

Configure Remote Support Authorization in ISE 3.4

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[RADKit Service Setup](#)

[Configure a Remote Support Authorization](#)

[Verify](#)

[Troubleshoot](#)

[Related Information](#)

Introduction

This document describes how to configure Remote Support Authorization on Cisco Identity Services Engine (ISE) 3.4 to permit access from Cisco Agents.

Prerequisites

Requirements

Cisco recommends that you have basic knowledge of Cisco ISE®.

To setup the RADKit Service, the ISE Primary Administration Node must have HTTPS connectivity to prod.radkit-cloud.cisco.com either directly or through a configured proxy. Additionally, a valid CCO account is required.

Components Used

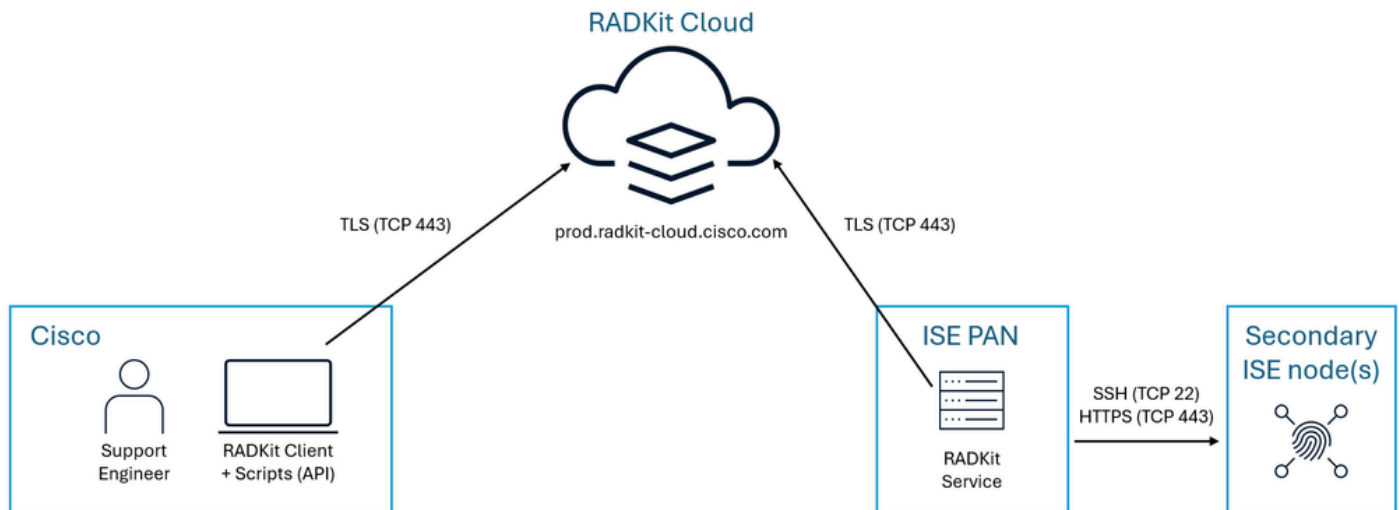
The information in this document is based on these software and hardware versions:

- Cisco ISE version 3.4 patch 2

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configure

The Remote Support Authorization feature leverages Cisco RADKit to provide Cisco Specialists with secure, audited, remote access to select ISE nodes in your environment to streamline troubleshooting.



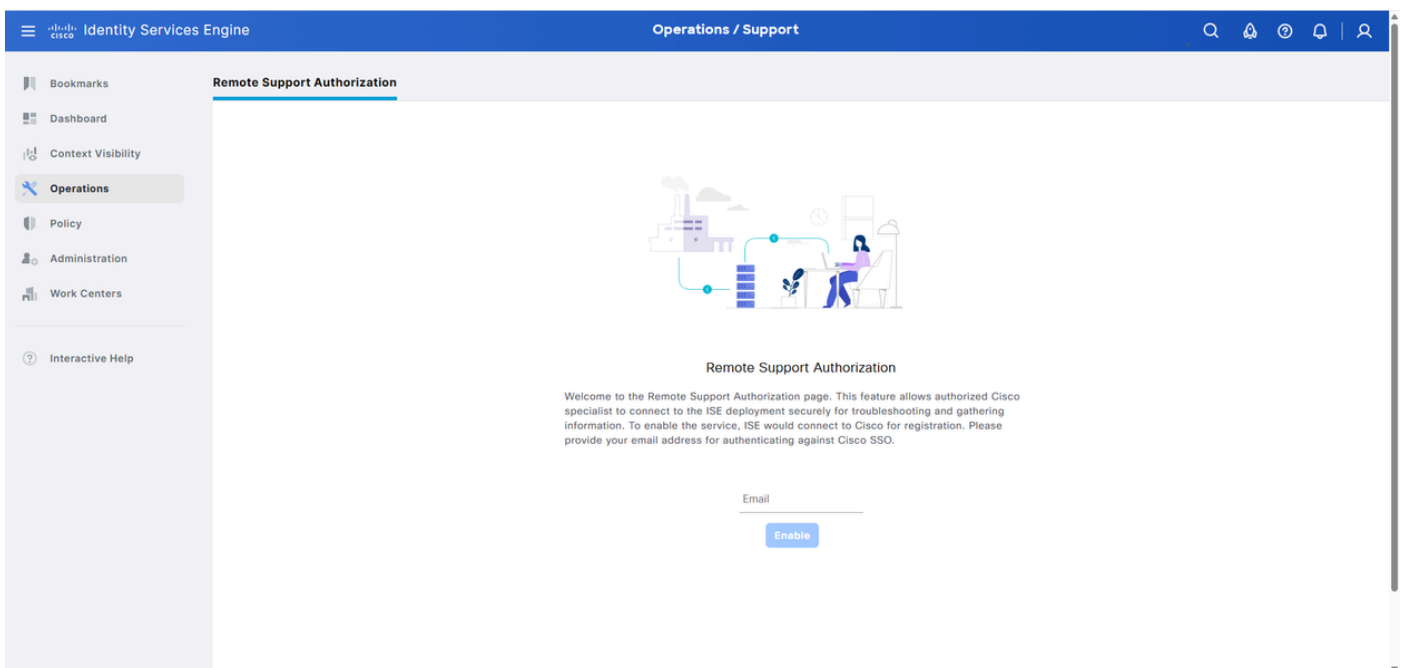
RADKit ISE Architecture Overview

RADKit is CSDL approved. CSDL is a Cisco process that reviews software for security risks, data privacy and third-party licensing compliance. RADKit underwent stringent security review: code quality and dependencies are analyzed throughout the development process; our services are constantly monitored. All data at rest or in transit is protected by industry standard algorithms (AES, RSA, SHA-2, ECDH...) and protocols (2-way authenticated TLS1.3, SSH) with industry-recommended parameters.

RADKit only facilitates data transfer but nothing is collected nor stored by RADKit in the RADKit Cloud. It is just an efficient way for you to collect data and a more secure way to exchange data with your support engineer than sending emails or manually uploading to an SR. The only exception to this rule is the audit trail that we generate for your security, that is owned by you and that never leaves your system.

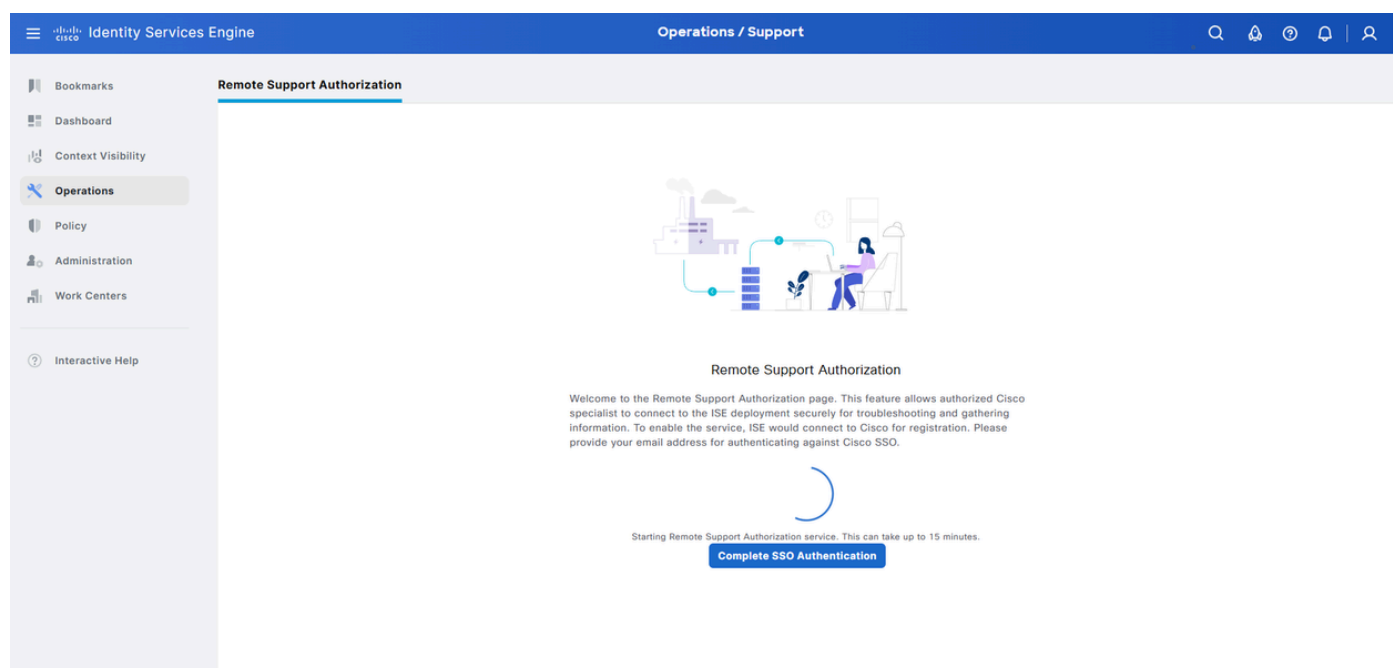
RADKit Service Setup

Navigate to **Operations > Support > Remote Support Authorization**. Enter your Cisco SSO associated email address for authentication.



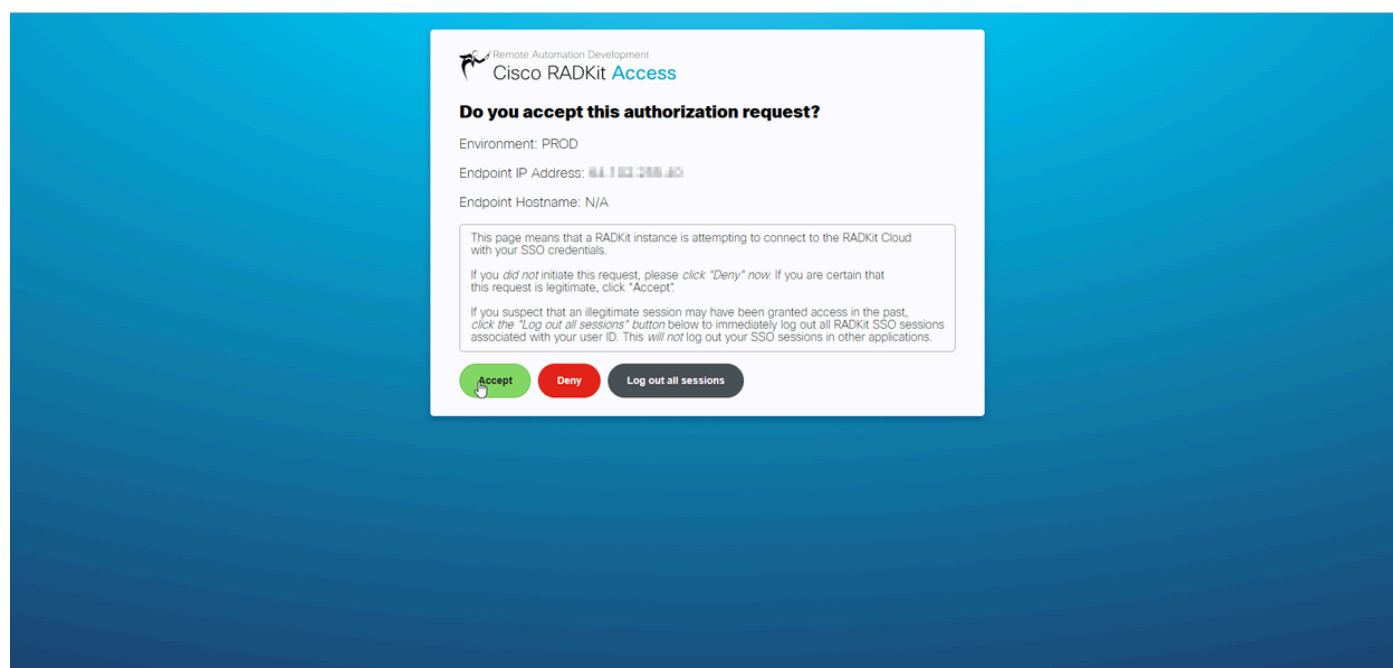
Initial Remote Support Authorization page where Email entry required

After the Remote Support Authorization service starts, click **Complete SSO Authentication**.



After entering Email, button appears to Complete SSO Authentication

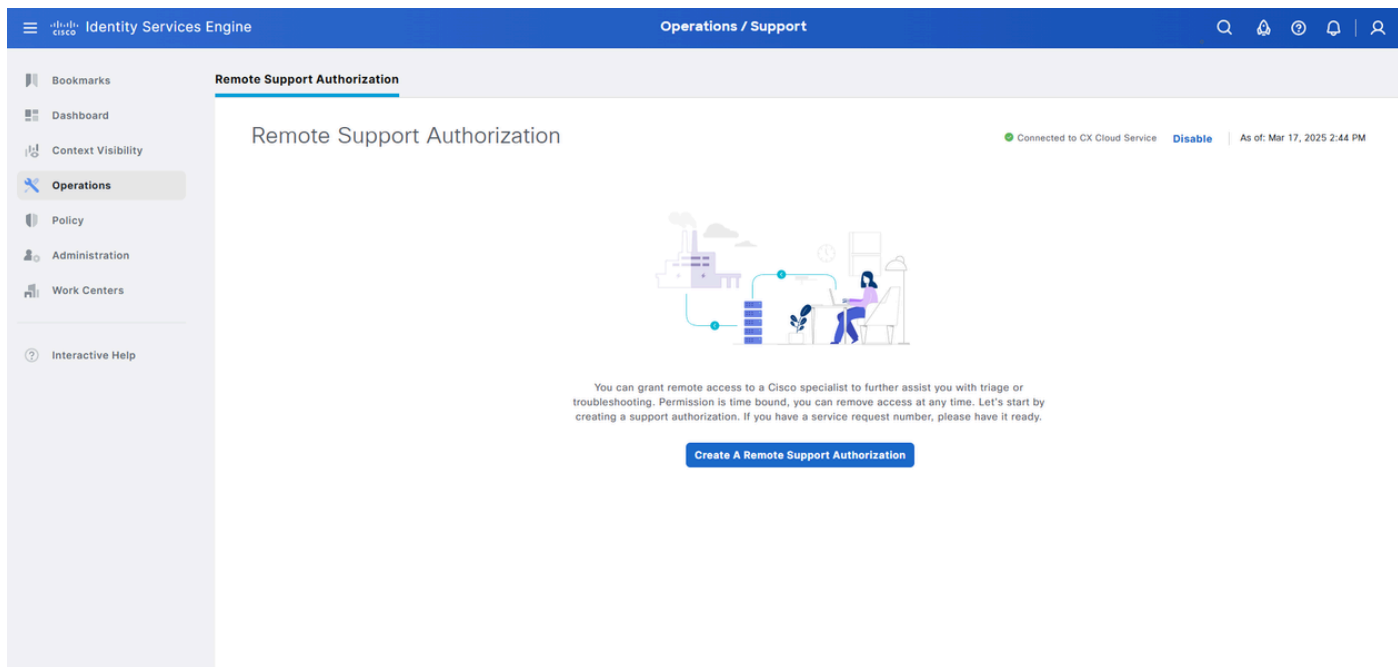
Click **Accept** on the newly opened window to complete the authorization to the Cisco RADkit Cloud.



SSO Authentication Page where Authorization completed

Configure a Remote Support Authorization

Click **Create A Remote Support Authorization** to configure a remote access session.



After authentication, option to Create Remote Support Authorization appears

Enter the email address of the Cisco Specialist that you want to provide access to. Select **Observer (Read-Only)** to provide read-only access to the Cisco Specialist, or **Admin (Read-Write)** to provide full read-write access to the Cisco Specialist. If this access is related to an existing TAC Service Request, you can enter the SR number as well as any other justification for the remote access. Click **Next** after entering the required information.

 **Note:** Providing the SR numbers allows TAC to upload the collected logs automatically without any intervention. As well, this helps documenting the remote connection and commands in the SR.

First page of Authorization creation

Schedule the duration and timing for the remote authorization. To schedule the access immediately, select **Now**. To schedule the access for a later date or time, select **Scheduled** and set the required information in **Start Date**

and **Start Time**. Click **Next** after entering the required information.

The screenshot shows the 'Remote Support Authorization' page in the Cisco Identity Services Engine. The page has a blue header with the Cisco logo and 'Identity Services Engine' on the left, and 'Operations / Support' on the right. A left sidebar contains navigation links: Bookmarks, Dashboard, Context Visibility, Operations (highlighted), Policy, Administration, Work Centers, and Interactive Help. The main content area has a progress bar with four steps: 1. Setup up the Authorization (completed), 2. Schedule the Access (active), 3. Access Permission Agreement, and 4. Summary. Below the progress bar, the 'Schedule the Access' section includes a sub-header and a description: 'Take your network schedule into consideration, select a time period that is the most suitable for the Cisco specialist to access Cisco ISE for troubleshooting.' There are two sections: 'Duration' with radio buttons for 24h (selected), 48h, and 72h; and 'Schedule' with radio buttons for Now (selected) and Scheduled. At the bottom right, there are 'Back' and 'Next' buttons. At the bottom left, there is an 'Exit' button.

Second page of Authorization creation

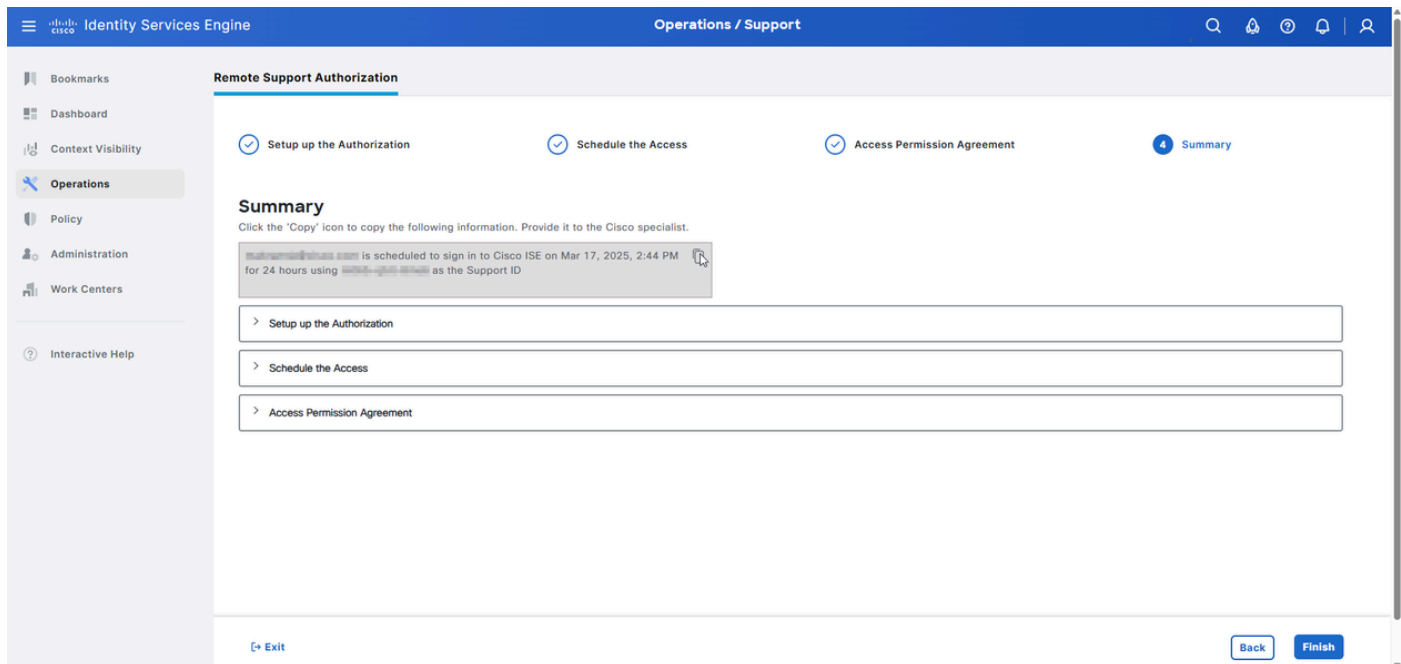
Select each ISE node that you would like to give access to. To enable remote CLI access to the nodes, select **I Agree to give access to CLI**. To enable remote UI access to the nodes, select **I Agree to give access to UI**. Click **Next** after entering the required information.

 **Note:** To provide UI access, you must configure a UI administrator username/password. This account is used to create a new admin user that the Cisco specialist uses to sign in with the specified access level, thus the entered account must have the required permissions to create a new admin account. The credentials must be for an internal admin user unless Active Directory is configured as a UI identity source in which case AD admin credentials can also be used.

The screenshot shows the 'Access Permission Agreement' step in the Remote Support Authorization process. The page layout is similar to the previous one. The progress bar now shows step 3, 'Access Permission Agreement', as the active step. The 'Access Permission Agreement' section includes a sub-header and a description: 'A Cisco specialist will use the Cisco Remote Support Authorization credentials to access Cisco ISE.' There is a 'Select Node(s)*' dropdown menu. Below it, there are two checkboxes: 'I Agree to give access to CLI' (checked) and 'I Agree to give access to UI' (checked). There are two text input fields: 'Username*' with the value 'admin' and 'Password*' with a masked password and a 'Show' button. At the bottom right, there are 'Back' and 'Next' buttons. At the bottom left, there is an 'Exit' button.

Third page of Authorization creation

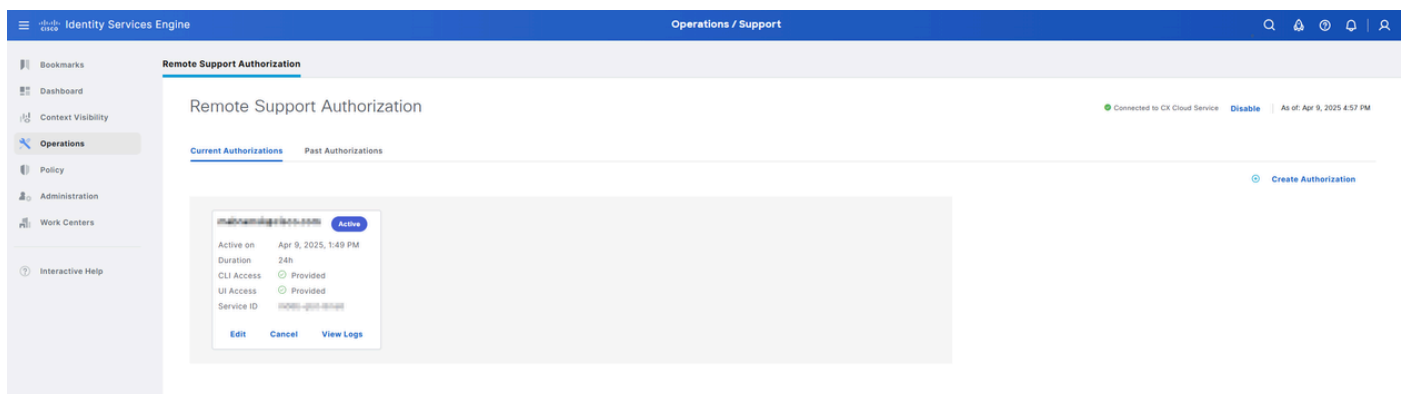
Click the copy icon to copy the remote support authorization information and provide this to the Cisco Specialist. Click **Finish** to finalize the remote access authorization.



Summary page of Authorization creation

Verify

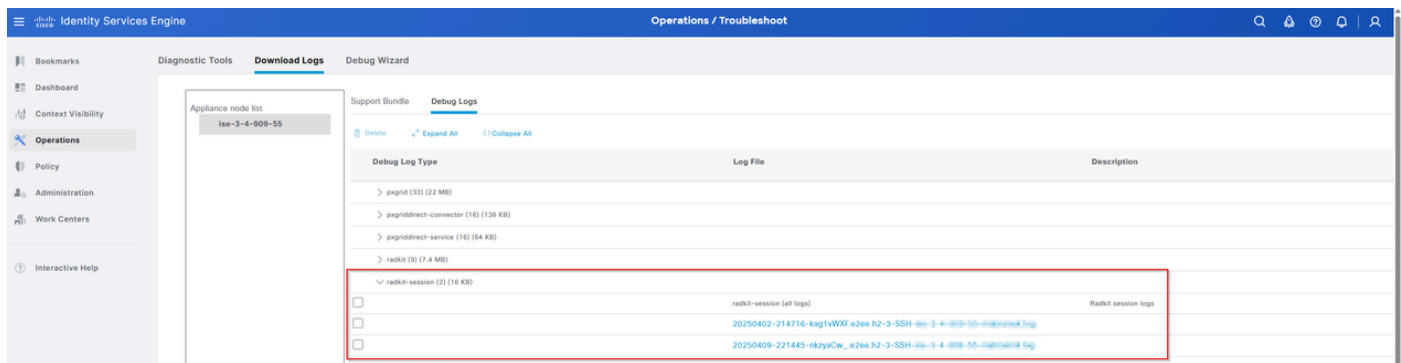
You can verify all currently active remote support authorizations on the **Current Authorizations** tab. You can view any previous remote support authorizations on the **Past Authorizations** tab.



Verify Active Authorizations

To view CLI session audit logs for a node, navigate to **Operations > Support > Troubleshoot > Download Logs**, select the node you want to download the logs for, then select **Debug Logs**. All CLI sessions can be found in the radkit-session folder. Click on the file name to download the audit logs.

 **Note:** CLI session monitoring must be done per node. Each node has its own radkit-session folder with specific audit logs for the node.



CLI Audit Logs

To view UI audit logs, you can use the audit reports in the ISE UI. Navigate to **Operations > Reports > Audit > Administrator Logins** to view any administrator logins to the UI or CLI. Navigate to **Operations > Reports > Audit > Change Configuration Audit** to view any changes made by administrators in the UI.

Note: Cisco Specialists that sign into the UI use username **<user>-CustomerSupport** where **<user>** is the username supplied in the remote support authorization. Cisco Specialists that sign into the CLI use username **customersuppadmin** if they have Admin (Read-Write) access, or **customersuppreadonly** if they have Observer (Read-Only) access.

Troubleshoot

To view logs on the container starting during the initial setup process where the email is entered on the UI, we need to view the ADE.log file. From the CLI, enter the **show logging system ade/ADE.log tail** command:

```
2025-05-20T14:21:07.670874-05:00 ise-3-4-909-55 root: info:[application:operation:radkit-control.sh] Co
2025-05-20T14:21:07.818398-05:00 ise-3-4-909-55 root: info:[application:operation:radkit-control.sh] do
2025-05-20T14:21:07.821281-05:00 ise-3-4-909-55 root: info:[application:operation:radkit-control.sh] St
2025-05-20T14:21:07.824667-05:00 ise-3-4-909-55 root: info:[application:operation:radkit-control.sh] in
2025-05-20T14:21:07.828862-05:00 ise-3-4-909-55 ADEOSShell[594468]: ADEAUDIT 2061, type=USER, name=RADK
2025-05-20T14:21:07.829439-05:00 ise-3-4-909-55 root: info:[application:operation:radkit-control.sh] in
2025-05-20T14:21:07.877488-05:00 ise-3-4-909-55 root: info:[application:operation:radkit-control.sh] in
2025-05-20T14:21:08.057775-05:00 ise-3-4-909-55 root: info:[application:operation:radkit-control.sh] Im
2025-05-20T14:21:08.060665-05:00 ise-3-4-909-55 root: info:[application:operation:radkit-control.sh] Do
2025-05-20T14:21:08.063583-05:00 ise-3-4-909-55 root: info:[application:operation:radkit-control.sh] Do
2025-05-20T14:21:08.066214-05:00 ise-3-4-909-55 root: info:[application:operation:radkit-control.sh] Se
```

ISE monitors the container to check if it is running and if the RADKit application is ready before marking the Remote Authorization Service as started.

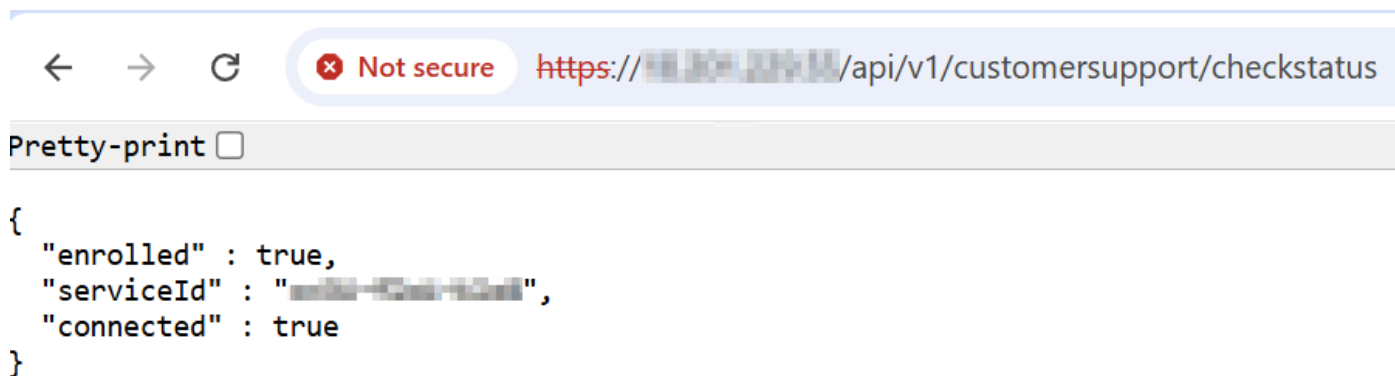
```
2025-05-20T14:21:24.477946-05:00 ise-3-4-909-55 root: info:[application:operation:radkit-control.sh] Co
2025-05-20T14:21:24.800804-05:00 ise-3-4-909-55 root: info:[application:operation:radkit-control.sh] In
2025-05-20T14:21:24.804531-05:00 ise-3-4-909-55 root: info:[application:operation:radkit-control.sh] IS
2025-05-20T14:21:27.859691-05:00 ise-3-4-909-55 root: info:[application:operation:radkit-control.sh] Co
2025-05-20T14:21:28.024853-05:00 ise-3-4-909-55 root: info:[application:operation:radkit-control.sh] In
2025-05-20T14:21:28.028121-05:00 ise-3-4-909-55 root: info:[application:operation:radkit-control.sh] IS
2025-05-20T14:21:31.079596-05:00 ise-3-4-909-55 root: info:[application:operation:radkit-control.sh] Co
2025-05-20T14:21:31.232927-05:00 ise-3-4-909-55 root: info:[application:operation:radkit-control.sh] In
```

```

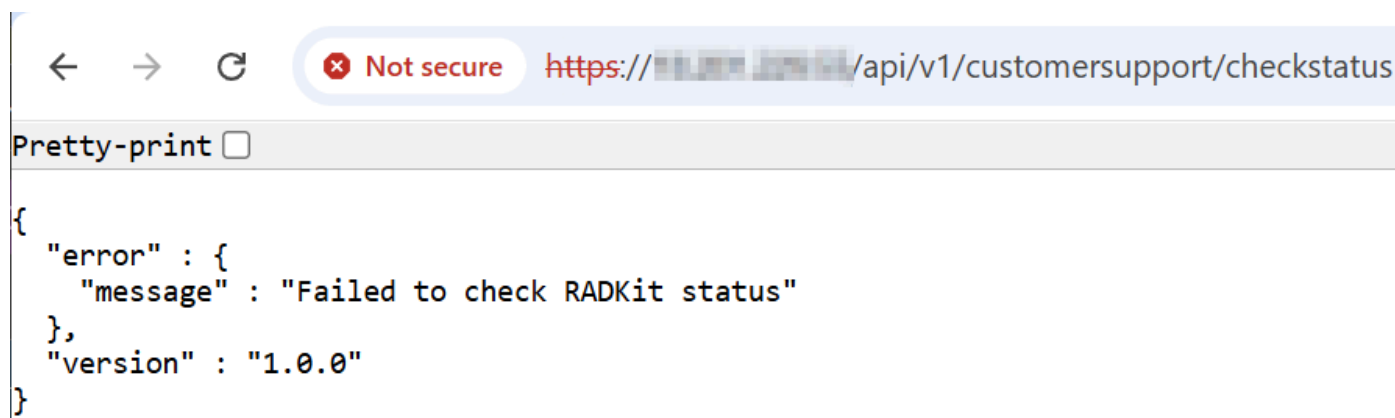
2025-05-20T14:21:31.236149-05:00 ise-3-4-909-55 root: info:[application:operation:radkit-control.sh] IS
2025-05-20T14:21:34.287758-05:00 ise-3-4-909-55 root: info:[application:operation:radkit-control.sh] Co
2025-05-20T14:21:34.426699-05:00 ise-3-4-909-55 root: info:[application:operation:radkit-control.sh] In
2025-05-20T14:21:34.429983-05:00 ise-3-4-909-55 root: info:[application:operation:radkit-control.sh] IS
2025-05-20T14:21:37.486192-05:00 ise-3-4-909-55 root: info:[application:operation:radkit-control.sh] Co
2025-05-20T14:21:37.621712-05:00 ise-3-4-909-55 root: info:[application:operation:radkit-control.sh] Re

```

You can also check the status of the RADKit Service using the API call https://<ISE_PPAN>/api/v1/customersupport/checkstatus .



Output when RadKit Service is running



Output when RadKit Service is not running

To view the RADKit Service logs once the Remote Support Authorization Service is started, enter the **show logging application radkit/service/service.log** command. When the service is first started, some basic setup is done with the RADKit application.

```

2025-05-20T19:21:31.730Z INFO | internal | MainThread <main> [] RADKit Service [version='1.6.12']
2025-05-20T19:21:31.731Z INFO | internal | MainThread <main> [] STDIN is not a terminal; assuming --he
2025-05-20T19:21:31.732Z INFO | internal | MainThread <main> [] This RADKit release does not expire
2025-05-20T19:21:34.101Z INFO | internal | MainThread radkit_service.database.service_db [DB] Creating
2025-05-20T19:21:34.102Z INFO | internal | MainThread radkit_service.database.service_db [DB] Storing
2025-05-20T19:21:34.104Z INFO | internal | MainThread radkit_service.database.service_db [DB] Opening
2025-05-20T19:21:34.105Z INFO | internal | MainThread radkit_service.backup [SYSTEM] Ensuring backup d

```

The RADKit service which is available for connections is created.


```

2025-05-20T19:22:25.284Z INFO | radkit_control/superadmin/184f89f8 | MainThread radkit_service.service
2025-05-20T19:22:25.655Z INFO | radkit_control/superadmin/184f89f8 | MainThread Service(0x7F92596171D0)
2025-05-20T19:22:25.664Z INFO | radkit_control/superadmin/184f89f8 | MainThread SingleWebSocketForward
2025-05-20T19:22:25.679Z INFO | radkit_control/superadmin/c5f2549f | MainThread radkit_service.webserv

```

When you add a remote support authorization in the GUI, the Cisco Specialist is created as a remote user.

```

2025-05-20T19:24:10.599Z INFO | radkit_control/superadmin/5d496186 | MainThread DBOperationsAPI(0x7F92
2025-05-20T19:24:10.600Z INFO | radkit_control/superadmin/5d496186 | MainThread radkit_service.webserv

```

When the Cisco Specialist connects to the service and accesses an ISE node, it is shown in these logs.

```

2025-05-20T19:26:02.766Z INFO | cloud-rpc/mabramsk@cisco.com/4Kkevny_ | MainThread RPCServer(0x7F925A1
2025-05-20T19:26:03.033Z INFO | cloud-rpc/mabramsk@cisco.com/4Kkevny_ | MainThread CapabilitiesRespond
2025-05-20T19:26:03.117Z INFO | cloud-rpc/mabramsk@cisco.com/4Kkevny_ | MainThread CapabilitiesRespond
2025-05-20T19:26:03.121Z INFO | cloud-rpc/mabramsk@cisco.com/4Kkevny_ | MainThread RPCServer(0x7F925A1
2025-05-20T19:26:04.863Z INFO | cloud-rpc/mabramsk@cisco.com/cjZPy-yR | MainThread EncryptedRPCServerT
2025-05-20T19:26:04.864Z INFO | cloud-rpc/mabramsk@cisco.com/cjZPy-yR.e2ee | MainThread H2Multiplexing
2025-05-20T19:26:04.869Z INFO | cloud-rpc/mabramsk@cisco.com/cjZPy-yR.e2ee.h2-1 | MainThread RPCServer
2025-05-20T19:26:04.879Z INFO | cloud-rpc/mabramsk@cisco.com/cjZPy-yR.e2ee.h2-1 | MainThread Inventory
2025-05-20T19:26:04.882Z INFO | cloud-rpc/mabramsk@cisco.com/cjZPy-yR.e2ee.h2-1 | MainThread Inventory
2025-05-20T19:26:04.885Z INFO | cloud-rpc/mabramsk@cisco.com/cjZPy-yR.e2ee.h2-1 | MainThread RPCServer
2025-05-20T19:26:26.083Z INFO | cloud-rpc/mabramsk@cisco.com/cjZPy-yR.e2ee.h2-3 | MainThread RPCServer
2025-05-20T19:26:26.090Z INFO | cloud-rpc/mabramsk@cisco.com/cjZPy-yR.e2ee.h2-3 | MainThread TerminalP
2025-05-20T19:26:26.146Z INFO | cloud-rpc/mabramsk@cisco.com/cjZPy-yR.e2ee.h2-3 | MainThread SSHPTYStr
2025-05-20T19:26:26.198Z INFO | cloud-rpc/mabramsk@cisco.com/cjZPy-yR.e2ee.h2-3 | MainThread radkit_se
2025-05-20T19:26:43.932Z INFO | cloud-rpc/mabramsk@cisco.com/cjZPy-yR.e2ee.h2-3 | MainThread TerminalP
2025-05-20T19:26:43.935Z INFO | cloud-rpc/mabramsk@cisco.com/cjZPy-yR.e2ee.h2-3 | MainThread RPCServer

```

Once the remote authorization expires or is removed, the remote user is deleted from the RADKit service.

```

2025-05-20T19:26:55.195Z INFO | radkit_control/superadmin/8fd4246f | MainThread radkit_service.webserv
2025-05-20T19:26:55.196Z INFO | radkit_control/superadmin/8fd4246f | MainThread radkit_service.webserv

```

Related Information

- [Cisco Identity Services Engine Administrator Guide, Release 3.4](#)
- [Release Notes for Cisco Identity Services Engine, Release 3.4](#)