Cisco ISE Cloud Central Agent Integration Guide

Cisco Identity Services Engine
Updated November 12, 2026

Topics included

1 Onboard and install Cisco ISE Cloud Central Agent....4
Cisco ISE Cloud Central Agent....5
Benefits of Cisco ISE integration with Cisco Cloud Control....5
Requirements for the Cisco ISE Cloud Central Agent....6
Certificate requirements for Cisco ISE nodes....9
Integrate an on-premises Cisco ISE deployment with Cisco Cloud Control....10
Install and configure the Cisco ISE Cloud Central Agent....11
Verify the Cisco ISE Cloud Central Agent connection....13
Cisco ISE Cloud Central Agent behavior after setup....13
Upgrade the Cisco ISE Cloud Central Agent....14
Known issues and limitations....15
Related documentation....16

2 Cisco ISE integration features in Cisco Cloud Control....18
Cisco ISE integration feature history....19
Cisco ISE Health Dashboard fields and charts....19
User inventory....21
Endpoint inventory....21

3 Troubleshooting Cisco ISE Cloud Central Agent Issues....24
Cisco ISE Cloud Central Common Setup Issues....25

1 Onboard and install Cisco ISE Cloud Central Agent

Topics:

- Cisco ISE Cloud Central Agent
- Benefits of Cisco ISE integration with Cisco Cloud Control
- Requirements for the Cisco ISE Cloud Central Agent
- Certificate requirements for Cisco ISE nodes
- Integrate an on-premises Cisco ISE deployment with Cisco Cloud Control
- Install and configure the Cisco ISE Cloud Central Agent
- Verify the Cisco ISE Cloud Central Agent connection
- Cisco ISE Cloud Central Agent behavior after setup
- Upgrade the Cisco ISE Cloud Central Agent
- Known issues and limitations
- Related documentation

Cisco ISE Cloud Central Agent

Describes how Cisco Cloud Control provides a centralized view of Cisco ISE deployment health, authentication performance, node utilization, connectivity, user identities, and endpoints. It explains how administrators use these views to monitor deployments and investigate identity and device issues.

Cisco Cloud Control provides a centralized view of connected Cisco ISE deployments, including deployment health, authentication performance, node utilization and connectivity, and user and endpoint inventories. The Cisco ISE Cloud Central Agent is installed on the Cisco ISE Policy Administration Node (PAN) and connects the on-premises deployment to Cisco Cloud Control. Use the ISE Health Dashboard to monitor deployment health, and use the user and endpoint inventories to view identity and device details.

You can use the **ISE Health Dashboard** to monitor the connected deployment and overall health. Then use the user and endpoint inventories to investigate identity and device details.

Monitor Cisco ISE deployments

The **ISE Health Dashboard** in Cisco Cloud Control (**Identity** > **ISE Monitoring** > **ISE Health Dashboard**) brings together agent status, deployment details, authentication and session activity, node status, and performance metrics. Use it to monitor authentication availability, identify performance degradation or unusual latency, review node connectivity, investigate issues before they affect your network, and speed root-cause analysis.

The dashboard includes Cisco ISE Cloud Central Agent information such as heartbeat, reachability, uptime, agent version, host, last collection time, and traffic. Deployment information includes the Cisco ISE release and patch version, deployment admin IP address, total node count, active sessions, and average authentication latency. The charts show authentication latency, active sessions, CPU and memory, server load, disk usage, RADIUS request volume, RADIUS authentication latency, and RADIUS authentication failures.

Review users and endpoints

The **Users** page in Cisco Cloud Control (**Identity** > **Users**) provides a centralized inventory of discovered identities that combines identity context, activity, posture, and TrustSec information. You can use it to monitor users, identify inactive or unprovisioned accounts, distinguish internal users, and find inconsistent identity data.

The **Endpoints** page in Cisco Cloud Control (**Identity** > **Endpoints**) provides a centralized inventory of discovered devices. You can search by serial number, hardware ID, or computer SID and use the inventory to identify unmanaged or unregistered devices, find endpoints with unknown operating systems, distinguish desktops, laptops, and mobile devices, and review manufacturing and hardware details.

You can also apply tags for ownership, encryption, or investigation status to identify newly discovered endpoints. This endpoint view brings together device identity, ownership posture, and authentication context to support device investigation and access policy decisions.

Benefits of Cisco ISE integration with Cisco Cloud Control

Explains the features available after Cisco ISE integration, including endpoint risk scores, automated response policies, additional Cisco ISE nodes, and diagnostic reports.

Cisco ISE integration with Cisco Cloud Control is a connection that sends identity and session data from a Cisco ISE deployment to Cisco Cloud Control for monitoring and diagnostics.

Features available after integration

After you connect Cisco ISE, you can use Cisco Cloud Control to:

- View endpoint risk scores based on endpoint behavior and identity context.

- Configure automated response policies to quarantine or alert on compromised endpoints. The agent carries out the configured action on Cisco ISE.
- Connect additional Cisco ISE nodes to the same tenant. Each node has its own Cisco ISE Cloud Central Agent and requires a separate tethering token.
- Review diagnostic information. The agent uploads a diagnostic report to Cisco Cloud Control daily, and Cisco Support can access the report.

For Cisco ISE integration Agent features introduced in each Cisco Cloud Control release, see Cisco ISE integration feature history on page 19

For deployment metrics, refer to Cisco ISE Health Dashboard fields and charts. For identity and endpoint inventories, refer to User inventory on page 21 and Endpoint inventory on page 21.

Requirements for the Cisco ISE Cloud Central Agent

Explains the requirements needed to successfully deploy the Cisco ISE Cloud Central Agent to integrate an on-premises Cisco ISE deployment to Cisco Cloud Control.

Refer to this topic to determine whether a Cisco ISE deployment and setup environment meet the requirements for Cisco Cloud Control integration using Cisco ISE Cloud Central Agent.

The table lists the requirements for installing and connecting the Agent successfully.

Table 1: Requirements for Cisco Cloud Control

Item	Description
Approved email address	Use the same email address for the Cisco products you plan to connect; ask each product administrator to grant access to that address if needed. For more information, see Getting Started Guide.
Access to ISE tenant	You have administrator access to the Cisco ISE tenant and any product tenants you want to connect. An administrator must be able to sign in to the product and accept the terms and conditions.
Region availabillity	Generally Available in the United States only. See Getting Started Guide

Table 2: Requirements for the Cisco ISE Cloud Central Agent

Item	Requirement
Cisco ISE Release	Use one of the following supported Cisco ISE releases and patches: Cisco ISE Releases 3.5 Patch 4, 3.4 Patch 7, and 3.3 Patch 12. Use a supported Cisco ISE server with a 64-bit x86 processor and application installation access. **Note** If you use Cisco ISE on AWS or Azure or OCI, apply Hotpatch of CSCwx12499 on top of Cisco ISE 3.3 Patch 12 before installing the Cisco ISE Cloud Central Agent. For patch details, refer to the Cisco ISE 3.3 software downloads.
Cisco ISE node and deployment type	Install the Cisco ISE Cloud Central Agent on the Primary Administration Node (PAN) of a supported Cisco ISE deployment.
Disk Space	Ensure that at least 4 GB of free disk space is available on your Cisco ISE appliance.
pxGrid	Enable pxGrid on the Cisco ISE node to receive real-time session updates. In Cisco ISE, choose **Administration** > **pxGrid Services**. Enable Allow password based account creation to create a pxGrid client.
ISE Administrator account	Use a Cisco ISE administrator account with either the Super Admin role or both the ERS Admin and MnT Admin roles to tether the Cisco ISE Cloud Central Agent. The installer prompts you for these credentials during setup.
ISE API settings	Before installing the agent, enable ERS API and OpenAPI at in Cisco ISE (in the Cisco ISE GUI, go to **Administration** > **System** > **Settings** > **API Settings**). The agent uses these APIs to access Cisco ISE configuration and operational data.
Cisco ISE Admin and pxGrid certificates	Use a valid Cisco ISE Admin certificate. As an administrator, your browser must trust the certificate's issuing chain. Use a complete public or enterprise trust chain and an FQDN present in the certificate SAN. For each Cisco ISE node that the agent connects to, use valid Admin and pxGrid certificates whose SAN includes the node's FQDN as a DNS name. If a certificate is CA-signed, add its issuing CA certificates to the Cisco ISE Trusted Certificates store. For the Admin certificate, your browser must trust a complete public or enterprise issuing chain.

Item	Requirement
Cisco ISE Cloud Central Agent installation package	1. Download the latest Cisco ISE Cloud Central Agent installation package (`.tar.gz`) from Cisco Cloud Control. 2. Keep the package's original filename. 3. Create a Cisco ISE repository on the PAN and copy the package to the repository. 4. Note the repository name. You'll need it during installation. **Note** For more information on creating repository, refer to Configure Repository on ISE.
Cisco ISE tethering token	Copy the Cisco ISE tethering token from Cisco Cloud Control. In the **New Cisco Identity Services Engine (ISE) Integration** page on Cisco Cloud Control, select **Copy Tethering Token**.
Internet access	Allow required outbound cloud connectivity. Configure an outbound proxy when needed; Cisco ISE is normally reached directly. The agent supports a proxy when direct internet access is unavailable.
CLI access	Ensure Cisco ISE CLI access over SSH.

Outbound connectivity requirements for the Cisco ISE Cloud Central Agent

The Cisco ISE Cloud Central Agent requires outbound TCP port 443 access to the following production destinations. An HTTPS proxy using CONNECT is supported for all three destinations.

Destination	Purpose
`ise-bootstrap.prod-us.cii.identityfabric.security.cisco.com`	Bootstrap during installation
`<prefix>-ats.iot.us-east-2.amazonaws.com`	AWS IoT Core connection using MQTT over TLS on port 443. Replace `<prefix>` with the provisioned hostname prefix.
`cnt-fabric-prod-us-data.s3.us-east-2.amazonaws.com`	Amazon S3 uploads, including large data batches and diagnostic logs

Exclude all three destinations from TLS inspection or SSL decryption. The AWS IoT Core connection uses client-certificate authentication and Amazon's root CA; TLS inspection can break the connection.

Note

- Use the provisioned `<prefix>-ats.iot.us-east-2.amazonaws.com` hostname for AWS IoT Core. The pattern `*.ats.iot.us-east-2.amazonaws.com` does not match this hostname because `-ats` is part of the first label.

  Large batches of 512 KiB or more, batches of 1,000 items or more, and diagnostic log uploads go directly to pre-signed Amazon S3 URLs. S3 access is required for these uploads.
- For production, use `ise-bootstrap.prod-us.cii.identityfabric.security.cisco.com`. The `ise-bootstrap.staging.cii.identityfabric.security.cisco.com` hostname is for staging. Do not use the broader `*.cii.identityfabric.security.cisco.com` wildcard when the exact production bootstrap hostname is sufficient.

Certificate requirements for Cisco ISE nodes

Lists the certificate and SAN requirements for Cisco ISE nodes in order to ensure secure and successful integration with the Cisco ISE Cloud Central Agent.

The Cisco ISE Cloud Central Agent verifies the identity of each Cisco ISE node it connects to, including over pxGrid. The node's Admin and pxGrid certificates must meet these requirements:

- The Subject Alternative Name (SAN) must include the node's fully qualified domain name (FQDN) as a DNS name, such as `DNS:ise1.example.com`.
- The SAN can also include the node's IP address.
- The certificate must be within its validity period.
- If the certificate is CA-signed, the issuing CA certificates must be in the Cisco ISE Trusted Certificates store.

Cisco ISE-generated certificates, including the default self-signed certificate and pxGrid certificates issued by the Cisco ISE internal CA, meet these requirements. If you use a certificate signed by an external CA, make sure the SAN includes the node's FQDN as a DNS name.

The agent does not support certificates that identify the node only by its Common Name (CN) or IP address.

If a certificate is unsupported, installation does not complete. Reissue it with the node's FQDN as a DNS name in the SAN, then run the installation again.

Table 3: Certificate requirements for Cisco ISE nodes

Certificate identity	Supported
SAN includes `DNS:ise1.example.com`	Yes
SAN includes `DNS:ise1.example.com` and `IP:192.0.2.10`	Yes
CN is `ise1.example.com`; SAN includes only `IP:192.0.2.10`	No
CN is `ise1.example.com`; certificate has no SAN	No

Certificate identity	Supported
SAN includes a DNS name that does not match the node's FQDN	No

Why the agent checks the certificate?

The agent sends Cisco ISE administrator credentials and receives session and endpoint data. It checks the DNS name in the SAN to verify the identity of the Cisco ISE node before exchanging this information. RFC 9525 specifies that clients identify DNS names using the `dNSName` SAN and must not use the CN for this purpose.

Check the certificate SAN

Run this command from a host that can reach the Cisco ISE node:

```
openssl s_client -connect <ISE-node-FQDN>:8910 </dev/null 2>/dev/null | openssl
 x509 -noout -ext subjectAltName
```

The output must include `DNS:<ISE-node-FQDN>`. To inspect the Admin certificate, use port `443` instead of `8910`. This command displays the SAN; it does not confirm certificate validity or CA-chain trust.

Integrate an on-premises Cisco ISE deployment with Cisco Cloud Control

Provides step-by-step instructions on how to integrate on-premises Cisco ISE deployment to Cisco Cloud Control.

Use this procedure to create the Cisco ISE integration, download the Cisco ISE Cloud Central Agent package, and complete Cisco ISE Cloud Central Agent setup.

Before you begin

Ensure that you have configured a supported Cisco ISE deployment and can access its Admin portal. During installation, the Cisco ISE Cloud Central Agent enables pxGrid if needed. If setup creates a new pxGrid client, approve it in Cisco ISE at **Administration** > **pxGrid Services** Services. Installation pauses until you approve the client.

For release-specific configuration instructions, see the Cisco ISE Administrator Guide for your release.

Procedure

1. Log in to Cisco Cloud Control and choose your tenant with necessary Cisco ISE entitlements.
   Authenticate to log in to your tenant. For information on new product or tenant setup, refer to Cisco Cloud Control.
2. Click **Identity** and choose **Integrations**. Click **+ Add Integration**.

   Cisco Cloud Control displays the available integration providers.
3. In the **Cisco Identity Services Engine (ISE)** tile, click **+ Add Integration**.

   The **New Cisco Identity Services Engine (ISE) Integration** page appears.
4. Enter a name and an optional description for the Cisco ISE integration, and click **Generate tethering token**. Ensure that you have the prerequisites ready before generating the token.

   The page displays setup instructions to integrate your on-premises Cisco ISE deployment with Cisco Cloud Control.
5. Click **Copy tethering token**.

> **Note**
>
> The tethering token is valid for 24 hours and can be used only once. Copy it before leaving this page. If it expires or you leave the page without copying it, open the integration's edit page and reset the agent credentials to generate a new token.TThe tethering token

6. Click **Download agent bundle** to download the Cisco ISE Cloud Central Agent package from Cisco Cloud Control.
7. Install and configure the Cisco ISE Cloud Central Agent using the step-by-step instructions provided in Install and configure the Cisco ISE Cloud Central Agent.
8. After the Cisco ISE Cloud Central Agent is installed successfully and the agent configuration status is displayed as **Running**, return to the **New Cisco Identity Services Engine (ISE) Integration** page in Cisco Cloud Control and click **Finish setup**.

   Click **Yes, finish setup** in the displayed popup.

Your on-premises Cisco ISE deployment is integrated with Cisco Cloud Control through the Cisco ISE Cloud Central Agent.

What to do next

Verify the connection. Refer to Verify the Cisco ISE Cloud Central Agent connection.

Install and configure the Cisco ISE Cloud Central Agent

Provides step-by-step instructions on how to install and configure the Cisco ISE Cloud Central Agent and start cloud tethering.

Use this procedure to install the Cisco ISE Cloud Central Agent on the PAN and start cloud tethering.

Follow these steps to install and configure the Cisco ISE Cloud Central Agent in the Cisco ISE CLI after you create the integration, download the Cisco ISE Cloud Central Agent installation package, and copy the tethering token.

Before you begin

Complete steps 1 through 6 in Integrate an on-premises Cisco ISE deployment with Cisco ISE Cloud Central to create the integration, download the Cisco ISE Cloud Central Agent installation package, and copy the tethering token. Step 7 in that procedure directs you to this task.

Before you start this procedure, confirm that all the prerequisites are complete.

Procedure

---

1. Log in to the Cisco ISE CLI over SSH on the PAN.
2. From the Cisco ISE CLI, run this command to install the Cisco ISE Cloud Central Agent: **application install ISE-CLOUD-CENTRAL-AGENT-bundle-spa-<version>.tar.gz**. The file name is auto-updated.

   The standard Cisco application installation process checks that your Cisco ISE appliance meets the requirements and starts the agent's initial setup service.

   The Cisco ISE Cloud Central Agent installer installs the agent in four simple steps. It hides the secrets you enter in the Cisco ISE CLI and does not store them.

3. When prompted during installation, enter these details in the Cisco ISE CLI:

a. **Connect to Cisco Cloud Control**: Enter the Cisco ISE tethering token copied from Cisco Cloud Control. If Cisco ISE uses a proxy to reach the internet, enter an HTTPS proxy in host:port format.

   If the tethering token is rejected, it may have expired or already been used.

   Open the integration's edit page and reset the agent credentials to generate a new token. Enter the replacement token at the CLI prompt. You do not need to reinstall the agent.

b. **Configure the ISE connection and pxGrid client**: The Cisco ISE node details are populated by default.

   You must enter the Cisco ISE administrator username and password.

   You can create a pxGrid client, or use an existing registered and approved pxGrid client.

   When creating a new pxGrid client, if one with that name already exists, use a different name.

   The Cisco ISE Cloud Central Agent installer enables pxGrid if needed, which can restart Cisco ISE application services.

c. **Start the ISE Cloud Central Agent**: The installer uses the provided details to install the Cisco ISE Cloud Central Agent.

d. **Check the pxGrid connection**: Validate that the pxGrid client is active.

   It might take upto 90 seconds for a new client to become active. You must approve any new pxGrid clients in Cisco ISE (choose **Administration** > **pxGrid Services** and approve the new pxGrid client).

   > **Attention**
   >
   > The Cisco ISE Cloud Central Agent installation remains halted until any new pxGrid client is approved in Cisco ISE.

After successful installation, **Setup complete** is displayed in the Cisco ISE CLI.

The **ISE Cloud Central Agent** GUI link is also displayed in the Cisco ISE CLI. This GUI link can be used to monitor or change the settings of the tethered Cisco ISE Cloud Central Agent.

4. In a browser that can reach the Cisco ISE Admin IP address, open: `https://<ISE-IP>/ise-cloud-central-agent/setup/`.

   The **ISE Cloud Central Agent** setup page opens. You can use this page to update or modify the settings of the currently tethered Cisco ISE Cloud Central Agent.

5. In the **Verify ISE credentials** page:

   a. Enter your Cisco ISE administrator username and password.

   b. Select **Verify ISE credentials**.

6. After your Cisco ISE node is successfully verified, you can use the **Agent configuration** page to modify the proxy host and pxGrid client details of your tethered Cisco ISE Cloud Central Agent.

   a. If Cisco ISE uses a proxy to reach the internet, enter an HTTPS proxy in `host:port` format in **Proxy host** and **Proxy port**. The default port is 80. Leave the proxy host blank for a direct connection.

   b. To continue using the same pxGrid client, do not modify the name in **pxGrid client name**.

      To create a new pxGrid client, enter a different name in **pxGrid client name**. When creating a new pxGrid client, if one with that name already exists, you must use a different name.

7. Click **Apply configuration** to save and apply any changes.

The **Agent status** section displays the agent name, IP address, agent status, uptime, connected Cisco ISE IP address, and pxGrid client name.

The **Configuration progress** section displays the current status and activity logs of the agent configuration.

What to do next

Return to the **New Cisco Identity Services Engine (ISE) Integration** page in Cisco Cloud Control and complete the final step in Integrate an on-premises Cisco ISE deployment with Cisco ISE Cloud Central.

Then verify the connection by referring to Verify the Cisco ISE Cloud Central Agent connection.

Verify the Cisco ISE Cloud Central Agent connection

Provides step-by-step instructions to confirm the Agent status on its setup page and in Cisco Cloud Control. It identifies the status details that indicate a completed connection.

Before you begin

Install and configure the Cisco ISE Cloud Central Agent.

Procedure

1. Check the Cisco ISE Cloud Central Agent status on the **ISE Cloud Central Agent** setup page.

   Under **Agent status**, confirm that the table shows the agent name, IP address, status of `Running`, uptime, connected Cisco ISE IP address, and pxGrid client name.

   If you encounter any issues, refer to Cisco ISE Cloud Central Common Setup Issues on page 25 for troubleshooting information.

2. Check the integration status in Cisco Cloud Control.

   In Cisco Cloud Control, choose **Identity** > **Integrations**.

   Confirm that the connected Cisco ISE node has a green **Active** status.

The Cisco ISE deployment is connected successfully when the **ISE Cloud Central Agent** setup page reports `Running` and Cisco Cloud Control (**Identity** > **Integrations**) reports `Active`.

What to do next

If the status of the Cisco ISE Cloud Central Agent is shown as `Not found` or `Disconnected`, refer to Cisco ISE Cloud Central Agent connection problems to troubleshoot common issues.

Cisco ISE Cloud Central Agent behavior after setup

Lists the expected Cisco ISE Cloud Central Agent activity after setup, including initial connection, data synchronization, session updates, health signals, and software update checks.

Refer to this topic to understand when the Agent connects, synchronizes data, reports health, and checks for software updates.

Initial and incremental identity-object synchronization

After a fresh installation, the Cisco ISE Cloud Central Agent performs a one-time inventory and uploads identity objects to the Cisco Cloud Control dashboard. The time required for user and endpoint objects to appear depends on factors such as traffic in the Cisco ISE deployment, database size, and latency between Cisco ISE and Cisco Cloud Control.

The Cisco ISE Cloud Central Agent's CPU, memory, and disk limits are tuned internally based on the size of the PAN node and the deployment type. For Cisco ISE deployment sizing information, see the Cisco ISE Performance and Scalability Guide.

Sample time for user and endpoint objects to appear after fresh installation

Table 4: Sample time for user and endpoint objects to appear after fresh installation

Cisco ISE database contents	Approximate time
150,000 endpoints (active and inactive)	60 minutes
1 million endpoints (active and inactive)	4 hours
4 million endpoints (active and inactive)	12 hours
25,000 internal users	60 minutes

These are approximate times based on sample test data. Actual times vary by deployment. After the initial upload, the agent runs periodic discovery checks every 15 minutes to find and update incremental objects.

Upgrade the Cisco ISE Cloud Central Agent

Provides step-by-step instructions to upgrade the Cisco ISE Cloud Central Agent infrastructure and bundled Agent by installing a new signed application bundle through the Cisco ISE CLI.

Use this procedure to upgrade the Cisco ISE Cloud Central Agent from the Cisco ISE CLI.

By default, Cisco ISE uses the signed image included in the installed application bundle. The default installation does not use manifest-based image updates.

Manifest-based image updates are optional. They require a configured update manifest and public key.

Before you begin

- Obtain the signed Cisco ISE Cloud Central Agent bundle for the target version.
- Copy the bundle to a Cisco ISE repository that the PAN can access. Keep the bundle's original filename.
- Note the repository name.

Procedure

1. Log in to the Cisco ISE CLI over SSH on the PAN.
2. Run the upgrade command, specifying the bundle filename and repository name.

```
application upgrade <bundle-filename> <repository-name>
```

For example,

```
application upgrade ISE-CLOUD-CENTRAL-AGENT-bundle-spa-1.0.150.tar.gz nas
```

Use the filename for the bundle you are upgrading to and the name of the repository that contains it.

3. Wait for the CLI upgrade to finish.
4. Verify the agent on the Cisco ISE Cloud Central Agent setup page. Confirm that the agent status is **Running**.
5. In Cisco Cloud Control, choose **Identity** > **Integrations**. Confirm that the Cisco ISE integration is **Active**.

The Cisco ISE Cloud Central Agent and its infrastructure are upgraded.

Verify that the Cisco ISE Cloud Central Agent is running the target agent version. This procedure upgrades the agent only; it does not upgrade Cisco ISE software.

Note

You can integrate a Cisco ISE deployment running an earlier patch level. Cisco recommends upgrading Cisco ISE to a recommended patch level before installing the Cisco ISE Cloud Central Agent. If the agent is already installed when you upgrade Cisco ISE, you might need to uninstall the agent before the ISE upgrade, then reinstall the agent and establish the Cisco Cloud Control connection again.

Known issues and limitations

Lists the known limitations of the Cisco ISE Cloud Central Agent to help understand any functionality constraints.

Refer to this topic to understand the limitationsns in the Cisco ISE Cloud Central Agent .

Table 5: Known Issues

Issue	Condition	Recommended action
The agent cannot connect after a pxGrid certificate expires.	The pxGrid certificate on the ISE deployment is expired.	Replace the expired certificate in Cisco ISE, then check the agent connection again.
The agent is disconnected after a PAN or MnT failover.	The agent status is Not found or Disconnected after a failover.	Reinstall the Cisco ISE Cloud Central Agent using the supported installation procedure.
The deployment has multiple agent installations.	An agent was installed on more than one ISE node in the same deployment.	Install the agent on the Primary PAN (PPAN) only.
The Users page may not show endpoint updates in real time.	An endpoint receives an update, but the change has not appeared in Cisco Cloud Control.	Check again later; if the information remains stale, contact Cisco Support.
Deleted endpoints may still appear in Cisco Cloud Control.	Endpoints have been purged from Cisco ISE but remain visible in Cisco Cloud Control.	Contact Cisco Support if the records remain visible.
The agent connection is unavailable after the agent stops unexpectedly.	The agent process has stopped and has not restarted automatically.	stopped and has not restarted automatically.Restart the agent using the supported Cisco ISE procedure

Issue	Condition	Recommended action
A certificate issue may prevent integration.	The Cisco ISE system certificate or pxGrid certificate is invalid, expired, or otherwise unsuitable.	Check certificate status in Cisco ISE and replace any expired or invalid certificate.
The agent connection may be lost after an ISE upgrade.	After a Cisco ISE upgrade, the agent status is not found or disconnected.	Reinstall the agent using the supported installation procedure.

Related documentation

Lists the key documentation resources for Cisco Cloud Control onboarding, Cisco ISE configuration, API guides, and release information.

Use these resources for Cisco Cloud Control onboarding and for Cisco ISE configuration, APIs, and release information.

- Cisco Cloud Control Getting Started: Learn about Cisco Cloud Control access, product tenants, and creating an environment.
- Cisco Identity in Cisco Cloud Control: Identity service setup, integration prerequisites, roles, and Cisco ISE data in Cisco Cloud Control.
- Cisco ISE documentation by release: Select the deployed Cisco ISE release to find its Administrator, CLI, installation, and upgrade guides.
- Cisco ISE API documentation: Find details about ERS and Open APIs used with Cisco ISE.
- Cisco ISE release notes: Check release changes and known issues for the deployed Cisco ISE version.

2 Cisco ISE integration features in Cisco Cloud Control

Topics:

- Cisco ISE integration feature history
- Cisco ISE Health Dashboard fields and charts
- User inventory
- Endpoint inventory

Cisco ISE integration feature history

Lists the Cisco ISE integration capabilities including feature descriptions, availability, and references to related topics.

The table summarizes Cisco ISE integration Agent features introduced in each Cisco Cloud Control release, describing the functionality provided, availability, limitations, and links to related topics.

Table 6: Cisco ISE integration feature history

Agent version	Capability	What it provides
1.0.171	Agent setup and lifecycle	Connect an on-premises Cisco ISE deployment to Cisco Cloud Control using the Cisco ISE Cloud Central Agent. Install and configure the agent, upgrade it from the Cisco ISE CLI, verify the connection, and troubleshoot common setup issues.
	Deployment health and monitoring	View agent and deployment status, node information, authentication and session activity, resource utilization, and RADIUS metrics in the ISE Health Dashboard.
	User inventory	Review discovered identities and user context, including activity, posture, and TrustSec information.
	Endpoint inventory	Review discovered devices, including identity, hardware, operating system, management and registration status, ownership, and tags.
	Endpoint risk and response	View endpoint risk scores and configure automated quarantine or alert policies in Cisco Cloud Control.
	Diagnostic reports	The agent uploads a diagnostic report daily. Cisco Support can access the report.

Cisco ISE Health Dashboard fields and charts

Describes the agent status, deployment information, node details, and charts in the Cisco ISE Health Dashboard. Use these details to monitor Cisco ISE connectivity, authentication performance, session activity, and node utilization.

Refer to this topic to interpret the agent, deployment, node, and chart information in the Cisco ISE Health Dashboard.

ISE Health Dashboard overview

In Cisco Cloud Control, choose **Identity** > **ISE Monitoring** > **ISE Health Dashboard** to view Cisco ISE deployment details for your tenant.

You can use **Connect another deployment** to add a new Cisco ISE deployment. You can refresh the dashboard to synchronize status and use the dashboard settings to configure and optimize the dashboard.

ISE Agent

The **ISE Agent** area reports the connection and collection status of the agent associated with the Cisco ISE deployment.

Table 7: ISE Agent fields

Field	Description
ISE heartbeat	Reports whether the agent sends its heartbeat every 60 seconds.
ISE reachable	Reports whether the agent is connected to Cisco ISE.
Uptime	Reports how long Cisco ISE Cloud Central has been integrated with Cisco ISE.
Agent version	Reports the Cisco ISE Cloud Central Agent version.
Host	Reports the hostname of the Cisco ISE deployment.
Last collected	Reports when information was last collected.
Traffic	Displays current network traffic.

Deployment

The **Deployment** area summarizes the Cisco ISE release, deployment size, session count, and authentication latency.

Table 8: Deployment fields

Field	Description
ISE version	Shows the Cisco ISE release and patch details.
Deployment Admin IP	Shows the deployment admin IP address.
Total nodes	Shows the number of nodes in the Cisco ISE deployment.
Sessions	Shows the number of active sessions.
Avg Auth Latency	Shows the average authentication latency in the deployment.

Charts

The charts provide information about authentication performance, session activity, resource utilization, and RADIUS traffic.

Table 9: Dashboard charts

Chart	Information shown
Authentication latency chart	Compares average and maximum latency for the last 24 hours. Use it to identify performance degradation or unusual latency spikes.
Active sessions chart	Shows real-time session growth and stabilization.

Chart	Information shown
CPU & Memory	Shows CPU and memory information for monitoring node utilization.
Avg Server Load	Shows average server load.
Disk Usage	Shows disk usage.
RADIUS Request Volume	Shows the volume of RADIUS requests.
RADIUS Avg Auth Latency	Shows average RADIUS authentication latency.
RADIUS Auth Failure Rate	Shows the RADIUS authentication failure rate for the last 24 hours.

The Cisco ISE Health Dashboard serves as a proactive monitoring tool. Use it to review deployment issues before they affect the network, investigate root causes, and monitor authentication availability.

Node table

The node table provides visibility into the status and performance of individual Cisco ISE nodes. It shows:

- The role of each node, such as administration, policy service, or monitoring.
- The services used by each node, such as session, Profiler, and pxGrid.
- The system performance, RADIUS authentication status, and connectivity status of each node.

User inventory

Outlines the identity inventory and user fields available in Cisco Cloud Control for monitoring accounts, checking identity data, and identifying inactive or unprovisioned users.

Refer to this topic to understand the identities and account details shown on the **Users** page in Cisco Cloud Control.

Users page

The **Users** page (**Identity** > **Users**) in Cisco Cloud Control provides an inventory of discovered identities. It combines identity context, activity, posture, and TrustSec information.

You can use the **Users** page to monitor users, identify inactive or unprovisioned accounts, distinguish internal users, and identify inconsistent identity data.

The user inventory includes these fields for easy access and identification of users: **User**, **Checks**, **# IPs** (number of IP addresses), **# Logins**, **Last Seen (UTC)**, **Last IP Address**, **Last Location**, **MFA**, **Sources**, **Status**, **Tags**, and **Compiled Status**.

Endpoint inventory

Outlines the endpoint inventory, search keys, and displayed device details available in Cisco Cloud Control to help administrators review discovered endpoints.

Refer to this topic to understand how the **Endpoints** page presents devices discovered in a Cisco ISE deployment.

Endpoints page

The **Endpoints** page (**Identity** > **Endpoints**) in Cisco Cloud Control provides an inventory of discovered devices and endpoints. Search for a device by its serial number, hardware ID, or computer SID.

You can use the **Endpoints** page to identify unmanaged or unregistered devices and endpoints with unknown operating systems. You can distinguish desktops, laptops, and mobile devices, and review manufacturing and hardware details.

You can also apply tags for ownership, encryption, or investigation status to identify a newly discovered endpoint. The **Endpoints** page connects device identity, ownership posture, and authentication context for device investigation and access policy decisions.

The endpoint inventory includes these fields for easy access and identification of endpoints: **Name**, **Type**, **Sources**, **Managed**, **Registered**, **OS**, **Tags**, **Assigned**, **Used By**, and **Last Seen (UTC)**.

3 Troubleshooting Cisco ISE Cloud Central Agent Issues

Topics:

- Cisco ISE Cloud Central Common Setup Issues

Explains key attributes, causes, and examples related to Cisco ISE Cloud central agent issues.

Cisco ISE Cloud Central Common Setup Issues

Lists common issues of the Cisco ISE Cloud Central Agent and troubleshooting tips.

The Cisco ISE Cloud Central Agent setup page displays the recent operation output after you initiate cloud tethering for easy reference and troubleshooting.

Use this table to identify and troubleshoot common issues of the Cisco ISE Cloud Central Agent.

Table 10: Common setup issues and actions

Issue	Condition	Recommended action
The installation bundle or repository cannot be found.	Installation fails with a message that the bundle or repository is missing.	Confirm that the repository name is correct and that the bundle is in that repository under its original filename. Run the installation command again.
The Cisco ISE release or available disk space is unsupported.	Installation fails because the ISE release is unsupported or the appliance does not have enough free space.	Confirm that your Cisco ISE release and patch meet requiremens and that at least 4 GB of free space is available on the node.
The tethering token is rejected.	The token has expired or was previously used.	The token might have expired or already been used. In Cisco Cloud Control, open the integration's edit page and reset the agent credentials. Enter the replacement token at the CLI prompt. You do not need to reinstall the agent.
Cisco ISE cannot reach Cisco Cloud Control.	The agent cannot connect or the integration does not become active.	Confirm that outbound HTTPS traffic from Cisco ISE to Cisco Cloud Control is allowed. For the required destination IP addresses, refer to Outbound connectivity requirements. These addresses apply to Cisco ISE Cloud Central Agent connectivity.
Cisco ISE sign-in fails during setup.	The installer rejects the administrator credentials.	Use a Cisco ISE account with the Super Admin role and check the password. The installer prompts you to sign in again.
The pxGrid client does not become active.	Setup is waiting for a new pxGrid client to become active.	In Cisco ISE, approve the pxGrid client by choosing **Administration** > **pxGrid Services** > **Client Management**. You can also change settings in the Cisco ISE Cloud Central Agent GUI at `https://<ISE node>/ise-cloud-central-agent/setup/`. If your browser displays a certificate warning, do not continue. Install the Cisco ISE Admin certificate first.
The agent is already installed on this node.	Installation reports that the agent is already installed.	Do not reinstall until the correct procedure is confirmed.
Setup was interrupted or Finish setup was selected too early.	You left the page or selected **Finish setup** too early.	In Cisco Cloud Control, open the Cisco ISE integration from **Integrations** in Cisco Cloud Control and select **Resume setup**. Generate a new token if the existing token has expired or was already used..

Issue	Condition	Recommended action
The agent cannot connect after a pxGrid certificate expires.	The pxGrid certificate on the ISE deployment is expired.	Replace the expired pxGrid certificate in Cisco ISE, then check the agent connection. For certificate requirements, refer to Certificate requirements for Cisco ISE nodes.
The agent is disconnected after a PAN or MnT failover.	The agent status is Not found or Disconnected after a failover.	Reinstall the Cisco ISE Cloud Central Agent using the supported installation procedure.
The deployment has multiple agent installations.	An agent was installed on more than one ISE node in the same deployment.	Install the agent on the Primary PAN (PPAN) only.
The Users page may not show endpoint updates in real time.	An endpoint receives an update, but the change has not appeared in Cisco Cloud Control.	Check again later; if the information remains stale, contact Cisco Support.
Deleted endpoints may still appear in Cisco Cloud Control.	Endpoints have been purged from Cisco ISE but remain visible in Cisco Cloud Control.	Contact Cisco Support if the records remain visible.
The agent connection is unavailable after the agent stops unexpectedly.	The agent process has stopped and has not restarted automatically.	stopped and has not restarted automatically.Restart the agent using the supported Cisco ISE procedure
A certificate issue may prevent integration.	The Cisco ISE system certificate or pxGrid certificate is invalid, expired, or otherwise unsuitable.	Check the Cisco ISE system and pxGrid certificates. Replace any expired or invalid certificate. For certificate requirements, refer to Certificate requirements for Cisco ISE nodes
The agent connection may be lost after an ISE upgrade.	Cisco ISE is upgraded from 3.3 Patch 12 to 3.5 Patch 5, or from 3.4 Patch 7 to 3.5 Patch 4 and the agent no longer connects.	Reinstall the agent using the supported installation procedure.

Contact Support

If the issue persists, open a Cisco Support case.

Include the following information:

- Cisco ISE release and patch
- Cisco ISE Cloud Central Agent version
- The time the issue occurred
- The agent and integration status shown in the setup page and Cisco Cloud Control
- The agent logs from [location] and the Cisco ISE logs from [location]