Configure Cisco DNA Center Remote Support Authorization Feature

Contents

Introduction

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

Prerequisites

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

- Cisco DNA Center must be version 2.3.5.x or higher.
- The Support Services package needs to be installed in Cisco DNA 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 DNA Center version 2.3.3.x but has limited functionality. Only network device access is permitted, Cisco DNA Center CLI access is not present in this earlier version.

Description

Cisco RADKit (radkit.cisco.com) provides secure interactive connectivity to remote terminals and Web UIs. Cisco RADKit features are integrated in Cisco DNA Center and is called Remote Support Authorization. When users utilize the Remote Support Authorization feature, users can have Cisco's TAC remote into their Cisco DNA Center environment to help gather information or troubleshoot issues. This helps reduce the amount of time users need to sit on video calls as the 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 DNA Center, they prompt for credentials. Remote Support Authorization does not automate the handling of these credentials, so you may need to share these credentials with the support engineer.

- Through the Remore Support Authorization service it is not possible to connect to the Graphical User Interface (GUI) of the Cisco DNA Center or to any GUI of the network devices.

- It is not possible to provide remote access to devices that are not in the Cisco DNA Center inventory but that may be necessary for troubleshooting (e.g. ISE).

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

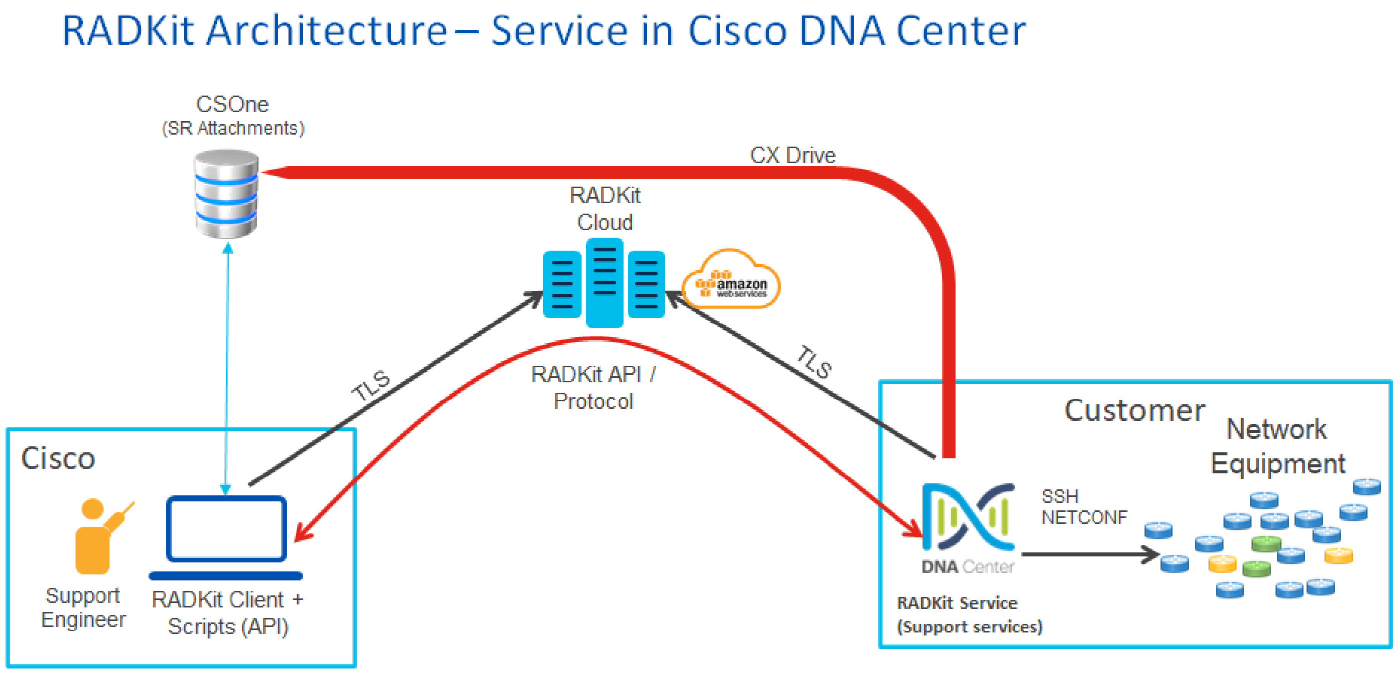
- By creating an authorization you allow access to all devices in the Cisco DNA Center inventory. It is not possible to restrict access to certain network devices.

To overcome these limitations, you may 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 DNA 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 DNA Center environment, the Cisco RADKit client uses the Support ID to connect to the Cisco DNA 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.
4. Create a new authorization.

Step 1

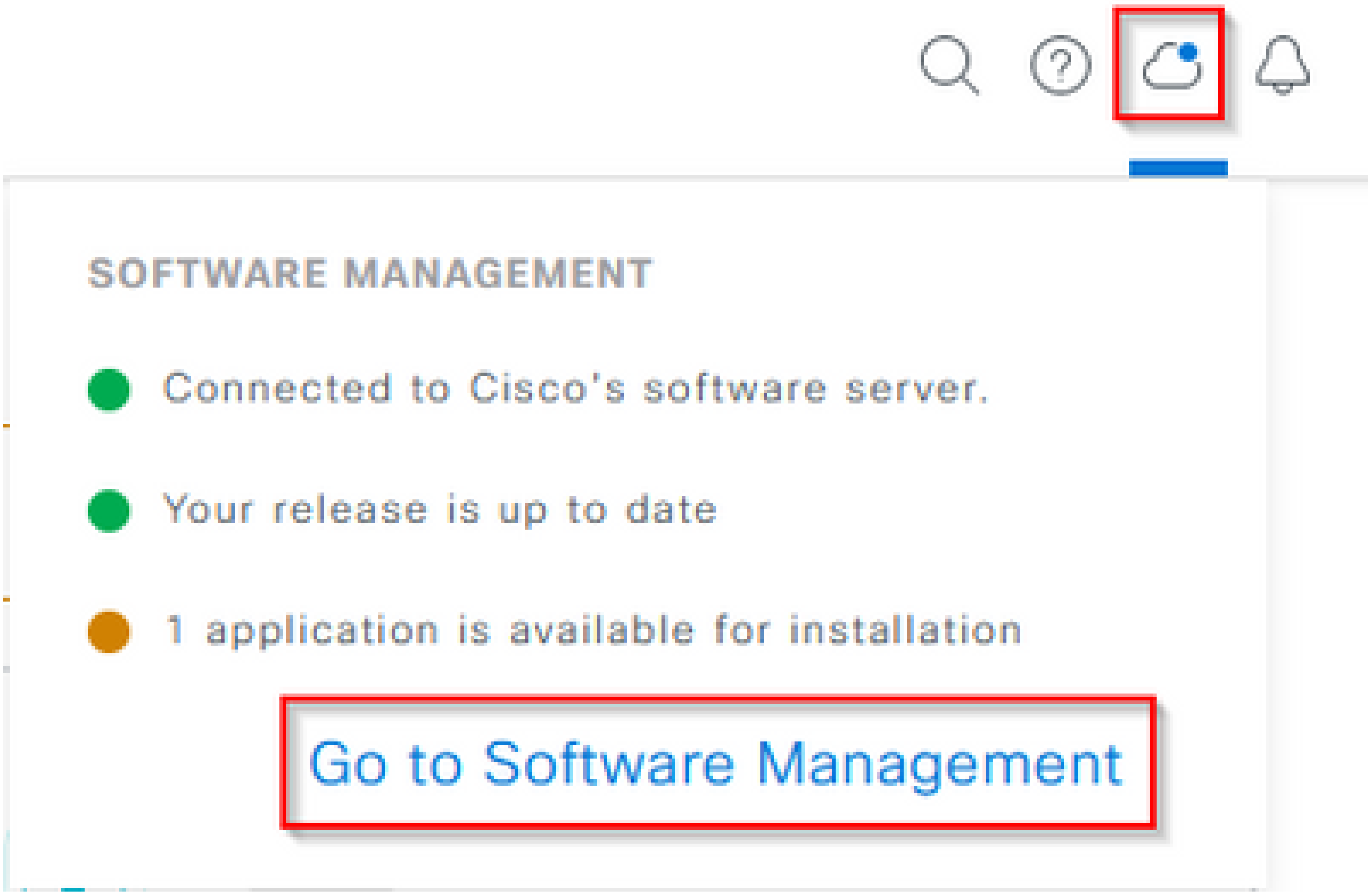
For Remote Support Authorization to work Cisco DNA Center connector must be able to communicate with the AWS connector. To ensure this communication, this URL must be allowed through the firewall if one is configured:
wss://prod.radkit-cloud.cisco.com:443

Tip: For more information on specific ports and URLs that are required to be allowed/open for

Cisco DNA 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 DNA 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 DNA Center UI. From the Home screen of the Cisco DNA Center UI select the cloud icon at the top-right of the screen and choose Go to Software Management.



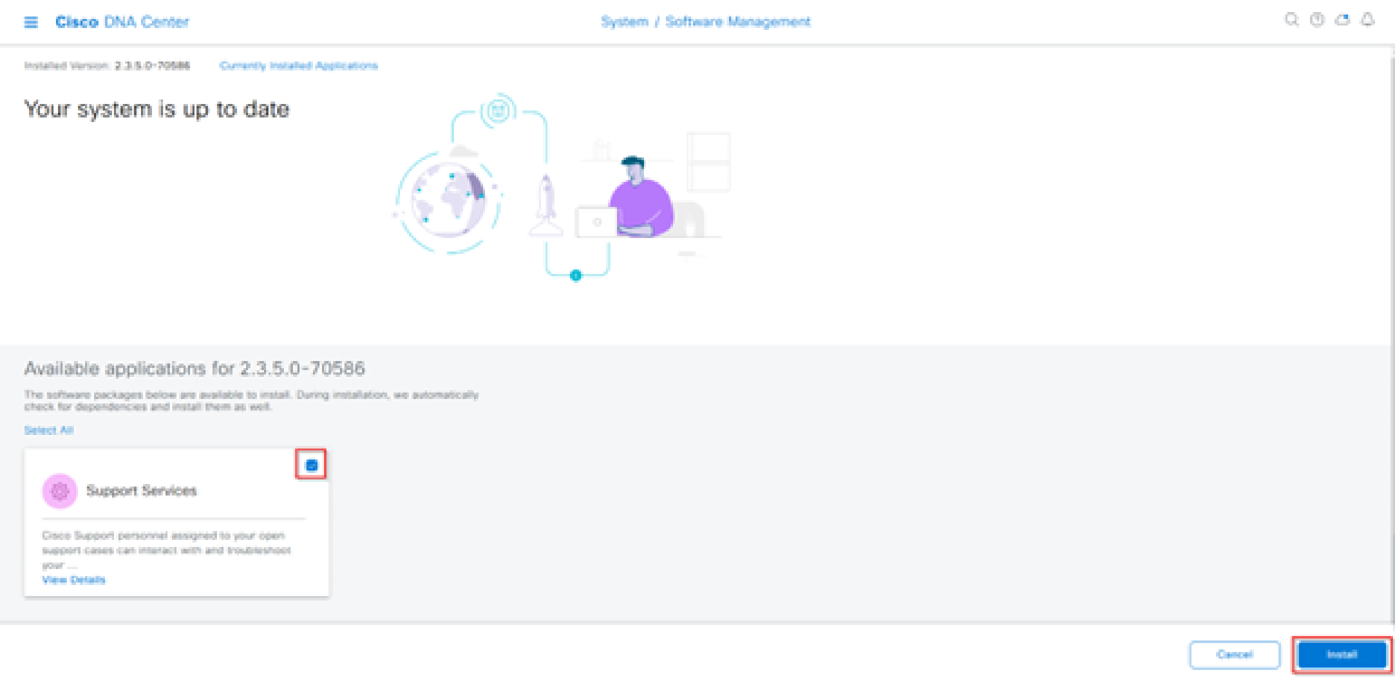
SOFTWARE MANAGEMENT

● Connected to Cisco's software server.

● Your release is up to date

● 1 application is available for installation

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.



Cisco DNA Center
System / Software Management
Installed Version: 2.3.5.0-70586
Currently Installed Applications
Select All
View Details
Cancel
Install

Your system is up to date

Available applications for 2.3.5.0-70586

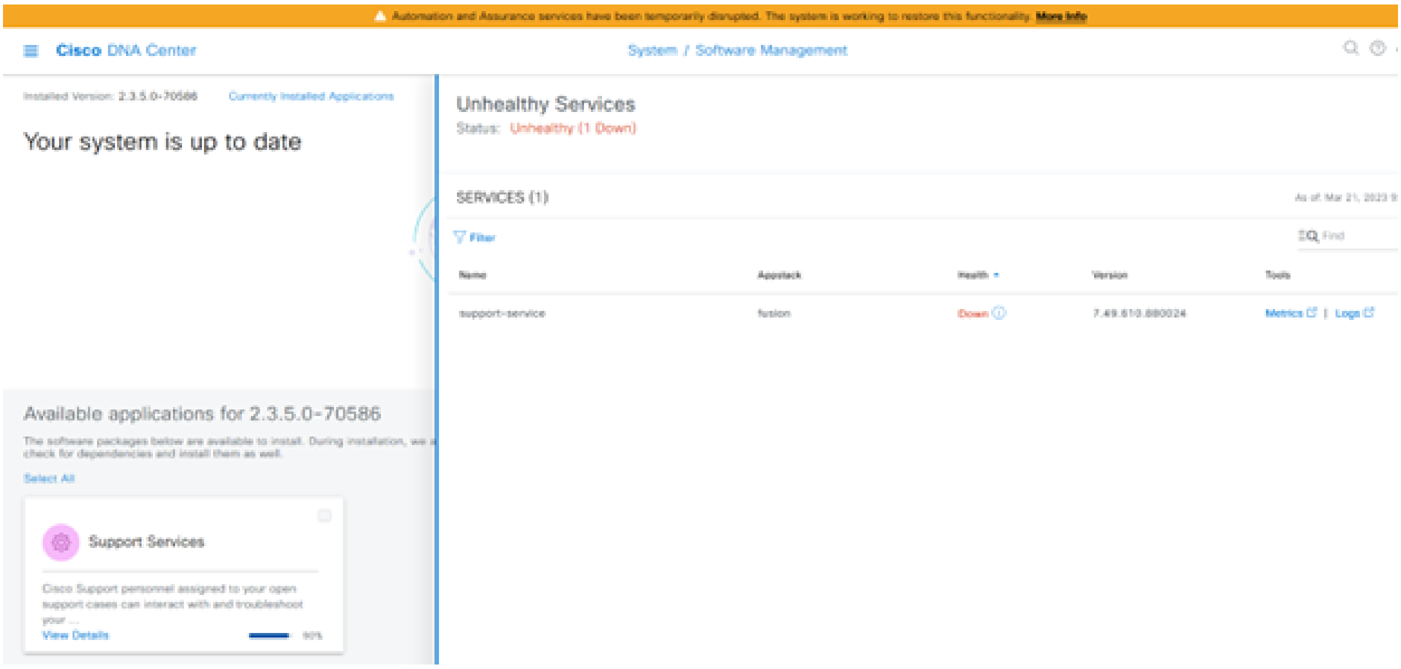
The software packages below are available to install. During installation, we automatically check for dependencies and install them as well.

Support Services ☑

Cisco Support personnel assigned to your open support cases can interact with and troubleshoot your ...

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.



Cisco DNA Center
System / Software Management
Installed Version: 2.3.5.0-70586
Currently Installed Applications
Select All
View Details
90%
Filter
Find

Automation and Assurance services have been temporarily disrupted. The system is working to restore this functionality. More Info

Your system is up to date

Available applications for 2.3.5.0-70586

The software packages below are available to install. During installation, we a... check for dependencies and install them as well.

Support Services

Cisco Support personnel assigned to your open support cases can interact with and troubleshoot your ...

Unhealthy Services

Status: Unhealthy (1 Down)

SERVICES (1)

As of: Mar 21, 2023 9

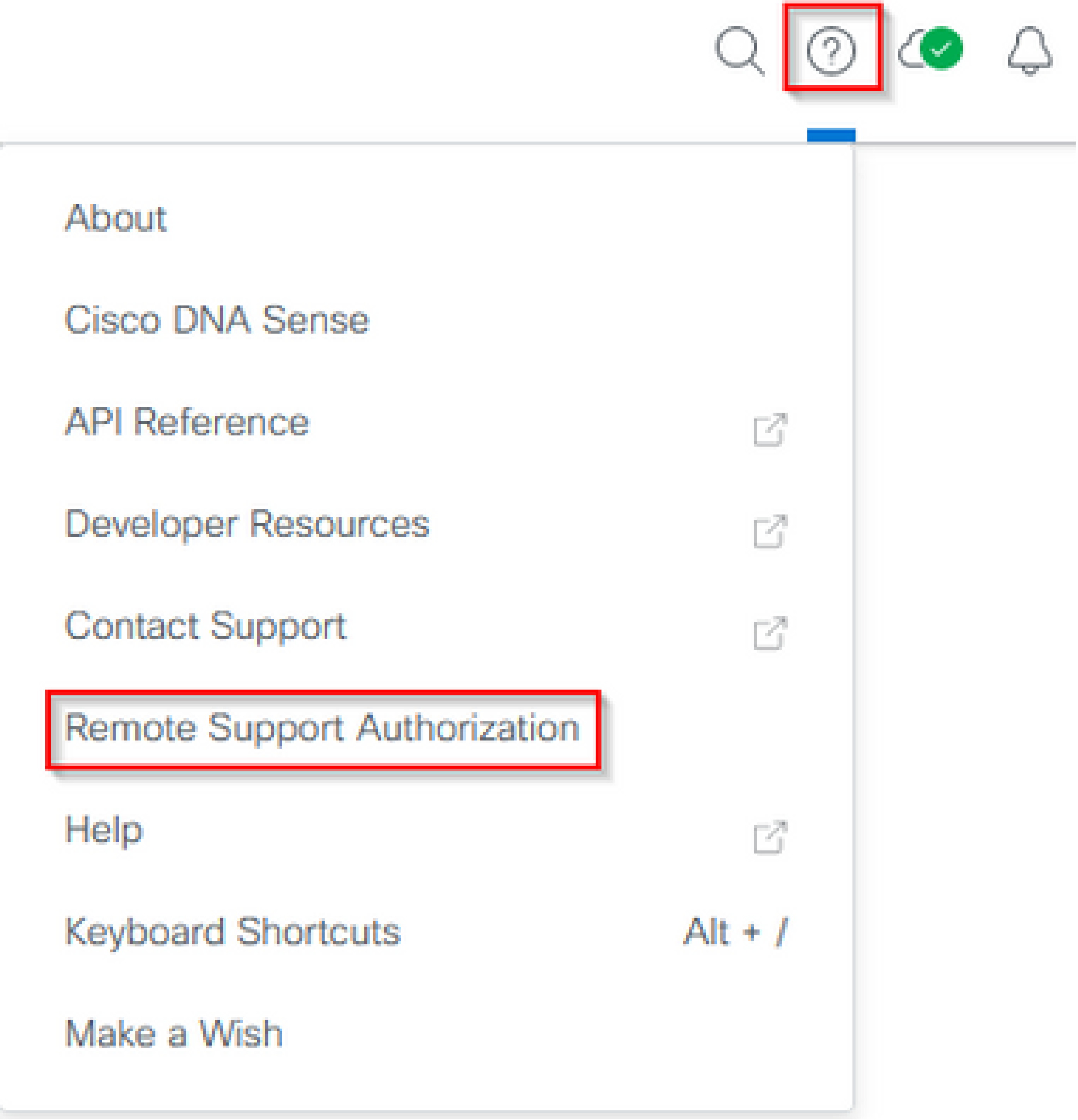
Name	Appstack	Health	Version	Tools
support-service	fusion	Down	7.49.610.880024	Metrics | Logs

After roughly 10 to 20 minutes, the new pod will be 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 will 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 DNA Center UI. From the list, choose Remote Support Authorization.

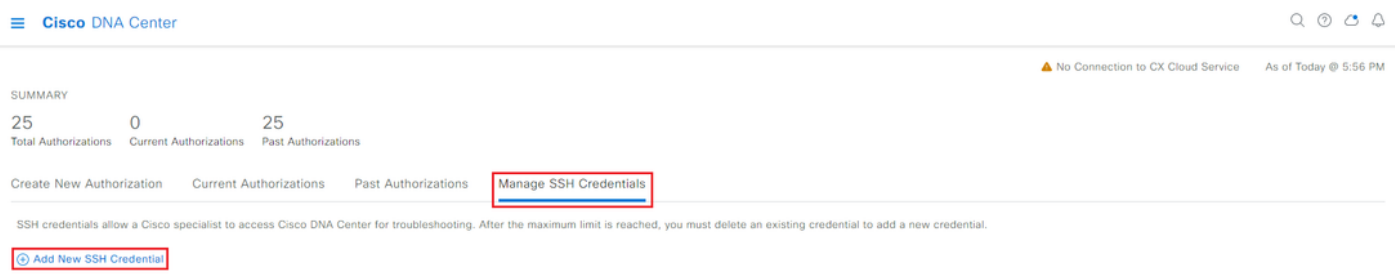
Note: Please note that Remote Support Authorization only shows after the Support Services package has been installed and the browser has been refreshed. Please refer to step 2 on how to accomplish this.



You are redirected to the Remote Support Authorization page. Four tabs are listed:

- Create New Authorization
- Current Authorizations
- Past Authorizations
- Manage SSH Credentials

Navigate to the Manage SSH Credential tab. Choose Add New SSH Credential.



Cisco DNA Center

No Connection to CX Cloud Service   As of Today @ 5:56 PM

SUMMARY

25 Total Authorizations   0 Current Authorizations   25 Past Authorizations

Create New Authorization   Current Authorizations   Past Authorizations   Manage SSH Credentials

SSH credentials allow a Cisco specialist to access Cisco DNA Center for troubleshooting. After the maximum limit is reached, you must delete an existing credential to add a new credential.

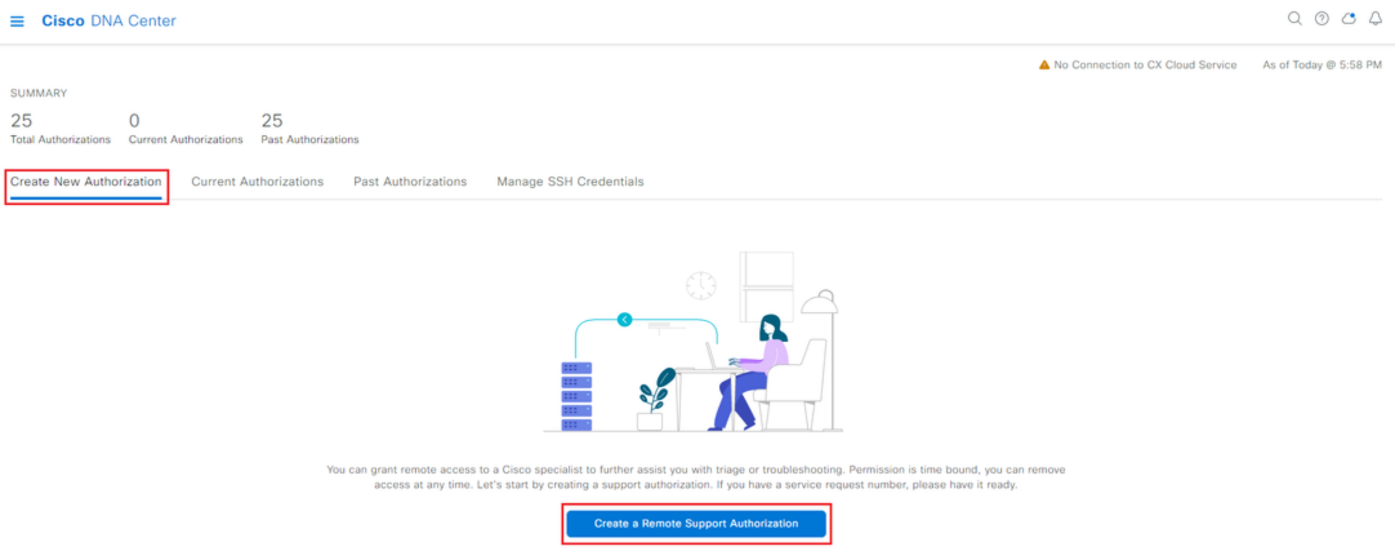
⊕ Add New SSH Credential

A new window opens. Enter in the current SSH password for the Cisco DNA Center appliance and a description. The password must match what is currently used to SSH into the Cisco DNA Center appliance. Choose Add. An entry now shows under EXISTING SSH CREDENTIALS.

Note: Please note that for single node deployments, only one credential can be created. For three node deployments, up to three credentials can be created. However, if the SSH password is the same for all three nodes, only one credential must be created.

Step 4

Navigate to the Create New Authorization tab in the Remote Support Authorization page. Choose Create a Remote Support Authorization.



SUMMARY

25	0	25
Total Authorizations	Current Authorizations	Past Authorizations

You can grant remote access to a Cisco specialist to further assist you with triage or troubleshooting. Permission is time bound, you can remove access at any time. Let's start by creating a support authorization. If you have a service request number, please have it ready.

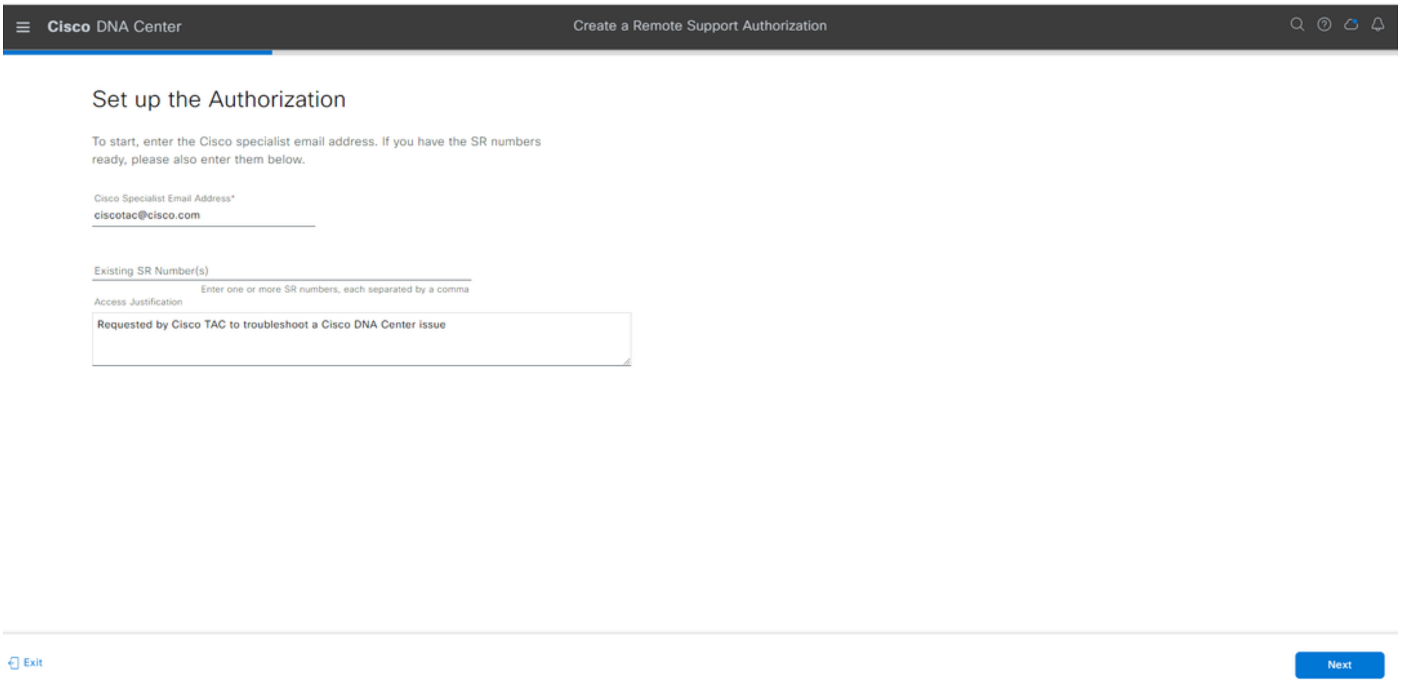
You are redirected to a workflow page to start the setup of the authorization. You must enter in the TAC engineer’s email address. For example: “ciscotac@cisco.com”.

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.



Set up the Authorization

To start, enter the Cisco specialist email address. If you have the SR numbers ready, please also enter them below.

Cisco Specialist Email Address*: ciscotac@cisco.com

Existing SR Number(s)

Enter one or more SR numbers, each separated by a comma

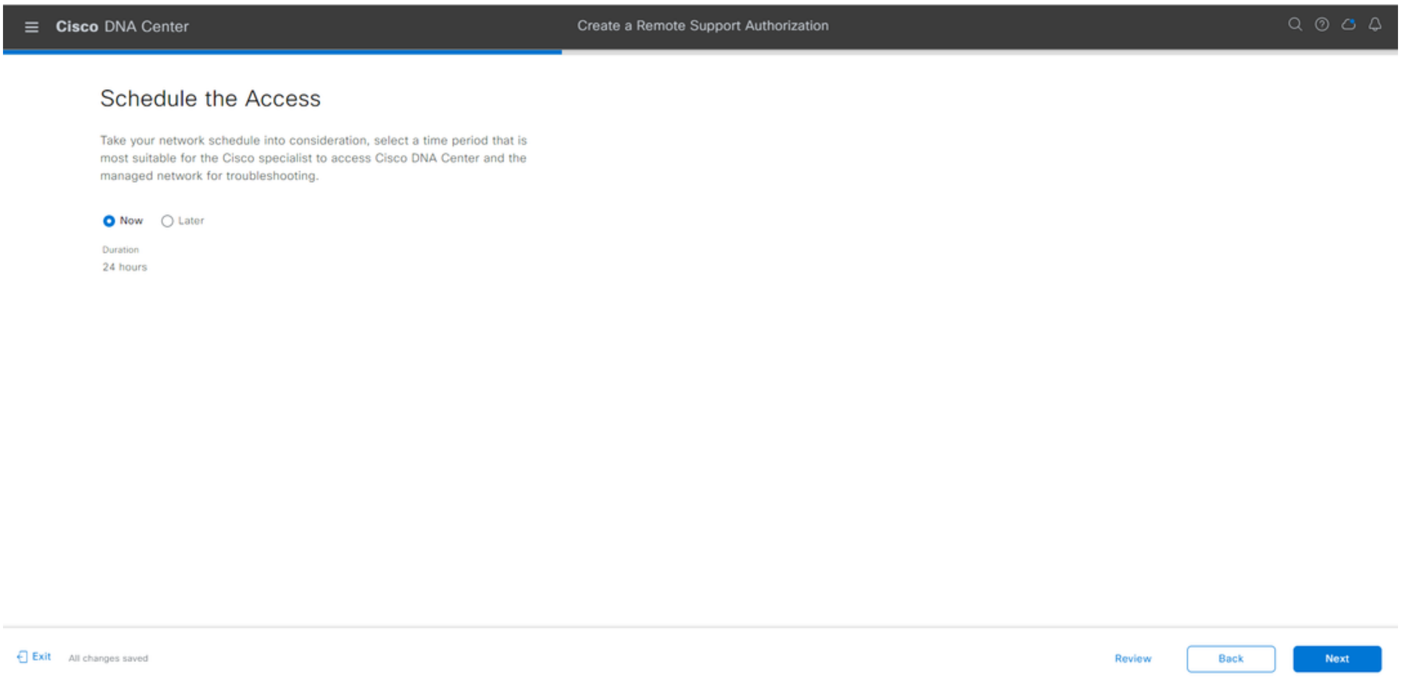
Access Justification: Requested by Cisco TAC to troubleshoot a Cisco DNA Center issue

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.

Choose Now, then click Next.



Schedule the Access

Take your network schedule into consideration, select a time period that is most suitable for the Cisco specialist to access Cisco DNA Center and the managed network for troubleshooting.

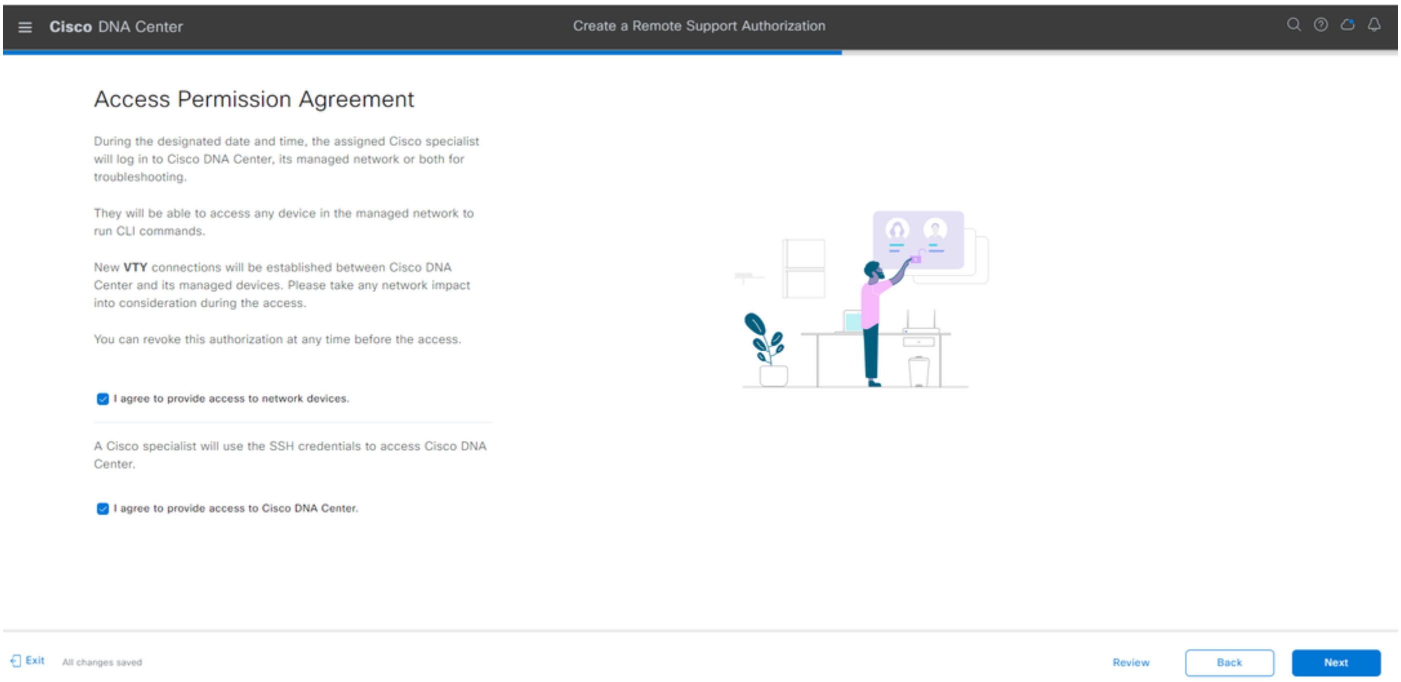
● Now ○ Later

Duration
24 hours

You are redirected to the Access Permission Agreement page. This page has two options:

- New VTY connections between Cisco DNA Center and the devices managed in Inventory.
- Access to the CLI of the Cisco DNA Center appliance(s)

To establish an SSH connection with the network devices managed by Cisco DNA Center, the first option must be selected. If this option is not selected, TAC engineers will not be able to SSH into the devices with Cisco RADKit. To establish an SSH connection to the Cisco DNA Center appliance(s) then the second option must be selected. If this option is not selected, TAC engineers will not be able to access the Cisco DNA 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.



Access Permission Agreement

During the designated date and time, the assigned Cisco specialist will log in to Cisco DNA Center, its managed network or both for troubleshooting.

They will be able to access any device in the managed network to run CLI commands.

New **VTY** connections will be established between Cisco DNA Center and its managed devices. Please take any network impact into consideration during the access.

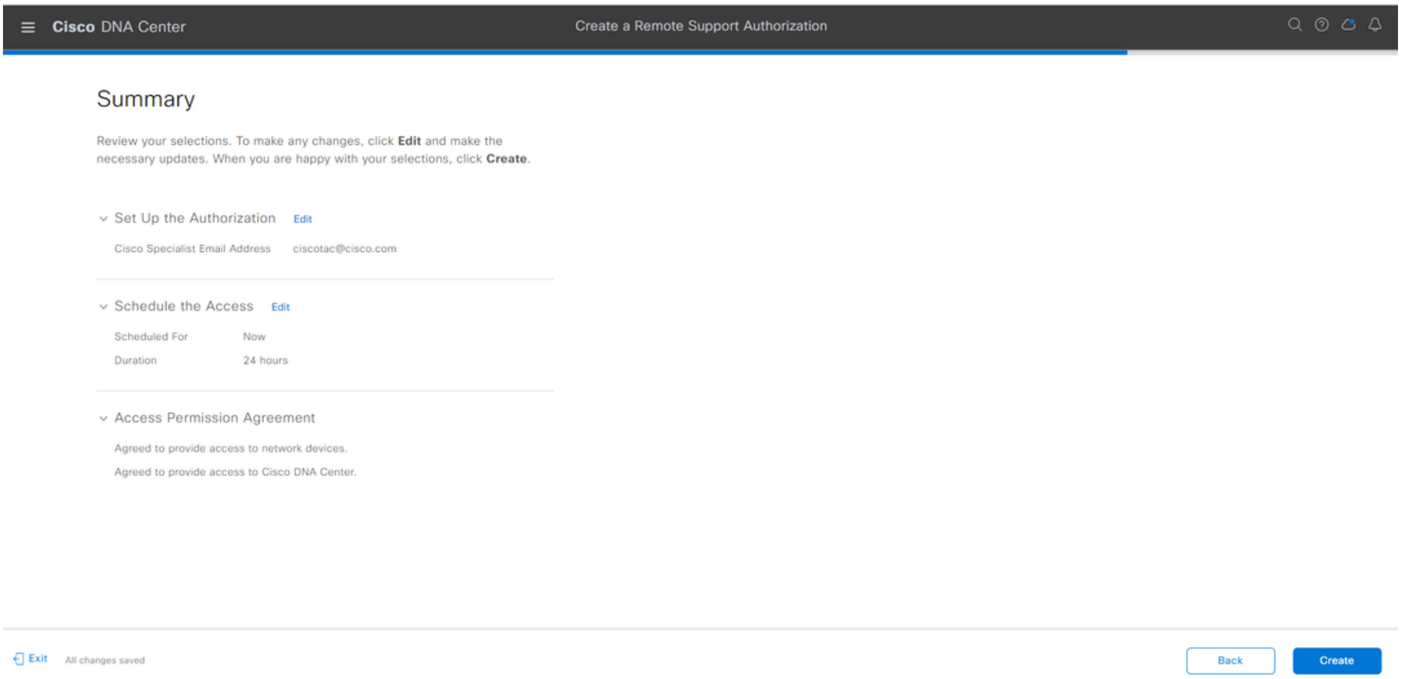
You can revoke this authorization at any time before the access.

☑ I agree to provide access to network devices.

A Cisco specialist will use the SSH credentials to access Cisco DNA Center.

☑ I agree to provide access to Cisco DNA Center.

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.



Summary

Review your selections. To make any changes, click **Edit** and make the necessary updates. When you are happy with your selections, click **Create**.

Set Up the Authorization

Cisco Specialist Email Address ciscotac@cisco.com

Schedule the Access

Scheduled For Now
Duration 24 hours

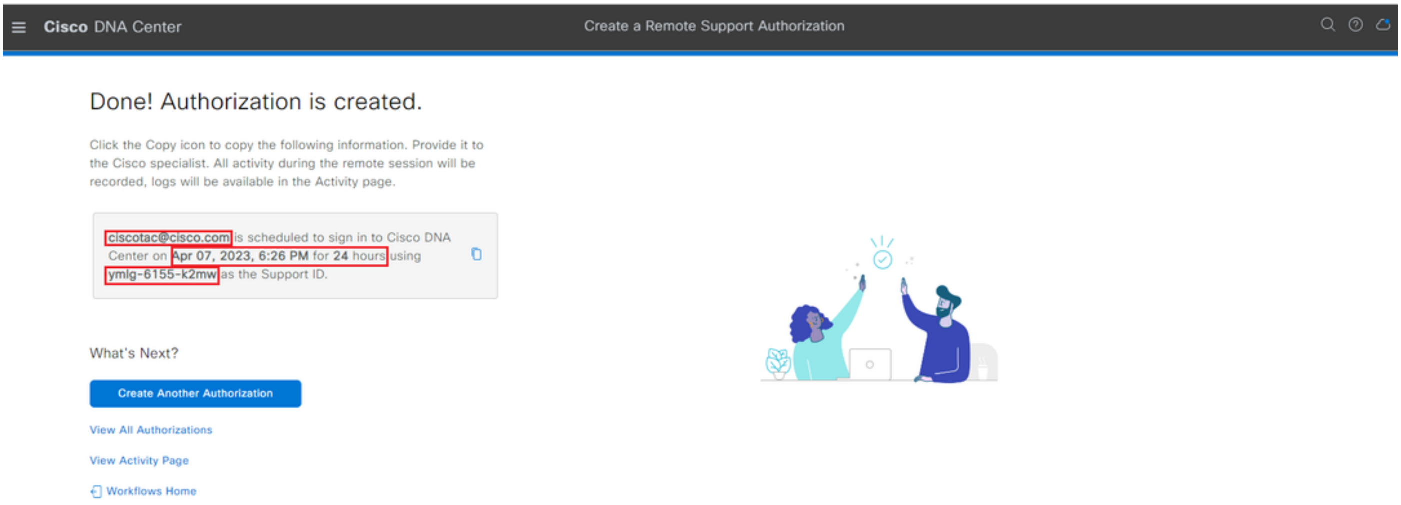
Access Permission Agreement

Agreed to provide access to network devices.
Agreed to provide access to Cisco DNA Center.

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's 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.



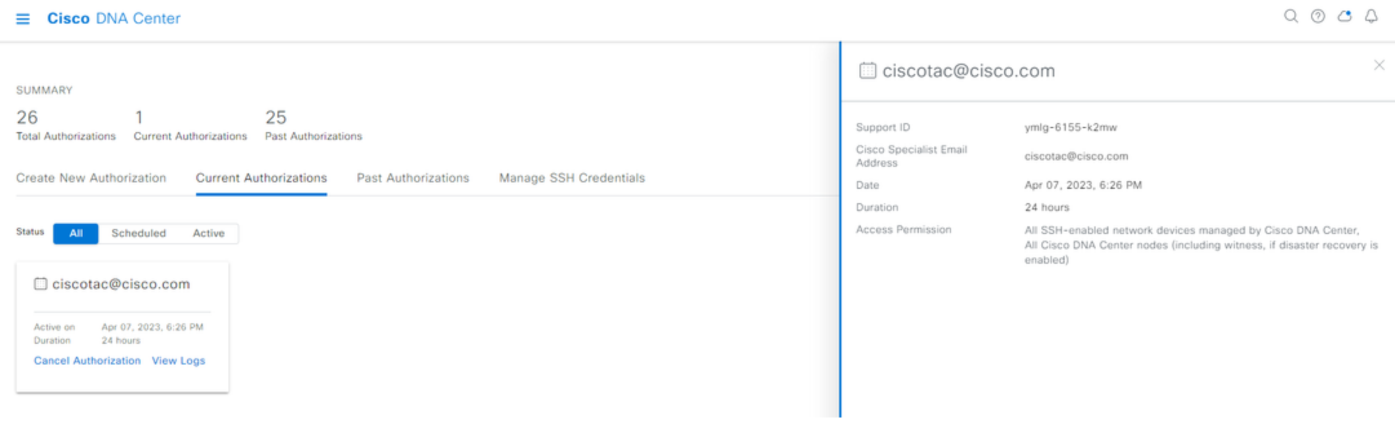
Done! Authorization is created.

Click the Copy icon to copy the following information. Provide it to the Cisco specialist. All activity during the remote session will be recorded, logs will be available in the Activity page.

ciscotac@cisco.com is scheduled to sign in to Cisco DNA Center on Apr 07, 2023, 6:26 PM for 24 hours using ymlg-6155-k2mw as the Support ID.

What's Next?

From this page you have the option to choose Create Another Authorization, View All Authorizations, View Activity Page, or Workflow Home. 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.



SUMMARY

26	1	25
Total Authorizations	Current Authorizations	Past Authorizations

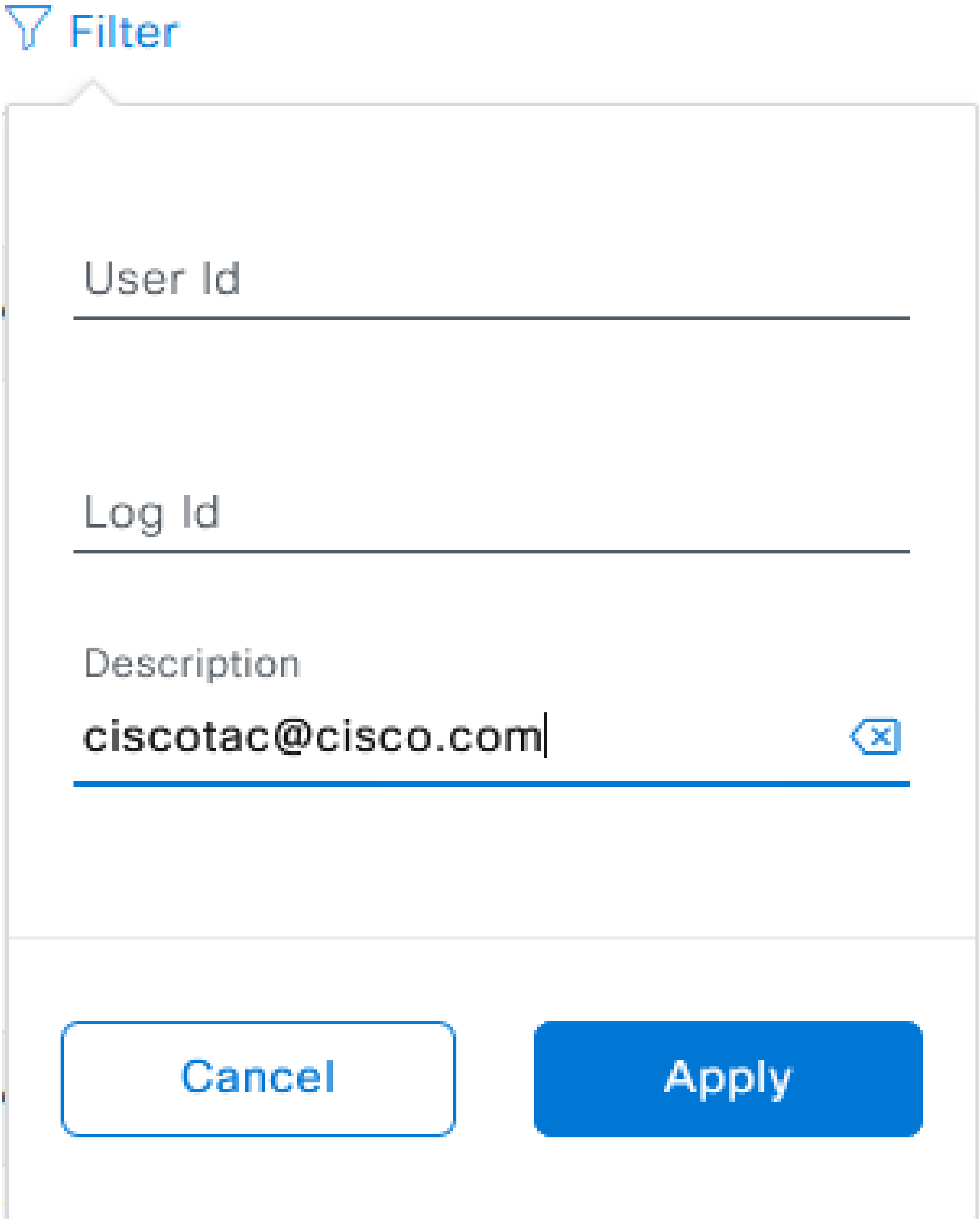
ciscotac@cisco.com

Active on Apr 07, 2023, 6:26 PM
Duration 24 hours

ciscotac@cisco.com

Support ID	ymlg-6155-k2mw
Cisco Specialist Email Address	ciscotac@cisco.com
Date	Apr 07, 2023, 6:26 PM
Duration	24 hours
Access Permission	All SSH-enabled network devices managed by Cisco DNA Center, All Cisco DNA Center nodes (including witness, if disaster recovery is enabled)

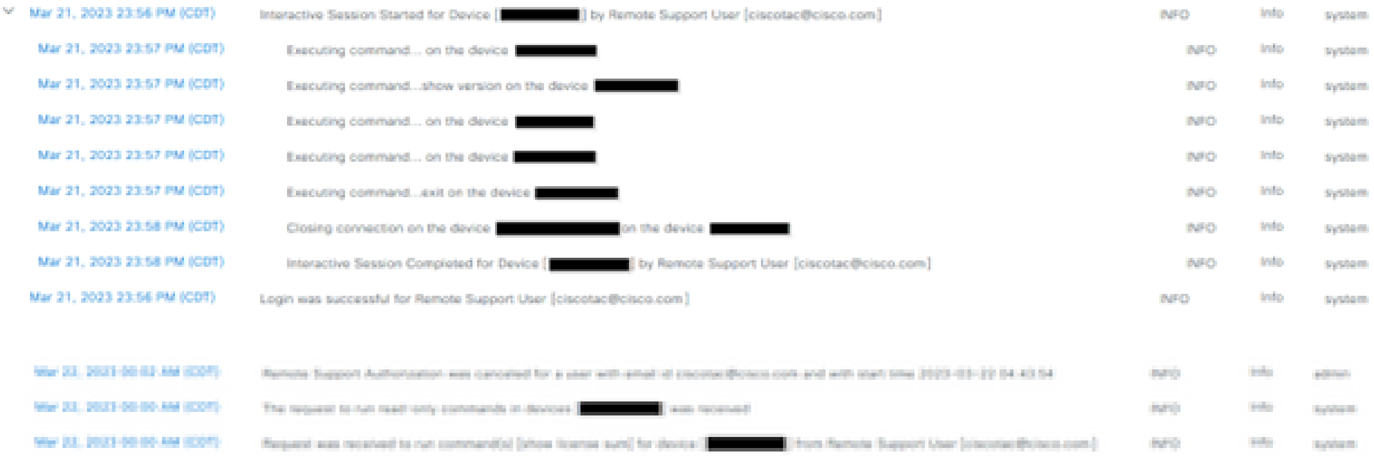
You can choose to cancel the authorization or to view the audit logs of what the TAC engineer has done with your deployment. You can choose to switch to the Past Authorizations tab to get historical information on previous authorizations. Choose View Logs to be redirected to the Audit Logs page. From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



Description

ciscotac@cisco.com

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

Mar 22, 2023 00:02 AM (CDT)    Remote Support Authorization was canceled for a user with email id ciscotac@cisco.com and with start time 2023-03-22 04:43:54    INFO    Info    admin
Mar 22, 2023 00:00 AM (CDT)    The request to run read-only commands in devices [[redacted]] was received    INFO    Info    system
Mar 22, 2023 00:00 AM (CDT)    Request was received to run command(s) [show license sum] for device [[redacted]] from 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 DNA Center version 2.3.5.x is tested with Cisco RADKit client 1.4.x.