anomalies, root cause anomalies only, uncorrelated anomalies only, or all anomalies.	6.5.1	Root cause anomalies, Correlated anomalies, Uncorrelated anomalies, Analyze anomalies
Custom thresholds for capacity and hardware anomalies	You to can customize the thresholds that determine whether an anomaly is assigned the warning, major, or critical level.	6.5.1	Global rules, Customize anomaly level thresholds
Device serial number validation to reduce false positive Advisories results for field notices.	When the Advisories functionality of Cisco Nexus Dashboard Insights identifies field notices that can potentially impact the network fabrics that it is monitoring, Nexus Dashboard Insights now 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 Insights excludes that field notice.	6.5.1	Advisories
Terminology change	The term " sites" is renamed to " fabrics" .	6.5.1	Entire document

This document is available from your Cisco Nexus Dashboard Insights GUI as well as online at www.cisco.com. For the latest version of this document, visit Cisco Nexus Dashboard Insights Documentation.

Anomalies

Anomalies

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

Nexus Dashboard Insights monitors different sets of data from all nodes in the fabric and baselines the data to identify “normal” behavior. Any deviation is represented as an anomaly. Your time is better spent in resolving the issue instead of tracking the issue. Additionally, it can estimate the impact of the anomaly and generate a recommendation depending on the nature of the anomaly and thus reducing the Mean Time to Troubleshooting and Resolution (MTTR).

The Anomalies page allows you to

- shorten the mean time to resolution for troubleshooting
- increase operational efficiency and network availability with proactive monitoring, and
- remediate.

The Anomalies page displays the anomalies by level and category for a particular fabric based on the selected time range.

The anomaly levels include critical, major, and warning.

Some of the categories include

- hardware
- capacity
- compliance
- connectivity
- configuration
- integrations, and
- active bugs.

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

A correlated anomaly is an anomaly that occurred because of another anomaly, which is referred to as the root cause anomaly. Resolving the root cause anomaly should resolve the correlated anomalies without you needing to take further action for the correlated anomalies.

Uncorrelated anomalies

An uncorrelated anomaly is an anomaly that did not cause any correlated anomalies and was not

caused by a root cause anomaly. Therefore, such an anomaly does not affect any other anomalies. You must resolve these anomalies individually.

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

How the anomalies functionality correlates anomalies

The anomalies functionality analyzes the cause and effect relationship between various anomalies within a certain time window. The functionality correlates anomalies based on various attributes, such as device, interface, and protocols, to find the root cause anomaly, which might be the cause of secondary anomalies (the correlated anomalies).

Anomaly levels

Anomalies are classified into these levels:

- **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
- **Warning**: Anomalies are shown as warning when the network is impacted. An example includes:
  - When connectivity to a given prefix or endpoint is degraded

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

To configure properties on an anomaly see Configure anomaly properties.

You can acknowledge anomalies in the following 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.

View Anomalies

In Nexus Dashboard Insights, you can view anomalies in the following ways:

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

OR

1. Navigate to **Overview** > **Global View**.
2. Choose online fabrics or snapshot fabrics from the drop-down menu.
3. Click the **Anomalies Level** card.
4. In the Anomalies page, click **View all anomalies**.

OR

1. Navigate to **Manage** > **Fabrics**.
2. Choose a fabric.
3. Click **Anomalies**.

OR

1. Navigate to **Manage** > **Inventory**.
2. Click **Controllers** or **Switches**.
3. Choose a controller or switch.
4. Click **Anomalies**.

Analyze anomalies

1. Navigate to **Analyze** > **Anomalies**.
2. Choose **Online fabrics** or **Snapshot fabrics** from the drop-down menu.
3. From the **All Anomalies** drop-down menu, choose **Grouped** or **Ungrouped**.
   - 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.
4. From the **Date and Time** selector, choose the time range. By default, **Active Now** is chosen.

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

   - The level donut chart displays the total number of anomalies of critical, major, and warning severity.
   - The category donut chart displays the total number of anomalies by various categories, such as Hardware, Capacity, Compliance, Connectivity, Configuration, Integrations, and Active bugs.
   - For the anomalies displayed for a snapshot fabric, the anomaly levels are across all snapshots and not just the latest snapshot.

5. Use the filter field to filter the anomalies. You can filter for affected objects such as interface, VRF instance, EPG, or BD and view the associated anomalies.
    a. When viewing the ungrouped anomalies, you can use the drop-down menu next to the filter field to filter for unacknowledged or acknowledged anomalies. The default is **Unacknowledged**.
    b. You can use the drop-down menu next to the unacknowledged and acknowledged anomalies drop-down menu to filter by root cause and uncorrelated anomalies, root cause anomalies only, uncorrelated anomalies only, or all anomalies. The default is **Root Cause and Uncorrelated Anomalies**.

       For more information about the filters, see Anomaly filters.

6. The Anomaly Type 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 viewing the ungrouped anomalies and you configured the table to display the **Status** column, the status can be Active or Cleared. 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.

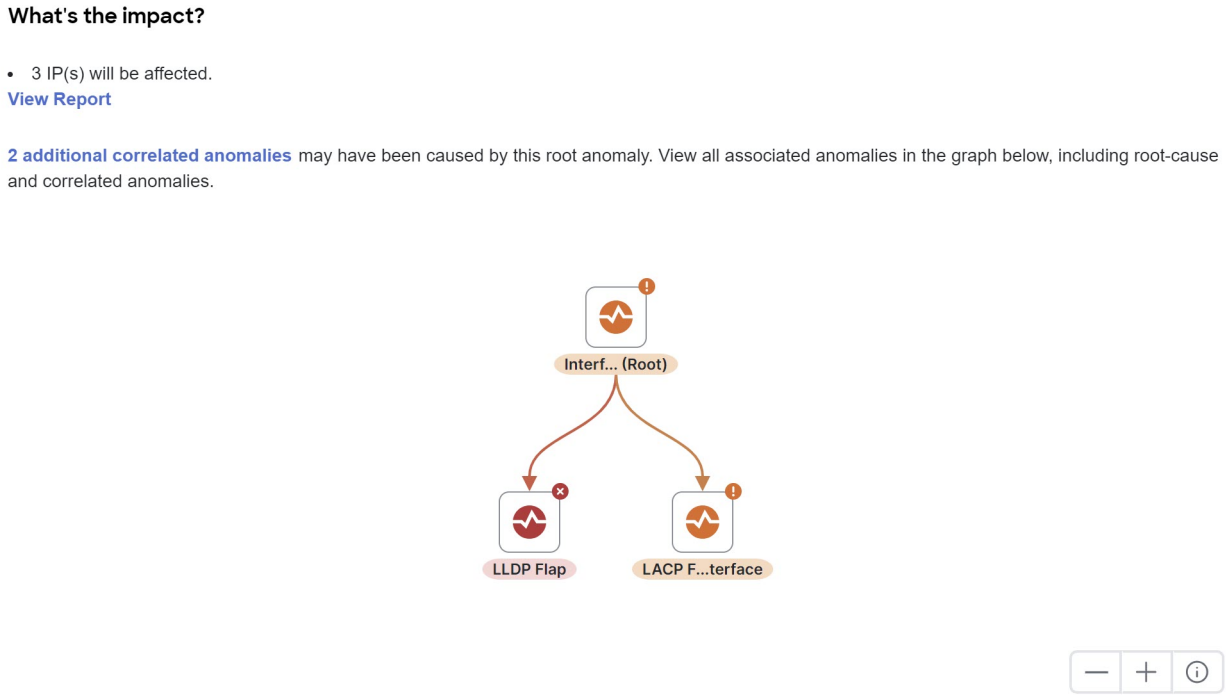
7. Click the gear icon to configure which columns display in the Anomalies table.

   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 of the anomalies in that group are root cause anomalies.

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

8. Click an anomaly to view more information.
    - What's wrong? provides problem description with the specific affected objects.
    - What triggered this anomaly? provides the root cause of the anomaly, including a link that you can click to see information about the root cause anomaly. 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 what will happen if the problem is not fixed. If the anomaly is a root cause, this area specifies the quantity of correlated anomalies, which you can click to see a table of those 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 viewing the correlated anomalies page and you configured 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.

9. From the Anomalies drop-down menu, choose **Ungrouped**.
   a. Select anomalies from the Anomalies table and click **Acknowledge Anomalies** to acknowledge the anomalies.
   b. You can also click an anomaly and in the Anomalies page choose **Acknowledge Anomaly** from the **Actions** menu.
   c. By default, all the unacknowledged anomalies are displayed in the anomalies table. After you acknowledge an anomaly, choose **Acknowledged** from the drop-down menu to view all the acknowledged anomalies.
10. To bookmark an anomaly, click an anomaly to view the Anomaly page, then click the bookmark icon.
11. To add a widget for an anomaly to your custom dashboard, click an anomaly to view the Anomaly page, then click **Actions > Pin page to custom dashboards**.

Guidelines and Limitations for Anomalies

- In the following scenarios, anomalies are not displayed in the Anomalies page.
  - Anomalies that belong to the category "System" are not displayed in the Anomalies page by default.
  - When there is any collection or login failure, in the **Admin** > **System Settings** > **System Status Details** page, Assurance status is displayed as Healthy. At the same time, in the **Admin** > **System Settings** > **System Issues** page, anomalies related to any collection or login failure

are not displayed.

To view the anomalies, perform the following steps:

1. To view these anomalies, 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.

Configure anomaly properties

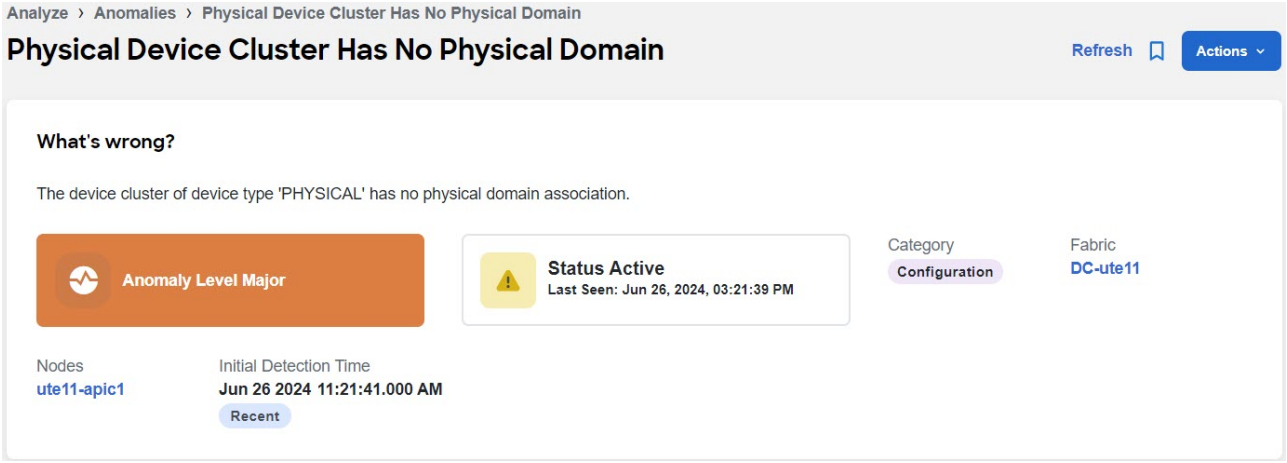
Use the following procedure to configure properties on an anomaly.

1. Navigate to **Analyze** > **Anomalies**.
2. Select Online fabrics or Snapshot fabrics from the drop-down menu.
3. From the Anomalies drop-down menu, 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** menu.
   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**.
2. If you want determine the object from the ungrouped anomalies, choose **Ungrouped** from the drop-down menu.
3. If you want determine the object from the grouped anomalies, choose **Grouped** from the drop-down menu, then click the desired anomaly type in the table.
4. Choose an anomaly from the Anomalies table.
5. In the What's the impact? area, the primary affected objects are highlighted in bold.

Global rules

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** > **Rules** > **Global Rules**.
2. In the **Status** column for the desired anomaly category, click **Customize**.
3. 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.

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

   After you customize the thresholds, Nexus Dashboard Insights 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 Insights will not raise any anomalies for that severity. If you enter 0 for all of the severities, Nexus Dashboard Insights 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**.

Anomaly rules

Anomaly rules

Anomaly rules feature enables you to acknowledge all new detected anomalies that match the criteria and adjust the anomaly score accordingly. You can also match an alert against an anomaly rule using the match criteria.

It also 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.

- 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, event name, and object match rule, to define the match criteria for the anomaly rule.
- A match criteria can contain one attribute or multiple attributes.
  - If a match criteria contains multiple attributes, then the anomalies containing all the attributes will be matched. The **AND** operator will apply to the attributes.
  - If a match criteria contains multiple affected object match rules, then the anomalies containing all of the affected object match rules will be matched.
- If an anomaly rule contains multiple match criteria, then the anomalies containing the union of the match criteria will be matched. Any anomalies that match any criteria will apply to the rule. The **OR** operator will apply to the criteria.
- Anomaly Rules using **Match Criteria** with **Object Match Rule** will only support the **Equals to** regex 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 created multiple anomaly rules, all rules that match get applied.
- If you specified multiple attributes in an anomaly rule, the conditions of each attribute must be met for the rule to apply.
- If you specified multiple conditions for an attribute, any of the conditions must be met for the attribute to evaluate as true.
- If you specified multiple match criteria within an affected object, each criteria must be met.

Guidelines and Limitations

- Deleting or disabling an anomaly rule containing either **Acknowledge** or **Customize Anomaly** action will not delete or disable the anomaly rule from active anomalies. The anomaly rule will be not be applied to any new instance of the anomaly only.
- When you edit an anomaly rule containing either Acknowledge or Customize Anomaly action, the updates are not applied to active anomalies. The anomaly rule updates will be applied to any new instance of the anomaly only.

- If an anomaly rule contains both Acknowledge and Customize Anomaly action, and you edit the anomaly rule by removing either the Acknowledge and Customize Anomaly action, then the updates are not applied to active anomalies.
- When you delete or disable an anomaly rule containing **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.
- 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

1. Navigate to **Manage** > **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 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 **Fabric** 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. Click **Add Code Rule** to define the check code for the match criteria.

f. Select severity from the drop-down list.

g. Click **Save**.

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

a. Use 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 toggle to choose **Customize Anomaly**.

> 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 to new instance of anomalies.

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

1. Navigate to **Manage** > **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 disabled, the rule will not be applied during the next analysis.

Advisories

Advisories

Nexus Dashboard Insights identifies field notices, software and hardware end-of-life and end-of-sale announcements, as well as PSIRTs 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 Insights provide details of relevant impact from field notices, PSIRTs, 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.

When Advisories identifies field notices that can potentially impact the network fabrics that it is monitoring, Nexus Dashboard Insights 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 Insights excludes that field notice. For Advisories to validate the device serial numbers, Cisco 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
- PSIRTs 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 PSIRT 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 PSIRT 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 PSIRT has been issued for a switch or software version currently running in your network.

View Advisories

In Nexus Dashboard Insights, you can view advisories in the following ways:

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

OR

1. Navigate to **Overview** > **Global View**.
2. Select online fabrics or snapshot fabrics from the drop-down menu.
3. Click **Advisories Level** card.
4. In the Advisories page, click **View all advisories**.

OR

1. Navigate to **Manage** > **Fabrics**.
2. Select a fabric.
3. Click **Advisories**.

OR

1. Navigate to **Manage** > **Inventory**.
2. Click **Controllers** or **Switches**.
3. Select a controller or switch.
4. Click **Advisories**.

Analyze Advisories

1. Navigate to **Analyze** > **Advisories**.
2. Select Online fabrics or Snapshot fabrics from the drop-down menu.
3. Click the Date and Time selector to select 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.

4. Use the search bar to filter the advisories.
5. 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.

6. Click the gear icon to configure the columns in the Advisories table. By default, the columns Title, Level, Category, and Fabric are displayed.
7. 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.

8. Select advisories from the Advisory table and click Acknowledge Advisories to acknowledge advisories.
   a. You can also click an advisory and in the Advisory page select **Acknowledge Advisory** from the Actions menu.

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

9. Click an advisory to view the Advisory page. Click the bookmark icon to bookmark the advisory.
10. Click an advisory to view the Advisory page. Click the pin icon to pin the advisory.

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.

Copyright