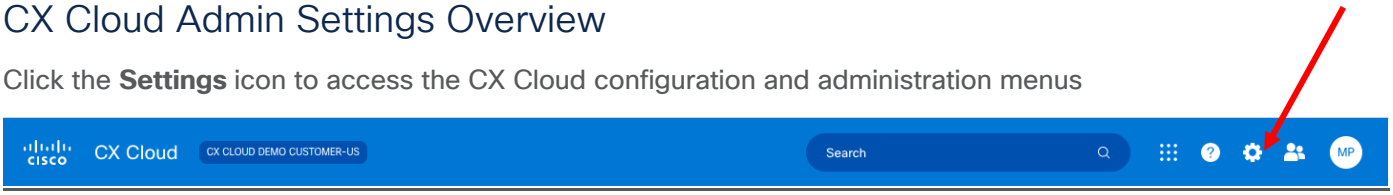
CX Cloud Admin Settings

User Guide

Contents

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**

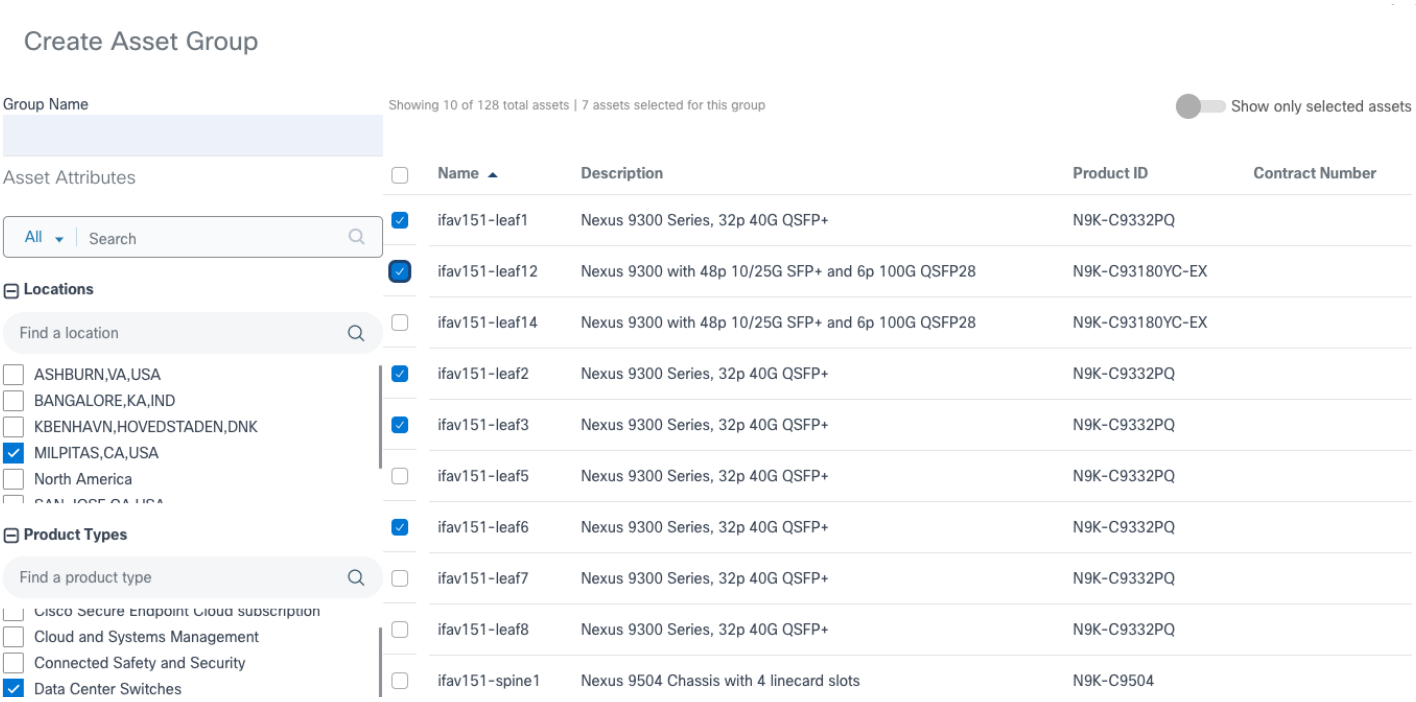
   a. Click the **Create New Group** button

   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)

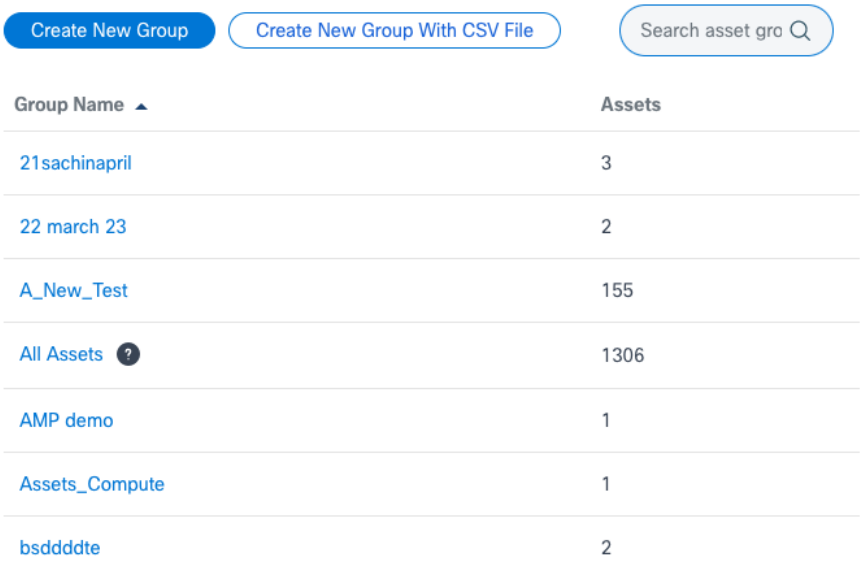
   e. Click **SAVE**



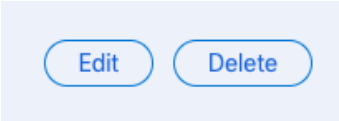
2) Edit or Delete an Asset Group

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)



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

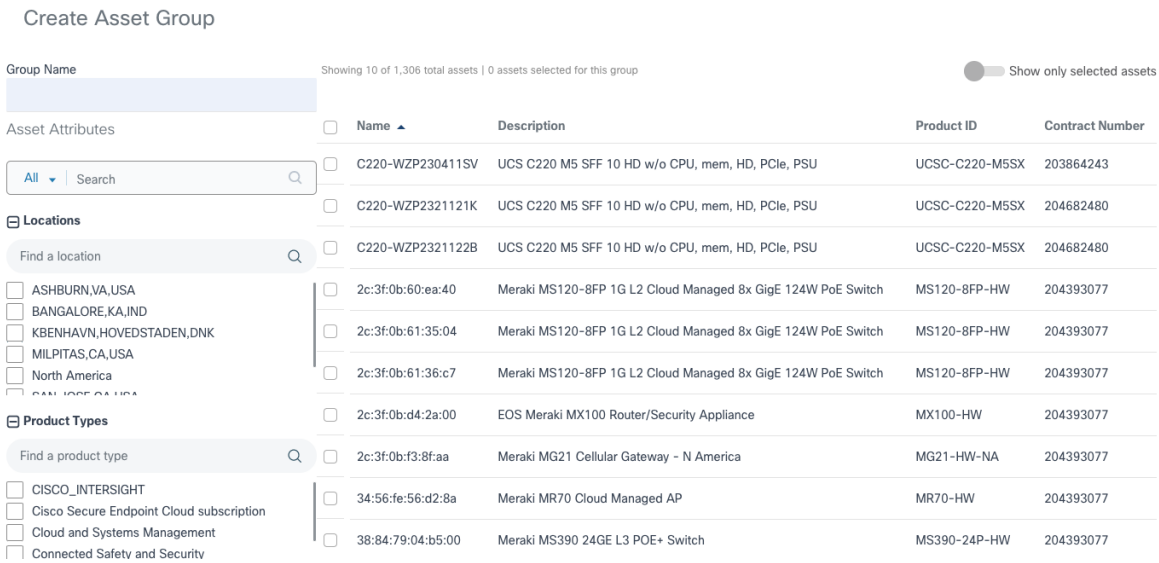


If editing...

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**



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.

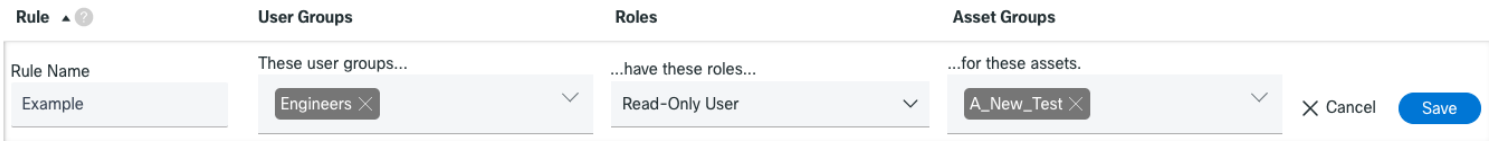
2) **Rules** – Rules specify which users can access which assets. Rules also define what permissions the users have on those assets. A rule combines a user group with an asset group. User groups must have a rule to determine which role applies to its users.

Create a Rule

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

b. Enter a **Rule Name**, **User Group, Role,** and **Asset Group**

c. Click **SAVE**

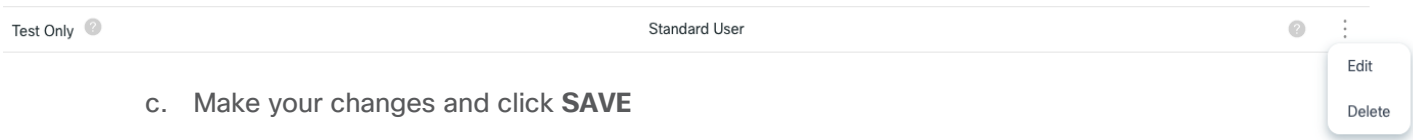


Edit or Delete a Rule

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**



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

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

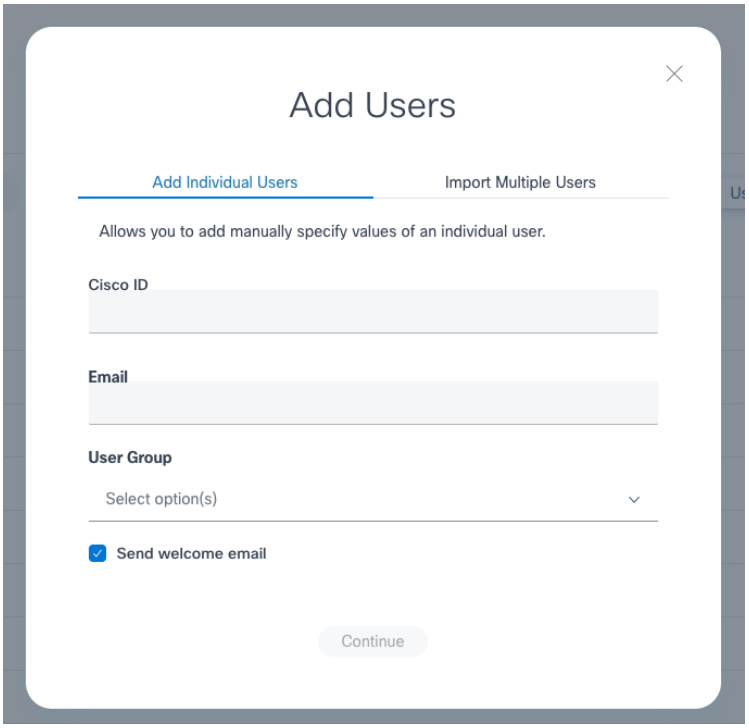
a. Select the **Users** toggle button

b. Click the **Add User** button

c. Enter the **Cisco ID**, **Email**, and **User Group**

d. Check the "Send welcome email" box so new users receive an email to log in

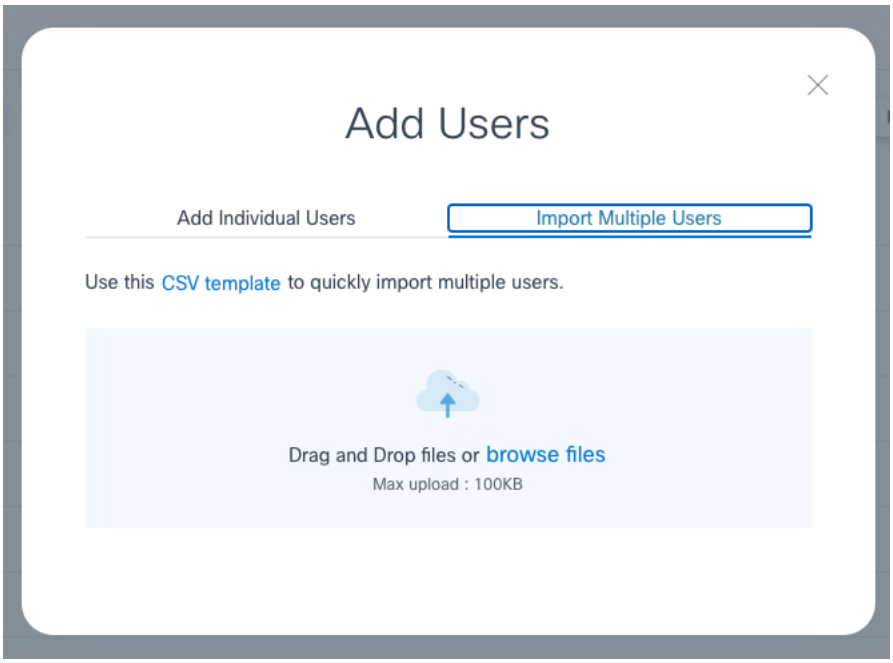
e. Click **Continue**



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

a. Select **Import Users from File**

b. 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**

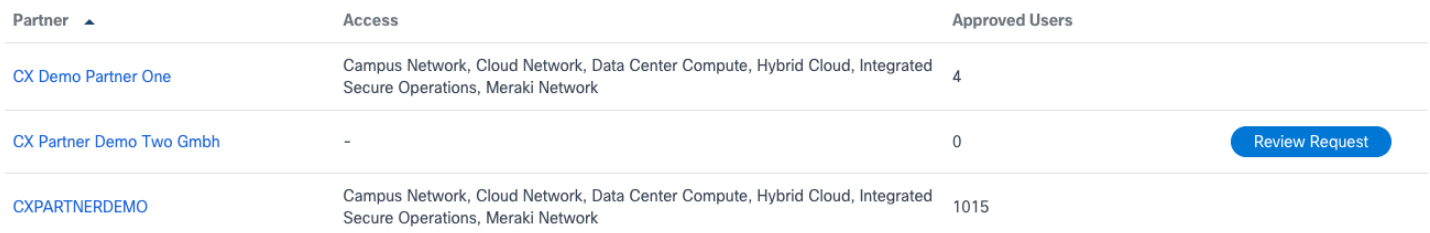
d. (Optional) – Select Users you want to add to the group

e. Click **SAVE**

Partner Access

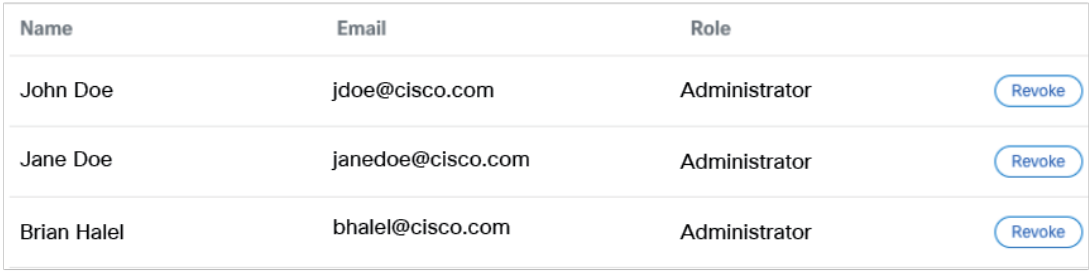
Partner Access settings allow you to approve, deny, and modify Partner access to your CX Cloud data

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



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

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



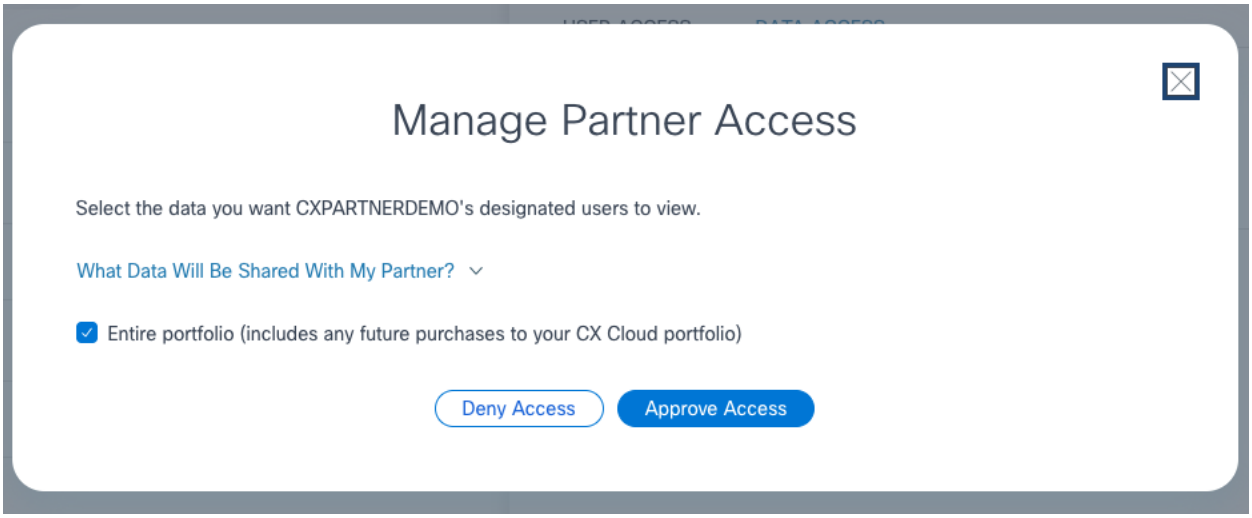
    d. Excluded Users will be shown in the **No Access** tab

3) Revoke All Partner Access

a. Click on the Partner you want to modify

b. Click **Data Access**

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



Data Collection

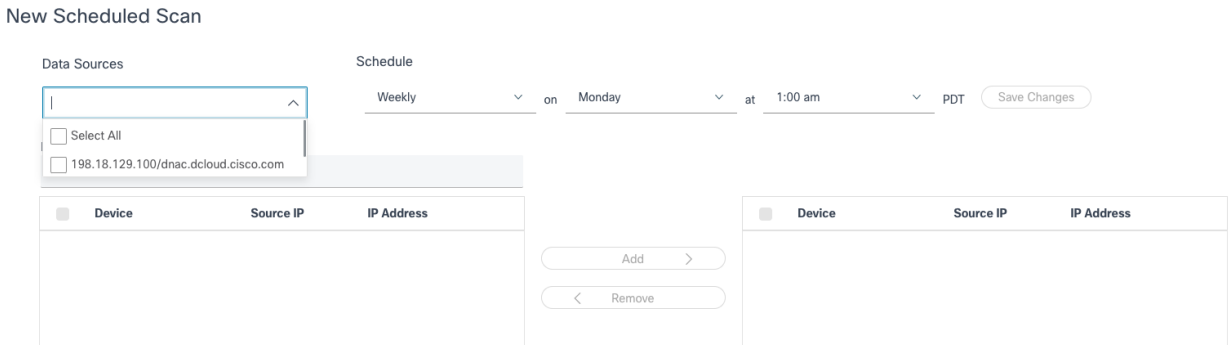
Schedule Asset inventory scans and Diagnostic Scans from DNA Center to enable Insights and Analytics. Enable Rapid Problem Resolution to automatically attach diagnostic scan output to TAC cases.

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.

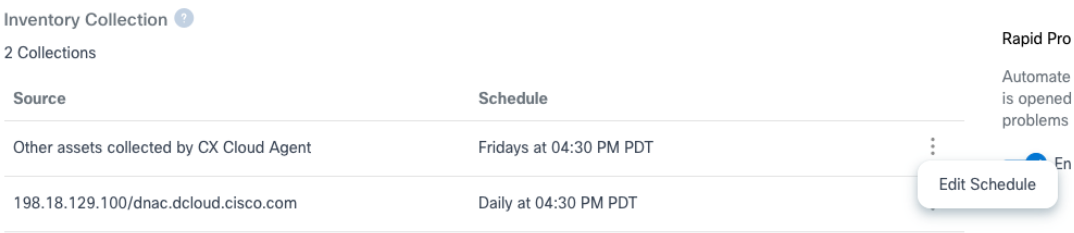
Inventory scans verify the presence of devices on your network. Regular inventory scans ensure the assets shown in CX Cloud will always be up-to-date. You can customize the inventory scan schedule to ensure that data collection doesn't disrupt your network.

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**

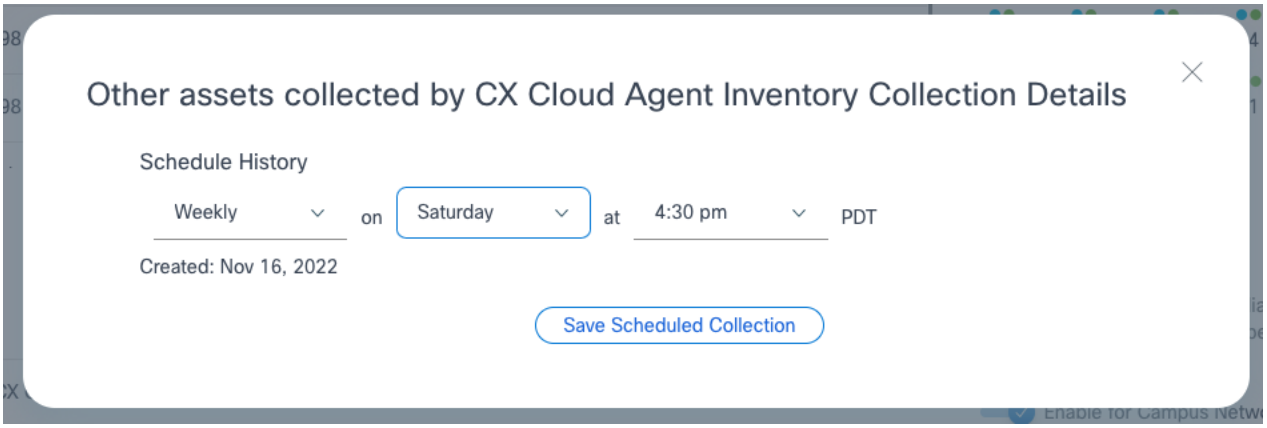


2) Schedule Inventory Scan
    a. Click on the three dots on the right side of a row in the **Inventory Collection**
    b. Select **Edit Schedule**



c. Choose a Schedule (**Daily/Weekly/Monthly, Day, Time)**

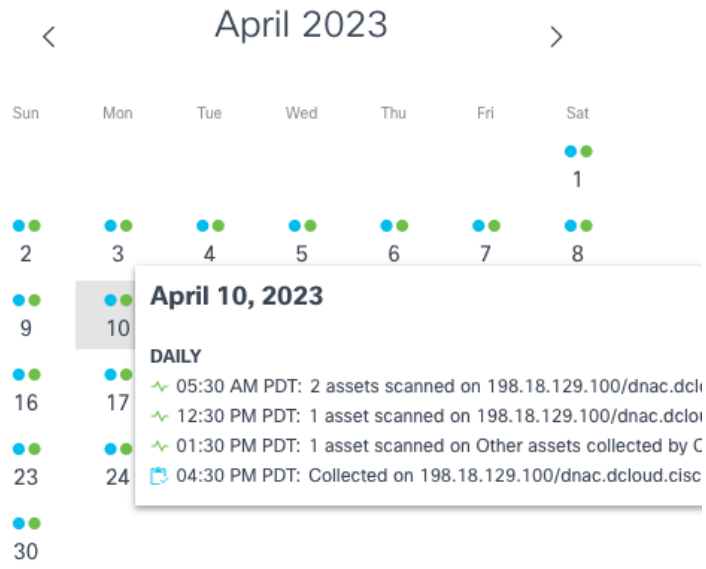
d. Click **Save Scheduled Collection**



3) View Scan Schedule

a. Click Calendar Arrows <> to view Future or Past scan schedules

b. Hover over specific dates to view the details

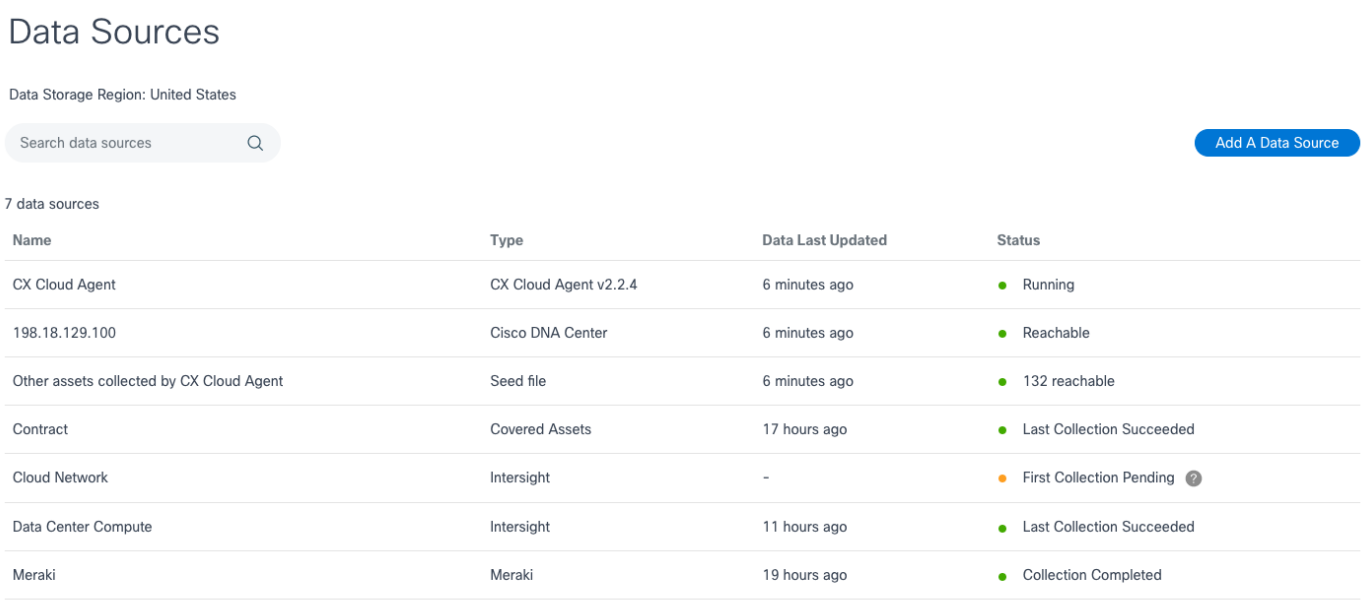


4) Enable/Disable Rapid Problem Resolution

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

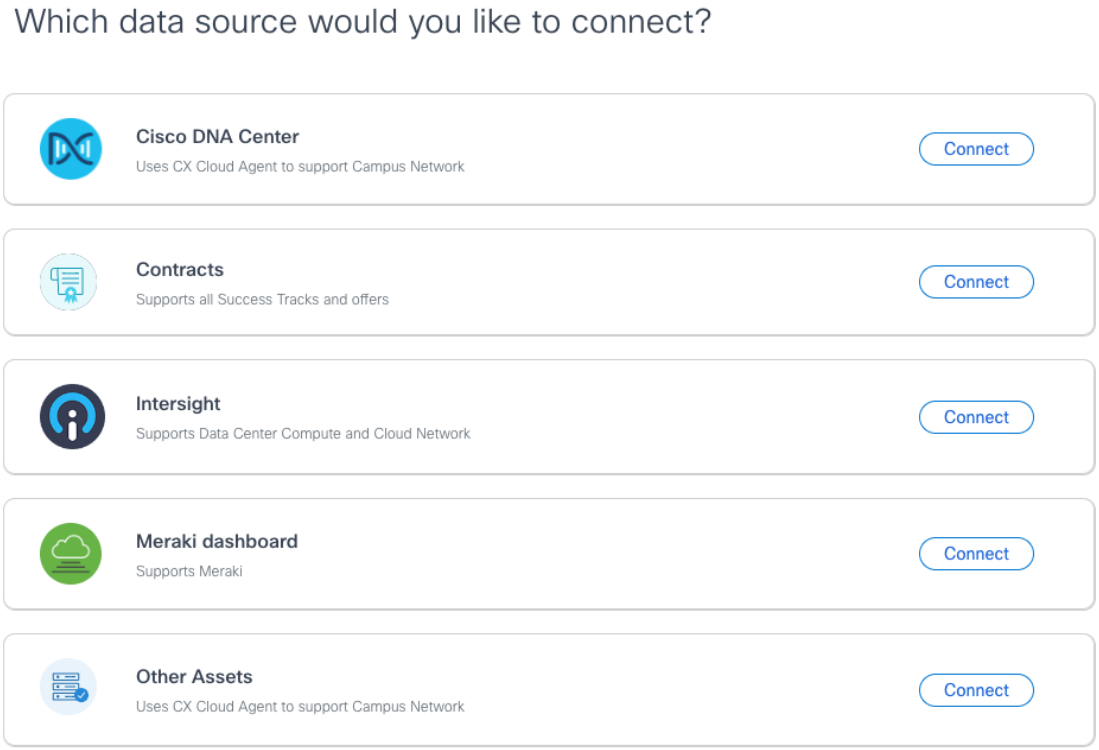
Data Sources

View current Data Sources



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

Select a Data Source to connect

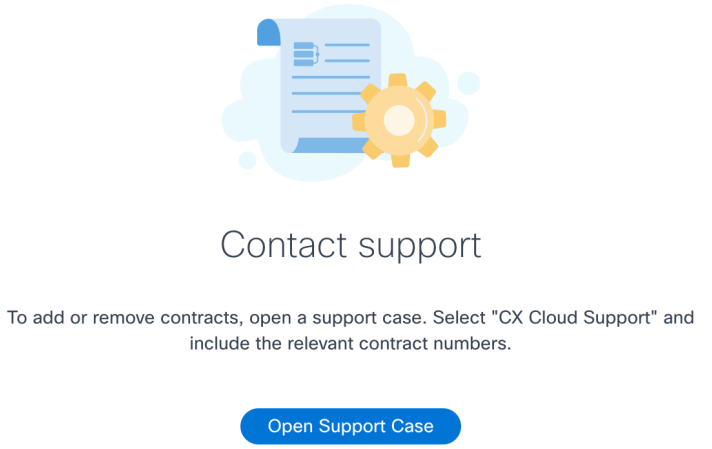


1) For the Campus Network Success Track, Install and Configure DNA Center and CX Agent
    a. Refer to installation guides: Installing CX Agent and CX Agent Overview

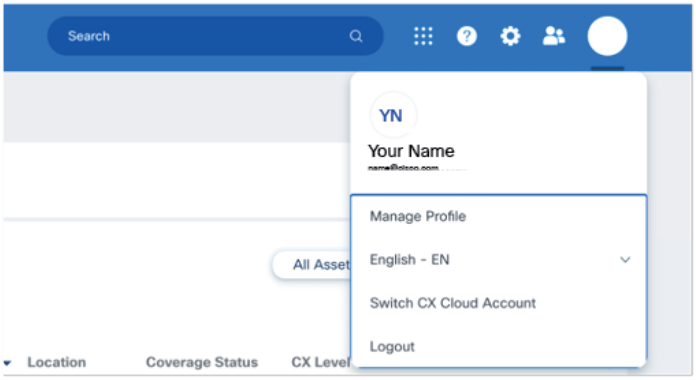
2) For Cloud Network or Data Center Compute Success Tracks, connect Intersight
    a. Refer to installation guides: Integrating Intersight with CX Cloud and Intersight Overview

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



    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**

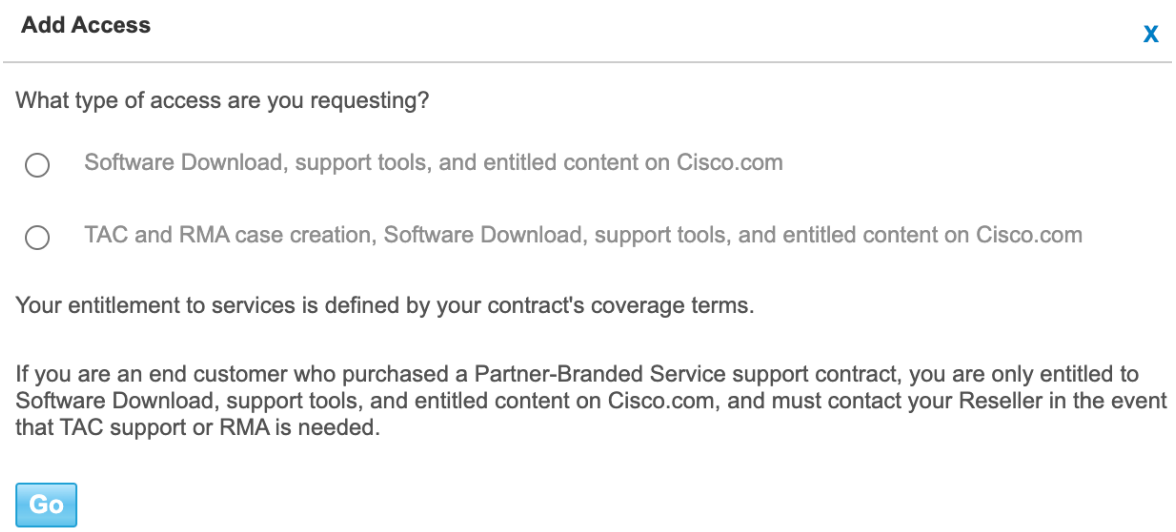


iii. Click Edit Personal Information

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**



vii. Click **Go**

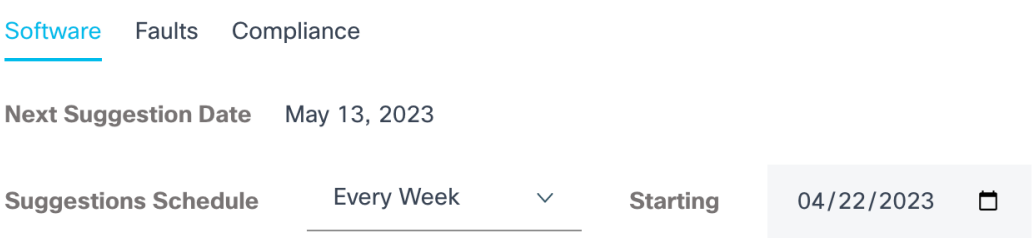
viii. Enter the contract numbers and submit

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



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

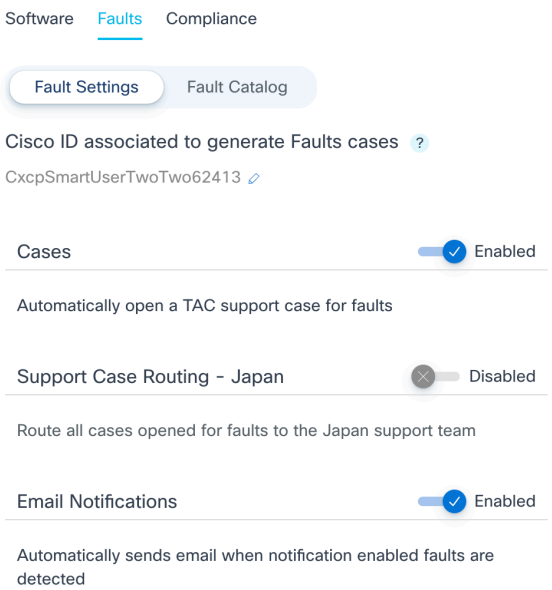
    a. Select the **Faults** Tab

    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)

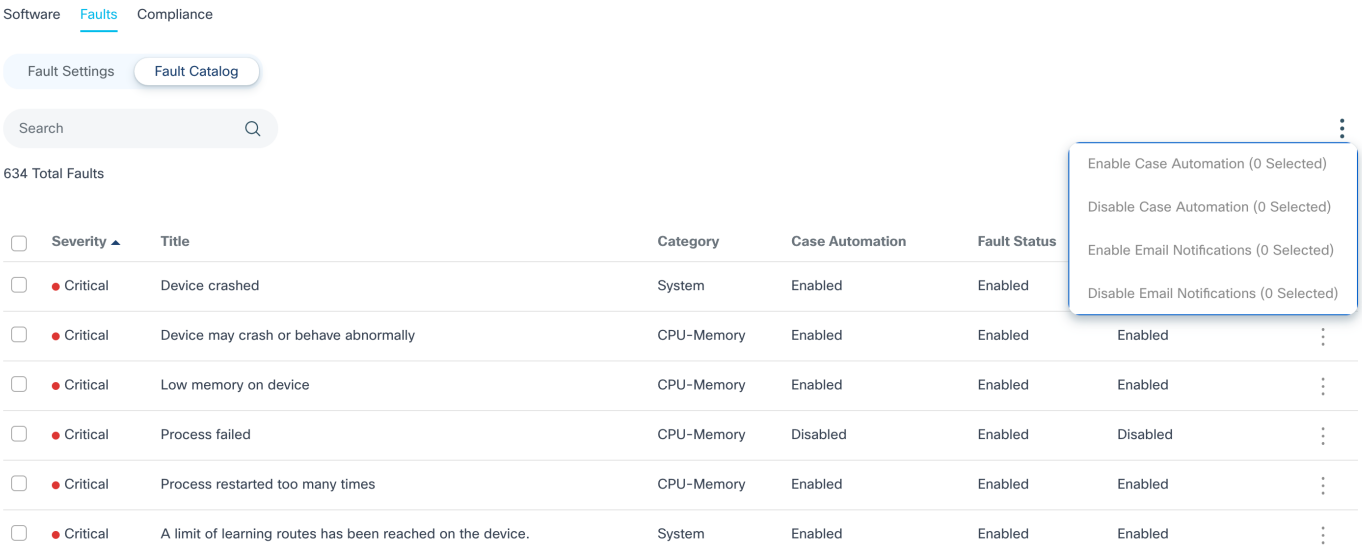
    c. Click the Toggle button to Enable/Disable Automatic **Cases** creation and **Email Notifications**

    d. Note that Support Case Routing is only for Japan support teams



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

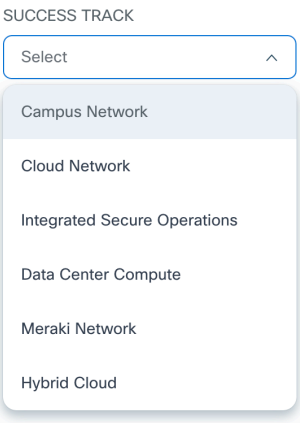
f. Enable/Disable Faults, Cases and Email Notifications by selecting a Fault or multiple Faults, then click the 3 vertical dots (kebab) menu on the right side to expand the menu



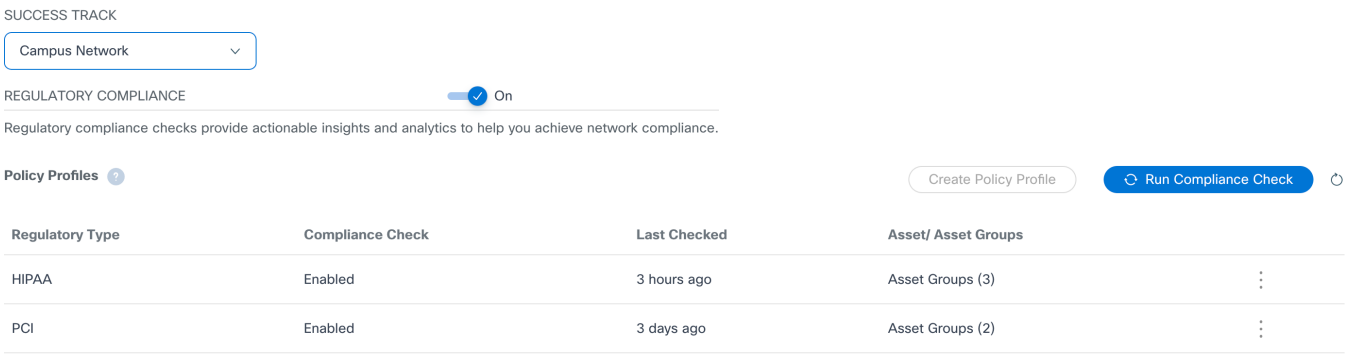
3) **Compliance** settings enable PCI and HIPAA regulatory compliance check for specific Asset Groups

a. Select the **Compliance** Tab

b. Select a Success Track



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



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**.