



CX Cloud Admin Settings

User Guide

Contents

CX Cloud Admin Settings Overview	3
Asset Groups	4
Identity & Access	6
Partner Access.....	9
Data Collection.....	11
Data Sources	13
Insights	16

CX Cloud Admin Settings Overview

Click the **Settings** icon to access the CX Cloud configuration and administration menus



Requirements:

Super Admin role is required to manage all CX Cloud settings.

Admin role only has permission to modify Data Collection, Data Sources, and Insights configuration.



Asset Groups

Asset groups is a customizable field that can be assigned to devices in order to control granular user access to devices. Asset groups can also be used for compliance policies and reporting. Devices may be assigned to multiple asset groups.



Identity & Access

Identity and Access settings allow you to manage user access and permissions to CX Cloud. You can update Rules, Users, and Roles from this menu.



Partner Access

Partner Access settings allow you to approve, deny, and modify Partner access to your CX Cloud data.



Data Collection

Schedule asset inventory scans and diagnostic scans to enable Advisories plus Insights and Analytics capabilities including Rapid Problem Resolution.



Data Sources

Add contracts to view more assets in CX Cloud. Configure telemetry data sources for CX Cloud, including CX Cloud Agent, DNA Center, and Intersight. Configure Meraki API connection to CX Cloud.



Insights

Set up L2 Insights features including Optimal Software Versions, Automated Fault Management, and Regulatory Compliance.

Asset Groups

Asset groups is a customizable field that can be assigned to devices in order to control granular user access to devices. Asset groups can also be used for compliance policies and reporting. Devices may be assigned to multiple asset groups. The default asset group is “All Assets” which automatically includes all devices.

1) Create an Asset Group

- a. Click the **Create New Group** button



- b. Enter a **Group Name**
- c. (Optional) **Search** for Devices or Filter on **Location** and **Product Types**
- d. Select the Devices you want to add to the group (or select ALL)
- e. Click **SAVE**

Create Asset Group

Group Name

Showing 10 of 128 total assets | 7 assets selected for this group Show only selected assets

Asset Attributes

All | Search

Locations

Find a location

- ASHBURN,VA,USA
- BANGALORE,KA,IND
- KBENHAVN,HOVEDSTADEN,DNK
- MILPITAS,CA,USA
- North America
- SAN JOSE,CA,USA

Product Types

Find a product type

- Cisco Secure Endpoint Cloud subscription
- Cloud and Systems Management
- Connected Safety and Security
- Data Center Switches

<input type="checkbox"/>	Name ▲	Description	Product ID	Contract Number
<input checked="" type="checkbox"/>	ifav151-leaf1	Nexus 9300 Series, 32p 40G QSFP+	N9K-C9332PQ	
<input checked="" type="checkbox"/>	ifav151-leaf12	Nexus 9300 with 48p 10/25G SFP+ and 6p 100G QSFP28	N9K-C93180YC-EX	
<input type="checkbox"/>	ifav151-leaf14	Nexus 9300 with 48p 10/25G SFP+ and 6p 100G QSFP28	N9K-C93180YC-EX	
<input checked="" type="checkbox"/>	ifav151-leaf2	Nexus 9300 Series, 32p 40G QSFP+	N9K-C9332PQ	
<input checked="" type="checkbox"/>	ifav151-leaf3	Nexus 9300 Series, 32p 40G QSFP+	N9K-C9332PQ	
<input type="checkbox"/>	ifav151-leaf5	Nexus 9300 Series, 32p 40G QSFP+	N9K-C9332PQ	
<input checked="" type="checkbox"/>	ifav151-leaf6	Nexus 9300 Series, 32p 40G QSFP+	N9K-C9332PQ	
<input type="checkbox"/>	ifav151-leaf7	Nexus 9300 Series, 32p 40G QSFP+	N9K-C9332PQ	
<input type="checkbox"/>	ifav151-leaf8	Nexus 9300 Series, 32p 40G QSFP+	N9K-C9332PQ	
<input type="checkbox"/>	ifav151-spine1	Nexus 9504 Chassis with 4 linecard slots	N9K-C9504	

2) Edit or Delete an Asset Group

- a. Click on an Asset Group from the list

(Note: if you have a large number of asset groups, you can use search to limit the list results)

Create New Group
Create New Group With CSV File
Search asset gro

Group Name ▲	Assets
21sachinapril	3
22 march 23	2
A_New_Test	155
All Assets ?	1306
AMP demo	1
Assets_Compute	1
bsdddte	2

- b. Select **Edit** or **Delete**



If editing...

- c. **Search** for Devices or Filter on **Location** and **Product Types**
- d. Select or de-select devices you want to add or remove
- e. Click **SAVE**

Create Asset Group

Group Name

Showing 10 of 1,306 total assets | 0 assets selected for this group Show only selected assets

Asset Attributes	<input type="checkbox"/> Name ▲	Description	Product ID	Contract Number
<input type="checkbox"/> All Search <input type="text"/>	<input type="checkbox"/>	C220-WZP230411SV UCS C220 M5 SFF 10 HD w/o CPU, mem, HD, PCIe, PSU	UCSC-C220-M5SX	203864243
<input type="checkbox"/> Locations	<input type="checkbox"/>	C220-WZP2321121K UCS C220 M5 SFF 10 HD w/o CPU, mem, HD, PCIe, PSU	UCSC-C220-M5SX	204682480
<input type="checkbox"/> Find a location <input type="text"/>	<input type="checkbox"/>	C220-WZP2321122B UCS C220 M5 SFF 10 HD w/o CPU, mem, HD, PCIe, PSU	UCSC-C220-M5SX	204682480
<input type="checkbox"/> ASHBURN,VA,USA	<input type="checkbox"/>	2c:3f:0b:60:ea:40 Meraki MS120-8FP 1G L2 Cloud Managed 8x GigE 124W PoE Switch	MS120-8FP-HW	204393077
<input type="checkbox"/> BANGALORE,KA,IND	<input type="checkbox"/>	2c:3f:0b:61:35:04 Meraki MS120-8FP 1G L2 Cloud Managed 8x GigE 124W PoE Switch	MS120-8FP-HW	204393077
<input type="checkbox"/> KBENHAVN,HOVEDSTADEN,DNK	<input type="checkbox"/>	2c:3f:0b:61:36:c7 Meraki MS120-8FP 1G L2 Cloud Managed 8x GigE 124W PoE Switch	MS120-8FP-HW	204393077
<input type="checkbox"/> MILPITAS,CA,USA	<input type="checkbox"/>	2c:3f:0b:d4:2a:00 EOS Meraki MX100 Router/Security Appliance	MX100-HW	204393077
<input type="checkbox"/> North America	<input type="checkbox"/>	2c:3f:0b:f3:8f:aa Meraki MG21 Cellular Gateway - N America	MG21-HW-NA	204393077
<input type="checkbox"/> SAN JOSE,CA,USA	<input type="checkbox"/>	34:56:fe:56:d2:8a Meraki MR70 Cloud Managed AP	MR70-HW	204393077
<input type="checkbox"/> Product Types	<input type="checkbox"/>	38:84:79:04:b5:00 Meraki MS390 24GE L3 POE+ Switch	MS390-24P-HW	204393077
<input type="checkbox"/> Find a product type <input type="text"/>	<input type="checkbox"/>			
<input type="checkbox"/> CISCO_INTERSIGHT				
<input type="checkbox"/> Cisco Secure Endpoint Cloud subscription				
<input type="checkbox"/> Cloud and Systems Management				
<input type="checkbox"/> Connected Safety and Security				

Identity & Access

Identity and Access settings allow you to manage user access and permissions to CX Cloud. You can update **Rules**, **Users**, and **Roles** from this menu.

- 1) **Roles** – Click on a Role to view the permissions associated with them. Roles cannot be edited.

Role	Summary
Super Admin	Can access all capabilities across all assets. Can manage all CX Cloud users and their access.
Admin	Can install/configure CX Collector and set scan/collection schedules, in addition to all capabilities of a Standard User.
Standard User	Can access Lifecycle features and insights, cases, advisories, and other information related to assets.
Read-Only User	Can access limited Lifecycle features and view certain information about assets.
Assets User	Cannot access any Lifecycle features, but can access insights, cases, advisories, and other information related to assets.

- 2) **Rules** – Rules specify which users can access which assets. Rules also define what permissions the users have on those assets. A rule combines a user group with an asset group. User groups must have a rule to determine which role applies to its users.

Create a Rule

- a. Click on the **Create Rule** button



- b. Enter a **Rule Name**, **User Group**, **Role**, and **Asset Group**
- c. Click **SAVE**

Rule [?]	User Groups	Roles	Asset Groups	
Rule Name Example	These user groups... Engineers ×	...have these roles... Read-Only User ▼	...for these assets. A_New_Test ×	× Cancel Save

Edit or Delete a Rule

- a. Find the Rule you want to modify

(Note: if you have a large number of rules, you can use search to limit the list results)

- b. Select **Edit** or **Delete**

Test Only [?]	Standard User	? ⋮
------------------------	---------------	-------------------------------

c. Make your changes and click **SAVE**

Edit

Delete

- 3) **Users** – This menu will allow you to Add Users, Remove Users, and Assign Users to User Groups. Use the Toggle switch to choose between **User Group** or **Users**

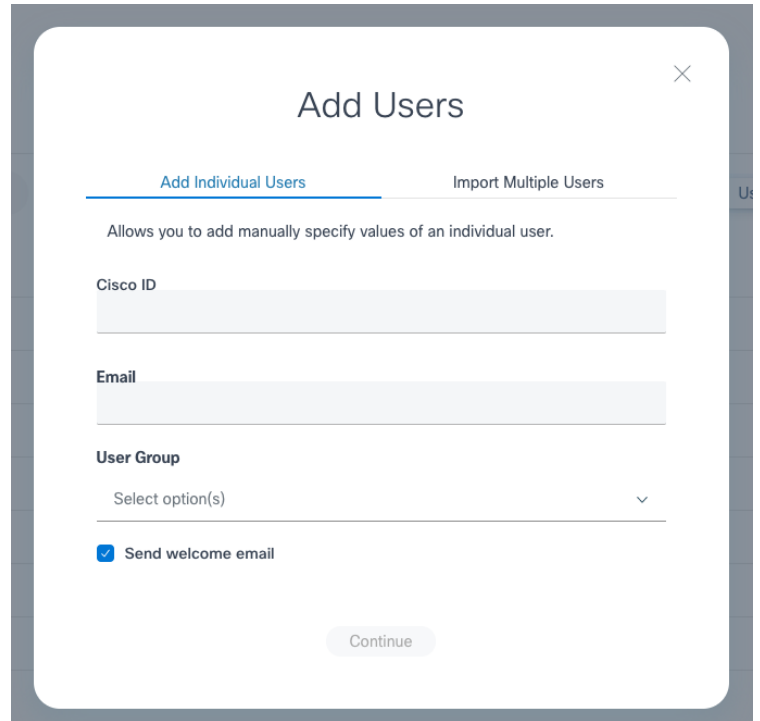


Add a User

- Select the **Users** toggle button
- Click the **Add User** button

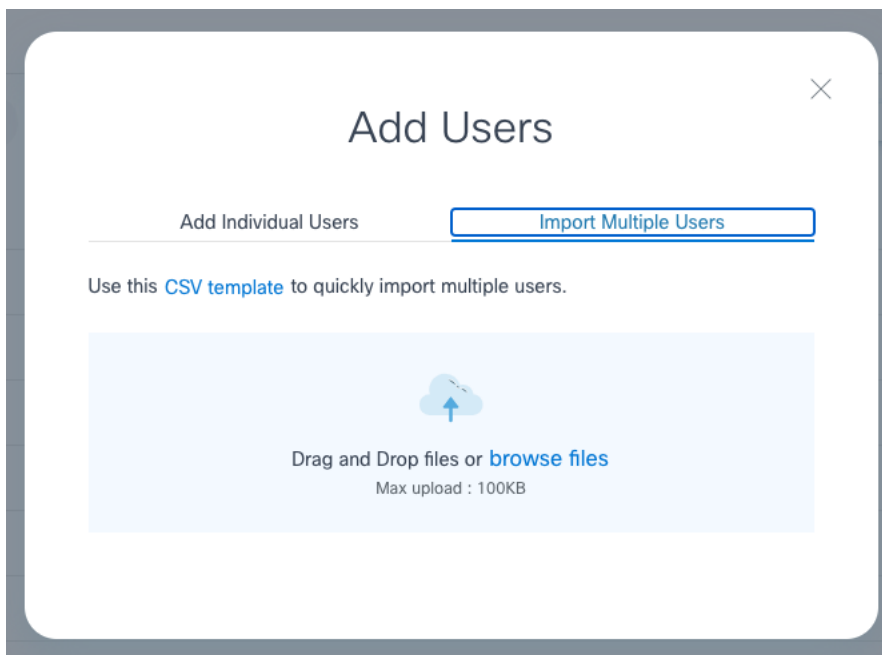


- Enter the **Cisco ID, Email, and User Group**
- Check the "Send welcome email" box so new users receive an email to log in
- Click **Continue**



You also have the option to import users from a comma - separated (CSV) file.

- Select **Import Users from File**
- Use the Template provided and Upload into CX Cloud



Delete a User

- a. Find the User you want to Delete

(Note: if you have a large number of users, you can use search to limit the list results)

- b. Select **Remove user from CX Cloud**



4) User Group

- a. Select the **User Group** toggle button
- b. Click the **Create User Group** button
- c. Enter a **Group Name**
- d. (Optional) - Select Users you want to add to the group
- e. Click **SAVE**



Partner Access

Partner Access settings allow you to approve, deny, and modify Partner access to your CX Cloud data

- 1) Grant Access for Partners
 - a. Click Review Request and approve or deny access

Partner ▲	Access	Approved Users	
CX Demo Partner One	Campus Network, Cloud Network, Data Center Compute, Hybrid Cloud, Integrated Secure Operations, Meraki Network	4	
CX Partner Demo Two GmbH	-	0	Review Request
CXPARTNERDEMO	Campus Network, Cloud Network, Data Center Compute, Hybrid Cloud, Integrated Secure Operations, Meraki Network	1015	

- 2) Revoke Partner Access for Individual Users
 - a. Click on the Partner you want to modify
 - b. Click **User Access** to revoke access from individual users within the partner

[USER ACCESS](#) [DATA ACCESS](#)

- c. Click **Revoke Access** on the users you want to exclude

Name	Email	Role	
John Doe	jdoe@cisco.com	Administrator	Revoke
Jane Doe	janedoe@cisco.com	Administrator	Revoke
Brian Halel	bhalel@cisco.com	Administrator	Revoke

- d. Excluded Users will be shown in the **No Access** tab



3) Revoke All Partner Access

- a. Click on the Partner you want to modify
- b. Click **Data Access**

USER ACCESS DATA ACCESS

- c. Click **Manage Access** to Deny or Approve all access for this partner

Manage Access

Manage Partner Access

Select the data you want CXPARTNERDEMO's designated users to view.

What Data Will Be Shared With My Partner? ▾

Entire portfolio (includes any future purchases to your CX Cloud portfolio)

Deny Access Approve Access

Data Collection

Schedule Asset inventory scans and Diagnostic Scans from DNA Center to enable Insights and Analytics. Enable Rapid Problem Resolution to automatically attach diagnostic scan output to TAC cases.

Diagnostic scans collect data regarding the health and configuration of devices in your network. This information allows CX Cloud to diagnose problems and recommend fixes. CX Cloud also makes proactive recommendations to prevent network issues before they arise. Diagnostic scans can be performed individually on devices covered at CX Level 1. Devices covered at CX Level 2 and above can be scanned in bulk, on a regular schedule.

Inventory scans verify the presence of devices on your network. Regular inventory scans ensure the assets shown in CX Cloud will always be up-to-date. You can customize the inventory scan schedule to ensure that data collection doesn't disrupt your network.

Pre-requisite: To schedule scans, telemetry must be installed and configured.

1) Schedule Diagnostic Scan

- a. Click **Schedule New Diagnostic Scan**
- b. Select your **DNA Center**
- c. Choose a Schedule (**Daily/Weekly/Monthly, Day, Time**)
- d. Select **All** or Select individual Devices
- e. Click **Add** , Click **Save Changes**

New Scheduled Scan

The screenshot shows the 'New Scheduled Scan' configuration page. On the left, under 'Data Sources', there is a dropdown menu with 'Select All' and '198.18.129.100/dnac.dcloud.cisco.com' as options. To the right, the 'Schedule' section is configured with 'Weekly' frequency, 'Monday' day, and '1:00 am' time in 'PDT'. Below these settings are two empty tables with columns 'Device', 'Source IP', and 'IP Address'. Between the tables are 'Add' and 'Remove' buttons. A 'Save Changes' button is located at the top right of the configuration area.

2) Schedule Inventory Scan

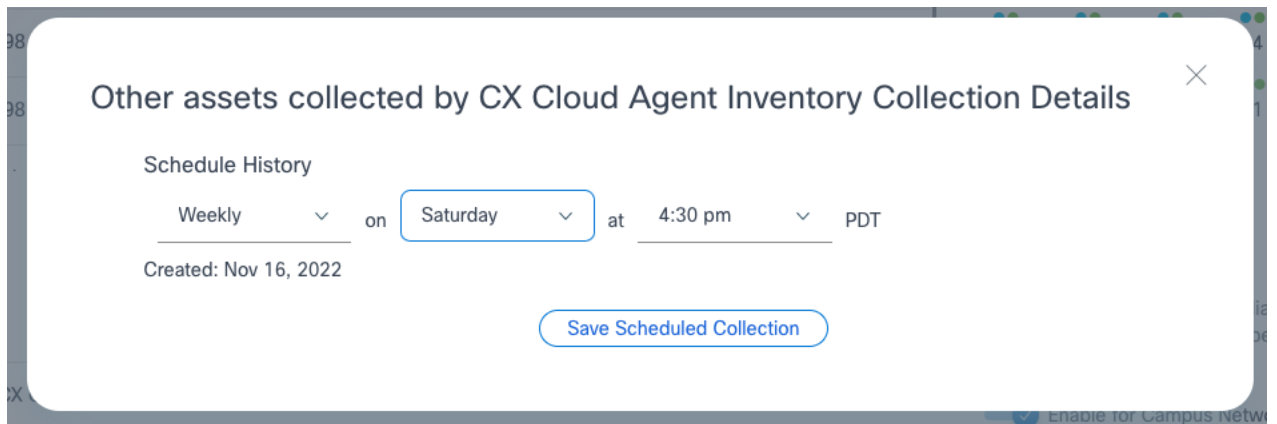
- a. Click on the three dots on the right side of a row in the **Inventory Collection**
- b. Select **Edit Schedule**

The screenshot shows the 'Inventory Collection' table with the following data:

Source	Schedule
Other assets collected by CX Cloud Agent	Fridays at 04:30 PM PDT
198.18.129.100/dnac.dcloud.cisco.com	Daily at 04:30 PM PDT

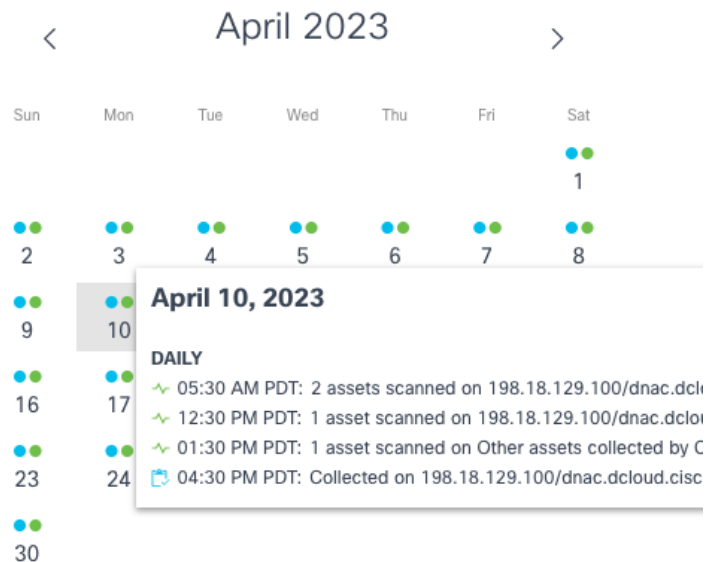
A 'Rapid Pro' banner is present on the right side of the table, and an 'Edit Schedule' button is overlaid on the table's right side.

- c. Choose a Schedule (**Daily/Weekly/Monthly, Day, Time**)
- d. Click **Save Scheduled Collection**



3) View Scan Schedule

- a. Click Calendar Arrows <> to view Future or Past scan schedules
- b. Hover over specific dates to view the details



4) Enable/Disable Rapid Problem Resolution

- a. Select/Deselect the **Enable for Campus Network** Toggle Button to turn Rapid Problem Resolution on/off

Rapid Problem Resolution

Automate data collection and diagnostics when a support case is opened. This helps Cisco experts diagnose and troubleshoot problems faster.



Data Sources

View current Data Sources

Data Sources

Data Storage Region: United States

Add A Data Source

7 data sources






Name	Type	Data Last Updated	Status
CX Cloud Agent	CX Cloud Agent v2.2.4	6 minutes ago	● Running
198.18.129.100	Cisco DNA Center	6 minutes ago	● Reachable
Other assets collected by CX Cloud Agent	Seed file	6 minutes ago	● 132 reachable
Contract	Covered Assets	17 hours ago	● Last Collection Succeeded
Cloud Network	Intersight	-	● First Collection Pending ?
Data Center Compute	Intersight	11 hours ago	● Last Collection Succeeded
Meraki	Meraki	19 hours ago	● Collection Completed

To configure telemetry connections or add contracts, click Add A Data Source

Add A Data Source

Select a Data Source to connect

Which data source would you like to connect?

-  **Cisco DNA Center**
Uses CX Cloud Agent to support Campus Network Connect
-  **Contracts**
Supports all Success Tracks and offers Connect
-  **Intersight**
Supports Data Center Compute and Cloud Network Connect
-  **Meraki dashboard**
Supports Meraki Connect
-  **Other Assets**
Uses CX Cloud Agent to support Campus Network Connect

- 1) For the Campus Network Success Track, Install and Configure DNA Center and CX Agent
 - a. Refer to installation guides: [Installing CX Agent](#) and [CX Agent Overview](#)
- 2) For Cloud Network or Data Center Compute Success Tracks, connect Intersight
 - a. Refer to installation guides: [Integrating Intersight with CX Cloud](#) and [Intersight Overview](#)
- 3) For Meraki, connect the Meraki dashboard
 - a. Refer to installation guide: [Integrating Meraki with Cisco CX Cloud](#)
 - b. Enter your Meraki API Credentials into CX Cloud
- 4) To add contracts, click Connect and and Open a Support Case

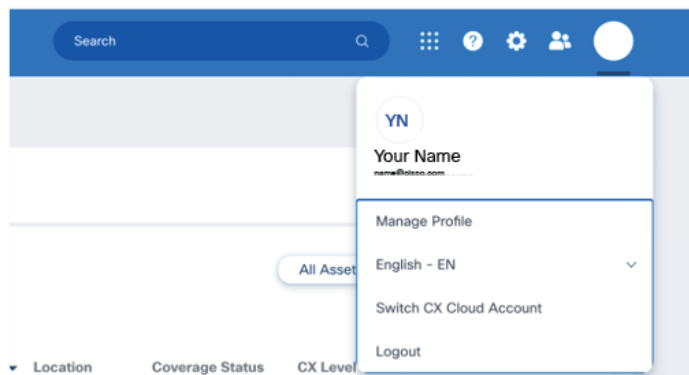


Contact support

To add or remove contracts, open a support case. Select "CX Cloud Support" and include the relevant contract numbers.

[Open Support Case](#)

- a. Ensure your CCO ID is associated with the contracts you request to add by emailing web-help-sr@cisco.com with your company name, CCO ID, and contract numbers.
- b. Another way to associate your CCO ID is to:
 - i. Click the **Initials Icon** in CX Cloud
 - ii. Click **Manage Profile**



iii. Click Edit Personal Information



iv. Once redirected to id.cisco.com, click **Access Management**



v. Click **Add Access**



vi. Select **TAC and RMA case creation, Software Download, support tools, and entitled content on Cisco.com**

Add Access X

What type of access are you requesting?

Software Download, support tools, and entitled content on Cisco.com

TAC and RMA case creation, Software Download, support tools, and entitled content on Cisco.com

Your entitlement to services is defined by your contract's coverage terms.

If you are an end customer who purchased a Partner-Branded Service support contract, you are only entitled to Software Download, support tools, and entitled content on Cisco.com, and must contact your Reseller in the event that TAC support or RMA is needed.

Go

vii. Click **Go**

viii. Enter the contract numbers and submit

Insights

Insights Tab will only appear if you have the Campus Network Level 2 Success Track.
Configure Optimal Software Version, Automated Fault Management, and Regulatory Compliance.

- 1) **Optimal Software Version** will set the schedule for updating new Software Version Suggestions and Trending

- a. Select **Software** Tab

[Software](#) [Faults](#) [Compliance](#)

Next Suggestion Date May 13, 2023

Suggestions Schedule Every Week **Starting** 04/22/2023

- 2) **Automated Fault Management (AFM)** will automatically create a TAC case and/or send an E-mail notification if a device Fault is detected.

- a. Select the **Faults** Tab
 - b. Select the Enter Cisco ID to be used for automatically generated Cases
(ID must be mapped to ALL support contracts for case creation entitlement)
 - c. Click the Toggle button to Enable/Disable Automatic **Cases** creation and **Email Notifications**
 - d. Note that Support Case Routing is only for Japan support teams

Software [Faults](#) Compliance

Fault Settings [Fault Catalog](#)

Cisco ID associated to generate Faults cases ?
CxcpsmartuserTwoTwo62413 [↗](#)

Cases Enabled
Automatically open a TAC support case for faults

Support Case Routing - Japan Disabled
Route all cases opened for faults to the Japan support team

Email Notifications Enabled
Automatically sends email when notification enabled faults are detected

- e. Click the **Fault Catalog** toggle button



- f. Enable/Disable Faults, Cases and Email Notifications by selecting a Fault or multiple Faults, then click the 3 vertical dots (kebab) menu on the right side to expand the menu

Software [Faults](#) Compliance

Fault Settings **Fault Catalog**

Search

634 Total Faults

<input type="checkbox"/>	Severity ▲	Title	Category	Case Automation	Fault Status	
<input type="checkbox"/>	● Critical	Device crashed	System	Enabled	Enabled	⋮
<input type="checkbox"/>	● Critical	Device may crash or behave abnormally	CPU-Memory	Enabled	Enabled	Enabled ⋮
<input type="checkbox"/>	● Critical	Low memory on device	CPU-Memory	Enabled	Enabled	Enabled ⋮
<input type="checkbox"/>	● Critical	Process failed	CPU-Memory	Disabled	Enabled	Disabled ⋮
<input type="checkbox"/>	● Critical	Process restarted too many times	CPU-Memory	Enabled	Enabled	Enabled ⋮
<input type="checkbox"/>	● Critical	A limit of learning routes has been reached on the device.	System	Enabled	Enabled	Enabled ⋮

Enable Case Automation (0 Selected)
 Disable Case Automation (0 Selected)
 Enable Email Notifications (0 Selected)
 Disable Email Notifications (0 Selected)

3) **Compliance** settings enable PCI and HIPAA regulatory compliance check for specific Asset Groups

- a. Select the **Compliance** Tab
- b. Select a Success Track

SUCCESS TRACK

Select ▲

- Campus Network
- Cloud Network
- Integrated Secure Operations
- Data Center Compute
- Meraki Network
- Hybrid Cloud

c. Click the **Regulatory Compliance** toggle button to turn this feature on/off

SUCCESS TRACK

Campus Network

REGULATORY COMPLIANCE

On

Regulatory compliance checks provide actionable insights and analytics to help you achieve network compliance.

Policy Profiles

Create Policy Profile

Run Compliance Check



Regulatory Type	Compliance Check	Last Checked	Asset/ Asset Groups
HIPAA	Enabled	3 hours ago	Asset Groups (3)
PCI	Enabled	3 days ago	Asset Groups (2)

Americas Headquarters

Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters

Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters

Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at <https://www.cisco.com/go/offices>.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)