



View and Manage Issues

- [About Issues, on page 1](#)
- [About the Machine Reasoning Engine, on page 2](#)
- [About the Layer 2 Loop Issue Involving VLANs, on page 2](#)
- [View Open Issues, on page 2](#)
- [Troubleshoot Wired Client Issues Using MRE, on page 15](#)
- [View Resolved Issues, on page 17](#)
- [View Ignored Issues, on page 19](#)
- [Resolve or Ignore Issues, on page 21](#)
- [No Activity on Radio Issue Triggers, on page 22](#)
- [Automatic Issue Resolution, on page 22](#)
- [Manage Global Issue Settings, on page 25](#)
- [Manage User-Defined Issue Settings, on page 26](#)
- [Manage Custom Issue Settings, on page 27](#)
- [Enable Issue Notifications, on page 29](#)
- [Assurance, Cisco AI Network Analytics, and MRE Issues, on page 31](#)

About Issues

Assurance provides both system-guided as well as self-guided troubleshooting. For a large number of issues, Assurance provides a system-guided approach, where multiple Key Performance Indicators (KPIs) are correlated, and the results from tests and sensors are used to determine the root cause of the problem, and then possible actions are provided to resolve the problem. The focus is on highlighting an issue rather than monitoring data. Quite frequently, Assurance performs the work of a Level 3 support engineer.

With Cisco DNA Center, you can view and troubleshoot AI-driven issues using Cisco AI Network Analytics. Cisco AI Network Analytics leverages a cloud-based learning platform with advanced artificial intelligence (AI) and machine learning (ML) technologies to provide intelligent issue detection and analysis. It detects anomalies to determine their root causes and ease troubleshooting.

Cisco AI Network Analytics can detect the following types of cloud-based AI-driven issues:

- **Connection Issues** (Onboarding Issues): Excessive Time, Excessive Failures, Excessive Association Time, Excessive Association Failures, Excessive Authentication Time, Excessive Authentication Failures, Excessive DHCP Time, and Excessive DHCP Failures

- **Application Experience Issues:** Total Radio Throughput, Media Application Throughput, Cloud Application Throughput, Collab Application Throughput, and Social Application Throughput.

About the Machine Reasoning Engine

The Machine Reasoning Engine (MRE) is a network automation engine that uses artificial intelligence (AI) to automate complex network operation workflows. It encapsulates human knowledge and expertise into a fully automated inference engine to help you perform complex root cause analysis, detect issues and vulnerabilities, and either manually or automatically perform corrective actions. MRE is powered by a cloud-hosted knowledge base, built by Cisco networking experts.

You can use the MRE to troubleshoot wired client, Layer 2 loop, and PoE issues. For the list of issues, see [MRE Issues, on page 47](#).

For procedures, see [Troubleshoot Wired Client Issues Using MRE, on page 15](#), [Issue Instance Details for Layer 2 Loop Issue, on page 11](#), and [Issue Instance Details for a PoE Issue, on page 13](#).

About the Layer 2 Loop Issue Involving VLANs

A Layer 2 Loop issue occurs when a forwarding loop forms in the path of one or more VLANs. In this case, packets are forwarded and multiplied indefinitely along the affected path, until the links and devices reach maximum capacity. A broadcast storm occurs and the entire Layer 2 network shuts down very quickly. The MRE enables you to troubleshoot the Layer 2 Loop issue by:

- Viewing the VLANs and ports that are involved in the probable loop.
- Viewing the devices that are associated with the loop.



Note The scale constraints for the Layer 2 loop are the following:

- The number of VLANs is 10.
- The number of devices per VLAN is 30.



Important

Currently, the MRE does not perform root cause analysis on Layer 2 loops that occur as a result of unmanaged network devices, virtual machines, or other entities that are not part of the topology known to Cisco DNA Center.

View Open Issues

Use this procedure to view all open issues, which fall under the following categories:

- **Threshold-based issues:** Issues detected by Assurance.

- **AI-Driven Issues:** Issues detected by Cisco AI Network Analytics. These issues are triggered based on deviations from the predicted baseline for your specific network environment.

If you have installed and configured the Cisco AI Network Analytics application with Cisco DNA Center, you can view the following types of cloud-based, AI-driven issues:

- **Connection Issues (Onboarding Issues):** Excessive Time, Excessive Failures, Excessive Association Time, Excessive Association Failures, Excessive Authentication Time, Excessive Authentication Failures, Excessive DHCP Time, and Excessive DHCP Failures.



Note For Connection issues to display, make sure that the APs are properly assigned to sites.

- **Application Experience Issues:** Total Radio Throughput, Media Application Throughput, Cloud Application Throughput, Collab Application Throughput, and Social Application Throughput.



Note For Application Experience issues to display, make sure that Application Visibility and Control (AVC) is enabled on the wireless controllers. The throughput issues rely on the AVC data for baselining and anomaly detection.

- **Layer 2 Loop Issue and PoE Issue:** Issues detected by Assurance that you can troubleshoot using the MRE workflow. See [About the Machine Reasoning Engine, on page 2](#).

Before you begin

- To view AI-driven, cloud-based issues that use artificial intelligence (AI) and machine learning (ML) technologies to provide intelligent issue detection and analysis, make sure that you have configured Cisco AI Network Analytics data collection. See [Configure Cisco AI Network Analytics](#).
- To view syslog messages, make sure that you have configured syslog. See [Configure Syslog, SNMP Traps, NetFlow Collector Servers, and Wired Client Data Collection Using Telemetry](#) in the [Cisco Digital Network Architecture Center User Guide](#).

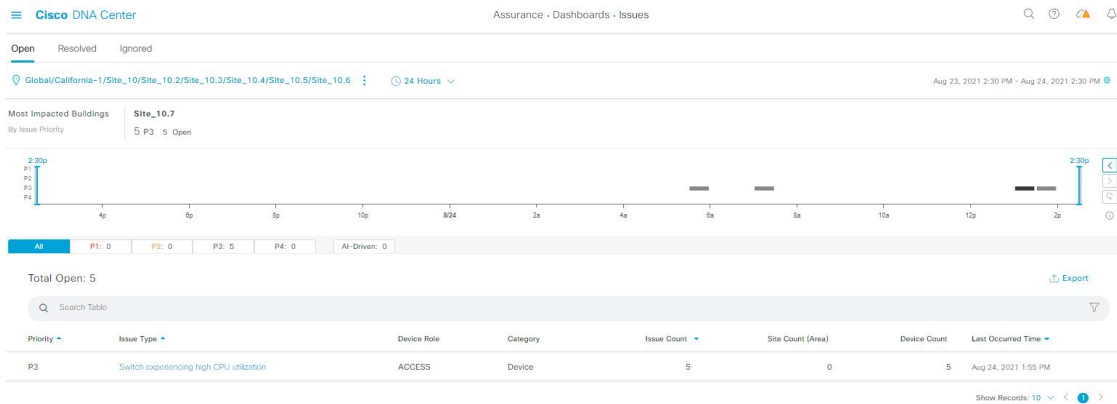
Step 1

Do one of the following:






- From the Cisco DNA Center home page, in the **Assurance Summary > Critical Issues** area, choose **View Details**.
- From the top-left corner, click the menu icon and choose **Assurance > Issues and Events**.




The **Open Issues** dashboard appears with the following information:

Figure 1: Open Issues Dashboard




Open Issues Dashboard

| Item | Description |
|---------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  Global | <ul style="list-style-type: none"> Click  Global in the top menu bar to choose the site, building, or floor from the Site hierarchy. Click  next to the location icon and choose Site Details to view the Sites table. Choose Hierarchical Site View or Building View from the drop-down list. Based on what you choose, the table is refreshed. From the Go to sites column, click  for a site or building to display data only for that location on the Open Issues dashboard. |
|  Time Range setting | <p>Allows you to display information on the window based on the time range you select. The default is 24 Hours. Do the following:</p> <ol style="list-style-type: none"> From the 24 Hours drop-down list, choose a time range: 3 hours, 24 hours, or 7 days. Specify the Start Date and time, and the End Date and time. Click Apply. <p>This sets the range of the timeline.</p> |


| Open Issues Dashboard | |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Item | Description |
| Timeline Slider | <p>Allows you to specify a more granular time range. Click and drag the timeline boundary lines to specify the time range.</p> <p>The colors represent the issue priority:</p> <p>: P1</p> <p>: P2</p> <p>: P3 and P4</p> <p>Note The intensity of the color indicates its significance, whether more or fewer issues have occurred for that priority level. For example, a lighter shade of yellow indicates fewer P2 issues (still open) than a deeper shade of yellow.</p> |
| Most Impacted Areas | Provides information about the areas that are most impacted based on issue priority. Click the hyperlinked location to drill down to the exact building and floor where the issue occurred. |

Step 2 Click the **All**, **P1**, **P2**, **P3**, **P4**, or **AI-Driven** tab to display a list of issues in that category in the **Issue Type** table.

| Issue Type Table in the Open Issues Window | |
|--------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Item | Description |
| Total Open | <p>Provides the total count of open issues that require action.</p> <p>The Total Open value changes depending on the tab you choose. Options are All (the default), P1, P2, P3, P4, and AI-Driven.</p> |
| Priority | Preassigned priority level of the issue type. |
| Issue Type | <p>Type of issue.</p> <p>Note For AI-driven issues, the  icon appears in front of the issue type.</p> |
| Device Role | Role assigned to the device on which the issue was detected. The role is Access, Core, Distribution, Border Router, or Unknown. |
| Category | Category under which the issue type falls, such as Connectivity, Availability, Onboarding, and Utilization. |
| Issue Count | Number of times this type of issue occurred. |
| Site Count (Area) | Number of sites where this type of issue occurred. |
| Device Count | Number of devices that were impacted by this type of issue. |
| Last Occurred Time | Most recent date and time this issue occurred. |

Step 3 From the **Issue Type** table, click an issue type.

The first slide-in pane, **Issue Instances**, lists all the issues for that issue type with the following information:

| Issue Instances (First Slide-In Pane) | |
|---------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Item | Description |
| Open Issues | Number of open issues for that issue type. |
| Area | Number of buildings and floors that are impacted by the issue. |
| Device | Number of devices that are impacted by the issue. |
| Actions drop-down list | Allows you to resolve or ignore a single issue or a bulk of issues at a time. See Resolve or Ignore Issues, on page 21 . |
| Issue | Description of the issue. If you're an admin user, you can add, edit, and delete notes. Click the Note icon () and then click Add . If you're any other type of user, you can only view note information. |
| Site | Site, building, or floor that was impacted by the issue. |
| Device | Device that was impacted by the issue. Click the device name to open the Device 360 window. |
| Device Type | Type of device that was impacted by the issue. |
| Issue Count | Number of times this type of issue occurred. |
| Last Occurred Time | Date and time this issue occurred. |
| Last Updated Time | Date and time this issue was last updated. |
| Updated By | Name of the entity who updated this issue. |

Step 4 From the **Issue** column in the **Issue Instances** slide-in pane, click an issue.

A second slide-in pane, **Issue Instance Details**, provides specific details about the issue. Depending on the issue, the description and suggested actions are displayed. See the following sections for more details about these issues:




- [Issue Instance Details for AI-Driven Issues, on page 6](#)
- [Issue Instance Details for AP-Disconnect Issues, on page 10](#)
- [Issue Instance Details for Layer 2 Loop Issue, on page 11](#)
- [Issue Instance Details for a PoE Issue, on page 13](#)

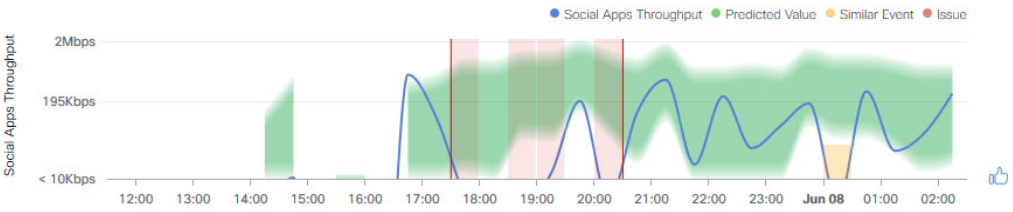
Issue Instance Details for AI-Driven Issues



Note The **Issue Instance Details** slide-in pane is part of the **Open Issues** workflow. See [Step 4 in View Open Issues, on page 2](#).

For AI-driven issues, the **Issue Instance Details** (second slide-in pane) provides the following information:

| Issue Instance Details (Second Slide-In Pane) | |
|-------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Item | Description |
| Description | Description of the issue. |
| Status drop-down list | Allows you to change the status of the issue. Do the following: <ul style="list-style-type: none"> To resolve an issue, from the Status drop-down list, choose Resolve. To stop an issue from being reported, do the following: <ol style="list-style-type: none"> From the Status drop-down list, choose Ignore. Set the number of hours to ignore the issue on the slider, and then click Confirm. |
| Note icon () | If you're an admin user, you can add, edit, and delete notes. Click the Note icon () and then click Add . If you're any other type of user, you can only view note information. |
| Summary area | Brief summary of the issue, which can include information such as the radios that are impacted, the location of the radios, the time and date the issue occurred, and the location of the issue. |
| Impacted Summary for this Network | Displays information about the location that was impacted and the number of clients that were impacted by the issue. |
| Feedback icon | Click the  icon to provide your comments on whether the information on this page was helpful, and then click Submit . |

| Issue Instance Details (Second Slide-In Pane) | |
|-----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Item | Description |
| Problem | <p>Provides brief text that describes the problem along with a chart that provides a visual of how the actual KPI value deviated from the predicted normal behavior.</p> <p>By default, the chart is zoomed-in, 6 hours before and 6 hours after the issue, as shown in the following figure:</p> <p>Figure 2: Problem Chart</p>  <p>The chart details for the AI-driven issues are represented by different colors.</p> <ul style="list-style-type: none"> • Green band: Predicted normal behavior for your network based on machine learning. • Solid blue line: Actual KPI value. • Vertical red line or bars: Indicates an issue. When the blue line (actual KPI value) falls outside the green band (predicted normal behavior), an issue is raised. • Vertical yellow bars: Indicates that a similar event has occurred. <p>Hover and move your cursor over the charts to view synchronized information, such as the KPI value, the predicted lower value, and the predicted upper value at a selected point in time.</p> |
| Impact | <p>Provides information about the connected clients, APs, devices, and applications that are impacted by the issue.</p> <p>For Excessive Onboarding Time and Failures; and Excessive DHCP, Association, or Authentication Time and Failures, the following tabs are provided: Impacted Clients and Top 10 Impacted APs.</p> <p>For Total Radio Throughput and Applications Throughput (Cloud, Collab, Media, and Social), the following tabs are provided: Impacted Clients, Device Breakout, and Applications by TX/RX.</p> <p>Click the tab to update the chart and the table below the chart.</p> |

Issue Instance Details (Second Slide-In Pane)

| Item | Description |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Root Cause Analysis | <p>Provides the issue along with the probable network causes for that issue, displayed in charts, as shown in the following figure:</p> <p>Figure 3: Root Cause Analysis Charts</p> <p>For Excessive Onboarding Time and Failures, the following tabs are provided: Network Causes, Failed Distribution, Failed Percentage, and Failed Count.</p> <p>For Excessive DHCP, Association, or Authentication Time, the following tabs are provided: Network Causes, Top Impacted APs, and Top Impacted Times.</p> <p>For Excessive DHCP, Association, or Authentication Failures, the following tabs are provided: Network Causes, Top Impacted APs, and Top Impacted Failures.</p> <p>For Total Radio Throughput and Applications Throughput (Cloud, Collab, Media, and Social), the following tabs are provided: Network Causes.</p> <p>Click the tab to update the charts below.</p> <p>To view the charts for additional KPIs, click the KPI icon, choose the KPI, and then click Apply.</p> |
| Suggested Actions | <p>Provides the actions you can take to resolve the issue.</p> |

Issue Instance Details for AP-Disconnect Issues



Note The **Issue Instance Details** slide-in pane is part of the **Open Issues** workflow. See [Step 4 in View Open Issues, on page 2](#).

For AP-Disconnect issues, the **Issue Instance Details** (second slide-in pane) provides the following information:

| AP-Disconnect Issue Instance Details (Second Slide-In Pane) | |
|-------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Item | Description |
| Status drop-down list | <ul style="list-style-type: none"> To resolve an issue, from the Status drop-down list, choose Resolve. To stop an issue from being reported, do the following: <ol style="list-style-type: none"> From the Status drop-down list, choose Ignore. Set the number of hours to ignore the issue on the slider, and then click Confirm. |
| Note icon (📄) | If you're an admin user, you can add, edit, and delete notes. Click the Note icon (📄) and then click Add . If you're any other type of user, you can only view note information. |
| Insights | Provides a brief summary of the issue, which can include information such as the switch that is impacted, the date and time of the issue, and the location of the switch. |
| Impact Summary | Displays the counts of impacted sites, clients, and APs. |
| Problem Details | Provides the following details: <ul style="list-style-type: none"> Description of the devices involved with the issue, if known. Related issue, if any, with a link directly to the issue details. Details about the problem, such as the impacted APs, their location and power information, and the reason for the disconnect. Physical neighbor topology, which includes the switch and the neighboring devices that are connected to it. |
| Impact Details | Lists the wireless clients that were connected to the impacted APs and their locations. |
| Suggested Actions | Provides the actions you can take to resolve the issue. |

Issue Instance Details for Layer 2 Loop Issue



Note The **Issue Instance Details** slide-in pane is part of the **Open Issues** workflow. See [Step 4 in View Open Issues, on page 2](#).

To understand the Layer 2 Loop issue and the Machine Reasoning Engine, see [About the Machine Reasoning Engine, on page 2](#).


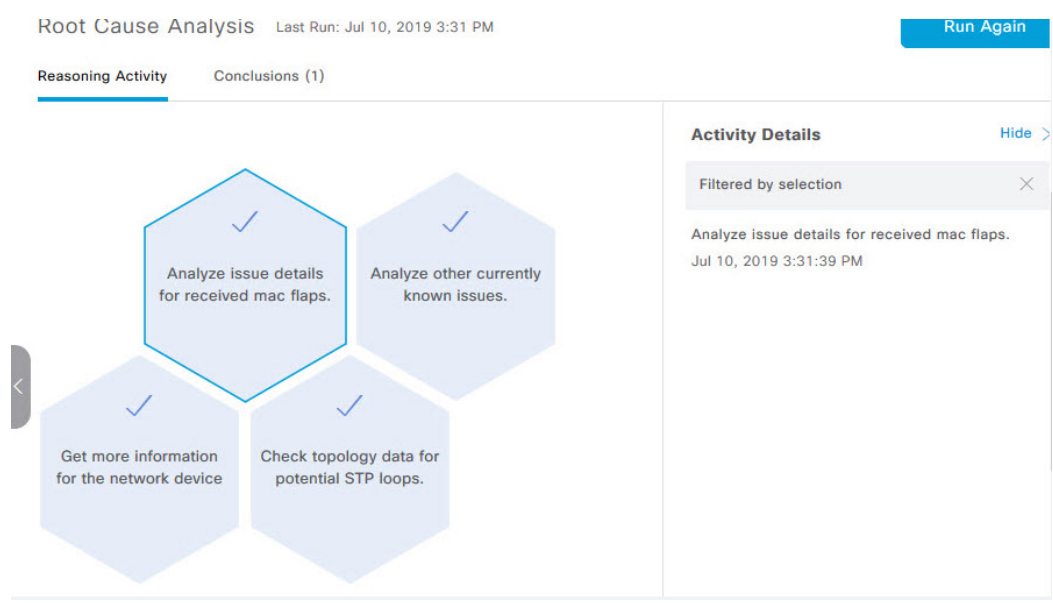



Note The scale constraints for the Layer 2 Loop are the following:

- Number of VLANS is 10.
- Number of devices per VLAN is 30.

For the Layer 2 Loop issue, which supports Machine Reasoning, the **Issue Instance Details** slide-in pane contains the following information:

| Issue Instance Details (Second Slide-In Pane) | |
|-----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Item | Description |
| Status drop-down list | <p>Allows you to change the status of the issue. Do the following:</p> <ul style="list-style-type: none"> • To resolve an issue, from the Status drop-down list, choose Resolve. • To stop an issue from being reported, do the following: <ol style="list-style-type: none"> 1. From the Status drop-down list, choose Ignore. 2. Set the number of hours to ignore the issue on the slider, and then click Confirm. |
| Note icon (📄) | If you're an admin user, you can add, edit, and delete notes. Click the Note icon (📄) and then click Add . If you're any other type of user, you can only view note information. |
| Summary | Brief summary of the issue, which can include information, such as device, role, time, location, and potential root cause. This also provides the initial assessment, such as the VLANs and ports in the potential loop. |
| Problem Details | <p>Provides a brief text that describes the problem along with the following:</p> <ul style="list-style-type: none"> • Relevant Events drop-down list: Lists the events that occurred during the loop. Click an event to view details in the side pane. • Potential Loop Details drop-down list: Provides loop information, such as the device, role, port in the loop, duplex mode, and VLAN that was involved in the loop. |

| Issue Instance Details (Second Slide-In Pane) | |
|-----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Item | Description |
| Root Cause Analysis | <p>The Machine Reasoning Engine (MRE) allows you to perform complex root cause analysis and suggests corrective actions.</p> <ol style="list-style-type: none"> 1. Click Run Machine Reasoning to allow the MRE to start troubleshooting. After the troubleshooting is completed, the Machine Reasoning Completed pop-up dialog box appears. 2. In the pop-up dialog box, click View Details. The Root Cause Analysis area appears with the Conclusions tab opened by default providing the details of the root cause analysis. 3. From the Conclusions area, click View Relevant Activities to view activity details. The activity shows commands that were used at each step of the root cause analysis. 4. Click the  icon to provide your feedback, whether the information on this page was helpful or not, and then click Submit. 5. Click the Reasoning Activity tab to understand how the MRE reached that conclusion. Each reasoning activity is provided in hexagon shaped blocks as shown in the following figure. Click each hexagon shaped block to view activity details in the right pane. <p>To cancel the reasoning activity while it is running, click Stop.</p> <p>Note The check mark indicates that the step is complete.</p> <p>Figure 4: Reasoning Activity</p>  <p>The screenshot shows the 'Reasoning Activity' tab selected. It displays four hexagonal activity blocks, each with a checkmark indicating completion. The blocks are: 'Analyze issue details for received mac flaps.', 'Analyze other currently known issues.', 'Get more information for the network device', and 'Check topology data for potential STP loops.'. To the right, the 'Activity Details' pane is open, showing a filter 'Filtered by selection' and the details for the selected activity: 'Analyze issue details for received mac flaps.' with a timestamp of 'Jul 10, 2019 3:31:39 PM'. A 'Run Again' button is visible in the top right corner of the interface.</p> <ol style="list-style-type: none"> 6. Click Run Again if you want to rerun the MRE. |
| Topology icon | Click the  icon to view the topology of the network segment in which the loop occurred. |


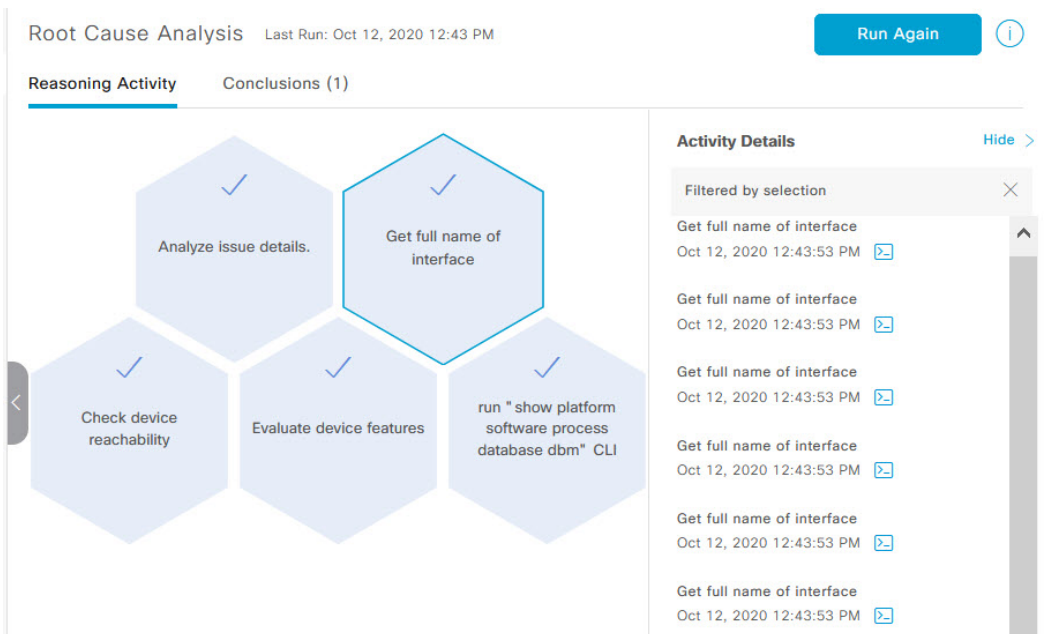
Issue Instance Details for a PoE Issue



Note The **Issue Instance Details** slide-in pane is part of the **Open Issues** workflow. See [Step 4 in View Open Issues, on page 2](#).

For a PoE issue, which supports Machine Reasoning, the Issue Instance Details slide-in pane contains the following information:

| Issue Instance Details (Second Slide-In Pane) | |
|-----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Item | Description |
| Status drop-down list | Allows you to change the status of the issue. Do the following: <ul style="list-style-type: none"> • To resolve an issue, from the Status drop-down list, choose Resolve. • To stop an issue from being reported, do the following: <ol style="list-style-type: none"> 1. From the Status drop-down list, choose Ignore. 2. Using the slider, set the number of hours to ignore the issue and click Confirm. |
| Note icon (📄) | If you're an admin user, you can add, edit, and delete notes. Click the Note icon (📄) and then click Add . If you're any other type of user, you can only view note information. |
| Summary | Summary of the issue, which can include information, such as device, role, time, location, and potential root cause. |
| Problem Details | Provides a brief description of the problem along with the following: <ul style="list-style-type: none"> • Event Types tabs: Contains tabs for the types of events that occurred. Click an event tab to view the list of errors for the event type. • Errors: Errors that occurred for each event type. The errors are refreshed based on the Event Types tab you click. • Detailed Information Click an error to view additional information about it. |

| Issue Instance Details (Second Slide-In Pane) | |
|-----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Item | Description |
| Root Cause Analysis | <p>The Machine Reasoning Engine (MRE) allows you to perform complex root cause analysis and suggests corrective actions.</p> <ol style="list-style-type: none"> 1. Click Run Machine Reasoning to allow the MRE to start troubleshooting. After the troubleshooting is completed, the Machine Reasoning Completed dialog box appears. 2. In the pop-up dialog box, click View Details. The Root Cause Analysis area appears with the Conclusions tab opened by default providing the details of the root cause analysis. 3. From the Conclusions area, click View Relevant Activities to view activity details. The activity shows commands that were used at each step of the root cause analysis. 4. Click the  icon to provide your feedback, whether the information on this page was helpful or not. 5. Click the Reasoning Activity tab to understand how the MRE reached that conclusion. Each reasoning activity is provided in hexagon shaped blocks as shown in the following figure. Click each hexagon shaped block to view Activity Details in the right pane. <p>To cancel the reasoning activity while it is running, click Stop.</p> <p>Note The check mark indicates that the step is complete.</p> <p>Figure 5: Reasoning Activity</p>  <p>The screenshot shows the 'Root Cause Analysis' interface. At the top, it says 'Last Run: Oct 12, 2020 12:43 PM' and has a 'Run Again' button. Below this are two tabs: 'Reasoning Activity' (selected) and 'Conclusions (1)'. The 'Reasoning Activity' section displays five hexagonal blocks, each with a checkmark and a description: 'Analyze issue details.', 'Get full name of interface', 'Check device reachability', 'Evaluate device features', and 'run "show platform software process database dbm" CLI'. The 'Get full name of interface' block is highlighted with a blue border. To the right, the 'Activity Details' pane is open, showing a list of activities filtered by selection. The list includes six entries, all with the text 'Get full name of interface' and the timestamp 'Oct 12, 2020 12:43:53 PM', each followed by a small icon.</p> 6. Click Run Again if you want to rerun the MRE. |

Troubleshoot Wired Client Issues Using MRE

Use this procedure to view wired client issues detected by Assurance and troubleshoot them using the MRE workflow. For a list of wired client issues that support MRE, see [MRE Issues, on page 47](#).

Before you begin

Make sure that the MRE knowledge base is updated with the latest knowledge packs. See [Update the Machine Reasoning Knowledge Base](#).

Step 1 From the top-left corner, click the menu icon and choose **Assurance > Health**.

The **Overall** health dashboard is displayed.

Step 2 Click the **Client** tab.

The **Client** health dashboard appears.

Step 3 In the **Wired Clients** summary area, click **View Details** to open a slide-in pane.

Step 4 In the slide-in pane, in the **Wired Clients** chart, click **Authentication** or **DHCP**.

If you click **Authentication**, the following information is displayed below the chart: Top Authentication Failure Reason, Top Location, Top Switch, Top Host Device Type. A table is also displayed, which provides a list of clients that failed authentication.

If you click **DHCP**, the following information is displayed below the chart: Top DHCP Failure Reason, Top Location, Top Switch, Top Host Device Type. A table is also displayed.



Step 5 Do one of the following:


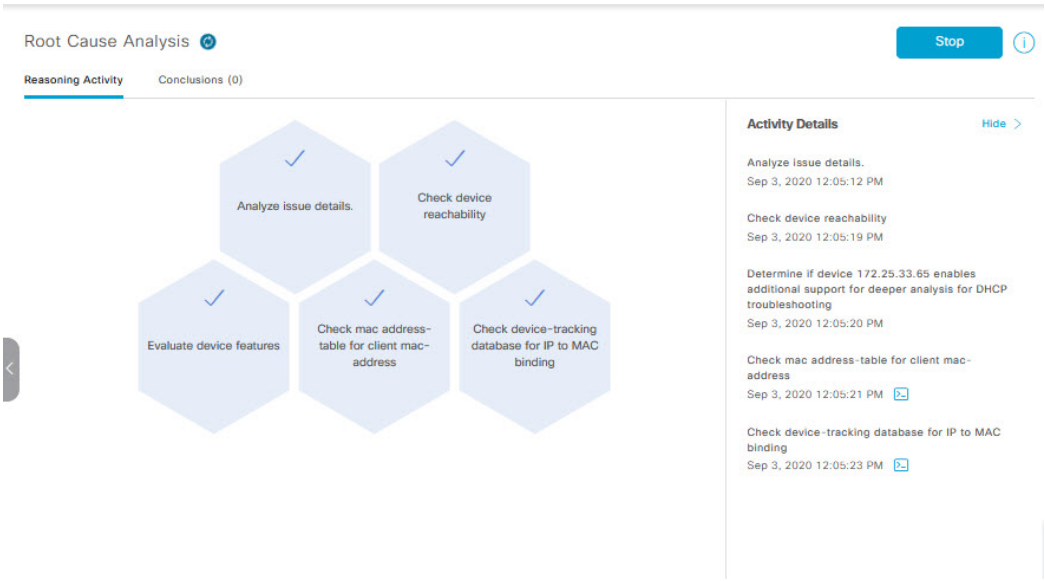
- If you are a user with SUPER-ADMIN-ROLE privileges, enter the client's MAC address in the search tool.
- In the table, from the **Identifier** column, click the hyperlinked identifier.

The **Client 360** window for the client is displayed.

Step 6 In the **Client 360** window, from the **Issues** dashlet, click an authentication or DHCP issue.

The **Issue Details** window is displayed with the following information:

| Issue Details | |
|---------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Item | Description |
| Status drop-down list | Provides the current status of the issue, which you can change. Do the following: <ul style="list-style-type: none"> • To resolve an issue, from the Status drop-down list, choose Resolve. • To stop an issue from being reported, do the following: <ol style="list-style-type: none"> a. From the Status drop-down list, choose Ignore. b. Set the number of hours to ignore the issue on the slider, and then click Confirm. |
| Note icon () | If you're an admin user, you can add, edit, and delete notes. Click the Note icon () and then click Add . If you're any other type of user, you can only view note information. |

| Issue Details | |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Item | Description |
| Summary | Brief summary of the issue, which can include information, such as device, role, time, location, and potential root cause. |
| Root Cause Analysis | <p>The Machine Reasoning Engine (MRE) allows you to perform complex root cause analysis and suggests corrective actions.</p> <ol style="list-style-type: none"> Click Run Machine Reasoning to allow the MRE to start troubleshooting. After the troubleshooting is completed, the Machine Reasoning Completed dialog box appears. In the dialog box, click View Details. The Root Cause Analysis area appears with the Conclusions tab opened by default providing the details of the root cause analysis. From the Conclusions area, click View Relevant Activities to view activity details. Click the  icon to provide your feedback, whether the information on this page was helpful or not, and then click Submit. Click the Reasoning Activity tab to understand how the MRE reached that conclusion. Each reasoning activity is provided in hexagon shaped blocks, as shown in the following figure. Click each hexagon shaped block to view activity details in the right pane. <p>To stop the reasoning activity while it is running, click Stop.</p> <p>Note The check mark indicates that the step is complete.</p> <p>Figure 6: Reasoning Activity</p>  <p>The screenshot shows the 'Root Cause Analysis' interface. At the top, there is a 'Reasoning Activity' tab and a 'Conclusions (0)' tab. A 'Stop' button is visible in the top right. The main area displays five hexagonal blocks, each with a checkmark and a description: 'Analyze issue details.', 'Check device reachability', 'Evaluate device features', 'Check mac address-table for client mac-address', and 'Check device-tracking database for IP to MAC binding'. On the right, the 'Activity Details' pane is open, showing a list of activities with timestamps and status icons.</p> <ol style="list-style-type: none"> Click Run Again if you want to rerun the MRE. |

View Resolved Issues

Use this procedure to view all resolved issues, which fall under the following categories:

- Threshold-based issues: Issues detected by Assurance.
- AI-driven issues: Issues detected by Cisco AI Network Analytics. These issues are triggered based on deviations from the predicted baseline for your specific network environment.

Before you begin

To view AI-driven resolved issues, make sure that you have configured Cisco AI Network Analytics data collection. See [Configure Cisco AI Network Analytics](#).






Step 1 From the top-left corner, click the menu icon and choose **Assurance > Issues and Events**.

The **Open Issues** dashboard appears.

Step 2 From the **Status** drop-down list, choose **Resolved**.


The **Resolved Issues** window appears.

Step 3 Use the **Resolved Issues** window to view the following information:


| Resolved Issues Window | |
|-------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Item | Description |
|  | <ul style="list-style-type: none"> • Click  Global  in the top menu bar to choose the site, building, or floor from the Site hierarchy. • Click  next to the location icon and choose Site Details to view the Sites table. • Choose Hierarchical Site View or Building View from the drop-down list. Based on what you choose, the table is refreshed. • From the Go to sites column, click  for a site or building to display data only for that location on the Resolved Issues dashboard. |
| 24 Hours drop-down list | <p>Allows you to display information on the window based on the time range you select. The default is 24 Hours. Do the following:</p> <ol style="list-style-type: none"> From the 24 Hours drop-down list, choose a time range: 3 hours, 24 hours, or 7 days. Specify the Start Date and time and the End Date and time. Click Apply. <p>This sets the range of the timeline.</p> |

| Resolved Issues Window | |
|------------------------|-------------------------------------------------------------------------------------------------------------------------|
| Item | Description |
| Timeline slider | Allows you to specify a more granular time range. Click and drag the timeline boundary lines to specify the time range. |

Step 4 Click the **All**, **P1**, **P2**, **P3**, **P4**, or **AI-Driven** tab to display a list of issues in that category in the **Issue Type** table.

| Issue Type Table in the Resolved Issues Window | |
|------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Item | Description |
| Total Resolved | Provides the total count of resolved issues. The Total Resolved value changes depending on the tab you choose. Options are All (the default), P1 , P2 , P3 , P4 , and AI-Driven . |
| Priority | Preassigned priority level of the issue type. |
| Issue Type | Type of issue. Note For AI-driven issues, the  icon appears in front of the issue type. |
| Device Role | Role assigned to the device on which the issue was detected. Roles are Access, Core, Distribution, Border Router, or Unknown. |
| Category | Category under which the issue type falls, such as Connectivity, Availability, Onboarding, and Utilization. |
| Issue Count | Number of times this type of issue occurred. |
| Site Count (Area) | Number of sites where this type of issue occurred. |
| Device Count | Number of devices that were impacted by this type of issue. |
| Last Occurred Time | Most recent date and time this issue occurred. |


Step 5 From the **Issue Type** table, click an issue type.

The first slide-in pane, **Issue Instances**, lists all the resolved issues for that issue type and information such as site, device, device type, occurrence, last occurrence timestamp, last updated timestamp, and the name of the entity that updated the issue. If you're an admin user, you can add, edit, and delete notes. Click the Note icon () and then click **Add**. If you're any other type of user, you can only view note information.

If the issue condition no longer exists, the system automatically resolves the issue and displays **System** in the **Updated By** column. See [Automatic Issue Resolution, on page 22](#).

Step 6 From the **Issue** column in the **Issue Instances** slide-in pane, click an issue.

A second slide-in pane, **Issue Instance Details**, provides details about the issue, the name of the entity that resolved the issue, and the timestamp. Depending on the issue, the description and suggested actions are displayed. If you're an admin

user, you can add, edit, and delete notes. Click the Note icon () and then click **Add**. If you're any other type of user, you can only view note information.

View Ignored Issues

Use this procedure to view all issues that are marked as ignored. Ignored issues fall under the following categories:

- Threshold-based issues: Issues detected by Assurance.
- AI-driven Issues: Issues detected by Cisco AI Network Analytics. These issues are triggered based on deviations from the predicted baseline for your specific network environment.

Before you begin

To view the AI-driven ignored issues, make sure that you have configured Cisco AI Network Analytics data collection. See [Configure Cisco AI Network Analytics](#).






Step 1 From the top-left corner, click the menu icon and choose **Assurance > Issues and Events**.

The **Open Issues** dashboard appears.

Step 2 From the **Status** drop-down list, choose **Ignored**.


The **Ignored Issues** window appears.

Step 3 Use the **Ignored Issues** window to view the following information:

| Ignored Issues Window | |
|---------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Item | Description |
|  Global | <ul style="list-style-type: none"> • Click  Global  in the top menu bar to choose the site, building, or floor from the Site hierarchy. • Click  next to the location icon and choose Site Details to view the Sites table. • Choose Hierarchical Site View or Building View from the drop-down list. Based on what you choose, the table is refreshed. • From the Go to sites column, click  for a site or building to display data only for that location on the Ignored Issues dashboard. |

| Ignored Issues Window | |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Item | Description |
| 24 Hours drop-down list | <p>Allows you to display information on the window based on the time range you select. The default is 24 Hours. Do the following:</p> <ol style="list-style-type: none"> From the 24 Hours drop-down list, choose a time range: 3 hours, 24 hours, or 7 days. Specify the Start Date and time and the End Date and time. Click Apply. <p>This sets the range of the timeline.</p> |
| Timeline slider | Allows you to specify a more granular time range. Click and drag the timeline boundary lines to specify the time range. |


Step 4 Click the **All**, **P1**, **P2**, **P3**, **P4**, or **AI-Driven** tab to display a list of issues in that category in the **Issue Type** table.

| Issue Type Table in the Ignored Issues Window | |
|-----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Item | Description |
| Total Ignored | <p>Provides the total count of ignored issues.</p> <p>The Total Ignored value changes depending on the tab you choose. Options are All (the default), P1, P2, P3, P4, and AI-Driven.</p> |
| Priority | Preassigned priority level of the issue type. |
| Issue Type | <p>Type of issue.</p> <p>Note For AI-driven issues, the  icon appears in front of the issue type.</p> |
| Device Role | Role assigned to the device on which the issue was detected. Roles are Access, Core, Distribution, Border Router, or Unknown. |
| Category | Category under which the issue type falls, such as Connectivity, Availability, Onboarding, and Utilization. |
| Issue Count | Number of times this type of issue occurred. |
| Site Count (Area) | Number of sites where this type of issue occurred. |
| Device Count | Number of devices that were impacted by this type of issue. |
| Last Occurred Time | Most recent date and time this issue occurred. |

Step 5 From the **Issue Type** table, click an issue type.

The first slide-in pane, **Issue Instances** lists all the ignored issues for that issue type and information such as site, device, device type, occurrence, and the time stamp of the last occurrence.

Step 6 From the **Issue** column in the **Issue Instances** slide-in pane, click an issue.

A second slide-in pane, **Issue Instance Details**, provides details about the issue. Depending on the issue, the description and suggested actions are displayed. If you're an admin user, you can add, edit, and delete notes. Click the Note icon () and then click **Add**. If you're any other type of user, you can only view note information.

Resolve or Ignore Issues


Use this procedure to resolve or ignore a bulk of issues or to resolve or ignore a single issue.

Step 1 From the top-left corner, click the menu icon and choose **Assurance > Issues and Events**.

The **Open Issues** dashboard appears.

Step 2 To resolve or ignore a bulk of issues, do the following:

a) From the **Issue Type** table in the **Open Issues** dashboard, click an issue type.

The first slide-in pane, **Issue Instances**, opens, which lists all the open issues for that issue type. This slide-in-pane allows you to resolve or ignore a bulk of issues. If you're an admin user, you can add, edit, and delete notes. Click the Note icon () and then click **Add**. If you're any other type of user, you can only view note information.

b) Do one of the following:

- To resolve or ignore specific issues, check the check boxes adjacent to those issues.
- To resolve or ignore all open issues that are displayed in the browser window for an issue type, check the check box adjacent to the **Issue** column. All the issues that are displayed in the browser window are selected.
- If the open issue count is more than 25 (for example, 100), the first 25 issues are displayed in the browser window. To select all the open issues, do the following:

1. Check the check box adjacent to the **Issue** column.

The first 25 issues are selected and the **Select all *number* open issues** tab appears next to the **Actions** drop-down list.

2. Click the **Select all *number* open issues** to select all open issues for that issue type (for example, all 100 issues).

3. (Optional) To view the next 25 issues in the browser window, click **Show More** located on the bottom of the page. The next 25 issues are appended to the browser window increasing the displayed issue count to 50. Click **Show More** to view the next 25 issues on the browser window, and so on.

c) To resolve the issues, from the **Actions** drop-down list, choose **Resolve**.

A Warning dialog box appears. Click **Yes** in the Warning dialog box to proceed with the action.

After the issues are resolved, the **View resolved issues** tab is displayed. Click the **View resolved issues** to open the **Resolved Issues** window.

d) To ignore the issues, from the **Actions** drop-down list, choose **Ignore**.


Set the number of hours to ignore the issues on the slider, and then click **Confirm**.

After the issues are ignored, the **View ignored issues** tab is displayed. Click the **View ignored issues** tab to open the **Ignored Issues** window.

Note If you try to resolve or ignore more than 750 issues, a warning message appears letting you know that it might take up to a minute to complete the action.

Step 3 To resolve or ignore a single issue, do the following:

a) From the **Issue** column in the **Issue Instances** slide-in pane (first slide-in pane), click an issue.

A second slide-in pane, **Issue Instance Details**, opens, which provides details about the issue. This second slide-in-pane allows you to resolve or ignore the issue that you are viewing. If you're an admin user, you can add, edit, and delete notes. Click the Note icon () and then click **Add**. If you're any other type of user, you can only view note information.

b) To resolve an issue, from the **Status** drop-down list, choose **Resolve**.

c) To stop an issue from being reported, do the following:

1. From the **Status** drop-down list, choose **Ignore**.
2. Set the number of hours to ignore the issue on the slider, and then click **Confirm**.

No Activity on Radio Issue Triggers

A "No Activity on Radio" issue is triggered when all of the following conditions are met for 60 minutes, which is the default trigger time.



Note To change the default trigger time, choose **Assurance > Manage > Issue Settings**. See [Manage Global Issue Settings, on page 25](#).

- The AP radio operation state is **up**.
- The AP mode is Local or FlexConnect.
- The client count on this radio is equal to 0.
- The RX data or management frame count is *not* increasing.
- The AP radio channel utilization is equal to 0.
- The AP is not an **isolated** AP.

Automatic Issue Resolution

For the following issues, if the issue condition no longer exists, the system automatically resolves the issue:

| Issue Name |
|------------------------------------------------|
| Wireless Controller/Switch/Router unreachable. |
| Switch fan failure. |
| Switch power failure. |
| Interface is down. |
| Stack Member Removal. |
| Stack Port Link has failed |
| AP Disconnect from wireless controller. |
| No activity on radio. |

The following issues are auto resolved based on time duration since the last occurrence:

| Issue Name | Time Duration to Auto Resolve |
|--------------------------------------------------|-------------------------------|
| Network Device Interface Connectivity - BGP Flap | 24 hours |
| Interface is Flapping On Network Device | 24 hours |
| Network Device HA Switchover | 24 hours |
| WLC Reboot Unexpectedly | 24 hours |
| AP Reboot Crash | 24 hours |
| Device Reboot | 24 hours |
| AP Anomaly | 24 hours |
| AP Flap | 24 hours |
| Poor RF (5 GHz) on a floor | 24 hours |
| Radio Poor RF (6 GHz) | 24 hours |
| Poor RF (2.4 GHz) on a floor | 24 hours |
| AP CPU High Utilization | 24 hours |
| AP Memory High Utilization | 24 hours |
| AP License Exhausted on WLC | 24 hours |
| Switch experiencing high memory utilization | 24 hours |
| Device experiencing high memory utilizatio | 24 hours |
| Switch experiencing high CPU utilization | 24 hours |
| Router experiencing high CPU utilization | 24 hours |

| Issue Name | Time Duration to Auto Resolve |
|---------------------------------------------------------------------------|-------------------------------|
| High input/output utilization on Switch interfaces | 24 hours |
| High input/output error on Switch interfaces | 24 hours |
| High input/output discard on Switch interfaces | 24 hours |
| High input/output discard on Switch WAN interfaces | 24 hours |
| High input/output utilization on Switch WAN interfaces | 24 hours |
| High input/output utilization on Router interfaces | 24 hours |
| High input/output utilization on Router WAN interfaces | 24 hours |
| High input/output discard on Router interfaces | 24 hours |
| High input/output discard on Router WAN interfaces | 24 hours |
| High input/output utilization on Router WAN interfaces | 24 hours |
| Fabric BGP session from Border node to Transit Control Plane node is down | 6 hours |
| Fabric BGP session status is down with Peer Device (per VN) | 6 hours |
| BGP session from Border node to Control Plane node is down | 6 hours |
| Fabric Border node internet is unavailable (per VN) | 6 hours |
| Fabric Border node remote internet is unavailable (per VN) | 6 hours |
| Fabric AAA Server Status | 6 hours |
| Fabric LISP Session Status to Control Plane node | 6 hours |
| Fabric LISP PubSub session status per VN is dow | 6 hours |
| Cisco TrustSec Environment data is not complete on Fabric node | 6 hours |
| Fabric LISP Extranet policy status is down | 6 hours |
| High input/output utilization on Third Party Device interfaces | 24 hours |
| High input/output error on Third Party Device interfaces | 24 hours |
| High input/output discard on Third Party Device interfaces | 24 hours |
| High input/output utilization on Third Party Device WAN interfaces | 24 hours |
| High input/output discard on Third Party Device WAN interfaces | 24 hours |
| TCAM Utilization High Issues | 24 hours |

| Issue Name | Time Duration to Auto Resolve |
|-------------------------------------------------------|-------------------------------|
| Fabric Devices Connectivity - Border Underlay | 6 hours |
| Fabric Devices Connectivity - Border Overlay | 6 hours |
| Fabric Devices Connectivity - Multicast RP | 6 hours |
| Fabric Devices Connectivity - Control Underlay | 6 hours |
| Fabric Devices Connectivity - Control Border Underlay | 6 hours |
| Fabric Devices Connectivity - AAA Server | 6 hours |
| Fabric Devices Connectivity - DHCP Overlay | 6 hours |
| Fabric Devices Connectivity - DHCP Underlay | 6 hours |
| Fabric Devices Connectivity - DNS Overlay | 6 hours |
| Fabric Devices Connectivity - DNS Underlay | 6 hours |
| Fabric WLC to MapServer Connectivity | 6 hours |
| Fabric LISP session status on Control Plane node | 6 hours |
| Fabric LISP PubSub session status is down | 6 hours |
| Fabric Border node internet is unavailable | 6 hours |
| Fabric Border node remote internet is unavailable | 6 hours |
| Fabric BGP session status is down with Peer Device | 6 hours |

You can view whether an issue is resolved automatically or manually. In the **Issue Settings > Global Profile** window, the **Issue Resolution** column displays either **Auto** for issues that are resolved by the system or **Manual** for issues that you must resolve.

After the issue is resolved, the **Updated By** column in the **Resolved Issues > Issue Instance** slide-in pane displays **System**. See [View Resolved Issues, on page 17](#).

Manage Global Issue Settings

Use this procedure to manage the settings for issues. You can enable or disable specific issues that can be triggered, change the priority for issues, change the threshold for when an issue is triggered, and subscribe to external notifications for issues when they are triggered.

Step 1 From the top-left corner, click the menu icon and choose **Assurance > Issue Settings**.

The **Issue Settings** window appears, with the **Global Profile** tab selected.

Step 2 Set the **DEVICE TYPE** and **CATEGORY** filters to view the type of issues you want to configure.

To view the AI-driven issues, click the **AI-Driven** tab in the **CATEGORY** filter.

Step 3 Click an issue in the **Issue Name** column to open a slide-in pane with the following settings:

Note For some issues, changes made to the settings are shared across multiple device types. In the slide-in pane, hover your cursor over the information icon (i) to display the affected device types.

- a) To enable or disable if the issue can be triggered, click the **Enabled** toggle.
- b) To set the issue priority, click the **Priority** drop-down list and select the priority. The options are:
 - **P1**: A critical issue that needs immediate attention which can result in wider impact on network operations.
 - **P2**: A major issue that can potentially impact multiple devices or clients.
 - **P3**: A minor issue that has a localized or minimal impact.
 - **P4**: A warning issue that may not be an immediate problem but addressing it can optimize the network performance.
- c) (For certain issues) In the **Trigger Condition** area, you can change the threshold value for when the issue is reported.

Note For "No Activity on Radio" trigger conditions, see [No Activity on Radio Issue Triggers, on page 22](#).

Examples of a trigger condition:

```
No Activity on Radio(2.4 GHz) >= 60 minutes.
```

```
Memory Utilization of Access Points greater than 90%
```

- d) (Optional) If there are any changes to the settings, you can hover your cursor over **View Default Settings** to display the default issues. Click **Use Default** to restore all the issue settings to the default values.
- e) Click **Apply**.

Step 4 (For certain issues) Click **Manage Subscription** to subscribe to external notifications for supported issues when they are triggered. See [Enable Issue Notifications, on page 29](#).

Manage User-Defined Issue Settings

Use this procedure to manage user-defined issue settings. You can create user-defined issues, enable or disable specific issues that can be triggered, change the priority for issues, change the threshold for when an issue is triggered, and subscribe to external notifications for issues when they are triggered.

Step 1 From the top-left corner, click the menu icon and choose **Assurance > Issue Settings**.

The **Issue Settings** window appears, with the **Global Profile** tab selected.

Step 2 Click the **User Defined** tab to view the list of user-defined issues.

Step 3 Click an issue in the **Issue Name** column to open the **Create an Issue** slide-in pane.

Step 4 To configure user-defined issues based on the syslog details, do the following in the **Create an Issue** slide-in pane:

- a) In the **Issue Name** field, enter the issue name.
- b) In the **Description** field, enter the description of the issue.

- c) In the **Syslog Details**, from the **Severity** drop-down list, choose a severity from 0 to 6.
- d) In the **Facility** field, enter the facility name.
- e) In the **Mnemonic** field, enter the mnemonic name and click **Next**.
- f) In the **Message Pattern** field, enter the syslog message. You can preview the syslog message below the message pattern.
- g) In the **Occurrences** field, enter the value for occurrences.
- h) In the **Duration** drop-down list, choose the duration of an issue.
- i) To enable or disable if the issue can be triggered, click the **Enabled** toggle.
- j) To set the issue priority, click the **Priority** drop-down list and choose a priority level:
 - **P1**: A critical issue that needs immediate attention and can have a wide impact on network operations.
 - **P2**: A major issue that can potentially impact multiple devices or clients.
 - **P3**: A minor issue that has a localized or minimal impact.
 - **P4**: A warning issue that may not be an immediate problem but addressing it can optimize the network performance.
- k) To enable or disable the issue notification, click the **Notification** toggle.
- l) Click **Save**.

Step 5

Click **Manage Subscription** to subscribe to external notifications for issues when they are triggered. See [Enable Issue Notifications, on page 29](#). You will create a subscription for the User Defined Issue Notification event, shown as follows:

Figure 7: User Defined Issue Notification event

Step 1 - Select Site and Events

Pick the site and events for your notification

Select a site ▼

Q user X 🔖

1 Selected

| <input checked="" type="checkbox"/> Event Name | Channels Supported |
|---------------------------------------------------------------------|-----------------------------------|
| <input checked="" type="checkbox"/> User Defined Issue Notification | REST SYSLOG EMAIL WEBEX PAGERDUTY |

Manage Custom Issue Settings

You can create custom issue settings for a specific site or group of sites. These settings are called network profiles for Assurance and can be managed from both Assurance and Cisco DNA Center.

By creating a network profile for Assurance, you can control which issue settings are monitored, and you can change the issue priority.

Notes:

- Synchronization to the network device health score is available only for global issue settings, not custom issue settings. For information, see [Monitor and Troubleshoot the Health of a Device](#).
- Some global issues are not customizable. These issues are not displayed in the list of custom issues for you to modify.
- To display modified issues at the top of the list, sort by **Last Modified**.
- To delete custom settings, you need to unassign all the sites first.

Step 1 From the top-left corner, click the menu icon and choose **Assurance > Issue Settings**.

The **Issue Settings** window appears, with the **Global Profile** tab selected.

Step 2 Click the **Custom Profile** tab.

Step 3 Click **+Add a Profile**.

Step 4 In the **Profile Name** field, enter a valid profile name and click **Next**.

Cisco DNA Center adds the profile and the profile table is displayed with Profile Name, Sites, and Action.

Step 5 To assign the profile to sites, click **Assign Sites** in the **Sites** column name to open a **Add Sites to Profile** slide-in pane. Check the check box next to the sites that you want to associate with this profile and click **Save**.

The **Edit Profile** window appears.

Note You can select a parent node or the individual sites. If you select a parent node, all the children under the parent node are also selected. You can uncheck the check box to deselect a site.

Step 6 Set the **DEVICE TYPE** and **CATEGORY** filters to view the type of issues you want to configure.

Step 7 Click the **User Defined** tab to view the list of user-defined issues.

Step 8 Click an issue in the **Issue Name** column to open a slide-in pane with the settings.

Note For some issues, changes made to the settings are shared across multiple device types. In the slide-in pane, Cisco DNA Center displays a caution that indicates the affected device types.

Step 9 To enable or disable whether Cisco DNA Center monitors the issue, click the **Enabled** toggle button.

Step 10 To set the issue priority, click the **Priority** drop-down list and select the priority. The options are:

- **P1**: A critical issue that needs immediate attention which can result in wider impact on network operations.
- **P2**: A major issue that can potentially impact multiple devices or clients.
- **P3**: A minor issue that has a localized or minimal impact.
- **P4**: A warning issue that may not be an immediate problem but addressing it can optimize the network performance.

Step 11 (For certain issues) In the **Trigger Condition** area, you can change the threshold value for when the issue is reported.

Examples of a trigger condition:

No Activity on Radio(2.4 GHz) >= 60 minutes.

Memory Utilization of Access Points greater than 90%

Step 12 (Optional) If there are any changes to the settings, you can hover your cursor over **View Default Settings** to display the default settings. Click **Use Default** to restore all the issue settings to the default values.

Step 13 Click **Apply**.

Step 14 (For certain issues) Click **Manage Subscription** to subscribe to external notifications for supported issues when they are triggered.

Step 15 Click **Edit** in the issue syslog message to edit a user-defined issue and click **Save**.

Step 16 Click **Done**.

The newly added profile appears on the **Issue Settings** window, in the **Custom Profile** tab.

Enable Issue Notifications

Use this procedure to receive external notifications for when specific issues are triggered in Assurance. When an issue is triggered and there is a status change, Assurance can generate a REST or email notification.

Step 1 From the top-left corner, click the menu icon and choose **Assurance > Issue Settings**.

The **Issue Settings** window is displayed.

Step 2 Click **Manage Subscription**.

The **Platform > Developer Toolkit > Event Notifications** window is displayed.

Each notification is represented by a tile and contains a link to view notification details.

Step 3 From the **CHANNELS** area in the left pane, click the radio button next to the channels for which you want to view the respective notification tiles.

The supported channels are **REST**, **PAGERDUTY**, **SNMP**, **SYSLOG**, **WEBEX** and **EMAIL**. Assurance events do not support SNMP.

- Note**
- You must create a notification for an event with respective channels and trigger the notification. For more information, see **Create an Event Notification** in the [Cisco DNA Center User Guide](#).
 - One event notification supports more than one channel.

Step 4 Click a notification tile link for which you want to view the notification details.

The **Notification Details** slide in pane displays the following notification details based on the selected channel:

- **Name:** Name of the event.
- **Description:** Event description
- **Sites**
- **Events**
- **REST:** Appears only when you want to view REST notification details. The **REST** area shows the following information:
 - **URL:** URL address of the REST API endpoint that event will be sent to.
 - **Method:** Either the PUT or POST method.

- **Trust certificate:** Whether a trust certificate is required for REST API endpoint notification.
- **Headers:** The **Header Name** and **Header Value**.
- **PAGERDUTY:** Appears only when you want to view PAGERDUTY notification details. The **PAGERDUTY** area shows the following information:
 - PagerDuty Events API URL
 - PagerDuty Integration Key
 - PagerDuty Events API Version
- **SNMP:** Appears only when you want to view **SNMP** notification details.
- **SYSLOG:** Appears only when you want to view **SYSLOG** notification details.
- **WEBEX:** Appears only when you want to view **WEBEX** notification details.
- **EMAIL:** Appears only when you want to view **EMAIL** notification details. The **EMAIL** area shows the email recipients **From** and **To** along with email **Subject**.

Step 5 In the **Notification Details** slide-in pane, click the toggle button at the top-right corner to enable or disable the respective notification.

Step 6 To edit a particular notification, click the **Actions** drop-down list and choose **Edit**.

Step 7 In the **EDIT NOTIFICATION** window, configure the following based on the selected channel:

- a. In the **Name** field, enter a unique name.
- b. In the **Description** field, enter the description of respective event.
- c. Expand the **Site and Events** and choose a site from the **Select a site** drop-down list.
- d. Click the plus icon next to an event, or click **Add All** to add all the events to the respective notification.
- e. To remove an event from the notification, click the cross icon next to an event that you want to remove, or click **Remove All** to remove all events from the respective notification.
- f. Expand **Configuration** to edit the configuration of the selected notification channel.

To specify details in the **Configuration** area, see **Create an Event Notification** in the [Cisco DNA Center User Guide](#).

Note In the **Configuration** area, the fields shown depend on the type of selected notification channel.

Step 8 Click the toggle button at the top-right corner to toggle between the tile view and list view.

Step 9 Click the **Event Catalog** tab to view the list of created events.

Note You can adjust the events that are displayed by entering a keyword in the **Search** field.

Step 10 Review the data on an individual event within the table.

The following **Event Details** tab data is displayed:

- **Description:** Brief description of the event and how it is triggered.
- **Event ID:** Identification number of the event.

- **Version:** Version number of the event.
- **Namespace:** Namespace of the event.
- **Severity:** 1 through 5.
 - Note** Severity 1 is the most important or critical priority and should be assigned for this type of an event.
- **Domain:** REST API domain to which the event belongs.
- **Subdomain:** Subgroup under the REST API domain to which the event belongs.
- **Category:** Error, Warn, Info, Alert, Task Progress, Task Complete.
- **Note:** Additional information about the event or to assist in further understanding the event.
- **Event Link:** Event broadcast using REST URL.
- **Tags:** Tags indicate what Cisco DNA Center component is affected by the event.
- **Channels:** What channels are supported for the event notifications (REST API, email, webex, and so on).
- **Model Schema:** Presents model schema about the event:
 - **Details:** Example of model schema detail for the event.
 - **REST Schema:** REST schema format for the event.

Step 11 Click the **Notifications** tab to view the active notification associated to the respective event.

Assurance, Cisco AI Network Analytics, and MRE Issues

Router Issues

The following table lists the router issues detected by Assurance:

| Router Issues | | |
|---------------|--------------------------------------------------|----------------------------------------------------------------------------------------------------------|
| Category | Issue Name | Summary |
| Connectivity | BGP tunnel connectivity | Border Gateway Protocol (BGP) connectivity failure with peer due to wrong autonomous system (AS) number. |
| Connectivity | Interface connecting network devices is down | An interface connecting to network devices is down. |
| Connectivity | Layer 2 loop symptoms | Host MAC address flapping seen on network device. |
| Connectivity | Network device Interface connectivity - BGP Flap | Border Gateway Protocol (BGP) connectivity is flapping with neighbor. |
| Connectivity | Network Device Interface Connectivity - BGP Down | BGP connectivity is down with neighbor. |

| Router Issues | | |
|---------------|-----------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Category | Issue Name | Summary |
| Connectivity | Network device interface connectivity - EIGRP adjacency failure | Enhanced Interior Gateway Routing Protocol (EIGRP) adjacency failed with neighbor. |
| Connectivity | Network device interface connectivity - Interface down | Interface on device is down. |
| Connectivity | Network device interface connectivity - ISIS adjacency failure | Intermediate System Intermediate System (ISIS) adjacency failed on device. |
| Connectivity | Network device interface connectivity - OSPF adjacency failure | Open Shortest Path First (OSPF) adjacency failed with neighbor. |
| Connectivity | WAN Interface Down | A WAN interface is down. |
| Connected | Failure to install an access policy for SGT | Failure to install a Security Group Access Control List (SGACL) access policy for a Security Group Tag (SGT). |
| Connected | High input/output error on router interfaces | A high input or output error is detected on the router interfaces. The threshold values can be customized. |
| Connected | High input/output discards on router interfaces | A high input or output discard is detected on the router interfaces. The threshold values can be customized. |
| Connected | High input/output utilization on router interfaces | High input or output utilization is detected on the router interfaces. The threshold values can be customized. |
| Connected | High input/output discards on router WAN interfaces | A high input or output discard is detected on the router's WAN interface. The threshold values can be customized. |
| Connected | High input/output utilization on router WAN interfaces | High input/output utilization on WAN interfaces. High input or output utilization is detected on the router's WAN interfaces. The threshold values can be customized. |
| Connected | SGT access policy download failed on the device | Failed to download the Security Group Access Control List (SGACL) access control entries ACEs for a Security Group Tag (SGT). |
| Connected | SGT access policy installation failed on the device | Failure to install an access policy for a Security Group Tag (SGT). Policy rule error found in Role Based Access Control List (RBACL). |
| Connected | Unable to download SGT access policy from the policy server | Failure to download the source list for access policy for Security Group Tag (SGT). |
| Connected | Uninstall of SGT access policy failed on the device | Failure to uninstall an Security Group Access Control List (SGACL) access policy for Security Group Tag (SGT). |
| Device | DNA Center and network device time has drifted | Excessive time lag between Cisco DNA Center and device. |
| Device | Issues based on syslog events - High temperature | Issues created by single occurrence of syslog event related to high temperature. |

| Router Issues | | |
|---------------|---------------------------------------------|---------------------------------------------------------------------------------------------|
| Category | Issue Name | Summary |
| Device | Router experiencing high CPU utilization | The router is experiencing high CPU utilization. The threshold values can be customized. |
| Device | Router experiencing high memory utilization | The router is experiencing high memory utilization. The threshold values can be customized. |
| Availability | Network device HA switchover | The network device went through an High Availability (HA) switchover. |
| Availability | Router unreachable | The router is unreachable from Cisco DNA Center through ICMP or SNMP. |

Core, Distribution, and Access Issues

The following table lists the core, distribution, and access issues detected by Assurance:

| Core, Distribution, and Access Issues | | |
|---------------------------------------|-----------------------------------------------------------------|--------------------------------------------------------------------------------------|
| Category | Issue Name | Summary |
| Connectivity | BGP tunnel connectivity | BGP connectivity failure with peer due to wrong autonomous system (AS) number. |
| Connectivity | Interface connecting network devices is down | An interface connecting to network devices is down. |
| Connectivity | Layer 2 loop symptoms | Host MAC address flapping seen on a network device. |
| Connectivity | Network Device Interface Connectivity- BGP Down | BGP connectivity is down with neighbor. |
| Connectivity | Network device Interface connectivity - BGP Flap | BGP connectivity is flapping with neighbor. |
| Connectivity | Network device interface connectivity - EIGRP adjacency failure | EIGRP (Enhanced Interior Gateway Routing Protocol) adjacency failed with neighbor. |
| Connectivity | Network device interface connectivity - Interface down | Interface on device is down. |
| Connectivity | Network device interface connectivity - ISIS adjacency failure | Intermediate System Intermediate System (IS-IS) adjacency failed on the device. |
| Connectivity | Network device interface connectivity - OSPF adjacency failure | Open Shortest Path First (OSPF) adjacency failed with neighbor. |
| Connectivity | WAN Interface Down | A WAN interface is down. |
| Connectivity | Dual Active Detection link failed on network device | The Dual Active Detection link has failed on the network device <i>Switch Name</i> . |

| Core, Distribution, and Access Issues | | |
|---------------------------------------|-------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|
| Category | Issue Name | Summary |
| Connectivity | StackWise Virtual link failed on network device | The StackWise Virtual link has failed on the network device <i>Switch Name</i> . |
| Connectivity | StackWise link failed on network device | The StackWise link has failed on the network device <i>Switch Name</i> . |
| Connected | Fabric devices connectivity - Border overlay | The fabric edge lost connectivity to the fabric border in the virtual network. |
| Connected | Fabric devices connectivity - Border underlay | The fabric edge lost connectivity to the fabric border in the physical network. |
| Connected | Fabric devices connectivity - Control border underlay | The fabric node lost connectivity to the co-located fabric border and control plane in the physical network. |
| Connected | Fabric devices connectivity - Control underlay | The fabric node lost connectivity to the fabric control plane device in the physical network. |
| Connected | Fabric devices connectivity - DHCP overlay | The fabric node lost connectivity to the DHCP server in the virtual network. |
| Connected | Fabric devices connectivity - DHCP underlay | The fabric node lost connectivity to the DHCP server in the physical network. |
| Connected | Fabric devices connectivity - DNS overlay | The fabric node lost connectivity to the DNS server in the virtual network. |
| Connected | Fabric devices connectivity - DNS underlay | The fabric node lost connectivity to the DNS server in the physical network. |
| Connected | Fabric devices connectivity - External URL | The fabric border cannot reach the user-provisioned external URL. |
| Connected | Fabric devices connectivity - ISE server | The fabric edge lost connectivity to the ISE server in the physical network. |
| Connected | Fabric WLC to MapServer connectivity | The fabric wireless controller lost connectivity to the fabric control plane node. |
| Connected | Fabric facing port channel connectivity | The fabric node connecting the port channel is down. |
| Connected | Fabric AAA Server Status | The AAA server status on the fabric node is down. |
| Connected | Fabric devices connectivity - Multicast RP | The fabric border node lost connectivity to the multicast rendezvous point (RP). |
| Connected | BGP session Status to Fabric Control Plane | The BGP session is down on the border with the control plane in the fabric site. |
| Connected | Fabric Control Plane - LISP Session Status | The LISP session to the control plane node is down. |

| Core, Distribution, and Access Issues | | |
|----------------------------------------------|-------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|
| Category | Issue Name | Summary |
| Connected | Fabric Devices Connectivity - Internet Availability | The internet is unavailable because the default route on the control plane node is lost. |
| Connected | Fabric Extranet policy status | The fabric extranet policy status is down. |
| Connected | Fabric Control Plane - LISP Pubsub Session Status | The LISP PubSub session to the control plane node is down. |
| Connected | Fabric devices connectivity - AAA server | The fabric edge node lost connectivity to the AAA server in the physical network. |
| Connected | Fabric Devices Connectivity - Remote Internet Availability | The remote internet service on the control plane node is lost. |
| Connected | BGP session Status to Peer Device | The BGP session is down on the border for the IP transit peer in the site. |
| Connected | BGP session Status to Transit Control Plane | The BGP session is down on the border connected to the SD-Access transit. |
| Connected | Fabric devices connectivity - Border anchored | The fabric border node lost connectivity to the fabric anchored border node in the physical network. |
| Connected | Failure to install an access policy for SGT | Failure to install an SGACL access policy for SGT. |
| Connected | High input/output error on switch interfaces | A high input or output error is detected on the switch interfaces. The threshold values can be customized. |
| Connected | High input/output discard on switch interfaces | A high input or output discard is detected on the switch interfaces. The threshold values can be customized. |
| Connected | High input/output utilization on switch interfaces | High input or output utilization is detected on the switch interfaces. The threshold values can be customized. |
| Connected | SGT access policy download failed on the device | Failed to download SGACL ACEs for SGT. |
| Connected | SGT access policy installation failed on the device | Failure to install an access policy for SGT. Policy rule error found in RBACL. |
| Connected | Unable to download SGT access policy from the policy server | Failure to download the source list for access policy for SGT. |
| Connected | Uninstall of SGT access policy failed on the device | Failure to uninstall an SGACL access policy for SGT. |
| Device | Device reboot crash | Device has rebooted due to a hardware or software crash. |
| Device | Device time has drifted from Cisco DNA Center | Excessive time lag between Cisco DNA Center and the device network. |

| Core, Distribution, and Access Issues | | |
|----------------------------------------------|--------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Category | Issue Name | Summary |
| Device | Interface is flapping on network device | A port interface is flapping on a switch. By default, this issue is triggered when the interface flaps three or more times within a 30-minute period. You can change the default flap trigger. |
| Device | Issues based on syslog events - High temperature | Issues created by single occurrence of syslog event related to high temperature. |
| Device | Issues based on syslog events - POE | Issues created by single occurrence of syslog event related to power. |
| Device | PoE port in error state | PoE port is error disabled as reported by a syslog event. |
| Device | PoE powered device flagged faulty | PoE-capable device connected to a PoE port has been flagged faulty as reported by a syslog event. |
| Device | Power denied for PoE powered device | PoE-capable device connected to a PoE port has been power denied as reported by a syslog event. |
| Device | Stack member removal | Stack member was removed. |
| Device | Stack member running incompatible image | Stack member is running an incompatible image. |
| Device | Switch experiencing high CPU utilization | The switch is experiencing high CPU utilization. The threshold values can be customized. |
| Device | Switch experiencing high memory utilization | The switch is experiencing high memory utilization. The threshold values can be customized. |
| Device | Switch fan failure | Fan failure on the switch. |
| Device | Switch power failure | Power supply failure on the switch. |
| Device | TCAM utilization high issues | Issues for TCAM exhaustion in Layer 2, Layer 3, QoS, and SGACL. |
| Availability | Network device HA switchover | The network device went through an HA switchover. |
| Availability | Switch unreachable | The switch is unreachable from Cisco DNA Center through ICMP or SNMP. |
| Utilization | Map cache limit reached | Map cache entries have exceeded the limit on the map server. |

Third-Party Device Issues

The following table lists the third-party device issues detected by Assurance:

| Third-Party Device Issues | | |
|----------------------------------|--------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| Category | Issue Name | Summary |
| Availability | Third Party Device unreachable | The Third-Party device is unreachable from the Cisco DNA Center via ICMP or SNMP. |
| Connected | High input/output error on Third-Party Device interfaces | High input or output error is detected on the third-party device interfaces. The threshold values can be customized. |
| Connected | High input/output discard on Third-Party Device interfaces | A high input or output discard is detected on the third-party device interfaces. The threshold values are customized. |
| Connected | High input/output utilization on Third-Party Device interfaces | High input or output utilization is detected on the third-party device interfaces. The threshold values can be customized. |
| Connected | High input/output discards on Third-Party Device WAN interfaces | A high input or output discard is detected on the third-party device WAN interfaces. The threshold values can be customized. |
| Connected | High input/output utilization on Third-Party Device WAN interfaces | High input or output utilization is detected on the third-party device WAN interfaces. The threshold values can be customized. |

Controller Issues

The following table lists the controller issues detected by Assurance:

| Controller Issues | | |
|--------------------------|-----------------------------------------------|------------------------------------------------------------------------------------|
| Category | Issue Name | Summary |
| Connectivity | Interface connecting network devices is down | An interface connecting to network devices is down. |
| Connected | Fabric WLC to MapServer connectivity | The fabric wireless controller lost connectivity to the fabric control plane node. |
| Device | Device time has drifted from Cisco DNA Center | Excessive time lag between Cisco DNA Center and the network device. |
| Availability | Network device HA switchover | The network device went through an HA switchover. |
| Availability | WLC monitor | The network controller is not receiving data from the wireless controller. |
| Availability | WLC power supply failure | The power supply failed on this wireless controller. |
| Availability | WLC reboot crash | A wireless controller reboot crash occurred. |

| Controller Issues | | |
|-------------------|-----------------------------|------------------------------------------------------------------------------------|
| Category | Issue Name | Summary |
| Availability | WLC unreachable | The wireless controller is unreachable from Cisco DNA Center through ICMP or SNMP. |
| Utilization | AP license exhausted on WLC | The wireless controller currently has no free AP licenses. |
| Utilization | WLC memory high utilization | The wireless controller is experiencing high memory utilization. |

Access Point Issues

The following table lists the access point issues detected by Assurance:

| Access Point Issues | | |
|---------------------|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Category | Issue Name | Summary |
| Availability | AP coverage hole | The wireless LAN controller detected a coverage hole around the AP. |
| Availability | AP Disconnect from Cisco WLC | The AP is disconnected from the wireless LAN controller. The AP's CAPWAP link to the wireless LAN controller is down. |
| Availability | AP flap | The AP has flapped. The AP disconnected from the wireless LAN controller and then connected back to the wireless LAN controller. This issue is triggered when the AP flaps more than two times within a 15-minute period. |
| Availability | AP reboot crash | AP has rebooted due to a hardware or software crash. |
| Utilization | AP CPU high utilization | AP is experiencing high CPU utilization. |
| Utilization | AP memory high utilization | AP is experiencing high memory utilization. |
| Utilization | Radio high utilization (2.4GHz) | 2.4-GHz radios on APs are experiencing high utilization. |
| Utilization | Radio high utilization (5GHz) | 5-GHz radios on APs are experiencing high utilization. |
| Utilization | Radio high utilization (6GHz) | 6-GHz radios on APs are experiencing high utilization. |
| Utilization | No activity on radio (2.4GHz) | No activity on 2.4-GHz radio on AP. |
| Utilization | No activity on radio (5GHz) | No activity on 5-GHz radio on AP. |
| Utilization | No activity on radio (6GHz) | No activity on 6-GHz radio on AP. |
| AP Anomaly | AP anomaly | AP encountered anomaly issue. |
| Availability | Poor RF (2.4 GHz) on a floor | This issue is triggered when APs have a poor wireless experience. The poor RF issue occurs when at least one AP has interference or noise above the threshold within a 30-minute timeframe. |

| Access Point Issues | | |
|---------------------|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Category | Issue Name | Summary |
| Availability | Poor RF (5 GHz) on a floor | This issue is triggered when APs have a poor wireless experience. The poor RF issue occurs when at least one AP has interference or noise above the threshold within a 30-minute timeframe. |
| Availability | Poor RF (6 GHz) on a floor | This issue is triggered when APs have a poor wireless experience. The poor RF issue occurs when at least one AP has interference or noise above the threshold within a 30-minute timeframe. |
| Availability | Radio Down (2.4GHz) | 2.4-GHz radio is down on AP. |
| Availability | Radio Down (5GHz) | 5-GHz radio is down on AP. |
| Availability | Radio Down (6GHz) | 6-GHz radio is down on AP. |

Wired Client Issues

The following table lists the wired client issues detected by Assurance:

| Wired Client Issues | | |
|---------------------|-------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| Category | Issue Name | Summary |
| Onboarding | Client DHCP reachability issue | The client has failed to obtain an IP address from DHCP server. |
| Onboarding | Client DNS reachability issue | The client failed to obtain a response from the DNS server. |
| Onboarding | Wired client authentication failures - Dot1.x failure | The wired client failed authentication due to Dot1.x problems. Note This issue is applicable only for single wired clients. |
| Onboarding | Wired client authentication failures - MAB failure | The wired client failed authentication due to MAC authentication bypass problems. Note This issue is applicable only for single wired clients. |

Wireless Client Issues

The following table lists the wireless client issues detected by Assurance:



Note These issues are applicable for both single clients and multiple clients.

| Wireless Client Issues | | |
|-------------------------------|-------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Category | Issue Name | Summary |
| Onboarding | 802.11r client roaming slowly | While roaming, a wireless client capable of fast roaming is doing full authentication instead of fast authentication. |
| Onboarding | Client DHCP reachability issue | The client has failed to obtain an IP address from DHCP server. |
| Onboarding | Client DNS reachability issue | The client failed to obtain a response from the DNS server. |
| Onboarding | Wireless client excluded - Client was excluded before roaming | Wireless client excluded - Client was excluded before roaming. |
| Onboarding | Wireless client failed to connect - Client timeout | Wireless client failed to connect - Failed to authenticate due to client timeout. |
| Onboarding | Wireless client failed to connect - DHCP timeout | Wireless clients took longer than 10 seconds to connect. The delay was in the IP Learning phase due to DHCP server or client timeout. |
| Onboarding | Wireless client failed to connect - Incorrect PSK | Multiple wireless clients failed to connect and were excluded by the wireless controller. They were excluded because the client's PSK did not match the configured WLAN PSK. |
| Onboarding | Wireless client failed to connect - WLC internal error | Wireless client failed to connect - wireless controller internal error. |
| Onboarding | Wireless client failed to roam - AAA server rejected client | Wireless client failed to roam - AAA server rejected client. |
| Onboarding | Wireless client failed to roam - AAA server timeout | Wireless client failed to roam - AAA server timeout. |
| Onboarding | Wireless client failed to roam - Client PMK not found | Wireless client failed to roam - Client PMK not found. |
| Onboarding | Wireless client failed to roam - Client timeout | Wireless client failed to roam - Failed to authenticate due to client timeout. |
| Onboarding | Wireless client failed to roam - Security parameter mismatch | Wireless client failed to roam - Security parameter mismatch. |
| Onboarding | Wireless client failed to roam - WLC configuration error | Wireless client failed to roam - wireless controller configuration error. |
| Onboarding | Wireless client failed to roam - WLC internal error | Wireless client failed to roam - wireless controller internal error. |
| Onboarding | Wireless client failed to roam between APs - External error | Wireless client failed to roam between APs - External error. |
| Onboarding | Wireless client failed to roam between APs - WLC configuration mismatch | Multiple wireless clients failed to roam between APs due to a wireless LAN controller configuration mismatch. |

| Wireless Client Issues | | |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Category | Issue Name | Summary |
| Onboarding | Wireless clients took a long time to connect - Excessive time due to authentication timeouts | Multiple wireless clients took a long time to connect. The excessive onboarding time was due to authentication timeouts. The clients that run into this problem are grouped by AAA server or wireless controller. |
| Onboarding | Wireless clients took a long time to connect - Excessive time due to DHCP server failures | Multiple wireless clients took a long time to connect. The excessive onboarding time is due to DHCP server failures. The clients that run into this problem are grouped by the DHCP server or wireless controller. |
| Onboarding | Wireless clients took a long time to connect - Excessive time due to failed credentials | Multiple wireless clients took a long time to connect. The excessive onboarding time was due to authentication delays caused by failed credentials. The clients that run into this problem are grouped by AAA server or wireless controller. |
| Onboarding | Wireless clients took a long time to connect - Excessive time due to WLC failures | Multiple wireless clients took a long time to connect. The excessive onboarding time was due to wireless LAN controller failures during authentication. The clients that run into this problem are grouped by wireless controller. |
| Onboarding | Wireless clients took a long time to connect - Excessive time for authentication due to AAA server or network delays | Multiple wireless clients took a long time to connect. The excessive onboarding time was due to authentication delays. The authentication delays were caused by AAA server or network delays. |
| Onboarding | Wireless clients excluded - IP theft issue | Multiple wireless clients have been excluded from connecting to the wireless network. IP theft issues were detected on the clients. The clients that run into this problem are grouped by wireless controller. |
| Onboarding | Wireless clients failed to connect - AAA server rejected clients | Multiple wireless clients failed during authentication with a AAA Server Reject failure reason. The AAA server rejected the client's authentication requests. The clients that run into this problem are grouped by AAA server or wireless controller. |
| Onboarding | Wireless clients failed to connect - AAA server timeout | Multiple wireless clients failed during authentication with a AAA Server Timeout failure. This failure occurs when the wireless controller doesn't receive a response from the AAA to the client's authentication messages and times out after retries. The clients that run into this problem are grouped by AAA server or wireless controller. |
| Onboarding | Wireless clients failed to connect - Client PMK not found | Multiple wireless clients failed to connect due to authentication problems. The client's PMK was not found. |
| Onboarding | Wireless clients failed to connect - DHCP server timeout | Multiple wireless clients failed to connect. The failure was in the IP Learning phase due to DHCP server timeout. The DHCP server timed out and did not respond to DHCP messages. The clients that run into this problem are grouped by DHCP server or wireless controller. |
| Onboarding | Wireless clients failed to connect - Failed to authenticate due to client timeouts | Multiple wireless clients failed to connect. They failed to authenticate due to client timeouts. The clients failed to respond in time to authentication messages. The clients that run into this problem are grouped by site or AP group. |

| Wireless Client Issues | | |
|-------------------------------|--------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Category | Issue Name | Summary |
| Onboarding | Wireless clients failed to connect - Failed to get an IP address due to client timeouts | Multiple wireless clients failed to connect. They failed to get an IP address due to client timeouts. The clients failed to respond in time to DHCP messages. The clients that run into this problem are grouped by site or AP group. |
| Onboarding | Wireless clients failed to connect - Failed to get an IP address due to DHCP server or client timeouts | Multiple wireless clients failed to connect. They failed to get an IP address due to DHCP server timeouts or client timeouts. Either the DHCP server or the clients failed to respond in time to DHCP messages. The clients that run into this problem are grouped by site or AP group. |
| Onboarding | Wireless clients failed to connect - Security parameter mismatch | Multiple wireless clients failed to connect due to authentication problems caused by a security parameter mismatch. |
| Onboarding | Wireless clients failed to connect - WLC configuration error | Multiple wireless clients failed to connect due to authentication problems. There are wireless LAN controller configuration errors. The clients that run into this problem are grouped by wireless controller. |
| Onboarding | Wireless clients failed to roam - Client exclusion policies on the WLC | Multiple wireless clients failed to roam. Clients were excluded due to client exclusion policies on the wireless LAN controller. The clients that run into this problem are grouped by wireless controller. |
| Onboarding | Wireless clients failed to roam - Clients were excluded before roaming | Multiple wireless clients failed to roam. The clients were excluded on the wireless LAN controller before roaming. The clients that run into this problem are grouped by wireless controller. |
| Onboarding | Wireless clients failed to roam - WLC configuration mismatch | Multiple wireless clients failed to roam between APs due to a wireless LAN controller configuration mismatch. |
| Onboarding | Wireless clients took a long time to connect - WLC failures | Multiple wireless clients took a long time to connect. The excessive onboarding time was due to wireless LAN controller failures during authentication. The clients that run into this problem are grouped by wireless controller. |
| Connected | Dual band capable client prefers 2.4 GHz over 5 GHz | Dual-band capable client is consistently connecting to a 2.4-GHz radio, even though a 5-GHz radio that provides a better experience is available. |
| Connected | Wireless client has poor RF | Wireless client is experience poor RF condition because the client has no better neighboring APs to roam to. |
| Connected | Wireless client shows sticky behavior | Wireless client is maintaining an association with an AP that has a weaker signal. It should roam to an available AP that has the stronger signal. |

Enable AAA Failure Root Cause Analysis Issues

Cisco DNA Center integrates with Cisco ISE syslogs to troubleshoot the following issues:

- Wireless clients failed to connect: AAA server rejected clients
- Wireless clients failed to connect: AAA server timeout

The troubleshooting workflow is an MRE workflow that you access from a single client issue in the **Client 360** window, or from wireless client issues in the **Issues** dashboard.

Cisco DNA Center shows the syslogs generated by Cisco ISE for client authentication failures, enabling you to determine the root cause of the client authentication failure without having to log in to Cisco ISE and search for clients there.

To enable AAA Failure Root Cause Analysis issues in Assurance, do the following:

-
- Step 1** In Cisco DNA Center, choose **System > Settings > External Services > Authentication and Policy Servers** and add and configure Cisco ISE to the Cisco DNA Center cluster. This step adds the Cisco ISE policy service node (PSN) to the syslog allowed list.
- Step 2** In Cisco ISE, choose **Administration > System > Logging > Remote Logging Targets** and add Cisco DNA Center as a syslog destination.
- Step 3** In Cisco ISE, choose **Administration > System > Logging > Logging Categories** and add the target that you added in the previous step to the following logging categories: **Failed Attempts**, **Authentication Flow Diagnostics**, and **RADIUS Diagnostics**.
Cisco ISE syslogs can now be sent to Cisco DNA Center. Cisco DNA Center processes and saves the Cisco ISE syslogs for client onboarding problems.
-

Application Issues

The following table lists the application issues detected by Assurance:

| Application Issues | | |
|--------------------|-------------------------------|--------------------------------------------------|
| Category | Issue Name | Summary |
| Application | Application experience issues | All issues pertaining to Application Experience. |

Sensor Issues

The following table lists the sensor issues detected by Assurance.

When two or more sensors on the same floor fail a test in a 30-minute period, the sensor can raise an issue based on the failed root cause. These sensor issues are all global issues, meaning that the sensor issue from any floor is escalated and shown in the **Issues** dashboard.

| Sensor Issues | | |
|---------------|---------------------------------|------------------------------------------------------------------------------------|
| Category | Issue Name | Summary |
| Sensor Test | Sensors - Speed test HTTP error | Multiple sensors are reporting speed test HTTP error while accessing query server. |
| Sensor Test | Sensors - DHCP failures | Multiple sensors failed to get an IPv4 address. |
| Sensor Test | Sensors - DNS resolution failed | Multiple sensors failed to resolve domain name with DNS server. |






| Sensor Issues | | |
|----------------------|--------------------------------------------------|-------------------------------------------------------------------------------------------------------|
| Category | Issue Name | Summary |
| Sensor Test | Sensors - Failed association during onboarding | Multiple sensors failed to associate during onboarding. |
| Sensor Test | Sensors -Failed authentication during onboarding | Multiple sensors failed to authenticate during onboarding. |
| Sensor Test | Sensors - FTP test fail | Multiple sensors are reporting unable to connect to FTP server. |
| Sensor Test | Sensors - FTP transfer fail | Multiple sensors are reporting failed to transfer file with FTP server. |
| Sensor Test | Sensors - FTP unreachable | Multiple sensors are reporting unreachable FTP server. |
| Sensor Test | Sensors - IPerf invalid config error | Multiple sensors have failed to conduct the iPerf test due to receiving invalid iPerf configurations. |
| Sensor Test | Sensors - IPerf server busy | Multiple sensors have failed to conduct the iPerf test due to an iPerf busy error. |
| Sensor Test | Sensors - IPerf test network error | Multiple sensors have failed to conduct the iPerf test due to an iPerf network error. |
| Sensor Test | Sensors - IPerf undefined error | Multiple sensors have failed to conduct the iPerf test due to an undefined error. |
| Sensor Test | Sensors - IPSLA no IP address | Multiple sensors are reporting IPSLA test IP address not received from Cisco DNA Center. |
| Sensor Test | Sensors - IPSLA no response | Multiple sensors are reporting IPSLA test - no response from IPSLA responder. |
| Sensor Test | Sensors - IPSLA socket error | Multiple sensors are reporting IPSLA test socket error. |
| Sensor Test | Sensors - IPSLA test fail | Multiple sensors are reporting IPSLA test failed. |
| Sensor Test | Sensors - IPSLA unsupported probe type | Multiple sensors are reporting IPSLA test unsupported probe type. |
| Sensor Test | Sensors - Mail server test fail | Multiple sensors are reporting failed to connect to mail server. |
| Sensor Test | Sensors - Mail server unreachable | Multiple sensors are reporting unreachable mail server. |
| Sensor Test | Sensors - No NDT server | Multiple sensors are reporting speed test NDT server does not exist. |
| Sensor Test | Sensors - Onboarding failures | Sensors failed to connect to the wireless network. |
| Sensor Test | Sensors - Outlook server test fail | Multiple sensors are reporting failed to connect to Outlook Web Access. |
| Sensor Test | Sensors - Outlook server unreachable | Multiple sensors are reporting unreachable Outlook Web Access host. |
| Sensor Test | Sensors - Query server timeout | Multiple sensors are reporting speed test query server timeout. |
| Sensor Test | Sensors - RADIUS authentication fail | Multiple sensors are reporting failed to authenticate with RADIUS server. |

| Sensor Issues | | |
|---------------|-----------------------------------------|-----------------------------------------------------------------------------------|
| Category | Issue Name | Summary |
| Sensor Test | Sensors - Speed test fail | Multiple sensors are reporting speed test failed. |
| Sensor Test | Sensors - Speed test generic error | Multiple sensors are reporting speed test generic failure. |
| Sensor Test | Sensors - Speed test uplink timeout | Multiple sensors are reporting speed test uplink test timeout. |
| Sensor Test | Sensors - Speed test URL error | Multiple sensors are reporting speed test URL error while accessing query server. |
| Sensor Test | Sensors - Unreachable host | Multiple sensors are reporting ping failure to the host. Unreachable host. |
| Sensor Test | Sensors - Unreachable RADIUS | Multiple sensors are reporting unreachable RADIUS server. |
| Sensor Test | Sensors - Web authentication fail | Multiple sensors are reporting clients are failing web authentication test. |
| Sensor Test | Sensors - Web server test failed | Multiple sensors are reporting failed to load page from web server. |
| Sensor Test | Sensors - Web server unreachable | Multiple sensors are reporting unreachable web server. |
| Sensor Test | Sensors - Web socket error | Multiple sensors are reporting speed test websocket error during the test. |
| Sensor Test | Sensors - Speed test uplink proxy error | Multiple sensors are reporting speed test uplink test proxy error. |

The following table contains all the rows in the preceding table, plus rows that we were asked to remove during Cyclops. The following table has the dnac_hide_content FID applied to it. We wanted to retain the rows (but keep everything hidden) in case we ever need to readd this information.

AI-Driven Issues

The following table lists the AI-Driven issues detected by Cisco AI Network Analytics:

| AI-Driven Issues | | |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| Connection Issues | | |
| Onboarding |  Excessive time to connect - High deviation from baseline | The network is experiencing excessive onboarding time compared to usual. Clients are taking longer than the usual time to connect to <i>SSID</i> . |
| Onboarding |  Excessive failures to connect - High deviation from baseline | The network is experiencing excessive onboarding failures compared to usual. Clients are taking longer than the usual time to connect to <i>SSID</i> . |
| Onboarding |  Wireless clients took a long time to connect - Total time above baseline | Wireless clients took longer to connect to <i>SSID</i> at <i>location</i> . |
| AAA |  Excessive time to get Associated - High deviation from baseline | Excessive time to get associated - At least <i>value</i> % increase in time on <i>SSID</i> . |
| AAA |  Excessive failures to Associate - High deviation from baseline | Excessive failures to get associated - At least <i>value</i> % increase in failures on <i>SSID</i> . |

| AI-Driven Issues | | |
|-------------------------------|----------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AAA | <input type="checkbox"/> AI Excessive time to get Authenticated - High deviation from baseline | Excessive time to get authenticated - At least <i>value</i> % increase in time on <i>SSID</i> . |
| AAA | <input type="checkbox"/> AI Excessive failures to get Authenticated - High deviation from baseline | Excessive failures to get authenticated - At least <i>value</i> % increase in failures on <i>SSID</i> . |
| DHCP | <input type="checkbox"/> AI Excessive time to get an IP Address - High deviation from baseline | Excessive time to get an IP address - At least <i>value</i> % increase in time from <i>server_IP</i> . |
| DHCP | <input type="checkbox"/> AI Excessive failures to get an IP address - High deviation from baseline | Excessive failures to get an IP address - At least <i>value</i> % increase in failures from <i>server_IP</i> . |
| Network Connectivity Issue | | |
| Connectivity | <input type="checkbox"/> AI Host MAC address flapping seen on network device | Network is experiencing Layer 2 loop symptoms. |
| Roaming Issues | | |
| Onboarding | <input type="checkbox"/> AI Excessive time to connect - High deviation from baseline | The network is experiencing excessive onboarding time compared to usual. |
| Onboarding | <input type="checkbox"/> AI Excessive failures to roam - High deviation from baseline | The network is experiencing excessive roaming time compared to usual. |
| Application Experience Issues | | |
| Throughput | <input type="checkbox"/> AI Drop in total radio throughput for All Applications | APs in network are experiencing a drop in total radio throughput for all applications. These radios are in the <i>frequency</i> band. These radios are located at <i>location</i> . |
| Throughput | <input type="checkbox"/> AI Drop in radio throughput for Cloud Applications | APs in network are experiencing a drop in Cloud Applications throughput. These radios are in the <i>frequency</i> band. These radios are located at <i>location</i> . |
| Throughput | <input type="checkbox"/> AI Drop in radio throughput for Social Applications | APs in network are experiencing a drop in Social Applications throughput. These radios are in the <i>frequency</i> band. These radios are located at <i>location</i> . |
| Throughput | <input type="checkbox"/> AI Drop in radio throughput for Media Applications | APs in network are experiencing a drop in Media Applications throughput. These radios are in the <i>frequency</i> band. These radios are located at <i>location</i> . |
| Throughput | <input type="checkbox"/> AI Drop in radio throughput for Collab Applications | APs in network are experiencing a drop in Collab Applications throughput. These radios are in the <i>frequency</i> band. These radios are located at <i>location</i> . |

MRE Issues

The following table lists the issues detected by Assurance that you can troubleshoot using the MRE workflow:

| MRE Issues | | |
|----------------------------|-------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| Category | Issue Name | Summary |
| Wired Client Issues | | |
| Onboarding | Client DHCP reachability issue | The client has failed to obtain an IPv4 address from the DHCP server. |
| Onboarding | Wired client authentication failures - Dot1.x failure | The wired client failed authentication due to Dot1.x problems. Note This issue is applicable only for single wired clients. |
| Onboarding | Wired client authentication failures - MAB failure | The wired client failed authentication due to MAC authentication bypass problems. Note This issue is applicable only for single wired clients. |
| PoE Issue | | |
| Device | PoE powered device flagged faulty | Syslog event flagged a PoE-capable device connected to a PoE port as faulty. |

