Configure Catalyst Center Remote Support Authorization Feature

Contents

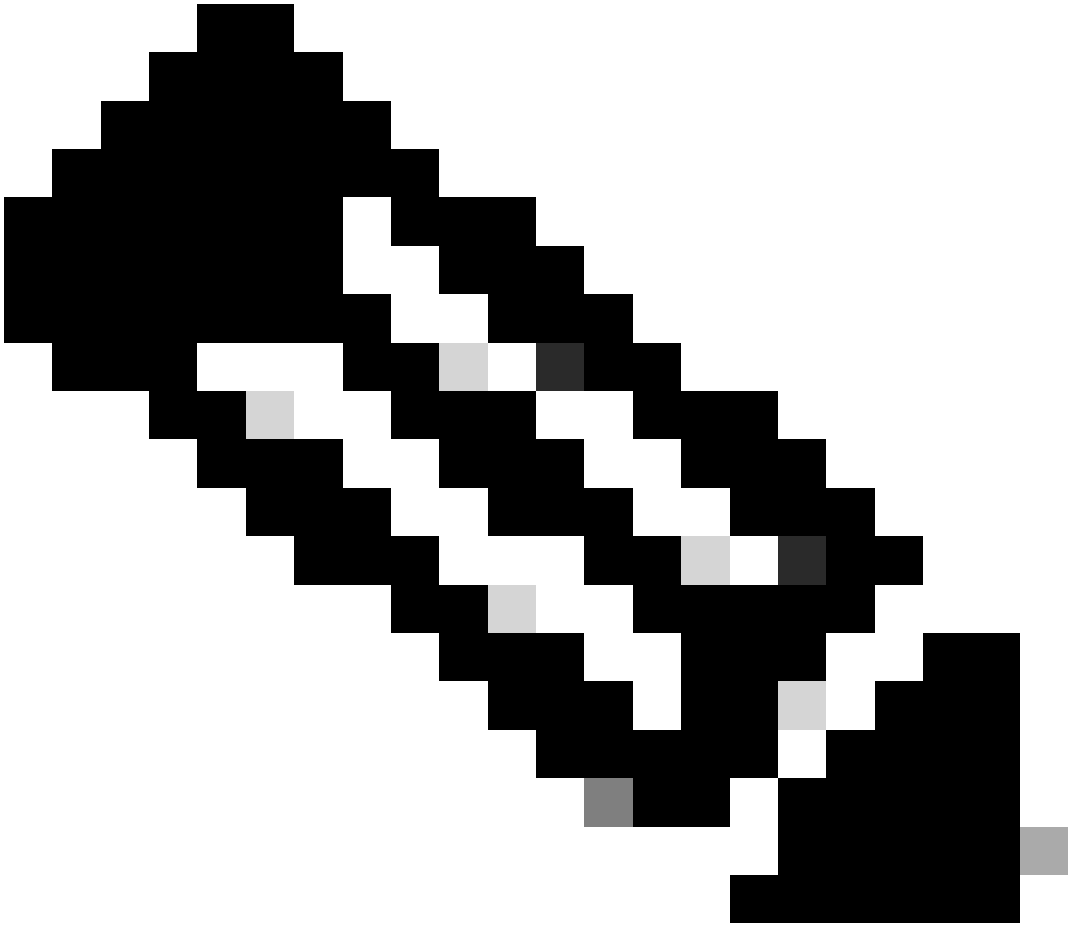
Introduction

This document describes how to set up the Remote Support Authorization feature in Cisco Catalyst Center (formerly Cisco DNA Center).

Prerequisites

To be able to fully utilize the new Remote Support Authorization feature in Cisco Catalyst Center, certain criteria must be met:

• Cisco Catalyst Center must be version 2.3.7.6 or higher.
• The Support Services package must to be installed in Cisco Catalyst Center.
• Allow remote authorization support through the firewall or proxy: wss://prod.radkit-cloud.cisco.com:443 .



Note: Remote Support Authorization is introduced in Cisco Catalyst Center version 2.3.3.x but has limited functionality. Only network device access is permitted, Cisco Catalyst Center CLI access is not present in this earlier version. Cisco Catalyst Center version 2.3.7.6+ offers web UI proxy access, role-based access control (RBAC) profiling and passwordless command access.

Description

Cisco RADKit (radkit.cisco.com) provides secure interactive connectivity to remote terminals and Web UIs. Cisco RADKit features are integrated in Cisco Catalyst Center and is called Remote Support Authorization. When users utilize the Remote Support Authorization feature, users can have Cisco TAC remote into their Cisco Catalyst Center environment to help gather information or troubleshoot issues. This helps reduce the amount of time users need to sit on video calls as TAC investigates issues that have occurred.

Limitations

The current version of Remote Support Authorization has these limitations compared to the RADKit standalone version:

- When the support engineer executes the "maglev", "sudo" or "rca" commands on your Cisco Catalyst Center, they prompt for credentials. Remote Support Authorization does not automate the handling of these credentials, so you must need to share these credentials with the support engineer. (*Feature added in Cisco Catalyst Center 2.3.7.6+*)

- Through the Remore Support Authorization service it is not possible to connect to the Graphical User Interface (GUI) of the Cisco Catalyst Center or to any GUI of the network devices. (*Feature added in Cisco Catalyst Center 2.3.7.6+*)

- It is not possible to provide remote access to devices that are not in the Cisco Catalyst Center inventory but that must be necessary for troubleshooting (for example ISE).

- It is not possible to provide remote access to wireless access points, even when they are in the Cisco Catalyst Center inventory.

- Remote access is limited to 24 hours at a time, to provide longer access a new authorization needs to be created every 24h.

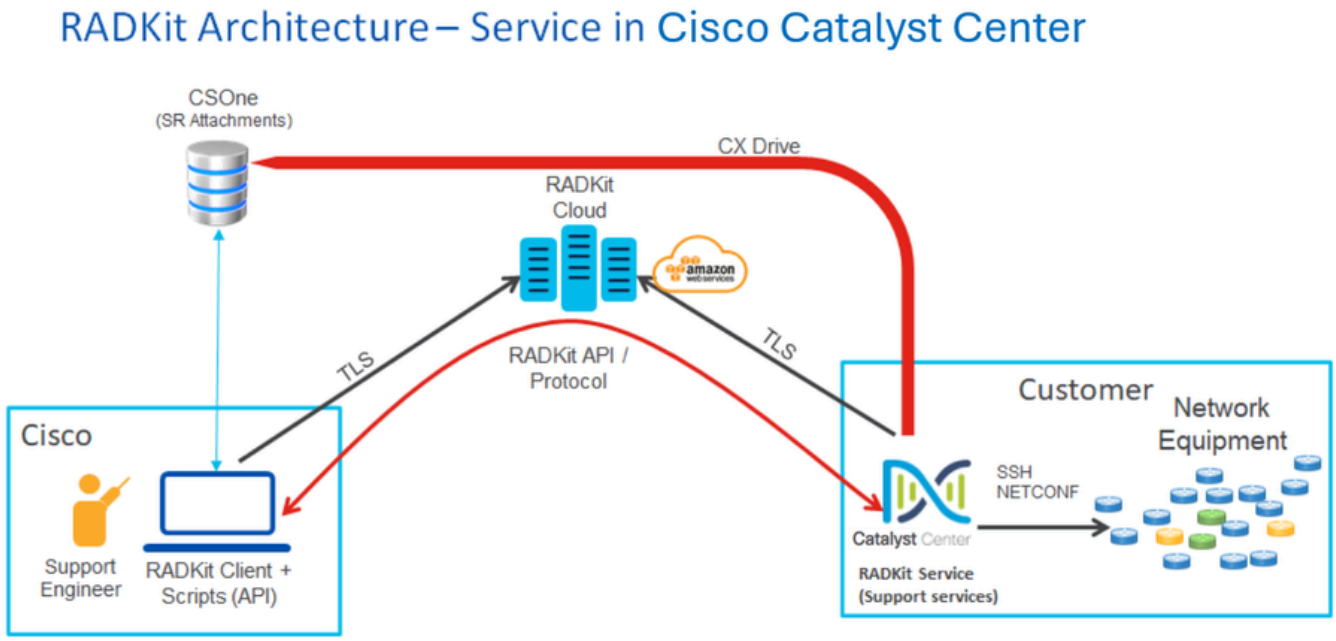
- By creating an authorization you allow access to all devices in the Cisco Catalyst Center inventory. It is not possible to restrict access to certain network devices.

To overcome these limitations, you can consider installing the standalone RADKit service instead. Installers are available for Windows, Mac and Linux. For further information please visit https://radkit.cisco.com

-

Network Connectivity

Cisco Catalyst Center connects to the Cisco RADKit connector over AWS. The Cisco RADKit connector is built into the Remote Support Authorization feature. TAC connects to the Cisco RADKit connector over AWS and uses a Cisco RADKit client. Once a Support ID is generated by the Cisco Catalyst Center environment, the Cisco RADKit client uses the Support ID to connect to the Cisco Catalyst Center.

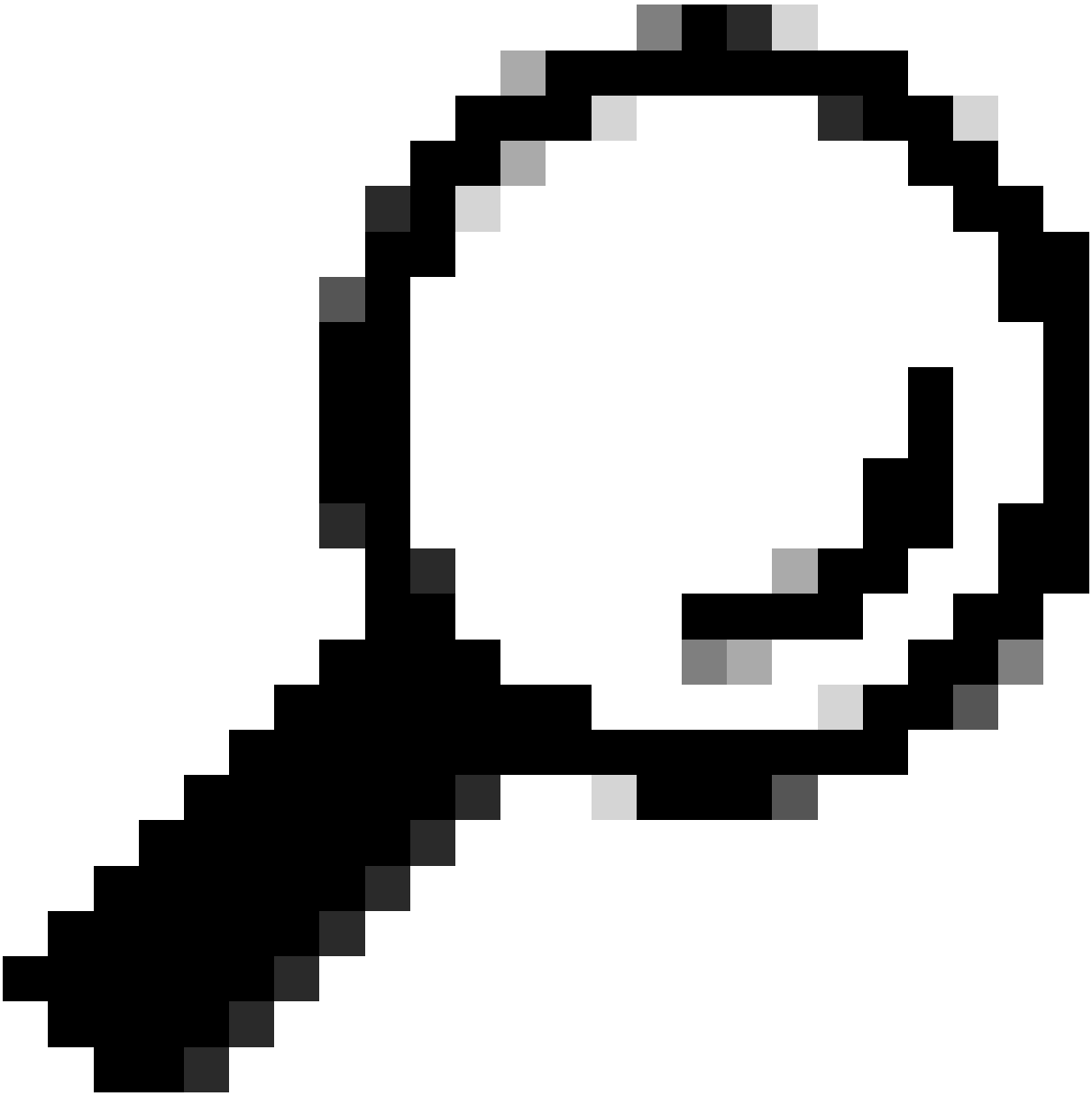


Set Up Remote Support Authorization

For Remote Support Authorization to be enabled so that the TAC can engage remotely, these steps must be completed:
1. Ensure the firewall allows the required URL through.
2. Install the Support Services package.
3. Configure the SSH credentials for the Remote Support Authorization workflow. (*No longer needed in Cisco Catalyst Center versions 2.3.7.6+*)
4. Create a new authorization.

Step 1

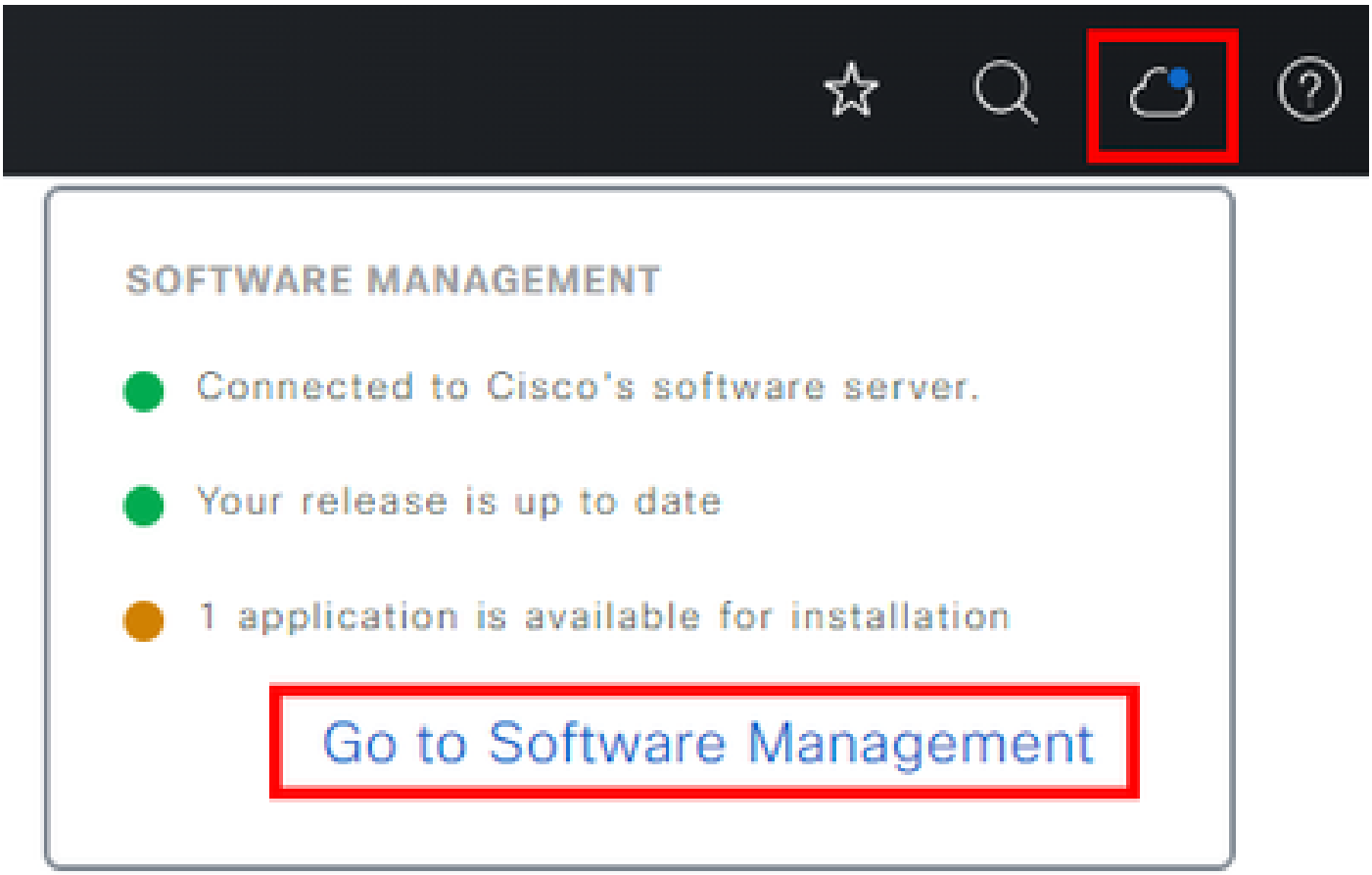
For Remote Support Authorization to work Cisco Catalyst Center connector must be able to communicate with the AWS connector. To ensure this communication, this URL must be allowed through the firewall if one is configured:
wss://prod.radkit-cloud.cisco.com:443



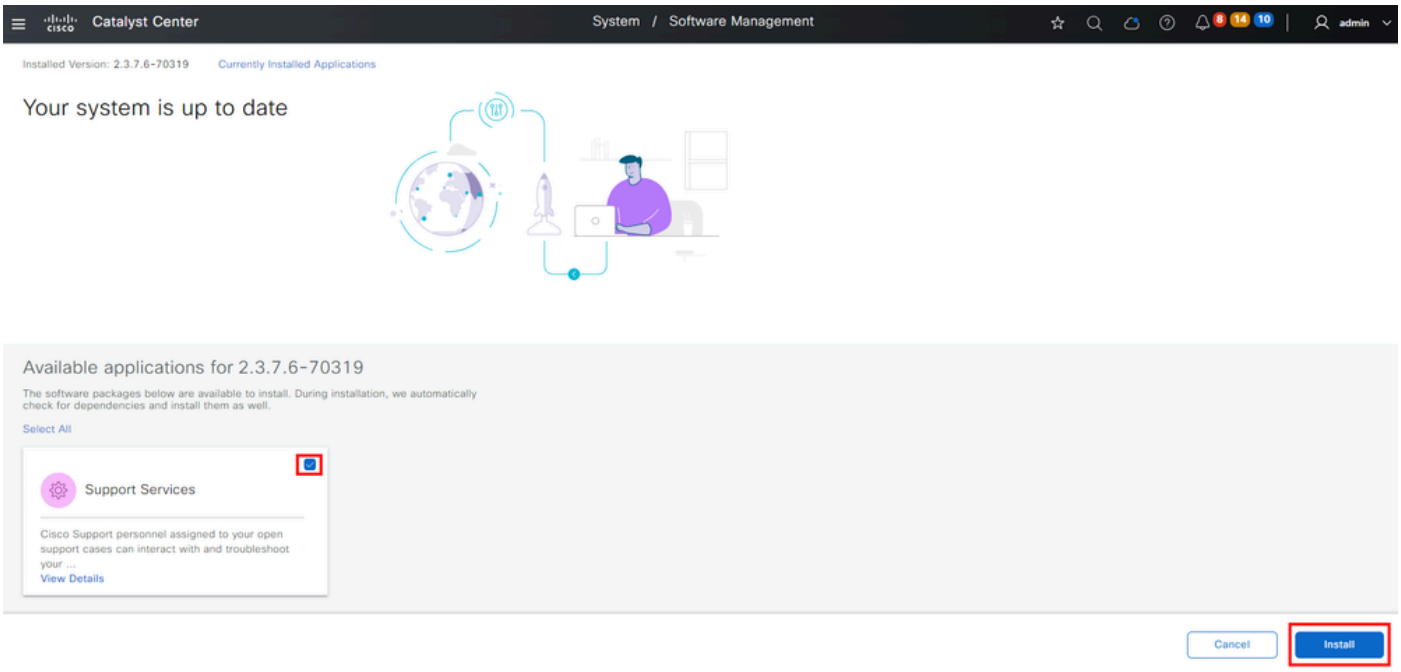
Tip: For more information on specific ports and URLs that are required to be allowed/open for Cisco Catalyst Center features to work, please review the Plan the Deployment section of the Installation Guide.

Step 2

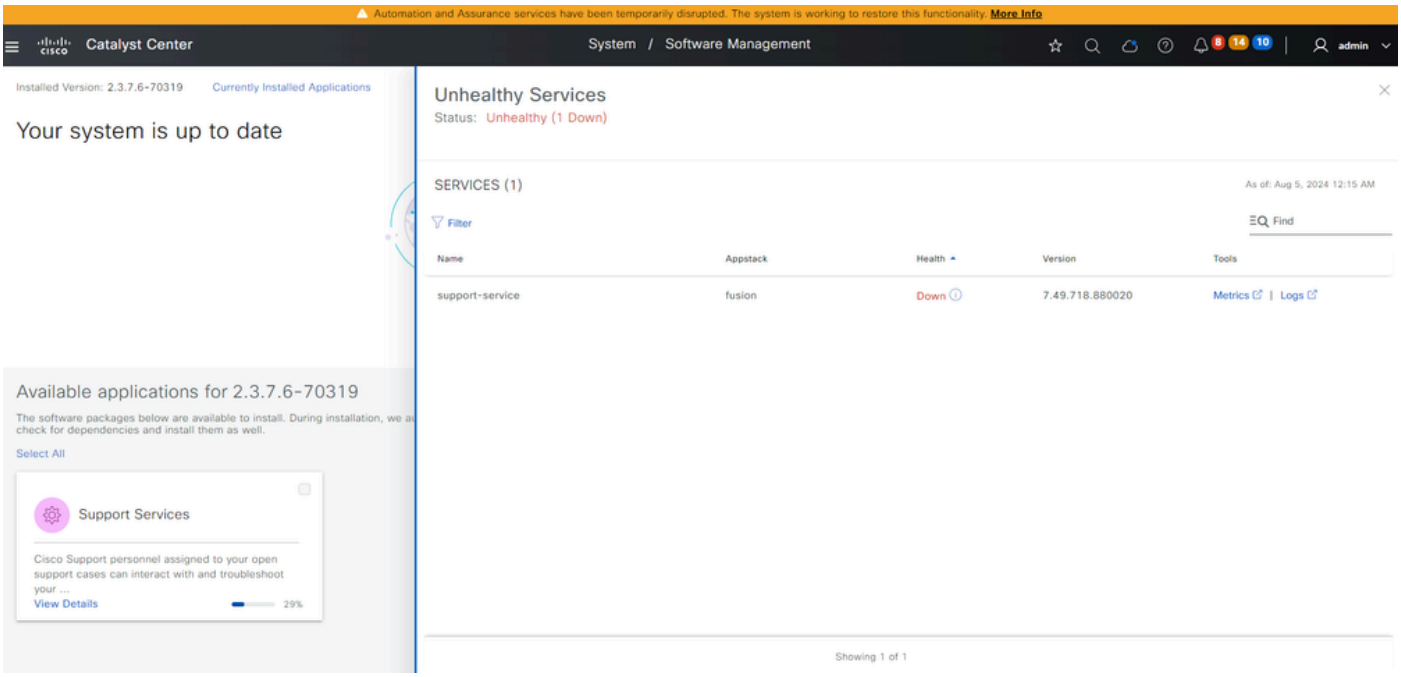
After a fresh install or an upgrade of Cisco Catalyst Center to version 2.3.5.x or higher is completed, the Support Services package must be manually installed. This is an optional package and is not installed by default. Navigate to the Cisco Catalyst Center UI. From the Home screen of the Cisco Catalyst Center UI select the cloud icon at the top-right of the screen and choose Go to Software Management.



Once on the Software Management page, you see the current installed release, any available release to upgrade to, and any available optional packages. The Support Services package is an optional package and is not installed automatically after a completed fresh install or an upgrade where the package was not previously deployed. Click the box for the Support Services package under the available packages list, then click the Install button on the bottom-right of the screen.



A pop-up window appears for a dependency check for the selected package(s). When the check is finished, choose Continue.
The selected package(s) then begins to install. The length of this process depends on the number of packages currently in the deployment process. As the package is in the deployment process, an orange banner appears at the top of the screen that states Automation and Assurance services have been temporarily disrupted. This occurs due to the new support-service pod this is created and is in the process of boot up.

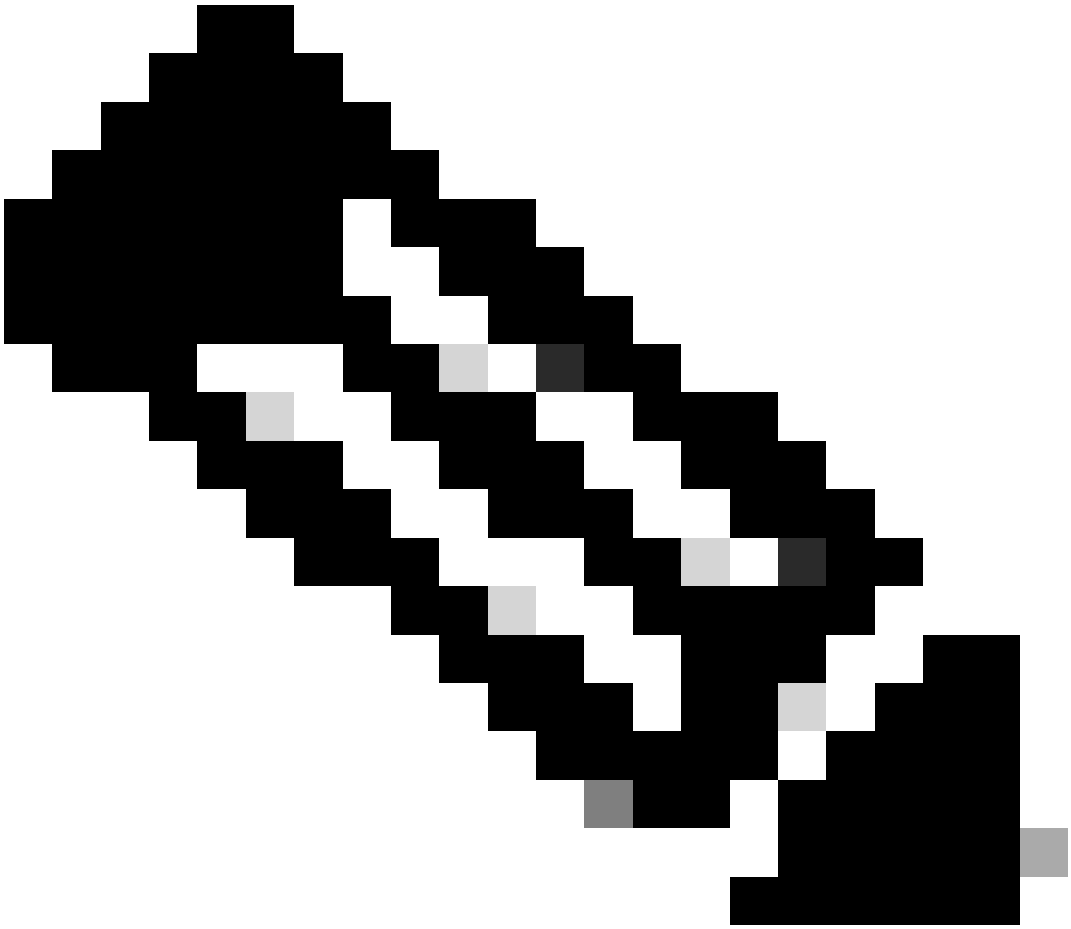


After roughly 10 to 20 minutes, the new pod is in a fully up state and the Support Services package installation completes. Once the package has been installed, refresh the browser, and proceed to step 3.

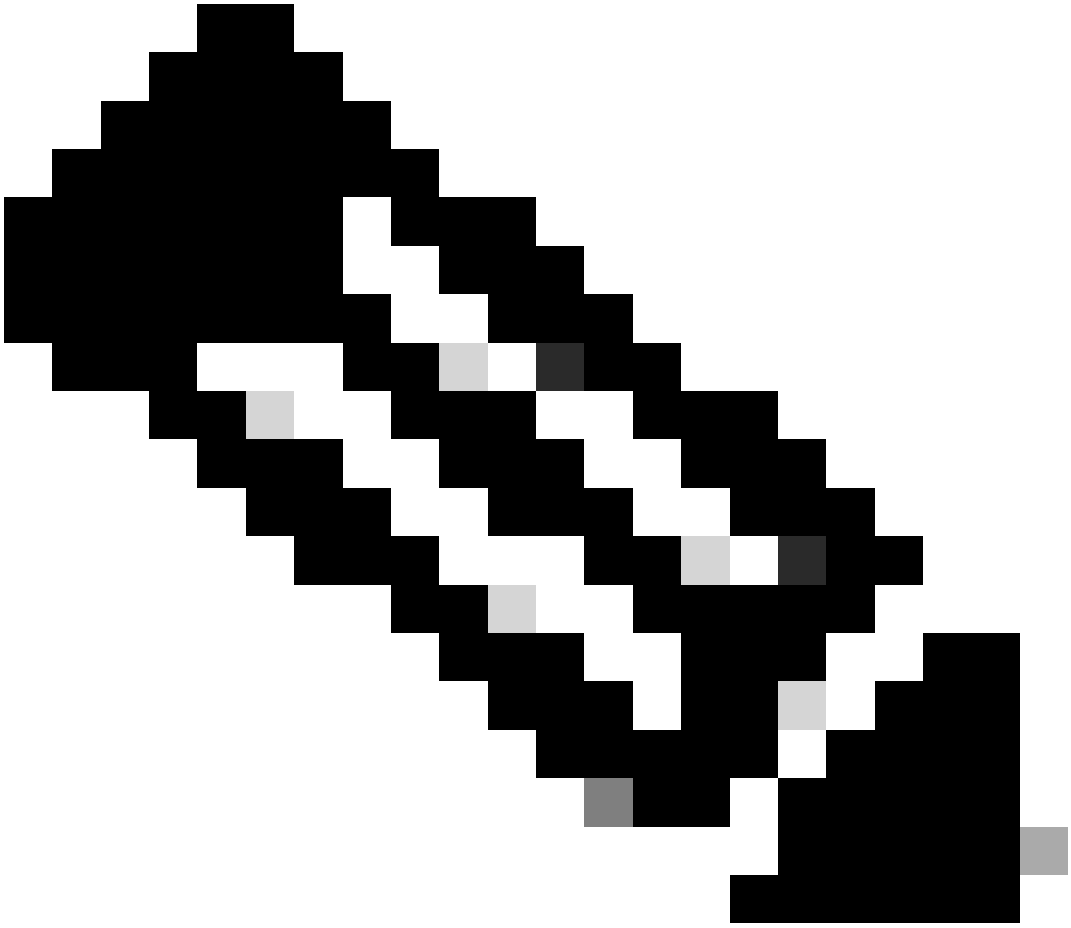
Step 3

Full access to the Remote Support Authorization feature requires that the SSH credentials be configured in the Remote Support Authorization settings. Without these credentials defined, the TAC is not be able to

utilize Cisco RADKit to troubleshoot remotely. To configure the SSH credentials, navigate to the question mark icon on the top-right of the Cisco Catalyst Center UI. From the list, choose Remote Support Authorization.

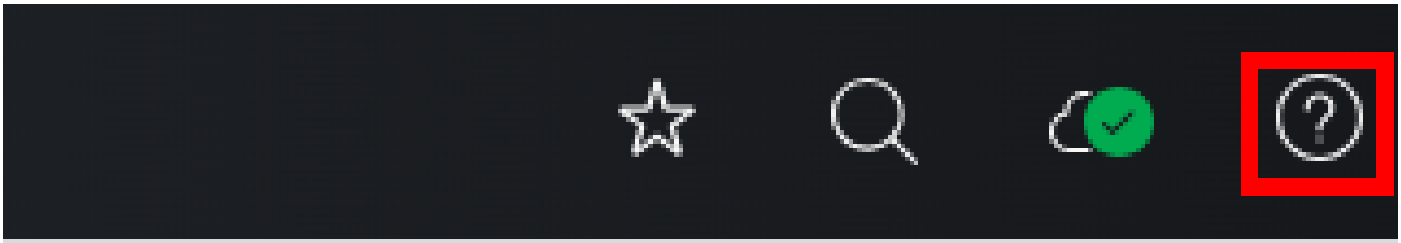


Note: Please note that Remote Support Authorization only shows after the Support Services package has been installed and the browser has been refreshed. Please refer to step 2 on how to accomplish this.

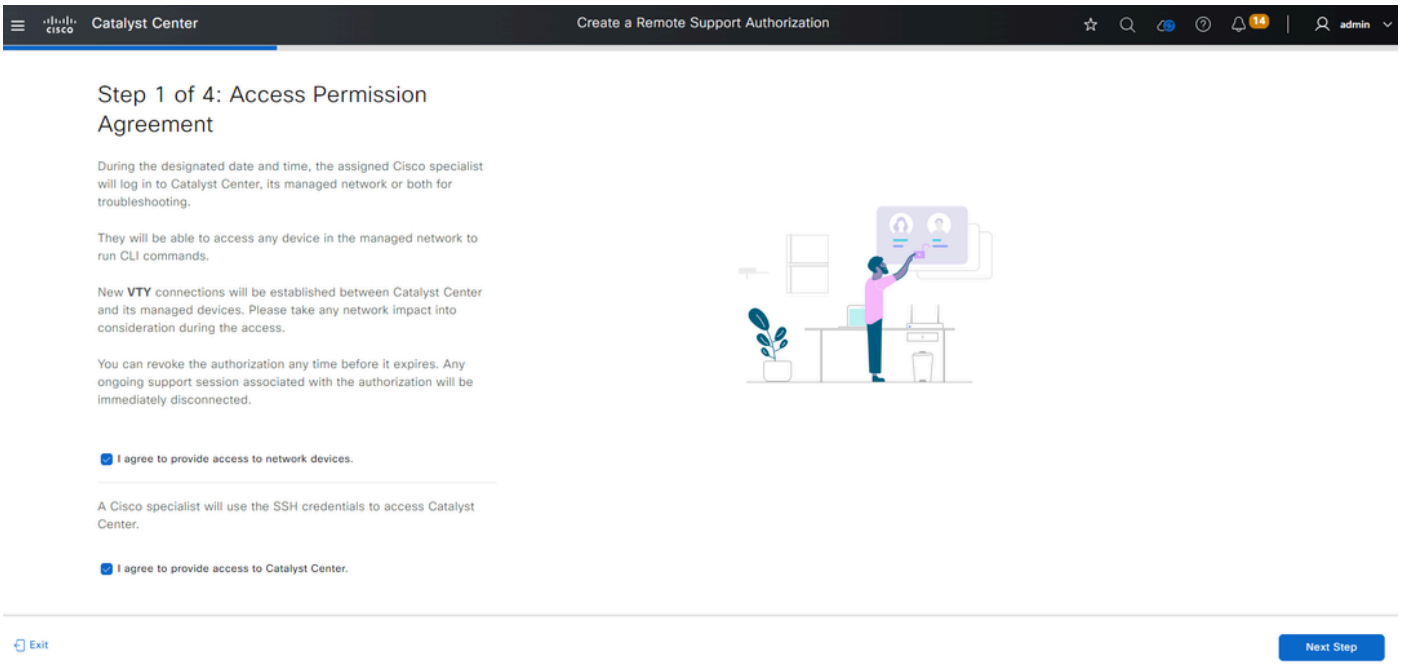


Note: SSH credentials are no longer needed to be configured in the Remote Support Authorization page starting in version 2.3.7.6 and above. This is part of the new passwordless feature. Cisco Catalyst Center pulls the credentials already stored internally so no credentials have to be configured or shared for TAC.

Spoiler (Highlight to read)

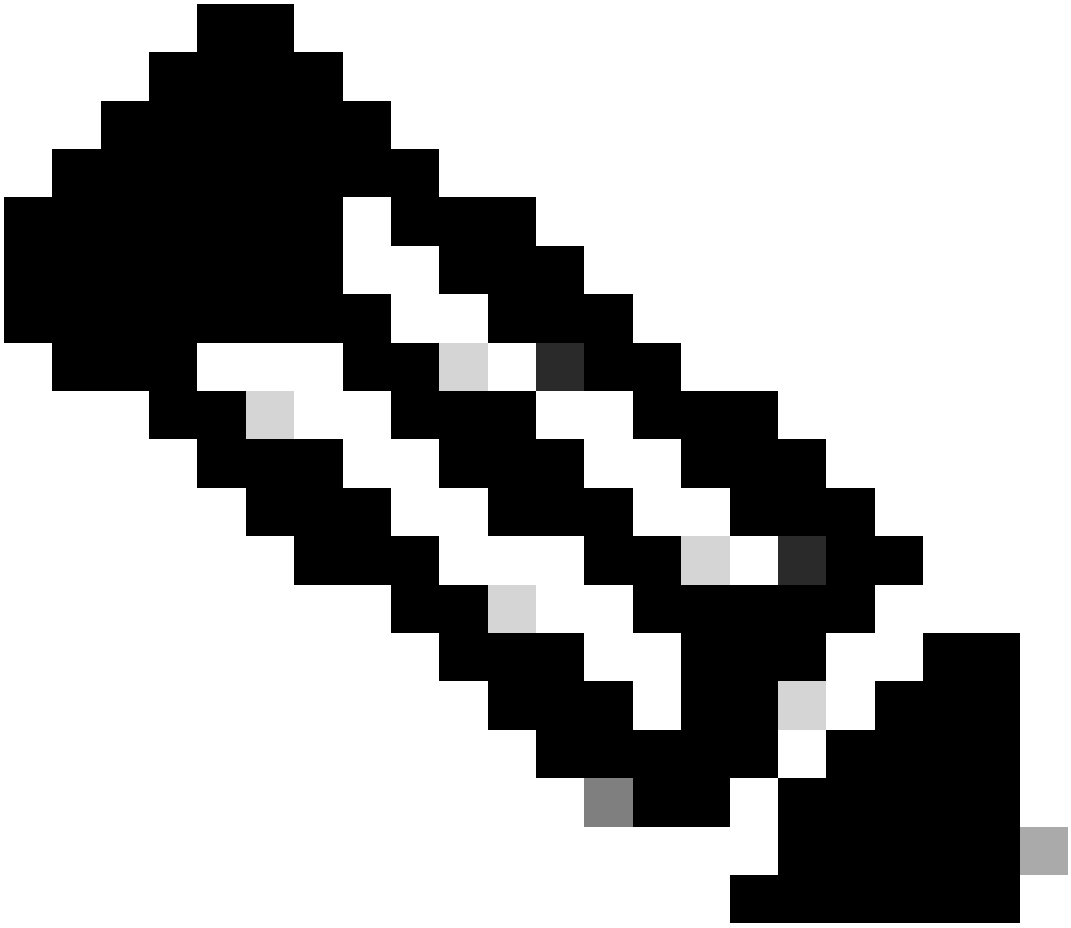

About
Cisco DNA Sense
API Reference
Developer Resources
Contact Support
Remote Support Authorization
Help
Interactive Help
Compatibility Information
Support Bundle
Keyboard Shortcuts
Alt + /

• New VTY connections between Cisco Catalyst Center and the devices managed in Inventory.
• Access to the CLI of the Cisco Catalyst Center appliance(s)
To establish an SSH connection with the network devices managed by Cisco Catalyst Center, the first option must be selected. If this option is not selected, TAC engineers do not have the ability to be able to SSH into the devices with Cisco RADKit. To establish an SSH connection to the Cisco Catalyst Center appliance(s) then the second option must be selected. If this option is not selected, TAC engineers do not have the ability to access the Cisco Catalyst Center with Cisco RADKit. For the best use of the Remote Support Authorization feature, it is recommended to select both options. After the desired options are selected, click Next.

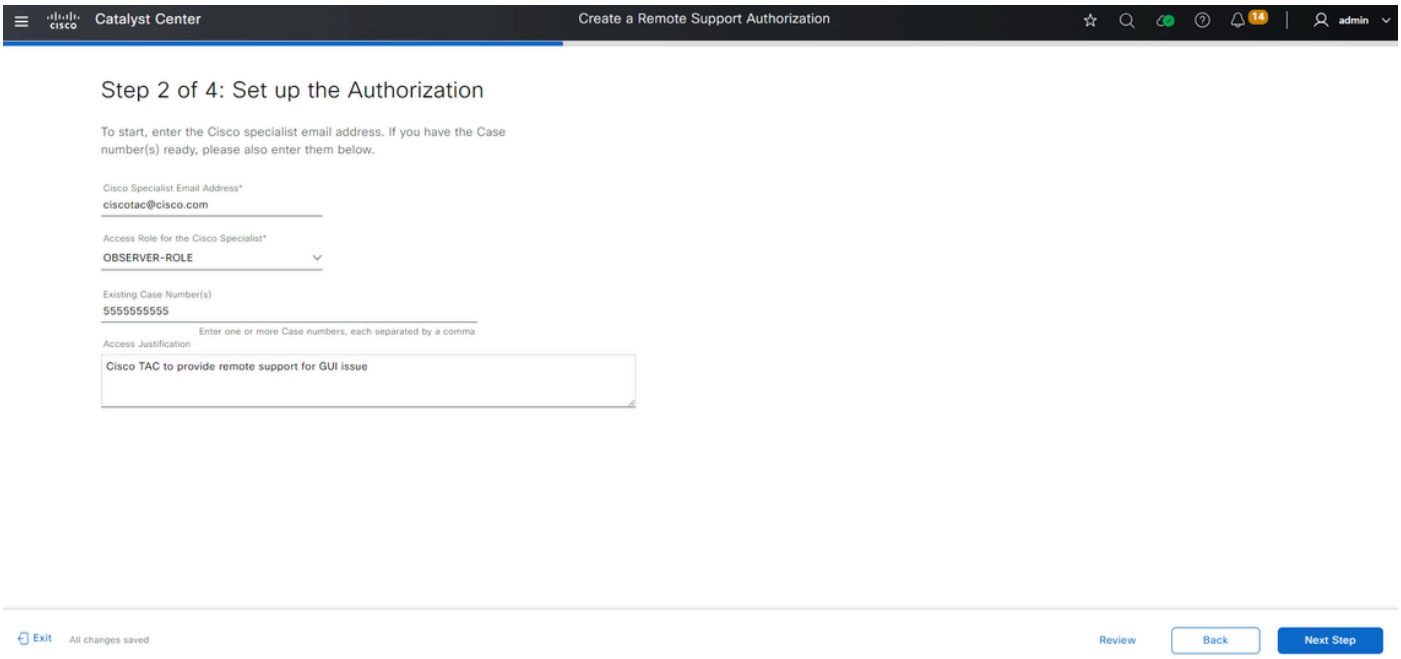


You are redirected to a workflow page to start the setup of the authorization. You must enter in the TAC engineer’s email address and the access role. For example: “ciscotac@cisco.com” and "OBSERVER-ROLE".
These two fields are optional:
• Existing SR Number(s)

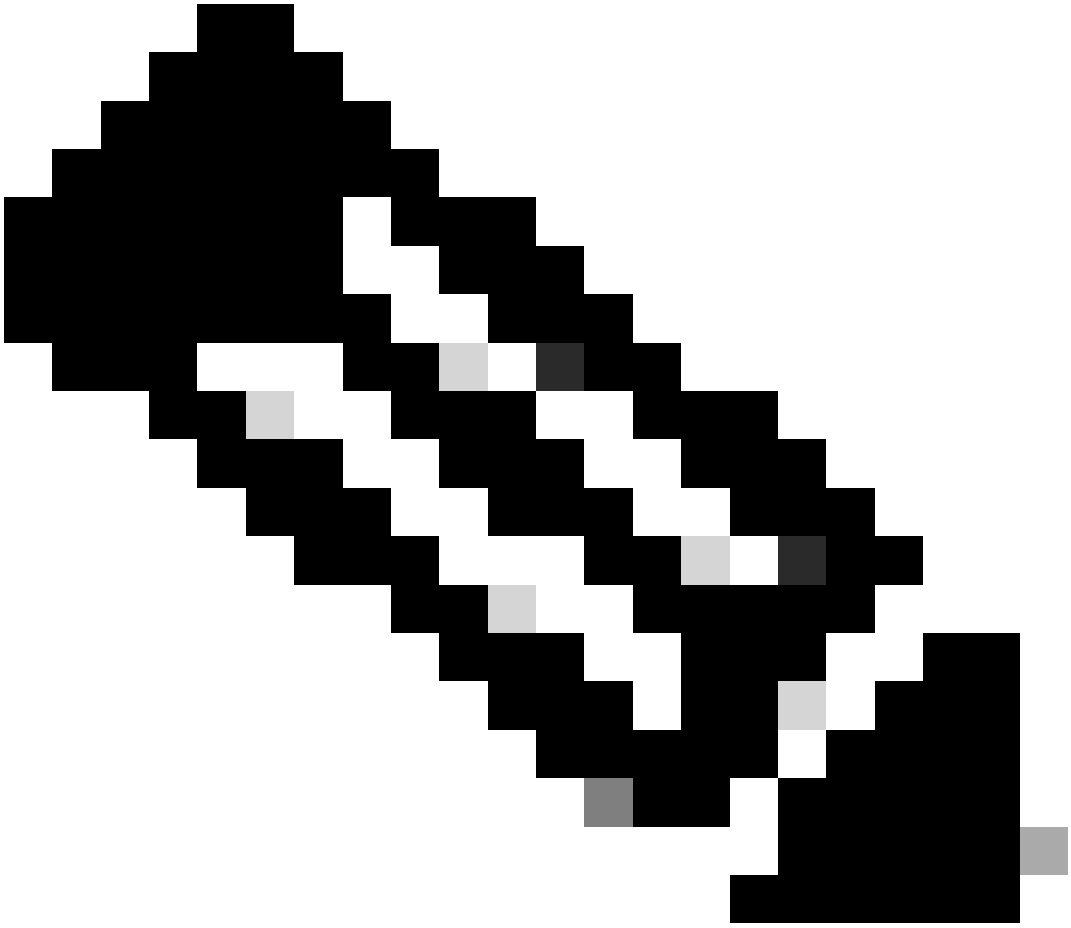
• Access Justification
If you have an open TAC service request, please enter that service request number into the Existing SR Number(s) field.
If you would like to add documentation for the Remote Support Authorization, please provide that in the Access Justification field such as, “Required by the TAC to help troubleshoot an issue seen”. Click Next.



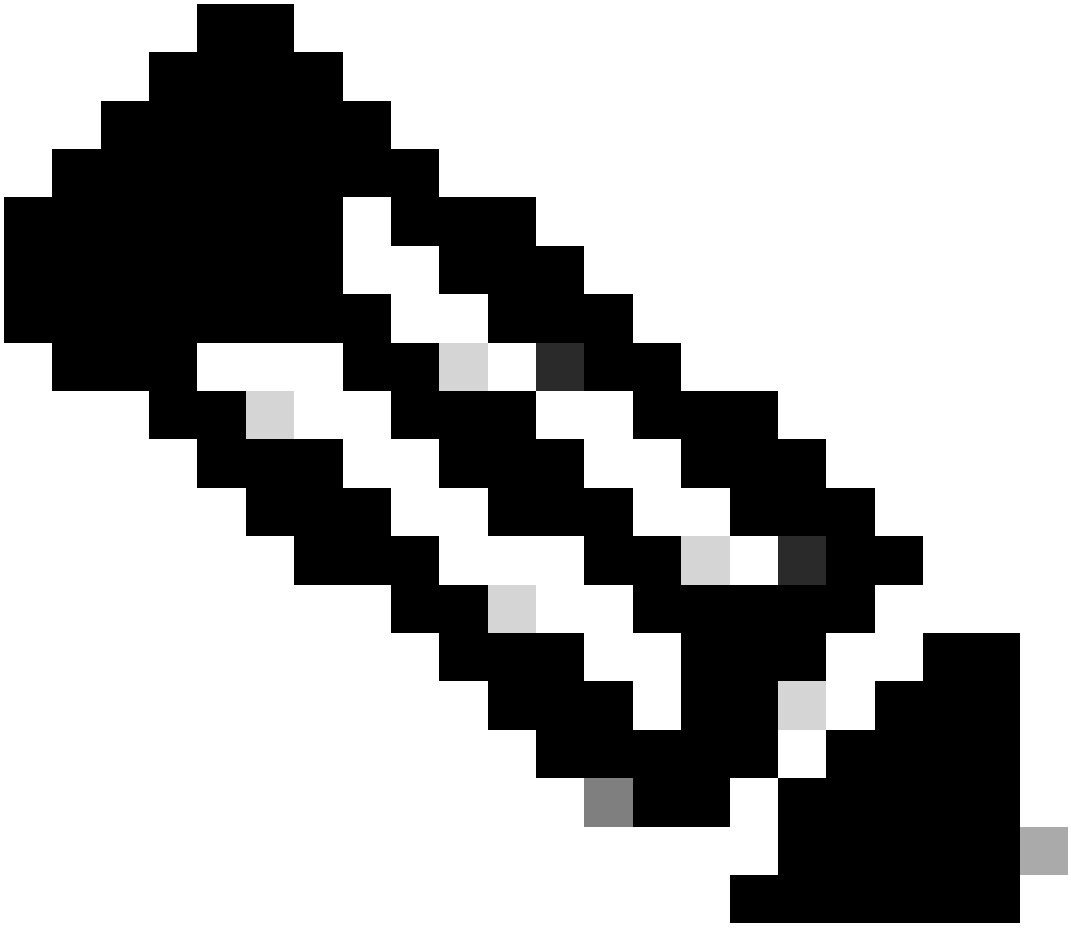
Note: Please note that the ability to use the GUI to generate the RCA or mini-RCA, run validation tool checks, or run any reports is disabled for OBSERVER-ROLE access as this is a read-only access role at this time.



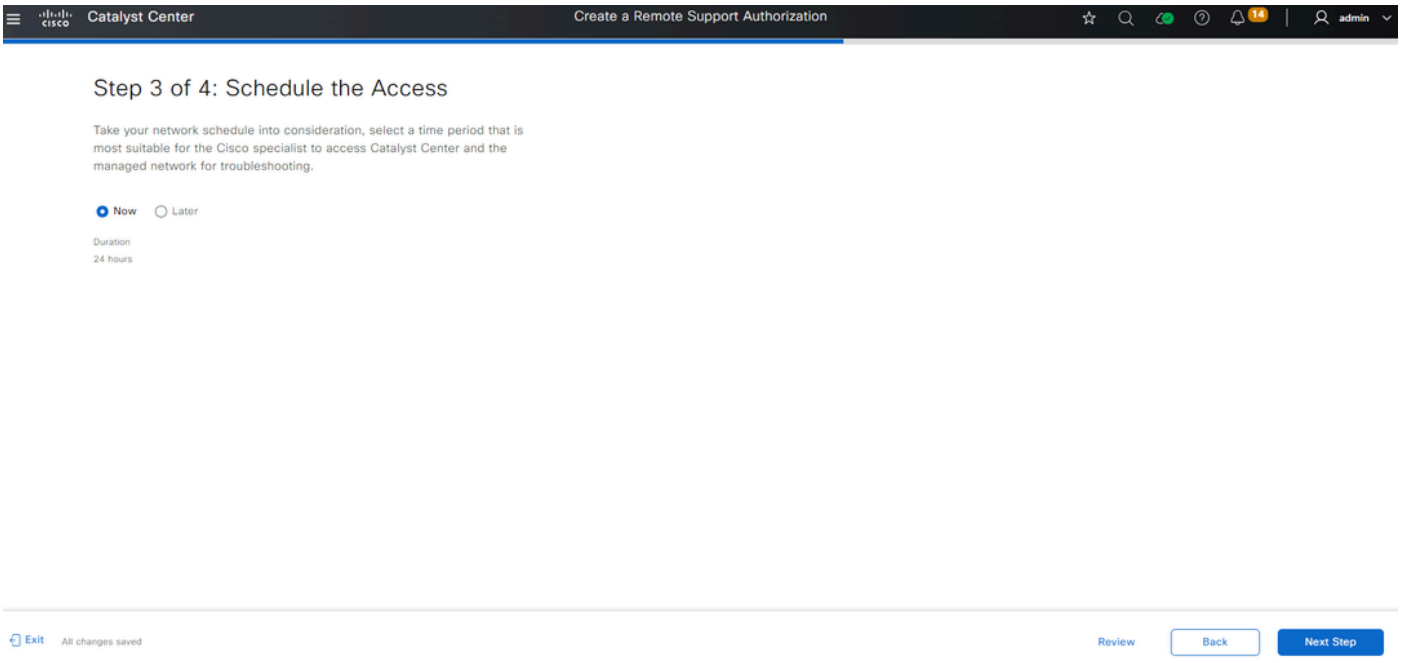
You are redirected to the Schedule the Access step. From here, you must either choose Now or Later. You can start the authorization immediately or schedule the authorization in advance.



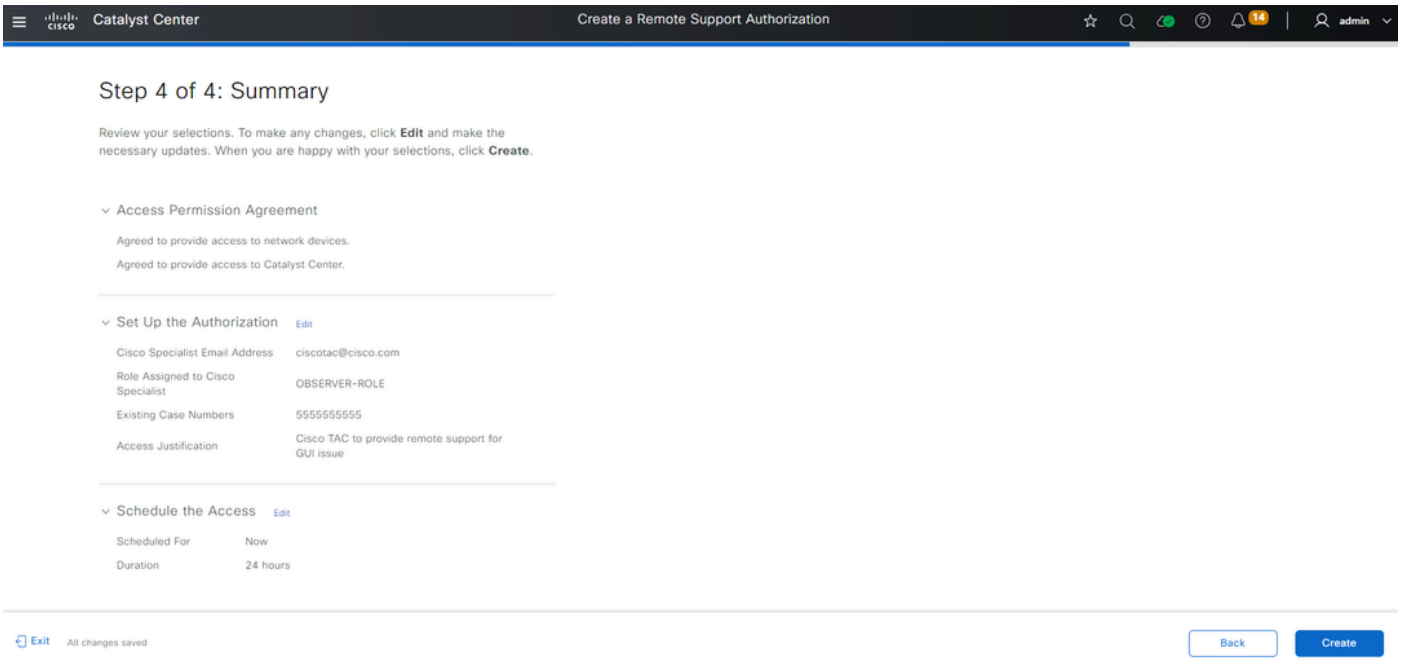
Note: Please note that the authorization can only be scheduled in advanced for up to 30 days from the current date the authorization request is created.



Note: Please note that the duration of the authorization request is 24 hours. Although authorization can be cancelled early, the duration cannot be changed from 24 hours.

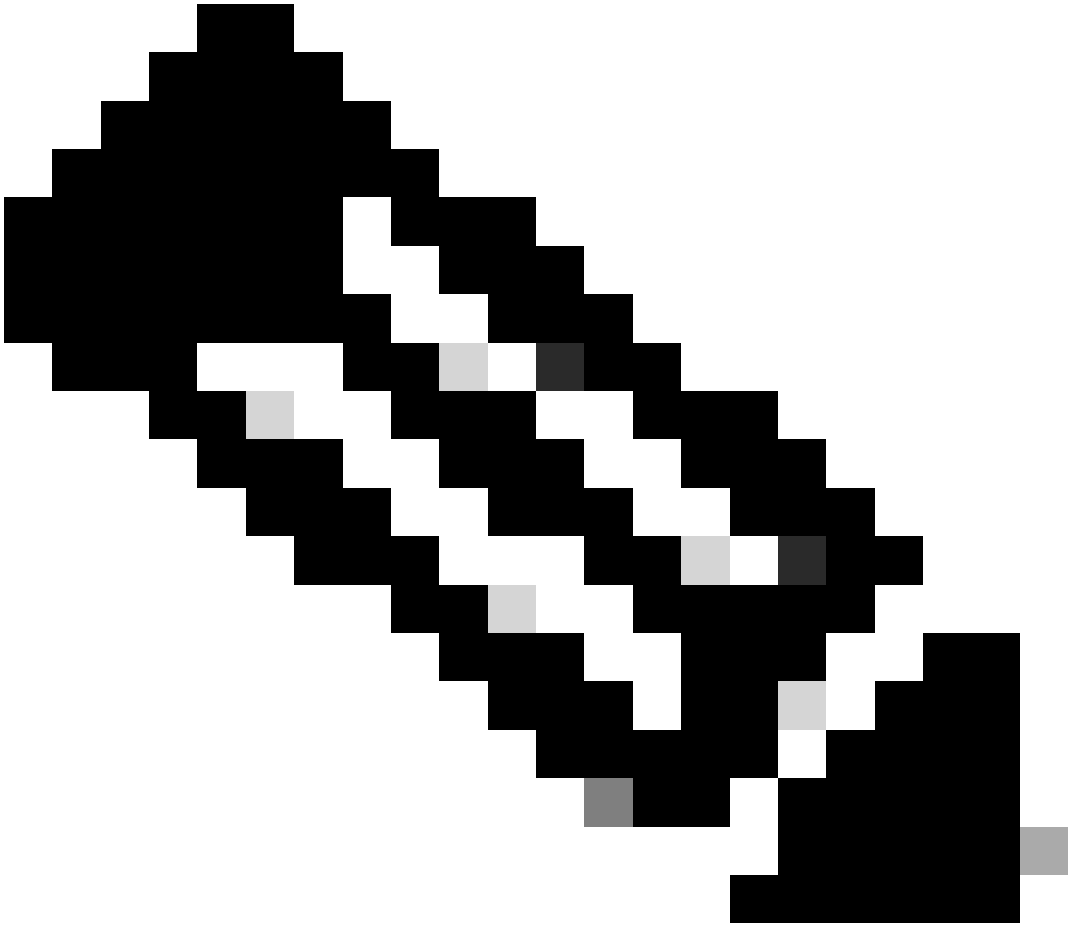


You are redirected to the Summary page that lists all that was configured with the Create a Remote Support Authorization workflow. Here you can confirm the settings are correct. If the settings are correct, click Create.

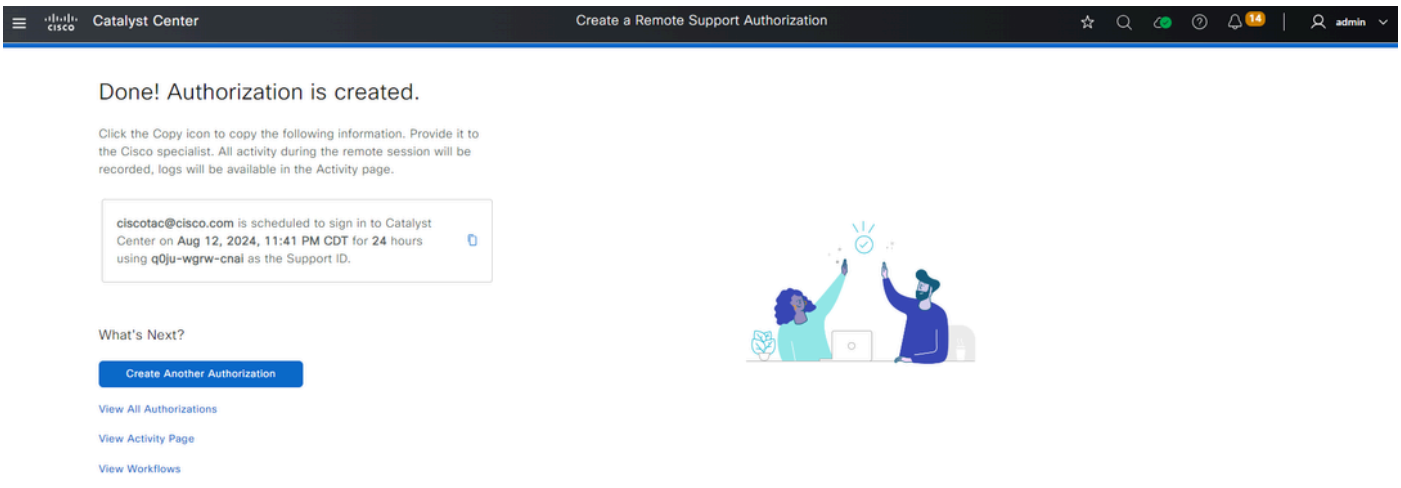


Click Create to proceed to the final step. You are redirected to a page that states the authorization has been created. Key items on this page include:

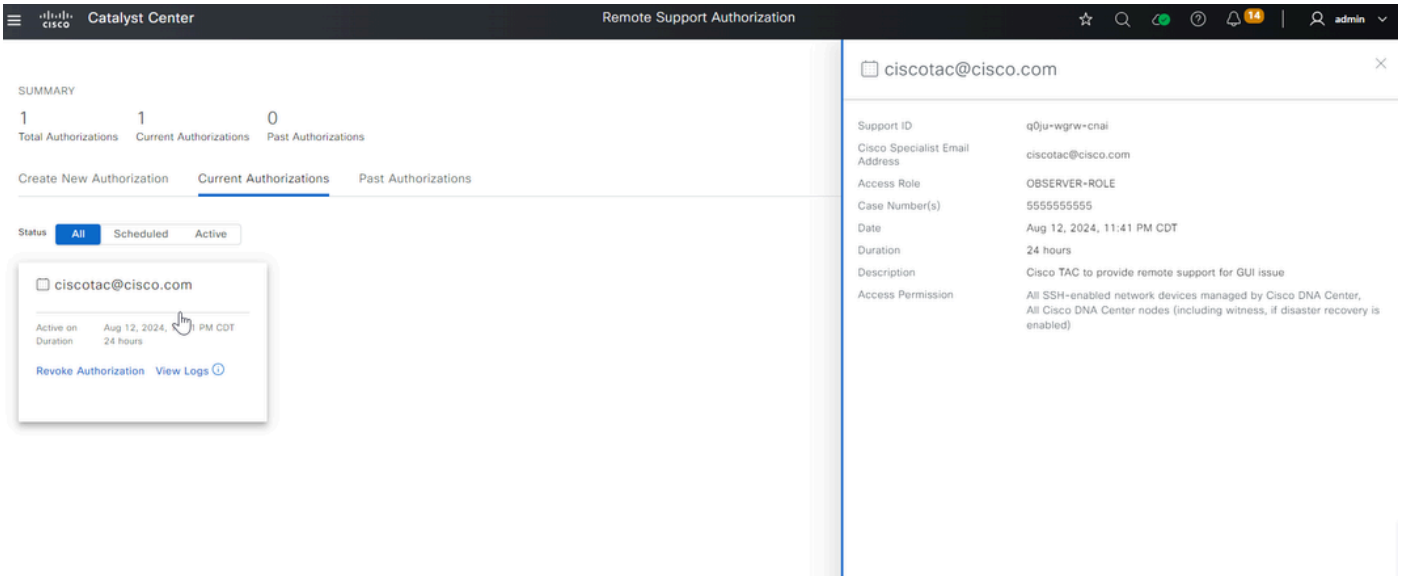
- TAC engineer email address
- Scheduled start time and duration of the authorization
- Support ID



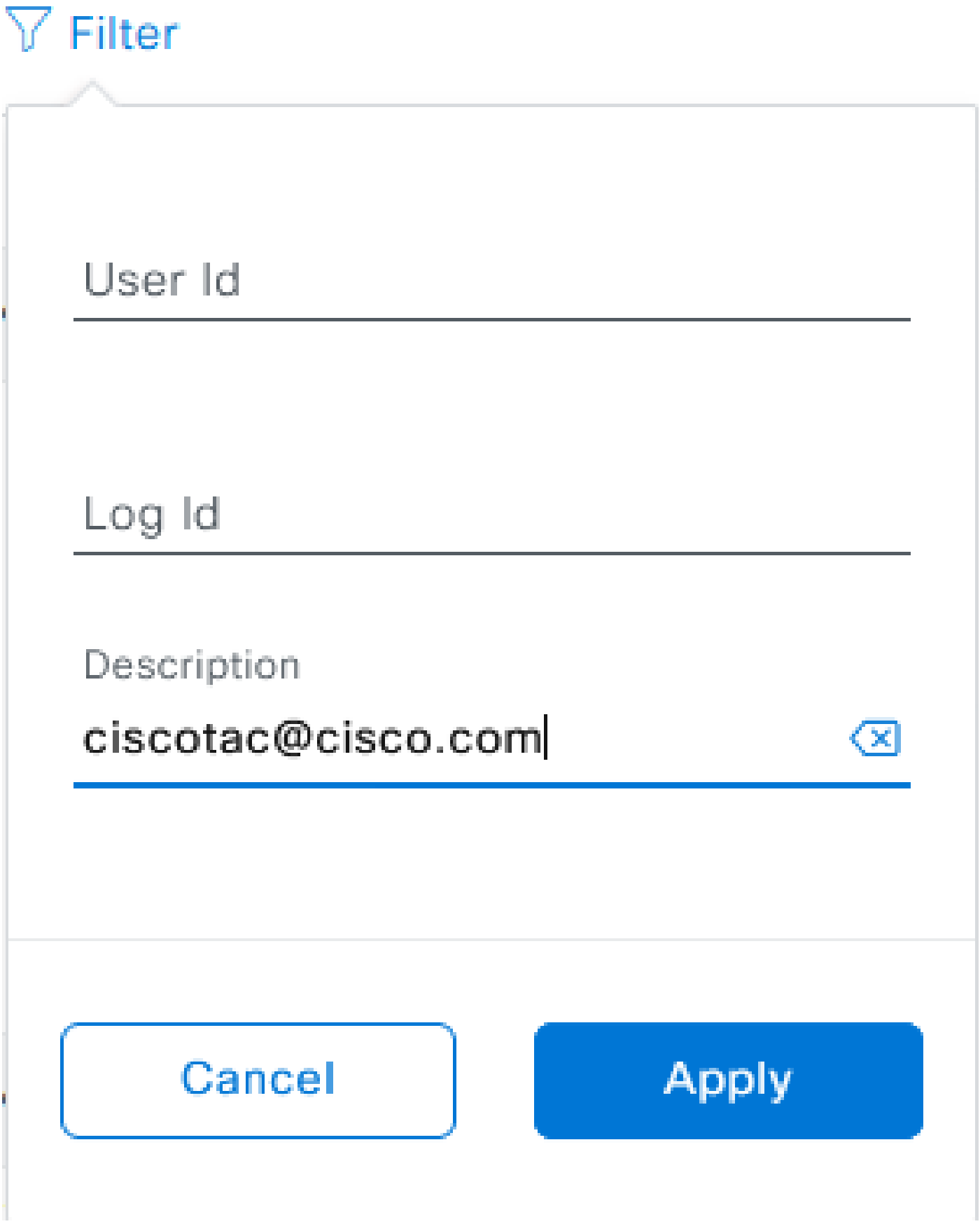
Note: Please note that the TAC engineer requires the Support ID to be able to connect with Cisco RADKit client to this authorization request. Copy the information provided and send it to the TAC engineer.



From this page you have the option to choose Create Another Authorization, View All Authorizations, View Activity Page, or View Workflows. If another authorization does not need to be created, you can choose View All Authorizations to see all current and past authorizations. View Activity Page redirects you to the Audit Logs page. View All Authorizations redirects you to the Current Authorizations page on the Remote Support Authorization section. You can view All, Scheduled, or Active authorizations. Click on an authorization to open a side window that displays the settings configured with the Create a Remote Support Authorization workflow.



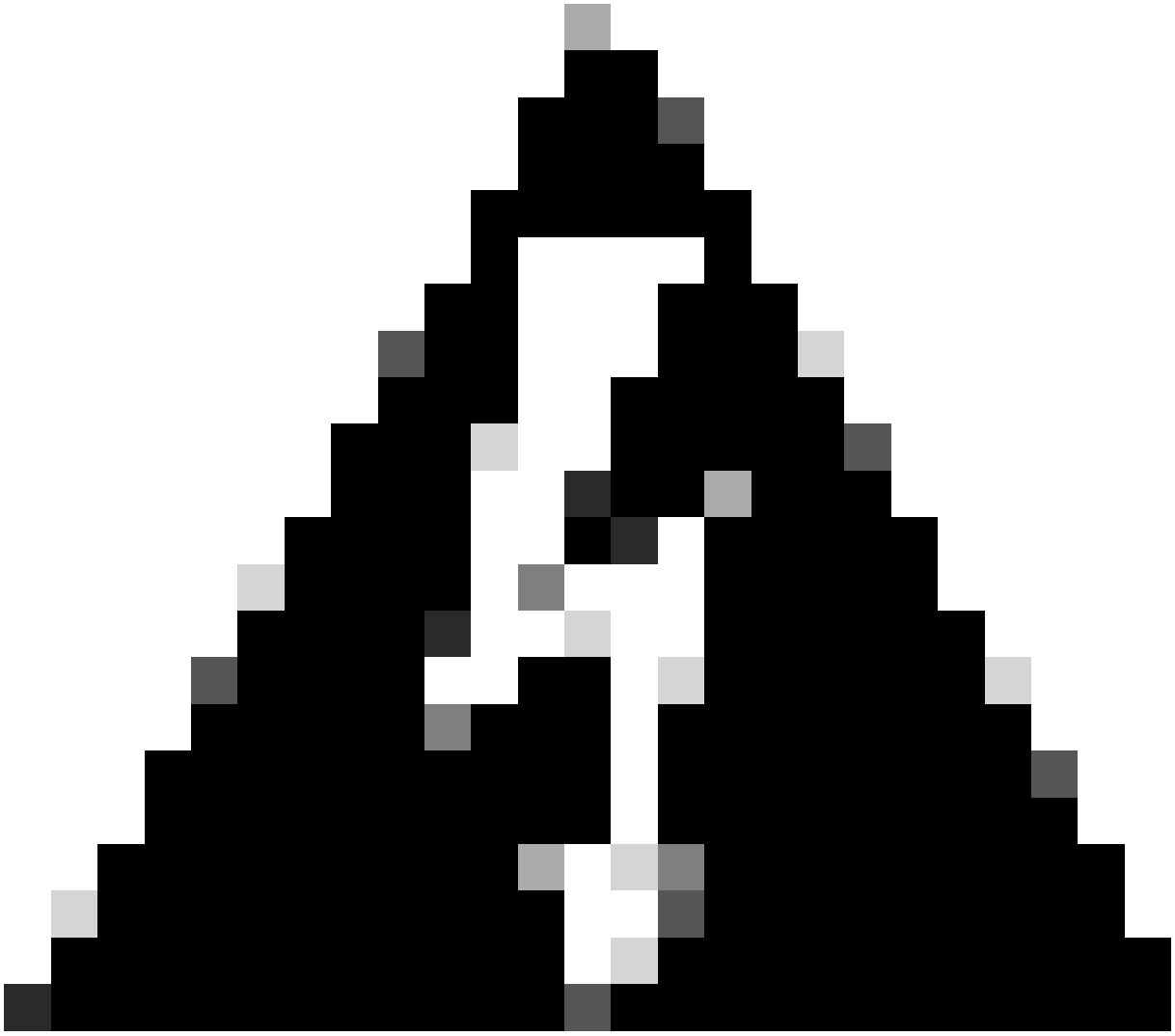
You can choose to cancel the authorization or to view the audit logs of what the TAC engineer has done with your deployment. You can choose to switch to the Past Authorizations tab to get historical information on previous authorizations. Choose View Logs to be redirected to the Audit Logs page. From the Audit Logs page, you can choose Filter, then filter by Description with the email address of the TAC engineer.



Choose Apply. This adds a filter based on the TAC engineer's email address as it shows in the description of the audit logs when Cisco RADKit is used to remote into the deployment.

Mar 21, 2023 23:56 PM (CDT)	Interactive Session Started for Device [[redacted]] by Remote Support User [ciscotac@cisco.com]	INFO	Info	system
Mar 21, 2023 23:57 PM (CDT)	Executing command... on the device [redacted]	INFO	Info	system
Mar 21, 2023 23:57 PM (CDT)	Executing command...show version on the device [redacted]	INFO	Info	system
Mar 21, 2023 23:57 PM (CDT)	Executing command... on the device [redacted]	INFO	Info	system
Mar 21, 2023 23:57 PM (CDT)	Executing command... on the device [redacted]	INFO	Info	system
Mar 21, 2023 23:57 PM (CDT)	Executing command...exit on the device [redacted]	INFO	Info	system
Mar 21, 2023 23:58 PM (CDT)	Closing connection on the device [redacted] on the device [redacted]	INFO	Info	system
Mar 21, 2023 23:58 PM (CDT)	Interactive Session Completed for Device [[redacted]] by Remote Support User [ciscotac@cisco.com]	INFO	Info	system
Mar 21, 2023 23:56 PM (CDT)	Login was successful for Remote Support User [ciscotac@cisco.com]	INFO	Info	system

From the audit logs you can see exactly what the TAC engineer did and when they signed on.



Warning: Remote Support Authorization feature of Cisco Catalyst Center version 2.3.7.6 is tested with Cisco RADKit client 1.6.11.
