

The Cisco Live! logo features the word "CISCO" in a dark blue, sans-serif font, followed by "Live!" in a dark blue, cursive script font. The background of the entire image is a vibrant, multi-colored abstract pattern of overlapping, wavy lines and geometric shapes, transitioning from dark blue on the left to bright yellow and white on the right, with a sunburst effect on the far right.

CISCO *Live!*

Let's go



The bridge to possible

# RADKit

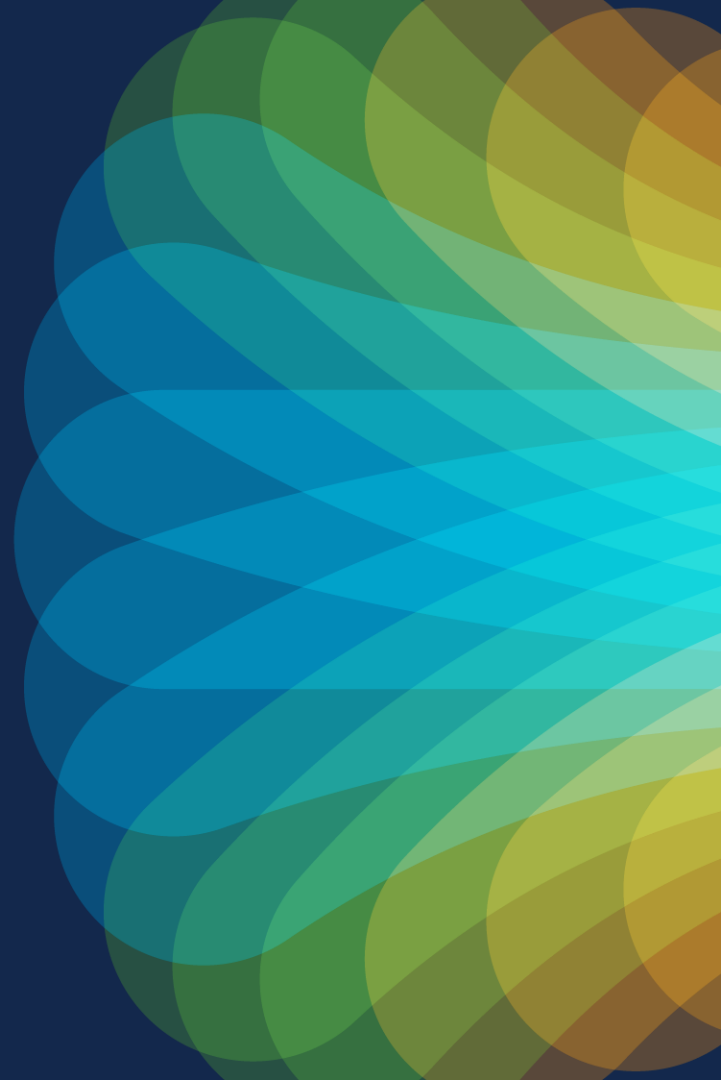
an SDK to control every device, everywhere,  
all at once

Frédéric Detienne  
Carlos Moreno

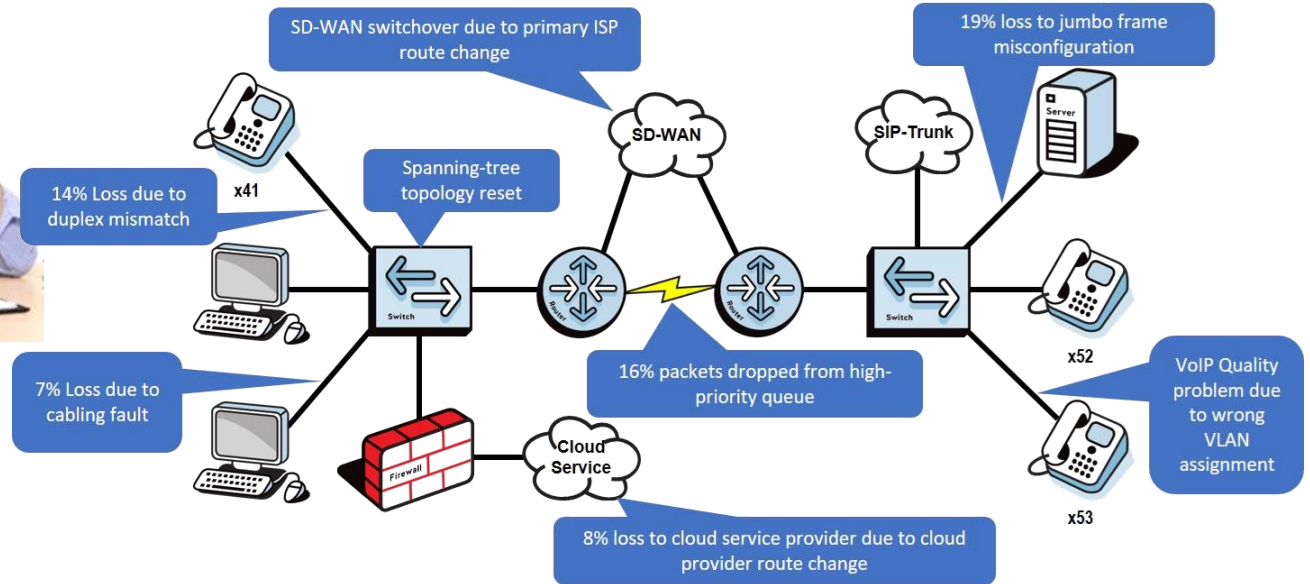
# Agenda

- Introduction – Why RADKit ?
- RADKit Overview
- RADKit in Action (demo)
- Deploying RADKit (demo)
- Importing Inventory (demo)
- Conclusion

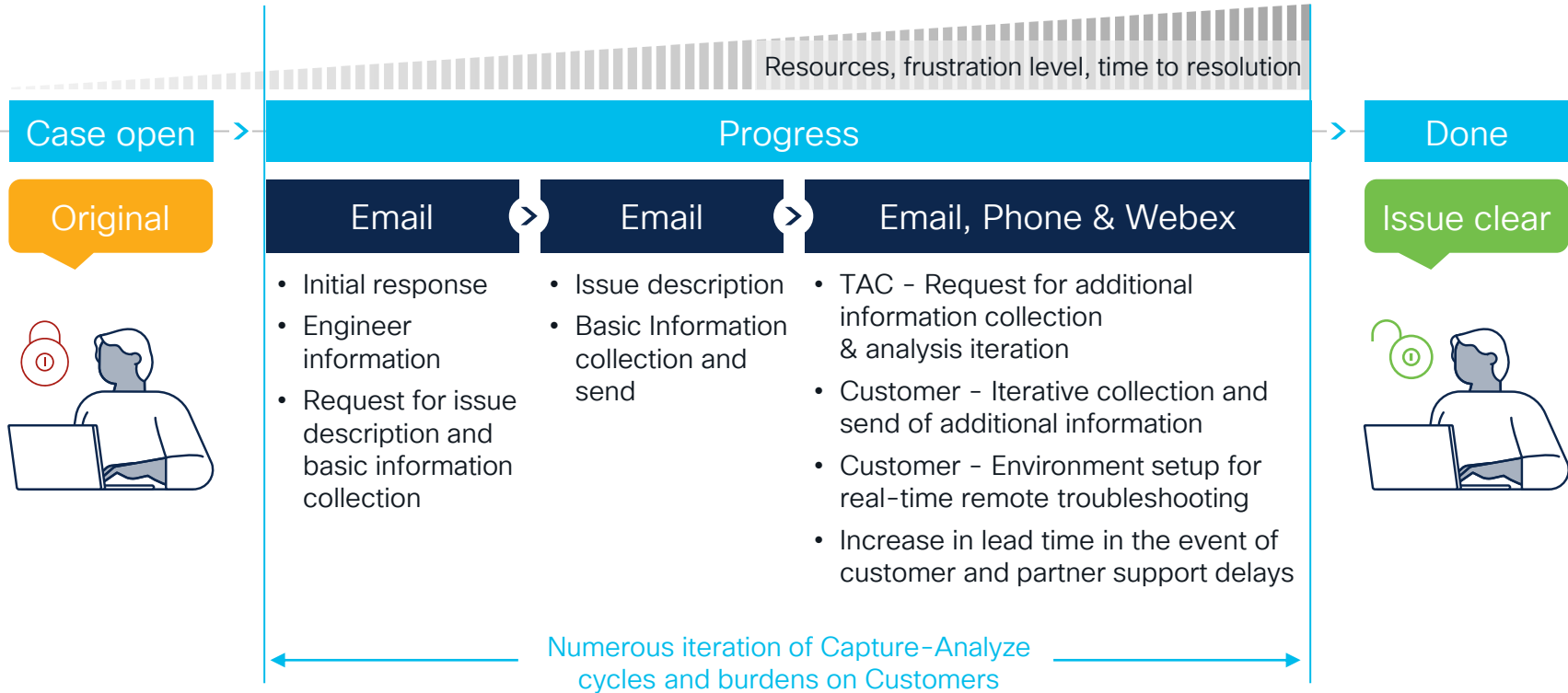
# Introduction



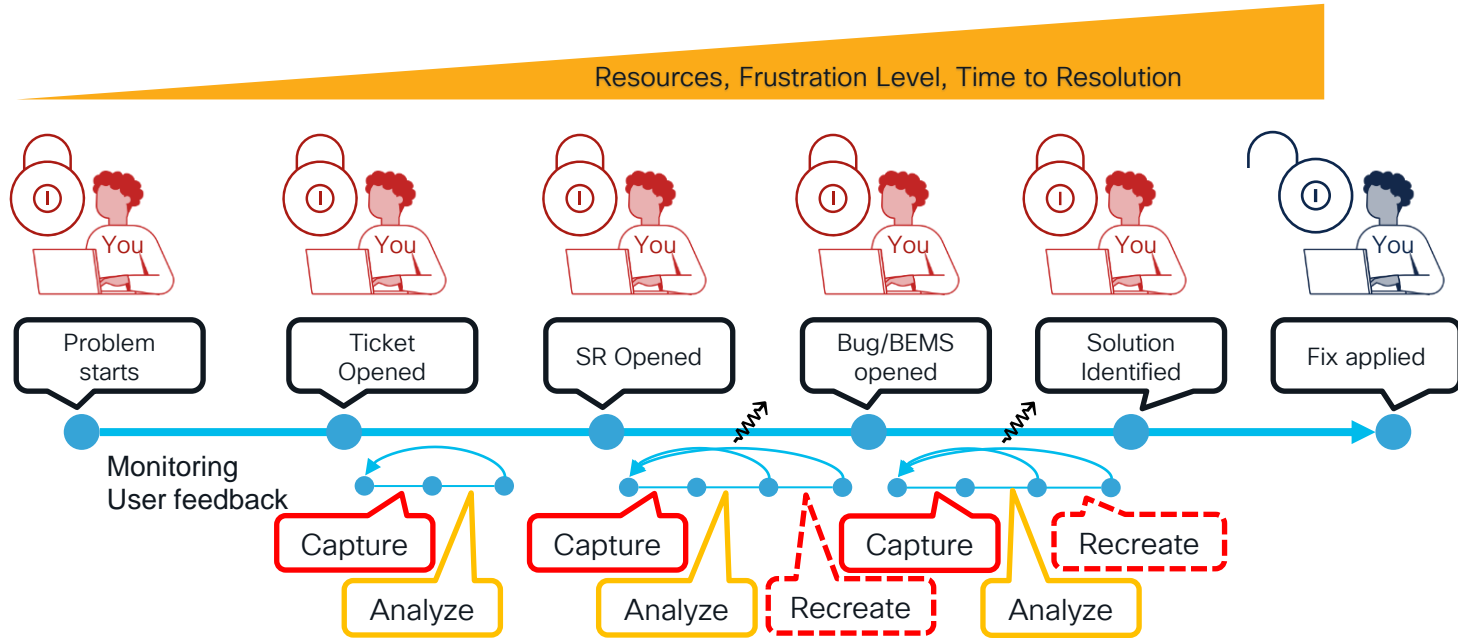
# How painful is this ?



# Current troubleshooting method



# The Churn in Issue Lifecycle



# 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 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

20% - 80%\*

Reduction in TFR

50 - 80%\*

Customer Effort Reduction

Enhanced Cisco Service capabilities

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

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



\*Note:

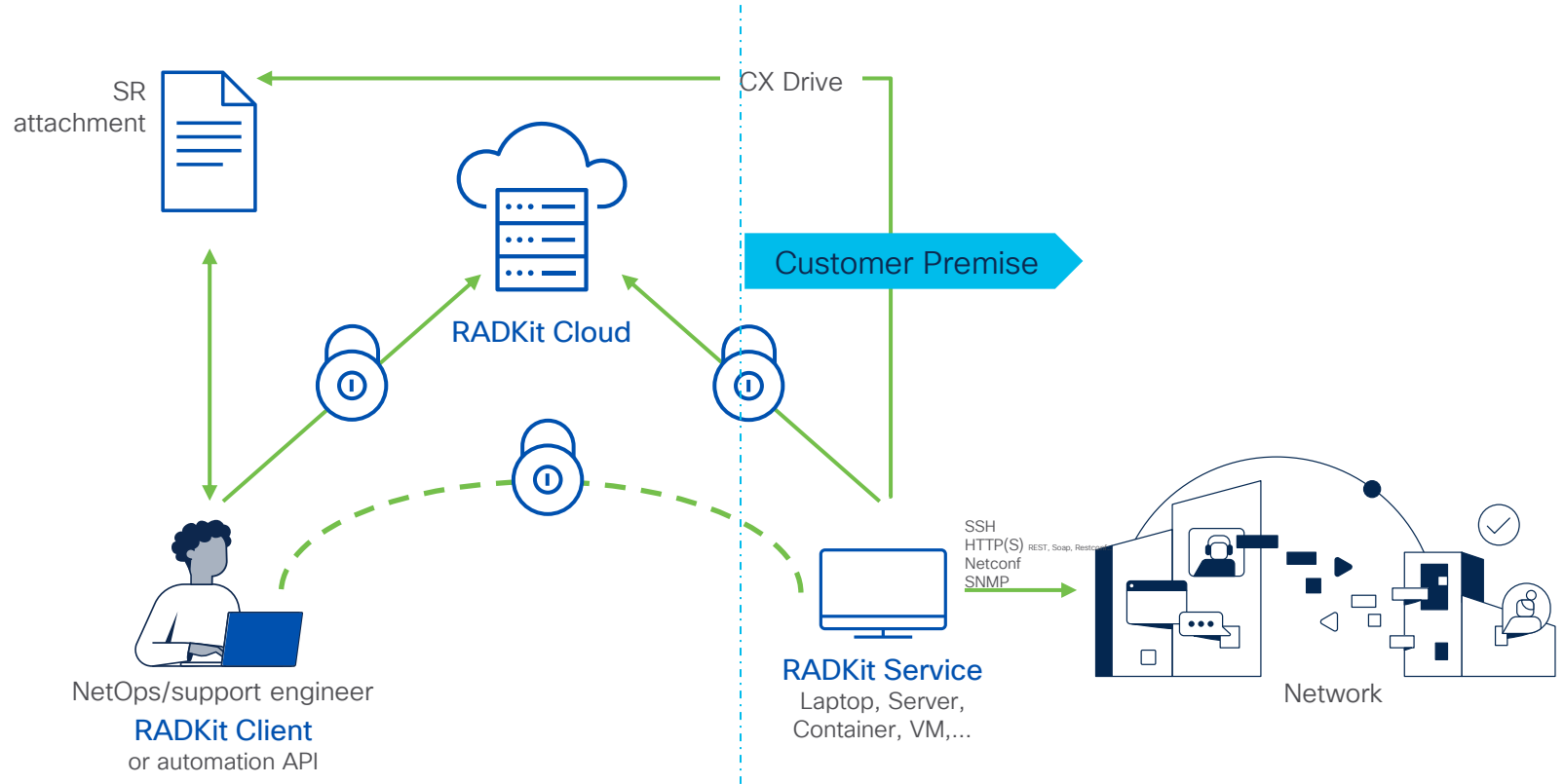
- deriving uniform ROI/Depends on extent RADKit capabilities utilized
- No known standard measure of "effort". Effort comprises attendance.

*The use of RADKit is projected to free up 100-120 business days where we can re-focus on critical work.*

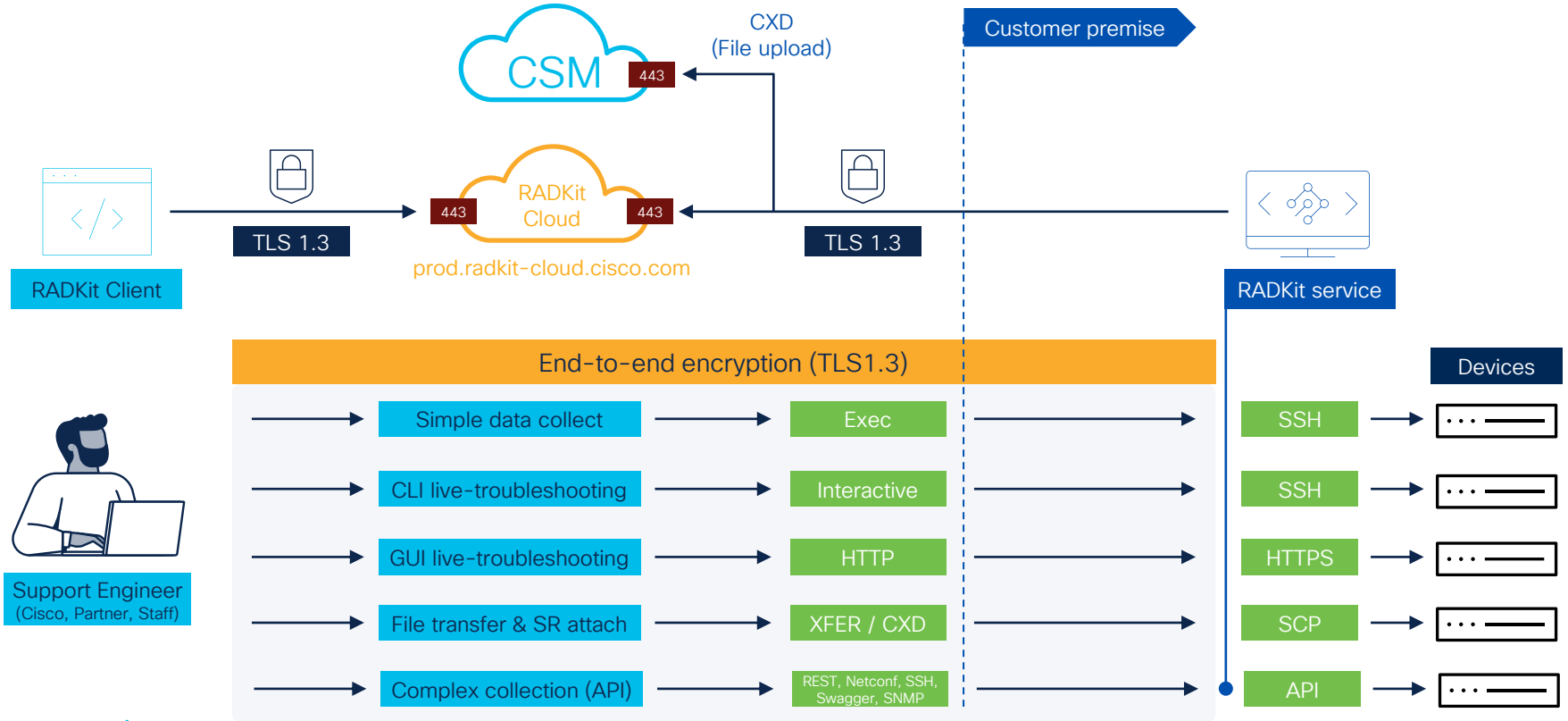
Jorge Carreno  
Sr. Product Owner  
Telstra, Australian Service Provider

# RADKit Overview

# RADKit General Architecture



# 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

Download the installer

- <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

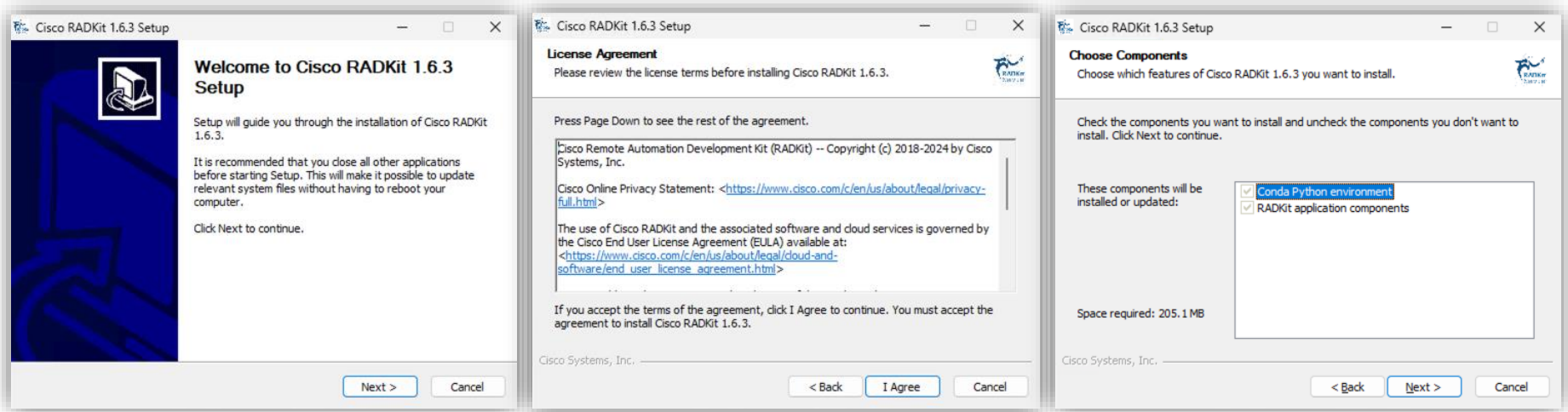
## INDEX OF DOWNLOADS/RELEASE/1.6.3/

|  |                   |           |
|--|-------------------|-----------|
| ../  |                   |           |
| docs/  |                   |           |
| <a href="#">ansible-cisco-radkit-0.6.1.tar.gz</a>          | 24-Jan-2024 09:31 | 3107061   |
| <a href="#">ansible-cisco-radkit-0.6.1.tar.gz.sig</a>      | 24-Jan-2024 09:31 | 3288      |
| <a href="#">cisco_radkit_1.6.3_doc_html.tgz</a>            | 24-Jan-2024 09:31 | 10461870  |
| <a href="#">cisco_radkit_1.6.3_doc_html.tgz.sig</a>        | 24-Jan-2024 09:31 | 3288      |
| <a href="#">cisco_radkit_1.6.3_linux_x86_64.sh</a>         | 24-Jan-2024 09:31 | 141605486 |
| <a href="#">cisco_radkit_1.6.3_linux_x86_64.sh.sig</a>     | 24-Jan-2024 09:31 | 3288      |
| <a href="#">cisco_radkit_1.6.3_macos_arm64_signed.pkg</a>  | 25-Jan-2024 20:26 | 83558219  |
| <a href="#">cisco_radkit_1.6.3_macos_x86_64_signed.pkg</a> | 25-Jan-2024 20:26 | 86285412  |
| <a href="#">cisco_radkit_1.6.3_pip_linux_arm.tgz</a>       | 24-Jan-2024 09:31 | 212815781 |
| <a href="#">cisco_radkit_1.6.3_pip_linux_arm.tgz.sig</a>   | 24-Jan-2024 09:31 | 3288      |
| <a href="#">cisco_radkit_1.6.3_pip_linux_x86.tgz</a>       | 24-Jan-2024 09:31 | 138442211 |
| <a href="#">cisco_radkit_1.6.3_pip_linux_x86.tgz.sig</a>   | 24-Jan-2024 09:31 | 3288      |
| <a href="#">cisco_radkit_1.6.3_pip_macos.tgz</a>           | 24-Jan-2024 09:31 | 122443167 |
| <a href="#">cisco_radkit_1.6.3_pip_macos.tgz.sig</a>       | 24-Jan-2024 09:31 | 3288      |
| <a href="#">cisco_radkit_1.6.3_pip_win.tgz</a>             | 24-Jan-2024 09:31 | 68943074  |
| <a href="#">cisco_radkit_1.6.3_pip_win.tgz.sig</a>         | 24-Jan-2024 09:31 | 3288      |
| <a href="#">cisco_radkit_1.6.3_win64_signed.exe</a>        | 24-Jan-2024 09:31 | 123799640 |
| <a href="#">radkit_verify.py</a>                           | 24-Jan-2024 09:31 | 3056      |

# RADKit – Installation on Windows

## Run the installer

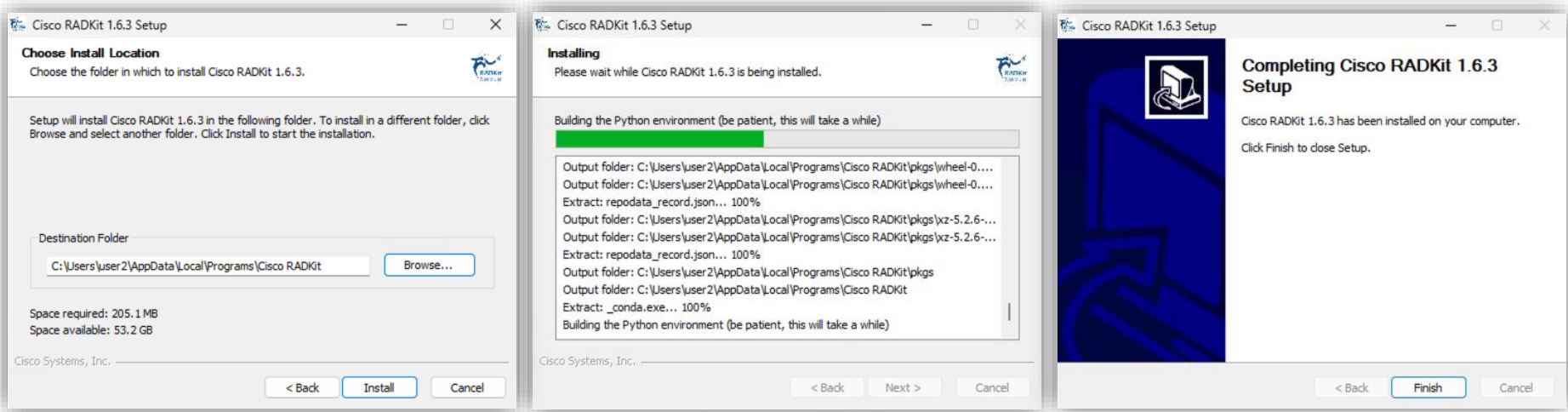
- Installation takes ~2 minutes



# RADKit - Installation on Windows

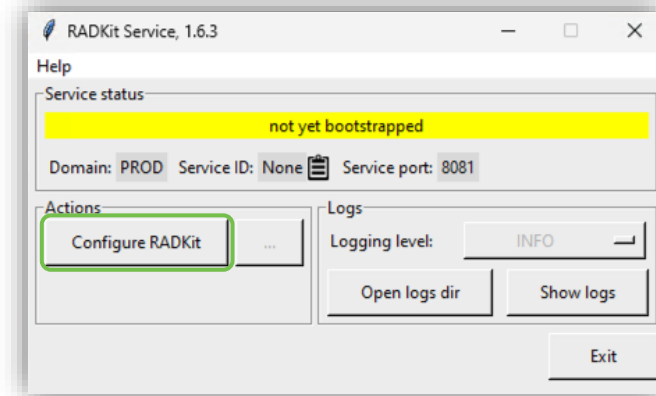
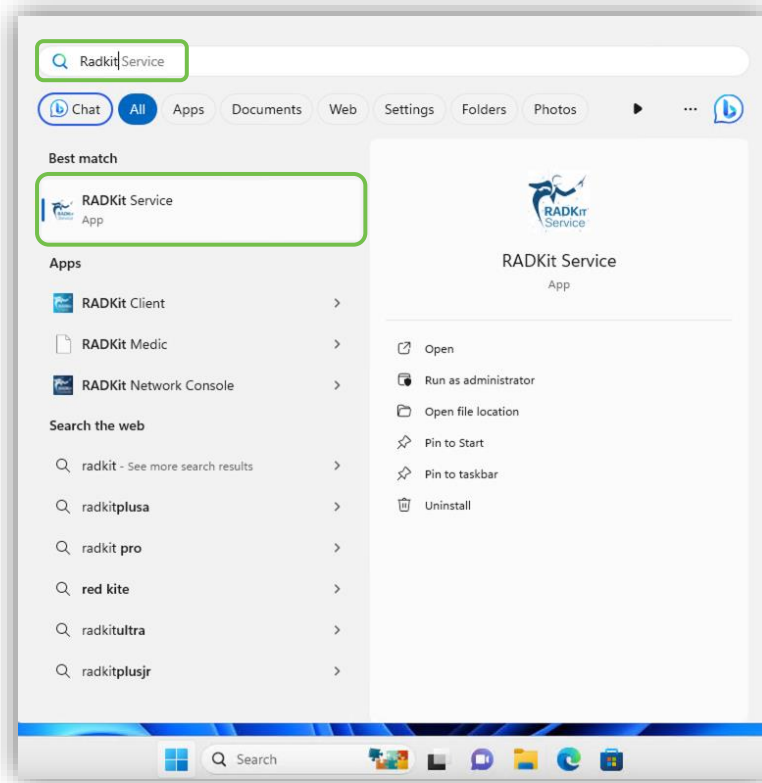
## Run the installer

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



# RADKit – Installation on Windows

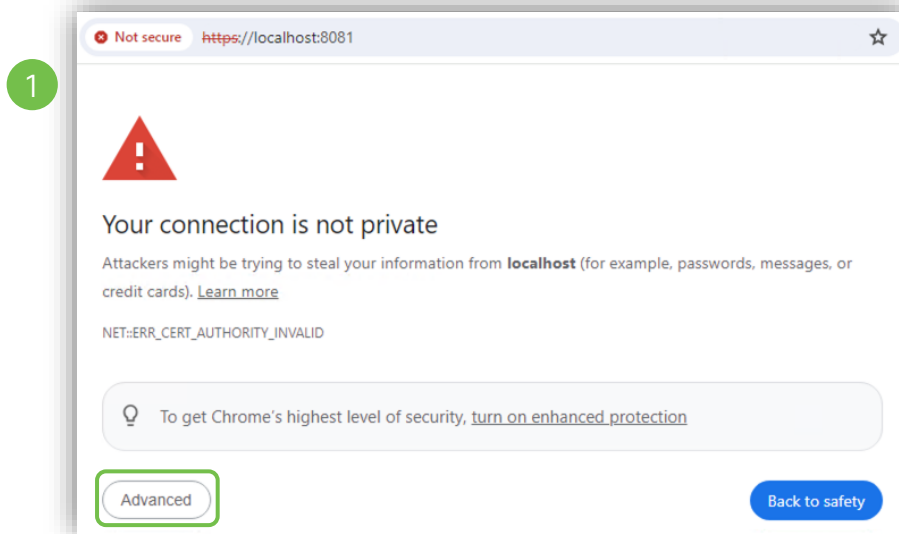
## Run the RADKit Service



# RADKit – Installation on Windows

## Access the GUI

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



# RADKit – Installation on Windows

## Access the GUI

- Create a *superadmin* password and log in

1

The screenshot shows the 'Register superadmin user' page. At the top, there are the Cisco logo and 'Remote Automation Development Kit RADKit Service'. Below the title, a message states: 'No superadmin user was found. Please fill in this form to create a superadmin account.' A green circle with the number '1' is in the top left corner. A green box highlights the 'Password \*' and 'Repeat Password \*' input fields. A 'Submit' button is at the bottom right.

Remote Automation Development Kit  
RADKit Service

### 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 \*  
.....

Repeat Password \*  
.....

Submit

2

The screenshot shows the 'Log in' page. At the top, there are the Cisco logo and 'Remote Automation Development Kit RADKit Service'. Below the title, there are two input fields: 'Username \*' with 'superadmin' entered, and 'Password \*' with '.....' entered. A blue 'Login' button is at the bottom right. A green circle with the number '2' is in the top left corner.

Remote Automation Development Kit  
RADKit Service

### Log in

Username \*  
superadmin

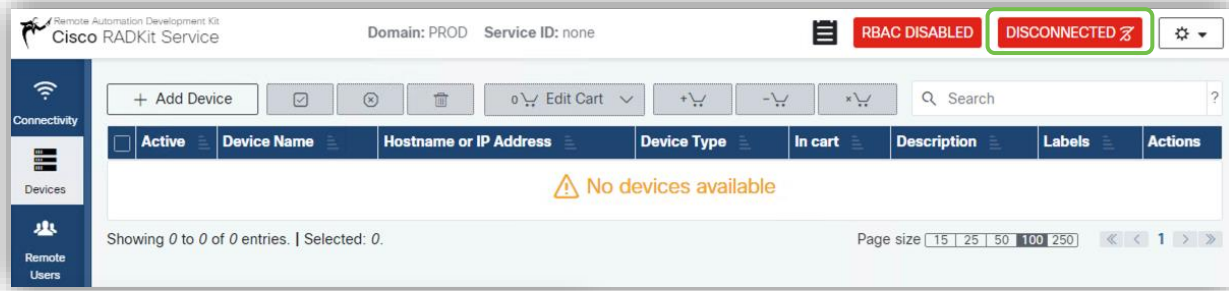
Password \*  
.....

Login

# RADKit - Installation on Windows

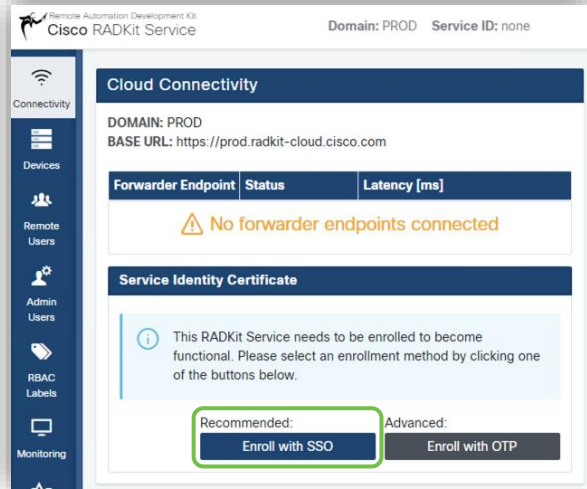
## Enroll the RADKit Service

1



The screenshot shows the Cisco RADKit Service dashboard. At the top, it displays "Domain: PROD" and "Service ID: none". There are two status indicators: "RBAC DISABLED" in a red box and "DISCONNECTED" in a red box with a crossed-out signal icon. The main content area shows a table with columns: Active, Device Name, Hostname or IP Address, Device Type, In cart, Description, Labels, and Actions. The table is empty, and a message "No devices available" is displayed in the center. Below the table, it says "Showing 0 to 0 of 0 entries. | Selected: 0." and "Page size" options (15, 25, 50, 100, 250).

2



The screenshot shows the Cisco RADKit Service dashboard with the "Cloud Connectivity" section expanded. It displays "DOMAIN: PROD" and "BASE URL: https://prod.radkit-cloud.cisco.com". Below this is a table with columns: Forwarder Endpoint, Status, and Latency [ms]. The table is empty, and a message "No forwarder endpoints connected" is displayed. Below the table is the "Service Identity Certificate" section, which contains an information icon and the text: "This RADKit Service needs to be enrolled to become functional. Please select an enrollment method by clicking one of the buttons below." At the bottom, there are two buttons: "Enroll with SSO" (highlighted with a green box) and "Enroll with OTP".

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



# RADKit - Installation on Windows

## Single Sign-On Enrollment

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

Single Sign-On Enrollment

1 ✓ Checking prerequisites

2 Email address

Provide email address for SSO login:

cmorenoa@cisco.com

Submit

3 Connecting to the Access Service

4 OAuth connect

5 Waiting for SSO

6 Requesting service certificate OTP

7 Requesting service certificate

8 Saving the identity

9 Starting/Restarting the service

Cancel

Single Sign-On Enrollment

1 ✓ Checking prerequisites

2 ✓ Email address

3 ✓ Connecting to the Access Service

4 ✓ OAuth connect

5 Waiting for SSO

Follow the SSO login link to continue: [\[CLICK HERE\]](#)

6 Requesting service certificate OTP

7 Requesting service certificate

8 Saving the identity

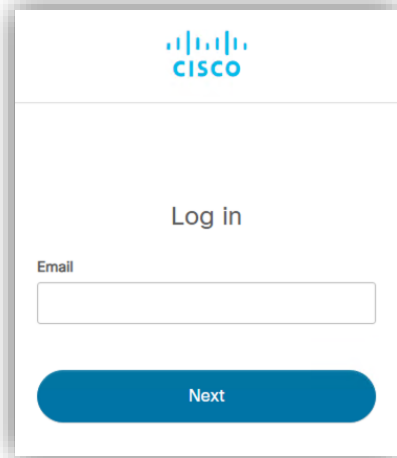
9 Starting/Restarting the service

Cancel

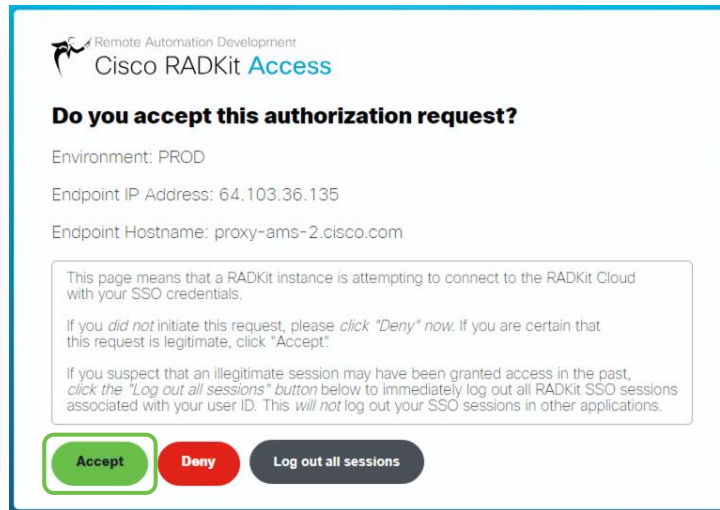
# RADKit - Installation on Windows

## Single Sign-On Enrollment

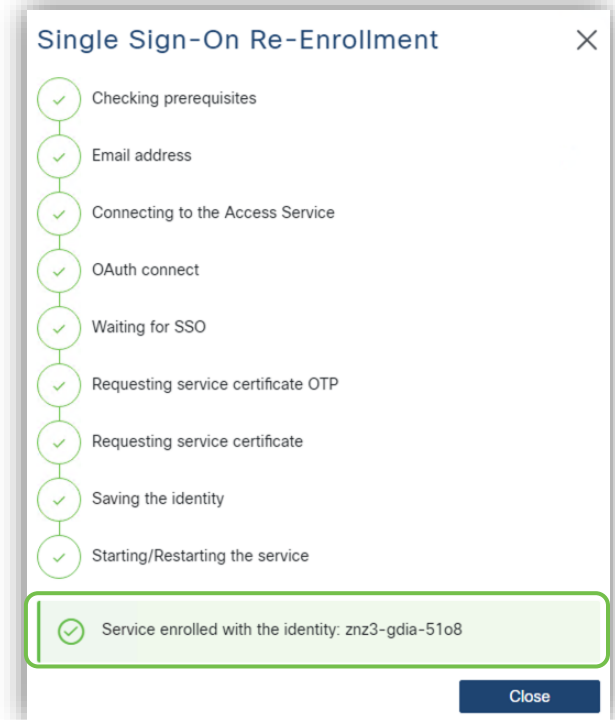
- Log in and accept the authorization request
- The service is enrolled with a unique Service ID



The image shows a Cisco login form. At the top left is the Cisco logo. In the center, it says "Log in". Below that is a text input field labeled "Email". At the bottom is a blue button labeled "Next".



The image shows an authorization request form from Cisco RADKit Access. It asks "Do you accept this authorization request?". The environment is "PROD", the endpoint IP address is "64.103.36.135", and the endpoint hostname is "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 you did not initiate the request, click "Accept" if you are certain it is legitimate, and click "Log out all sessions" if you suspect an illegitimate session. At the bottom are three buttons: "Accept" (green), "Deny" (red), and "Log out all sessions" (dark blue).

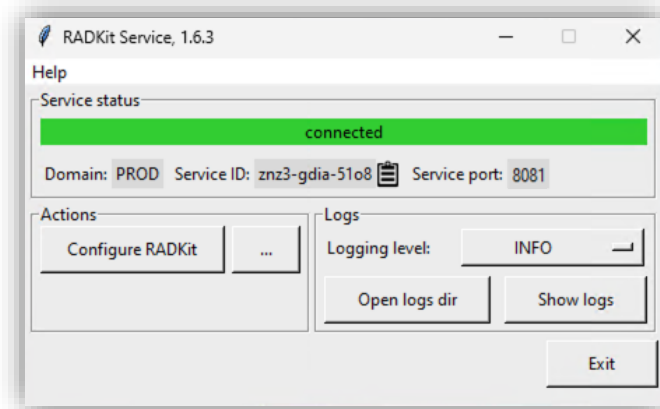


The image shows a "Single Sign-On Re-Enrollment" progress bar. It lists the following steps, each with a green checkmark in a circle: "Checking prerequisites", "Email address", "Connecting to the Access Service", "OAuth connect", "Waiting for SSO", "Requesting service certificate OTP", "Requesting service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

# RADKit - Installation on Windows

## Single Sign-On Enrollment

- 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] |
|---|-----------|--------------|
| <a href="https://prod.radkit-cloud.cisco.com/forwarder-2/">wss://prod.radkit-cloud.cisco.com/forwarder-2/</a> | CONNECTED | 62           |

### Service Identity Certificate

 Certificate valid. service is enrolled.

|                          |                                 |
|--------------------------|---------------------------------|
| <b>Subject Name:</b>     | serialNumber=znz3-gdia-51o8     |
| <b>Cert Serial:</b>      | 942c538212195cfa0d99fe925df7c54 |
| <b>Cert Owner:</b>       | cmorenoa@cisco.com              |
| <b>Cert Granter:</b>     | cmorenoa@cisco.com              |
| <b>Valid from:</b>       | Mon, Jan 29, 2024 2:54 PM       |
| <b>Valid until:</b>      | Sat, Jul 27, 2024 3:54 PM       |
| <b>Last validation:</b>  | Mon, Jan 29, 2024 3:54 PM       |
| <b>Renewal schedule:</b> | Thu, Jul 11, 2024 4:54 PM       |

# RADKit – Installation on Windows

## First steps – Add devices

- 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: znz3-gdia-51o8

RBAC DISABLED CONNECTED

+ Add Device

Connectivity

Devices

| 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

## First steps – Add devices

- 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)?  
access-switch-01

Device Type\*  
IOS XE

Management IP Address or Hostname\*?  
10.10.10.10

Jumphost Name  
- Optional jumphost -

Forwarded TCP ports ?  
Port ranges (eg. '1-1024;8888')

Description

Active (remotely manageable)

Available Management Protocols:  
 Terminal  Netconf  Swagger  HTTP  SNMP

Terminal

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

Allow connecting using obsolete/insecure SSH algorithms  
 Use SSH Tunneling when using this device as a jumphost

Username  
admin

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

Port  
22

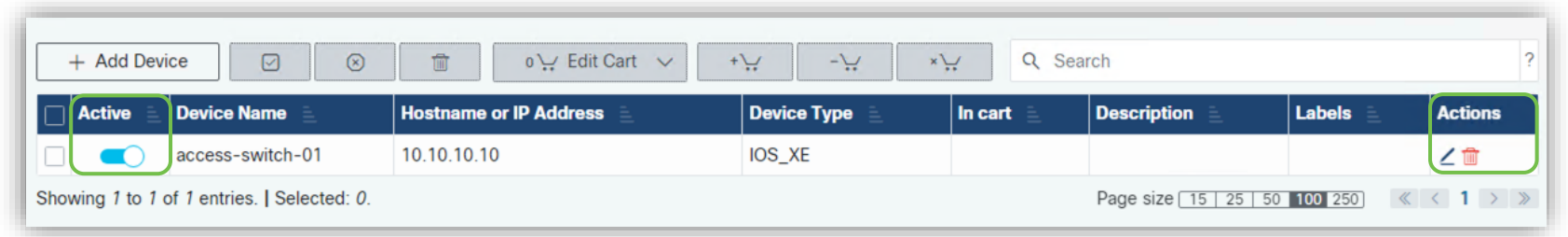
Enable Password ?  
.....  
If left blank, will be set to "" as default

Clear form Add & close Add & continue



# RADKit – Installation on Windows

## First steps – Add devices

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

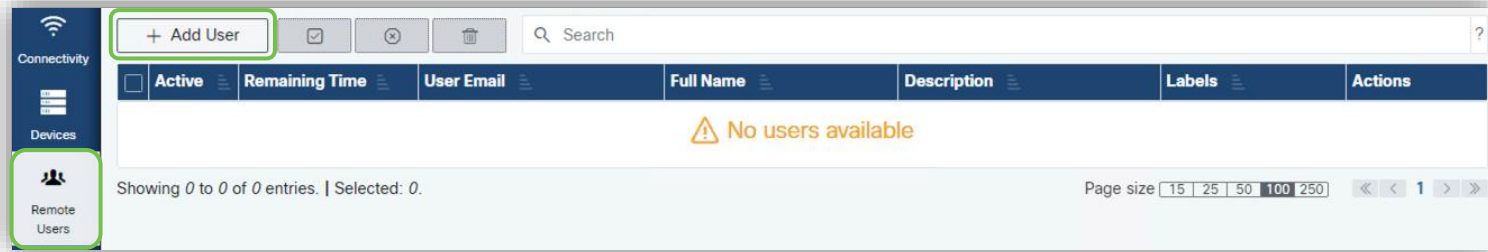


The screenshot displays the RADKit interface for managing devices. At the top, there is a toolbar with buttons for '+ Add Device', a checkmark, a close icon, a trash icon, 'Edit Cart', '+', '-', and 'x' icons, and a search bar. Below the toolbar is a table with the following columns: 'Active', 'Device Name', 'Hostname or IP Address', 'Device Type', 'In cart', 'Description', 'Labels', and 'Actions'. The first row of the table contains the following data: 'Active' (toggle is on), 'Device Name' (access-switch-01), 'Hostname or IP Address' (10.10.10.10), 'Device Type' (IOS\_XE), 'In cart' (empty), 'Description' (empty), 'Labels' (empty), and 'Actions' (edit and delete icons). The 'Active' toggle and the 'Actions' column are highlighted with green boxes. At the bottom of the table, it says 'Showing 1 to 1 of 1 entries. | Selected: 0.' and 'Page size' (15, 25, 50, 100, 250) with navigation arrows.

| Active                              | Device Name      | Hostname or IP Address | Device Type | In cart | Description | Labels | Actions   |
|-------------------------------------|------------------|------------------------|-------------|---------|-------------|--------|---|
| <input checked="" type="checkbox"/> | access-switch-01 | 10.10.10.10            | IOS_XE      |         |             |        |   |

# RADKit - Installation on Windows

## First steps - Add new user



- 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

**Add New User**

User Email\*  
fdetienn@cisco.com  Activate this user

Full Name  
Frederic Detienne

Description  
Remote access for Frederic

USER ACCESS POLICY  
 Manual  
 Time slice (h/m):  
4 00

Label search ? RBAC status: **DISABLED**

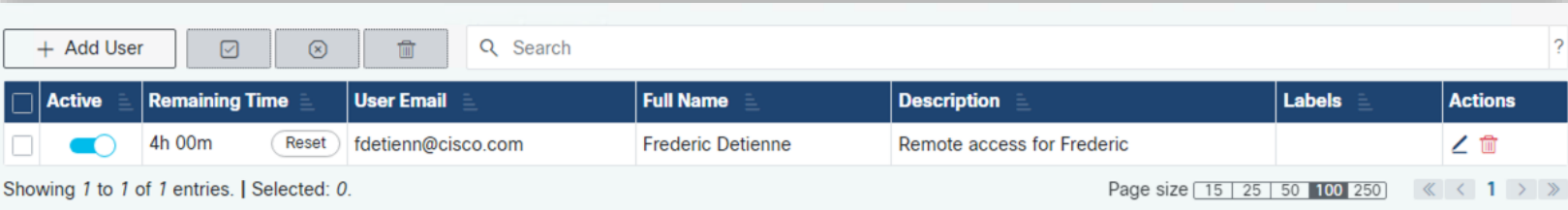
Available Labels - 0 of 0 (click to add)  
NO LABELS AVAILABLE

Selected Labels - 0 (click to delete)

# RADKit - Installation on Windows

## First steps - Add new user

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



The screenshot displays the RADKit user management interface. At the top, there is a '+ Add User' button, a search bar, and three utility icons (checkbox, close, delete). Below this is a table with the following columns: Active, Remaining Time, User Email, Full Name, Description, Labels, and Actions. A single user entry is shown with the following details:

| Active                   | Remaining Time            | User Email         | Full Name         | Description                | Labels | Actions |
|--------------------------|---------------------------|--------------------|-------------------|----------------------------|--------|---------|
| <input type="checkbox"/> | 4h 00m <span>Reset</span> | fdetienn@cisco.com | Frederic Detienne | Remote access for Frederic |        |         |

Below the table, it indicates 'Showing 1 to 1 of 1 entries. | Selected: 0.' and a 'Page size' dropdown menu set to 100.



# Importing devices in bulk from CSV file

# Import devices in bulk from CSV file

## Using RADKit Control

- 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

## CSV file structure

- 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

## CSV file format – sample structure

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  | jumphost | source | sourceDev | meta | enabled | forwarded | terminal.port | terminal.connection | terminal.username | terminal.enable | terminal.term | terminal.term | terminal.password | terminal.enable | terminal.term | terminal.term |
|-----------------|-----------------|-----------------------|--------------|----------|--------|-----------|------|---------|-----------|---------------|---------------------|-------------------|-----------------|---------------|---------------|-------------------|-----------------|---------------|---------------|
| 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

## Importing 1000 devices

2

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:

```
{
  "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
}
```

cmorenoa@cmorenoa-ubuntu:~/Downloads\$

# Import devices in bulk from CSV file

## Importing 1000 devices

- WebUI view after the import operation:

The screenshot displays the Cisco WebUI interface for device management. The top section shows a table with 6 devices (cat9300-001 to cat9300-006). The bottom section shows a table with 8 devices (cat9300-993 to cat9300-1000). The interface includes a sidebar with navigation options (Connectivity, Devices, Remote Users, Admin Users) and a top navigation bar with various controls like 'Add Device', 'Edit Cart', and search.

| Active                   | Device Name  | Hostname or IP Address | Device Type | In cart | Description      | Labels | Actions                              |
|--------------------------|--------------|------------------------|-------------|---------|------------------|--------|--------------------------------------|
| <input type="checkbox"/> | cat9300-001  | 10.0.1.1               | IOS_XE      |         | test switch 1    |        | <a href="#">↶</a> <a href="#">🗑️</a> |
| <input type="checkbox"/> | cat9300-002  | 10.0.1.2               | IOS_XE      |         | test switch 2    |        | <a href="#">↶</a> <a href="#">🗑️</a> |
| <input type="checkbox"/> | cat9300-003  | 10.0.1.3               | IOS_XE      |         | test switch 3    |        | <a href="#">↶</a> <a href="#">🗑️</a> |
| <input type="checkbox"/> | cat9300-004  | 10.0.1.4               | IOS_XE      |         | test switch 4    |        | <a href="#">↶</a> <a href="#">🗑️</a> |
| <input type="checkbox"/> | cat9300-005  | 10.0.1.5               | IOS_XE      |         | test switch 5    |        | <a href="#">↶</a> <a href="#">🗑️</a> |
| <input type="checkbox"/> | cat9300-006  | 10.0.1.6               | IOS_XE      |         | test switch 6    |        | <a href="#">↶</a> <a href="#">🗑️</a> |
| <input type="checkbox"/> | cat9300-993  | 10.0.4.243             | IOS_XE      |         | test switch 993  |        | <a href="#">↶</a> <a href="#">🗑️</a> |
| <input type="checkbox"/> | cat9300-994  | 10.0.4.244             | IOS_XE      |         | test switch 994  |        | <a href="#">↶</a> <a href="#">🗑️</a> |
| <input type="checkbox"/> | cat9300-995  | 10.0.4.245             | IOS_XE      |         | test switch 995  |        | <a href="#">↶</a> <a href="#">🗑️</a> |
| <input type="checkbox"/> | cat9300-996  | 10.0.4.246             | IOS_XE      |         | test switch 996  |        | <a href="#">↶</a> <a href="#">🗑️</a> |
| <input type="checkbox"/> | cat9300-997  | 10.0.4.247             | IOS_XE      |         | test switch 997  |        | <a href="#">↶</a> <a href="#">🗑️</a> |
| <input type="checkbox"/> | cat9300-998  | 10.0.4.248             | IOS_XE      |         | test switch 998  |        | <a href="#">↶</a> <a href="#">🗑️</a> |
| <input type="checkbox"/> | cat9300-999  | 10.0.4.249             | IOS_XE      |         | test switch 999  |        | <a href="#">↶</a> <a href="#">🗑️</a> |
| <input type="checkbox"/> | cat9300-1000 | 10.0.4.250             | IOS_XE      |         | test switch 1000 |        | <a href="#">↶</a> <a href="#">🗑️</a> |

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

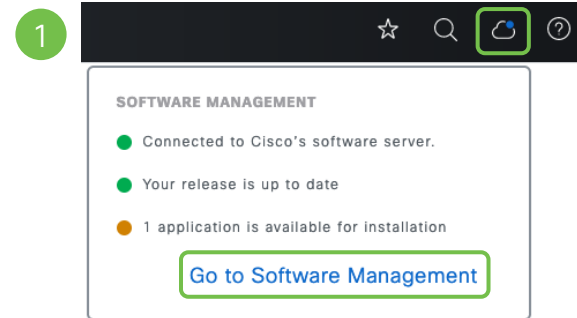
ex-Cisco DNA Center

# RSA – Remote Support Authorization

## Step 1 - Install Application Package

- 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 Cisco DNAC v2.3.5.x




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

## Step 2 – Manage SSH Credentials

- 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

## Step 2 – Manage SSH Credentials

- 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

## Step 2 – Manage SSH Credentials

- 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

## Step 3 – Create a New Authorization

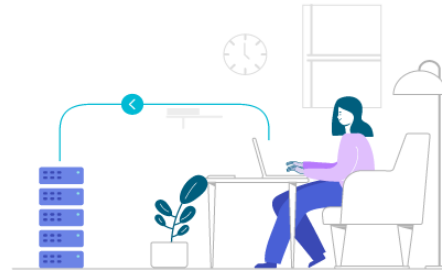
- Grant remote access to a Cisco specialist
- Access can be removed at any time
- Access is granted for 24 hours by default

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

## Step 3 – Create New 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.

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

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\*

cmorenoa@cisco.com

Existing Case Number(s)

0123456789

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

Access Justification

Remote Access for Carlos Moreno (TAC)

Review

Back

Next Step

### 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 3 – Create New 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 Cisco DNA Center.

#### Set Up the Authorization [Edit](#)

Cisco Specialist Email Address cmorenoa@cisco.com  
Existing Case Numbers 0123456789  
Access Justification Remote Access for Carlos Moreno (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.

cmorenoa@cisco.com is scheduled to sign in to Cisco DNA Center on **25 Jan 2024, 12:19 pm CET** for **24** hours using **hzmj-phk4-ztyb** 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

## Step 4 – Share the Support ID with the Cisco specialist

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

The screenshot displays the Catalyst Center interface for Remote Support Authorization. The top navigation bar includes the Cisco logo, 'Catalyst Center', and the page title 'Remote Support Authorization'. A user profile 'admin' is visible in the top right. The main content area is divided into a summary section and a detailed view section.

**SUMMARY**

|                      |                        |                     |
|----------------------|------------------------|---------------------|
| 18                   | 1                      | 17                  |
| Total Authorizations | Current Authorizations | Past Authorizations |

Navigation tabs: Create New Authorization, **Current Authorizations**, Past Authorizations, Manage SSH Credentials

Status: **All** | Scheduled | Active

**cmorenoa@cisco.com**

|           |                           |
|-----------|---------------------------|
| Active on | 25 Jan 2024, 12:19 pm CET |
| Duration  | 24 hours                  |

[Revoke Authorization](#) [View Logs](#)

**cmorenoa@cisco.com**

|                                |  |
|--------------------------------|--|
| Support ID                     | hzmj-phk4-ztyb   |
| Cisco Specialist Email Address | cmorenoa@cisco.com   |
| Case Number(s)                 | 0123456789   |
| Date                           | 25 Jan 2024, 12:19 pm CET  |
| Duration                       | 24 hours   |
| Description                    | Remote Access for Carlos Moreno (TAC)  |
| Access Permission              | All SSH-enabled network devices managed by Cisco DNA Center, All Cisco DNA Center nodes (including witness, if disaster recovery is enabled) |

Demo

CISCO *Live!*



# Help Us, Help You!



Visit <https://radkit.cisco.com> (documentation, downloads, help)



Try RADKit yourself at the Walk-in Labs (near the World of Solutions)



Talk to one of our engineers and ask for a 1:1 RADKit demo at the TAC booth (World of Solutions)



The bridge to possible

Thank you

CISCO *Live!*

The Cisco Live! logo features the word "CISCO" in a bold, black, sans-serif font, followed by "Live!" in a black, cursive script font. The background of the entire image is a vibrant, multi-colored abstract pattern of overlapping, wavy bands in shades of red, orange, yellow, green, and blue, creating a sense of motion and energy.

CISCO *Live!*

Let's go