



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 5](#)
- [Troubleshoot a Downed Interface, on page 6](#)
- [Troubleshoot Network Connectivity, on page 7](#)
- [Troubleshoot IP Connectivity of a Device, on page 7](#)
- [Troubleshoot Wireless Clients Using the MRE Workflow, on page 8](#)
- [Troubleshoot Wireless APs Using the MRE Workflow, on page 9](#)
- [Troubleshoot Unmonitored Devices Using the MRE Workflow, on page 10](#)
- [Troubleshoot HA on Cisco Wireless Controller Using the MRE Workflow, on page 10](#)

Network Reasoner Overview

The Network Reasoner tool allows you to troubleshoot various issues on your network quickly. From the top-left corner, 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 From the top-left corner, 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"> a. Click SDA Hardware Readiness Check. b. Click Run Machine Reasoning.
SDA Software Readiness Check	Checks whether the software is ready for Cisco SD-Access migration.	<ol style="list-style-type: none"> a. Click SDA Software Readiness Check. b. Click Run Machine Reasoning.
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"> a. Click Redundant Link Check. b. Select an appropriate device. c. Click Troubleshoot.
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"> a. Click L3 Access Check. b. Select an appropriate device. c. Click Troubleshoot.
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"> a. Click MTU Link Check. b. Select an appropriate device. c. Click Troubleshoot.
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"> a. Click Fabric Count. b. Click Run Machine Reasoning.

Workflow	Description	Action
SDA Health Check: Fabric Data Collection	Collects show command outputs from network devices to troubleshoot issues in a fabric network.	<ol style="list-style-type: none"> a. Click Fabric Data Collection. b. Choose the devices and click Troubleshoot. c. After Machine Reasoning is completed, click View Details. d. In the Conclusions tab, click the link to download the output file. The output file is a bundle of text files containing all executed commands on the selected devices.
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.	<ol style="list-style-type: none"> a. Click SDA Scale Limits Check. b. Click Run Machine Reasoning.
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.	<ol style="list-style-type: none"> a. Click Client Count. b. Click Run Machine Reasoning.
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.	<ol style="list-style-type: none"> a. Click Device Count. b. Click Run Machine Reasoning.
SDA Health Check: LISP PubSub Session Check	Checks the LISP PubSub health on the fabric border device. If a PubSub session is down, troubleshoot to find the root cause.	<ol style="list-style-type: none"> a. Click LISP PubSub Session Check. b. Choose the devices and click Troubleshoot. c. After Machine Reasoning is completed, click View Details.
SDA Health Check: LISP Session Check	Checks the status of all LISP sessions on the chosen device. If a session is down, troubleshoot to find the root cause	<ol style="list-style-type: none"> a. Click LISP Session Check. b. Choose the devices and click Troubleshoot. c. After Machine Reasoning is completed, click View Details.

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 From the top-left corner, 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 From the top-left corner, 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 From the top-left corner, 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** From the top-left corner, 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** From the top-left corner, 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** From the top-left corner, 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** From the top-left corner, 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** From the top-left corner, 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.




Troubleshoot HA on Cisco Wireless Controller Using the MRE Workflow

The MRE workflow analyzes the HA health on Cisco Wireless Controllers by processing the command outputs. This workflow is supported on the Cisco Catalyst 9800 Series Wireless Controllers and Cisco Catalyst 9800-CL

Wireless Controllers for Cloud running Cisco IOS XE Release 17.1 or later. Use this procedure to troubleshoot HA issues on wireless controllers using the MRE workflow.

Before you begin


Ensure 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** From the top-left corner, click the menu icon and choose **Tools > Network Reasoner**.
Alternatively, you can troubleshoot the HA issues on wireless controllers from the **Provision > Inventory** window. If there is an HA issue on a wireless controller, a red link icon () is displayed next to the wireless controller. To troubleshoot the HA issues, click the red link icon, and then click **HA SSO Analysis**. Skip to [Step 5, on page 11](#).
- Step 2** Click the **Catalyst 9800 Wireless Controller HA SSO Analysis** tile.
The **Devices** window displays the wireless controllers. If HA is configured on a wireless controller, Cisco DNA Center displays a link icon () next to the device name. A red link icon () indicates an HA issue on the wireless controller.
- Step 3** From the left hierarchy tree, choose the required site.
- Step 4** Click the radio button next to the device name that you want to troubleshoot, and then click **Troubleshoot**.
Optionally, to stop the ongoing reasoning activity, click **Stop**.
- Step 5** After the troubleshooting is complete, the **Machine Reasoning Completed** dialog box opens. Click **View Details**.
- Step 6** In the **Root Cause Analysis** area, the **Reasoning Activity** tab displays the parameters that are checked as part of the troubleshooting process. To view the details of an activity, click the corresponding activity tile.

The analysis uses the following parameters in the mentioned order:

Number	MRE Analysis Parameters	Description
1	Check Controller Manageability	<ul style="list-style-type: none"> • Checks if the wireless controller is running Cisco IOS XE Release 17.1 or later. • Checks if the wireless controller IP address is in reachable state. • Checks the SNMP, CLI credentials, and Netconf. • Checks if the wireless controller is Cisco Catalyst 9800 Series Wireless Controllers or Cisco Catalyst 9800-CL Wireless Controllers for Cloud.
2	Evaluate Cisco DNA Center platform	Checks if all the services in the platform are a part of the Cisco DNA Center ISO.
3	Check HA is configured in Controller	Checks if the sensors on the active and standby wireless controller are operating in normal threshold range.
4	Check Primary device and Secondary device status in HA Pair	Checks if the HA configuration is completed on the wireless controllers.

Number	MRE Analysis Parameters	Description
5	Show RP and RMI status	Checks the connectivity of the Redundancy Port (RP) link and Redundancy Management Interface (RMI) link between the active and standby wireless controllers running Cisco IOS XE Release 17.6 or later.
6	Check the HA Status	<ul style="list-style-type: none"> • Checks if the standby wireless controller is in HA removed state. • Checks if the standby wireless controller synchronization is in progress. • Checks if the power supply and RP network connectivity of the standby wireless controller are working as expected. • Checks if both active and standby wireless controllers are running the same image version.
7	Secondary device deletion check in DNAC	<ul style="list-style-type: none"> • Checks if HA is configured successfully. • Checks if the standby wireless controller is in deleted state.

Step 7 The **Conclusions** tab displays the troubleshooting information. Cisco DNA Center highlights an issue with the  icon. It displays suggested action to resolve the issue in the **Suggested Action** area below the issue.

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

What to do next

If your HA issue is not listed in the root cause or you need further assistance, contact Cisco Technical Assistance Center (TAC).