



AI Troubleshooting for Industrial Networks Installation Guide

Cisco AI Troubleshooting for Industrial Networks
Updated August 31, 2026

Topics included

1 Overview.....	4
Installation overview.....	5
Compatibility.....	5
Product features.....	6
Monitored OT issues.....	6
User roles.....	7
2 Deploy and configure.....	8
Prepare for deployment.....	9
Validate network configuration and service health.....	10
Validate application access from a browser.....	11
First-Time Setup.....	11
3 Troubleshoot.....	14
Common issues.....	15

1 Overview

Topics:

- [Installation overview](#)
- [Compatibility](#)
- [Product features](#)
- [Monitored OT issues](#)
- [User roles](#)

Use this chapter to review installation requirements, supported platforms, product capabilities, monitored OT conditions, and user roles.

Installation overview

Learn what the on-premises application does, where it stores operational data, and what to consider before deployment.

AI Troubleshooting for Industrial Networks is an on-premises AI agent for industrial operations. It helps maintenance users and network administrators maximize network availability by detecting industrial network issues, diagnosing likely root causes, and providing plain-language remediation guidance.

The offering is part of Cisco AgenticOps. It is intended for industrial environments where network issues can affect robots, sensors, programmable logic controllers (PLCs), human-machine interfaces (HMIs), safety systems, machines, cameras, access points, industrial switches, and connected monitoring systems. It brings ambient monitoring, alert triage, AI-assisted investigation, topology context, device inventory, and operational runbooks into one workspace.

Customer credentials, topology, logs, configurations, and operational data stay on-premises at the industrial site. Cloud connectivity, when configured, is used for software updates and agent operational telemetry.

Important

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.

Compatibility

Check the supported virtualization platforms, software versions, and Cisco IOS XE switch families for the installation.

Supported virtualization platform.

Supported virtualization platforms and switch families

Table 1: Supported virtualization platforms

Virtualization platform	Version or package requirement
VMware ESXi	8.0.3 and above
Nutanix	Prism Central pc.2024.3.1 and above

Supported IOS XE switches:

1. Cisco Catalyst IE3100 Rugged Series and Heavy Duty Series switches
2. Cisco Catalyst IE3200 Rugged Series switches
3. Cisco Catalyst IE3300 Rugged Series switches
4. Cisco Catalyst IE3400 Rugged Series and Heavy Duty Series switches
5. Cisco Catalyst IE3500 Rugged Series and Heavy Duty Series switches
6. Cisco Catalyst IE9300 Rugged Series switches
7. Cisco Catalyst 9300 Series switches

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.

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.

Area	Examples of monitored issues	Why this matters
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.

User roles

Compare the Admin and OT User responsibilities for application setup, alert triage, investigation, maintenance, and escalation.

AI Troubleshooting has two assignable application roles: **Admin** and **OT User**.

Role	Use it to
Admin	Set up and maintain the application, manage users, review settings, configure data sources, maintain agent update settings, review audit logs, and support escalation.
OT User	Triage alerts, open troubleshooting threads, search topology and inventory in view-only mode, review recommendations, and hand off remediation.

2 Deploy and configure

Topics:

- [Prepare for deployment](#)
- [Validate network configuration and service health](#)
- [Validate application access from a browser](#)
- [First-Time Setup](#)

Prepare the host and network, deploy the application, complete first-time setup, and verify service health and browser access.

Prepare for deployment

Verify the OVA, host resources, network values, DNS, cloud connectivity, and required allowlists before deployment.

Before you begin

1. Download the AI Troubleshooting for Industrial Networks OVA file from Cisco Software. Calculate the OVA file checksum and compare it with the published value.

```
shasum -a 256 <OVA-file>.ova # MacOS/Linux systems
Get-FileHash .\<OVA-file>.ova -Algorithm SHA256 # PowerShell
```



Note

Do not deploy the OVA if its calculated checksum does not exactly match Cisco's published SHA-256 checksum. Download a new copy and verify it again.

2. Ensure these system resources are available.
 - 32 x86 CPU cores
 - 48 GB RAM
 - 70 GB Disk Space
3. Collect the required network information.
 - **IPv4 address with CIDR:** The fixed network address assigned to the VM, including its subnet size. For example, 10.20.30.40/24. This is the address users and devices use to reach the appliance.
 - **IPv4 Gateway:** The router address for the VM's subnet. For example, 10.20.30.1.
 - **IPv4 DNS servers:** Comma separated list of DNS servers. You can provide site DNS servers, public DNS servers, or both, depending on site policy.
4. Create an FQDN that will be used to access the application. For example, `ai-troubleshooting.example.com`.
5. Create a DNS record for that name on the site's private DNS server that points to the VM's assigned IPv4 address. Ensure clients on the application network can resolve the name.
6. Based on your region, ensure that your VM can reach the appropriate cloud endpoint:
 - For US users: `https://agenticops.us.ciscoiot.com`
 - For EU users: `https://agenticops.eu.ciscoiot.com`

Important

The agent must be connected to the cloud tether. If tether connection is lost, the application UI displays warnings for a period of 60 days. If connectivity is not restored within 60 days, the agent is deactivated.

7. Whitelist these IP addresses for AI Troubleshooting for Industrial Networks.

Region	IP addresses
US	• 35.165.80.176 • 44.246.237.194 • 52.33.219.63
EU	• 99.80.74.162 • 99.81.71.205 • 54.171.207.39

Procedure

1. Deploy the OVA file.

Platform	Deployment guidance
Nutanix	Use an IDE disk
VMware ESXi	During deployment, you may see the message A required disk image was missing . You can close the message and select Finish .

2. Log in to the newly created virtual machine with the default credentials, user name **agentadmin**, and password **Cisco@123**. Change the default VM password when prompted and store it securely.
3. Configure the network settings. Enter the values for IPv4 address with CIDR, IPv4 Gateway, and IPv4 DNS servers.

```
sudo agentctl configure network
```

4. Validate the network configuration.

```
ip -4 addr
ping -c 3 <ipv4_gateway>
```

5. Run the command to configure the application.

```
sudo agentctl configure
```

6. Enter the application FQDN and set the admin password for the application UI. Store the admin password securely.
7. Run the command **sudo agentctl up** to start the application services.

Validate network configuration and service health

Run the provided commands on the application VM to verify network settings, service health, active profiles, listeners, and the installed release.

Check network configuration and service health of the application by using these commands on the virtual machine you have deployed the application on.

Table 2: Commands to check network configurations and service health

Command	Use it to
<code>sudo agentctl status</code>	Confirm the service stack health.
<code>sudo agentctl inventory</code>	View a sanitized inventory of active profiles, services, images, listeners, and non-sensitive settings.
<code>sudo agentctl version</code>	View the installed application release version.

Validate application access from a browser

Use a client on the application network to resolve the FQDN, open the application, and sign in with the default credentials.

From a client on the intended application network, resolve the application FQDN and open `http://<application-fqdn>`.

Procedure

1. From a client on the intended application network, resolve the application FQDN and open `https://<application-fqdn>`.
2. Log in with the user credentials you configured in the [Prepare for deployment](#) on page 9 task.

First-Time Setup

Activate the instance, discover devices, add network tags, and configure syslog alerts so the application has the context needed for diagnosis.

The first-time setup wizard involves activating your AI Troubleshooting for Industrial Networks instance, discovering the devices in your network, tagging your network, and setting up alerts.

Before you begin

- In the setup process, you can run a device discovery to collect device information and map connected devices so the agent has the network context needed to generate useful insights. For this discovery to perform as expected, ensure that LLDP is enabled on supported switches and that the switch credentials are correct.
- To activate the instance, you must have a valid cisco.com account that is assigned to a Cisco Smart Account.

Procedure

1. At the first log in, Cisco AI Troubleshooting for Industrial Networks offers a **First-Time Setup** wizard.
2. In the Activate this instance step, configure the region and proxy settings, and then activate the instance .
 - a) Select your region, **US** or **EU**.
 - b) If your site requires a proxy for outbound cloud access, click **Enable Proxy**. Then, enter the proxy host or IP address, including port. For example, `http://proxy.example.com:8080`.
 - c) If the proxy requires authentication, enter both the proxy username and password. If authentication is not needed, leave both fields empty.
 - d) You can activate the instance by connecting with Cisco SSO. The Cisco SSO button is active only after you select a region. A new tab will temporarily open to complete the activation process.

- e) If you have a setup key, enter it manually. If Cisco SSO fails and you do not have a key, write to aitin-activation@cisco.com to request one. Wait for AITIN cloud tether to validate and accept the key. Onboarding does not continue until validation succeeds.

Figure 1: Activation step in the first-time setup wizard for AI Troubleshooting for Industrial Networks

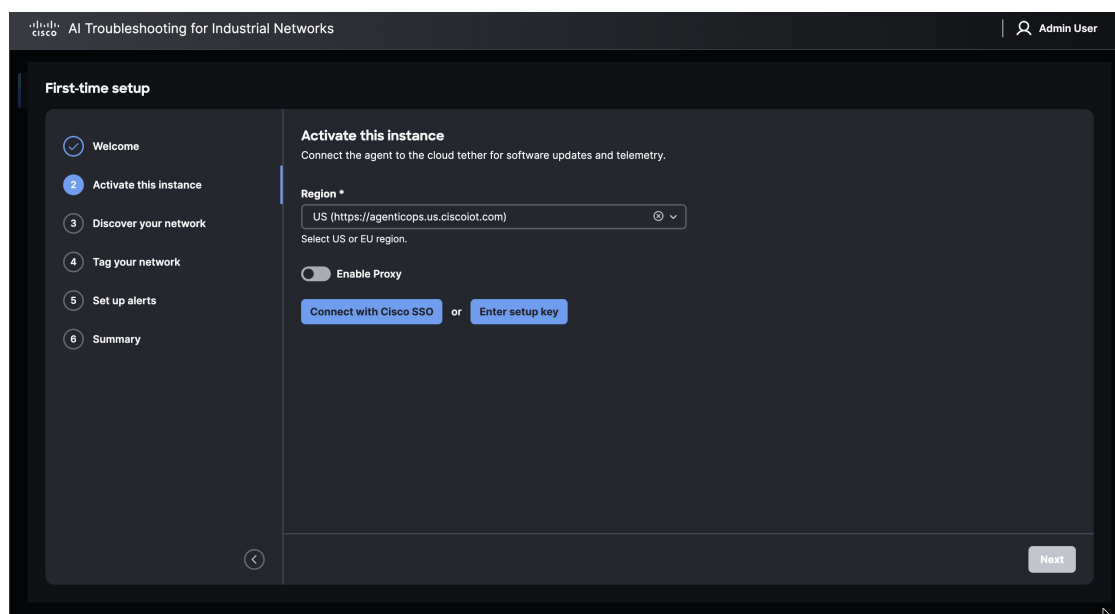
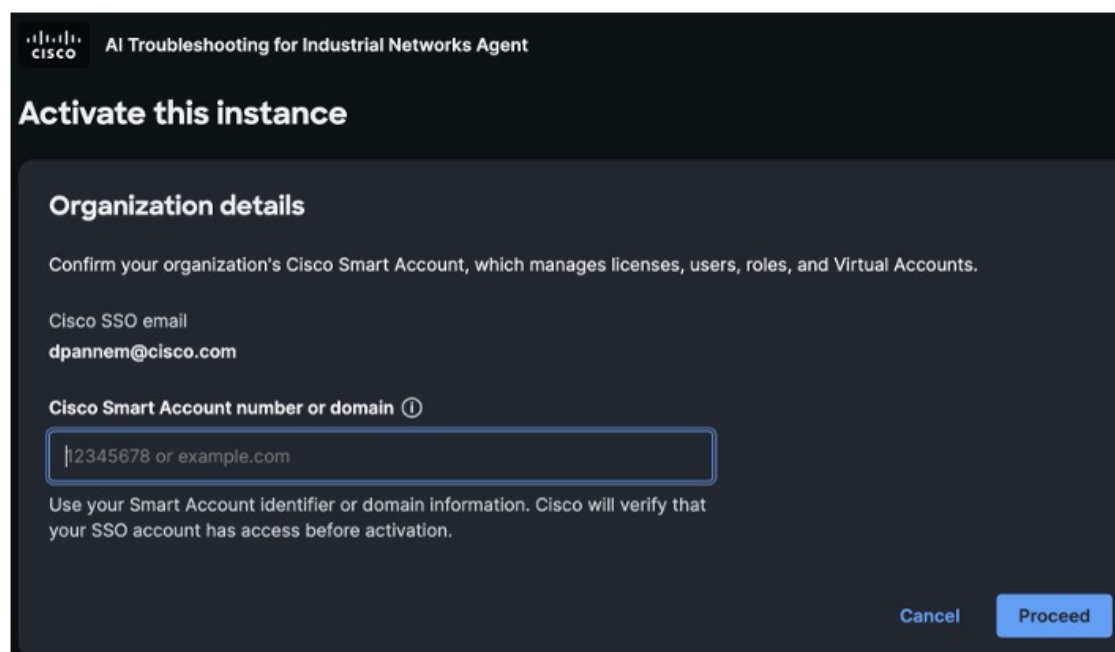


Figure 2: Activate AI Troubleshooting for Industrial Networks with SSO email and Cisco Smart Account



3. Discover your network either by connecting to a single network switch and then discovering connected devices, or by uploading a device list. If you choose the discovery method.
 - a) Enter the IP address, username, and password of the switch you want to start discovery with.
 - b) If the VM can only reach the switch through a proxy or jump host, enable proxy and enter that host's connection details.
 - c) Use the **Run Full Network Discovery** setting to control how far discovery follows LLDP neighbors from the selected switch. This setting is enabled by default and allows discovery of LLDP-supported neighbors for up to four levels total. To collect discovery information only from the selected switch, disable this setting.

4. Add network tags that describe the environment using familiar identifiers such as locations, production areas, line names, and machine names.

You can add more devices and custom tags on the **Inventory** page at any time, using the **Add Devices** or **Add custom field** options.

5. Set up alerts to detect problems automatically. Enable AI Troubleshooting to receive syslogs from network switches by running the **logging host <VM-IP-address> transport udp port 1514** command on each switch.

In this command, the VM IP address is the address that you configured when you ran `sudo agentctl configure network`. Ensure that the devices in your network can reach this address.

**Note**

Alternatively, if devices already forward logs to an existing syslog server, you can instead configure that server to forward the intended logs to the AI Troubleshooting syslog service.

6. View the summary of your onboarding setup and select **Get Started** to finalize the first time setup.
-

3 Troubleshoot

Topics:

- [Common issues](#)

Use service checks, log commands, and recovery guidance to diagnose common deployment and access issues.

Common issues

Match common deployment symptoms to service checks, log commands, and corrective actions for password, network, access, topology, and syslog issues.

Check the health of services on AI Troubleshooting for Industrial Networks. Then, check the logs of any affected services identify the issue.

Table 3: Common challenges and how to troubleshoot them

Issue	Troubleshooting
Forgot admin password	Use <code>sudo agentctl reset-admin-pwd</code> to reset the admin UI password
VM is not reachable after IP configuration	Verify the VM's selected port group, the configured IP/CIDR, gateway, DNS, NIC connection, and VLAN. Rerun <code>sudo agentctl configure network</code> if the in-guest values need correction.
AITIN cloud tether key cannot be validated	Confirm that the pasted key is valid and unexpired, that the VM has approved egress TCP 443, and that AITIN Cloud tether is reachable.
Application domain is not reachable	Confirm that the FQDN was entered correctly, the DNS record points to the VM address, TCP 443 is allowed, and the services are healthy.
Application redirects to sign-in but users cannot access the tool	Confirm the authentication page loads, credentials are valid, and the user has the expected role and is enabled before investigating application services.
Supported switch does not appear in topology	Confirm compatibility, Cisco IOS XE, LLDP enablement, SSH reachability from the VM, and current inventory.
Syslog alerts do not appear	Confirm that switches forward syslog directly to the agent or through the configured syslog server.

Procedure

1. Run the command `sudo agentctl ps <service-name>` to check the health of a service.
2. Run the `sudo agentctl service <service-name> logs` command to inspect the logs of the affected service.

Example

```
sudo agentctl service nginx logs
sudo agentctl service authelia logs
```

3. Correct the underlying issue and then run the `sudo agentctl up` command.