



# Troubleshoot Network Devices Using Network Reasoner

---

- [Network Reasoner Overview](#), on page 1
- [Validate Cisco SD-Access Migration Using the MRE Workflow](#), on page 1
- [Troubleshoot High CPU Utilization](#), on page 3
- [Troubleshoot a Power Supply Failure](#), on page 4
- [Troubleshoot a Downed Interface](#), on page 5
- [Troubleshoot Network Connectivity](#), on page 6
- [Troubleshoot IP Connectivity of a Device](#), on page 7
- [Troubleshoot Wireless Clients Using the MRE Workflow](#), on page 7
- [Troubleshoot Wireless APs Using the MRE Workflow](#), on page 8
- [Troubleshoot Unmonitored Devices Using the MRE Workflow](#), on page 9
- [Scan the Network for Bugs](#), on page 10
- [Scan Cisco DNA Center for Bugs](#), on page 13

## Network Reasoner Overview

The Network Reasoner tool allows you to troubleshoot various issues on your network quickly. Click the menu icon (☰) and choose **Tools > Network Reasoner** to launch the Network Reasoner dashboard. The Network Reasoner dashboard hosts separate workflows that you can use to proactively troubleshoot network issues. The dashboard provides a brief description of the workflows, the number of affected devices in the last 24 hours, and the impact of running a workflow on a network.



---

**Note** You must install the Machine Reasoning package to view the Network Reasoner feature under the **Tools** menu. For more information, see the [Cisco DNA Center Administrator Guide](#).

---

## Validate Cisco SD-Access Migration Using the MRE Workflow

The following Machine Reasoning Engine (MRE) workflows assist in planning your migration to Cisco SD-Access:

- SDA Hardware Readiness Check
- SDA Software Readiness Check
- Redundant Link Check
- L3 Access Check
- MTU Link Check
- SDA Health Check
- SDA Scale Limits Check

**Step 1** Click the menu icon (☰) and choose **Tools > Network Reasoner**.

**Step 2** In the **Network Reasoner** dashboard, click the following workflows as required:

Workflow	Description	Action
SDA Hardware Readiness Check	Checks whether the hardware is ready for Cisco SD-Access migration.	<ol style="list-style-type: none"> <li>a. Click <b>SDA Hardware Readiness Check</b>.</li> <li>b. Click <b>Run Machine Reasoning</b>.</li> </ol>
SDA Software Readiness Check	Checks whether the software is ready for Cisco SD-Access migration.	<ol style="list-style-type: none"> <li>a. Click <b>SDA Software Readiness Check</b>.</li> <li>b. Click <b>Run Machine Reasoning</b>.</li> </ol>
Redundant Link Check	Checks whether any redundant uplinks are present in your device and if there are ways to increase availability by configuring redundant uplinks on the access switches.	<ol style="list-style-type: none"> <li>a. Click <b>Redundant Link Check</b>.</li> <li>b. Select an appropriate device.</li> <li>c. Click <b>Troubleshoot</b>.</li> </ol>
L3 Access Check	Checks whether your network has access switches that are running Layer 3 routing protocols to move to Cisco SD-Access with minimal design changes.	<ol style="list-style-type: none"> <li>a. Click <b>L3 Access Check</b>.</li> <li>b. Select an appropriate device.</li> <li>c. Click <b>Troubleshoot</b>.</li> </ol>
MTU Link Check	Checks whether the links between the main network devices and the access, core, and other switches are configured with the correct MTU.	<ol style="list-style-type: none"> <li>a. Click <b>MTU Link Check</b>.</li> <li>b. Select an appropriate device.</li> <li>c. Click <b>Troubleshoot</b>.</li> </ol>
SDA Health Check: Fabric Count	Checks the health of the Cisco DNA Center cluster to determine whether it is reaching any scale limit thresholds due to managing fabrics.	<ol style="list-style-type: none"> <li>a. Click <b>Fabric Count</b>.</li> <li>b. Click <b>Run Machine Reasoning</b>.</li> </ol>

Workflow	Description	Action
SDA Health Check: SDA Scale Limits Check	Checks whether the number of client endpoints, network devices, and configured fabrics in Cisco DNA Center are within the published SDA limits.	<p>a. Click <b>SDA Scale Limits Check</b>.</p> <p>b. Click <b>Run Machine Reasoning</b>.</p>
SDA Health Check: Client Count	Checks the health of the Cisco DNA Center cluster to determine whether it is reaching any scale limit thresholds due to managing clients.	<p>a. Click <b>Client Count</b>.</p> <p>b. Click <b>Run Machine Reasoning</b>.</p>
SDA Health Check: Device Count	Checks the health of the Cisco DNA Center cluster to determine whether it is reaching any scale limit thresholds due to managing network devices.	<p>a. Click <b>Device Count</b>.</p> <p>b. Click <b>Run Machine Reasoning</b>.</p>

## Troubleshoot High CPU Utilization

CPU utilization troubleshooting support is available only for the following network devices with software version 16.9.3 and later:

- Cisco Catalyst 9400 Series Switches
- Cisco Catalyst 9300 Series Switches
- Cisco Catalyst 3850 Series Switches
- Cisco Catalyst 3650 Series Switches

### Before you begin

- Install the Machine Reasoning package. For more information, see Download and Install Packages and Updates in the [Cisco DNA Center Administrator Guide](#).
- Create a user role with write permissions for Machine Reasoning under the **System** function. For more information, see Configure Role-Based Access Control in the [Cisco DNA Center Administrator Guide](#).

**Step 1** Click the menu icon (☰) and choose **Tools > Network Reasoner**.

**Step 2** Click the **CPU Utilization** tab.

The **CPU Utilization** window displays the filtered list of devices with high CPU utilization in the past 24 hours.

Click **All** to see the list of all devices from the inventory, and you can choose any device to run the workflow.

**Step 3** Choose the device that you want to troubleshoot.

Click **Filter** and enter the devices by entering **Tag, Device Name, IP Address, Device Type, Site, or Reachability**.

**Step 4** Click **Troubleshoot**.

**Step 5** In the **Reasoner Input** window, enter the **CPU Utilization Threshold** percentage that you want to check against.

**Step 6** Click **Run Machine Reasoning**.

**Note** The following processes, if observed, are considered for detailed analysis:

- **MATM Process Group:** MATM RP Shim, NGWC Learning, and VMATM Callback
- **IOSXE Process Group:** IP Input, ARP Input, IOSXE-RP Punt Se, SISF Main Thread, DAI Packet, and ARP Snoop

In the **CPU Utilization** window, you can see the **Root Cause Analysis** of the high CPU utilization for the chosen device.

The **Reasoning Activity** tab shows the various parameters that are checked as part of the troubleshooting process.

**Step 7** (Optional) Click **Stop** to stop the ongoing reasoning activity.

**Step 8** Click the **Conclusion** tab to see the processes that consume more CPU and the utilization percentage.

**Step 9** Click **View Relevant Activities** for each process to view the **Activity Details** in the right pane.

**Step 10** (Optional) Click **Run Again** to rerun the troubleshooting process for the same device.

**Note** The Machine Reasoning Engine (MRE) implements a system-terminate algorithm that detects and terminates network reasoner workflows when thresholds exceed a specified level, or when no events are received from the timeout request for inactivity.

## Troubleshoot a Power Supply Failure

Power supply troubleshooting workflow support is available only for the following network devices with software version 16.6.1 and later:

- Cisco Catalyst 3650 Series Switches
- Cisco Catalyst 3850 Series Switches
- Cisco Catalyst 9300 Series Switches
- Cisco Catalyst 9400 Series Switches
- Cisco Catalyst 9500 Series Switches

### Before you begin

- Install the Machine Reasoning package. For more information, see Download and Install Packages and Updates in the [Cisco DNA Center Administrator Guide](#).
- Create a user role with write permissions for Machine Reasoning under the **System** function. For more information, see Configure Role-Based Access Control in the [Cisco DNA Center Administrator Guide](#).

**Step 1** Click the menu icon (☰) and choose **Tools > Network Reasoner**.

**Step 2** Click the **Power Supply** tab.

The **Power Supply** window displays the filtered list of devices with power supply failures in the past 24 hours.

Click **All** to see the list of all devices in the inventory. You can choose any device to run the workflow.

**Step 3** Choose the device that you want to troubleshoot.

Click **Filter** and filter the devices by entering **Tag**, **Device Name**, **IP Address**, **Device Type**, **Site**, or **Reachability**.

**Step 4** Click **Troubleshoot**.

In the **Power Supply** window, you can see the **Root Cause Analysis** of the power supply failure for the chosen device.

The **Reasoning Activity** tab shows the various parameters that are checked as part of the troubleshooting process.

**Step 5** (Optional) Click **Stop** to stop the ongoing reasoning activity.

**Step 6** Click the **Conclusion** tab to see the **Stack Identifier**, **Product ID**, **Serial Number**, and **Status** of the power supply for the chosen device and the suggested action.

**Step 7** Click **View Relevant Activities** for each stack identifier to view the **Activity Details** in the right pane.

**Step 8** (Optional) Click **Run Again** to rerun the troubleshooting process for the same device.

**Note** The Machine Reasoning Engine (MRE) implements a system-terminate algorithm that detects and terminates network reasoner workflows when thresholds exceed a specified level, or when no events are received from the timeout request for inactivity.

---

## Troubleshoot a Downed Interface


Interface down troubleshooting workflow support is available only for the following network devices with software version 16.9.3, and later:

- Cisco Catalyst 3650 Series Switches
- Cisco Catalyst 3850 Series Switches
- Cisco Catalyst 9300 Series Switches
- Cisco Catalyst 9400 Series Switches
- Cisco Catalyst 9500 Series Switches

### Before you begin

- Install the Machine Reasoning package. For more information, see Download and Install Packages and Updates in the [Cisco DNA Center Administrator Guide](#).
- Create a user role with write permissions for Machine Reasoning under the **System** function. For more information, see Configure Role-Based Access Control in the [Cisco DNA Center Administrator Guide](#).

---

**Step 1** Click the menu icon () and choose **Tools > Network Reasoner**.

**Step 2** Click the **Interface Down** tab.

The **Interface Down** window displays the filtered list of devices with an interface that went down in the past 24 hours. Click **All** to see the list of all devices from the inventory, and you can choose any device to run the workflow.

**Step 3** Choose the device that you want to troubleshoot.

Click **Filter** and enter the devices by entering **Tag, Device Name, IP Address, Device Type, Site, or Reachability**.

**Step 4** Click **Troubleshoot**.

**Step 5** In the **Reasoner Input** window, enter the interface name that you suspect has issues.

**Step 6** Click **Run Machine Reasoning**.

In the **Interface Down** window, you can see the **Root Cause Analysis** of the downed interface for the chosen device.

The **Reasoning Activity** tab shows the various parameters that are checked as part of the troubleshooting process.

**Step 7** (Optional) Click **Stop** to stop the ongoing reasoning activity.

**Step 8** Click the **Conclusion** tab to see the potential root causes for the interface down issue and the suggested action.

**Step 9** Click **View Relevant Activities** for each root cause analysis to view the **Activity Details** in the right pane.

**Step 10** (Optional) Click **Run Again** to rerun the troubleshooting process for the same device.

**Note** The Machine Reasoning Engine (MRE) implements a system-terminate algorithm that detects and terminates network reasoner workflows when thresholds exceed a specified level, or when no events are received from the timeout request for inactivity.

---

## Troubleshoot Network Connectivity

Only the following network devices running Cisco IOS-XE software version 16.9.3 or later support the network connectivity troubleshooting:

- Cisco Catalyst 9200 Series Switches
- Cisco Catalyst 9300 Series Switches
- Cisco Catalyst 9400 Series Switches
- Cisco Catalyst 9500 Series Switches
- Cisco Catalyst 9600 Series Switches

Use the following procedure to check the reachability of an endpoint from a device using IP address:

### Before you begin

- Install the Machine Reasoning package. For more information, see Download and Install Packages and Updates in the [Cisco DNA Center Administrator Guide](#).
- Create a user role with write permissions for Machine Reasoning under the **System** function. For more information, see Configure Role-Based Access Control in the [Cisco DNA Center Administrator Guide](#).

- 
- Step 1** Click the menu icon (☰) and choose **Tools > Network Reasoner**.
- Step 2** Click the **Network Connectivity** tab.
- Step 3** You can view the device table with details, such as **Device Name**, **IP Address**, **Device Type**, **Site**, **Reachability**, **Role**, and **Platform**.
- Step 4** Select a device and click **Troubleshoot**.
- Step 5** In the **Destination IP address** field of the **Reasoner Inputs** window, enter a valid IP address and click **Run Machine Reasoning**.
- Note** Provide the Virtual Routing and Forwarding (VRF) name, if applicable.
- Step 6** In the **Root Cause Analysis** window, under **Reasoning Activity**, you can view various workflows that are validated as a part of the troubleshooting process.
- Step 7** In the **Conclusions** tab, you can view the status of the validation check and the suggested action.
- 

## Troubleshoot IP Connectivity of a Device

As ping is a simple command, IP connectivity troubleshooting support is available for all the network devices.

### Before you begin

- Install the Machine Reasoning package. For more information, see Download and Install Packages and Updates in the [Cisco DNA Center Administrator Guide](#).
- Create a user role with write permissions for Machine Reasoning under the **System** function. For more information, see Configure Role-Based Access Control in the [Cisco DNA Center Administrator Guide](#).

- 
- Step 1** Click the menu icon (☰) and choose **Tools > Network Reasoner**.
- Step 2** In the **Network Reasoner** dashboard, click **Ping Device**.
- Step 3** In the **Devices** window, choose a device and click **Troubleshoot**.
- Step 4** In the **Reasoner Inputs** window, enter **Target IP Address** and click **Run Machine Reasoning**.
- Step 5** Click **View Details** to view the ping status.
- 

## Troubleshoot Wireless Clients Using the MRE Workflow


Use this procedure to troubleshoot wireless client issues using the MRE workflow.

**Note**

- Wireless client troubleshooting workflow support is available only for network devices with Cisco IOS-XE software version 17.3.4 and later.
- The MRE workflow doesn't support HA, which means that if a switchover occurs during the workflow, you must repeat the workflow.

**Before you begin**

Make sure that the Machine Reasoning Engine (MRE) knowledge base is updated with the latest knowledge packs. For more information, see the "Update the Machine Reasoning Knowledge Base" topic in the [Cisco DNA Center Administrator Guide](#).

- 
- Step 1** Click the menu icon () and choose **Tools > Network Reasoner**.
- Step 2** Click the **Wireless Client Data Collection** tile.  
The **Devices** window shows the filtered wireless controller devices.
- Step 3** Choose the wireless controller that you want to troubleshoot and click **Troubleshoot**.
- Step 4** In the **Reasoner Inputs** window, complete the following fields:
- **Troubleshoot Duration**
  - **Client MAC Address**
  - **PCAP Interface**: Click the drop-down arrow and choose an interface from the list. Use this option if packet capture is required.
- Step 5** Click **Run Machine Reasoning**.  
The **Wireless Client Data Collection** slide-in pane is displayed.
- Step 6** In the **Root Cause Analysis** area, the **Reasoning Activity** tab shows the various parameters that are checked as part of the troubleshooting process. Optionally, click **Stop** to stop the ongoing reasoning activity.
- Step 7** Wait for the troubleshooting process to complete. After it completes, you can view the troubleshooting files under the **Conclusions** tab.
- Step 8** (Optional) Click **Run Again** to rerun the troubleshooting process for the same device.
- Step 9** (Optional) You can view the last troubleshooting files in the **Wireless Client Data Collection** slide-in pane when you start the Wireless Client troubleshooting workflow.
- 

## Troubleshoot Wireless APs Using the MRE Workflow

Use this procedure to troubleshoot wireless AP issues using the MRE workflow.



**Note**

- Wireless AP troubleshooting workflow support is available only for network devices with Cisco IOS-XE software version 17.3.4 and later.
- The MRE workflow doesn't support HA, which means that if a switchover occurs during the workflow, you must repeat the workflow.

**Before you begin**

Make sure that the MRE knowledge base is updated with the latest knowledge packs. For more information, see [Update the Machine Reasoning Knowledge Base in the \*Cisco DNA Center Administrator Guide\*](#).



- 
- Step 1** Click the menu icon (☰) and choose **Tools > Network Reasoner**.
- Step 2** Click the **Wireless AP Data Collection** tile.
- Step 3** The **Devices** window shows the filtered wireless controller devices. Choose the wireless controller device that you want to troubleshoot for the AP and click **Troubleshoot**.
- Step 4** In the **Reasoner Inputs** window, complete the following fields:
- **Troubleshoot Duration**
  - **Two AP MAC Address:** Enter the AP MAC address for Ethernet and radio.
  - If packet capture is required, use the following option:
    - **PCAP Interface:** Click the drop-down list to choose the interface.
    - **AP IP Address:** Enter the AP IP address.
  - **AP Name**
- Step 5** Click **Run Machine Reasoning**.  
The **Wireless AP Data Collection** slide-in pane appears.
- Step 6** In the **Root Cause Analysis** area, the **Reasoning Activity** tab shows the various parameters that are checked as part of the troubleshooting process. Optionally, click **Stop** to stop the ongoing reasoning activity.
- Step 7** Wait for the troubleshooting process to complete. After it completes, you can view the troubleshooting files under the **Conclusions** tab.
- Step 8** (Optional) Click **Run Again** to rerun the troubleshooting process for the same device.
- Step 9** (Optional) You can view the last troubleshooting files in the **Wireless AP Data Collection** slide-in pane when you start the Wireless AP troubleshooting workflow.
- 

## Troubleshoot Unmonitored Devices Using the MRE Workflow

Use this procedure to troubleshoot unmonitored devices or devices that are not showing Assurance data. The Troubleshooting Unmonitored Devices workflow supports only switches, Cisco AireOS Wireless Controllers, and Cisco Catalyst 9800 Series Wireless Controllers.

### Before you begin

Make sure that the Machine Reasoning Engine (MRE) knowledge base is updated with the latest knowledge packs. For more information, see the "Update the Machine Reasoning Knowledge Base" topic in the [Cisco DNA Center Administrator Guide](#).

- 
- Step 1** Click the menu icon () and choose **Tools > Network Reasoner**.
- Step 2** Click the **Assurance Telemetry Analysis** tile.
- Step 3** The **Devices** window shows the filtered unmonitored devices. Choose the device that you want to troubleshoot and click **Troubleshoot**.
- The **Assurance Telemetry Analysis** slide-in pane is displayed. In the **Root Cause Analysis** area, the **Reasoning Activity** tab shows the various parameters that are checked as part of the troubleshooting process.
- Step 4** Click **Stop** to stop the ongoing reasoning activity.
- After the troubleshooting is complete, the **Machine Reasoning Completed** dialog box is displayed.
- Step 5** Click **View Details**.
- Step 6** You can view the troubleshooting files under the **Conclusions** tab. The issue is highlighted with an icon () and the **Suggested Action** is displayed below the issue.
- You can troubleshoot the unmonitored device with the suggestions provided.
- Step 7** Click **Run Again** to rerun the troubleshooting process for the same device.
- Step 8** You can also troubleshoot the devices from the **Inventory** tab. Scroll down to view the **Health Score** column. Click **No Health** under the **Health Score** column and click **View Assurance Telemetry Analysis** to run the troubleshooting process.
- 

## Scan the Network for Bugs

The Cisco DNA Center network bug identifier tool allows you to scan the network for a selected set of defects or bugs that have been identified previously and are known to Cisco.

The Cisco DNA Center network bug identifier helps in identifying specific patterns in the device configuration or in the operational data of the device and matches them with known defects based on those patterns. This tool provides both bug-focused and device-focused views.

Cisco DNA Center collects network device configuration and operational data by running CLI commands on network devices, and then sends the information to the CX Cloud to be processed for exposure to potential security advisories or bugs. Cisco DNA Center invokes the following CLI commands for the network bug identifier tool:


- **show buffers summary**
- **show cef interfaces**
- **show clock**
- **show crypto eli all**
- **show crypto isakmp sa detail**

- **show eigrp service-family ipv4 neighbors**
- **show environment all**
- **show interfaces counters error**
- **show interfaces summary**
- **show inventory**
- **show ip interface brief**
- **show ip nat translations verbose**
- **show ip nbar protocol-discovery**
- **show ip nbar resources flow**
- **show ip nhrp**
- **show ip nhrp summary**
- **show ip route**
- **show ip ssh**
- **show ip vrf**
- **show logging**
- **show performance monitor cache detail**
- **show platform software route-map fp active map**
- **show pnp profile**
- **show redundancy**
- **show redundancy application group**
- **show running-config all**
- **show scp status**
- **show stackwise-virtual**
- **show startup-config**
- **show terminal**
- **show version**

The following procedure explains how to identify bugs using the network bug identifier tool.

### **Before you begin**

- Install the Cisco DNA Center core package. For more information, see Download and Install Packages and Updates in the [Cisco DNA Center Administrator Guide](#).
- Install the Machine Reasoning package. For more information, see Download and Install Packages and Updates in the [Cisco DNA Center Administrator Guide](#).

**Step 1** Click the menu icon () and choose **Tools > Network Reasoner**.

**Step 2** Select **Network Bug Identifier**.

**Step 3** Click **Scan Network**.

**Step 4** In the **Scan Network** window, choose whether you want to scan your system for bugs **Now** or schedule it for **Later**.

The dashboard progress indicator shows the list of devices scanned in batches of 10. When the scan is done, the **Network Bug Identifier** window appears.

**Step 5** Use the top pane to view information about the results of the scan, rescan the network, and change scan settings, as follows:

Item	Description
<b>Bug Summary</b>	Number of <b>Catastrophic</b> , <b>Severe</b> , and <b>Moderate</b> bugs in your network.
<b>Affected Devices</b>	Number of the following device types that were scanned: <ul style="list-style-type: none"> <li>• <b>Routers</b></li> <li>• <b>Switches and Hubs</b></li> </ul>
<b>Scan Mode</b>	Method used to perform the scan: <ul style="list-style-type: none"> <li>• <b>Essential</b>: Scan performed using the Cisco Network Reasoner Engine (NRE).</li> <li>• <b>CX Cloud</b>: Scan performed using the CX Cloud.</li> </ul>
<b>Re-scan Network</b>	Click this button to scan your network again.
<b>Settings</b>	Click the <b>Settings</b> icon to do the following: <ul style="list-style-type: none"> <li>• Enable or disable weekly scans.</li> <li>• Enable or disable the CX Cloud to scan your network.</li> </ul>

**Step 6** Click the **Bugs on Devices** tab to view information about the bug, such as **Bug ID**, **Name**, **Affected Devices**, **Severity**, **Affected Versions**, and **Workaround**.

Click any hyperlinked value to display more information about it.

**Step 7** Click the **Devices** tab to view information about the devices, such as **Device Name**, **Image Version**, **IP Address**, **Device Type**, **Bugs**, **Scan Status**, **Scan Mode**, **Site**, and **Reachability**.

Click any hyperlinked value to display more information about it.

**Step 8** From the **Devices** tab, click **Tag Device** to create, edit, or delete tags on the devices.

# Scan Cisco DNA Center for Bugs

The **System Bug Identifier** tool provides an option to identify bugs in the Cisco DNA Center. The following procedure explains how to enable the **System Bug Identifier** tool:

## Before you begin

- Install the Cisco DNA Center core package. For more information, see Download and Install Packages and Updates in the *Cisco DNA Center Administrator Guide*.
- Install the Machine Reasoning package. For more information, see Download and Install Packages and Updates in the *Cisco DNA Center Administrator Guide*.

- 
- Step 1** Click the menu icon (☰) and choose **Tools > Network Reasoner**.
- Step 2** Select **System Bug Identifier**.
- Step 3** Click **Scan System**.
- Step 4** In the **Scan System** window, choose whether you want to scan your system for bugs **Now** or schedule it for **Later**.
- Step 5** The **System Bug Identifier** window shows the **BUG SUMMARY** and the **Bugs Identified on Your System** table. In addition to basic bug information, this window shows information, such as when the bug was first and last identified, the frequency that it was identified and affected versions.
- Step 6** Click the **Bug ID**. The **Bug Details** dialog box displays the details of the bug.
- Step 7** Click the arrow next to **Bug ID** to go to the **Bug Search Tools** window, which shows more details about the bugs.
-

