

RADKit: Automate your network securely and efficiently

CISCO Live !

Linda Wang
Senior Technical Leader
Customer Delivery Engineering

Cisco Webex App

Questions?

Use Cisco Webex App to chat with the speaker after the session

How

- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until 14 November 2025.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKOPS-3065>

Agenda

- 01 Introduction – Why RADKit ?
- 02 RADKit Overview
- 03 RADKit in Action (live demo)
- 04 Deploying RADKit (demo)
- 05 Importing Inventory (demo)
- 06 RADKit in Cisco Catalyst Center(demo)
- 07 Conclusion

Who is Linda?

- A problem solver, technical leader
- **Double CCIE** R&S, Security# **45307**
- Over **12** years @Cisco TAC
- AI enthusiast, pioneer
- A proud Mentor
- Working Mom of two young age kids
- A Foodie and **explorer**
- Always curious

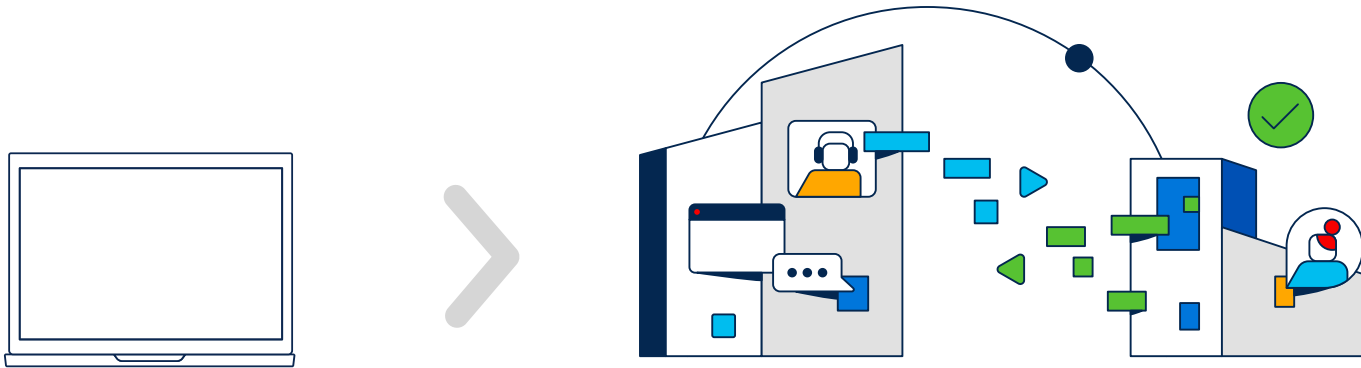


Introduction

Remote Automation Development Kit (RADKit)

Single window into the entire network for insights and connected support

Allows you and your customers to focus on critical business, not busywork



Traditional

Manage or troubleshoot individual devices

RADKit Way

Manage or troubleshoot on an entire network or solution architecture

- One hybrid interface platform for real-time remote connectivity
- Maps network activity to users, devices or Service Requests
- Automates diagnosis and speeds time to resolution with less effort

RADKit for all Activities

Manual
Webex
Expensive VPNs
Field/Site visits

RADKit

Remote Operations
Efficiency & Timeliness
Automation

Effort & Delay

Customer Satisfaction

Any Problem ?

Engage your Support

Engage Cisco TAC

Engage Engineering

Managed/Advanced Services

Remediation

CI/CD

Validation

Changes

Software Upgrades

Network Optimization

Monitoring

Licensing

Automation

Connectivity



Automation

Remote Automation Development Kit (RADKit)

A set of ready-to-use tools and Python modules allowing efficient and scalable interactions with local or remote networks to eliminate 50% of total time spent in problem solving Lifecycle



Expedite SR resolution
Get more out of Cisco
Service



Securely connect and
interact with remote
devices

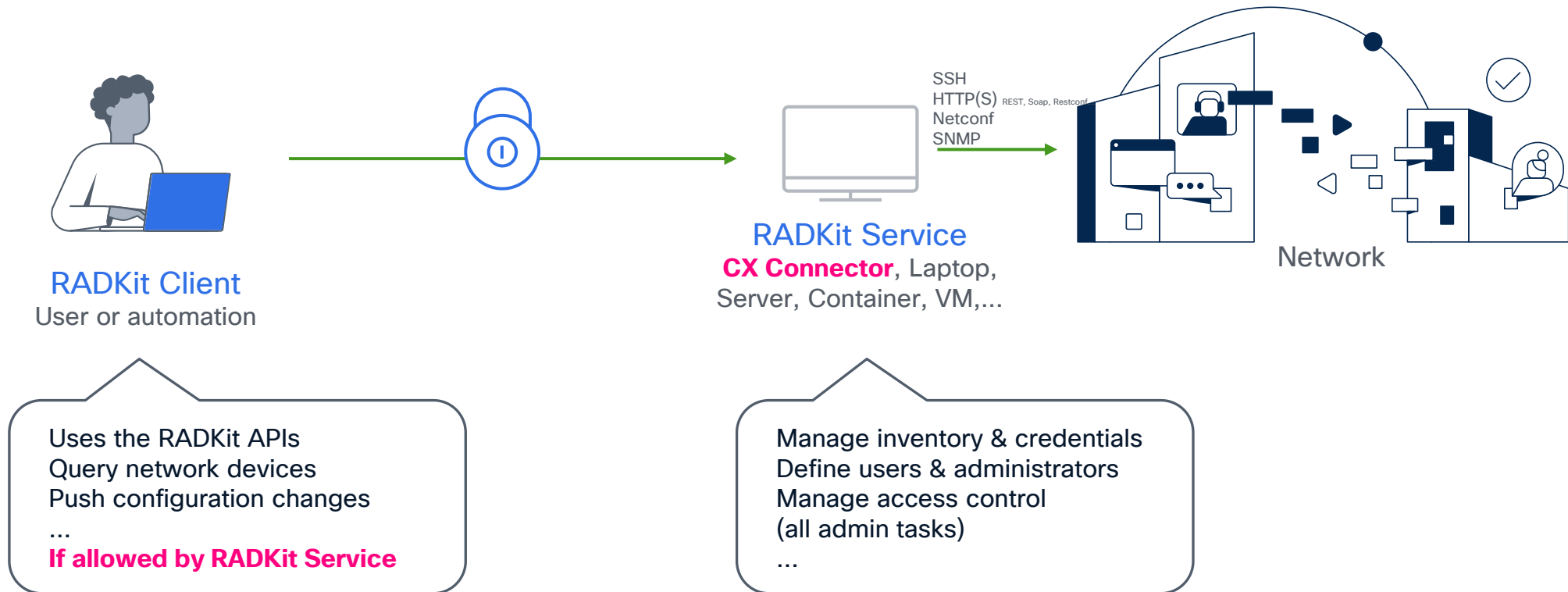


Powerful and easy
to use APIs for
automations

RADKit Minimal Architecture

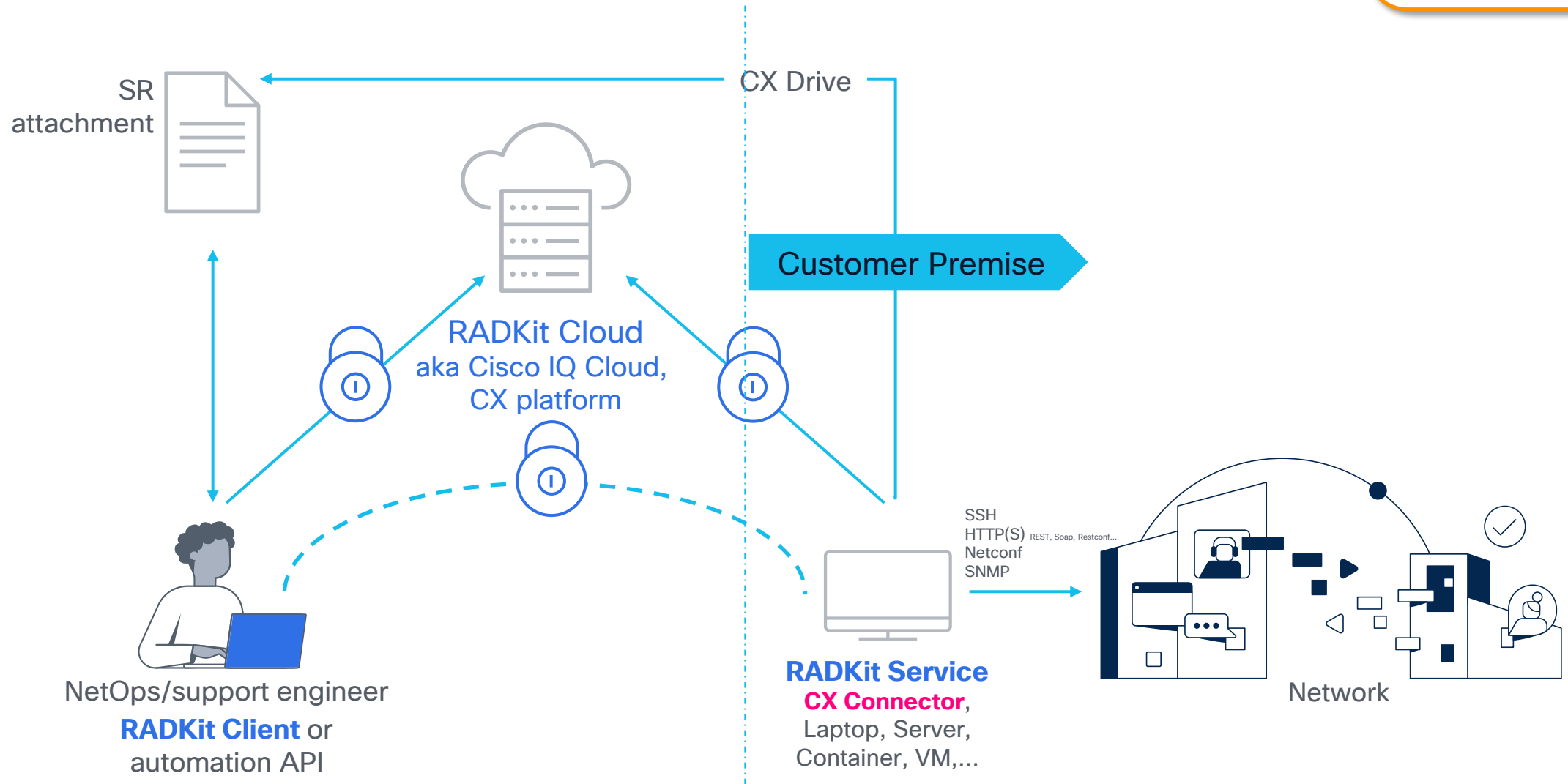
Airgap mode

CSDL Ready to Ship
Easy to deploy
Easy to learn



RADKit General Architecture

CSDL Ready to Ship
Easy to deploy
Easy to learn



RADKit Solution : What is in it for You ?

01

Secure Connectivity + Audit Trail allows TAC to react promptly under full customer supervision.

02

Role Based Access Control restricts TAC to specific devices.

03

No effort to capture or upload data to SR. Everything is handled by RADKit

04

Halve Webex time with TAC.

Secure & Trusted but verifiable means to authorize TAC to collect device data, and with this solving various challenges faced during remote triage via Webex like:

- Long Webex Hours, Customer tied to sharing screens
- Customer having to extract/file transfer
- Keyboard mapping issues/delays
- Scheduling/Time Zone wait times reduced
- With automation capabilities, address devices at scale and hence the possibilities for host of use cases

Enhanced Cisco Service capabilities

- ✓ Solve/Simplify challenges around data extraction/ collection and device updates
- ✓ Improved service restoration time, training time

20% – 80%*
Reduction in TFR

50 – 80%*
Customer Effort Reduction

Customer Effort Reduction [Freed from long Webex and data collection & File transfers]

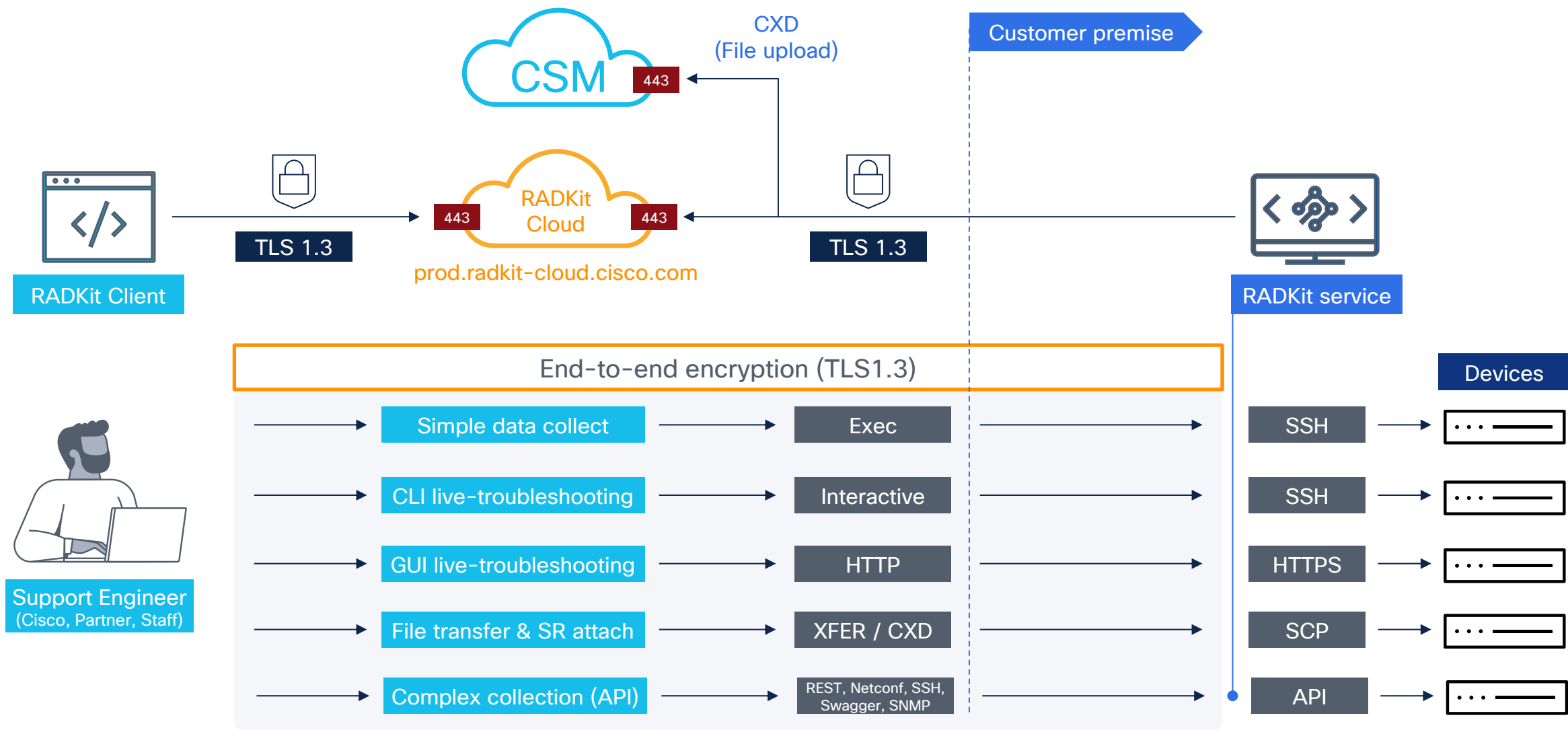


*Note:

- deriving uniform ROI/Depends on extent RADKit capabilities utilized
- No known standard measure of “effort”. Effort comprises attendance.

RADKit Overview

RADKit capabilities



Security & Data Privacy

[More at radkit.cisco.com](https://radkit.cisco.com) – FAQ section

- RADKit is CSDL compliant
 - Meets all stringent security, and data privacy criterias
 - Coding best practices, software inspection (static and runtime), signed software
- All data is encrypted at rest and in-transit
 - Strong algorithms and parameters (TLS1.3, RSA-4096, ECDH, ...)
- RADKit does not store any user data in the cloud
 - Only accelerates data capture and transfer between historical parties (troubleshooter and case attachment)
 - The data is opaque to the cloud service thanks to end-to-end encryption
- All data remains the customer property
 - Particularly the inventory and the credentials
- Only customer-authorized users can connect
 - Set duration, local policies. Cannot be overridden by Cisco
- Extensive audit trail
 - Customer property; cannot be altered by Cisco

RADKit in Action Demo

Demo List

Controllers	Network Devices
DNAC	IOS XE (IOS and derivatives)
ACI APIC	NX OS
Wireless Lan Controller	IOS XR
VManage	Linux
Identity Service Engine	Access Point
Firewall Management Console	cEdge

RADKit Service installation on Windows

RADKit - Installation on Windows

- <https://radkit.cisco.com> > Downloads
- Select the latest release and download the *win64* installer

1

Learn

Downloads

Documentation

2

INDEX OF DOWNLOADS/

[../](#)
[nonrelease/](#)
[release/](#)

3

INDEX OF DOWNLOADS/RELEASE/

[../](#)
[1.5.11/](#)
[1.5.12/](#)
[1.6.0/](#)
[1.6.1/](#)
[1.6.2/](#)
[1.6.3/](#)

4

INDEX OF DOWNLOADS/RELEASE/1.6.3/

[../](#)
[docs/](#)
[ansible-cisco-radkit-0.6.1.tar.gz](#)
[ansible-cisco-radkit-0.6.1.tar.gz.sig](#)
[cisco radkit 1.6.3 doc html.tgz](#)
[cisco radkit 1.6.3 doc html.tgz.sig](#)
[cisco radkit 1.6.3 linux x86 64.sh](#)
[cisco radkit 1.6.3 linux x86 64.sh.sig](#)
[cisco radkit 1.6.3 macos arm64 signed.pkg](#)
[cisco radkit 1.6.3 macos x86 64 signed.pkg](#)
[cisco radkit 1.6.3 pip linux arm.tgz](#)
[cisco radkit 1.6.3 pip linux arm.tgz.sig](#)
[cisco radkit 1.6.3 pip linux x86.tgz](#)
[cisco radkit 1.6.3 pip linux x86.tgz.sig](#)
[cisco radkit 1.6.3 pip macos.tgz](#)
[cisco radkit 1.6.3 pip macos.tgz.sig](#)
[cisco radkit 1.6.3 pip win.tgz](#)
[cisco radkit 1.6.3 pip win.tgz.sig](#)
[cisco radkit 1.6.3 win64 signed.exe](#)
[radkit verify.py](#)

24-Jan-2024 09:31

24-Jan-2024 09:31

24-Jan-2024 09:31

24-Jan-2024 09:31

24-Jan-2024 09:31

24-Jan-2024 09:31

25-Jan-2024 20:26

25-Jan-2024 20:26

24-Jan-2024 09:31

24-Jan-2024 09:31

24-Jan-2024 09:31

24-Jan-2024 09:31

24-Jan-2024 09:31

24-Jan-2024 09:31

24-Jan-2024 09:31

24-Jan-2024 09:31

24-Jan-2024 09:31

24-Jan-2024 09:31

24-Jan-2024 09:31

3107061

3288

10461870

3288

141605486

3288

83558219

86285412

212815781

3288

138442211

3288

122443167

3288

68943074

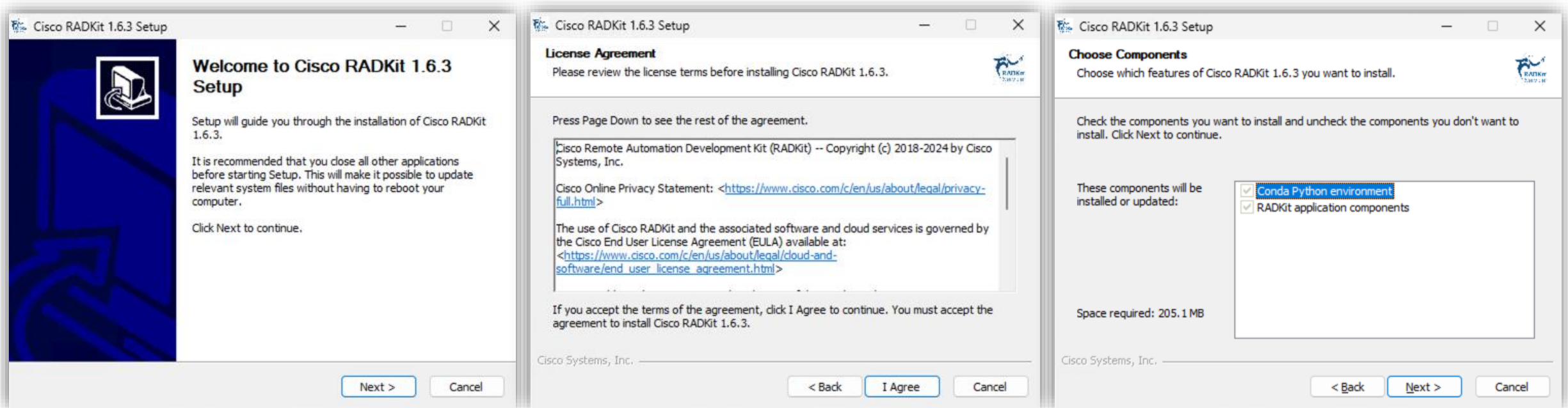
3288

123799640

3056

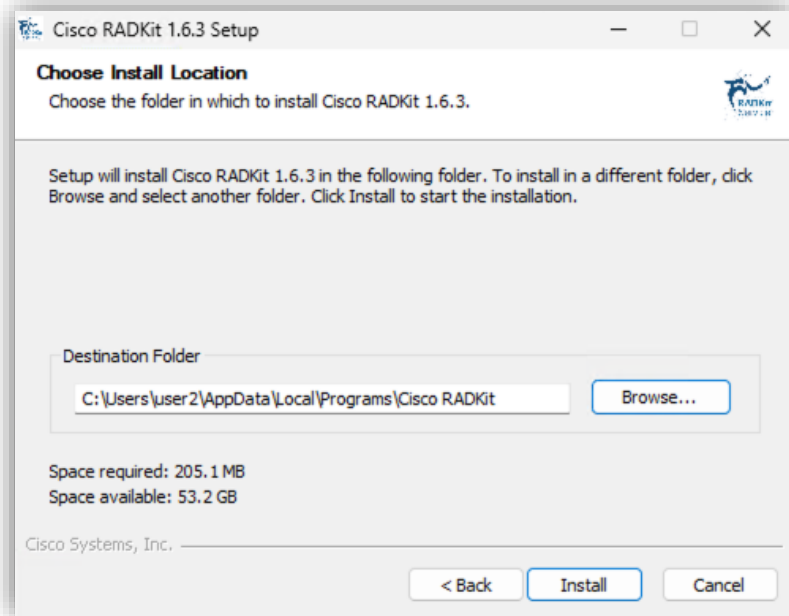
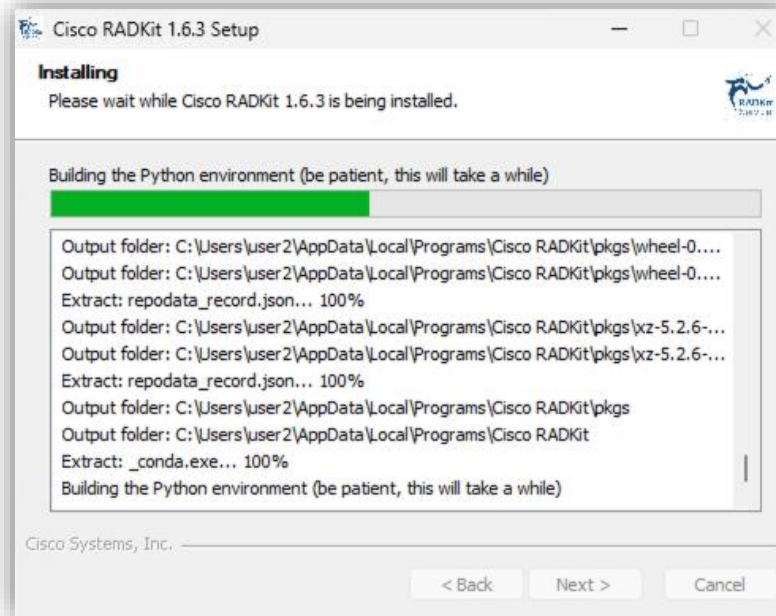
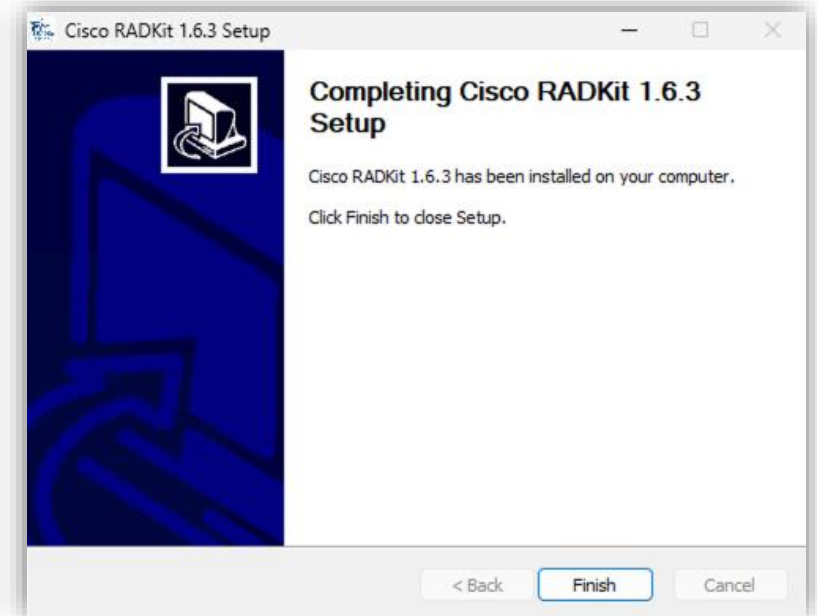
RADKit – Installation on Windows

- Installation takes ~2 minutes

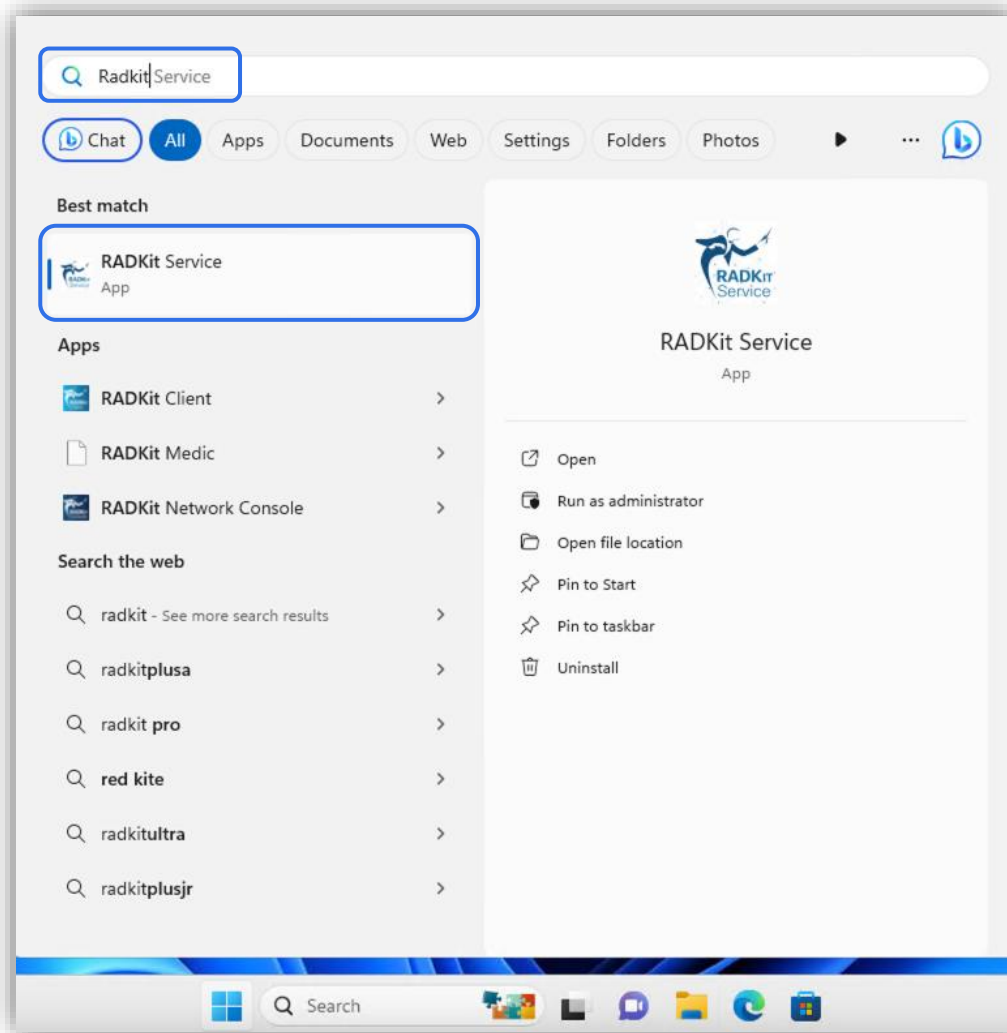
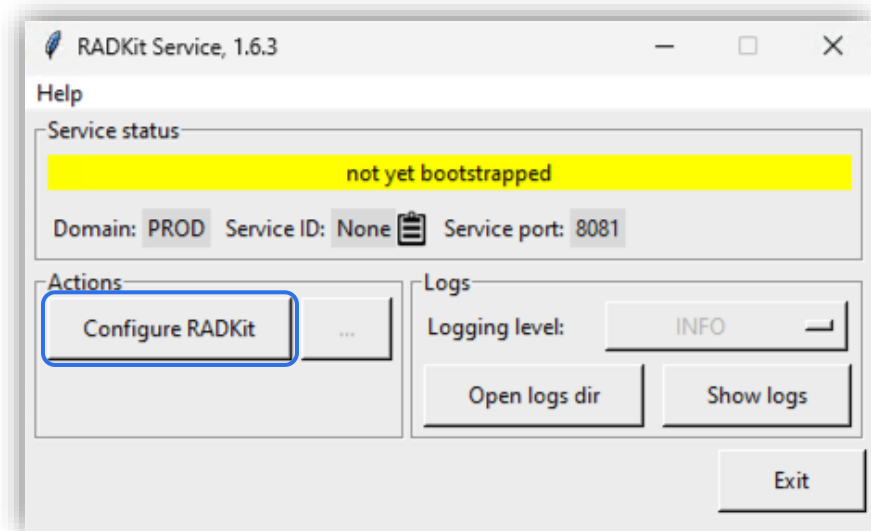


RADKit – Installation on Windows

- Installation path: *C:\Users\user\AppData\Local\Programs\Cisco Radkit*

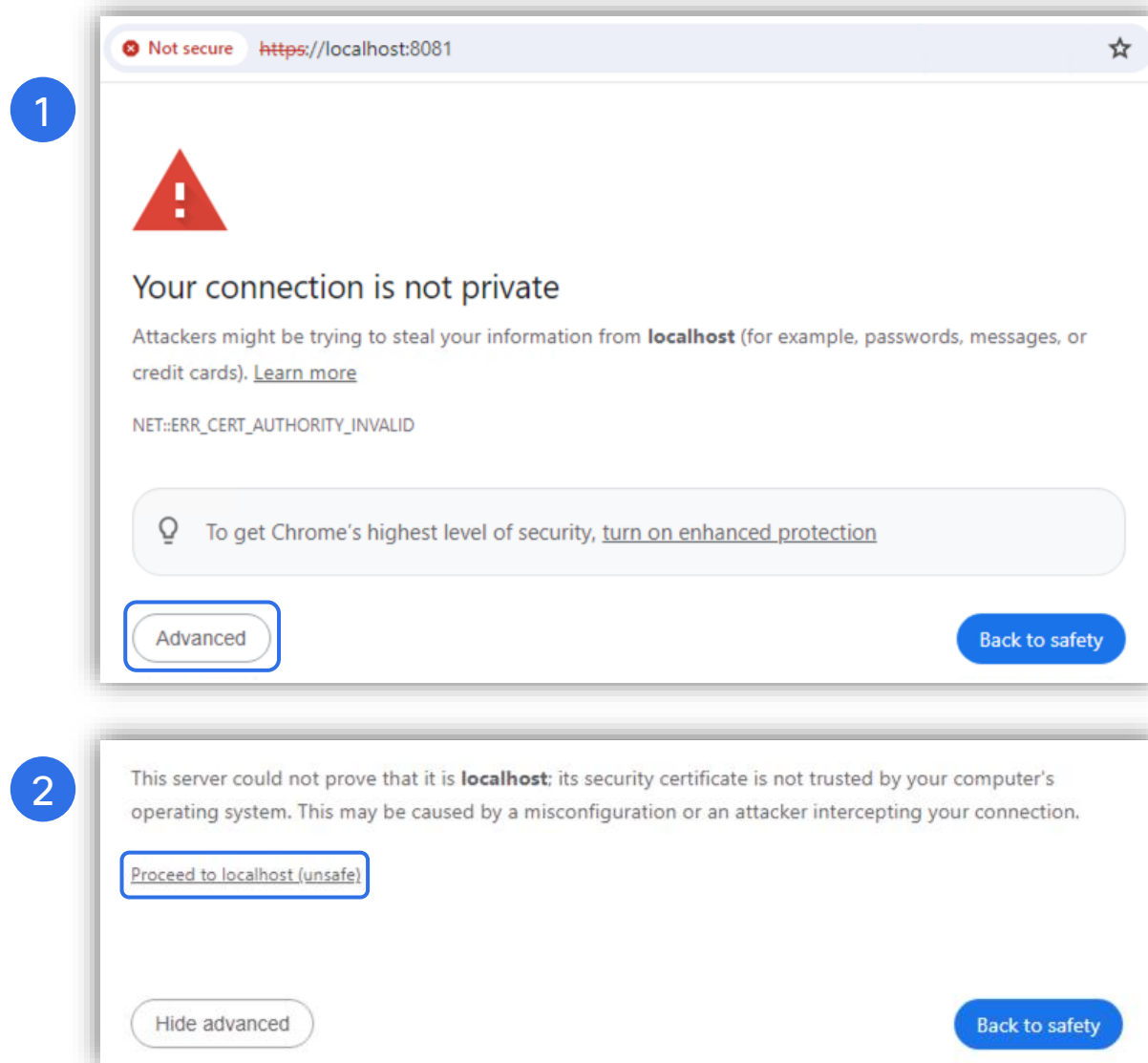


RADKit – Installation on Windows



RADKit - Installation on Windows

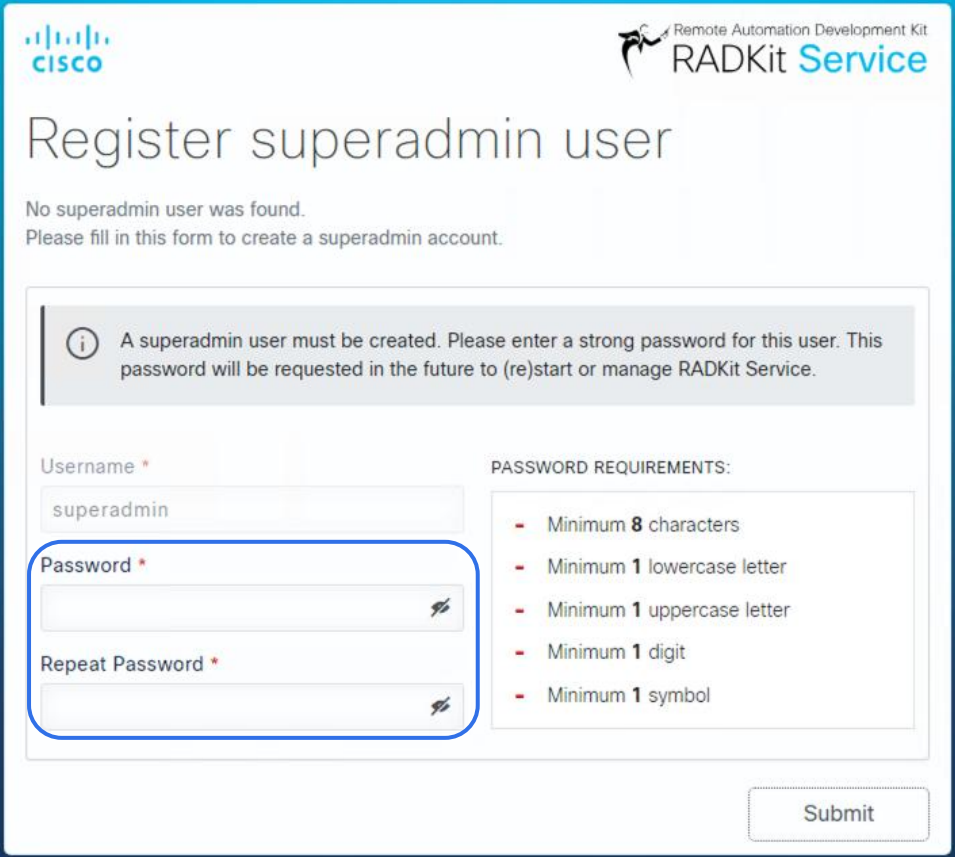
- The GUI is available at <https://localhost:8081>
- RADKit uses self-signed certificate
- Accept the warning



RADKit – Installation on Windows

- Create a *superadmin* password and log in

1



Register superadmin user

No superadmin user was found.
Please fill in this form to create a superadmin account.

i A superadmin user must be created. Please enter a strong password for this user. This password will be requested in the future to (re)start or manage RADKit Service.

Username *
superadmin

PASSWORD REQUIREMENTS:

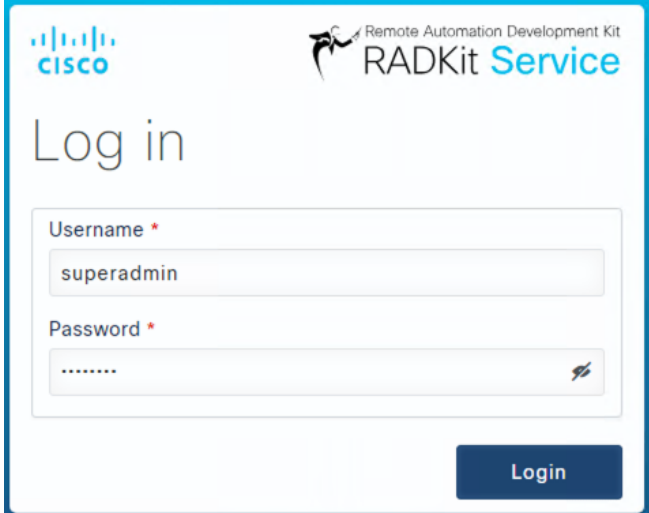
- Minimum 8 characters
- Minimum 1 lowercase letter
- Minimum 1 uppercase letter
- Minimum 1 digit
- Minimum 1 symbol

Password *
[password field]

Repeat Password *
[password field]

Submit

2



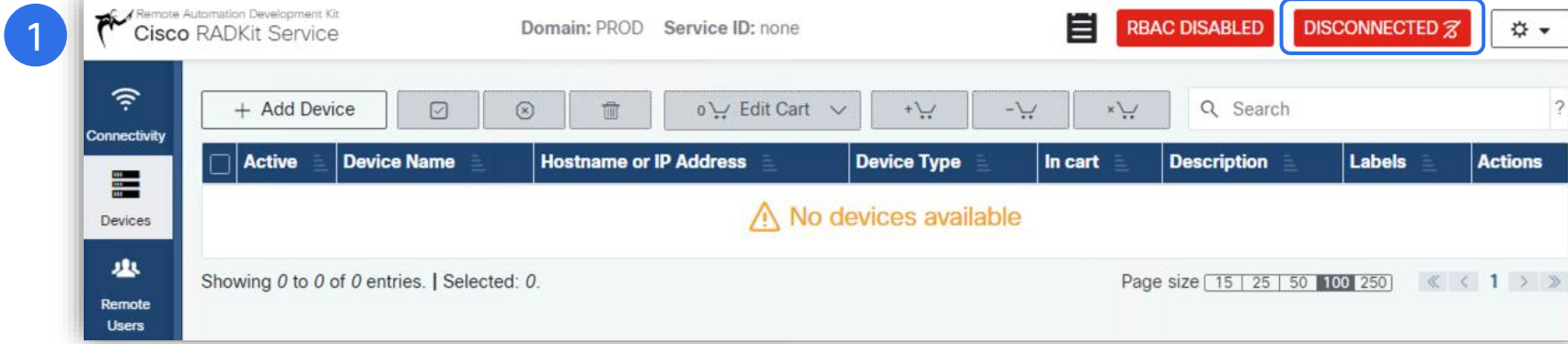
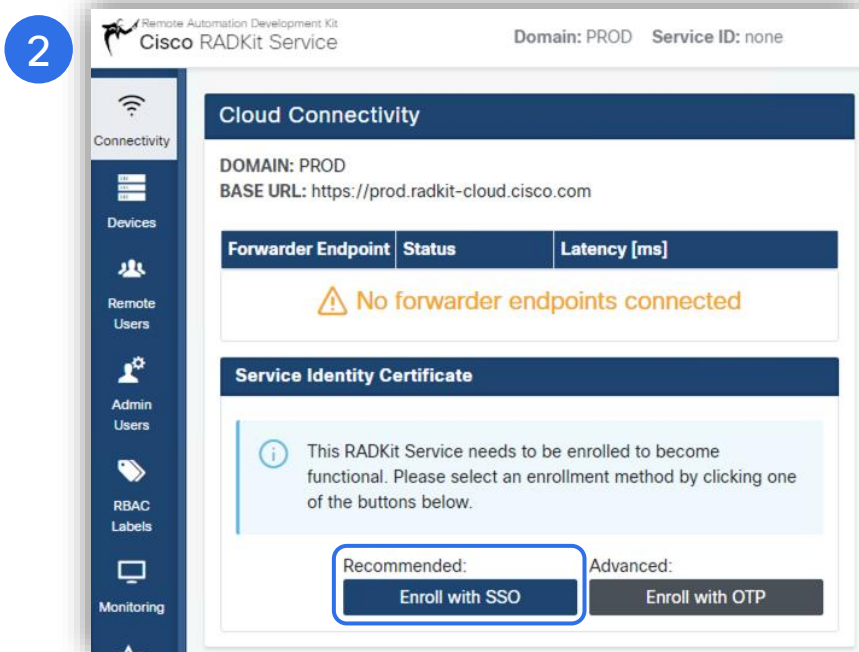
Log in

Username *
superadmin

Password *
[password field]

Login

RADKit – Installation on Windows



- The RADKit Service is disconnected at this point
- Enroll the RADKit Service using Single Sign-On (SSO)

RADKit - Installation on Windows

- Enter your *cisco.com* email address and click on the SSO login link

Single Sign-On Enrollment

✓

Checking prerequisites

2

Email address

Provide email address for SSO login:

lindawa@cisco.com

Submit

3

Connecting to the Access Service

4

Retrieving OAuth Connection Information

5

Waiting for SSO

Cancel

×

Single Sign-On Enrollment

✓

Checking prerequisites

✓

Email address

✓

Connecting to the Access Service

✓

Retrieving OAuth Connection Information

5

Waiting for SSO

Follow the SSO login link to continue: **CLICK HERE**

Close

Single Sign-On Enrollment

✓

Checking prerequisites

✓

Connecting to the Access Service

8

Requesting service certificate

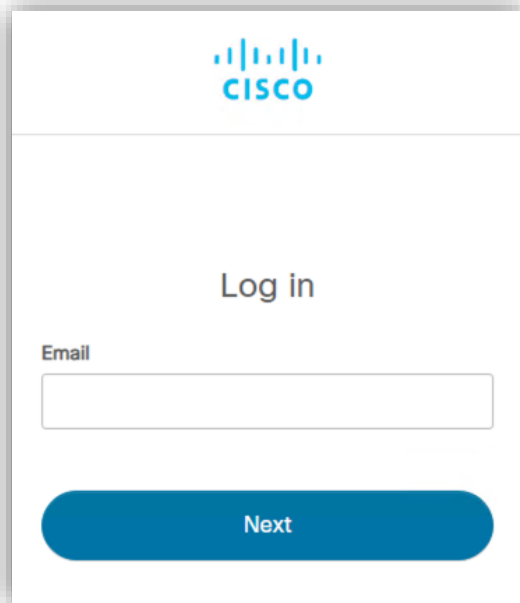
9

Starting/Restarting the service

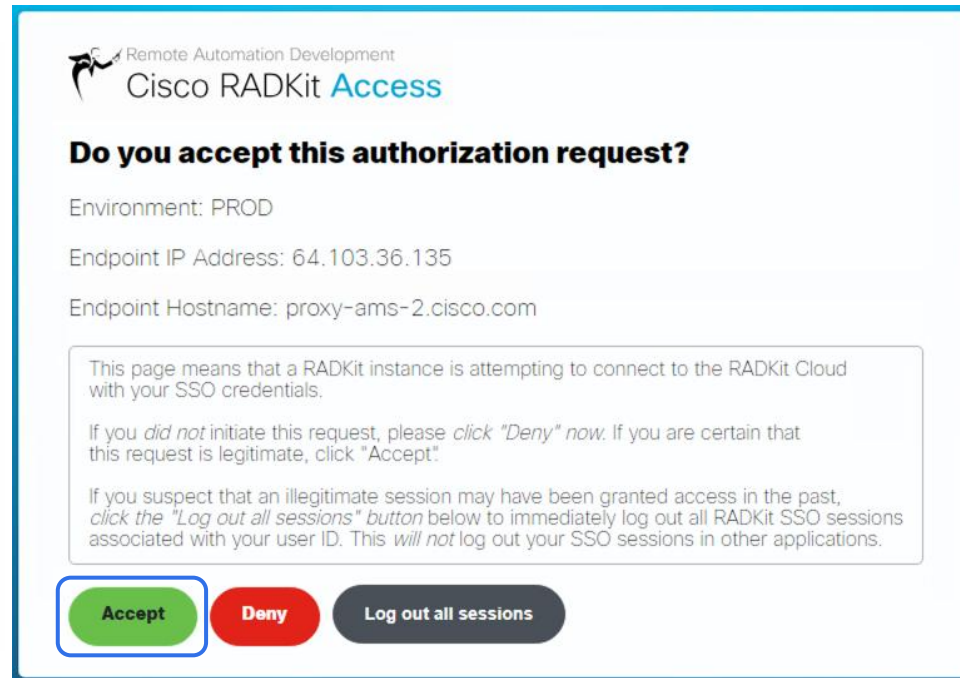
Cancel

RADKit – Installation on Windows

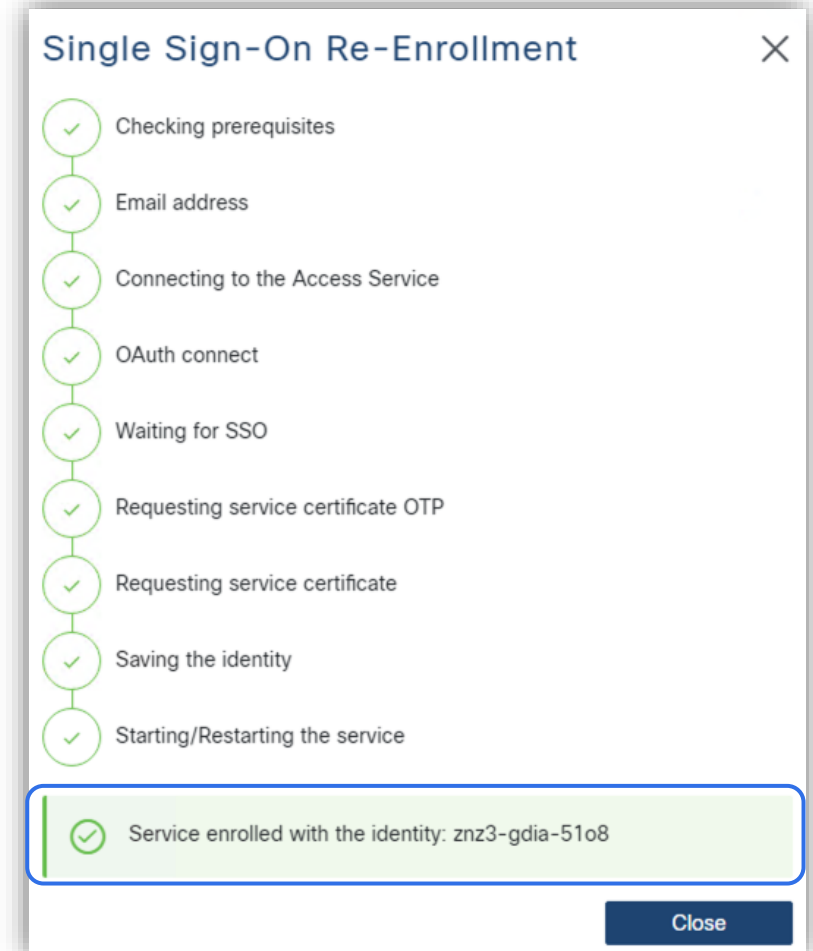
- Log in and accept the authorization request
- The service is enrolled with a unique Service ID



The image shows the Cisco Log in screen. At the top is the Cisco logo. Below it, the text "Log in" is centered. Underneath, there is a label "Email" followed by a text input field. At the bottom, there is a large blue button labeled "Next".



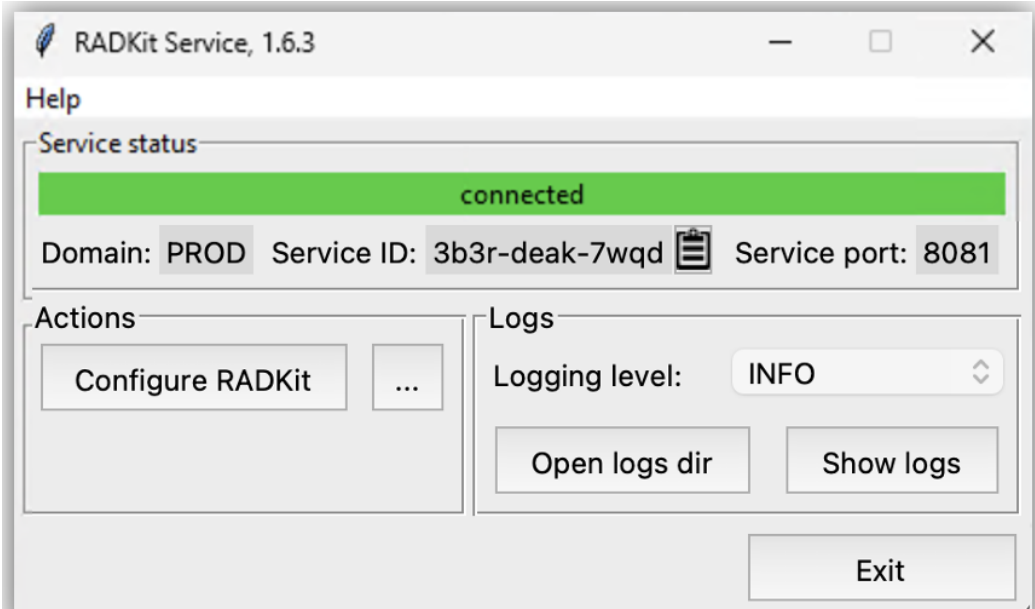
The image shows the Cisco RADKit Access authorization screen. At the top, it says "Remote Automation Development" and "Cisco RADKit Access". Below this, it asks "Do you accept this authorization request?". The screen displays the following information: Environment: PROD, Endpoint IP Address: 64.103.36.135, and Endpoint Hostname: proxy-ams-2.cisco.com. A text box explains that the page means a RADKit instance is attempting to connect to the RADKit Cloud with SSO credentials. It provides instructions on how to handle the request: click "Deny" if not initiated, or "Accept" if legitimate. It also includes a warning about logging out all sessions if an illegitimate session is suspected. At the bottom, there are three buttons: "Accept" (green), "Deny" (red), and "Log out all sessions" (dark grey).



The image shows the "Single Sign-On Re-Enrollment" progress screen. It features a vertical list of steps, each with a green checkmark in a circle: "Checking prerequisites", "Email address", "Connecting to the Access Service", "OAuth connect", "Waiting for SSO", "Requesting service certificate OTP", "Requesting service certificate", "Saving the identity", and "Starting/Restarting the service". At the bottom, a green bar highlights the final step: "Service enrolled with the identity: znz3-gdia-51o8". A "Close" button is located at the bottom right.

RADKit – Installation on Windows

- The RADKit Service window shows **connected** and the Service ID is displayed
- The GUI shows the Service Identity Certificate details



Cloud Connectivity

DOMAIN: PROD

BASE URL: https://prod.radkit-cloud.cisco.com

Forwarder Endpoint	Status	Latency [ms]
wss://prod.radkit-cloud.cisco.com/forwarder-3/	CONNECTED	286

Service Identity Certificate

✔ Certificate valid. Service is enrolled.

Subject Name:

serialNumber=3b3r-deak-7wqd

Cert Serial:

8f5e9198a1780fb313cc54e557838da8

Cert Owner:

lindawa@cisco.com

Cert Granter:

lindawa@cisco.com

Valid from:

Mon, Oct 20, 2025 23:11

Valid until:

Sun, Apr 19, 2026 00:11

Last validation:

Tue, Oct 21, 2025 00:20

Renewal schedule:

Fri, Apr 03, 2026 00:20

RADKit – Installation on Windows

- Network devices are found in the *Devices* page
- Click on *+Add Device* to add a new device

Remote Automation Development Kit
Cisco RADKit Service

Domain: PROD Service ID: 3b3r-deak-7wqd

RBAC DISABLED CONNECTED

Connectivity

Devices

Remote Users

+ Add Device

Search

0 Bulk Edit

	Active	Device Name	Hostname or IP Address	Device Type	In cart	Description	Labels	Actions
No devices available								

Showing 0 to 0 of 0 entries. | Selected: 0.

Page size 15 25 50 100 250

RADKit – Installation on Windows

- Fill out the device details
- Mandatory fields:
 - Device Name
 - Management IP / Hostname
 - Device Type
- Add details for Management Protocols such as:
 - Terminal
 - Netconf
 - Swagger
 - HTTP
 - SNMP

Add New Device

Device Name^{*}(as it will appear in RADKit)?

pod4-wlc1

Device Type^{*}

WLC (Wireless Lan Controller)

Management IP Address or Hostname^{*}?

10.66.56.150

Jumphost Name

– No legal jumphosts enabled –

☒ Active (remotely manageable)

Available Management Protocols:
☒ Terminal ☐ Netconf ☐ Swagger ☐ HTTP ☐ SNMP

Template Selector ?

– No template available –

Terminal

Connection method:
☒ SSH (Password) ☐ SSH (Public key) ☐ Telnet

Capabilities:
☒ Interactive ☒ Exec ☒ Upload ☒ Download

Username
admin

Port
22

☐ Device can be a jumphost
☐ Allow connecting using obsolete/insecure SSH algorithms

Password
.....
If left blank, will be set to "" as default ↵

☒ Enable Password ?
.....
If left blank, will be set to "" as default ↵

Clear form

Add & close

Add & continue

RADKit – Installation on Windows

- Devices can be edited or deleted
- Access to devices is defined by the “Active” toggle

+ Add Device

0 Bulk Edit

Search

<div></div>	<div>Active</div>	<div>Device Name</div>	<div>Hostname or IP Address</div>	<div>Device Type</div>	<div>In cart</div>	<div>Description</div>	<div>Labels</div>	<div>Actions</div>
<div></div>	<div><div></div></div>	<div>pod4-wlc1</div>	<div>10.66.56.150</div>	<div>WLC</div>				<div><div></div><div></div><div></div><div></div></div>

Showing 1 to 1 of 1 entries. | Selected: 0.

Page size

15

25

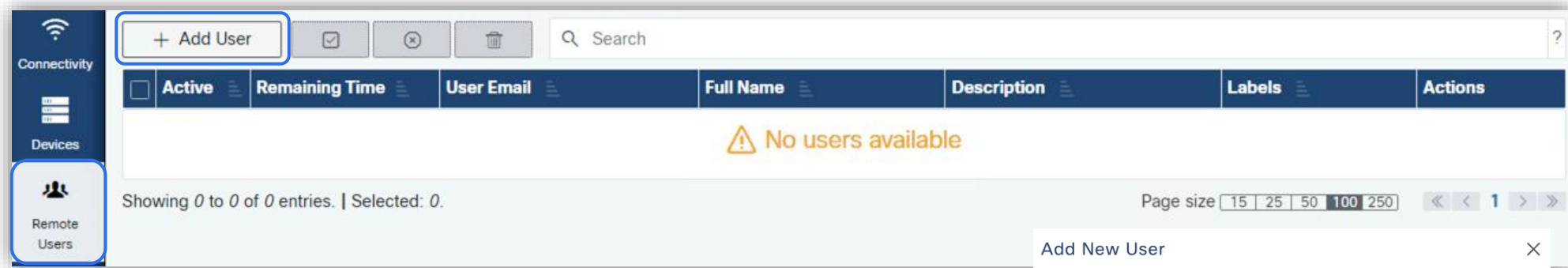
50

100

250

1

RADKit - Installation on Windows



- Use the *Remote Users* page (+Add User)
- Fill out the new user details
- Access can be provided for a fixed amount of time, or by using the manual toggle

A screenshot of the 'Add New User' form. The form includes fields for 'User Email*' (lindawa@cisco.com), 'Full Name' (Linda Wang), and 'Description' (Remote access for Linda). There is a toggle for 'Activate this user' and a section for 'USER ACCESS POLICY' with options for 'Manual' and 'Time slice (h/m):' (4 hours, 0 minutes). The 'AUTHENTICATION' section has a 'Type' dropdown set to 'Local token' and an 'E2EE validation token*?' field with the value 'X6dHZeRXKP+v7bbK'. The 'CONNECTION MODES' section has three toggles: 'Cloud', 'Direct' (selected), and 'Direct with SSO'. There is a 'Label search' field and an 'RBAC status: DISABLED' indicator. At the bottom, there are sections for 'Available Labels - 0 of 0 (click to add)?' and 'Selected Labels - 0 (click to delete)', both showing 'NO LABELS AVAILABLE'. The form ends with 'Clear form', 'Add & close', and '+ Add & continue' buttons.

RADKit - Installation on Windows

- Access for Remote Users can be revoked at any time by using the toggle

+ Add User

☒

☐

☐

Search

☐	Active	Remaining Time	User Email	Full Name	Description	Labels	Actions
☐	☒	4h 00m <div>Reset</div>	lindawa@cisco.com	Linda Wang	Remote access for Linda		<div><div></div><div></div></div>

Showing 1 to 1 of 1 entries. | Selected: 0.

Page size

15

25

50

100

250

<<

<

1

>

>>

Importing devices in bulk from CSV file

Import devices in bulk from CSV file

- RADKit Control allows to retrieve, create and modify RADKit service components
- It provides a way to manage RADKit components over the network, as an alternative to the WebUI

Command structure:

```
$ radkit-control [OPTIONS] COMMAND [ARGS]
```

Usage information:

```
$ radkit-control --help
```

```
$ radkit-control --help
Usage: radkit-control [OPTIONS] COMMAND [ARGS]...

    Control a remote or local RADKit Service

Options:
  --version                Display version and exit
  --service-certificate FILE Path to a certificate file identifying the
                           Service.
  --service-fingerprint TEXT Service certificate fingerprint used to verify
                           TLS connection. The fingerprint should use
                           SHA256 hash.
  --debug                 Enable debugging
  --trace                 Enable trace logging
  --radkit-directory DIRECTORY Root of the RADKit directories
  --settings-file FILE    Path to the custom settings file (can be both
                           absolute and relative to current working
                           directory)
  -s, --setting TEXT...   Override a specific setting
  --tracebacks             Enables full tracebacks for all exceptions
  --help                  Show this message and exit.

Commands:
  admin  setup RADKit Service
  device Operate on devices
  label  Operate on labels
  system RADKit Service system-level control
  user   Operate on users
```

Import devices in bulk from CSV file

- The CSV file requires a special structure
- Templates are available for different information components, such as terminal http, swagger, netconf, snmp and labels

To see the available CSV templates:

```
$ radkit-control device bulk-create --help
```

```
$ radkit-control device bulk-create --help
Usage: radkit-control device bulk-create [OPTIONS]

    Create multiple devices using JSON or CSV.

    Pass exactly one of --json-input, --json-data, --csv-input, or --
csv-data

Options:
  --json-input FILENAME  JSON file to pass to the API
  --json-data JSON       JSON text to pass to the API
  --csv-input FILENAME   CSV file to pass to the API
  --csv-data TEXT        CSV text to pass to the API
  --json-template         Show JSON template
  --csv-template          Show CSV template. Use `terminal`, `http`,
`swagger`,
                        `netconf`, `snmp` or `labels` to generate
                        substructures
  --output FILENAME      Save JSON response to a file instead of
displaying it
  --compact-json          Output JSON response on one line
  --help                 Show this message and exit.
```

Import devices in bulk from CSV file

Structure template for terminal (CLI) information:

```
$ radkit-control device bulk-create --csv-template terminal
```

```
$ radkit-control device bulk-create --csv-template terminal
name (mandatory) , host (mandatory) , deviceType (mandatory) , description , jumphostUuid , sourceKey , sourceDevUuid , metaData , enabled , forwardedTcpPorts , terminal.port , terminal.connectionMethod , terminal.username , terminal.enableSet , terminal.useInsecureAlgorithms , terminal.useTunnelingIfJumphost , terminal.password , terminal.enable , terminal.privateKeyPassword , terminal.privateKey
```

CSV file example:

```
name (mandatory) , host (mandatory) , deviceType (mandatory) , description , jumphostUuid , sourceKey , sourceDevUuid , metaData , enabled , forwardedTcpPorts , terminal.port , terminal.connectionMethod , terminal.username , terminal.enableSet , terminal.useInsecureAlgorithms , terminal.useTunnelingIfJumphost , terminal.password , terminal.enable , terminal.privateKeyPassword , terminal.privateKey
asr9001 , 1.2.3.4 , IOS_XR , test router1 , , , , True , , 22 , SSH , my-username , True , , , strong-password , True , ,
test-router2 , 1.1.1.2 , IOS_XE , test router2 , , , , True , , 22 , SSH , my-username , True , , , strong-password , True , ,
```

name(mandatory)	host(mandatory)	deviceType(mandatory)	description	jumphostUuid	sourceKey	sourceDevUuid	metaData	enabled	forwardedTcpPorts	terminal.port	terminal.connectionMethod	terminal.username	terminal.enableSet	terminal.useInsecureAlgorithms	terminal.useTunnelingIfJumphost	terminal.password	terminal.enable	terminal.privateKeyPassword	terminal.privateKey
asr9001	1.2.3.4	IOS_XR	test router1					True		22	SSH	my-username	True			strong-password	True		
test-router2	1.1.1.2	IOS_XE	test router2					True		22	SSH	my-username	True			strong-password	True		



Import devices in bulk from CSV file

Command:

```
$ radkit-control device bulk-create --csv-input file.csv
```

- *superadmin* password is required
- Details of every added device is printed in JSON format
- Success and error counts are displayed

1

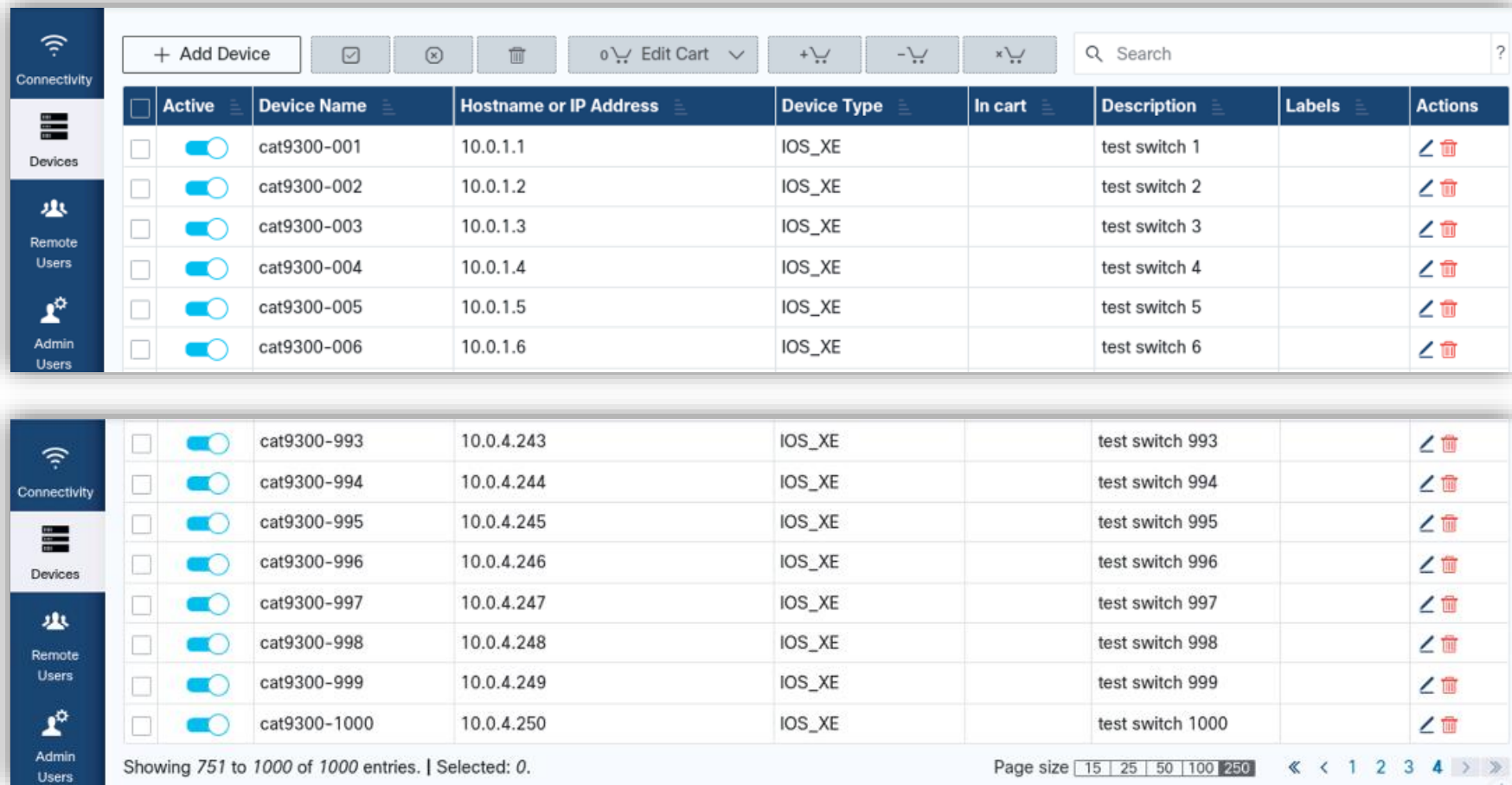
```
cmorenoa@cmorenoa-ubuntu:~/Downloads$ radkit-control device bulk-create --csv-input devices.csv  
superadmin's password:
```

2

```
{  
  "success": true,  
  "result": {  
    "uuid": "b9417c0e-9121-438a-90b6-c8b634fde792",  
    "name": "cat9300-1000",  
    "host": "10.0.4.250",  
    "deviceType": "IOS_XE",  
    "description": "test switch 1000",  
    "labels": [],  
    "jumpHostUuid": null,  
    "sourceKey": null,  
    "sourceDevUuid": null,  
    "metaData": [],  
    "enabled": true,  
    "terminal": {  
      "port": 22,  
      "connectionMethod": "SSH",  
      "username": "my-username",  
      "enableSet": true,  
      "useInsecureAlgorithms": false,  
      "useTunnelingIfJumpHost": true  
    },  
    "netconf": null,  
    "snmp": null,  
    "swagger": null,  
    "http": null,  
    "forwardedTcpPorts": ""  
  },  
  "count": 1000,  
  "success_count": 1000,  
  "error_count": 0,  
  "success": true  
}
```

Import devices in bulk from CSV file

- WebUI view after the import operation:



 Connectivity		<div><div>+ Add Device</div><div></div><div></div><div></div><div><div>0  Edit Cart</div><div></div><div></div><div></div></div><div><div> Search</div><div>?</div></div></div>						
☐	Active	Device Name	Hostname or IP Address	Device Type	In cart	Description	Labels	Actions
☐	☒	cat9300-001	10.0.1.1	IOS_XE		test switch 1		 
☐	☒	cat9300-002	10.0.1.2	IOS_XE		test switch 2		 
☐	☒	cat9300-003	10.0.1.3	IOS_XE		test switch 3		 
☐	☒	cat9300-004	10.0.1.4	IOS_XE		test switch 4		 
☐	☒	cat9300-005	10.0.1.5	IOS_XE		test switch 5		 
☐	☒	cat9300-006	10.0.1.6	IOS_XE		test switch 6		 
☐	☒	cat9300-993	10.0.4.243	IOS_XE		test switch 993		 
☐	☒	cat9300-994	10.0.4.244	IOS_XE		test switch 994		 
☐	☒	cat9300-995	10.0.4.245	IOS_XE		test switch 995		 
☐	☒	cat9300-996	10.0.4.246	IOS_XE		test switch 996		 
☐	☒	cat9300-997	10.0.4.247	IOS_XE		test switch 997		 
☐	☒	cat9300-998	10.0.4.248	IOS_XE		test switch 998		 
☐	☒	cat9300-999	10.0.4.249	IOS_XE		test switch 999		 
☐	☒	cat9300-1000	10.0.4.250	IOS_XE		test switch 1000		 

Showing 751 to 1000 of 1000 entries. | Selected: 0.

Page size 15 25 50 100 250 << < 1 2 3 4 > >>

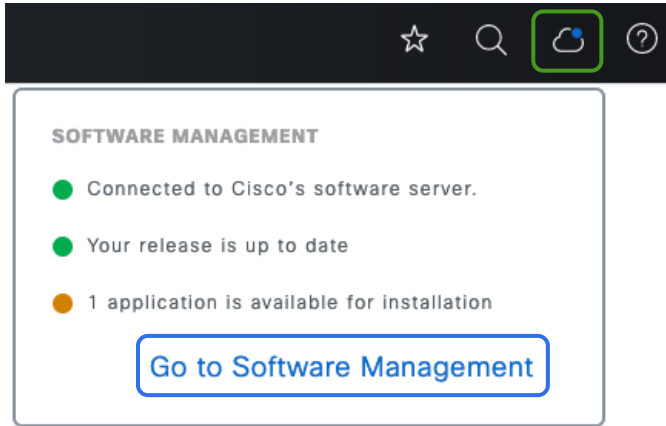
RADKit in Cisco Catalyst Center ex-Cisco DNA Center

RSA – Remote Support Authorization

- RSA requires the **Support Services** package to be installed from the *Software Management* page
- Installation takes ~5 minutes
- A new *Remote Support Authorization* option is added to the help (?) menu

Requires Catalyst Center
(formerly DNAC) 2.3.5.x or later"

1



SOFTWARE MANAGEMENT

- Connected to Cisco's software server.
- Your release is up to date
- 1 application is available for installation

[Go to Software Management](#)

2

Available applications for 2.3.7.4-70424

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

[Select All](#)

 Support Services 

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

[View Details](#)

[Cancel](#) [Install](#)

RSA – Remote Support Authorization

- Add the *maglev* password to allow access to Cisco Catalyst Center's CLI for troubleshooting

2

 **Catalyst Center** Remote Support Authorization

SUMMARY

15	0	15
Total Authorizations	Current Authorizations	Past Authorizations

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

SSH credentials provide Cisco DNA Center access to a Cisco specialist for troubleshooting.

The credentials should match those configured in the Cisco DNA Center node (associated with the maglev user) during the installation.

You can add as many credentials as Cisco DNA Center nodes, including the disaster recovery witness.

+ Add New SSH Credentials

1

★ 🔍 🔄 ✓ ?

- About
- Cisco DNA Sense
- API Reference 
- Developer Resources 
- Contact Support 
- Remote Support Authorization**
- Help 

RSA – Remote Support Authorization

- If nodes in a 3-node cluster use different maglev passwords, then multiple credentials can be added

Add New SSH Credentials

Add the SSH credentials of the maglev user configured in the Cisco DNA Center node during the installation.

Adding these credentials does not change the SSH credentials in Cisco DNA Center.

These SSH credentials will only be used to connect to the node(s) during a remote support session.

Password*

.....

SHOW

Name/Description*

CCC4_maglev_password

+

Cancel

Add SSH Credential

RSA – Remote Support Authorization

- Existing credentials can be edited, and more credentials can be added if needed

Create New Authorization

Current Authorizations

Past Authorizations

Manage SSH Credentials

SSH credentials provide Cisco DNA Center access to a Cisco specialist for troubleshooting.

The credentials should match those configured in the Cisco DNA Center node (associated with the maglev user) during the installation.

You can add as many credentials as Cisco DNA Center nodes, including the disaster recovery witness.

+ Add New SSH Credentials

CURRENT SSH CREDENTIALS

CCC4_maglev_password

Edit

Delete

RSA – Remote Support Authorization

- Grant remote access to a Cisco specialist
- Access can be removed at any time
- Access is granted for 24 hours by default

Connection to Remote Support (RADKit) Cloud is not established. ⓘ

As of: Jan 25, 2024 9:49 AM

SUMMARY

15

0

15

Total Authorizations

Current Authorizations

Past Authorizations

Create New Authorization

Current Authorizations

Past Authorizations

Manage SSH Credentials



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

Create a Remote Support Authorization

RSA – Remote Support Authorization

1

Step 1 of 4: 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 the authorization any time before it expires. Any ongoing support session associated with the authorization will be immediately disconnected.

☒ I agree to provide access to network devices.

☒ I agree to provide access to Cisco DNA Center.

Next Step

2

Step 2 of 4: Set up the Authorization

To start, enter the Cisco specialist email address. If you have the Case number(s) ready, please also enter them below.

Cisco Specialist Email Address*

lindawa@cisco.com

Access Role for the Cisco Specialist*

OBSERVER-ROLE

▼

Existing Case Number(s)

0123456789

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

3

Step 3 of 4: 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

Review

Back

Next Step

RSA – Remote Support Authorization

Step 4 of 4: Summary

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

Access Permission Agreement

- Agreed to provide access to network devices.
- Agreed to provide access to Catalyst Center.

Set Up the Authorization [Edit](#)

Cisco Specialist Email Address	<code>lindawa@cisco.com</code>
Role Assigned to Cisco Specialist	OBSERVER-ROLE
Existing Case Numbers	0123456789
Access Justification	Remote Access for Linda Wang (TAC)

Schedule the Access [Edit](#)

Scheduled For	Now
Duration	24 hours

Back

Create

 Connection to Remote Support (RADKit) Cloud is established. 

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.

`lindawa@cisco.com` is scheduled to sign in to Catalyst Center on **22 Oct 2025, 11:21 pm GMT+11** for 24 hours using `neim-coju-gdfr` as the Support ID. 

- The Support ID will be used by the Cisco specialist to log into your Cisco Catalyst Center to triage and troubleshoot issues that you reported

RSA – Remote Support Authorization

- Details (i.e. Service ID) are available in the *Current Authorizations* tab

Catalyst Center

Remote Support Authorization

admin

Connection to Remote

SUMMARY

10

Total Authorizations

1

Current Authorizations

9

Past Authorizations

Create New Authorization

Current Authorizations

Past Authorizations

Status

All

Scheduled

Active

lindawa@cisco.com

Active on

22 Oct 2025, 11:21 pm GMT+11

Duration

24 hours

Revoke Authorization

View Logs

lindawa@cisco.com

Support ID

neim-coju-gdfr

Cisco Specialist Email Address

lindawa@cisco.com

Access Role

OBSERVER-ROLE

Case Number(s)

0123456789

Date

22 Oct 2025, 11:21 pm GMT+11

Duration

24 hours

Description

Remote Access for Linda Wang (TAC)

Access Permission

All Cisco DNA Center nodes (including witness, if disaster recovery is enabled),
All SSH-enabled network devices managed by Cisco DNA Center

RSA – Additional notes

Available from Cisco Catalyst Center version 2.3.5.x and above

Remote access to the web interface (GUI) is currently not possible

Fixed 24-hour access period (can be revoked earlier)

No granular per-device access

Authorization can only be granted to *@cisco.com* users

Demo

Complete your session evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to claim a Cisco Live T-Shirt.



Earn up to 800 points by completing all surveys and climb the Cisco Live Challenge leaderboard.



Level up and earn exclusive prizes!



Complete your surveys in the Cisco Live Events app.

Continue your education



Visit the Cisco Stand for related demos



Book your one-on-one Meet the Expert meeting



Attend the interactive education with Capture the Flag, and Walk-in Labs



Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Thank you

CISCO Live !

