



AI Troubleshooting for Industrial Networks User Guide

Cisco AI Troubleshooting for Industrial Networks
Updated August 31, 2026

Topics included

1 AI-Assisted Industrial Network Diagnostics.....	4
Application overview.....	5
Monitored OT issues.....	5
Product features.....	6
User roles and permissions.....	6
Access at a glance.....	6
Permission-based access.....	7
2 Alert-first triage.....	8
Alert-first triage.....	9
Alert review and response.....	9
Notes and limitations.....	9
Review and resolve an alert.....	9
Workflows by role.....	11
OT user tasks.....	12
Admin tasks.....	12
Manage application settings and users.....	16
3 Resolve common issues.....	18
Common issues and first actions.....	19

1 AI-Assisted Industrial Network Diagnostics

Topics:

- [Application overview](#)
- [User roles and permissions](#)

Learn how the application combines alerts, AI-assisted analysis, topology, inventory, and guided next steps to help diagnose industrial network issues.

Application overview

Learn how the application supports industrial network troubleshooting, who can use it, and how to assess its recommendations.

AI Troubleshooting for Industrial Networks helps maintenance technicians and network administrators find and understand industrial network issues. It brings alerts, AI-assisted investigation, topology context, device inventory, and guided next steps into one workspace.

The application supports both **OT users**, who investigate active alerts, and **Admins**, who maintain the application and perform deeper troubleshooting. Available workflows and controls depend on the user's role and permissions.

Important

When using AI Troubleshooting for Industrial Networks, verify AI-generated recommendations against live plant conditions, source evidence, site operating procedures, and change-control requirements. Use the tool to accelerate diagnosis, not to bypass operational judgment.

Monitored OT issues

Review the endpoint, link, PoE, switch health, duplicate IP, L2NAT, and power-loss conditions monitored by the application.

Cisco AI Troubleshooting for Industrial Networks enables you to monitor a wide range of OT issues..

Monitored OT issues

Area	Examples of monitored issues	Why this matters
Endpoint offline or degraded	Port down, err-disabled port, endpoint moved, VLAN mismatch, unreachable device, duplex issues, or error issues	Identifies whether an endpoint is offline, moved, unreachable, or affected by access-layer symptoms.
Link, cable, and media faults	Link down or flapping, copper cable faults, fiber or SFP issues, unsupported transceivers, or degraded transceivers	Helps determine whether a port, cable, optic, fiber module, or media path is involved.
Power over Ethernet (PoE) and endpoint power	PoE disabled, power budget exhausted, port power limit issue, or powered device not detected	Identifies whether a powered endpoint is offline or unstable because of a power condition.
Switch power, health, and reachability	Power-supply issue, input-power loss, redundancy degraded, voltage warning, CPU pressure, memory pressure, or an unreachable/offline switch	Determines whether switch health, power, or reachability contributes to the issue.
Duplicate IP and L2NAT conflicts	Duplicate translated IP, L2NAT-reserved IP conflict, or multiple devices claiming the same IP	Distinguishes expected translation behavior from addressing conflicts.
Power-loss events	Dying gasp, input-power fault, or device dark after power loss or unplugging	Identifies equipment that may have gone offline because of power loss.

Product features

Review ambient monitoring, root-cause diagnosis, conversational queries, topology, evidence-backed recommendations, and on-premises data control.

Cisco AI Troubleshooting for Industrial Networks offers continuous industrial network monitoring, conversational troubleshooting, interactive topology, and rapid root-cause diagnosis.

Feature	Description
Ambient monitoring	The agent continuously monitors industrial network signals and alerts users before issues become longer outages.
Root-cause diagnosis	The agent correlates topology, device state, syslog, and configuration evidence to identify likely causes faster than manual investigation.
Conversational interface	Users can ask natural-language questions about devices, connections, VLANs, and network state without signing in to switches.
OT-friendly troubleshooting	Plain-language guidance, topology views, asset names, and operational context help users understand what happened and what to do next.
Interactive network topology	A searchable topology map helps identify affected switches, interfaces, endpoints, and locations.
Evidence-backed recommendations	Recommendations show how conclusions were determined from verified network data so users can validate findings before acting.
On-premises data control	Customer credentials, topology, logs, configurations, and operational data remain on-premises.

User roles and permissions

Compare Admin and OT user access to alerts, AI chat, topology, inventory, settings, and user management.

AI Troubleshooting has two application roles: **Admin** and **OT user**. Your assigned role determines which pages, controls, and actions are available to you.

Access at a glance

Compare the actions available to Admins and OT users across alerts, AI chat, topology, inventory, and custom fields.

Admin and OT user roles have different accesses and permissions over the features and capabilities of AI Troubleshooting for Industrial Networks.

Role-based access definitions

Area	Admin	OT user
Alerts and alert threads	View, investigate, manage, and mark alerts Resolved	View, investigate, and mark alerts Resolved

Area	Admin	OT user
AI chat	Create threads and send curated freeform prompts	Use preset follow-ups in alert threads only
Topology	Search, navigate, configure, and edit	Search and navigate in view-only mode
Devices inventory	View and manage device records	View device records in read-only mode
Proxies inventory	View and manage proxy records	View proxy records in read-only mode
Custom fields	Add, edit, and manage fields and values	View available fields and values only
Settings	Access application settings and user management	No access

Permission-based access

Understand which actions require Admin permissions and which controls OT users may see but cannot use.

OT users can investigate alerts, use supported follow-up prompts, and view Topology and Inventory. Only Admins can create independent threads, access Settings, or change device records and user access.



Note

If you have the **OT user** role, you might see **New Thread**, **Ask a question**, **Discuss this device**, **Add devices**, **Custom field**, or **Remove** without permission to use them. Inventory is view-only for OT users; **Settings** requires the Admin role.

2 Alert-first triage

Topics:

- [Alert-first triage](#)
- [Workflows by role](#)

Use this chapter to review alerts, examine evidence, work with topology and inventory, and complete approved next steps.

Alert-first triage

Use alerts, evidence, topology, and inventory to choose an approved action, resolve the issue, or hand it off with useful context.

AI Troubleshooting for Industrial Networks enables alert-first triage for both OT users and Admins. Both roles use the application to understand what happened and review the evidence it collected. Depending on their permissions, they can take an approved field or administrative action, resolve the alert, or hand it off with useful context.

Alert review and response

Follow the alert path from prioritization and thread review through evidence validation, approved action, resolution, or handoff.

Summary

The alert investigation process moves through these stages:

Workflow

These are the stages of alert investigation process.

1. Review and prioritize the alert.
2. Open the alert thread.
3. Read the report and review its evidence.
4. Inspect topology or inventory when additional network context is needed.
5. Use an available preset follow-up when another supported check is needed.
6. Validate the recommendation against live plant conditions and site procedures.
7. Complete the approved field action, resolve the alert, or hand it off with useful context.

Notes and limitations

Understand role limits for preset follow-ups, Topology and Inventory changes, and device-specific AI conversations.

OT users and Admins have different access to the same AI Troubleshooting for Industrial Networks features.

- OT users can use only the available preset follow-ups. They cannot type or edit the message sent by a preset.
- Both roles can view Topology and Inventory. OT users cannot add, edit, or remove inventory records, and passwords are not displayed. Only Admins can perform authorized inventory and topology changes.
- When you select a device, you may see the **Discuss this device** option. OT users cannot use this feature even if the option is displayed. Only Admins can use it to start an AI conversation from a topology device.

Review and resolve an alert

Open an alert, review its report and evidence, inspect network context, and resolve or hand off the issue.

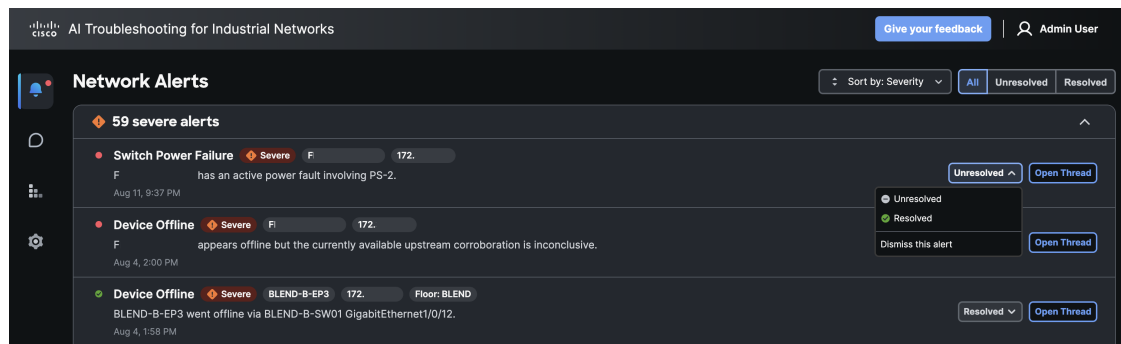
Follow these steps to investigate an alert and resolve or hand off the issue.

Procedure

1. From the AI Troubleshooting for Industrial Networks menu, choose **Alerts**.

- Review the alert details. Confirm the issue title, severity, affected device, switch, endpoint, or IP address; visible custom-field badges; description; detection time; current status; and **Open Thread** option. Filter to **Unresolved** for active work, and sort by **Severity** or **Status** as needed.

Figure 1: Alerts page showing alert filters and rows

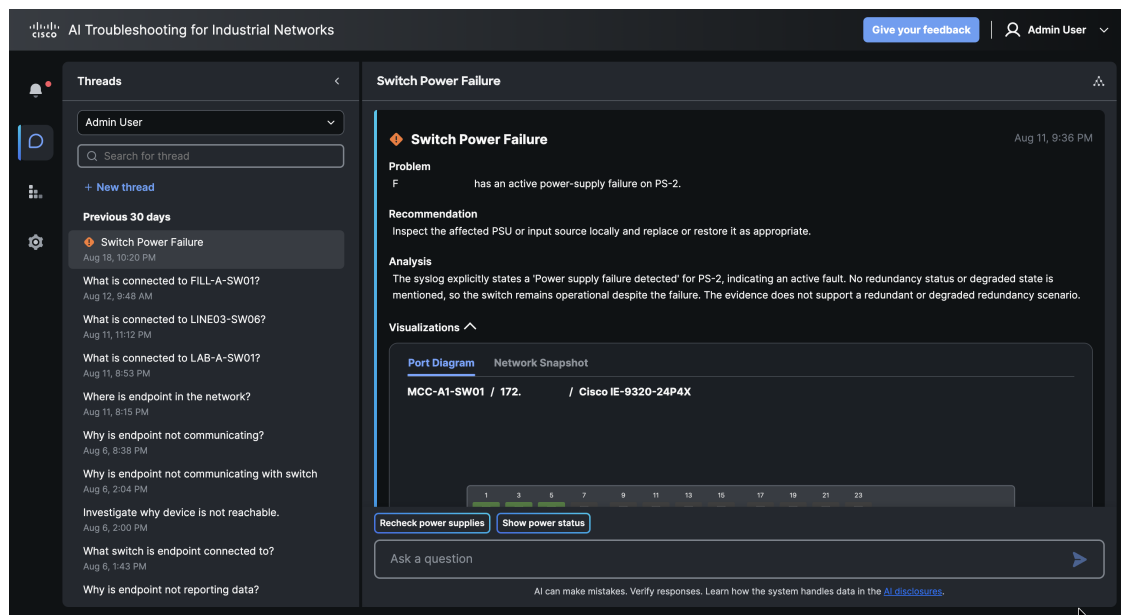


- Select **Open Thread** for the alert that needs investigation. The associated thread keeps the alert, report, evidence, and investigation history together.

The alert thread workspace is arranged from left to right: the threads list, the report and conversation panel, and the **Topology** panel. Drag a panel divider to resize it when available. Select the collapse or expand icon in a panel header to hide or restore that panel.

- Read the report's **Problem** and **Recommendation** sections first. Review **Analysis**, visualizations, and diagnostic evidence when you need more detail.
 - Select **Visualizations** to inspect a **Port Diagram** or **Network Snapshot**
 - Select **How this was determined** to review the diagnostic evidence.

Figure 2: Alert thread report showing the Problem and Recommendation sections



- Problem** states what appears to be wrong.
- Recommendation** presents the recommended action and next steps.
- Analysis** explains what the available evidence does and does not establish.

- Choose your next step based on the provided information.

If you need to...	OT users	Admins
Run another supported check	Select an available preset follow-up. You cannot edit the message.	Select an available preset follow-up, or use the Admin chat composer with a supported prompt.
Review network context	Inspect Topology and Inventory in view-only mode. Ask an Admin to correct device or proxy records when needed.	Inspect Topology and Inventory . Make authorized changes when needed.
Investigate a device	Review the device and its connected path. Do not use Discuss this device to start an AI conversation.	Select Discuss this device when available, choose a supported prompt, and fill the required values.
Continue an investigation that is not tied to an alert	Provide the alert and investigation context to an Admin.	Open Threads , select New Thread , and start a supported investigation.
Complete the recommended action	Verify the recommendation against live plant conditions and site procedures. Complete the approved field action or hand off the issue.	Verify the recommendation against live plant conditions and site procedures. Complete the authorized action or continue the investigation.
Close the issue	Record the action taken and select Resolved when the issue is complete.	Record the action taken and select Resolved when the issue is complete.
Hand off the issue	Include the alert, affected device, evidence, action taken, and current status.	Include the alert, affected device, evidence, action taken, and current status when escalating or transferring ownership.

6. Verify that the recommendation agrees with live plant conditions, source evidence, site procedures, and change-control requirements.
7. For the alert, select **Resolved** when the issue is fully addressed.

Workflows by role

See how Admins and OT users use the same alert process with different capabilities for investigation, network context, actions, and handoff.

Admins and OT users use an alert-first process. Both roles can use Topology and Inventory to understand an alert. OT users can view network and inventory information, while only Admins can change topology or manage device and proxy records.

Topology provides network context for an affected device. In **Topology**, pan across the map, scan connected devices and paths, zoom in or out, and use available search or viewing controls to understand where the device sits in the network.

Inventory provides device and proxy records for troubleshooting. Select the **Devices** or **Proxies** tab, then search, filter, sort, or paginate the table to find a record.

Inventory is read-only for OT users: they cannot add, edit, or remove records, and passwords are not displayed. Ask an Admin to correct inventory information when needed.

OT user tasks

Use preset follow-ups and view-only network context to review alerts, complete approved field actions, and close or hand off issues.

The OT user tasks support alert-first triage. Use them to understand what happened, review the evidence collected by the application, take the approved field action, and either resolve the alert or hand it off with useful context.

Admin tasks

Use supported prompts, topology, inventory, settings, and user management for broader diagnosis and administration.

Admin role required: The tasks in this section are available to users with the Admin role. Admins can use the shared alert-first process and the Admin tasks described here for broader troubleshooting and administration.



Note

Admin role required: The tasks in this section are available to users with the **Admin** role. Admins can use the shared alert-first process and the Admin tasks described here for broader troubleshooting and administration.

Admin process overview

Follow the Admin path for alert review, independent investigations, device analysis, inventory maintenance, and application administration.

Summary

Use the following process when you need to investigate an alert, continue an investigation, or maintain application data:

Workflow

These are the stages of admin process overview.

1. Start with the [shared alert investigation process](#) when an alert exists.
2. Use [Ask a targeted question](#) to start or continue an investigation that is not tied to an alert.
3. Use [Investigate a device in Topology](#) to review device paths and use supported device prompts.
4. Use [Maintain Inventory and custom fields](#) to correct records, discovery results, or identifying fields.
5. Use [Manage application settings and users](#) to review data sources, agent status, user access, and audit logs.

Ask targeted questions with prompt suggestions

Use supported prompts to investigate alerts, devices, topology, switch operations, endpoints, inventory, and configuration.

The Threads features provides prompt suggestions to help you initiate an alert or device examination. The prompts also allow you to choose a wide range of identifier values from drop-down lists, improving accuracy and the time taken to create a full, specific query.

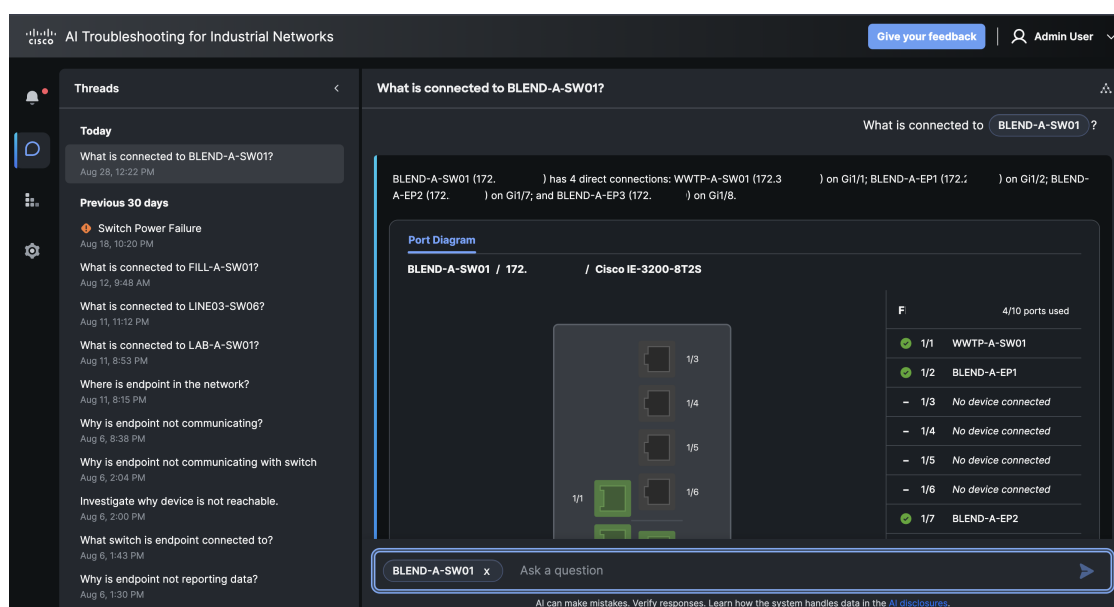
Supported prompt categories can include:

Prompt category	Example questions
Topology	Which devices are connected to this switch? Where is this endpoint located?

Prompt category	Example questions
Switch operations	What version is this switch running? What is the interface status?
Endpoint operations	Is this endpoint reachable? What is the parent-link status?
Inventory	List all IE-3500 switches. What devices are in Zone 3?
Configuration	What VLANs are configured? What is the PoE budget?

The response you receive typically also displays the device and device parts that the query is related to. The selected device remains visible as context for the conversation. You can remove the device context when it no longer applies to the question.

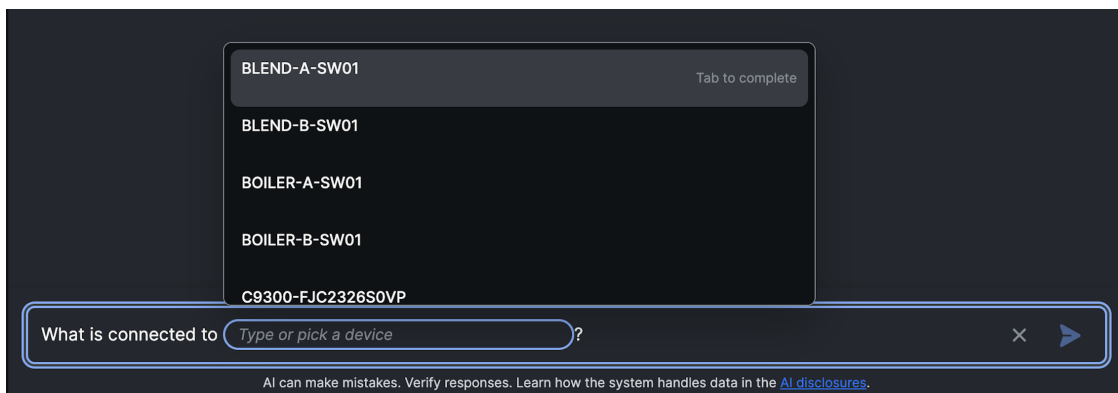
Figure 3: AI response showing the selected device as context



Procedure

- From the Cisco AI Troubleshooting for Industrial Networks menu, choose **Threads**.
- Identify or create a thread to work on.
 - Use the search field to find a thread by its title or visible content, and select a thread to view its contents.
 - Select **New Thread** to begin an investigation that is not tied to an existing alert. Start with the device name, location, and symptom.
- Admins can use the chat composer to investigate an alert, or a device. As you type, an autocomplete menu ranks supported prompt templates.
 - Select a suggested query to open its complete sentence with highlighted slots.
 - To enter a value for a device, zone, device model, port, or IP address, click the highlighted slot and select values from the dropdown lists. Depending on the prompt, a custom inventory field or grouping value can provide the value used by your team.

Figure 4: Prompt autocomplete list with supported queries



4. (Optional) If the desired question does not match a supported prompt, rewrite it using the equipment name, zone, switch, port, and symptom so the application can identify the intended context.
5. After you choose values for all the required slots in the prompt, submit the prompt.

What to do next

Use the **Rename thread** option when a clearer name will help the next shift find the conversation.

Investigate a device in Topology

Use the network map to locate a device, inspect its connected path, ask supported device questions, and maintain the site layout.

Use **Topology** as a searchable network map to move from a production symptom to the relevant switch, port, endpoint, location, or path. Search for the affected endpoint, switch, zone, or visible device name, then select the result to focus the map.



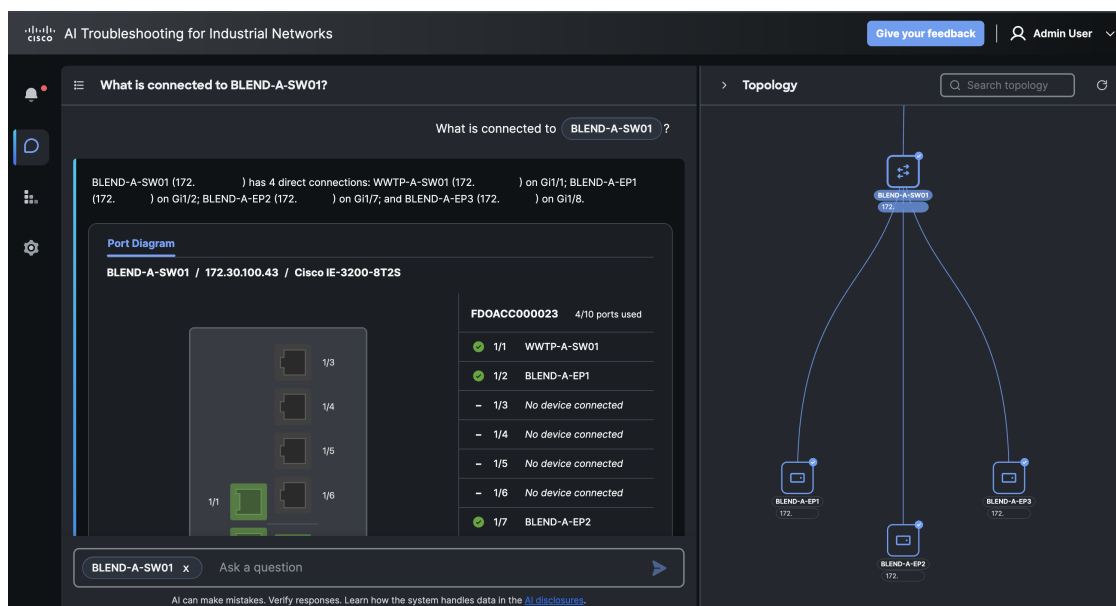
Note

When a network issue affects devices, the topology highlights the impacted devices.

Procedure

1. Use the search field to focus the map on a device and review its connected path.

Figure 5: Topology view showing connected devices and paths



2. Select **Discuss this device** to open the autocomplete prompt experience with the selected device supplied to a compatible device slot.
3. Use available display options to choose which inventory fields appear on device labels or to group devices by a site field such as zone or another custom field.
4. When the displayed layout needs to be arranged for the site, use **Edit topology**.

You select one or multiple devices and drag them into the desired positions.

Other controls available to you at this step include **Undo**, **Redo**, **Display options**, **Clean up**, **Reset to default layout**, and **Cancel**.

Note

Do not use the edit capability to represent a connection that has not been verified in the physical network, or in the discovery data.

5. After you finish editing the topology, click **Save**.

Maintain Inventory and custom fields

Add or update devices, proxies, custom fields, and discovery results so topology and diagnosis use current site data.

The **Inventory** pages help you to maintain the device records used by topology and troubleshooting.

- The **Devices** tab supports inventory search, custom-field filters, pagination, and admin controls for adding or editing device records.
- The **Proxies** tab lists the proxy records used to access devices.

Before you begin

Sign in as an **Admin**. OT users can view Inventory, but only Admins can add, edit, or remove records, manage custom fields, and run discovery.

Procedure

1. From the Cisco AI Troubleshooting for Industrial Networks menu, choose **Inventory**.
2. To add a custom field to the Inventory table, click **Custom field**.
 - a) Enter a clear field name such as **Zone**, **Manufacturer**, or **Device role**.
 - b) Then, save the field.
 - c) For the devices in the list, enter the values for the newly created custom field.
3. To add one or more devices to the inventory or to refresh the topology pages to align with any network changes, choose **Add Devices**.
 - Add a known device when that option is available.
 - Click **Run discovery again** to run an LLDP search from a switch.
 - Upload a .csv file of the devices you want to add.
 - a) Review the proposed changes and apply the changes only when they match the expected site state.

Manage application settings and users

Review discovery, syslog and alerting, agent status, audit logs, and user access; change configuration only under site procedures.

Only admins can access the **Settings** menu to review application input sources, the agent status, and user accesses. Follow site change-control procedures before changing any configuration.

Data sources

Review the information that is entering the application in the **Data sources** area.

Area	What to review
Network discovery	Discovery status, seed device, discovery protocol, and last scan time.
Syslogs and alerting	Whether syslogs are being received, event counts, generated alerts, and monitored event types.
Discovery controls	Reconfigure and other controls used to change discovery settings.
Syslog controls	Enable automatic log collection and analysis and Save syslog settings ,

Select **Reconfigure** or save syslog settings only when the change is authorized. If expected events are not received, confirm the switch or syslog server is forwarding them to the configured destination.

Agent

Review agent status, cloud tether key status, key rotation controls, and agent software version information in the **Agent** area. The page also provides information on the last update check, allows you to check for a new software update, and can provide an offline package upload control.

Audit logs

Review recorded user and application events using **Audit Logs**.

Control or column	Use it to
User Access Logs	Review sign-in and access activity.
Application Logs	Review recorded application events.
Refresh	Load the latest available events.
Time, Event, User, Resource, Outcome, Message	Understand what happened and whether an event succeeded.

Manage users

Add, review, edit, or remove application users and assign the Admin or OT user role.

Use this task to add, edit, or remove application users.

Before you begin

Sign in as an **Admin**. Only Admins can manage user access.

Procedure

1. From the Cisco AI Troubleshooting for Industrial Networks menu, choose **Settings > Users**
2. Select **Add** to create a user, or select an existing user to edit the account.
3. Enter or review **Username** and **Display Name**.
4. Select **Admin** or **OT User** in **Assigned Role**.
5. Review **Status** and **Last Accessed**, then select **Save**. Select **Cancel** to discard unsaved changes.
6. Select **Delete** only when the site access-control process permits removal.

3 Resolve common issues

Topics:

- [Common issues and first actions](#)

Use symptom-based guidance to identify likely causes and take the first recommended action.

Common issues and first actions

Find likely causes, the first action to try, and follow-up guidance for sign-in, alerts, thread context, topology, inventory, AI responses, procedure conflicts, and missing evidence.

Use this table to identify a likely cause and the first action to try. Follow the additional guidance under the matching symptom only when the first action does not resolve the issue.

Common issues

Use this table to identify a likely cause and the first action to try. Follow the additional guidance under the matching symptom only when the first action does not resolve the issue.

Symptom	Likely causes	Try this first	If the issue continues
Cannot sign in	User session, credentials, access policy, or authentication issue.	Refresh the page and sign in with your assigned credentials.	Ask an Admin to verify your role or activation status.
No alerts appear	Filters hide alerts, no current alerts exist, syslog forwarding is not configured, or alert processing is delayed.	Open Alerts and clear restrictive filters.	1. Select All or All Alerts. 2. Select Unresolved only when you need active alerts. 3. Ask an Admin to confirm that switches or the site's syslog server are forwarding events to AI Troubleshooting.
Thread context looks wrong	The wrong alert or device was opened, or the thread lacks required context.	Reopen the intended alert thread and verify the device in the report.	1. Return to Alerts, open the intended alert, and confirm the affected equipment in the report and its embedded visualizations. 2. If you are an Admin and the device name or location is wrong, check Inventory before continuing.
Topology view is blank or stale	Discovery has not run, inventory is missing, LLDP is disabled, or the data is out of date.	Refresh Topology and search for a known device.	1. Refresh the view and search for a known device when those controls are available. 2. Ask an Admin to verify that discovery completed, inventory is current, and the required discovery protocol is enabled.

Symptom	Likely causes	Try this first	If the issue continues
Inventory search misses a device	The device was not imported, was renamed, has the wrong zone or type, or discovery has not synchronized.	Clear filters and search by IP address, vendor, or model.	1. Search by IP address, vendor, or model. 2. Ask an Admin to review the latest discovery result or correct the inventory record according to site procedures.
AI response is incomplete	Required evidence or asset context is unavailable.	Review the available evidence and context.	If the response remains incomplete, treat it as unverified when required evidence is missing. Admins can use a more specific supported prompt and include the equipment name, location or zone, switch, port, and symptom. OT users should use the available preset follow-up actions for the alert.
Recommendation conflicts with site procedure	Local operating, safety, or change-control requirements take precedence.	Follow the approved site procedure.	Follow the approved site procedure. Do not perform an action that could affect production or safety systems simply because it appears in an AI recommendation. Record the conflict and escalate it for runbook or configuration review.
Expected data is missing	Evidence is unavailable or a supporting service cannot retrieve the required context.	Capture the alert title, timestamp, affected equipment, thread, and visible error.	Provide the information to an Admin or the next support team.

