Cisco DNA Center Platform User Guide, Release 2.3.2

First Published: 2021-12-15

Last Modified: 2023-07-11

C O N T E N T S

New and Changed Information

New and Changed Information

This table summarizes the new and changed features for this release and tells you where they are documented.

Table 1: New and Changed Features

Feature	Description	Where Documented
New Reports GUI Features	The Cisco DNA Center platform support is extended for the following enhancements in **Event**: • **Event** is renamed as **Event Notifications**. • Cisco DNA Center **Event Notification** allows you to create notification with respective channels and trigger the notification. • The Supported Channels for now is, **REST**, **PAGERDUTY**, **SNMP**, **SYSLOG**, **WEBEX**, **EMAIL**. • One event notification supports more than one channels.	For information, see Work with Event Notifications, on page 143.
New Reports	This Cisco DNA Center platform release supports the following new reports: • Unique Client and User Summary Report • Worst Interferer Report	For more information, see **New Reports** in the Cisco DNA Center Platform Release Notes.

CHAPTER 2

About Cisco DNA Center Platform

About Cisco DNA Center Platform

Cisco DNA Center provides an extensible platform that Cisco customers and partners can use to create value added applications that can be built on top of its native capabilities. You can leverage the following Cisco DNA Center platform features to enhance the overall network experience by optimizing end-to-end IT processes, reducing the Total Cost of Ownership (TCO), and developing new value networks:

- Intent APIs: The Intent APIs are Northbound REST APIs that expose specific capabilities of Cisco DNA Center platform. The Intent APIs provide policy-based abstraction of business intent, allowing you to focus on an outcome to achieve instead of struggling with the mechanisms that implement that outcome. The APIs conform to the REST API architectural style that are simple, extensible, secure to use and support the standard REST methods which includes the GET, POST, PUT and DELETE operations through HTTPS. For additional information, see Getting Started with the Cisco DNA Center Platform Intent API.

- Integration Flows: Integration capabilities are part of Westbound Interfaces. To meet the need to scale and accelerate operations in modern data centers, IT operators require intelligent, end-to-end work flows built with open APIs. Cisco DNA Center platform provides mechanisms for integrating Assurance workflows and data with third-party IT Service Management (ITSM) solutions. For additional information, see Integration APIs.

- Events and Notifications Services: Supported services are available for Cisco DNA Assurance events and Cisco DNA Center SWIM events to be captured and forwarded to third-party applications.

Note The Cisco DNA Center platform application is accessible to a user with a SUPER-ADMIN-ROLE. You can log in and view the Cisco DNA Center platform, as well as perform actions through its GUI after logging in as a user with a SUPER-ADMIN-ROLE. Additionally, as a user with a SUPER-ADMIN-ROLE, you are able to create a custom role with read, write, or deny permissions to various platform functionality (APIs, bundles, events, and reports). Click the menu icon (☰) and choose **System** > **Users & Roles** > **Role Based Action Access Control** to access this feature.

About Intent APIs

The Intent APIs are Northbound REST APIs that expose specific capabilities of Cisco DNA Center platform. The Intent APIs provide policy-based abstraction of business intent, allowing you to focus on an outcome to achieve instead of struggling with the mechanisms that implement that outcome.

The APIs conform to the REST API architectural styles that are simple, extensible, and secure to use and support the standard REST methods which includes the GET, POST, PUT and DELETE operations though HTTPS. A REST endpoint accepts and returns HTTPS messages that contain JavaScript Object Notation (JSON) documents. You can use any programming language to generate the messages and the JSON documents that contain the API methods. These APIs are governed by the Cisco DNA Center Role Based Access Control (RBAC) rules and as a security measure require the user to authenticate successfully prior to using the API.

The Intent APIs are listed in the API catalog located in the Cisco DNA Center platform GUI, that you can view. Click the menu icon (≡) and choose **Platform** > **Developer Toolkit** > **APIs**.

Note For additional information about Intent APIs, see Intent APIs. For general information about APIs used by the Cisco DNA Center platform, see Cisco DNA Center Platform Overview.

About Events and Notifications

Cisco DNA Center platform supports the ability to send custom notifications when specific events are triggered. This is valuable for third-party systems that take business actions based upon event type. For example, when a device in the network is out of compliance, a custom application may want to receive notifications and execute a software upgrade action.

You can view a list of available events for this release. Click the menu icon (≡) and choose **Platform** > **Manage** > **Configurations**. These events can be customized for IT Service Management (ITSM) incidents.

Deploy Cisco DNA Center Platform

Overview

To deploy the Cisco DNA Center platform, perform the following steps:

1. Install Cisco DNA Center, Release 2.3.2. For information, see Install Cisco DNA Center Platform, on page 5.

2. Configure the integration settings. For information, see Configure Integration Settings, on page 6.

After deploying the Cisco DNA Center platform, perform the following tasks:

• Review the API prerequisites. For information, see API Prerequisites, on page 7.

• Proceed to **Overview** in the GUI to review the brief feature descriptions to better understand the Cisco DNA Center platform. For information, see About Platform Overview, on page 11.

• Proceed to **Bundles** in the GUI to enable, configure, and activate any of the bundles necessary for your network. For information, see Bundle Features, on page 14.

Install Cisco DNA Center Platform

For this release, when performing a fresh install of Cisco DNA Center, you also install the Cisco DNA Center platform. A separate installation procedure for the Cisco DNA Center platform is no longer required. For information about installing Cisco DNA Center, see the Cisco DNA Center Installation Guide.

After the installation, a **Platform** option appears in the **Navigation** slide-in pane in the GUI. Click **Platform** to access the Cisco DNA Center platform. The Cisco DNA Center platform is accessible to a user with a SUPER-ADMIN-ROLE. You can log in and view the Cisco DNA Center platform, as well as perform actions through its GUI after logging in as a user with a SUPER-ADMIN-ROLE. Additionally, as a user with a SUPER-ADMIN-ROLE, you are able to create a custom role with read, write, or deny permissions to various

platform functionality (APIs, bundles, events, and reports). Click the menu icon (≡) and choose **System** > **Users & Roles** > **Role Based Action Access Control** to access this feature.

The NETWORK-ADMIN-ROLE and the OBSERVER-ROLE have more limited and restricted capabilities with Cisco DNA Center platform. For example, these two roles do not permit the user to perform the following actions:

- Generate reports
- Subscribe to events
- Configure event settings
- Enable and configure bundles
- Configure users and roles

Configure Integration Settings

In cases where firewalls or other rules exist between Cisco DNA Center and any third-party apps that need to reach Cisco DNA Center platform, you will need to configure **Integration Settings**. These cases occur when the IP address of Cisco DNA Center is internally mapped to another IP address that connects to the internet or an external network.

☞

Important   After a backup and restore of Cisco DNA Center, you need to access the **Integration Settings** page and update (if necessary) the **Callback URL Host Name** or **IP Address** using this procedure.

Before you begin

You have deployed Cisco DNA Center platform as described in the previous section.

Step 1   Click the menu icon (≡) and choose **System** > **Settings** > **System Configuration** > **Integration Settings**.

Step 2   Enter the **Callback URL Host Name** or **IP Address** that the third-party app needs to connect to when communicating with Cisco DNA Center platform.

Note   The **Callback URL Host Name** or **IP Address** is the external facing hostname or IP address that is mapped internally to Cisco DNA Center. Configure the VIP address for a three-node cluster setup.

Step 3   Click the **Apply** button.

What to do next

Review the API prerequisites for Cisco DNA Center platform.

API Prerequisites

To work with the Cisco DNA Center APIs and the Cisco DNA Center platform, you must meet the following API prerequisites.

Supported Programming Language

In order to use the code previews that Cisco DNA Center platform generates, you must use a supported programming language and perform any other necessary language-specific tasks to use the generated code.

For example, to use Python scripts generated by Cisco DNA Center platform, you must install the requests library. You can use pip (Pip Installs Packages) to install using a CLI command:

```
pip install requests
```

Cisco DNA Center platform is able to generate code previews for the following languages in the GUI:

- **Shell**

- **Node - HTTP**

- **Node - Unirest**

- **Node - Request**

- **Python**

- **Ruby**

- **JavaScript**

- **JQuery**

- **PHP**

- **Go**

- **Ansible**

Authentication

The Cisco DNA Center APIs use token-based authentication and the lifetime of a token is 60 seconds. You need to log into the APIs using an authentication script (using the supported programming language of your choice). As an example, run the following Python script to log in:

```
def get_token():
    token = requests.post(
        'https://<cluster IP>/api/system/v1/auth/token',
        auth=HTTPBasicAuth(
            username=<username>,
            password=<password>
        ),
    headers={'content-type': 'application/json'},
    verify=False,
     )
     data = token.json()
     return data['Token']
```

Role-Based Access Control Support for Platform

Cisco DNA Center platform supports role-based access control (RBAC), which enables a user with SUPER-ADMIN-ROLE privileges to define custom roles that permit or restrict users access to certain platform features.

Use this procedure to define a custom role and then assign a user to that role.

Note The Cisco DNA Center platform is accessible to a user with a SUPER-ADMIN-ROLE. You can log in and view the Cisco DNA Center platform, as well as perform actions through its GUI after logging in as a user with a SUPER-ADMIN-ROLE. The NETWORK-ADMIN-ROLE and the OBSERVER-ROLE have more limited and restricted capabilities with Cisco DNA Center platform. For example, these two roles do not permit the user to perform the following actions:

- Generate reports

- Subscribe to events

- Configure event settings

- Enable and configure bundles

- Configure users and roles

For more information, see the "Manage Users" chapter in the *Cisco Digital Network Architecture Center Administrator Guide*.

Before you begin

Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure.

Step 1   Define a custom role.

a)   Click the menu icon (≡) and choose **System** > **Users and Roles** > **Role Based Access Control**.

b)   Click **Create New Role**.

The **Create a Role** window appears. If this is your first iteration of RBAC, after you have created the new role, you will be asked to assign users to the new role.

c)   Click **Let's Do it**.

If you want to skip this screen in the future, check the **Don't show this to me again** check box.

The **Create a New Role** window appears.

d)   Enter a name for the role and then click **Next**.

The **Define the Access** window appears with a list of options.

e)   Click **>** next to **Platform** to expand it.

The following options listed below appear, which allow you to set **Deny** (the default), **Read**, or **Write** permissions for the new role.

- **APIs**: Allows you to view and try out the APIs.

- **Bundles**: Allows you to configure and activate the bundles and ITSM integration settings.

- **Events**: Allows you to configure event settings for email, REST API endpoints, and SNMP traps.

- **Reports**: Allows you to schedule, view, and download reports.

    f) Click **Next**.
The **Summary** window appears.

    g) Review the summary. If the summary information is correct, click **Create Role**. Otherwise, click **Edit** and make the appropriate changes.
The **Done,** *Role-Name* window appears.

Step 2   To assign a user to the custom role you just created, click **Add Users**.

The **User Management** > **Internal Users** window appears, which allows you to either assign the custom role to an existing user or to a new user.

- To assign the custom role to an existing user, do the following:

    a. In the **Internal Users** window, click the radio button next to the user to whom you want to assign the custom role, and then click **Edit**.

    The **Update Internal User** slide-in pane appears.

    b. From the **Role List** drop-down list, choose the custom role, and then click **Save**.

- To assign the custom role to a new user, do the following:

    a. Click .

    The **Create Internal User** slide-in pane appears.

    b. Enter the first name, last name, and username in the fields provided.

    c. From the **Role List** drop-down list, choose the custom role to assign to the new user.

    d. Enter the password and then confirm it.

    e. Click **Save**.

Step 3   If you are an existing user who was logged in when the administrator was making changes to your access permissions, you must log out of Cisco DNA Center and then log back in for the new permission settings to take effect.

CHAPTER 4

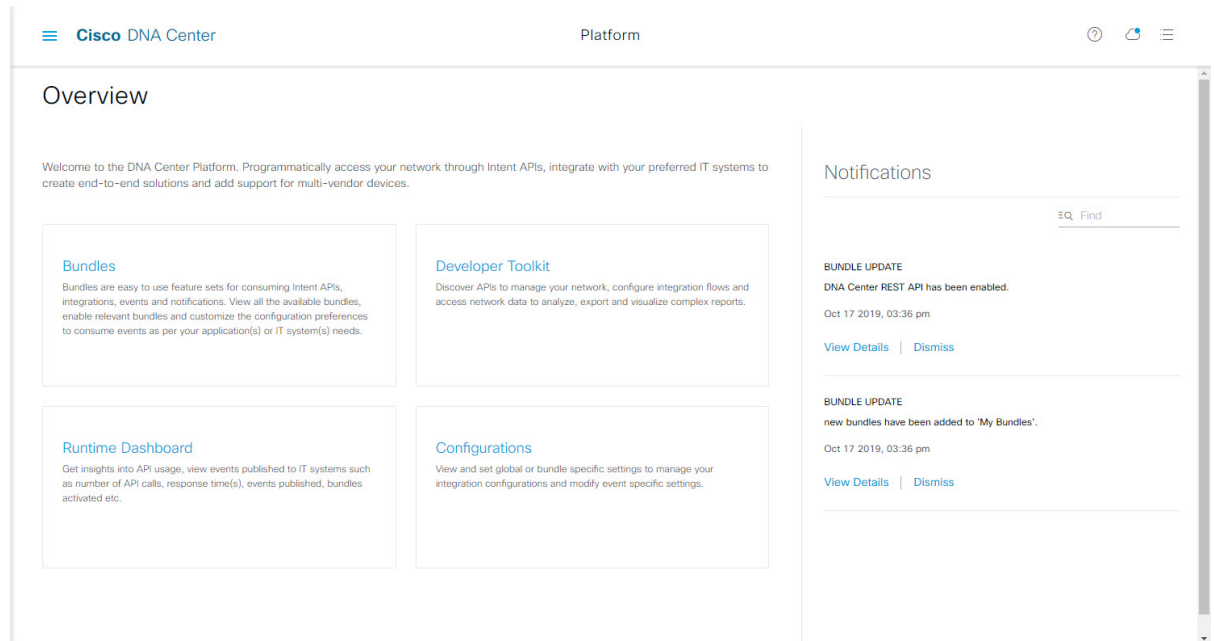# Platform Overview GUI

About Platform Overview

The **Overview** window is accessible by clicking the menu icon (≡) and choosing **Platform** > **Overview**. The **Overview** window supports the following features:

• Displays brief summaries and direct links to the Cisco DNA Center platform GUI features, including:

  • **Bundles**: Provides access to bundles that you can use to integrate your own applications to Cisco DNA Center with or to enhance the performance of Cisco DNA Center itself. Bundles are defined as groupings of APIs, DNA-Events, integration flows, data services, or applications. Additionally, provides access to a GUI (**Configurations**) where you can configure general or event global settings or settings for multiple bundles.

  • **Developer Toolkit**: Provides tools (APIs and integration flows) to access Cisco DNA Center, as well as integrate Cisco DNA Center with other applications.

  • **Runtime Dashboard**: Provides a dashboard where metrics are collected and you can view API, integration flow, and event summaries.

  • **Configurations**: Provides dashboards where you can configure the category, severity, and type of events for your network, as well as add/edit instances to bundles.

• Accesses the **Notifications** slide-in pane that presents any current Cisco DNA Center platform notifications, including bundle updates. Click **View Details** to view detailed data about the bundle under the **Bundles** tab. Click **Dismiss** to dismiss the bundle notification.

Review the Platform GUI

Perform this procedure to review the Cisco DNA Center platform features and functions that are available to you. You can review these features and functions using the **Overview** window in the Cisco DNA Center GUI.

Figure 1: Cisco DNA Center Platform Overview Window

Step 1   Click the menu icon (≡) and choose **Platform** > **Overview**.

Step 2   Review the options available to you in this window.

Step 3   Click the links to directly access the individual Cisco DNA Center platform feature.

Step 4   Review bundle update information using the **Notifications** slide-in pane.

| Note | The bundle update information concerns the bundle status (enabled, disabled, successfully configured, or ready to be configured). |

Platform Manage GUI

About Manage

The Cisco DNA Center platform GUI provides a **Manage** drop-down menu option that provides access to the following features:

- **Bundles**: Access to bundles that you can use to integrate Cisco DNA Center with your own applications or to enhance the performance of Cisco DNA Center itself. Bundles are comprised of groupings of APIs, DNA Events, integration flows, data services, or applications.

Note You can use the Cisco DNA Center platform GUI to view the bundle components (APIs and integration flows) by clicking the **Menu** icon (☰) > **Platform** > **Developer Toolkit** > **APIs** or **Platform** > **Developer Toolkit** > **Integration Flows**.

- **Configurations**: Access to a window to configure global settings for a single bundle or across multiple bundles for a custom platform experience.

About Bundles

Cisco DNA Center platform provides access to bundles that you can use to integrate Cisco DNA Center with your own applications or to enhance the performance of Cisco DNA Center itself.

The following Cisco DNA Center platform information is accessible using the GUI:

- Bundle name, vendor, version, version release date, and tags
- Status of the bundle:

- **NEW**: Bundle that is available through Cisco DNA Center platform, but has not yet been enabled. Click the **Enable** button to enable the bundle for configuration and subsequent activation.

- **ENABLED**: Bundle that has been enabled, but not yet configured. Once enabled, the bundle's integration flows and API code can be viewed under the **Contents** tab. Click the **Configure** button to configure at the bundle level.

  The enablement and configuration of bundles are two separate steps, since a business manager will usually enable a particular bundle as a business decision. The follow-up configuration of the bundle will usually be performed by an IT or network administrator.

- **DISABLED**: The bundle has been stopped from executing any further.

- **ACTIVE**: After either reviewing and/or configuring the bundle (configuring bundle-specific values), you can activate the bundle in your network by clicking the **Activate** button.

- **UPDATE**: When you upgrade from one version of Cisco DNA Center platform to a higher version of Cisco DNA Center platform.

- **ERROR**: There is an issue with the bundle and it cannot be activated within your network.
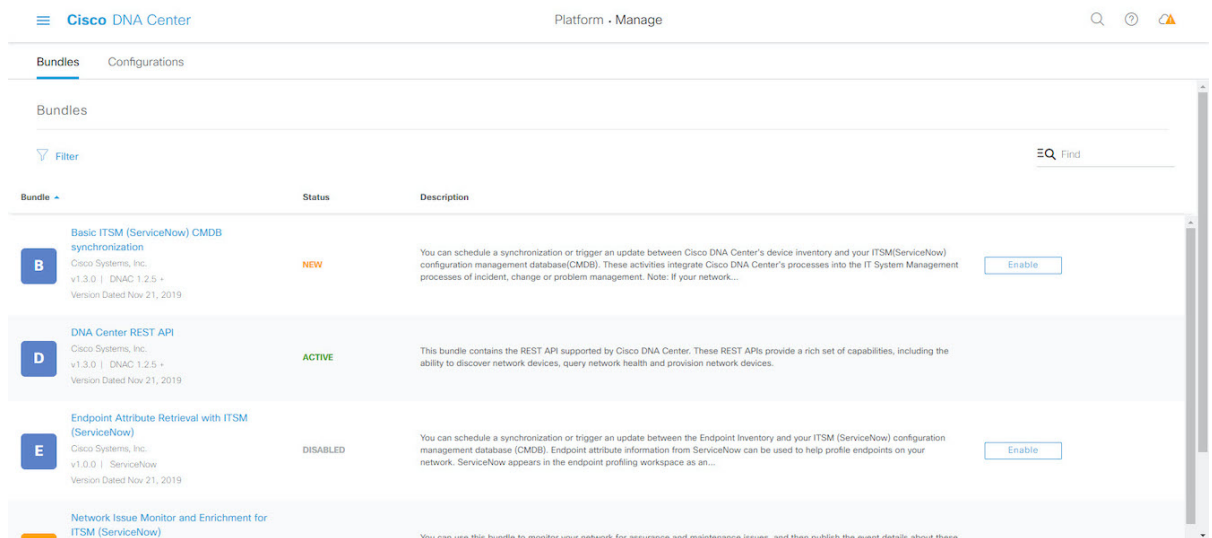
- Description of the bundle.

- Buttons to **Enable**, **Disable**, or **Configure** the bundle.

Bundle Features

You can review, enable, and configure bundles using the **Bundles** window in the Cisco DNA Center GUI.

Figure 2: Cisco DNA Center Platform Bundles Window

Access the bundles in the GUI to accomplish one or more of the following tasks:

- Review and try out supported Cisco DNA Center APIs. See for additional information.

• Enable Rogue Management and the Cisco Advanced Wireless Intrusion Prevention System (aWIPS) to detect wired and wireless threats, including rogue access points. See Work with APIs, on page 137 for additional information.

• Configure a destination (Event Management or REST API Endpoint) to receive events for ServiceNow. See Configure Bundles: Destination to Receive Events, on page 15 for information on using the GUI to configure a destination.

• Configure access settings for Cisco DNA Center to ServiceNow (hostname, username, password, and so on). See Configure Bundles: ServiceNow Access Settings, on page 18 for information on using the GUI to configure access settings to ServiceNow.

• Configure data synchronization between Cisco DNA Center and ServiceNow (including the option to configure operational and source identifiers). See Configure Bundles: CMDB Data Synchronization for ServiceNow, on page 22 for information on using the GUI to configure data synchronization.

Configure Bundles: Destination to Receive Events

Perform this procedure to configure a destination to receive events (network and SWIM) for ServiceNow within a bundle. You can review, enable, and configure bundles using the **Bundles** window in the Cisco DNA Center GUI.

Figure 3: Cisco DNA Center Platform Bundles Window
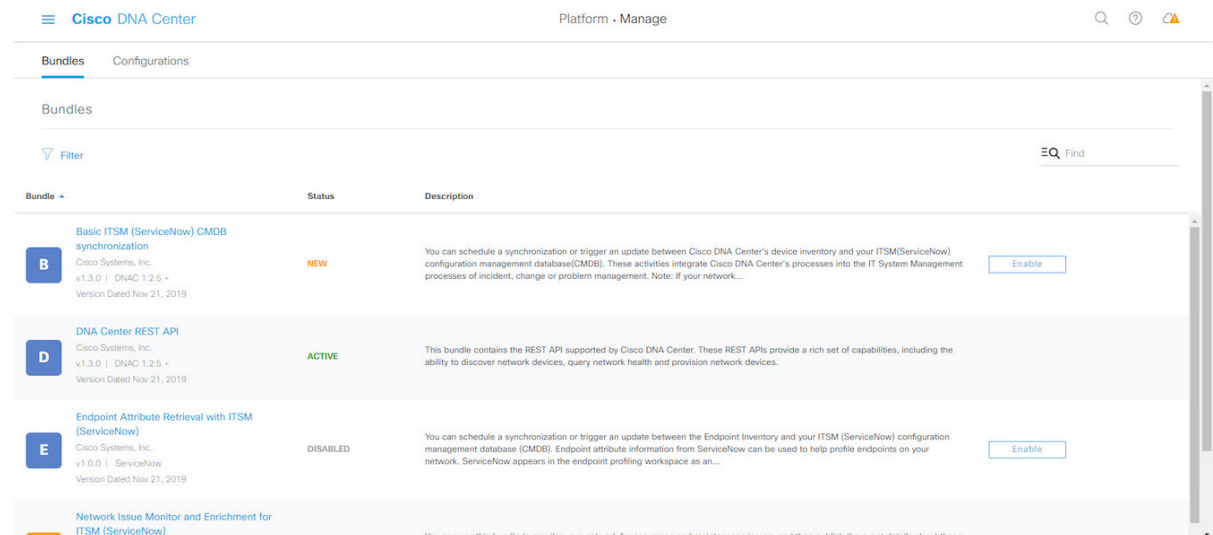
For this release, you configure a destination to receive events for ServiceNow within the following bundles:

• **Network Issue Monitor and Enrichment for ITSM (ServiceNow)**

• **Cisco DNA Center Automation events for ITSM (ServiceNow)**

Before you begin

See the latest Cisco DNA Center ITSM Integration Guide to understand how this procedure fits within a larger workflow when configuring a Cisco DNA Center-to-ServiceNow integration.

Step 1   Click the menu icon (☰) and choose **Platform** > **Manage** > **Bundles**.

Step 2   Review the displayed bundles and their status.

The following bundles are available with this release:

- **Basic ITSM (ServiceNow) CMDB synchronization**: Triggers or schedules a synchronization between Cisco DNA Center devices and your ServiceNow® CMDB system. The ServiceNow CMDB provides a single system of record for IT.

   Note   For an example of an integration flow and ServiceNow, see ServiceNow Integration.

- **Cisco DNA Center REST API**: Contains the REST API supported by Cisco DNA Center. This API provides a rich set of capabilities to query network knowledge, as well as to initiate network programming.

- **Endpoint Attribute Retrieval with ITSM (ServiceNow)**: This bundle retrieves detailed endpoint information and publishes it once or on a recurring schedule to Cisco DNA Center. This activity does not modify or delete any CIs on the existing ITSM (ServiceNow) tool.

- **Network Issue Monitor and Enrichment for ITSM (ServiceNow)**: Contains Cisco DNA Center components that monitor the network for assurance and maintenance issues, and publishes the event details to a ServiceNow system. It also contains APIs to access rich network context data.

- **Rogue and aWIPS**: Contains the REST API supported by Cisco DNA Center for Rogue Management and the Cisco Advanced Wireless Intrusion Prevention System (aWIPS). This API is used to detect wired and wireless threats, including rogue access points.

- **Cisco DNA Center Automation events for ITSM (ServiceNow)**: Monitor and publish events requiring software image updates (for compliance, security, or other operational triggers) to a ServiceNow system.

- **Disaster Recovery API**: This bundle contains the REST APIs supported by disaster recovery and provide support to monitor the disaster recovery system.

- **AI Endpoint Analytics**: This bundle allows you to access various services provided by AI endpoint analytics application. You must install **AI Endpoint Analytics** package in Cisco DNA Center to use this bundle.

You can adjust the bundles that are displayed in the GUI by clicking the **Filter** icon and using the filter, or by entering a keyword in the **Find** field.

Step 3   Click either the **Network Issue Monitor and Enrichment for ITSM (ServiceNow)** or the **Cisco DNA Center Automation events for ITSM (ServiceNow)** bundle link or icon.

The following information is provided:

- **General information**: Vendor, version, platform, tags displayed under the square icon.

   Note   Tags indicate what the Cisco DNA Center component is used for or is affected by the bundle.

- **Information**: Tab that displays general information (purpose of bundle and how bundle works in the network), sample schemas, mapping notes, configuration notes, and other data about the bundle.

- **Contents**: Tab that accesses information about the integration flows within the bundle.

- **Release Notes**: Tab that displays latest release information about the bundle, including its version.

Step 4   Click each of the above tabs and review the information about the bundle.

Step 5   Click the **Enable** button to enable the bundle.

An **Information** field appears in the window.

Step 6   In the **Information** field, click the **Enable** button to confirm enabling the bundle.

After clicking the **Enable** button to confirm, a Success message appears.

Step 7   Click **Okay** in the Success message.

Step 8   Click the **Configure** button to configure at the bundle level.

Step 9   In the configuration slide-in pane, click **Destination to receive events** to configure a Destination instance.

Figure 4: Example of Destination to Receive Events Configuration Fields
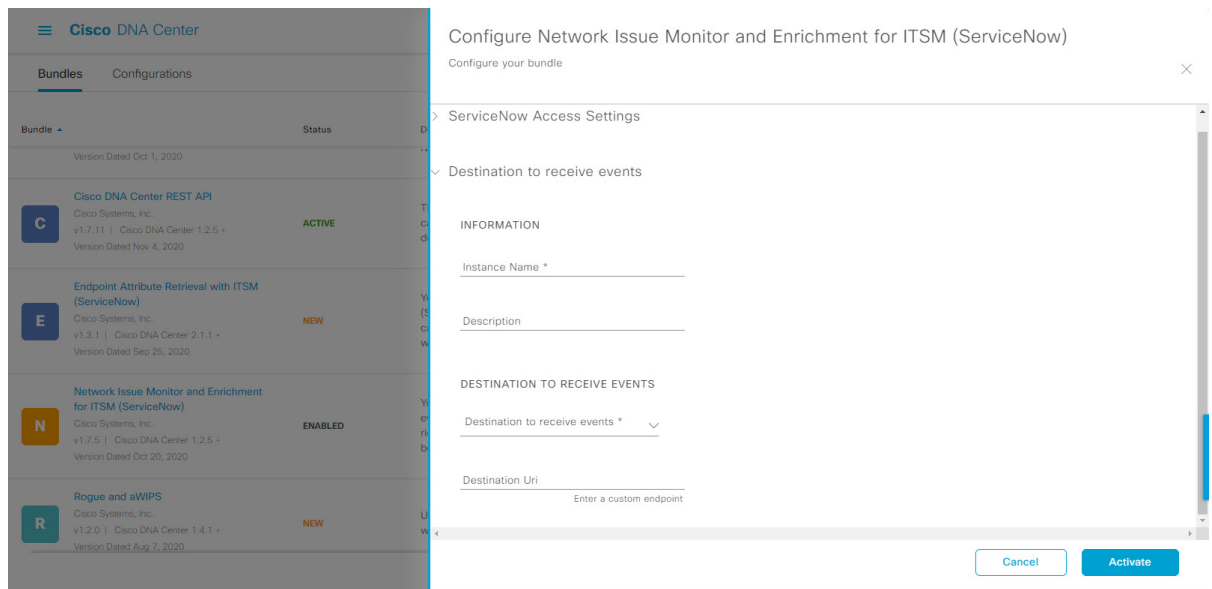
> **Note**   Use the **Destination to receive events** configuration options for ServiceNow to receive network event and Cisco DNA Center automation event details in a REST API endpoint and create an incident, problem, or change ticket, based on the configuration chosen by the user in Cisco DNA Center. For additional information about setting this up with ServiceNow, see the Cisco DNA Center ITSM Integration Guide.

Step 10   Click the radio button to configure either an existing Destination instance or configure a new instance.

For configuring an existing Destination instance, choose it from the drop-down list in the window and click **Activate**

Step 11   For configuring a new Destination instance, the following additional information must be entered.

- **Instance Name**: Name of the instance.

- **Description**: Descriptive text of the instance.

- **Destination to receive events**: Choose one of the following:

  - **Event Management**: When setting up Cisco DNA Center integration with ServiceNow without using the Cisco DNA App, choose the **Event Management** option. The **Event Management** option also requires that you have the Event Management plugin configured within the ServiceNow instance.

  - **REST API Endpoint**: The **REST API Endpoint** option can be used with the Cisco DNA App. Data is sent to a REST API endpoint within the Cisco DNA App with the **REST API Endpoint** option.

- **Generic REST Endpoint in ServiceNow**: For the **Generic REST Endpoint in ServiceNow** option, you can send the data to a different staging table in ServiceNow.

  For detailed information about integrating Cisco DNA Center with ServiceNow, see the *Cisco DNA Center ITSM Integration Guide* for this release.

- **Destination URI**: Enter a destination URI (Uniform Resource Identifier) for the **Generic REST Endpoint in ServiceNow** option. This field is mandatory for this option.

After entering this information, proceed to the next step.

Step 12 Click **Activate** to save your changes and activate the bundle or click **Cancel** to cancel the configuration and close the slide-in pane.

Note By clicking **Activate**, you enable the changes that are made to the bundle and the changes take effect immediately. Additionally, the bundle's status changes from **ENABLED** to **ACTIVE**.

What to do next

To review your configuration, click the menu icon (☰) > **Manage** > **Configurations** > **General Settings** and use the **Filter** or **Find** tools to locate the specific destination instance configured in this procedure.

If necessary, later on you can edit, update, or delete the instance in the **General Settings** window. For additional information, see Configure General Settings: Edit an Instance, on page 35.

Configure Bundles: ServiceNow Access Settings

Perform this procedure to configure access settings for ServiceNow within a bundle. You can review, enable, and configure bundles using the **Bundles** window in the Cisco DNA Center GUI.

Figure 5: Cisco DNA Center Platform Bundles Window
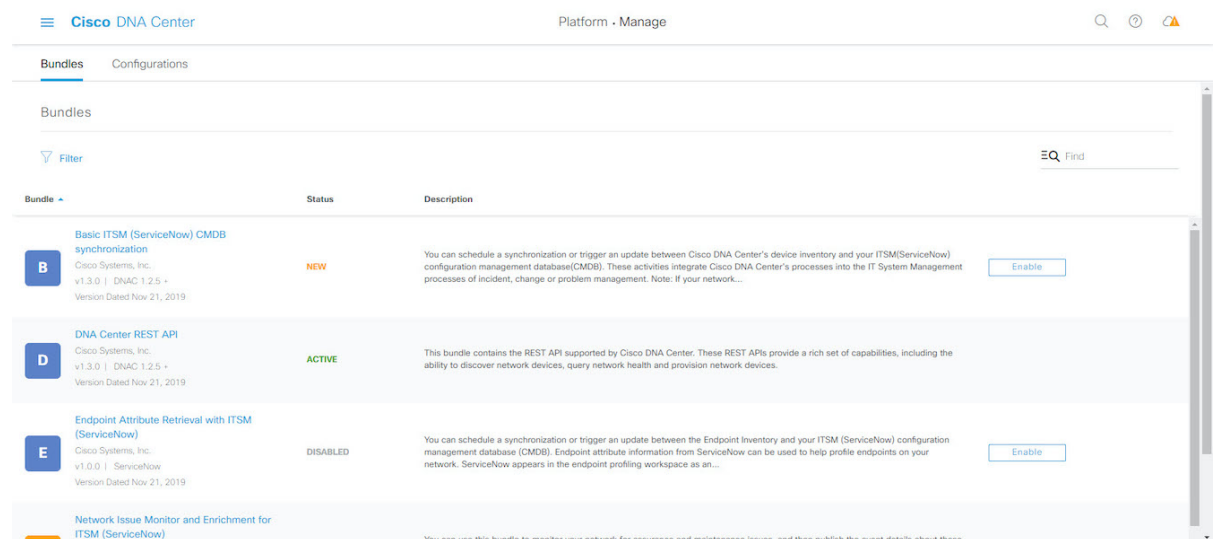
For this release, you configure ServiceNow access settings within the following bundles:

- **Endpoint Attribute Retrieval with ITSM (ServiceNow)**

- **Network Issue Monitor and Enrichment for ITSM (ServiceNow)**

- **Cisco DNA Center Automation events for ITSM (ServiceNow)**

Before you begin

See the latest Cisco DNA Center ITSM Integration Guide to understand how this procedure fits within a larger workflow when configuring a Cisco DNA Center to ServiceNow integration.

Step 1   Click the menu icon (≡) and choose **Platform** > **Manage** > **Bundles**.

Step 2   Review the displayed bundles and their current status.

The following bundles are available with this release:

- **Basic ITSM (ServiceNow) CMDB synchronization**: Triggers or schedules a synchronization between Cisco DNA Center devices and your ServiceNow® CMDB system. The ServiceNow CMDB provides a single system of record for IT.

Note	For an example of an integration flow and ServiceNow, see ServiceNow Integration.

- **Cisco DNA Center REST API**: Contains the REST API supported by Cisco DNA Center. This API provides a rich set of capabilities to query network knowledge, as well as to initiate network programming.

- **Endpoint Attribute Retrieval with ITSM (ServiceNow)**: This bundle retrieves detailed endpoint information and publishes it once or on a recurring schedule to Cisco DNA Center. This activity does not modify or delete any CIs on the existing ITSM (ServiceNow) tool.

- **Network Issue Monitor and Enrichment for ITSM (ServiceNow)**: Contains Cisco DNA Center components that monitor the network for assurance and maintenance issues, and publishes the event details to a ServiceNow system. It also contains APIs to access rich network context data.

- **Rogue and aWIPS**: Contains the REST API supported by Cisco DNA Center for Rogue Management and the Cisco Advanced Wireless Intrusion Prevention System (aWIPS). This API is used to detect wired and wireless threats, including rogue access points.

- **Cisco DNA Center Automation events for ITSM (ServiceNow)**: Monitor and publish events requiring software image updates (for compliance, security, or other operational triggers) to a ServiceNow system.

- **Disaster Recovery API**: This bundle contains the REST APIs supported by disaster recovery and provide support to monitor the disaster recovery system.

- **AI Endpoint Analytics**: This bundle allows you to access various services provided by AI endpoint analytics application. You must install **AI Endpoint Analytics** package in Cisco DNA Center to use this bundle.

You can adjust the bundles that are displayed in the GUI by clicking the **Filter** icon and using the filter, or by entering a keyword in the **Find** field.

Step 3   Click the **Network Issue Monitor and Enrichment for ITSM (ServiceNow)**, **Cisco DNA Center Automation events for ITSM (ServiceNow)**, or **Endpoint Attribute Retrieval with ITSM (ServiceNow)** bundle link or icon.

| Note | For this procedure and as an example, the **Endpoint Attribute Retrieval with ITSM (ServiceNow)** is selected. |

The following information is provided:

- **General information**: Vendor, version, platform, tags displayed under the square icon.

  | Note | Tags indicate what the Cisco DNA Center component is used for or is affected by the bundle. |

- **Information**: Tab that displays general information (purpose of bundle and how bundle works in the network), sample schemas, mapping notes, configuration notes, and other data about the bundle.

- **Contents**: Tab that provides access to information about the integration flows within the bundle.

  | Note | For the **Endpoint Attribute Retrieval with ITSM (ServiceNow)** bundle, access is provided to the **Scheduler for ServiceNow Asset Sync** integration flow. |

- **Release Notes**: Tab that displays latest release information about the bundle, including its version.

Step 4   Click each of the above tabs and review the information about the bundle.

Step 5   Click the **Enable** button to activate the link.

An **Information** field appears in the window.

Step 6   In the **Information** field, click the **Enable** button to confirm enabling the bundle.

After clicking the **Enable** button to confirm, a success message appears.

Step 7   Click **Okay** in the success message.

Step 8   Click the **Contents** tab.

For the **Endpoint Attribute Retrieval with ITSM (ServiceNow)** bundle, a link to the **Scheduler for ServiceNow Asset Sync** integration flow appears. Click the link to perform the following tasks:

- Review the **Description**, **Tags**, **How to Use this Flow**, and scheduler.

- Click **Run Now** (to run the scheduler now), **Run Later** (to schedule for a later time), or **Recurring** (to set up a recurring schedule).

  For **Run Later**, you must select a date, time, and time zone. For **Recurring**, you must set a repeating interval (daily or weekly), an interval duration (minutes or hours), and a start and end date.

- Click **Schedule** to enable the scheduler.

  | Important | Only configure and enable an integration flow schedule, after you have finished configuring the bundle itself as described in the following steps. You can configure and enable an integration flow schedule by returning to this view and clicking **Schedule** or by accessing the view by clicking the ,menu icon (≡) > **Platform** > **Developer Toolkit** > **Integration Flows** > **Scheduler for ServiceNow Asset Sync**. |

For the other two bundles, **Network Issue Monitor and Enrichment for ITSM (ServiceNow)** and **Cisco DNA Center Automation events for ITSM (ServiceNow)**, there is no link to an integration flow. Only information about integration flows is displayed.

Step 9   Click the **X** icon at the upper right of the window to close it and return to the previous bundle window.

Step 10   Click the **Configure** button to configure at the bundle level.

Step 11   In the configuration slide-in pane, click **ServiceNow Access Settings** to configure a ServiceNow instance.

Step 12 Click the radio button to configure either an existing ServiceNow instance or configure a new instance.

Figure 6: Example of ServiceNow Instance Configuration Fields
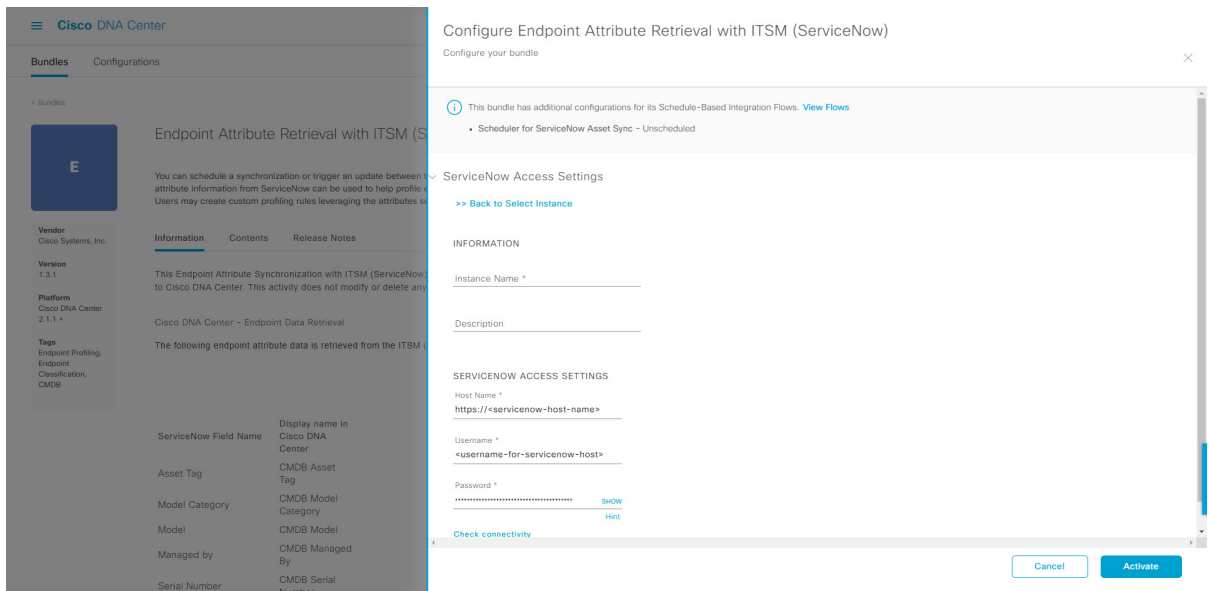
For configuring an existing ServiceNow instance, choose it from the drop-down list in the window and click **Activate**.

Step 13 For configuring a new ServiceNow instance, the following additional information must be entered.

- **Instance Name**: Name of the instance.

- **Description**: Descriptive text of the instance.

- **Host name**: Hostname for the ServiceNow system.

- **Username**: Username required to access the ServiceNow system.

- **Password**: Password required to access the ServiceNow system.

Step 14 Click **Check Connectivity** to test whether you can connect to the server where the endpoint is located.

After a successful test of connectivity to the server, proceed to the next step.

Step 15 Click **Activate** to save your changes and activate the bundle or click **Cancel** to cancel the configuration and close the slide-in pane.

Note By clicking **Activate**, you enable the changes that are made to the bundle and the changes take effect immediately. Additionally, the bundle's status changes from **ENABLED** to **ACTIVE**.

What to do next

To review your configuration, click the menu icon (☰) > **Manage** > **Configurations** > **General Settings** and use the **Filter** or **Find** tools to locate the ServiceNow instance configured in this procedure.

If necessary, later on you can edit, update, or delete the instance in the **General Settings** window. For additional information, see Configure General Settings: Edit an Instance, on page 35.

Configure Bundles: CMDB Data Synchronization for ServiceNow

Perform this procedure to configure data synchronization between Cisco DNA Center and ServiceNow (including the option to configure operational and source identifiers) within a bundle. You can review, enable, and configure bundles using the **Bundles** window in the Cisco DNA Center GUI.

Figure 7: Cisco DNA Center Platform Bundles Window
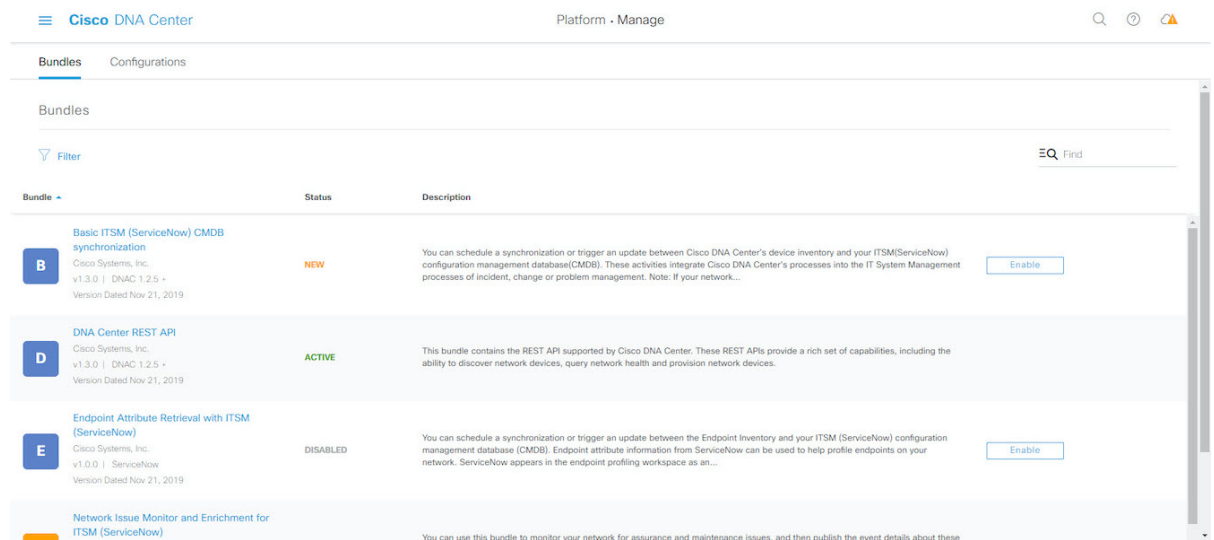
For this release, you configure data synchronization and set the operational limit and identifier for ServiceNow within the following bundle:

- **Basic ITSM (ServiceNow) CMDB synchronization**

Before you begin

See the latest Cisco DNA Center ITSM Integration Guide to understand how this procedure fits within a larger workflow when configuring a Cisco DNA Center-to-ServiceNow integration.

Step 1   Click the menu icon (☰) and choose **Platform** > **Manage** > **Bundles**.

Step 2   Review the displayed bundles and their current status.

The following bundles are available with this release:

- **Basic ITSM (ServiceNow) CMDB synchronization**: Triggers or schedules a synchronization between Cisco DNA Center devices and your ServiceNow® CMDB system. The ServiceNow CMDB provides a single system of record for IT.

  Note   For an example of an integration flow and ServiceNow, see ServiceNow Integration.

- **Cisco DNA Center REST API**: Contains the REST API supported by Cisco DNA Center. This API provides a rich set of capabilities to query network knowledge, as well as to initiate network programming.

- **Endpoint Attribute Retrieval with ITSM (ServiceNow)**: This bundle retrieves detailed endpoint information and publishes it once or on a recurring schedule to Cisco DNA Center. This activity does not modify or delete any CIs on the existing ITSM (ServiceNow) tool.

- **Network Issue Monitor and Enrichment for ITSM (ServiceNow)**: Contains Cisco DNA Center components that monitor the network for assurance and maintenance issues, and publishes the event details to a ServiceNow system. It also contains APIs to access rich network context data.

- **Rogue and aWIPS**: Contains the REST API supported by Cisco DNA Center for Rogue Management and the Cisco Advanced Wireless Intrusion Prevention System (aWIPS). This API is used to detect wired and wireless threats, including rogue access points.

- **Cisco DNA Center Automation events for ITSM (ServiceNow)**: Monitor and publish events requiring software image updates (for compliance, security, or other operational triggers) to a ServiceNow system.

- **Disaster Recovery API**: This bundle contains the REST APIs supported by disaster recovery and provide support to monitor the disaster recovery system.

- **AI Endpoint Analytics**: This bundle allows you to access various services provided by AI endpoint analytics application. You must install **AI Endpoint Analytics** package in Cisco DNA Center to use this bundle.

You can adjust the bundles that are displayed in the GUI by clicking the **Filter** icon and using the filter, or by entering a keyword in the **Find** field.

Step 3   Click the **Basic ITSM (ServiceNow) CMDB synchronization** bundle link or icon.

The following information is provided:

- **General information**: Vendor, version, platform, tags displayed under the square icon.

     Note   Tags indicate what the Cisco DNA Center component is used for or is affected by the bundle.

- **Information**: Tab that displays general information (purpose of bundle and how bundle works in the network), sample schemas, mapping notes, configuration notes, and other data about the bundle.

- **Contents**: Tab that accesses the integration flows that make up the bundle, or provides information about the integration flows that make up the bundle.

- **Release Notes**: Tab that displays latest release information about the bundle, including its version.

Step 4   Review the bundle data in the **Information** tab and click the **Contents** tab.

Step 5   Click the **Integration Flows** header.

Review the list of available integration flows (links) under the header. For detailed information about integration flows and their purpose, see .

Step 6   Click the **Enable** button to activate the links.

An **Information** field appears in the window.

Step 7   In the **Information** field, click the **Enable** button to confirm enabling the bundle.

After clicking the **Enable** button to confirm, a success message appears.

Step 8   Click **Okay** in the success message.

Step 9   Click the integration flow link to perform the following tasks:

- Review the **Description**, **Tags**, **How to Use this Flow**, and scheduler.

- Click **Run Now** (to run the scheduler now), **Run Later** (to schedule for a later time), or **Recurring** (to set up a recurring schedule).

  For **Run Later**, you need to select a date, time, and time zone. For **Recurring**, you need to set a repeating interval (daily or weekly), an interval duration (minutes or hours), and a start and end date.

- Click **Schedule** to enable the scheduler.

  Important   Only configure and enable an integration flow schedule, after you have finished configuring the bundle itself as described in this procedure. You can configure and enable an integration flow schedule by returning to this view and clicking **Schedule**, or by clicking the **View Flows** link in the **Configure Basic ITSM (ServiceNow) CMDB synchronization** slide-in pane (see following steps), or by accessing the view by clicking the menu icon (≡) > **Platform** > **Developer Toolkit** > **Integration Flows** > **Schedule to Publish Inventory Details-ServiceNow Connector**.

Step 10   Click the **X** icon at the upper right of the window to close it and return to the previous bundle window.

Step 11   Click the **Configure** button to configure at the bundle level.

A configuration slide-in pane appears. Review the CMDB synchronization information.

Step 12   Click the radio button to configure either existing or new ServiceNow access settings for the CMDB synchronization.

Figure 8: ServiceNow Access Settings
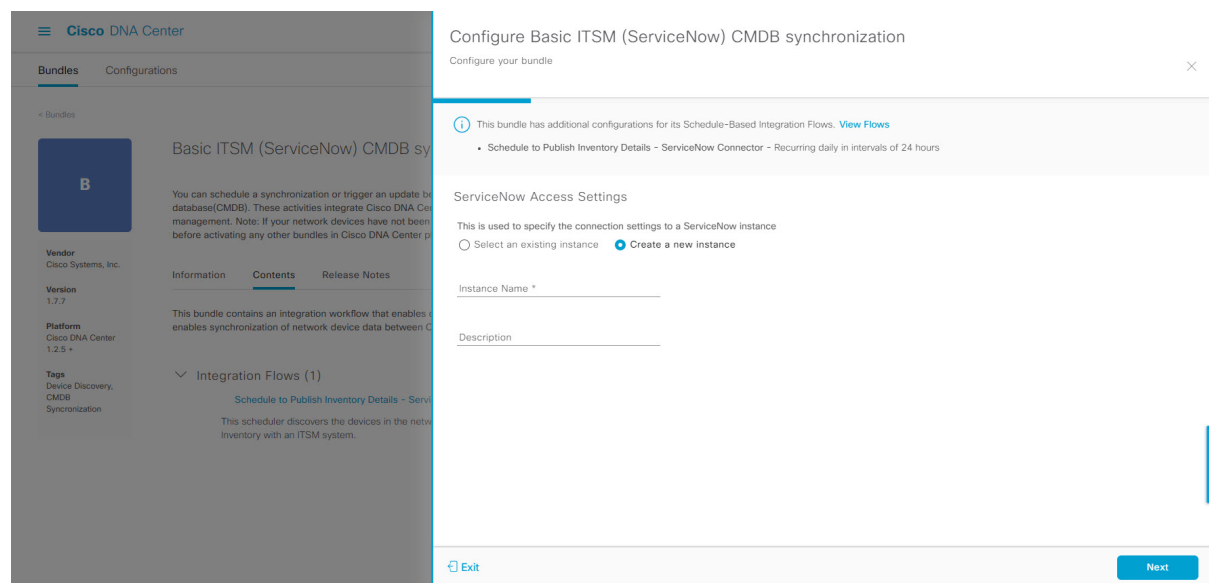
For configuring an existing setting, choose it from the drop-down menu in the window and click **Next**.

Step 13   For configuring a new access setting, the following instance information must be entered.

- **Instance Name**: Name of the instance.

- **Description**: Descriptive text of the instance.

Click **Next**.

Step 14 For configuring a new access setting, the following additional settings information must be entered.

Figure 9: ServiceNow Access Settings
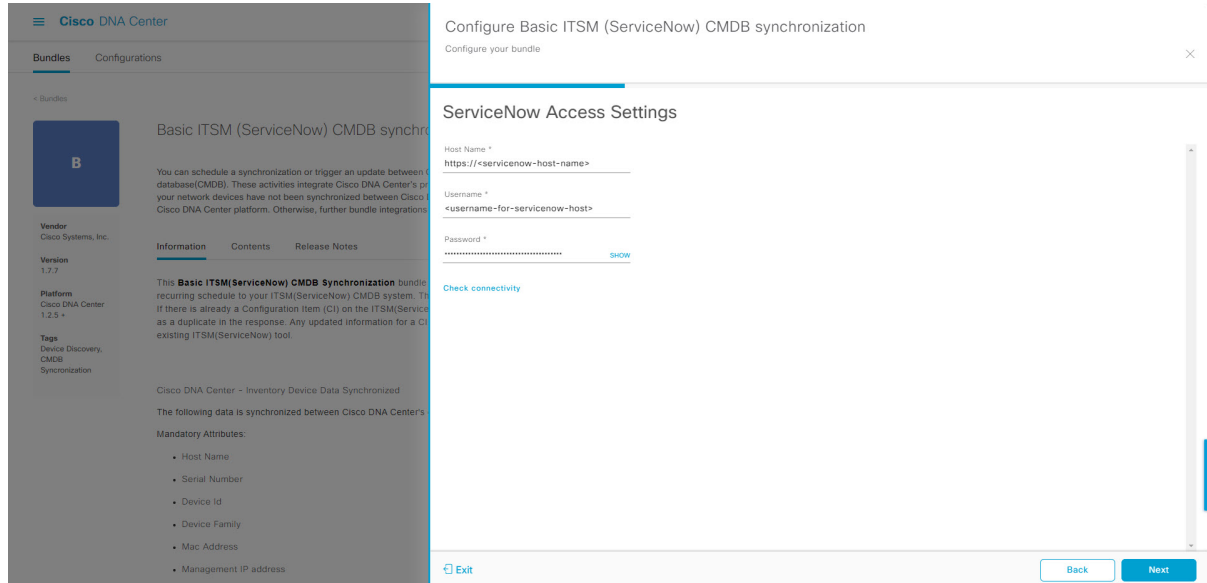
- **Hostname**: Hostname or IP address of the ServiceNow server.

- **Username**: Username for access to the ServiceNow server.

- **Password**: Password for access to the ServiceNow server.

Click **Check Connectivity** to check access to the ServiceNow server.

Click **Next**.

Step 15 Click the radio button to configure either an existing instance or configure a new instance for the CMDB inventory settings.

Figure 10: CMDB Inventory Settings
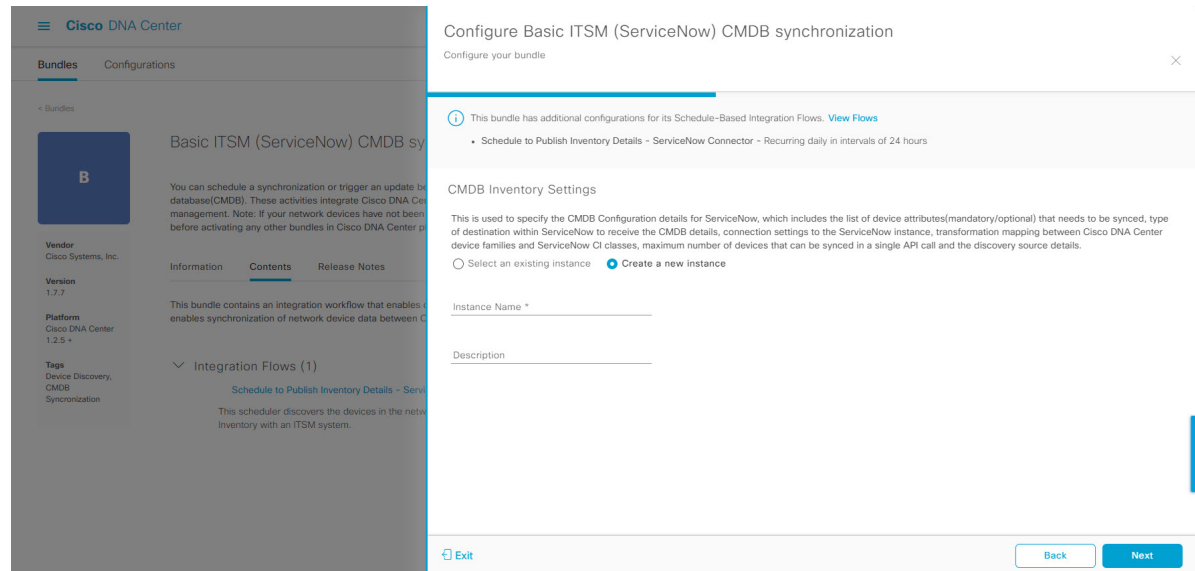
For configuring an existing instance, choose it from the drop-down menu in the window and click **Configure**.

Step 16 For configuring a new instance, the following additional information must be entered.

- **Instance Name**: Name of the instance.

- **Description**: Descriptive text of the instance.

Click **Next**.

Step 17 In the **Select Destination** window, enter the following information:

- **Destination Type**: There are two discovery source options to choose from:

    - **Synchronize device inventory directly with CMDB**

    - **Post device inventory details to a staging table**

    Note With a staging table, you can take the values from the table and map it to a ServiceNow CMDB.

- **Destination URI**: Uniform Resource Indicator (URI) of the ServiceNow server (CMDB) or staging table.

Figure 11: Select Destination Window
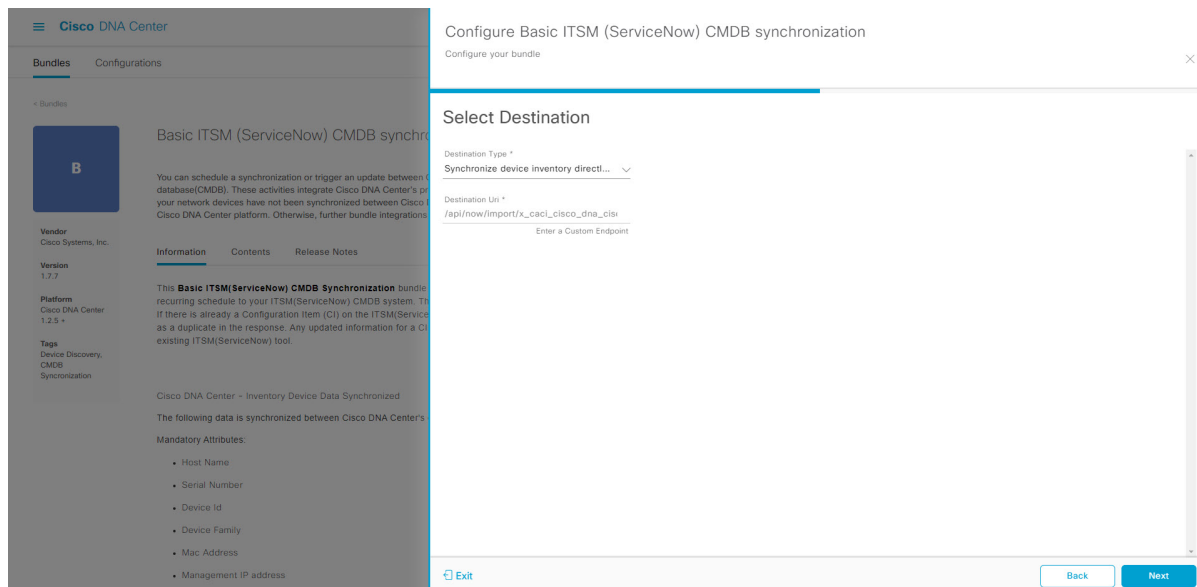
Click **Next**.

Step 18 In the **Select Inventory Data Fields** window, select the inventory data fields to by synchronized.

Note Inventory data fields are Cisco created data types that can be designated as an attribute or reference to be synchronized into a CMDB or staging table.

Clicking the top check box in the **Select Inventory Data Fields** window will select all of the inventory data fields for synchronization. Click this top check box if you want to sync all of the inventory data fields. Otherwise, review and click a check box at a time to create a smaller subset of inventory data fields for synchronization.

Figure 12: Select Inventory Data Fields Window
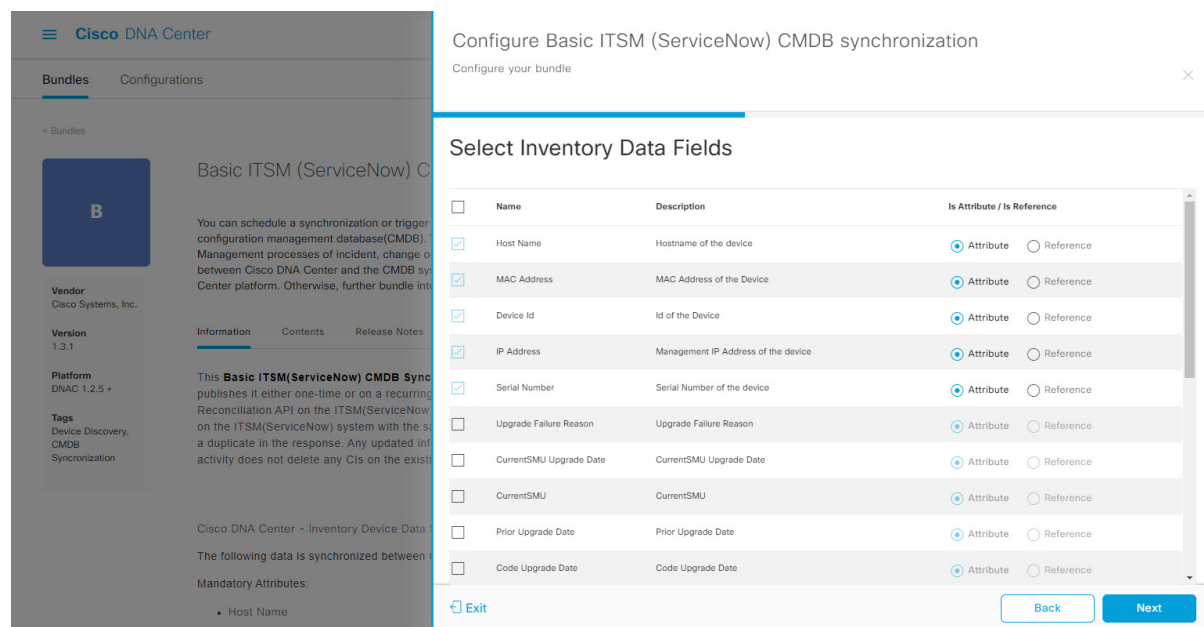
The **Select Inventory Data Fields** window consists of the following columns:

- **Name**: Name of the inventory data field.

- **Description**: Brief description of the inventory data field.

- **Is Attribute/Is Reference**: Whether the inventory data field is an attribute or a reference. A reference data field is used to create a relationship between two tables in a database. An attribute data field is used to add more data to a table in a database.

Step 19   For the data fields selected to be synchronized in the preceding step, review their default designation as either an attribute or reference.

To change a data field's default designation, just click the desired data field designation (**Attribute** or **Reference**).

After selecting the data fields to be synchronized and whether the data field is an attribute or reference, click **Next**.

Step 20   In the **Update Transforms** window, either accept or update the ServiceNow transformation mapping between the Cisco DNA Center device families and the ServiceNow CI classes.

Figure 13: Update Transforms Window
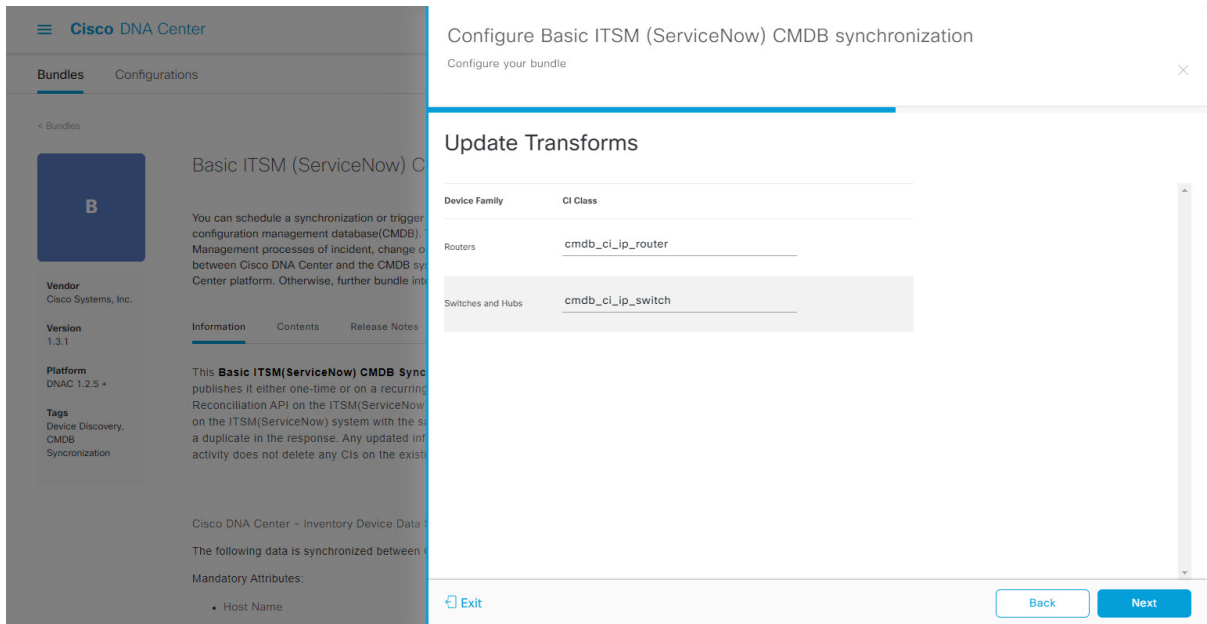
Device families are the Cisco DNA Center device classifications (for example, Unified AP, Routers, Wireless Controller, Switches, and Hubs), where the inventory attributes/references mapping to ServiceNow is already available in the existing Cisco DNA Center application in ServiceNow. The type and number of device families can vary depending upon the different Cisco devices in the user's network.

Note Cisco DNA Center platform is able to automatically retrieve all of the device families in the user's Cisco DNA Center network and display them in this GUI window.

CI classes are the database tables for ServiceNow (for example, cmdb_ci_wap_network, cmdb_ci_ip_router, cmdb_ci_ip_switch, and x_caci_cisco_dna_wireless_lan_controller). The **CI Class** column in the GUI window above is used to map the CI classes to their respective device families.

The following table displays the Cisco DNA Center default CI classes for each device family. The default CI classes can be modified by the user. In case of other device families not listed below, Cisco will not have any default values specified in the **CI Class** column. The ServiceNow application user needs to either manually create the corresponding CI Classes and attributes/references mapping or use a pre-existing CI class a 'parent' CI class.

Table 2: Default Device Family to CI Class Mapping List

Device Family	Corresponding CI Class
Unified AP	cmdb_ci_wap_network
Wireless Controller	x_caci_cisco_dna_wireless_lan_controller
Routers	cmdb_ci_ip_router
Switches and Hubs	cmdb_ci_ip_switch
Meraki Access Point	cmdb_ci_wap_network
Meraki Cameras	cmdb_ci_netgear

Device Family	Corresponding CI Class
Meraki Dashboard	cmdb_ci_netgear
Meraki Security Appliances	cmdb_ci_netgear
Meraki Switches	cmdb_ci_ip_switch

After accepting or updating the information in this window, click **Next**.

Step 21 In the **Set Source Identifier and Operational Limit** window, configure the data source and maximum limit.

Figure 14: Set Source Identifier and Operational Limit Window
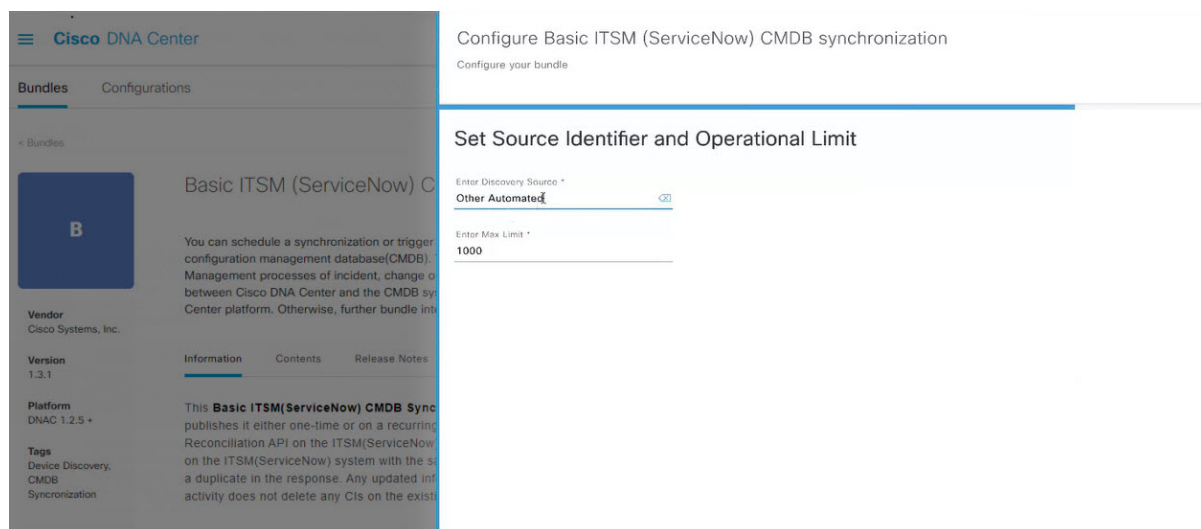
Configure the following values:

- **Enter Discovery Source**: Enter the same value as previously selected or keep the value at its default, **Other Automated**.

  - **Synchronize device inventory directly with CMDB**

  - **Post device inventory details to a staging table**

Note	**Other Automated** is a preconfigured value for the discovery source attribute in an OOB ServiceNow instance. This is the value that indicates the data source from where the ServiceNow CI was discovered. As a default, Cisco uses one of the existing preconfigured values for the integration.

- **Enter the Max Limit**: Maximum number of devices that can be synchronized in an iteration (single API call).

After entering the above information, click **Next**.

Step 22 In the **Summary** window, review the configuration summary.

Figure 15: Summary Window
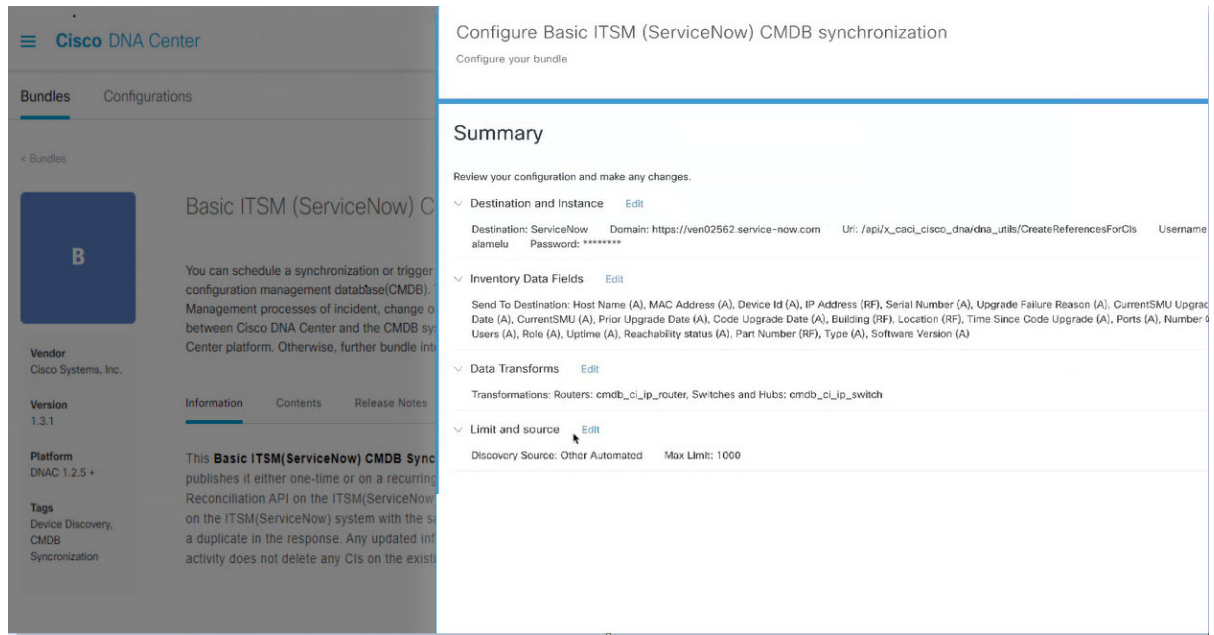
After reviewing the information, click **Configure**.

For a successful configuration, you will receive a **Done! Bundle Configured** message.

What to do next

Configure the Integration Flow for this bundle (**Schedule to Publish Inventory Details - ServiceNow Connector**), using one of the methods described in Step 9 above.

Review your configuration, click **Manage** > **Configurations** > **General Settings** and use the **Filter** or **Find** tools to locate the instance configured in this procedure. If necessary, later on you can edit, update, or delete the instance in the **General Settings** window. For additional information, see Configure General Settings: Edit an Instance, on page 35.

You can test the CMDB synchronization by performing the following tasks:

- In the Cisco DNA Center platform GUI, click the menu icon (☰) and choose **Platform** > **Runtime Dashboard** > **Event Summary**. Click **Refresh** to refresh the GUI view. Click the individual events in the window to view the event data and access links to ServiceNow.

- Go to ServiceNow and search for a synchronized device. Check the **Configuration** and **Other Attributes** tabs for the synchronized data in that device's record.

CHAPTER 6

Configurations

About Configurations

Cisco DNA Center platform provides you with **Configurations** to configure a customized network experience using the following options:

- **Event Settings**: Cisco DNA Center platform supports specific Cisco DNA Assurance events (or incidents) that may occur within your network. This means that Cisco DNA Center platform can recognize these events and permits you to configure settings that customize the type, category, and severity under which Cisco DNA Center reports them. Configuring this information in the GUI also permits you to customize the information that Cisco DNA Center sends to an external system, such as ServiceNow (or perhaps to one or more REST endpoints that you can configure).

- **General Settings**: You can add or edit REST and ITSM endpoint instances within a single or multiple bundles.

Note You can also configure various types of destinations to deliver the events from the Cisco DNA Center Platform. Click the menu icon (☰) and choose **System** > **Settings** > **External Services** > **Destinations** to access the GUI window to configure a webhook, email, syslog, SNMP trap, or ITSM destination.

Configure Event Settings

A preset number of issues (or events) that may occur within your network can be found in **Event Settings** in the **Configurations** window. You can configure the type, category, severity, and workflow of these events.

> **Note** The **Event Settings** window functionality is only applicable for an ITSM (ServiceNow) integration and not for generic event notifications. For guidance about how to use this procedure within a larger set of procedures to configure ITSM integration between Cisco DNA Center and ServiceNow, see the *Cisco DNA Center ITSM Integration Guide*. See the text at the top of this window and click the link (**here**) to access the **Events** window in platform, where you can subscribe to events and receive notifications by email, webhook (REST API), SNMP trap, or syslog server.

Figure 16: Event Settings Window

Step 1 Click the menu icon (≡) and choose **Platform** > **Manage** > **Configurations** > **Event Settings**.

Step 2 Review the **Event Settings** table that appears.

The following **Event Settings** information is displayed:

- **Event Name**: Name of the Cisco DNA Center event.

- **Domain**: Domain of the Cisco DNA Center event.

- **Type**: Network, App, System, Security, or Integrations type of event.

- **Category**: Error, Warn, Info, Alert, Task Progress, Task Complete.

- **Severity**: 1 through 5.

  Note Severity 1 is the most important or critical priority and should be assigned as such.

- **Workflow**: Incident, Problem, Event, or RFC.

- **Actions**: Edit.

You can adjust what is displayed in the table by clicking the **Filter** icon and using the filter, or by typing a keyword in the **Find** field. For example, to display all access point notifications, type 'AP' in the **Find** field. To view all network notifications, type 'Network' in the **Find** field. To view all severity 1 notifications, type '1' in the **Find** field.

You can edit the event, so that its notification is customized to your network standards and conventions.

Step 3   Click **Edit** in the **Actions** column to edit an event.

Choose a setting by clicking on the downward pointing angle and adjust the value. For example, click **Network** and adjust to **App**. This changes the event type from a network type to an application type. Click **Severity** and adjust to **1** from **5**. This raises the severity level from 5 to 1.

Step 4   Click the box next to the event name to enable notifications.

This enables notifications through Cisco DNA Center when the event occurs in the future.

Step 5   Click **Save** to save your configuration.

What to do next

- Click the menu icon (≡) > **Platform** > **Runtime Dashboard**.

  Notifications for events display in the **Events Summary** field.

- Click **View Details** to view the notifications.

Configure General Settings: Edit an Instance

You can edit an instance within a single or multiple bundles using **Configurations**.

Figure 17: Cisco DNA Center Platform Configurations Window

Before you begin

Enable, configure, and activate the bundles for your network in **Bundles**. For information about **Bundles** see Bundle Features, on page 14.

Step 1   Click the menu icon (☰) and choose **Platform** > **Manage** > **Configurations** > **General Settings**.

Step 2   Review the **General Settings** table that appears.

The following **General Settings** information is displayed:

- **Name**: Name of the instance and version.

- **Description**: Description of the settings that contain the instances.

- **Instances**: Number of instances currently configured.

- **Usage**: Number of bundles where the instance or instances are used.

- **Actions**: Specific task that you could perform for the setting (for example, edit or add an instance for the setting).

You can adjust what is displayed in the table by clicking the **Filter** icon and using the filter, or by entering a keyword in the **Find** field.

Step 3   Click the arrow for one of the displayed instances. For example, click the **CMDB Synchronization Settings (v1)** or **Destination to Receive Events (v1)** arrow.

The list of instances for that setting is displayed.

Step 4   In the **Usage** column, hover your mouse pointer over **Bundles**.

Cisco DNA Center displays the bundles that use the specified instance.

Step 5   Click the **Edit** icon ('Pad and Pen' icon) in the **Actions** column to edit an existing instance.

Edit the appropriate instance for your requirements in the following steps.

Step 6   (Optional) To edit the CMDB synchronization details for a **CMDB Synchronization Settings** instance, choose **Edit** > **Actions** and edit one or more of the following instance fields in the slide-in panes that appear:

- **ServiceNow Access Settings**: Select an instance from the drop-down menu.

- **CMDB Inventory Settings**: Enter an **Instance Name** and **Description**.

- **Select Destination**: Enter **Destination Type** and **Destination URI**. Options include **Synchronize device inventory directly with CMDB** or **Post device inventory details to a staging table**.

- **Select Inventory Data Fields**: Select both the Inventory Data Fields to synchronize, as well as whether the data field is an attribute or reference.

- **Update Transforms**: Accept or update the CI class to the device family.

- **Set Source Identifier and Operational Limit**: Configure the discovery source and maximum limit.

- **Summary**: Review the configuration and make any changes before saving.

Step 7   (Optional) To edit a **Destination to receive events** instance, choose **Edit** > **Actions** and edit one or more of the following fields in the slide-in pane:

• **Instance Name**: Name of instance.

• **Description**: Description of instance.

• **Destination to Receive Events**: Choose one of the following:

  • **Event Management**: When setting up Cisco DNA Center integration with ServiceNow without using the Cisco DNA App, choose the **Event Management** option. The **Event Management** option also requires that you have the Event Management plugin configured within the ServiceNow instance.

  • **REST API Endpoint**: The **REST API Endpoint** option can be used with the Cisco DNA App. Data is sent to a REST API endpoint within the Cisco DNA App with the **REST API Endpoint** option.

  • **Generic REST Endpoint in ServiceNow**: For the **Generic REST Endpoint in ServiceNow** option, you can send the data to a different staging table in ServiceNow.

• **Destination URI**: Enter a destination URI for the **Generic REST Endpoint in ServiceNow** option. This field is mandatory for this option.

For detailed information about integrating Cisco DNA Center with ServiceNow, see the *Cisco DNA Center ITSM Integration Guide* for this release.

Step 8 Click **Update** to save your edits to the instance.

The edits to the instance immediately take effect.

Configure General Settings: Add an Instance

You can add an instance within a single or multiple bundles using **Configurations**.

Figure 18: Cisco DNA Center Platform Configuration Window

Before you begin

Enable, configure, and activate the bundles for your network in **Bundles**. For information about **Bundles** see Bundle Features, on page 14.

Step 1   Click the menu icon (≡) and choose **Platform** > **Manage** > **Configurations** > **General Settings**.

Step 2   Review the **General Settings** table that appears.

The following **General Settings** information is displayed:

- **Name**: Name of the instance and version.

- **Description**: Description of the settings that contain the instances.

- **Instances**: Number of instances in setting.

- **Usage**: Number of bundles where the instance or instances are used.

- **Actions**: Specific task that you could perform for the setting (for example, edit or add an instance for the setting).

You can adjust what is displayed in the table by clicking the **Filter** icon and using the filter, or by entering a keyword in the **Find** field.

Step 3   Click the arrow for one of the displayed instances. For example, click the **CMDB Synchronization Settings (v1)** or **Destination to Receive Events (v1)** arrow.

The list of instances for that setting is displayed.

Step 4   In the **Usage** column, hover your mouse pointer over **Bundles**.

Cisco DNA Center displays the bundles that use the specified instance.

Step 5   Click the **Add Instances** link in the **Actions** column to add an instance.

Add the appropriate instance or instances for your requirements in the following steps.

Step 6   (Optional) To add a **CMDB Synchronization Settings** instance, click **Add Instance** in the **Actions** column and enter the following instance fields in the slide-in panes that appear:

- **ServiceNow Access Settings**: Select an instance from the drop-down menu.

- **CMDB Inventory Settings**: Enter an **Instance Name** and **Description**.

- **Select Destination**: Enter **Destination Type** and **Destination URI**. Options include **Synchronize device inventory directly with CMDB** or **Post device inventory details to a staging table**.

- **Select Inventory Data Fields**: Select both the Inventory Data Fields to synchronize, as well as whether the data field is an attribute or reference.

- **Update Transforms**: Accept or update the CI class to the device family.

- **Set Source Identifier and Operational Limit**: Configure the discovery source and maximum limit.

- **Summary**: Review the configuration and make any changes before saving.

Step 7   (Optional) To add a **Destination to receive events** instance, click **Add Instance** in the **Actions** column and enter the following instance fields in the slide-in pane:

- **Instance Name**: Name of instance.

- **Description**: Description of instance.

- **Destination to Receive Events**: Choose one of the following:

    - **Event Management**: When setting up Cisco DNA Center integration with ServiceNow without using the Cisco DNA App, choose the **Event Management** option. The **Event Management** option also requires that you have the Event Management plugin configured within the ServiceNow instance.

    - **REST API Endpoint**: The **REST API Endpoint** option can be used with the Cisco DNA App. Data is sent to a REST API endpoint within the Cisco DNA App with the **REST API Endpoint** option.

    - **Generic REST Endpoint in ServiceNow**: For the **Generic REST Endpoint in ServiceNow** option, you can send the data to a different staging table in ServiceNow.

- **Destination URI**: Enter a destination URI for the **Generic REST Endpoint in ServiceNow** option. This field is mandatory for this option.

For detailed information about integrating Cisco DNA Center with ServiceNow, see the *Cisco DNA Center ITSM Integration Guide* for this release.

Step 8   Click **Add** to save your instance addition.

The additions to the instance immediately take effect.

Configure a Webhook Destination

Cisco DNA Center supports a webhook destination for both events and reports.

To configure a webhook destination for events or reports, perform the following steps using the Cisco DNA Center GUI.

Step 1   Click the menu icon (☰) and choose **System** > **Settings** > **External Services** > **Destination** > **Webhook**.

Step 2   Review the **Webhook** tab.

Figure 19: Webhook Tab
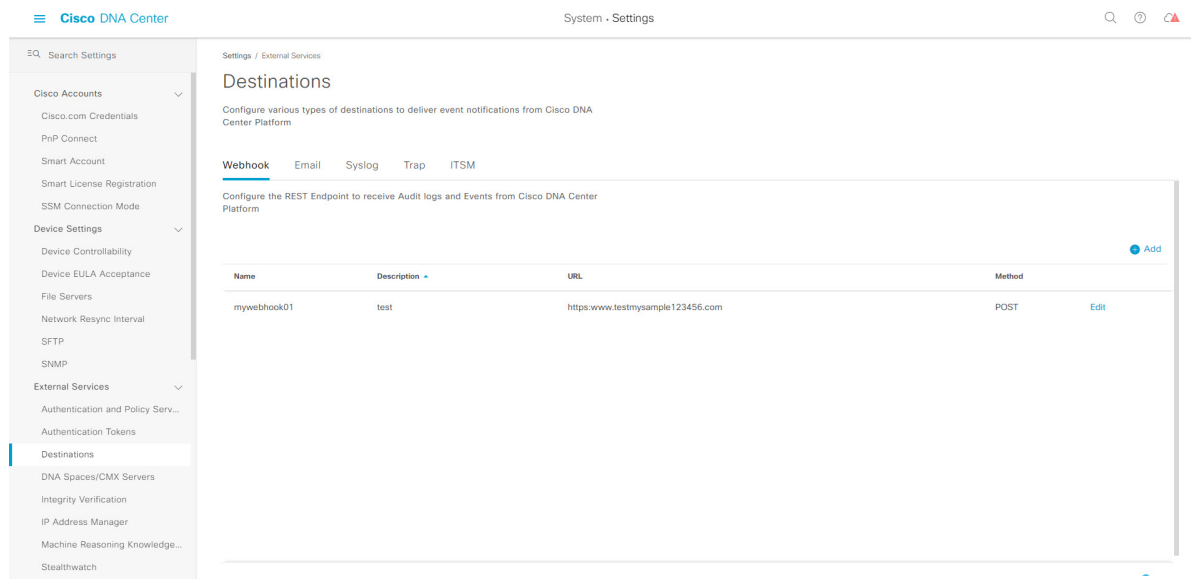
The following fields are displayed:

- **Name**: Name of the webhook.

- **Description**: Description (user provided) of the webhook.

- **URL**: URL of webhook (callback URL).

- **Method**: REST API method of webhook (POST).

- **Edit**: Link that opens field to edit the configured webhook fields. After editing the webhook configuration, click **Update** to save your changes.
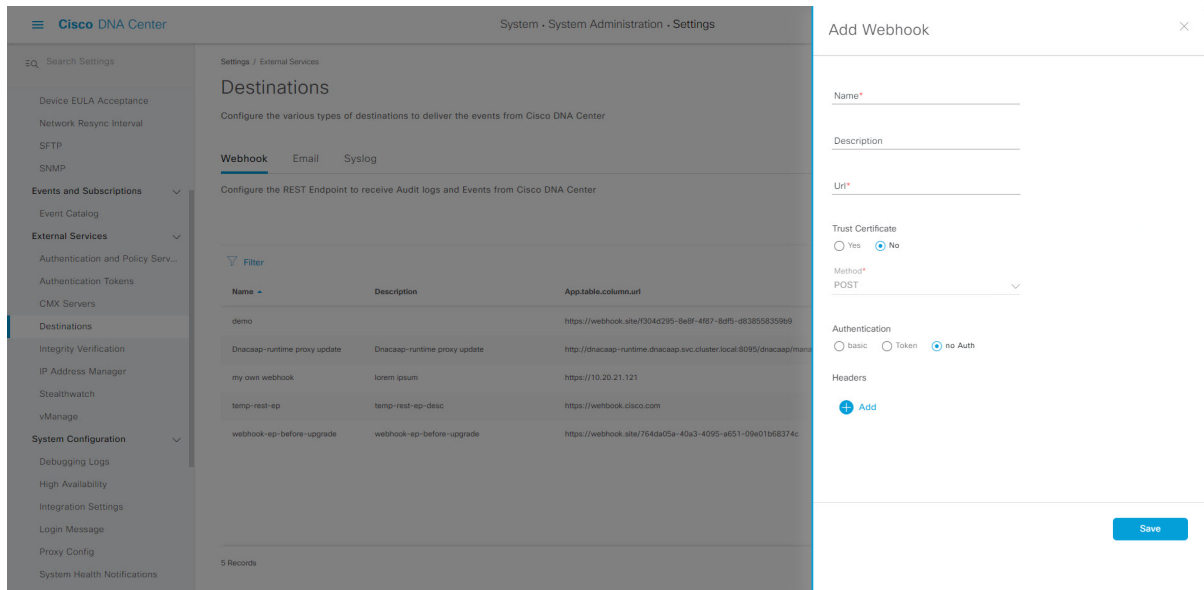
For this release, you can configure an IPv6 value for the URL.

Step 3   Click **Add** to configure a webhook.

An **Add Webhook** slide-in pane is displayed.

Step 4   Enter values in the fields in the **Add Webhook** slide-in pane to configure the webhook.

Figure 20: Add Webhook

- **Name**: Name of the webhook.

- **Description**: Description of the webhook.

- **URL**: URL address of the webhook (callback URL).

Step 5 Depending upon your webhook configuration, choose whether a trust certificate is associated with the webhook URL.

For the **Trust Certificate** radio button, click **Yes** or **No**.

Step 6 Depending upon your webhook configuration, choose the authentication type associated with your webhook URL.

For the **Authentication** radio button, choose one of the following:

- **Basic**: Authentication where the client sends HTTP requests with an Authorization header that contains the word **Basic**, followed by a space and a base64-encoded string *username:password*. If you select **Basic** in the GUI, the **Header Key** field is automatically populated with the **Authorization** value.

- **Token**: Authentication where users are authenticated using a security token that is provided by the server. If you select **Token**, the **Header Key** field below enters the value **X-Auth-Token**.

- **No Authentication**: No authentication needed.

Step 7 Under **Headers**, enter values for the **Header Name** and **Header Value**.

Click **Add** to add the header name and value.

Note Depending on the type of authentication you chose, header names and values may be automatically populated.

Step 8 Click **Save** to save your webhook destination configuration.

What to do next

Configure a webhook destination for either an event or a report. For information about the procedures to configure an event or a report using the webhook destination, see Work with Event Notifications, on page 143 and Run Your First Report, on page 50.

Configure an Email Destination

Cisco DNA Center supports email notification for both events and reports.

Note
- Emails are sent from Cisco DNA Center using the SMTP protocol. Cisco DNA Center only supports cleartext SMTP for email event notifications. If you use an email server that requires SSL/TLS support, you will not be able to receive the email event notifications.

- For the emails to have the correct Cisco DNA Center hyperlink, enter the IP address or hostname of Cisco DNA Center in the **Integrations Settings** window. To enter this information using the GUI, click the menu icon (≡) and choose **System** > **Settings** > **System Configuration** > **Integration Settings**. For more information, see Configure Integration Settings, on page 6.

You must have the appropriate permissions to perform the tasks described in this procedure. For information about role-based access control for the Cisco DNA Center platform, see Role-Based Access Control Support for Platform, on page 8.

Perform the following steps to configure an email destination for events or reports using the Cisco DNA Center GUI.

Figure 21: Email Tab

Step 1   Click the menu icon (☰) and choose **System** > **Settings** > **External Services** > **Destinations** > **Email**.

Step 2   Configure the required **Primary SMTP Server** fields:

• **Hostname/IP**: Hostname or IP address of the primary SMTP server. You can configure an IPv6 value for the hostname or IP address.

• **Port**: Port number of the server.

Step 3   Configure the optional **Secondary SMTP Server** fields:

• **Hostname/IP**: Hostname or IP address of the secondary SMTP server. You can configure an IPv6 value for the hostname or IP address.

• **Port**: Port number of the server.

Step 4   Configure the **Senders and Receivers** test email fields:

• **From**: Sender of the test email.

• **To**: Recipient of the test email.

• **Subject**: Enter text (up to a maximum of 200 characters) for a subject line for the test email.

Step 5 To test the email configuration, click **Test**.

After you click **Test**, a test email is sent using the parameters that are configured (for both primary and secondary SMTP server settings with **Cisco DNA Center SMTP configuration test email** as the subject line). A success (configuration validation) or failure message should appear depending on the test email connectivity results.

Step 6 To save the configuration, click **Save**.

To cancel the configuration, click **Cancel**.

What to do next

Configure an email destination for either an event or a report. For information, see Work with Event Notifications, on page 143 and Run Your First Report, on page 50.

Configure a Syslog Server Destination

Cisco DNA Center supports a syslog server destination for event notifications.

Perform the following steps to configure a syslog server destination for event notifications using the Cisco DNA Center GUI.

Step 1 Click the menu icon (≡) and choose **System** > **Settings** > **External Services** > **Destination** > **Syslog**.

Step 2 Review the **Syslog** tab.

Figure 22: Syslog Tab
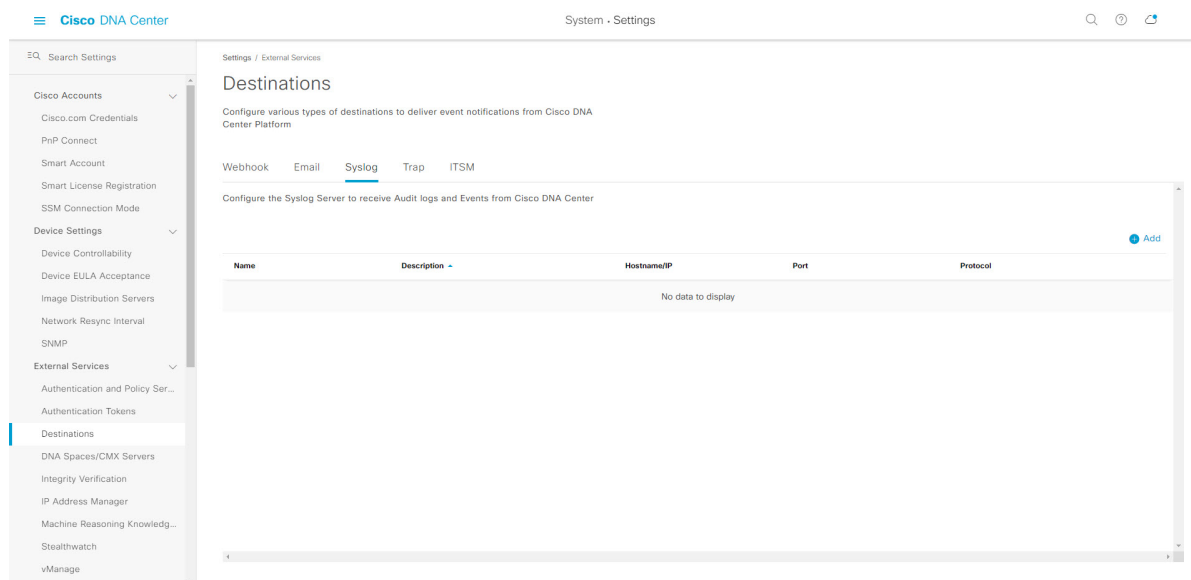
The following fields are displayed:

• **Name**: Name of the syslog server.

• **Description**: Description of the syslog server.

• **Hostname/IP**: Hostname or IP address of the syslog server.

• **Port**: Port number of the syslog server.

• **Protocol**: Either TCP or UDP protocol.

Step 3   To configure a syslog server, click the **Addition** icon (+).

Figure 23: Configure a Syslog Server

Step 4   In the **Name** field, enter a name for the syslog server.

Step 5   In the **Description** field, enter a brief description of the syslog server.

Step 6   In the **Syslog Server Address** field, enter a hostname or IP address.

Step 7   In the **Syslog Server Port** field, enter a port number.

Step 8   (Optional) To test out the configuration, click **Validate**.

Note   If your configuration was successful, then you will be presented with a validation message.

Step 9   To save your syslog server destination configuration, click **Save**.

To cancel your configuration, click **Cancel**.

What to do next

Configure a syslog server destination for an event notification. For information, see Work with Event Notifications, on page 143.
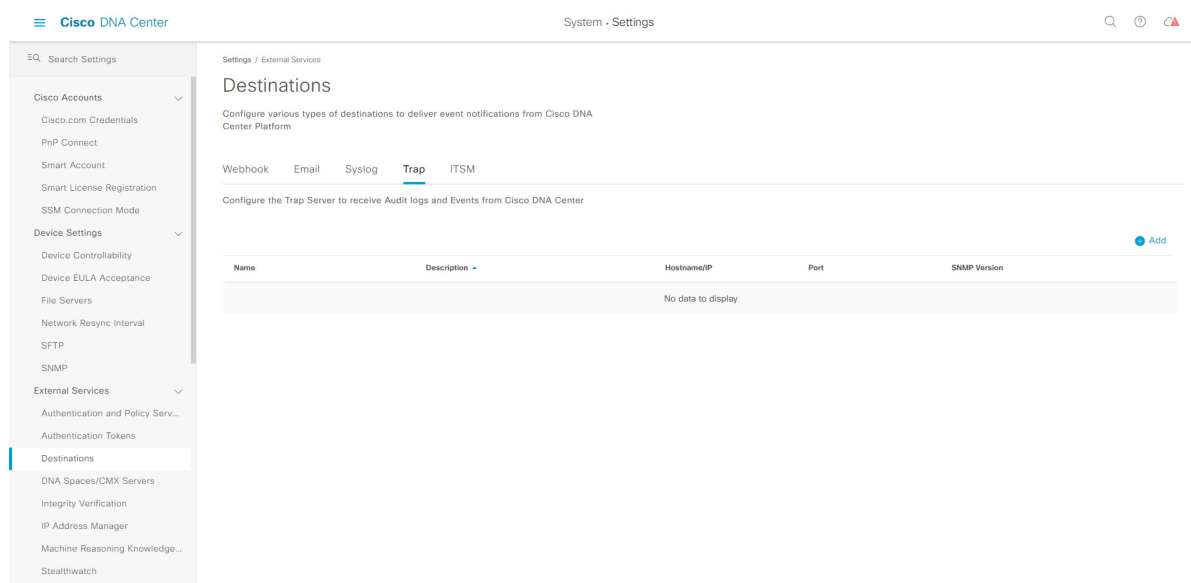
Configure a Trap Notification

Cisco DNA Center supports SNMP trap event notifications.

Perform the following steps to configure SNMP trap event notifications using the Cisco DNA Center GUI.

Step 1 Click the menu icon (☰) and choose **System** > **Settings** > **External Services** > **Destination** > **Trap**.

Step 2 Review the **Trap** window.
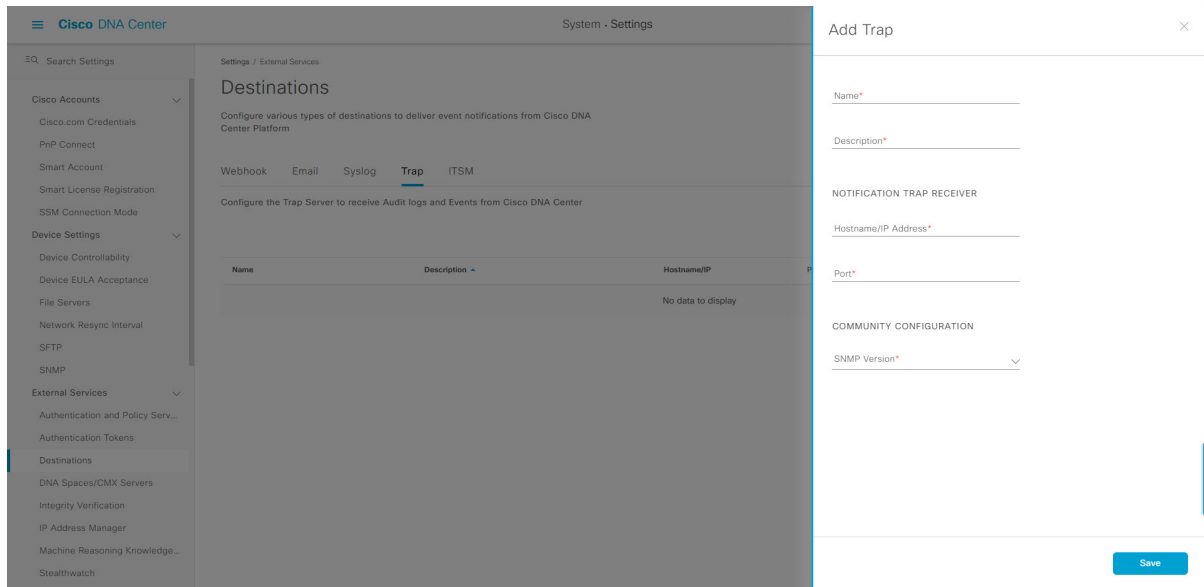
Figure 24: Trap Tab

The **Trap** window consists of a table with the following headers:

- **Name**

- **Description**

- **Hostname/IP**

- **Port**

- **SNMP Version**

Step 3 Click **Add** to configure a trap.

Figure 25: Add Trap

Step 4   Configure the following fields in the slide-in pane:

- **Name**: Name of the event.

- **Description**: Word or phrase about the event.

- **Hostname/IP Address**: Enter the hostname or IP address for the SNMP trap receiver (server).

    For this release, you can configure an IPv6 value for the **Hostname/IP address**.

- **Port**: Enter the port number for the SNMP trap receiver (server).

- **SNMP Version**: Choose the SNMP version from the drop-down list:

    - **SNMP V2C**: For SNMP Version 2C, enter the community string.

    - **SNMP V3**: For SNMP Version 3, enter the following additional information:

        - **Username**

        - **Mode**: Choose a mode from the drop-down list.

            - For **No Authentication, No Privacy** selection, no further configuration is required.

            - For **Authentication, No Privacy**, configure the Authentication Type (SHA or MD5), Authentication Password, Confirm Authentication Password.

            - For **Authentication and Privacy**, configure the **Authentication Type (SHA or MD5)**, **Authentication Password**, **Confirm Authentication Password**. Additionally, configure the **Privacy Type (AES128, DES)**, **Privacy Password**, and **Confirm Privacy Password**.

Step 5   To save your configuration, click **Save**.

What to do next

Access the **Events** window to select one or more events and subscribe to the configured SNMP trap destination. Click the **Menu** icon > **Platform** > **Developer Toolkit** > **Events** to access events. Choose an event that supports subscription to an SNMP trap destination (SYSTEM type event) and subscribe.

Reports

About Reports

You can utilize data from the **Reports** feature to derive insights into your network and its operation. By reporting this data in several formats and providing flexible scheduling and configuration options, both data and reports are easily customized to meet your operational needs.

The **Reports** feature supports the following use cases:

• Capacity planning: Understanding how devices within your network are being utilized.

• Change of pattern: Tracking how usage pattern trends change on the network. Usage pattern trends may include clients, devices, bands, or applications.

• Operational reporting: Reviewing reports about network operations, such as upgrade completions or provisioning failures.

• Network health: Determining the overall health of your network through reports.

Note New use cases for **Reports** will be added in future releases. Review future Cisco DNA Center platform release notes for information.

Run Your First Report

Perform this procedure to begin running specialized data reports about your network. You can configure data reports using the **Reports** window in the Cisco DNA Center GUI.

Figure 26: Reports Window
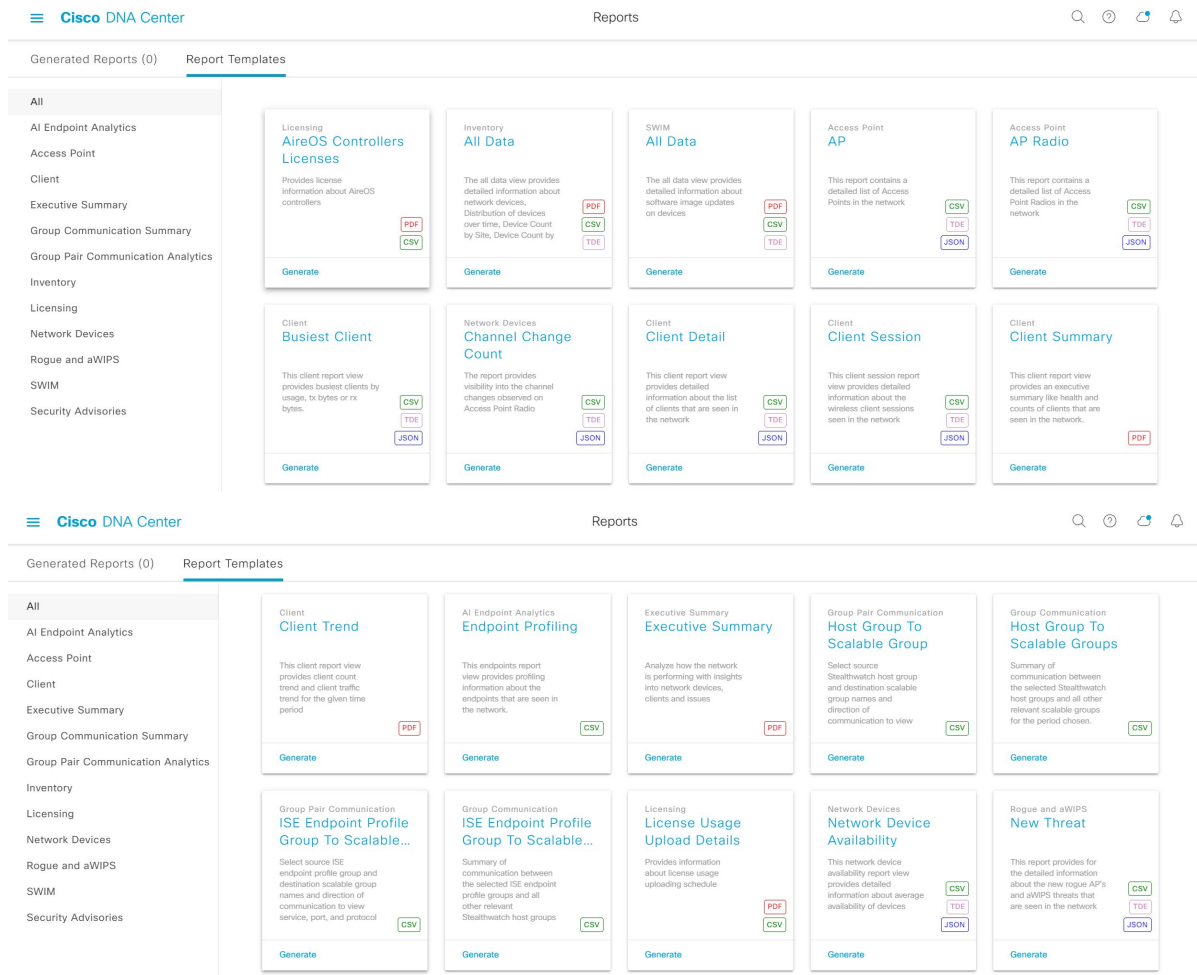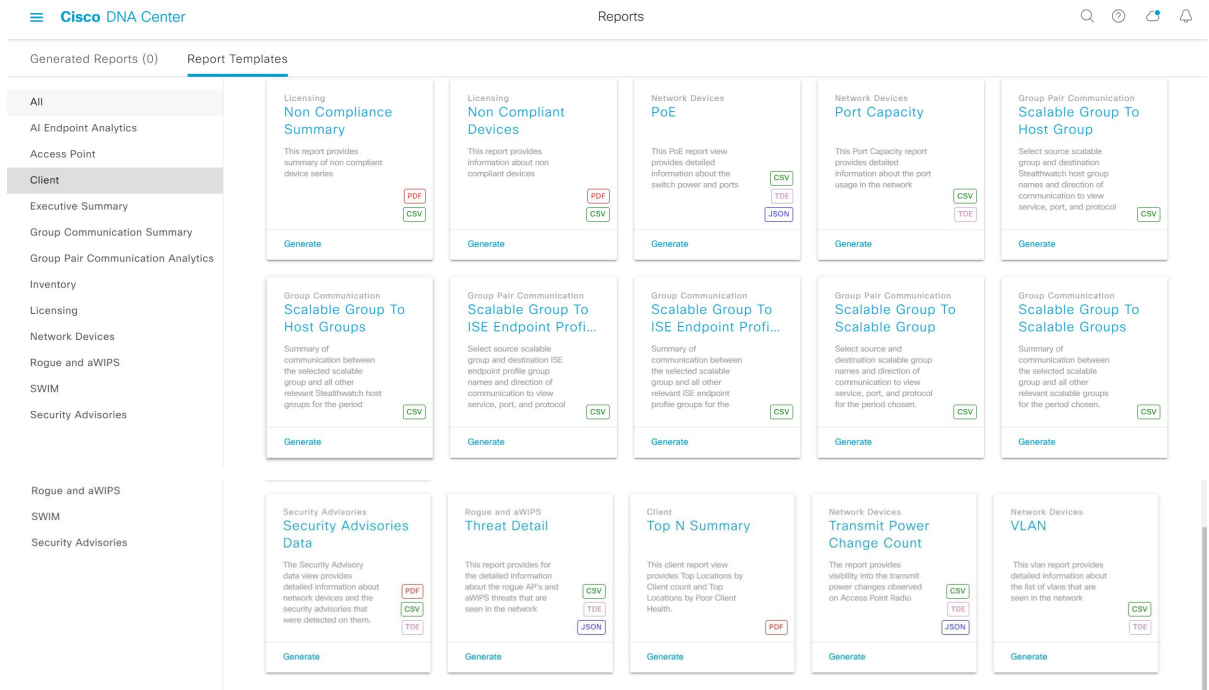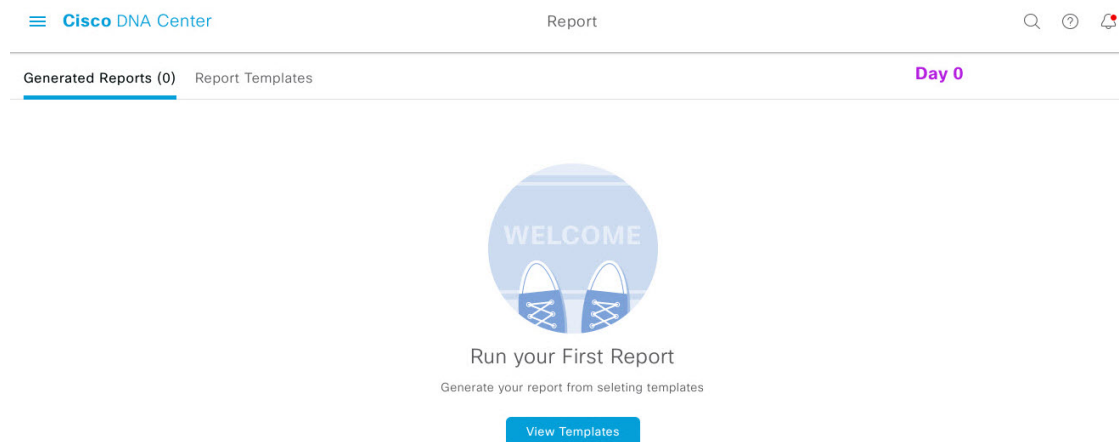
Before you begin

Run a successful **Discovery** job in Cisco DNA Center. You can check whether a **Discovery** job is successful in **Device Inventory**. From the Menu icon (≡), click **Provision** > **Inventory** to view the results.

Step 1   Click the menu icon (≡) and choose **Reports**.

A **Run Your First Report** window appears.

Figure 27: Run Your First Report Window

Step 2   Click **Start**.

The **Report Templates** window opens and displays the supported reporting categories in a slide-in pane. A link represents each category. Click a link to view only the supported reports for that category.

For this release, reporting is supported for the following categories:

Note	The Access Point, Client, and Executive Summary reports support up to 90 days of data retention.
	For this procedure and as an example, **Clients** is selected. Available options for the reports and displayed in the GUI are dependent upon the type of report selected.

Step 3 After clicking a link, review the **Report Templates** window for that selected category.

Figure 28: Reports Templates Window
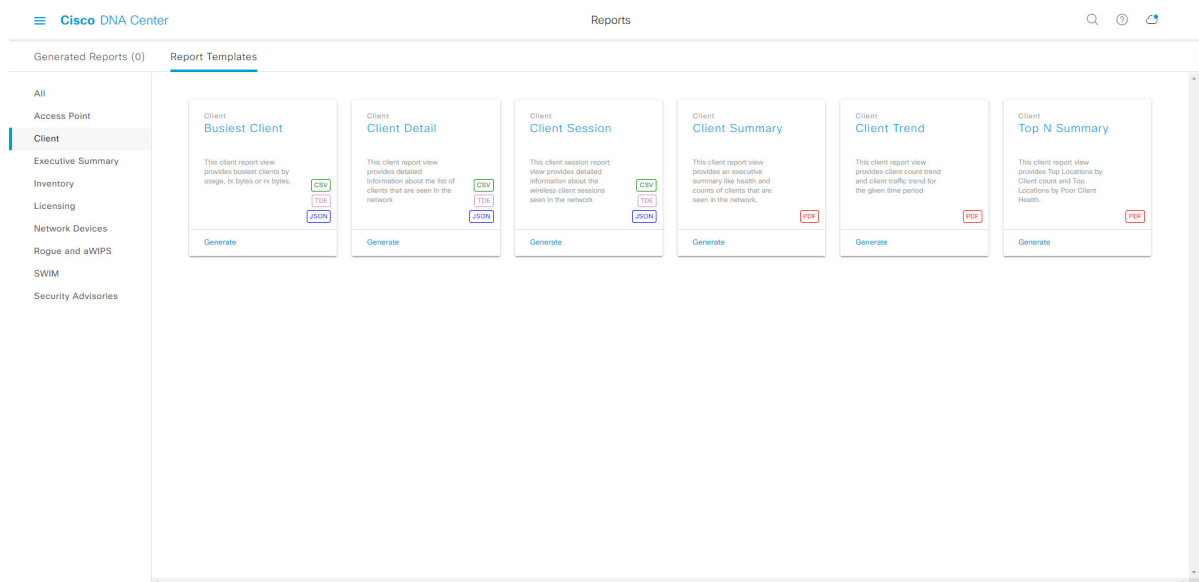
The **Report Templates** window displays supported report templates. Each template is represented by a tile and contains information about the report and links to configure (generate) a report. Determine which template you wish to use to generate a report. For example, for a **Client** report you can create a **Client Summary**, **Client Detail** , **Top N Summary**, **Client Trend**, or **Client Session** report. Within each tile are also icons that represent the supported file types for the reports (PDF, CSV, TDE, or JSON).

Step 4 In the tile, click the header to view a sample report.

A **Preview** window appears for the sample report. Use the side bar in the window to scroll down and review the entire sample report. The following data is presented:

- Applied filters (data filters that were used to build the report).

- Data metrics and summaries

- Graphical representation of the data (including line, bar, and pie graphs).

- Tables that assist you in analyzing the data.

| Note	You can use the sample report to plan how you want your report to look.

Step 5 Click **X** to close the preview.

Step 6 In the tile, click the **Generate** link to configure parameters to build a report.

The **Generate** window opens where you can select a format type for the report, apply data filters for your reports, as well as set up schedules for the actual report generation.

Step 7 In the **Generate a New Report** window, click **Let's Do It** to get started.
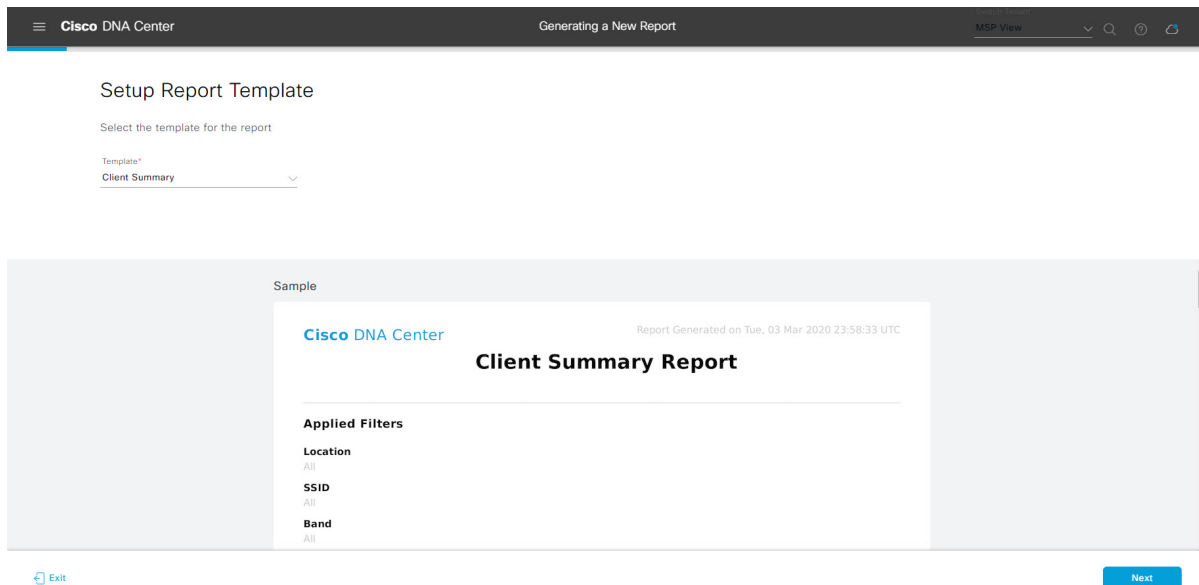
Figure 29: Generate a New Report
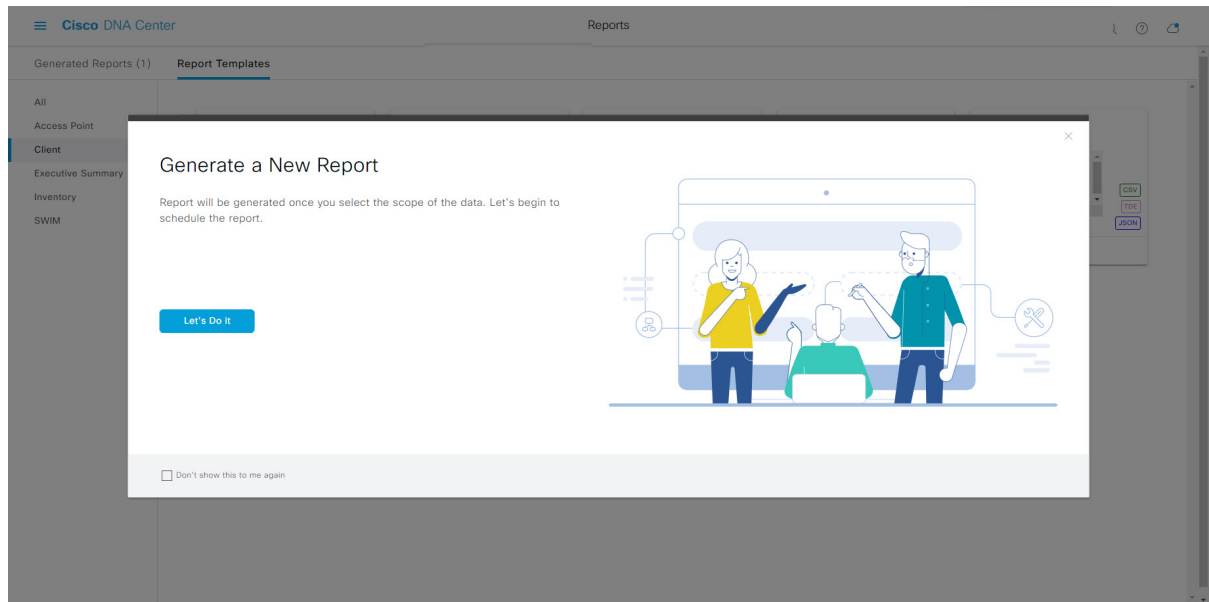
The **Select Report Template** window opens.

Step 8 In the **Select Report Template** window, select the template for the report.

The **Template** consists of the individual report types within the categories for the release.

You can review an autogenerated sample in the same window.

Figure 30: Setup Report Template

Click **Next**. The **Setup Report Scope** window opens.
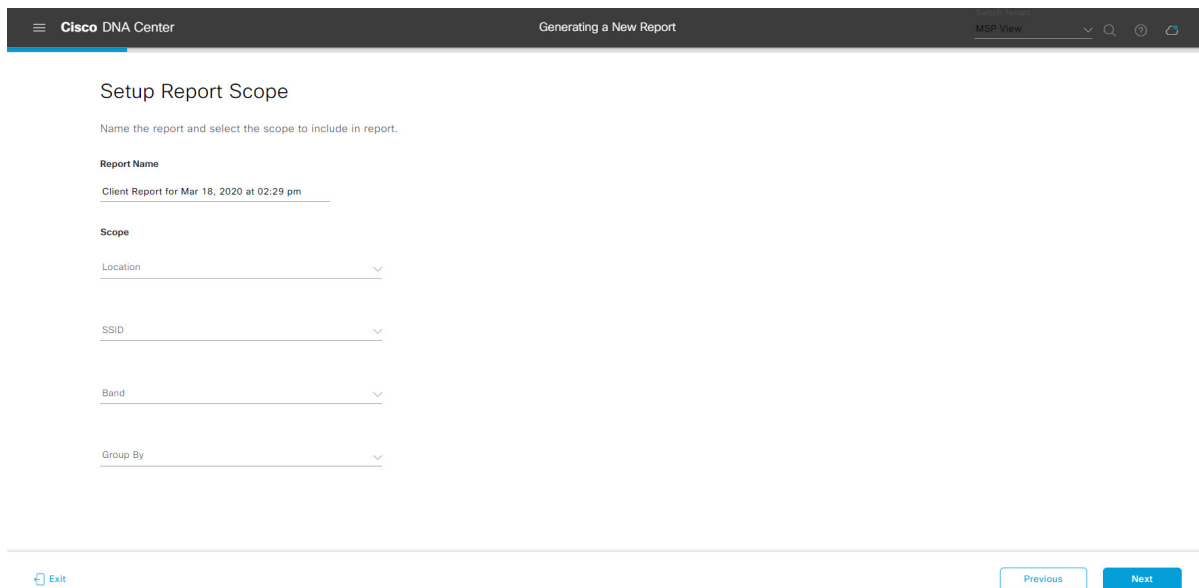
Step 9   In the **Setup Report Scope** window, enter a name for the report and select the scope.

Enter a report name in the **Report Name** field and click in the **Scope** field to display the available filter. Click the filter options that you want for the report.

Note   The **Setup Report Scope** options change depending upon the selected **Template Group**.

Figure 31: Setup Report Scope

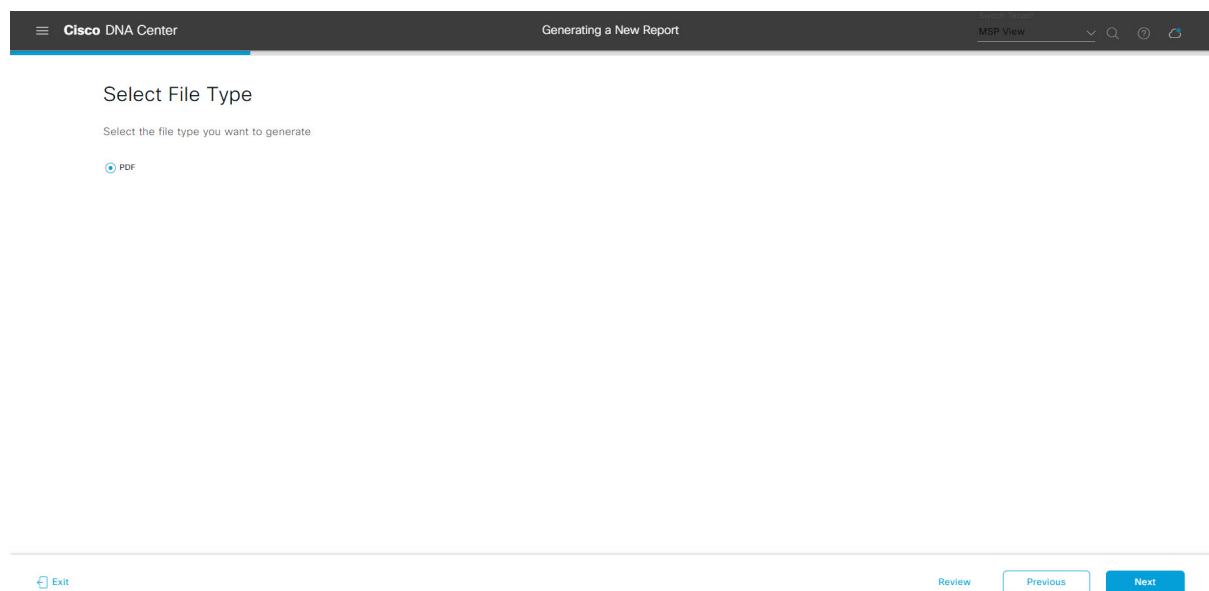Click **Next**. The **Select File Type** window opens.

Step 10   In the **Select File Type** window, select the file type for the report.

Depending upon the report that you are creating, the following **File Type** options may be available:

- **PDF**
- **CSV**
- **Tableau Data Extract**
- **JSON**

For the **CSV**, **JSON**, and **Tableau Data Extract** file types, a **Fields** option displays that permits you to select attributes (additional fields) for the CSV, JSON, and Tableau Data Extract results.

Figure 32: Select File Type

Click **Next**. The **Schedule Report** window opens.

Step 11   In the **Schedule Report** window, select the time range and schedule for the report.

The following **Time Range** options are available:

- **Last 3 hours**
- **Last 24 hours**
- **Last 7 days**
- **Custom**

Note	Clicking **Custom** opens up fields where you can choose the date and time interval per the specific report type, as well as the time zone (GMT) for the time range.

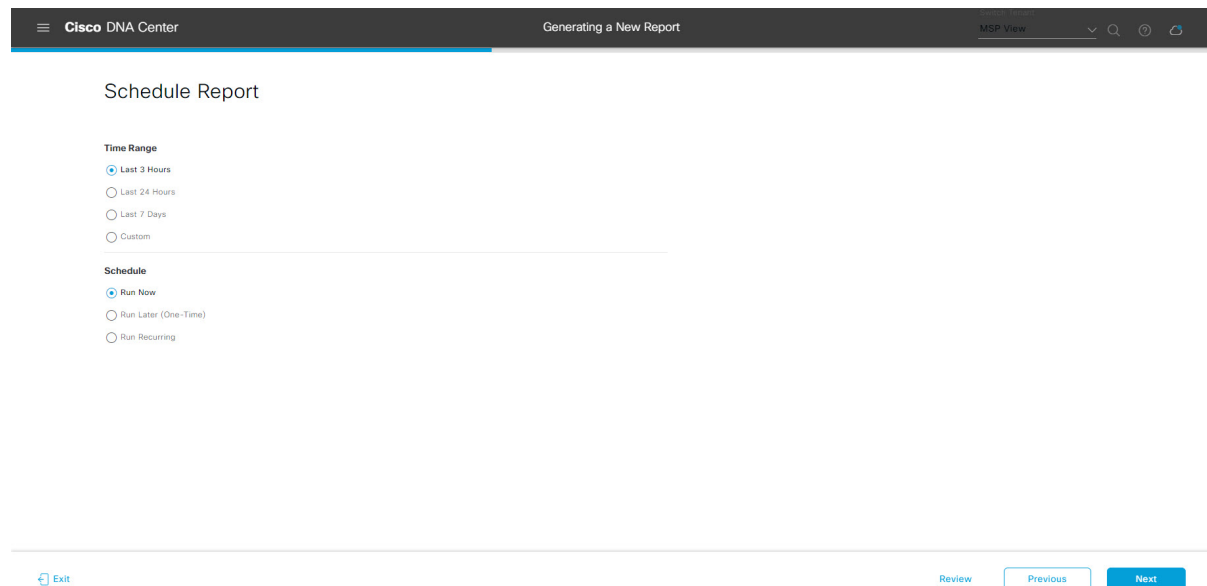The following **Schedule** options are available:

- **Run Now**

- **Run Later**

- **Run Recurring**

You can also select a time zone for the report when configuring with the following **Schedule** options:

- **Custom**

- **Run Later (One Time)**

- **Run Recurring**

Figure 33: Schedule Report

Click **Next**. The **Delivery and Notification** window opens.

Step 12 In the **Delivery and Notification** window, select the Delivery mechanism for the report.

The options include:

- **No delivery/notification**: No email or webhook notifications sent.

- **Email Report**: Email report is sent as a link or attachment.

Note If you have not yet configured an SMTP server for the emails, you will be prompted to configure one. Follow the prompts to the **Email** tab in the GUI to configure a SMTP server. Click **System** > **Settings** > **External Services** > **Destinations** > **Email** tab.

- **Link**: The email notification of a successfully compiled report has a link back to itself and the **Generated Reports** page under **Reports**. You can view and download the report from this link and location.

Note Email notifications with embedded links to reports support up to 20 email addresses. To add multiple email addresses, you need to add each email address separately and press **Enter** (on your keyboard) after each addition. Cisco DNA Center platform validates the email addresses and notifies you if the syntax is incorrect.

• **Attachment**: Report is attached to the email notification.

Note	PDF reports support email notification attachments of up to 20-MB in size and up to 10 email addresses. To add multiple email addresses, you need to add each email address separately and press **Enter** (on your keyboard) after each addition. Cisco DNA Center platform validates the email addresses and notifies you if the syntax is incorrect.

Cisco DNA Center sends out the following email notifications for the report:

• Report is in the queue waiting to be processed.

• Report processing is in progress.

• Report has successfully been compiled and is completed.

• **Webhook Notification**: Notification is sent as a webhook to the configured webhook URL address (callback URL). Select a webhook from the drop-down list **(Subscription Profile** field).

Note	If you have not yet created a webhook, you will be prompted to create one. Follow the prompts to the **Webhook** tab in the GUI to configure a webhook. In general, to configure a webhook, click **System** > **Settings** > **External Services** > **Destinations** > **Webhook** tab.

You will receive status webhook notifications for the report. For example, you will receive "In Queue", "In Progress", and "Success" webhook notifications. You will also be able to view these notifications in the GUI.
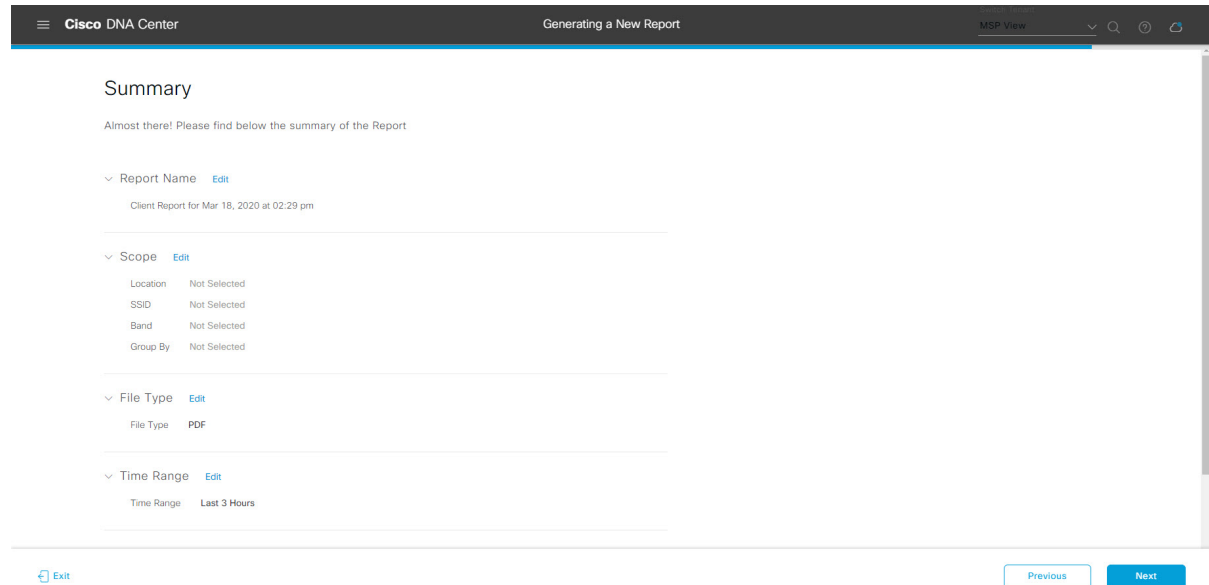
Figure 34: Delivery and Notification

Click **Next**. The **Summary** window opens.

Step 13 In the **Summary** window, review the configuration and if necessary edit any of the files.

Figure 35: Summary

Click the **Next** button.

After the report is generated, a success window appears.

Step 14   Click the **View the Generated Reports** link.

The **Generated Reports** window opens with instance details of the report that was scheduled.

Figure 36: Generated Reports

What to do next

Review your report instance in **Generated Reports** window.

✐

Note You can download, review, edit, duplicate, or delete the report in the **Generated Reports** window. For additional information, see View Generated Reports, on page 133.

Run an Access Point Report

Perform this procedure to configure **Access Point** reports for your network. You can configure **Access Point** reports using the **Reports** window in the Cisco DNA Center GUI.

Figure 37: Access Point Reports
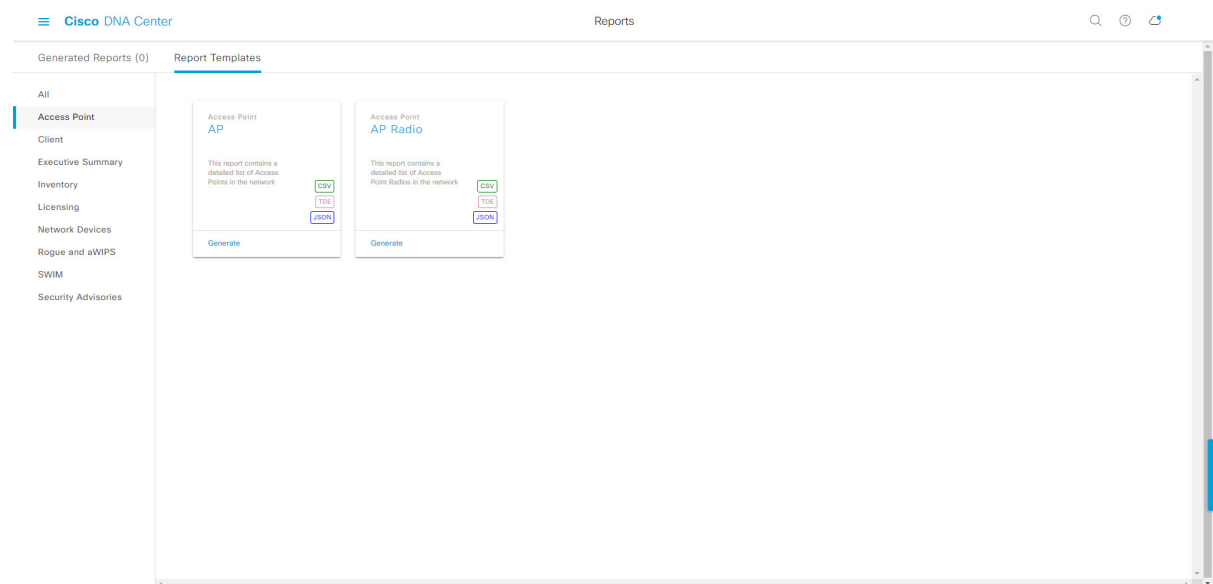
Before you begin

Run a successful **Discovery** job in Cisco DNA Center. You can check whether a **Discovery** job is successful in **Device Inventory**. From the Menu icon (≡), choose **Provision** > **Inventory** to view the results.

Step 1 Click the menu icon (≡) and choose **Reports** > **Report Templates**.

The **Report Templates** window opens and displays the supported reporting categories. A link represents each category. Click a link to view only the supported reports for that category.

For this release, reporting is supported for the following categories:

- **Access Point**: Reports that provide data about Access Points and Access Point Radios.

- **Client**: Reports that help with analyzing how the clients are performing in the network.

- **Executive Summary**: Report that helps with analyzing how devices, applications, and clients are performing in the network.

- **Inventory**: Report listing devices discovered by Cisco DNA Center.

- **Licensing**: Reports that lists devices that noncompliant devices and the reasons for noncompliance.

- **Network Devices**: Reports that provide data about the devices within your network.

- **Rogue and aWIPS**: Reports that provide data about threats within your network.

- **SWIM**: Report listing all the devices in network with software and versioning.

- **Security Advisories**: Report that provides Cisco security advisory information on the network devices.

Note   The Access Point, Client, and Executive Summary reports support up to 90 days of data retention.

Step 2   After clicking a link, review the **Report Templates** window for that selected category.

Figure 38: Report Templates Window
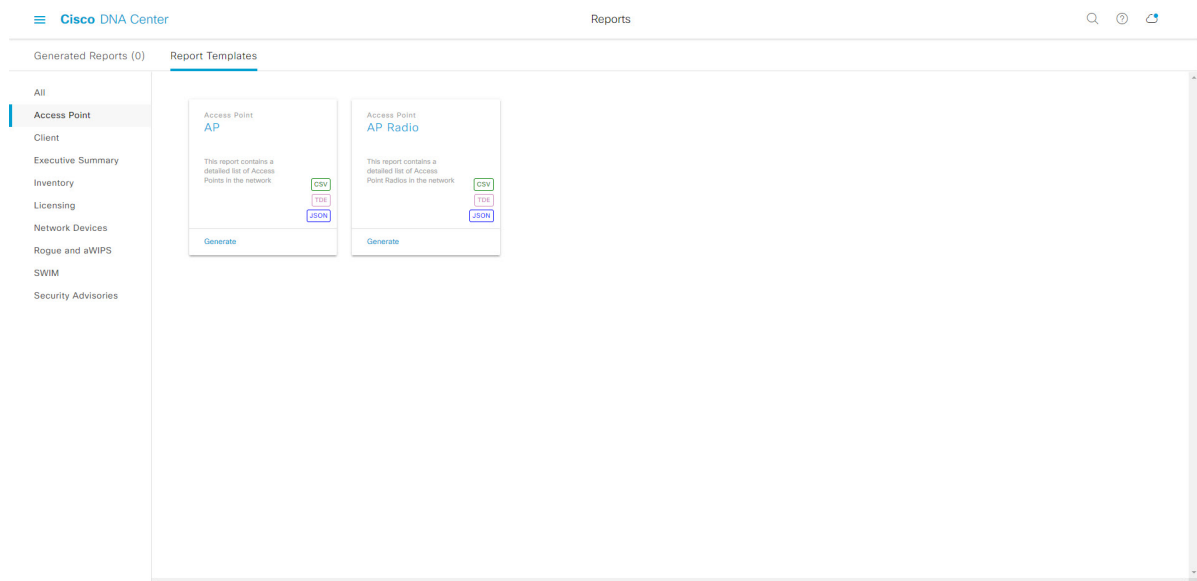
In the **Report Templates** window, each template is represented by a tile and contains information about the report and links to configure (generate) a report. Determine which template you want to use to generate a report. For an **Access Point** report, you can create an **AP**, **AP Radio**, or **AP Performance** report. For the **Access Point** report, supported file types are CSV, TDE, and JSON.

Step 3   In the tile, click the header to view a sample report.

A window appears for the sample report. Use the side bar in the window to scroll down and review the entire sample report.

Note   You can use the sample report to plan how you want your report to look.

**Step 4**   Click **X** to close the preview.

Step 5   In the tile, click the **Generate** link to configure parameters to build a report.

The **Generate** window opens where you can select a format type for the report, apply data filters for your reports, as well as set up schedules for the actual report generation.

Step 6   In the **Generate a New Report** window, click **Let's Do It** to get started.

To skip this screen in the future, check the **Don't show this to me again** check box.
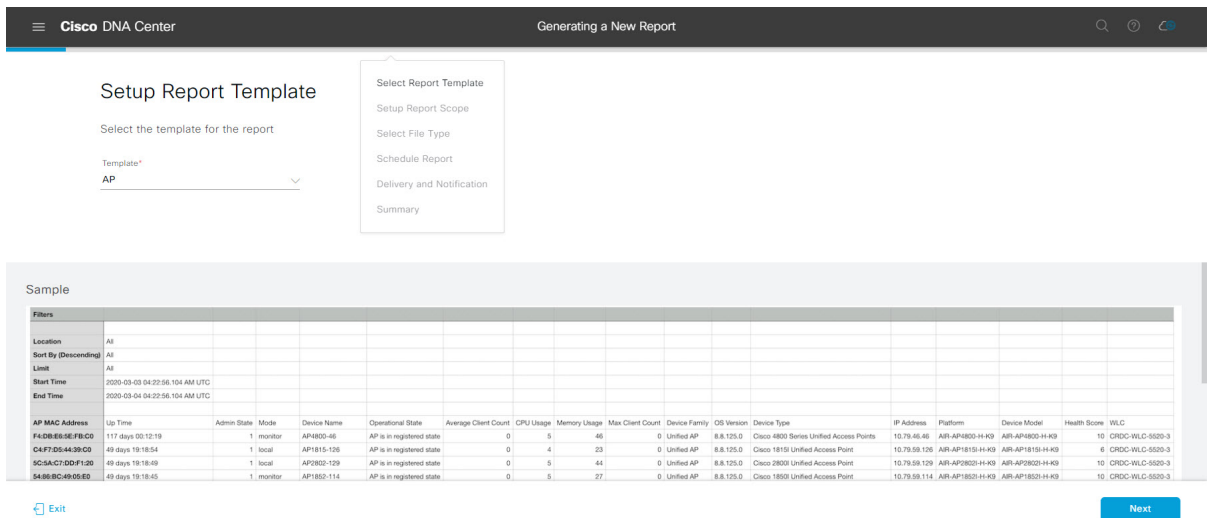
Figure 39: Generate a New Report
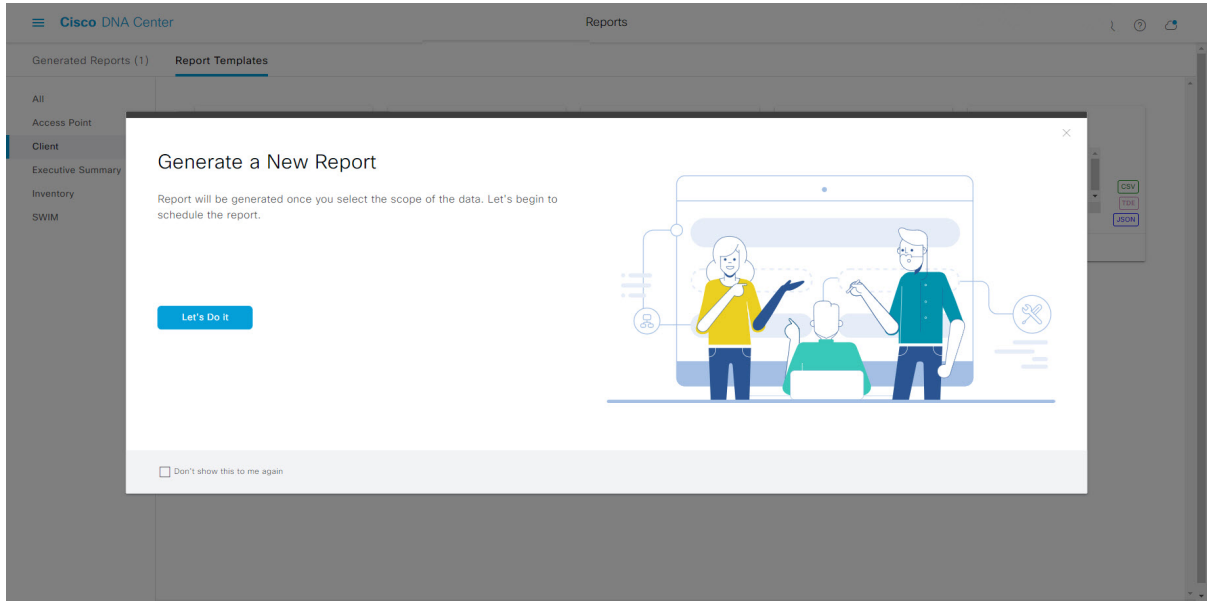
Step 7   In the **Select Report Template** window, choose the template from **Template** drop-down list.

Note   The **Template** consists of the individual report types within the categories for the release.

You can review an auto generated sample in the same window.

Figure 40: Setup Report Template

Step 8   Click **Next**.

The **Setup Report Scope** window appears.

Step 9   In the **Setup Report Scope** window, name the report and select the scope.

Enter a report name in the **Report Name** field and click in the **Scope** field to display the available filter. Click the filter options that you want for the report.

Note   The **Setup Report Scope** options change depending upon the selected **Template**.

Figure 41: Setup Report Scope

Step 10   Click **Next**.

Step 11   In the **Select File Type** window, select the file type for the report.

Depending upon the report that you are creating, the following **File Type** options may be available:

- **PDF**

- **CSV**

- **Tableau Data Extract**

- **JSON**

For the **CSV**, **JSON**, and **Tableau Data Extract** file types, a **Fields** option displays that permits you to select attributes (additional fields) for the CSV, JSON, and Tableau Data Extract results.

Figure 42: Select File Type

Step 12   Click **Next**.

Step 13   In the **Schedule Report** window, select the time range and schedule for the report.

The following **Time Range** options are available:

- **Last 3 hours**

- **Last 24 hours**

- **Last 7 days**

- **Custom**

  Note   Clicking **Custom** opens up fields where you can choose the date and time interval per the specific report type, as well as the time zone (GMT) for the time range.
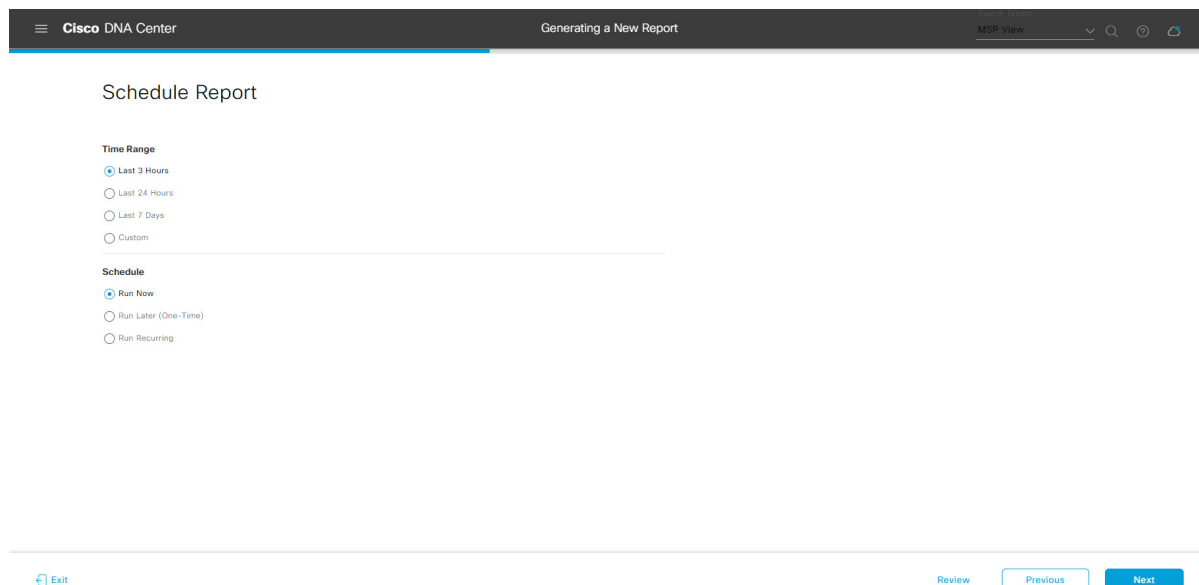
The following **Schedule** options are available to schedule the report:

- **Run Now**

- **Run Later (One-Time)**

- **Run Recurring**

Cisco DNA Center also allows you to choose a time zone for the report when configuring with the following **Schedule** options:

- **Custom**

- **Run Later (One Time)**

- **Run Recurring**

Figure 43: Schedule Report

Step 14   Click **Next**.

Step 15   In the **Delivery and Notification** window, select the delivery mechanism for the report.

The options include:

- **Email Report**: Email report is sent as a link or attachment.

Note	If you have not yet configured an SMTP server for the emails, you will be prompted to configure one. Follow the prompts to the **Email** tab in the GUI to configure a SMTP server. Click **System** > **Settings** > **External Services** > **Destinations** > **Email** tab.

  - **As a Link**: The email notification of a successfully compiled report has a link back to itself and the **Generated Reports** page under **Reports**. You can view and download the report from this link and location.

Note	Email notifications with embedded links to reports support up to 20 email addresses. To add multiple email addresses, you need to add each email address separately and press **Enter** (on your keyboard) after each addition. Cisco DNA Center platform validates the email addresses and notifies you if the syntax is incorrect.

  - **As an Attachment**: Report is attached to the email notification.

Note	PDF reports support email notification attachments of up to 20-MB in size and up to 10 email addresses. To add multiple email addresses, you need to add each email address separately and press **Enter** (on your keyboard) after each addition. Cisco DNA Center platform validates the email addresses and notifies you if the syntax is incorrect.

  Cisco DNA Center sends out the following email notifications for the report:

  - Report is in the queue waiting to be processed.

  - Report processing is in progress.

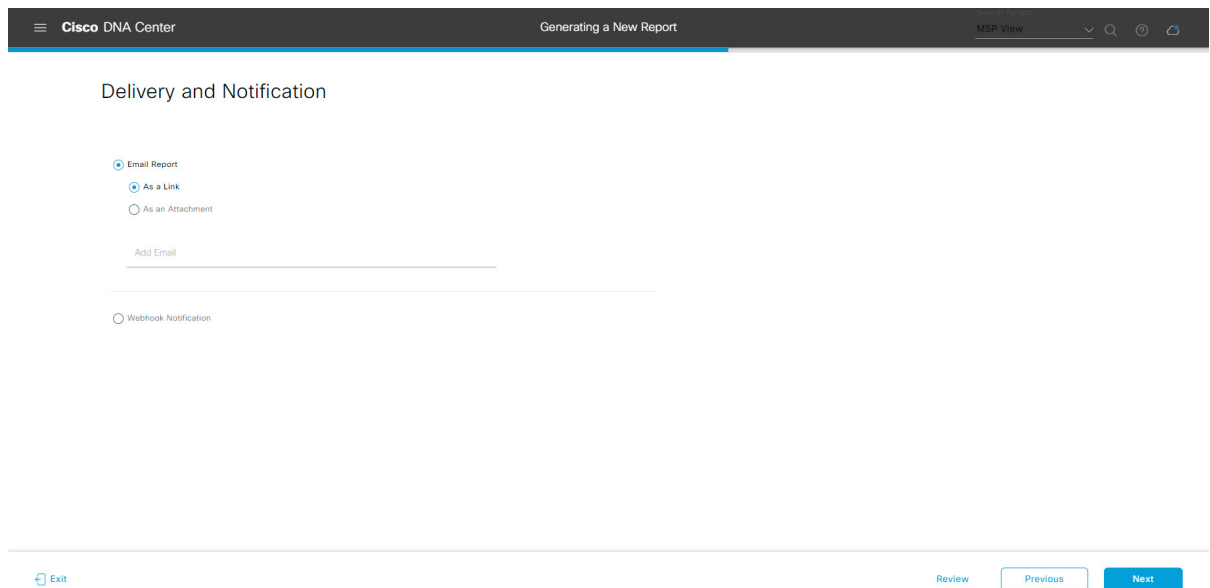 - Report has successfully been compiled and is completed.

- **Webhook Notification**: Notification is sent as a webhook to the configured webhook URL address (callback URL). Select a webhook from the drop-down list **(Subscription Profile** field).

Note	If you have not yet created a webhook, you will be prompted to create one. Follow the prompts to the **Webhook** tab in the GUI to configure a webhook. In general, to configure a webhook, click **System** > **Settings** > **External Services** > **Destinations** > **Webhook** tab.

  Cisco DNA Center sends you the following status webhook notifications for the report:
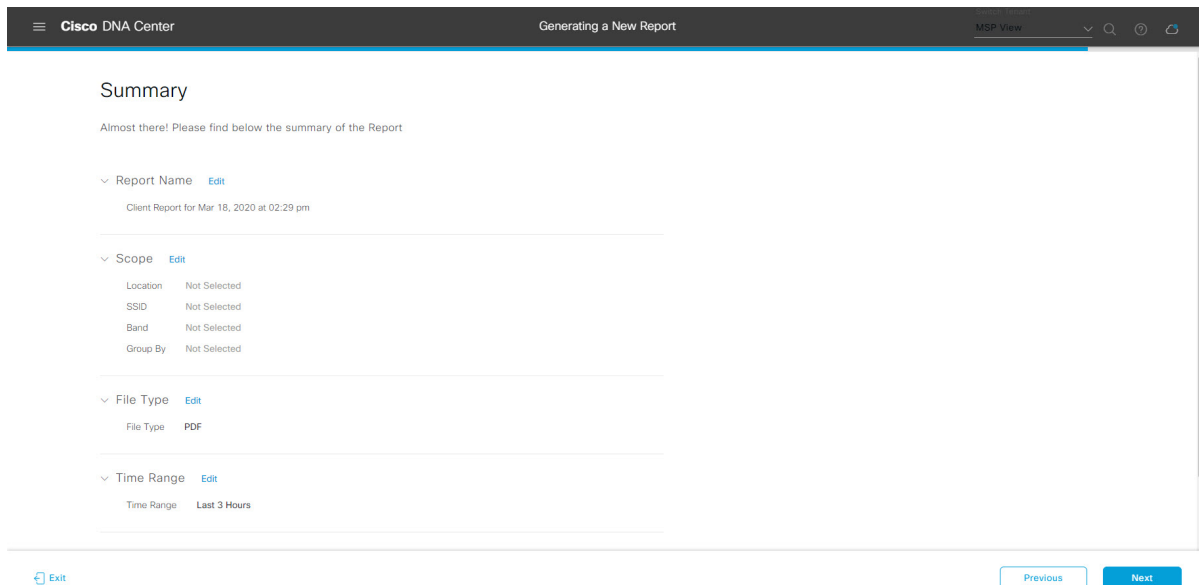
  - In Queue

  - In Progress

  - Success

Figure 44: Delivery and Notification

Step 16	Click **Next**.
Step 17	In the **Summary** window, review the configuration and if necessary edit any of the files.

Figure 45: Summary
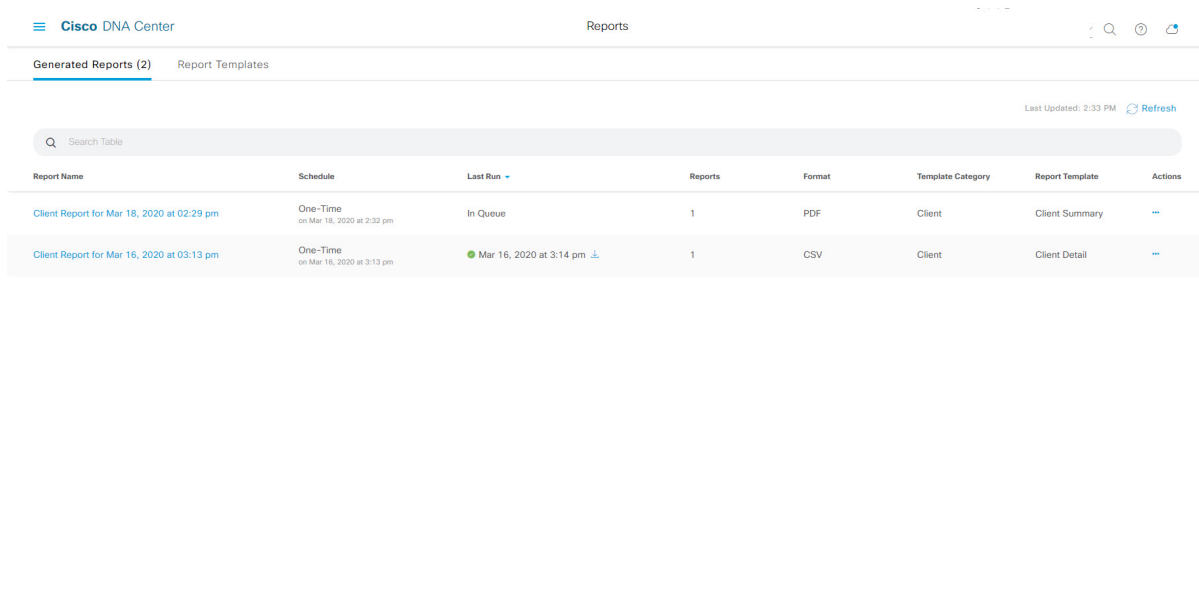

Click **Next**.

After the report is generated, a success window appears.

Step 18   Click the **View the Generated Reports** link.

The **Generated Reports** window opens with instance details of the report that was scheduled.

Figure 46: Generated Reports

What to do next

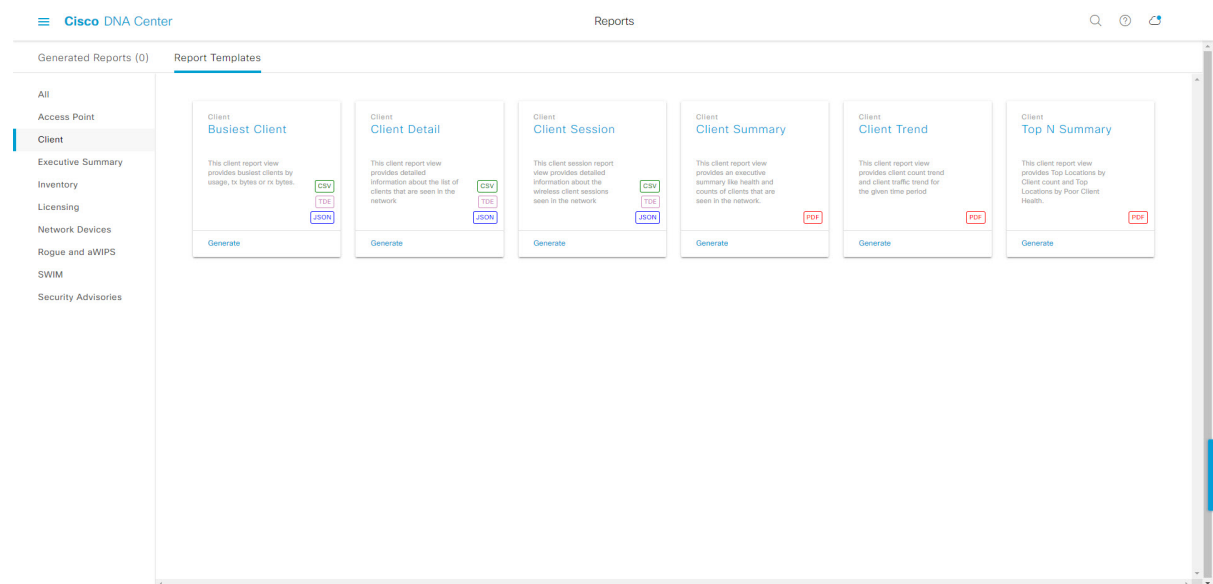Review your report instance in **Generated Reports** window.

✏️

Note You can download, review, edit, duplicate, or delete the report in the **Generated Reports** window. For additional information, see View Generated Reports, on page 133.

Run a Client Report

Perform this procedure to configure specialized **Client** reports for your network. You can configure **Client** reports using the **Reports** window in the Cisco DNA Center GUI.

Figure 47: Client Reports

Before you begin

Run a successful **Discovery** job in Cisco DNA Center. You can check whether a **Discovery** job is successful in **Device Inventory**. Click the menu icon (≡) and choose **Provision** > **Inventory** to view the results.

Step 1 Click the menu icon (≡) and choose **Reports** > **Report Templates**.

The **Report Templates** window opens and displays the supported reporting categories. A link represents each category. Click a link to view only the supported reports for that category.

For this release, reporting is supported for the following categories:

- **Access Point**: Reports that provide data about Access Points and Access Point Radios.

- **Client**: Reports that help with analyzing how the clients are performing in the network.

- **Executive Summary**: Report that helps with analyzing how devices, applications, and clients are performing in the network.

- **Inventory**: Report listing devices discovered by Cisco DNA Center.

- **Licensing**: Reports that lists devices that noncompliant devices and the reasons for noncompliance.

- **Network Devices**: Reports that provide data about the devices within your network.

- **Rogue and aWIPS**: Reports that provide data about threats within your network.

- **SWIM**: Report listing all the devices in network with software and versioning.

- **Security Advisories**: Report that provides Cisco security advisory information on the network devices.

Note   The Access Point, Client, and Executive Summary reports support up to 90 days of data retention.

Step 2   After clicking a link, review the **Report Templates** window for that selected category.

Figure 48: Reports Templates Window
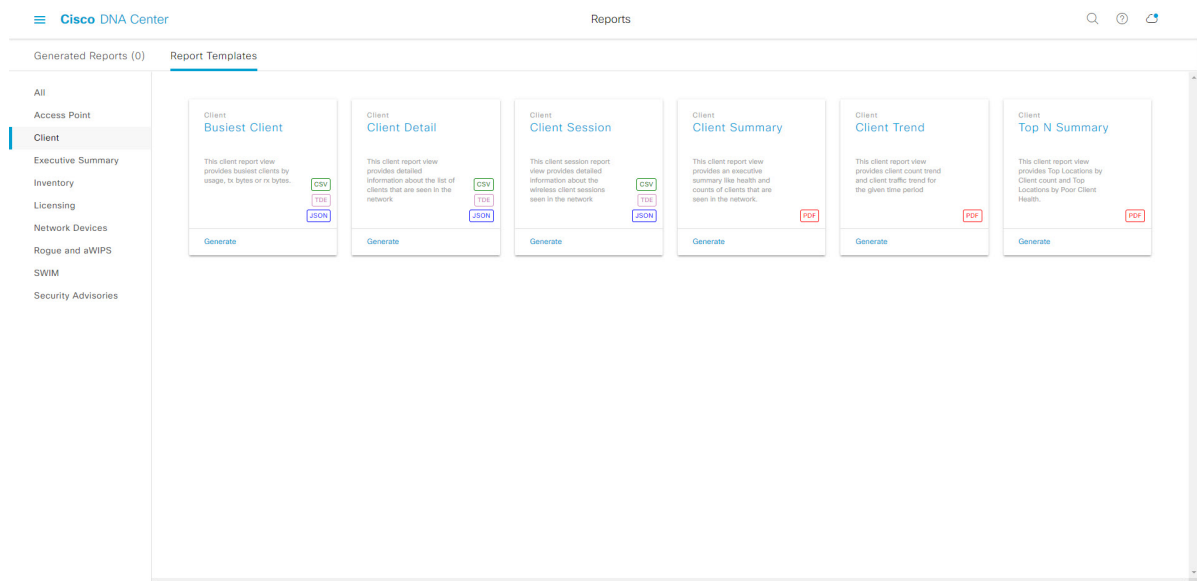
The **Report Templates** window displays supported report templates. Each template is represented by a tile and contains information about the report and links to configure (generate) a report. Determine which template you wish to use to generate a report. For example, for a **Client** report you can create a **Busiest Client**, **Client Summary**, **Client Detail** , **Top N Summary**, **Client Trend - Count and Traffic**, or **Client Session** report. Within each tile are also icons that represent the supported file types for the reports (PDF, CSV, TDE, or JSON).

Step 3   In the tile, click the header to view a sample report.

A window appears for the sample report. Use the side bar in the window to scroll down and review the entire sample report. For some of the client reports, the following data is presented:

- Applied filters (data filters that were used to build the report).

- Data metrics and summaries

- Graphical representation of the data (including line, bar, and pie graphs).

• Tables that assist you in analyzing the data.

**Note**   You can use the sample report to plan how you want your report to look.

Step 4   Click **X** to close the preview.

Step 5   In the tile, click the **Generate** link to configure parameters to build a report.

The **Generate** window opens where you can select a format type for the report, apply data filters for your reports, as well as set up schedules for the actual report generation.

Step 6   In the **Generate a New Report** window, click **Let's Do It** to get started.

Figure 49: Generate a New Report
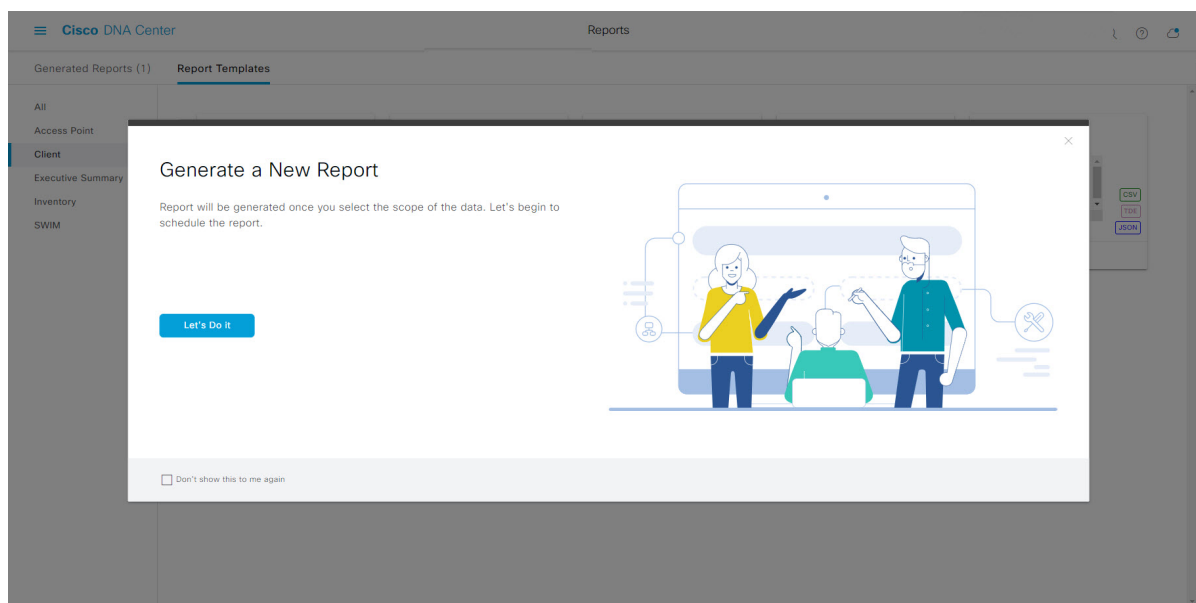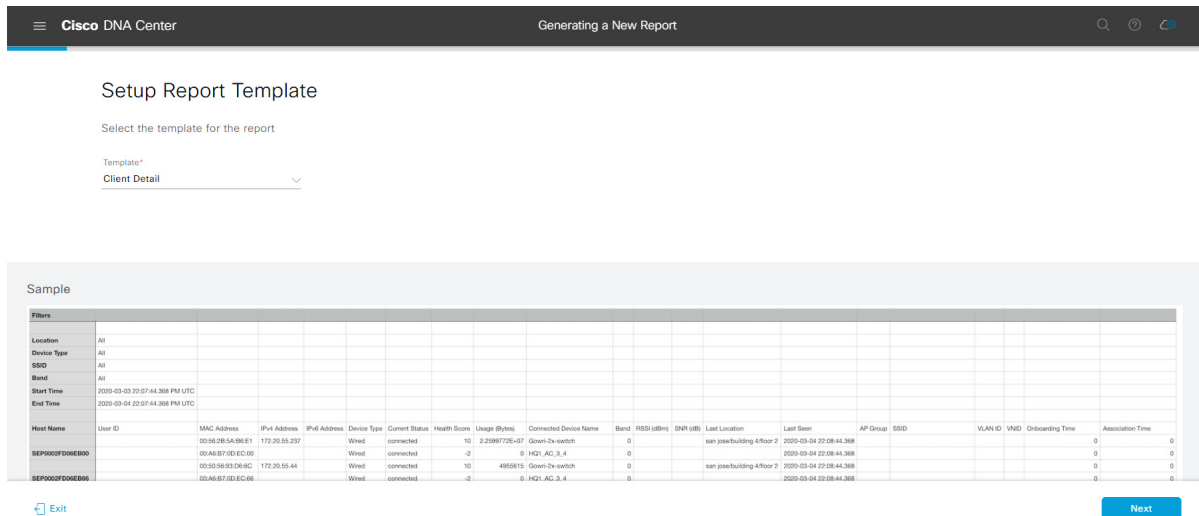

The **Select Report Template** window opens.

Step 7   In the **Select Report Template** window, select the template for the report.

Choose the **Template** from the drop-down lists.

Note   The **Template** consists of the individual report types within the categories for the release.

You can review an autogenerated sample in the same window.

Figure 50: Setup Report Template

Click **Next**. The **Setup Report Scope** window opens.
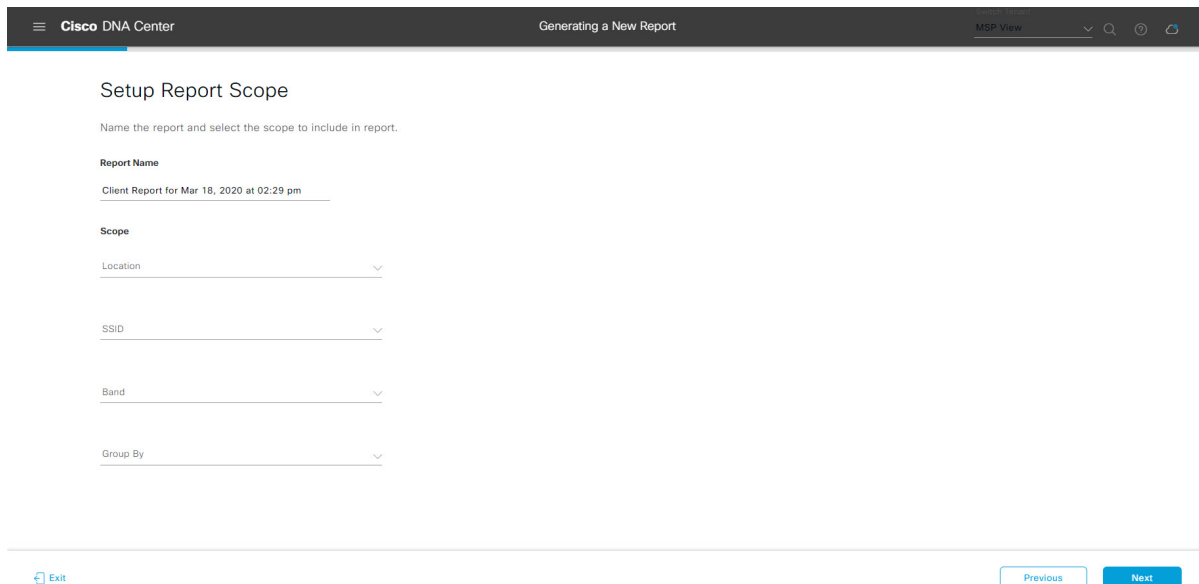
Step 8 In the **Setup Report Scope** window, name the report and select the scope.

Enter a report name in the **Report Name** field and click in the **Scope** field to display the available filter. Click the filter options that you want for the report.

Note The **Setup Report Scope** options change depending upon the selected **Template**.

Figure 51: Setup Report Scope

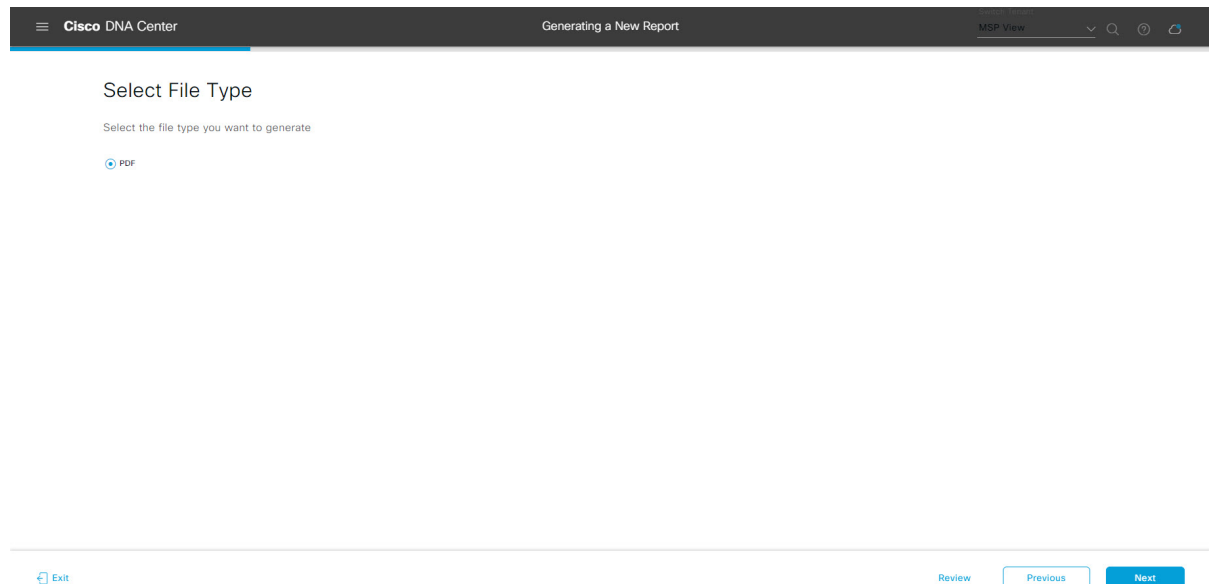Click **Next**. The **Select File Type** window opens.

Step 9 In the **Select File Type** window, select the file type for the report.

Depending upon the report that you are creating, the following **File Type** options may be available:

- **PDF**

- **CSV**

- **Tableau Data Extract**

- **JSON**

For the **CSV**, **JSON**, and **Tableau Data Extract** file types, a **Fields** option displays that permits you to select attributes (additional fields) for the CSV, JSON, and Tableau Data Extract results.

Figure 52: Select File Type

Click **Next**. The **Schedule Report** window opens.

Step 10   In the **Schedule Report** window, select the time range and schedule for the report.

The following **Time Range** options are available:

- **Last 3 hours**

- **Last 24 hours**

- **Last 7 days**

- **Custom**

  Note   Clicking **Custom** opens up fields where you can choose the date and time interval per the specific report type, as well as the time zone (GMT) for the time range.

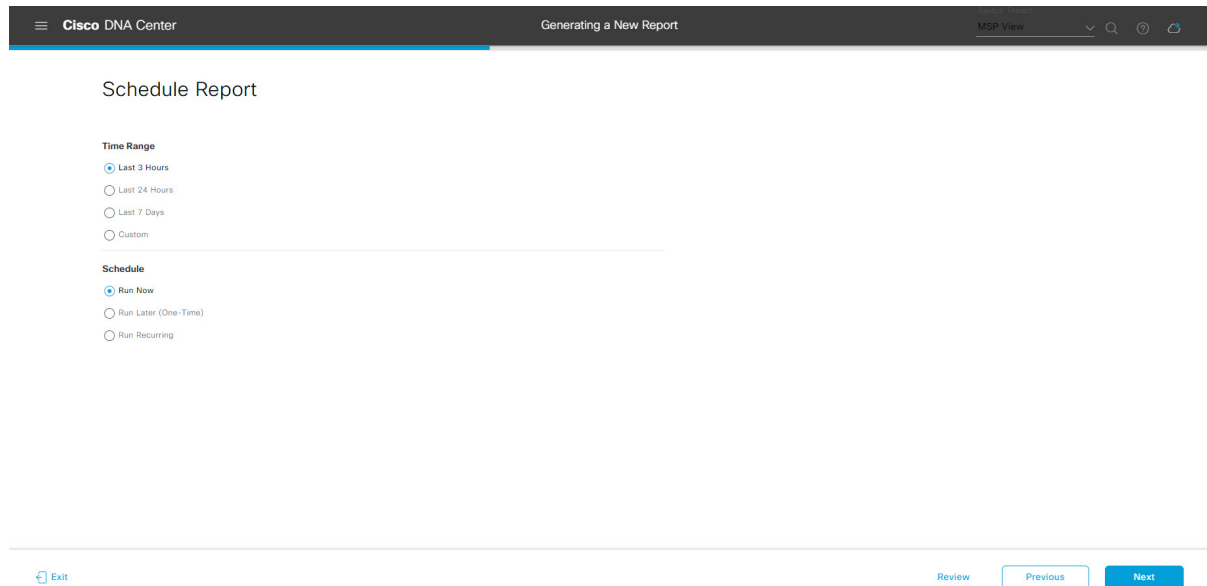The following **Schedule** options are available:

- **Run Now**

- **Run Later**

• **Run Recurring**

You can also select a time zone for the report when configuring with the following **Schedule** options:

• **Custom**

• **Run Later (One Time)**

• **Run Recurring**

Figure 53: Schedule Report

Click **Next**. The **Delivery and Notification** window opens.

Step 11 In the **Delivery and Notification** window, select the Delivery mechanism for the report.

The options include:

• **Email Report**: Email report is sent as a link or attachment.

> **Note** If you have not yet configured an SMTP server for the emails, you will be prompted to configure one. Follow the prompts to the **Email** tab in the GUI to configure a SMTP server. Click **System** > **Settings** > **External Services** > **Destinations** > **Email** tab.

• **Link**: The email notification of a successfully compiled report has a link back to itself and the **Generated Reports** page under **Reports**. You can view and download the report from this link and location.

> **Note** Email notifications with embedded links to reports support up to 20 email addresses. To add multiple email addresses, you need to add each email address separately and press **Enter** (on your keyboard) after each addition. Cisco DNA Center platform validates the email addresses and notifies you if the syntax is incorrect.

• **Attachment**: Report is attached to the email notification.

Note	PDF reports support email notification attachments of up to 20-MB in size and up to 10 email addresses. To add multiple email addresses, you need to add each email address separately and press **Enter** (on your keyboard) after each addition. Cisco DNA Center platform validates the email addresses and notifies you if the syntax is incorrect.

Cisco DNA Center sends the following email notifications for the report:

- Report is in the queue waiting to be processed.

- Report processing is in progress.

- Report has successfully been compiled and is completed.

- **Webhook Notification**: Notification is sent as a webhook to the configured webhook URL address (callback URL). Select a webhook from the drop-down list **(Subscription Profile** field).

Note	If you have not yet created a webhook, you will be prompted to create one. Follow the prompts to the **Webhook** tab in the GUI to configure a webhook. In general, to configure a webhook, click **System** > **Settings** > **External Services** > **Destinations** > **Webhook** tab.

You will receive status webhook notifications for the report. For example, you will receive "In Queue," "In Progress," and "Success" webhook notifications. You will also be able to view these notifications in the GUI.
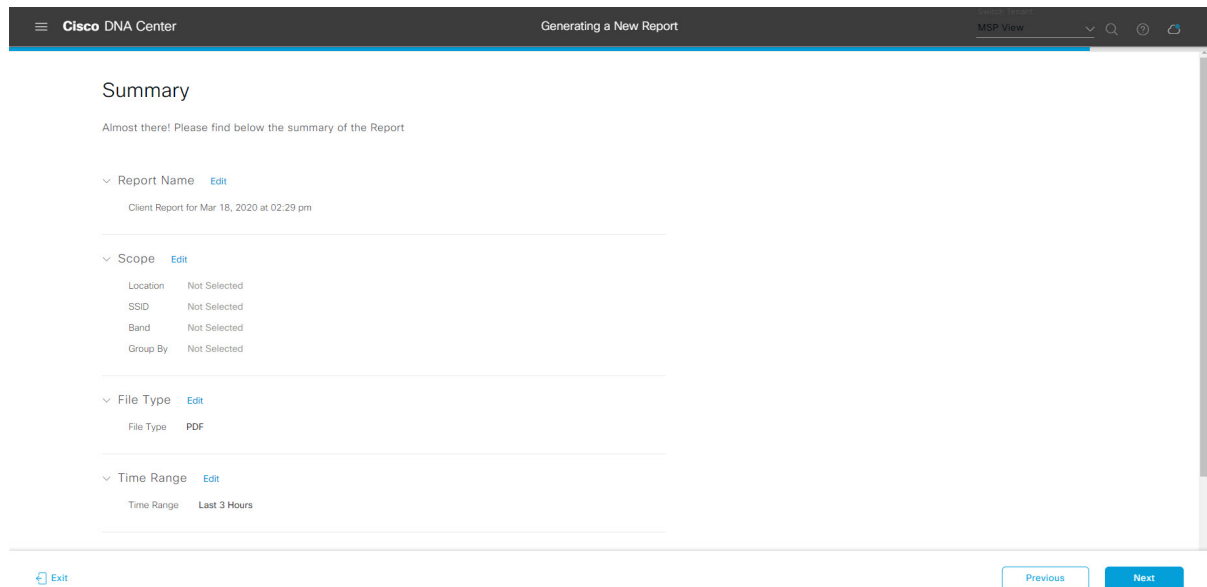
Figure 54: Delivery and Notification

Click **Next**. The **Summary** window opens.

Step 12 In the **Summary** window, review the configuration and if necessary edit any of the files.
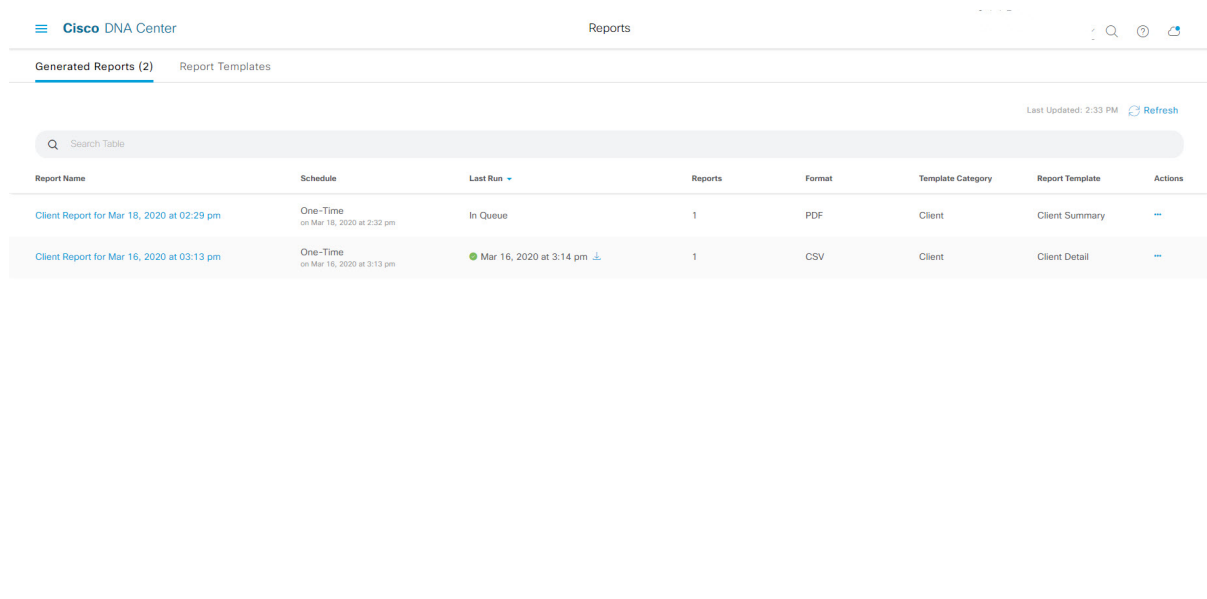
Figure 55: Summary

Click **Next**.

After the report is generated, a success window appears.

Step 13 Click the **View the Generated Reports** link.

The **Generated Reports** window opens with instance details of the report that was scheduled.

Figure 56: Generated Reports

What to do next
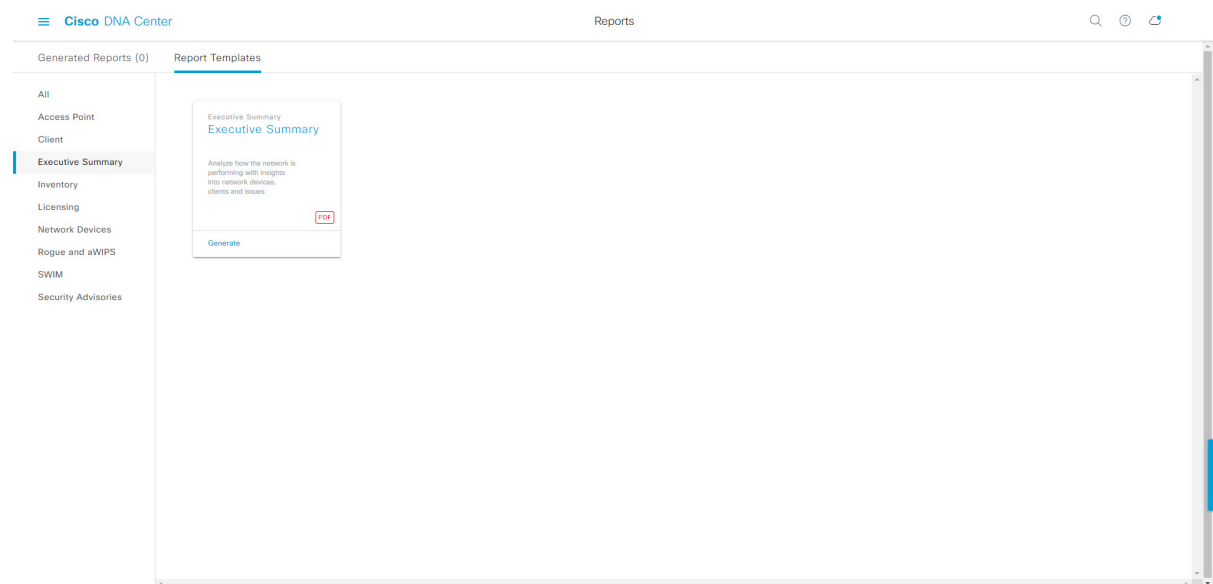
Review your report instance in **Generated Reports** window.

Note	You can download, review, edit, duplicate, or delete the report in the **Generated Reports** window. For additional information, see .

Run an Executive Summary Report

Perform this procedure to configure **Executive Summary** reports for your network. You can configure **Executive Summary** reports using the **Reports** window in the Cisco DNA Center GUI.

Figure 57: Executive Summary Reports

Before you begin

Run a successful **Discovery** job in Cisco DNA Center. You can check whether a **Discovery** job is successful in **Device Inventory**. Click the menu icon (☰) and choose **Provision** > **Inventory** to view the results.

Step 1 Click the menu icon (☰) and choose **Reports** > **Report Templates**.

The **Report Templates** window opens and displays the supported reporting categories. A link represents each category. Click a link to view only the supported reports for that category.

For this release, reporting is supported for the following categories:

  • **Access Point**: Reports that provide data about Access Points and Access Point Radios.

  • **Client**: Reports that help with analyzing how the clients are performing in the network.

- **Executive Summary**: Report that helps with analyzing how devices, applications, and clients are performing in the network.

- **Inventory**: Report listing devices discovered by Cisco DNA Center.

  If the individual counts for devices (wireless or wired clients, routers, switches, APs, and so on) exceed 200,000, the count is an estimated count.

- **Licensing**: Reports that lists devices that noncompliant devices and the reasons for noncompliance.

- **Network Devices**: Reports that provide data about the devices within your network.

- **Rogue and aWIPS**: Reports that provide data about threats within your network.

- **SWIM**: Report listing all the devices in network with software and versioning.

- **Security Advisories**: Report that provides Cisco security advisory information on the network devices.

Note The Access Point, Client, and Executive Summary reports support up to 90 days of data retention.

Step 2 After clicking a link, review the **Report Templates** window for that selected category.

Figure 58: Report Templates Window
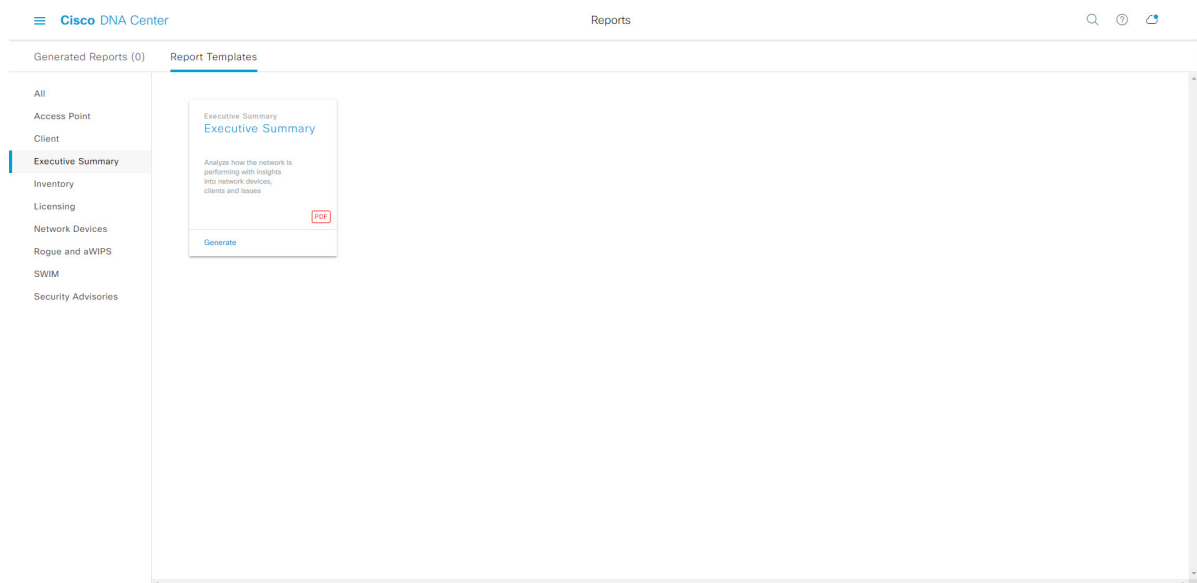
The **Report Templates** window displays supported report templates. Each template is represented by a tile and contains information about the report and links to configure (generate) a report. Determine which template you wish to use to generate a report. For example, for an **Executive Summary** report you can create an **Executive Summary** report. Within the tile are also icons that represent the supported file types for the reports (PDF).

Step 3 In the tile, click the header to view a sample report.

A window appears for the sample report. Use the side bar in the window to scroll down and review the entire sample report. The following data is presented:

- Data metrics and summaries

- Graphical representation of the data (including line, bar, and pie graphs).

• Tables that assist you in analyzing the data.

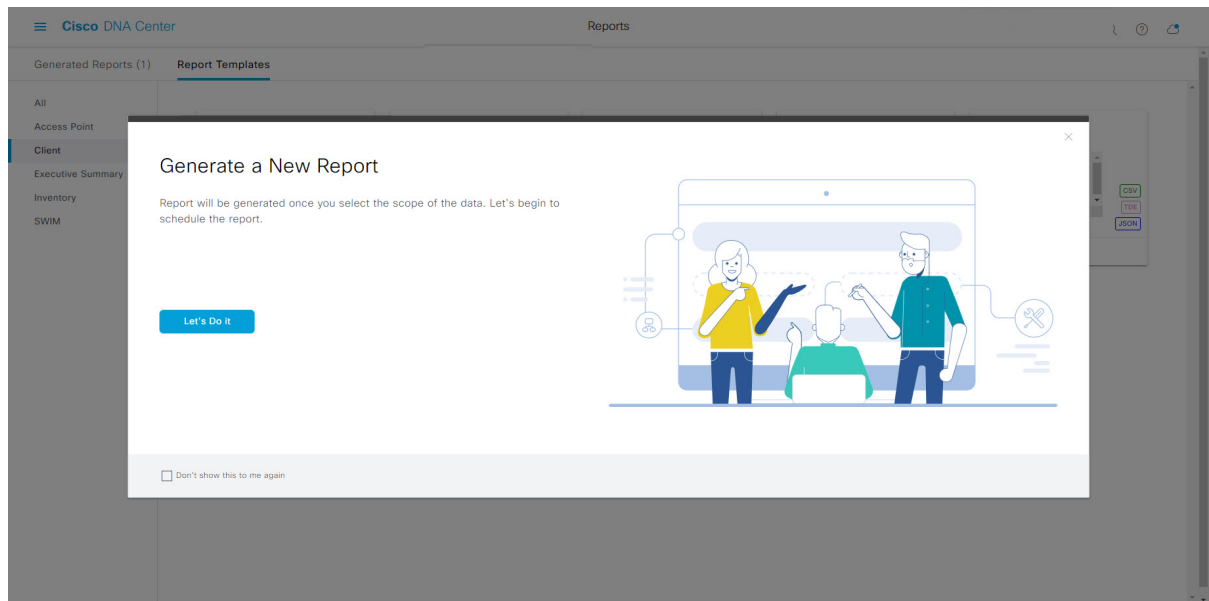**Note**　　　You can use the sample report to plan how you want your report to look.

Step 4　　Click **X** to close the preview.

Step 5　　In the tile, click the **Generate** link to configure parameters to build a report.

The **Generate** window opens where you can select a format type for the report, apply data filters for your reports, as well as set up schedules for the actual report generation.

Step 6　　In the **Generate a New Report** window, click **Let's Do It** to get started.

Figure 59: Generate a New Report

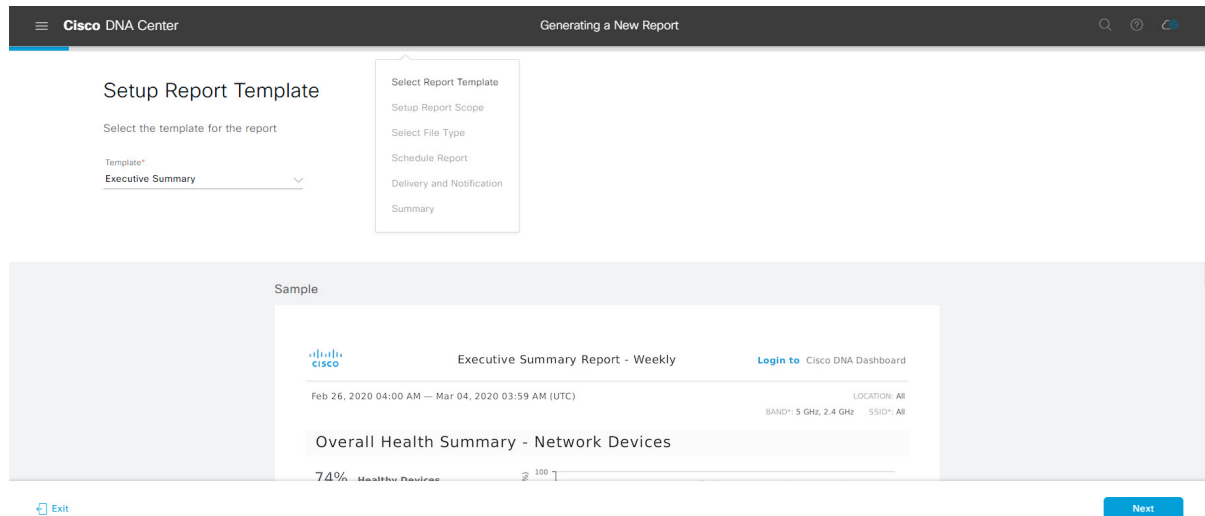The **Select Report Template** window opens.

Step 7　　In the **Select Report Template** window, select the template for the report.

Choose the **Template** from the drop-down lists.

Note　　　The **Template** consists of the individual report types within the categories for the release.

You can review an autogenerated sample in the same window.

Figure 60: Setup Report Template

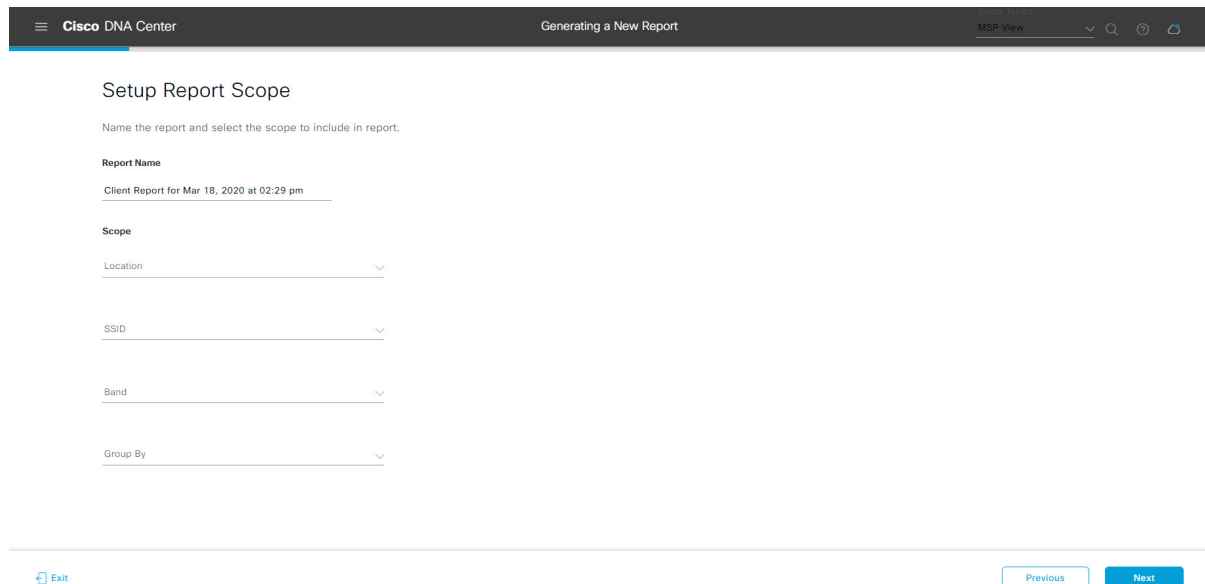Click **Next**. The **Setup Report Scope** window opens.

Step 8   In the **Setup Report Scope** window, name the report and select the scope.

Enter a report name in the **Report Name** field and click in the **Scope** field to display the available filter. Click the filter options that you want for the report.

Note   The **Setup Report Scope** options change depending upon the selected **Template**.

Figure 61: Setup Report Scope

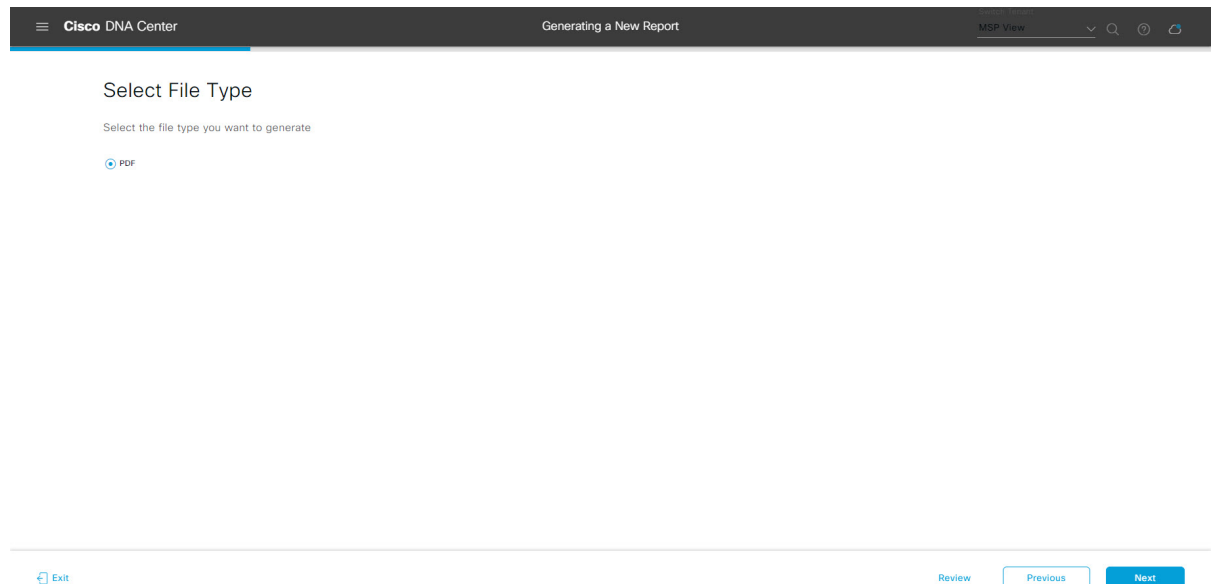Click **Next**. The **Select File Type** window opens.

Step 9   In the **Select File Type** window, select the file type for the report.

Depending on the report that you are creating, the following **File Type** options may be available:

- **PDF**

- **CSV**

- **Tableau Data Extract**

- **JSON**

For the **CSV**, **JSON**, and **Tableau Data Extract** file types, a **Fields** option displays that permits you to select attributes (additional fields) for the CSV, JSON, and Tableau Data Extract results.

Figure 62: Select File Type

Click **Next**. The **Schedule Report** window opens.

Step 10   In the **Schedule Report** window, select the time range and schedule for the report.

The following **Time Range** options are available:

- **Last 3 hours**

- **Last 24 hours**

- **Last 7 days**

- **Custom**

    Note   Clicking **Custom** opens up fields where you can choose the date and time interval per the specific report type, as well as the time zone (GMT) for the time range.

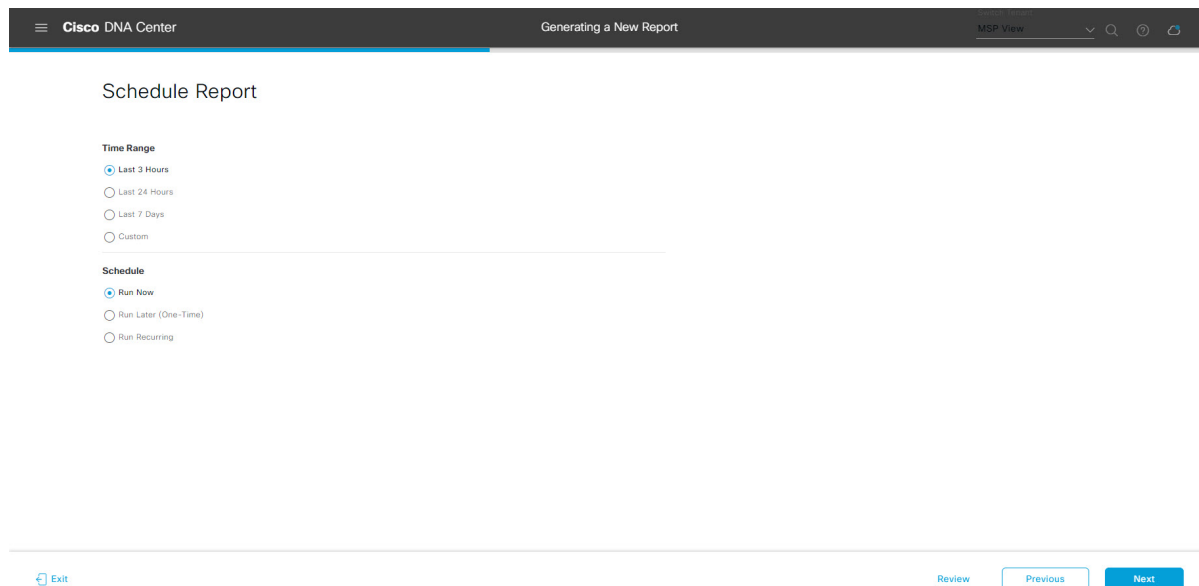The following **Schedule** options are available:

- **Run Now**

- **Run Later**

        • **Run Recurring**

You can also select a time zone for the report when configuring with the following **Schedule** options:

        • **Custom**

        • **Run Later (One Time)**

        • **Run Recurring**

Figure 63: Schedule Report

Click **Next**. The **Delivery and Notification** window opens.

Step 11   In the **Delivery and Notification** window, select the Delivery mechanism for the report.

The options include:

        • **Email Report**: Email report is sent as a link or attachment.

            Note   If you have not yet configured an SMTP server for the emails, you will be prompted to configure one. Follow the prompts to the **Email** tab in the GUI to configure a SMTP server. Click **System** > **Settings** > **External Services** > **Destinations** > **Email**.

          • **Link**: The email notification of a successfully compiled report has a link back to itself and the **Generated Reports** page under **Reports**. You can view and download the report from this link and location.

              Note   Email notifications with embedded links to reports support up to 20 email addresses. To add multiple email addresses, you need to add each email address separately and press **Enter** (on your keyboard) after each addition. Cisco DNA Center platform validates the email addresses and notifies you if the syntax is incorrect.

          • **Attachment**: Report is attached to the email notification.

Note	PDF reports support email notification attachments of up to 20-MB in size and up to 10 email addresses. To add multiple email addresses, you need to add each email address separately and press **Enter** (on your keyboard) after each addition. Cisco DNA Center platform validates the email addresses and notifies you if the syntax is incorrect.

Cisco DNA Center sends the following email notifications for the report:

- Report is in the queue waiting to be processed.

- Report processing is in progress.

- Report has successfully been compiled and is completed.

- **Webhook Notification**: Notification is sent as a webhook to the configured webhook URL address (callback URL). Select a webhook from the drop-down list **(Subscription Profile** field).

Note	If you have not yet created a webhook, you will be prompted to create one. Follow the prompts to the **Webhook** tab in the GUI to configure a webhook. In general, to configure a webhook, click **System** > **Settings** > **External Services** > **Destinations** > **Webhook** tab.

You will receive status webhook notifications for the report. For example, you will receive "In Queue," "In Progress," and "Success" webhook notifications. You will also be able to view these notifications in the GUI.
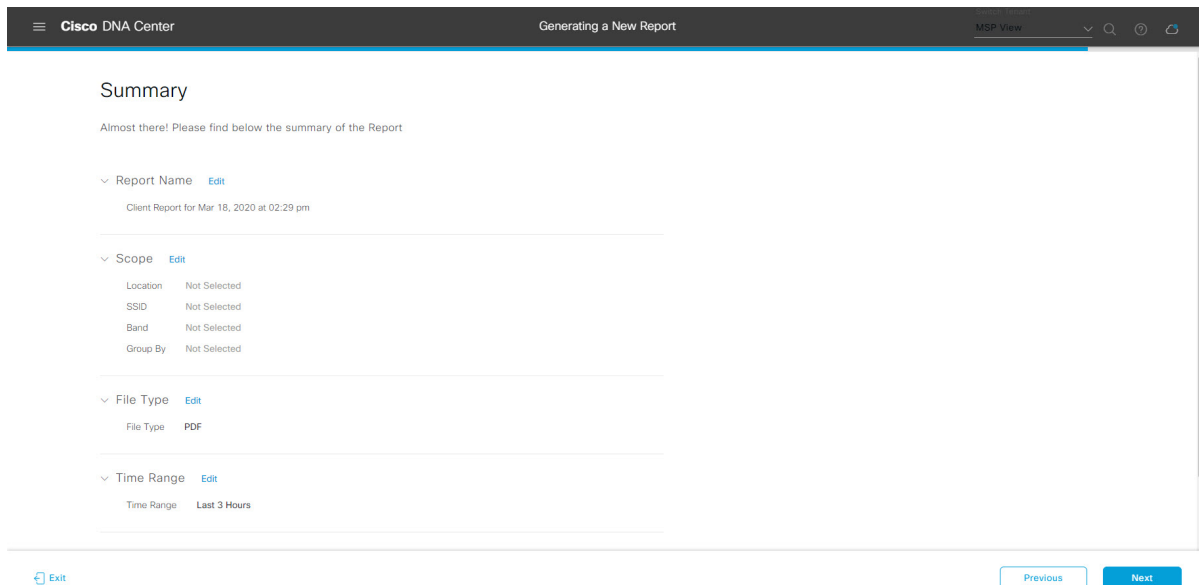
Figure 64: Delivery and Notification

Click **Next**. The **Summary** window opens.

Step 12 In the **Summary** window, review the configuration and if necessary edit any of the files.

Figure 65: Summary
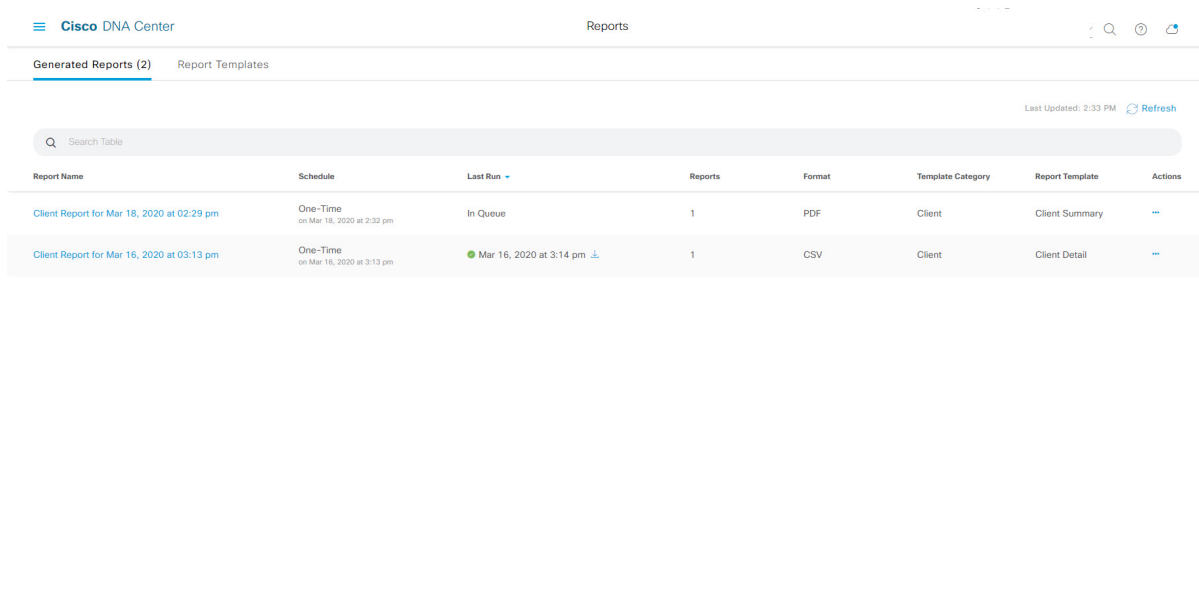

Click **Next**.

After the report is generated, a success window appears.

Step 13   Click the **View the Generated Reports** link.

The **Generated Reports** window opens with instance details of the report that was scheduled.

Figure 66: Generated Reports

What to do next

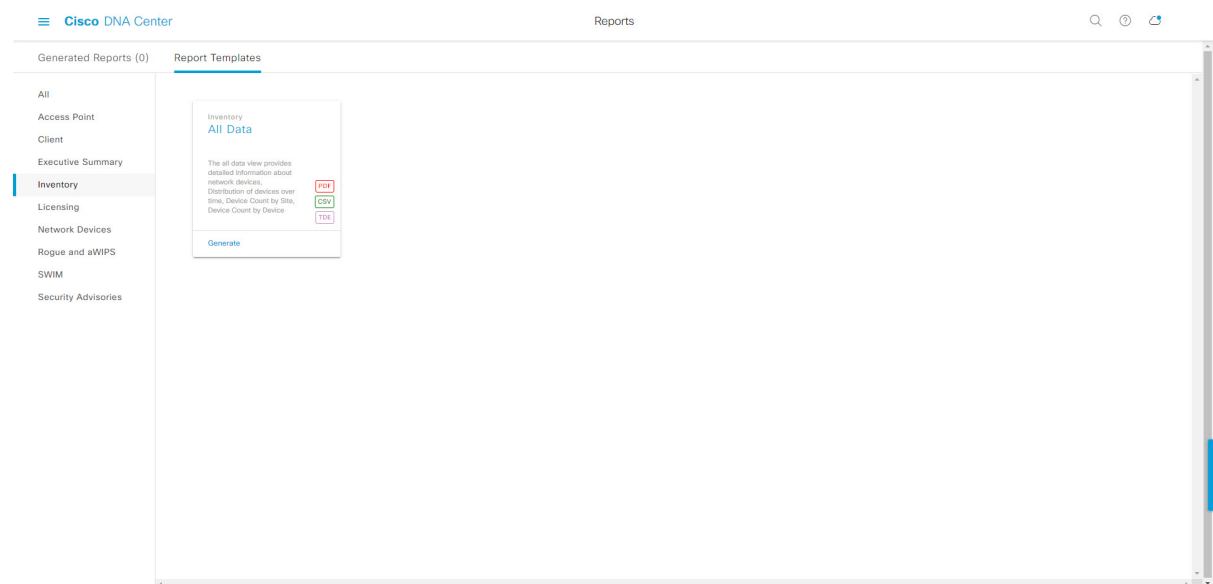Review your report instance in **Generated Reports** window.

> **Note** You can download, review, edit, duplicate, or delete the report in the **Generated Reports** window. For additional information, see View Generated Reports, on page 133.

Run an Inventory Report

Perform this procedure to configure **Inventory** reports for your network. You can configure **Inventory** reports using the **Reports** window in the Cisco DNA Center GUI.

Figure 67: Inventory Reports

Before you begin

Run a successful **Discovery** job in Cisco DNA Center. You can check whether a **Discovery** job is successful in **Device Inventory**. Click the menu icon (☰) and choose **Provision** > **Inventory** to view the results.

Step 1 Click the menu icon (☰) and choose **Reports** > **Report Templates**.

The **Report Templates** window opens and displays the supported reporting categories. A link represents each category. Click a link to view only the supported reports for that category.

For this release, reporting is supported for the following categories:

- **Access Point**: Reports that provide data about Access Points and Access Point Radios.

- **Client**: Reports that help with analyzing how the clients are performing in the network.

- **Executive Summary**: Report that helps with analyzing how devices, applications, and clients are performing in the network.

- **Inventory**: Report listing devices discovered by Cisco DNA Center.

- **Licensing**: Reports that lists devices that noncompliant devices and the reasons for noncompliance.

- **Network Devices**: Reports that provide data about the devices within your network.

- **Rogue and aWIPS**: Reports that provide data about threats within your network.

- **SWIM**: Report listing all the devices in network with software and versioning.

- **Security Advisories**: Report that provides Cisco security advisory information on the network devices.

Note   The Access Point, Client, and Executive Summary reports support up to 90 days of data retention.

Step 2   After clicking a link, review the **Report Templates** window for that selected category.

Figure 68: Report Templates Window
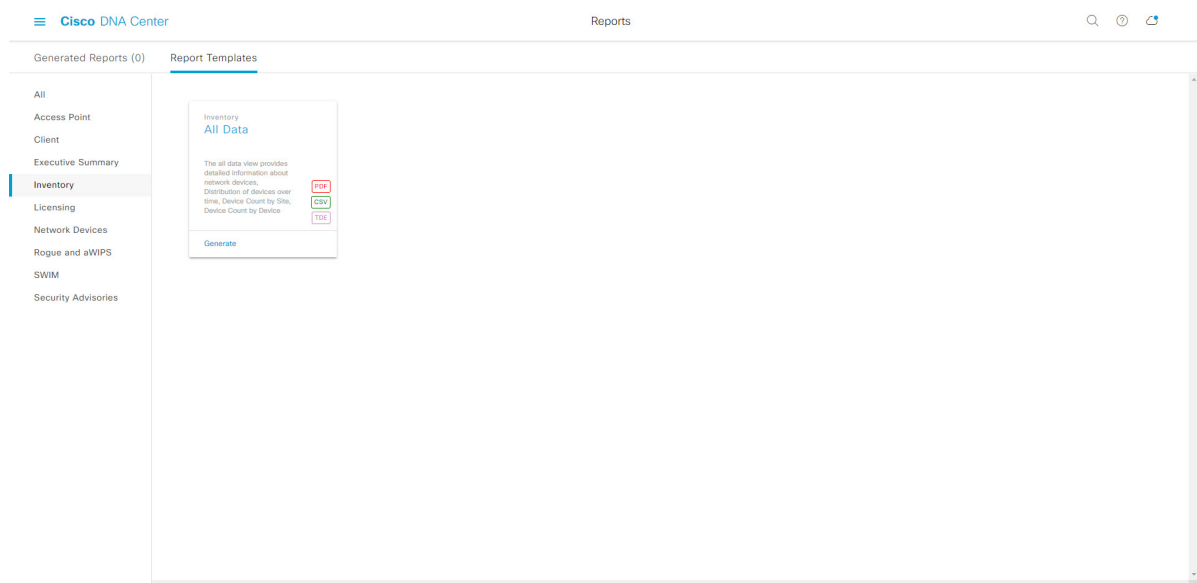
The **Report Templates** window displays supported report templates. Each template is represented by a tile and contains information about the report and links to configure (generate) a report. Determine which template you wish to use to generate a report. For example, for an **Inventory** report you can create an **All Data** report. Within the tile are also icons that represent the supported file types for the reports (PDF, CSV, or TDE).

Step 3   In the tile, click the header to view a sample report.

A window appears for the sample report. Use the side bar in the window to scroll down and review the entire sample report. The following data is presented:

- Applied filters (data filters that were used to build the report).

- Data metrics and summaries

- Graphical representation of the data (including line, bar, and pie graphs).

• Tables that assist you in analyzing the data.

**Note**   You can use the sample report to plan how you want your report to look.

Step 4   Click **X** to close the preview.

Step 5   In the tile, click the **Generate** link to configure parameters to build a report.

The **Generate** window opens where you can select a format type for the report, apply data filters for your reports, as well as set up schedules for the actual report generation.

Step 6   In the **Generate a New Report** window, click **Let's Do It** to get started.

Figure 69: Generate a New Report
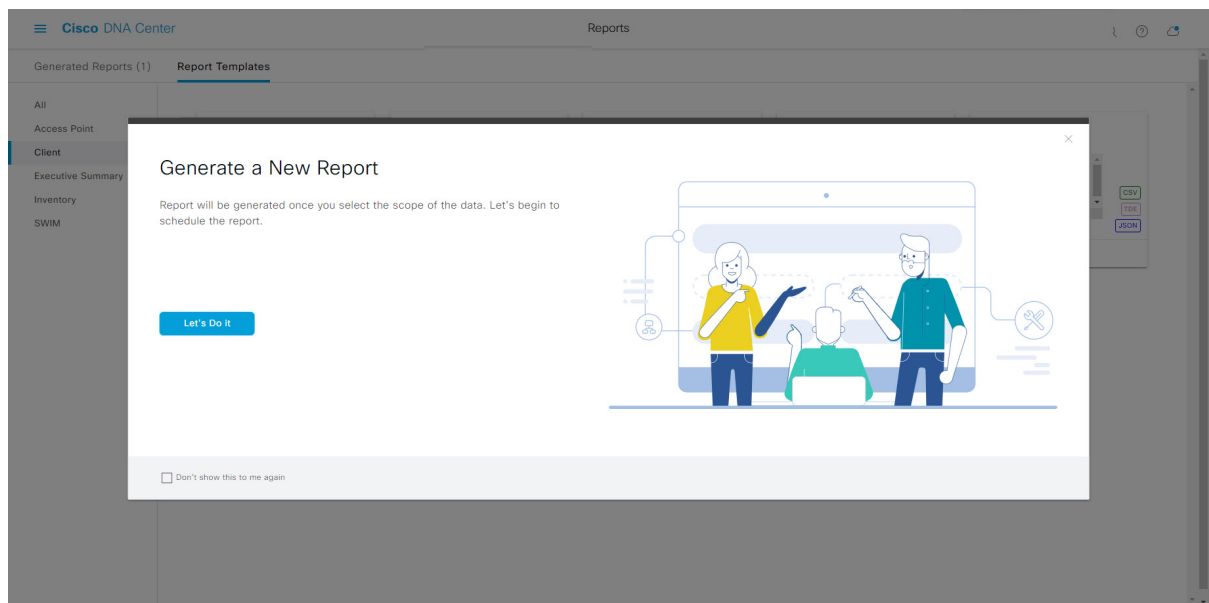
The **Select Report Template** window opens.

Step 7   In the **Select Report Template** window, select the template for the report.

Choose the **Template** from the drop-down lists.

Note   The **Template** consists of the individual report types within the categories for the release.

You can review an autogenerated sample in the same window.

Figure 70: Setup Report Template

Click **Next**. The **Setup Report Scope** window opens.

Step 8   In the **Setup Report Scope** window, name the report and select the scope.

Enter a report name in the **Report Name** field and click in the **Scope** field to display the available filter. Click the filter options that you want for the report.

Note   The **Setup Report Scope** options change depending upon the selected **Template**.

Figure 71: Setup Report Scope

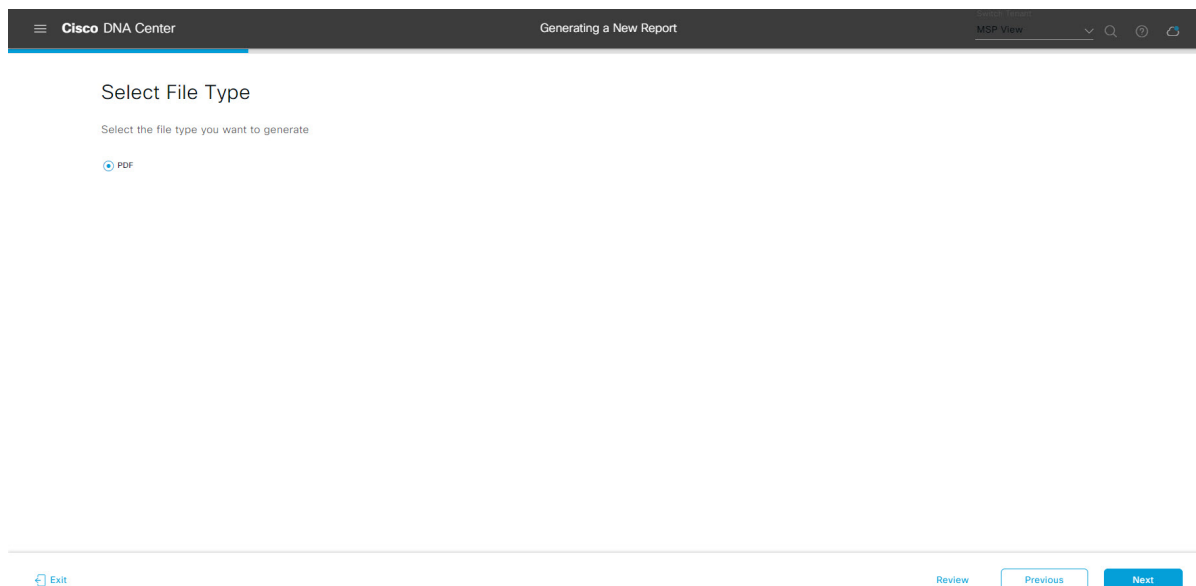Click **Next**. The **Select File Type** window opens.

Step 9   In the **Select File Type** window, select the file type for the report.

Depending on the report that you are creating, the following **File Type** options may be available:

- **PDF**

- **CSV**

- **Tableau Data Extract**

- **JSON**

For the **CSV**, **JSON**, and **Tableau Data Extract** file types, a **Fields** option displays that permits you to select attributes (additional fields) for the CSV, JSON, and Tableau Data Extract results.

Figure 72: Select File Type

Click **Next**. The **Schedule Report** window opens.

Step 10 In the **Schedule Report** window, select the time range and schedule for the report.

The following **Time Range** options are available:

- **Last 3 hours**

- **Last 24 hours**

- **Last 7 days**

- **Custom**

  Note Clicking **Custom** opens up fields where you can choose the date and time interval per the specific report type, as well as the time zone (GMT) for the time range.

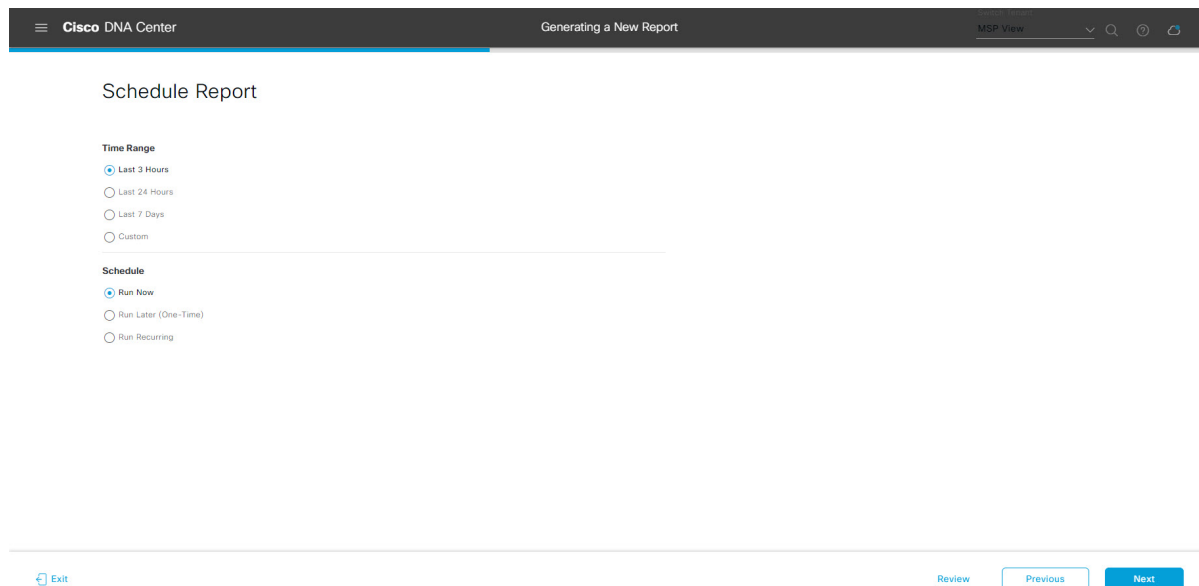The following **Schedule** options are available:

- **Run Now**

- **Run Later**

- **Run Recurring**

You can also select a time zone for the report when configuring with the following **Schedule** options:

- **Custom**

- **Run Later (One Time)**

- **Run Recurring**

Figure 73: Schedule Report

Click **Next**. The **Delivery and Notification** window opens.

Step 11   In the **Delivery and Notification** window, select the Delivery mechanism for the report.

The options include:

- **Email Report**: Email report is sent as a link or attachment.

Note	If you have not yet configured an SMTP server for the emails, you will be prompted to configure one. Follow the prompts to the **Email** tab in the GUI to configure a SMTP server. Click **System** > **Settings** > **External Services** > **Destinations** > **Email**.

- **Link**: The email notification of a successfully compiled report has a link back to itself and the **Generated Reports** page under **Reports**. You can view and download the report from this link and location.

Note	Email notifications with embedded links to reports support up to 20 email addresses. To add multiple email addresses, you need to add each email address separately and press **Enter** (on your keyboard) after each addition. Cisco DNA Center platform validates the email addresses and notifies you if the syntax is incorrect.

- **Attachment**: Report is attached to the email notification.

Note   PDF reports support email notification attachments of up to 20-MB in size and up to 10 email addresses. To add multiple email addresses, you need to add each email address separately and press **Enter** (on your keyboard) after each addition. Cisco DNA Center platform validates the email addresses and notifies you if the syntax is incorrect.

Cisco DNA Center sends the following email notifications for the report:

- Report is in the queue waiting to be processed.

- Report processing is in progress.

- Report has successfully been compiled and is completed.

- **Webhook Notification**: Notification is sent as a webhook to the configured webhook URL address (callback URL). Select a webhook from the drop-down list **(Subscription Profile** field).

Note   If you have not yet created a webhook, you will be prompted to create one. Follow the prompts to the **Webhook** tab in the GUI to configure a webhook. In general, to configure a webhook, click **System** > **Settings** > **External Services** > **Destinations** > **Webhook** tab.

You will receive status webhook notifications for the report. For example, you will receive "In Queue," "In Progress," and "Success" webhook notifications. You will also be able to view these notifications in the GUI.
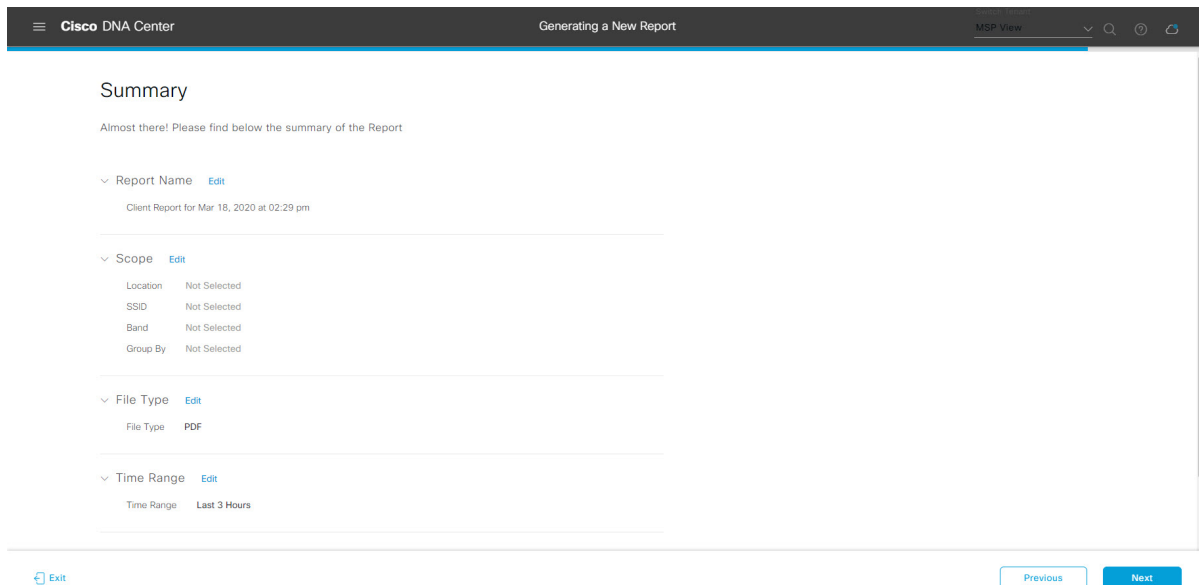
Figure 74: Delivery and Notification

Click **Next**. The **Summary** window opens.

Step 12   In the **Summary** window, review the configuration and if necessary edit any of the files.

Run an Inventory Report

Figure 75: Summary
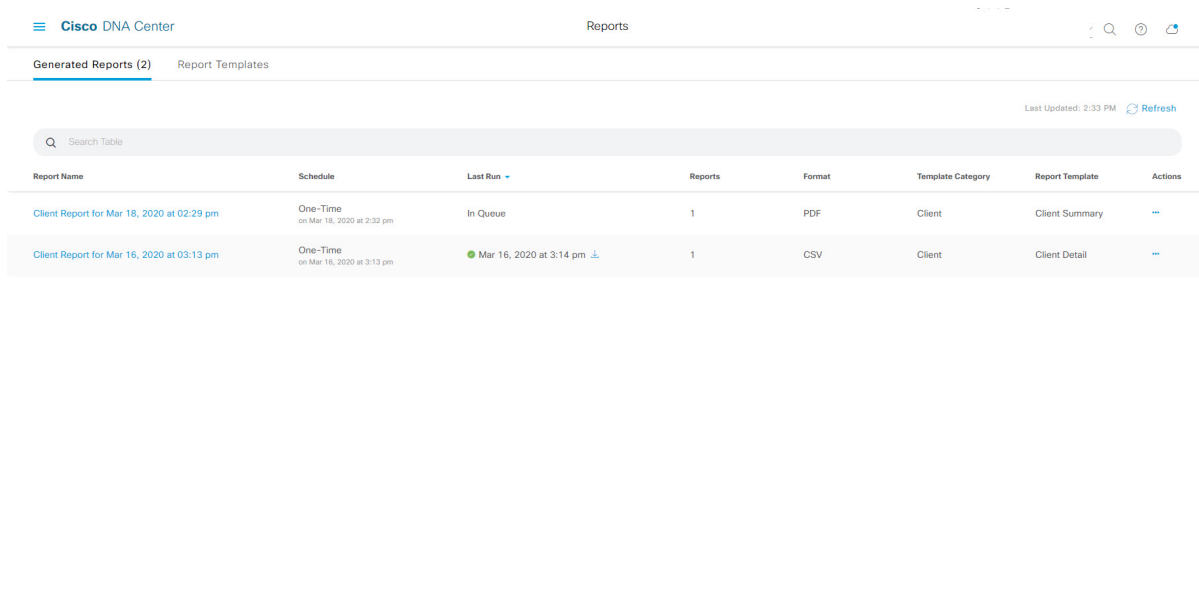

Click **Next**.

After the report is generated, a success window appears.

Step 13   Click the **View the Generated Reports** link.

The **Generated Reports** window opens with instance details of the report that was scheduled.

Figure 76: Generated Reports

What to do next

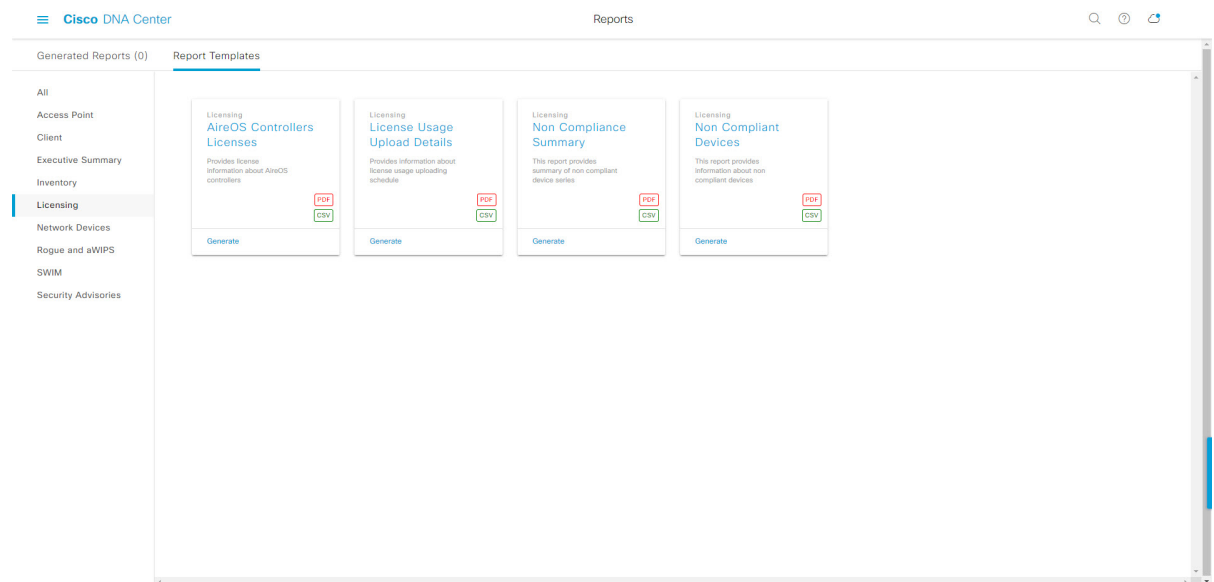Review your report instance in **Generated Reports** window.

Note You can download, review, edit, duplicate, or delete the report in the **Generated Reports** window. For additional information, see View Generated Reports, on page 133.

Run a Licensing Report

Perform this procedure to configure **Licensing** reports about your network. You can configure **Licensing** reports using the **Reports** window in the Cisco DNA Center GUI.

Figure 77: Licensing Reports

Before you begin

Run a successful **Discovery** job in Cisco DNA Center. You can check whether a **Discovery** job is successful in **Device Inventory**. Click the menu icon (≡) and choose **Provision** > **Inventory** to view the results.

Step 1 Click the menu icon (≡) and choose **Reports** > **Report Templates**.

The **Report Templates** window opens and displays the supported reporting categories. A link represents each category. Click a link to view only the supported reports for that category.

For this release, reporting is supported for the following categories:

- **Access Point**: Reports that provide data about Access Points and Access Point Radios.

- **Client**: Reports that help with analyzing how the clients are performing in the network.

- **Executive Summary**: Report that helps with analyzing how devices, applications, and clients are performing in the network.

- **Inventory**: Report listing devices discovered by Cisco DNA Center.

- **Licensing**: Reports that lists devices that noncompliant devices and the reasons for noncompliance.

- **Network Devices**: Reports that provide data about the devices within your network.

- **Rogue and aWIPS**: Reports that provide data about threats within your network.

- **SWIM**: Report listing all the devices in the network, along with their software and versioning.

- **Security Advisories**: Report that provides Cisco security advisory information on the network devices.

Note   The Access Point, Client, and Executive Summary reports support up to 90 days of data retention.

Step 2   After clicking a link, review the **Report Templates** window for that selected category.

Figure 78: Report Templates Window
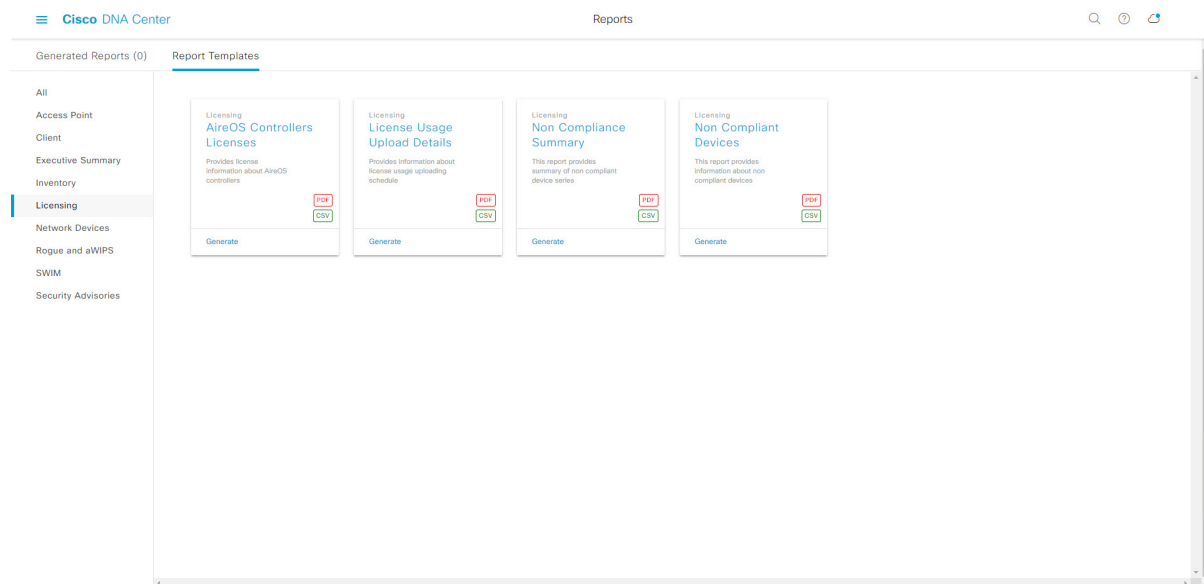
The **Report Templates** window displays supported report templates. Each template is represented by a tile and contains information about the report and links to configure (generate) a report. Determine which template you wish to use to generate a report. For example, for a **Licensing** report you can create an **AireOS Controllers Licenses** report. Within the tile are also icons that represent the supported file types for the reports (PDF or CSV).

Step 3   In the tile, click the header to view a sample report.

A window appears for the sample report. Use the side bar in the window to scroll down and review the entire sample report. The following data is presented:

- Applied filters (data filters that were used to build the report).

- Data metrics and summaries

- Tables that assist you in analyzing the data.

**Note** You can use the sample report to plan how you want your report to look.

Step 4 Click **X** to close the preview.

Step 5 In the tile, click the **Generate** link to configure parameters to build a report.

The **Generate** window opens where you can select a format type for the report, apply data filters for your reports, as well as set up schedules for the actual report generation.

Step 6 In the **Generate a New Report** window, click **Let's Do It** to get started.

Figure 79: Generate a New Report
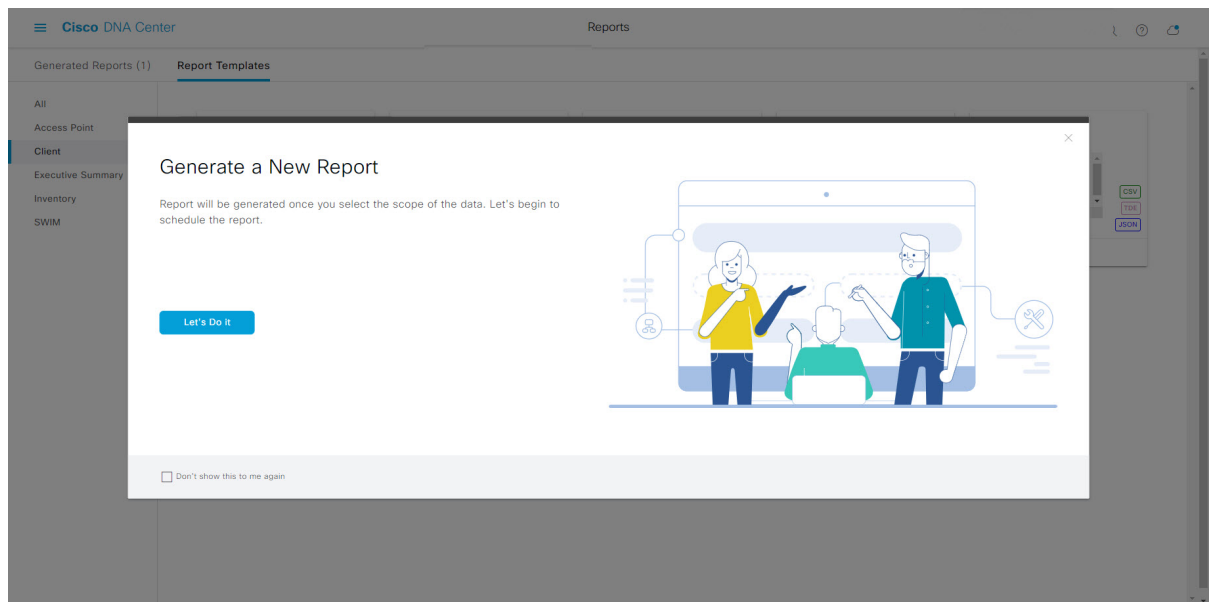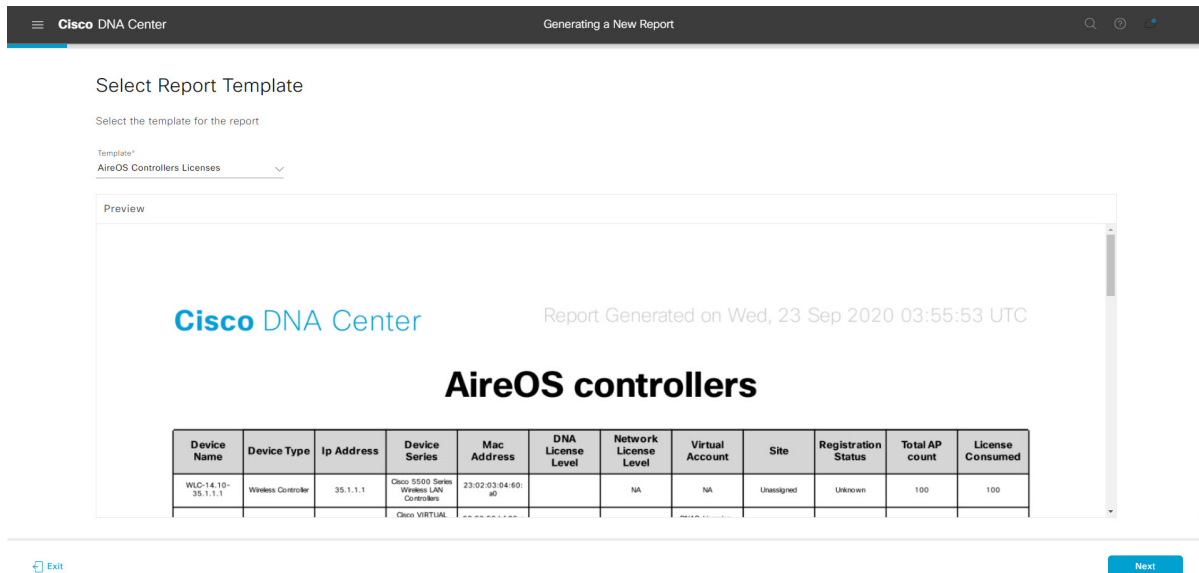

The **Select Report Template** window opens.

Step 7 In the **Select Report Template** window, select the template for the report.

Choose the **Template** from the drop-down lists.

Note The **Template** consists of the individual report types within the categories for the release.

You can review an autogenerated sample in the same window.

Figure 80: Select Report Template

Click **Next**. The **Setup Report Scope** window opens.
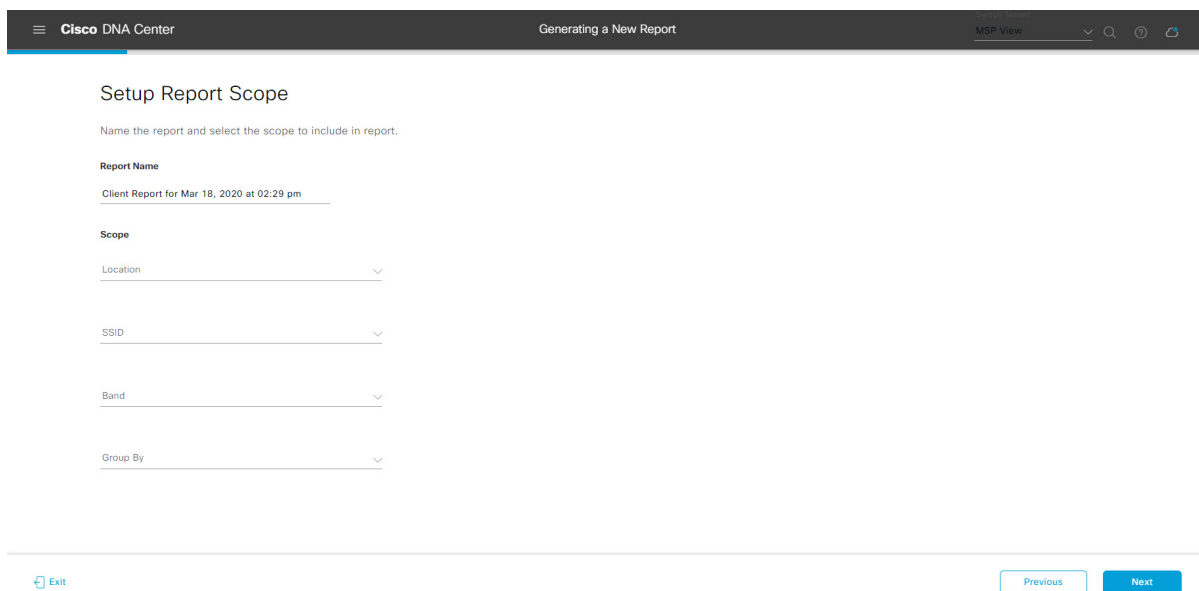
Step 8 In the **Setup Report Scope** window, name the report and select the scope.

In the **Report Name** field, enter a report name and click inside the **Scope** field to display the available filter. Click the filter options that you want for the report.

Note The **Setup Report Scope** options change depending upon the selected **Template**.

Figure 81: Setup Report Scope

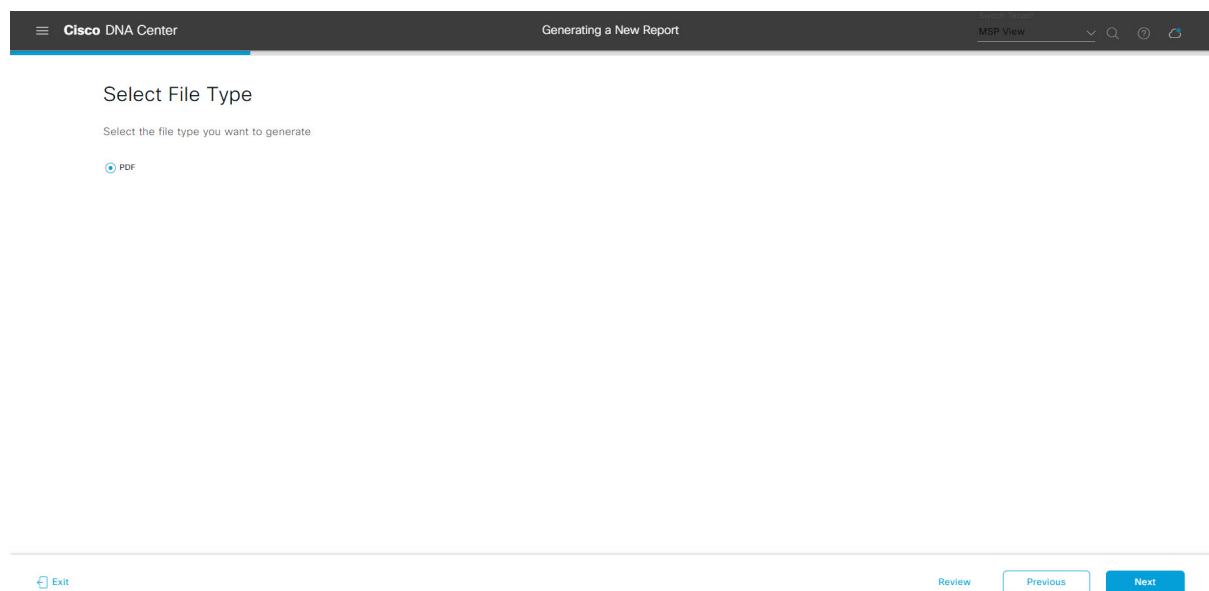Click **Next**. The **Select File Type** window opens.

Step 9   In the **Select File Type** window, select the file type for the report.

Depending on the report that you are creating, the following **File Type** options may be available:

- **PDF**

- **CSV**

- **Tableau Data Extract**

- **JSON**

For the **CSV**, **JSON**, and **Tableau Data Extract** file types, a **Fields** option displays that permits you to select attributes (additional fields) for the CSV, JSON, and Tableau Data Extract results.

Figure 82: Select File Type

Click **Next**. The **Schedule Report** window opens.

Step 10   In the **Schedule Report** window, select the time range and schedule for the report.

The following **Time Range** options are available:

- **Last 3 hours**

- **Last 24 hours**

- **Last 7 days**

- **Custom**

    Note   Clicking **Custom** displays fields where you can choose the date and time interval for a specific report type, and the time zone (GMT) for the time range.
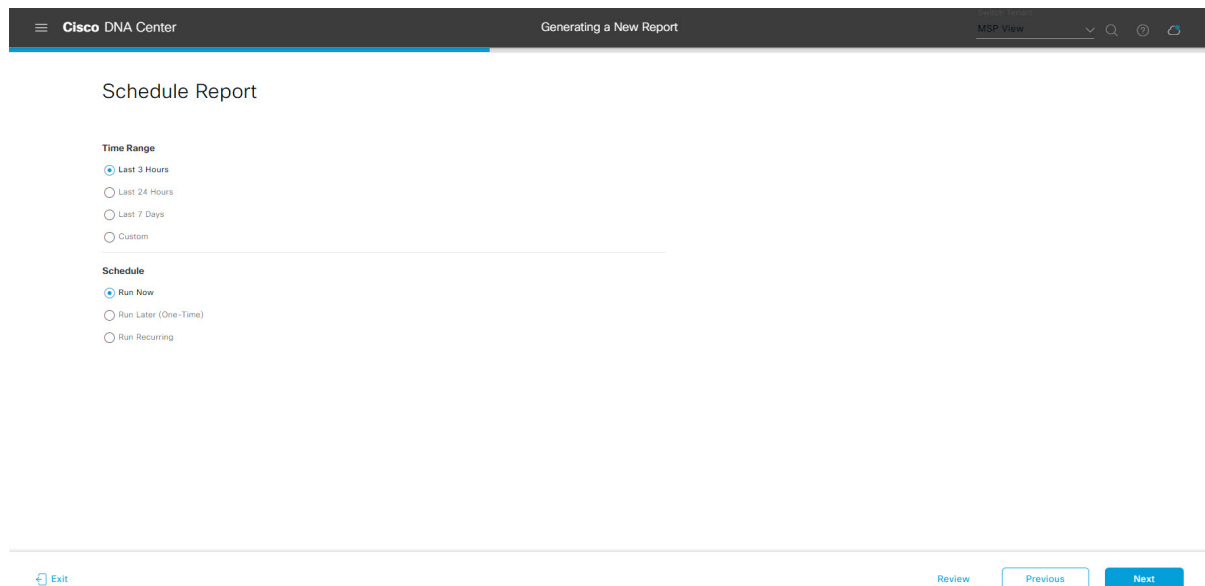
The following **Schedule** options are available:

- **Run Now**

        • **Run Later**

        • **Run Recurring**

You can also select a time zone for the report when configuring with the following **Schedule** options:

        • **Custom**

        • **Run Later (One Time)**

        • **Run Recurring**

Figure 83: Schedule Report

Click **Next**. The **Delivery and Notification** window opens.

Step 11   In the **Delivery and Notification** window, select the delivery mechanism for the report:

        • **Email Report**: Email report is sent as a link or attachment.

           Note   If you have not configured an SMTP server for the emails, you are prompted to configure one. Follow the prompts to the **Email** tab in the GUI to configure an SMTP server. Click **System** > **Settings** > **External Services** > **Destinations** > **Email** tab.

           • **Link**: The email notification of a successfully compiled report has a link to the report and to the **Generated Reports** page under **Reports**. You can view and download the report from this location.

              Note   Email notifications with embedded links to reports support up to 20 email addresses. To add multiple email addresses, you need to add each email address separately and press **Enter** (on your keyboard) after each addition. Cisco DNA Center platform validates the email addresses and notifies you if the syntax is incorrect.

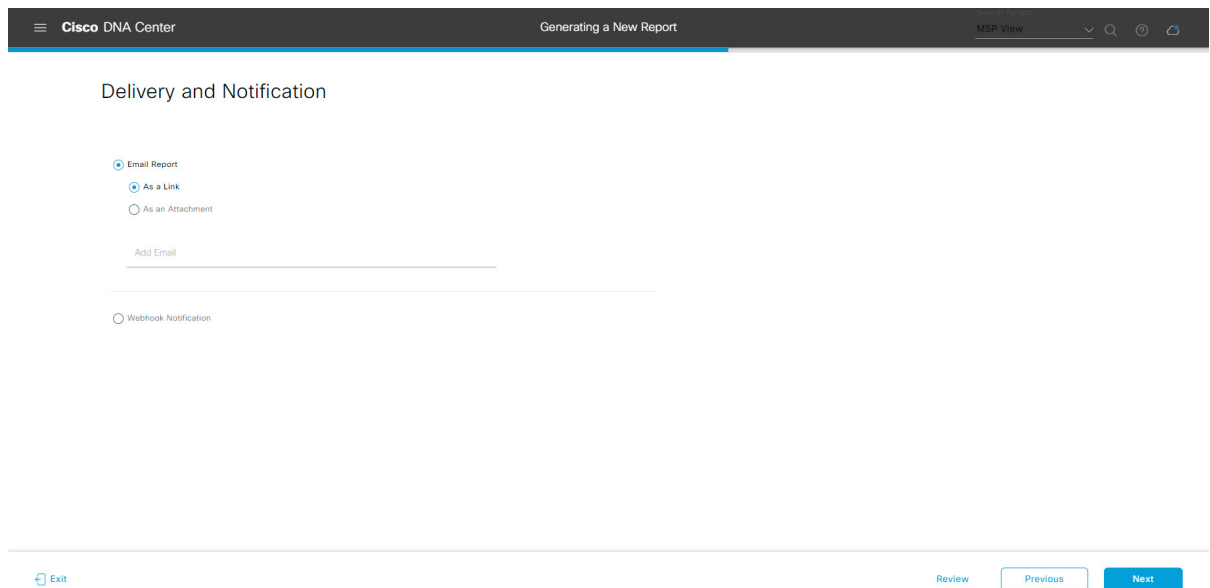   • **Attachment**: Report is attached to the email notification.

Note PDF reports support email notification attachments of up to 20-MB in size and up to 10 email addresses. To add multiple email addresses, you need to add each email address separately and press **Enter** (on your keyboard) after each addition. Cisco DNA Center platform validates the email addresses and notifies you if the syntax is incorrect.

Cisco DNA Center sends the following email notifications for the report:

- Report is in the queue waiting to be processed.

- Report processing is in progress.

- Report has successfully been compiled and is completed.

- **Webhook Notification**: Notification is sent as a webhook to the configured webhook URL address (callback URL). Select a webhook from the drop-down list **(Subscription Profile** field).

Note If you have not yet created a webhook, you are prompted to create one. Follow the prompts to the **Webhook** tab in the GUI to configure a webhook. In general, to configure a webhook, click **System** > **Settings** > **External Services** > **Destinations** > **Webhook**.

You receive status webhook notifications for the report, for example, **In Queue**, **In Progress**, and **Success**. You are also able to view these notifications in the GUI.
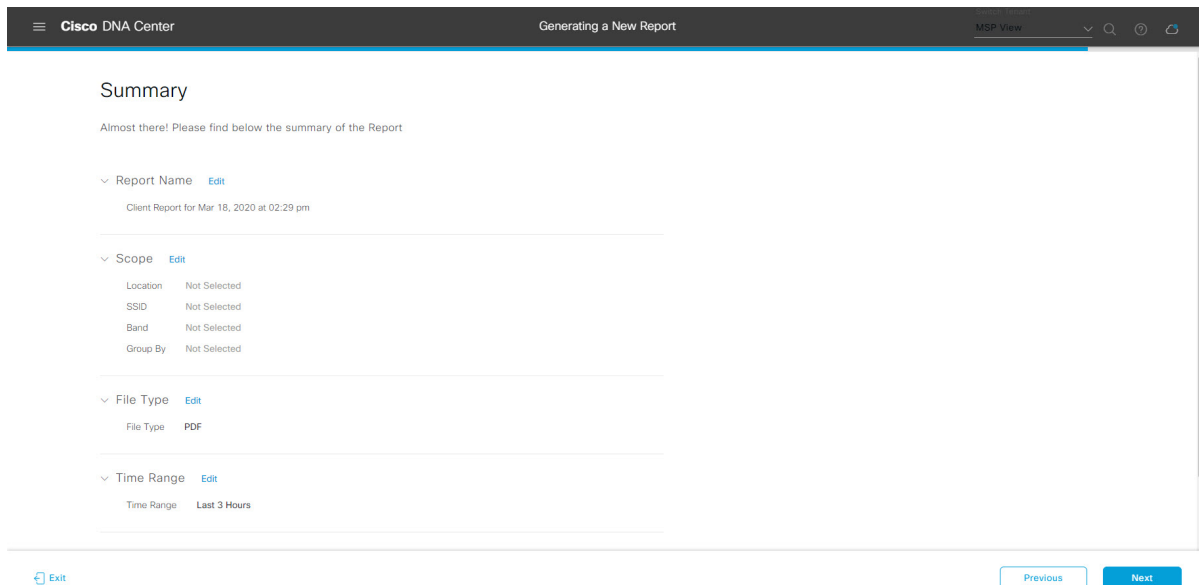
Figure 84: Delivery and Notification

Click **Next**. The **Summary** window opens.

Step 12 In the **Summary** window, review the configuration and, if necessary, edit the files.
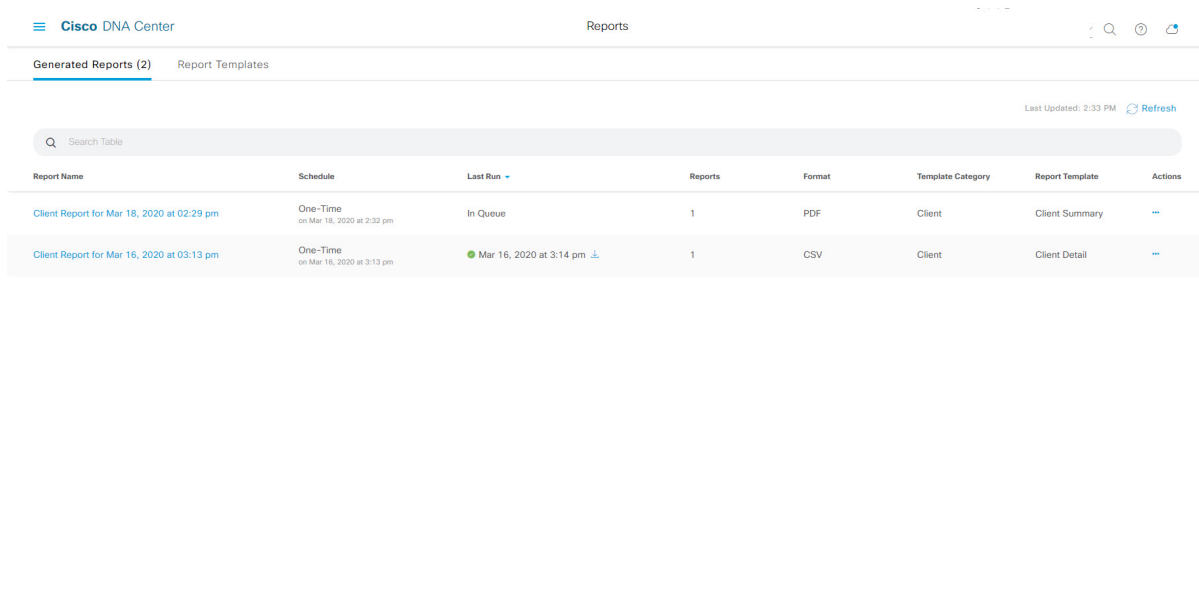
Figure 85: Summary

Click **Next**.

After the report is generated, a success window appears.

Step 13 Click the **View the Generated Reports** link.

The **Generated Reports** window is displayed with instance details of the report that was scheduled.

Figure 86: Generated Reports

What to do next

Review your report instance in **Generated Reports** window.

Note	You can download, review, edit, duplicate, or delete the report in the **Generated Reports** window. For additional information, see .

Run a Network Devices Report

Perform this procedure to configure **Network Devices** reports for your network. You can configure **Network Devices** reports using the **Reports** window in the Cisco DNA Center GUI.

Figure 87: Network Devices Reports
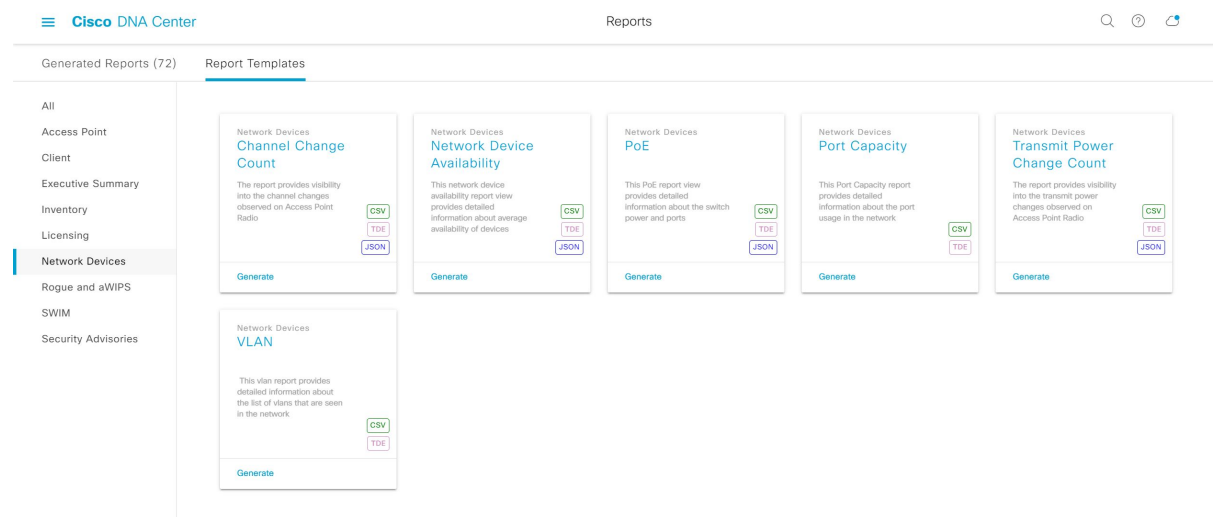
Before you begin

Run a successful **Discovery** job in Cisco DNA Center. You can check whether a **Discovery** job is successful in **Device Inventory**. Click the menu icon (☰) and choose **Provision** > **Inventory** to view the results.

|	
Step 1	Click the menu icon (☰) and choose **Reports** > **Report Templates**.
	The **Report Templates** window opens and displays the supported reporting categories. Each category is represented by link. Click a link to view only the supported reports for that category.
	For this release, reporting is supported for the following categories:
	• **Access Point**: Reports that provide data about Access Points and Access Point Radios.
	• **Client**: Reports that help with analyzing how the clients are performing in the network.
	• **Executive Summary**: Report that helps with analyzing how devices, applications, and clients are performing in the network.

     • **Inventory**: Report that lists devices discovered by Cisco DNA Center.

     • **Licensing**: Reports that list noncompliant devices and the reasons for noncompliance.

     • **Network Devices**: Reports that provide data about the devices in your network.

     • **Rogue and aWIPS**: Reports that provide data about threats in your network.

     • **SWIM**: Report that lists the software and version of the devices in your network.

     • **Security Advisories**: Report that provides Cisco security advisory information on the network devices.

Note   The Access Point, Client, and Executive Summary reports support up to 90 days of data retention.

Step 2   After clicking a link, review the **Report Templates** window for that selected category.

Figure 88: Network Devices Reports
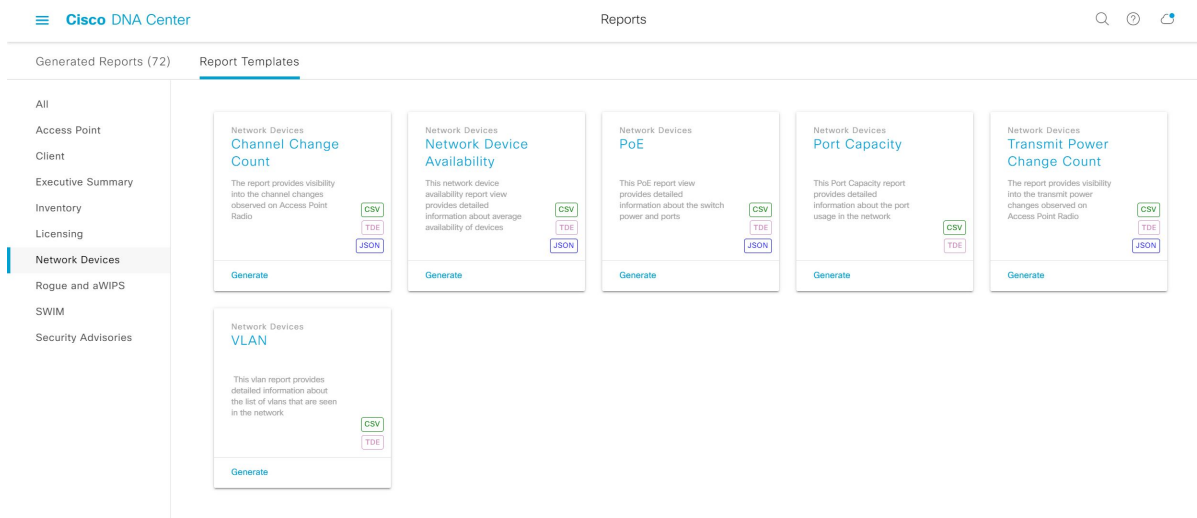
The **Report Templates** window displays supported report templates. Each template is represented by a tile and contains information about the report and links to configure (generate) a report. Determine which template you wish to use to generate a report. For example, for a **Network Devices** report you can create a **Channel Change Count**, **Network Device Availability**, **PoE**, **Port Capacity**, **Transmit Power Change Count**, or **VLAN** report. Within the tile are also icons that represent the supported file types for the reports (CSV, TDE, or JSON).

Step 3   In the tile, click the header to view a sample report.

A window appears for the sample report. Use the side bar in the window to scroll down and review the entire sample report. The following data is presented:

     • Applied filters (data filters that were used to build the report).

     • Data metrics and summaries

     • Graphical representation of the data (including line, bar, and pie graphs).

     • Tables that assist you in analyzing the data.

Note   You can use the sample report to plan how you want your report to look.

Step 4   Click **X** to close the preview.

Step 5   In the tile, click the **Generate** link to configure parameters to build a report.

The **Generate** window opens where you can select a format type for the report, apply data filters for your reports, as well as set up schedules for the actual report generation.

Step 6   In the **Generate a New Report** window, click **Let's Do It** to get started.

Figure 89: Generate a New Report
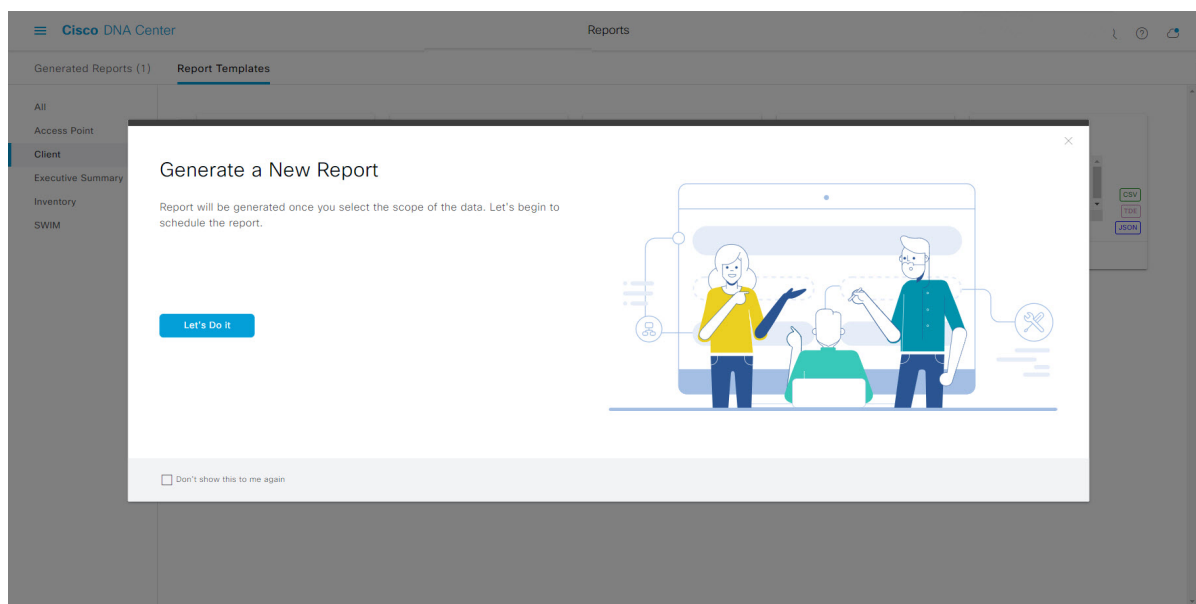
The **Setup the Report Template** window opens.
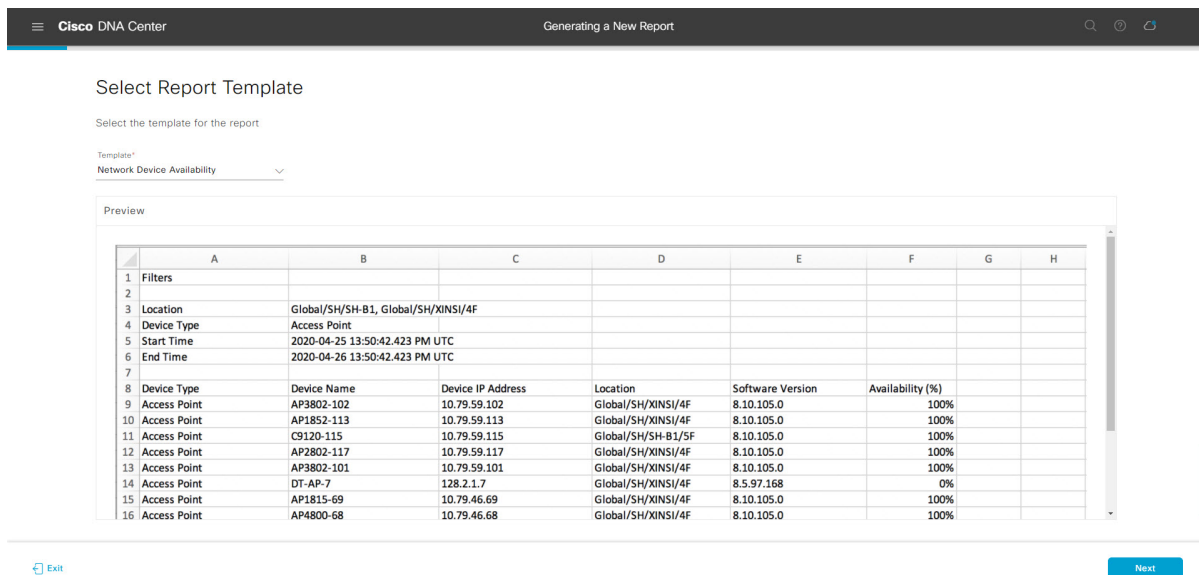
Step 7   In the **Setup the Report Template** window, select the template for the report.

Choose the **Template** from the drop-down menus.

Note   The **Template** consists of the individual report types within the categories for the release.

You can review an auto-generated sample in the same window.

Figure 90: Setup Report Template

Click **Next**. The **Setup Report Scope** window opens.

Step 8 In the **Setup Report Scope** window, name the report and select the scope.

Enter a report name in the **Report Name** field and click in the **Scope** field to display the available filter. Click on the filter options that you want for the report.

Note   The **Setup Report Scope** options will change depending upon the selected **Template**.

Figure 91: Setup Report Scope

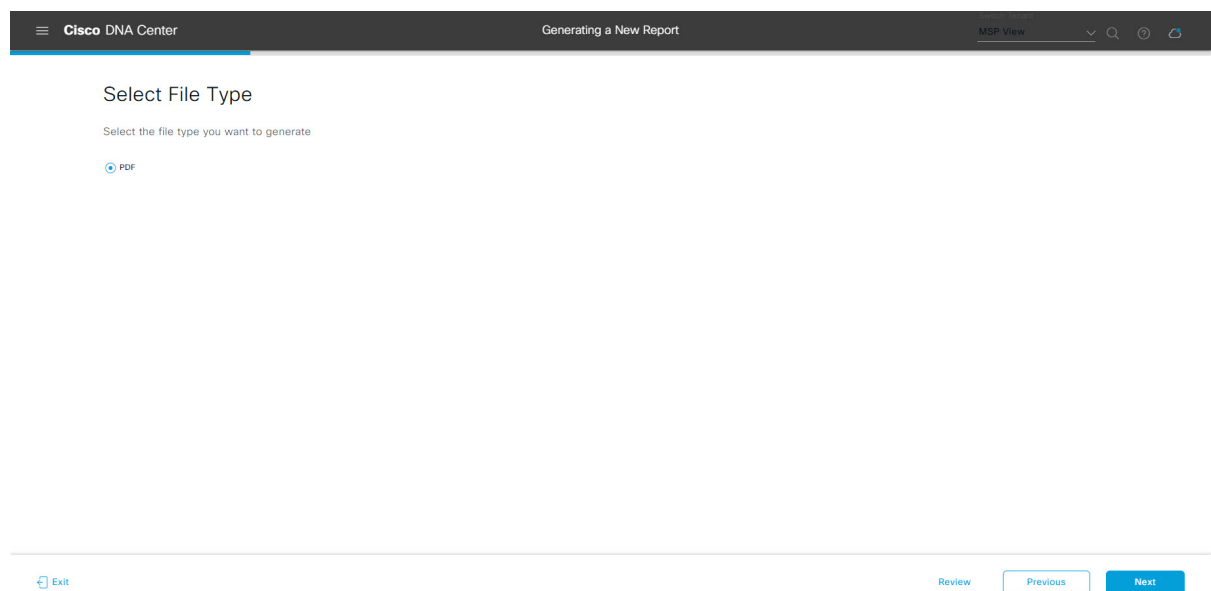Click **Next**. The **Select File Type** window opens.

Step 9 In the **Select File Type** window, select the file type for the report.

Depending on the report that you are creating, the following **File Type** options may be available:

- **PDF**

- **CSV**

- **Tableau Data Extract**

- **JSON**

For the **CSV**, **JSON**, and **Tableau Data Extract** file types, a **Fields** option will display that permits you to select attributes (additional fields) for the CSV, JSON, and Tableau Data Extract results.

Figure 92: Select File Type

Click **Next**. The **Schedule Report** window opens.

Step 10 In the **Schedule Report** window, select the time range and schedule for the report.

The following **Time Range** options are available:

- **Last 3 hours**

- **Last 24 hours**

- **Last 7 days**

- **Custom**

  Note Clicking **Custom** opens up fields where you can choose the date and time interval per the specific report type, as well as the time zone (GMT) for the time range.
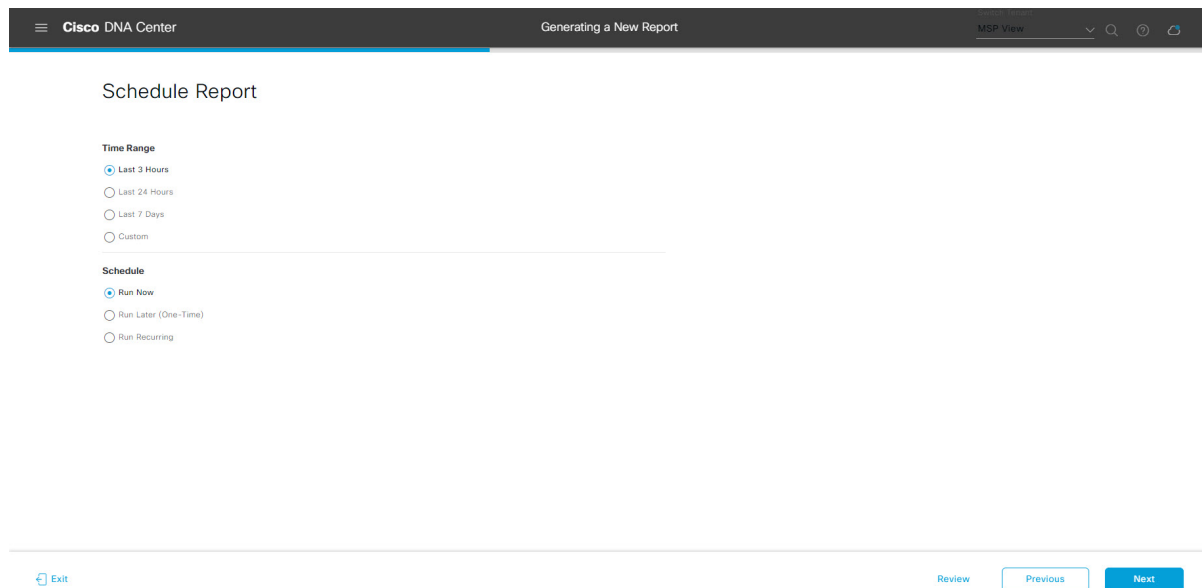
The following **Schedule** options are available:

- **Run Now**

> • **Run Later**

> • **Run Recurring**

You can also select a timezone for the report when configuring with the following **Schedule** options:

> • **Custom**

> • **Run Later (One Time)**

> • **Run Recurring**

Figure 93: Schedule Report

Click **Next**. The **Delivery and Notification** window opens.

Step 11   In the **Delivery and Notification** window, select the delivery mechanism for the report.

The options include:

> • **Email Report**: Email report is sent as a link or attachment.

> > **Note**   If you have not yet configured a SMTP server for the emails, you will be prompted to configure one. Follow the prompts to the **Email** tab in the GUI to configure a SMTP server. Click **System** > **Settings** > **External Services** > **Destinations** > **Email**.

> > • **Link**: The email notification of a successfully compiled report will have a link back to itself and the **Generated Reports** page under **Reports**. You can view and download the report from this link and location.

> > > **Note**   Email notifications with embedded links to reports support up to 20 email addresses. To add multiple email addresses, you need to add each email address separately and press **Enter** (on your keyboard) after each addition. Cisco DNA Center platform validates the email addresses and notifies you if the syntax is incorrect.

> > • **Attachment**: Report is attached to the email notification.

Note	PDF reports support email notification attachments of up to 20-MB in size and up to 10 email addresses. To add multiple email addresses, you need to add each email address separately and press **Enter** (on your keyboard) after each addition. Cisco DNA Center platform validates the email addresses and notifies you if the syntax is incorrect.

Cisco DNA Center sends the following email notifications for the report:

- Report is in the queue waiting to be processed.

- Report processing is in progress.

- Report has successfully been compiled and is completed.

- **Webhook Notification**: Notification is sent as a webhook to the configured webhook URL address (callback URL). Select a webhook from the drop-down menu **(Subscription Profile** field).

Note	If you have not yet created a webhook, you will be prompted to create one. Follow the prompts to the **Webhook** tab in the GUI to configure a webhook. In general, to configure a webhook, click **System** > **Settings** > **External Services** > **Destinations** > **Webhook** tab.

You will receive status webhook notifications for the report. For example, you will receive "In Queue," "In Progress," and "Success" webhook notifications. You will also be able to view these notifications in the GUI.
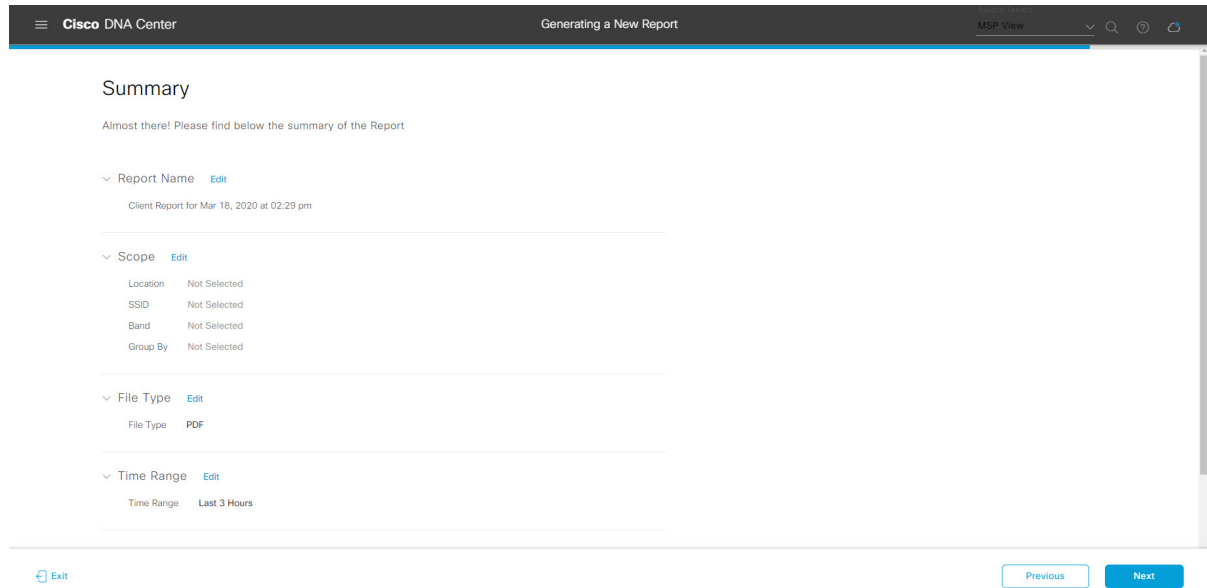
Figure 94: Delivery and Notification
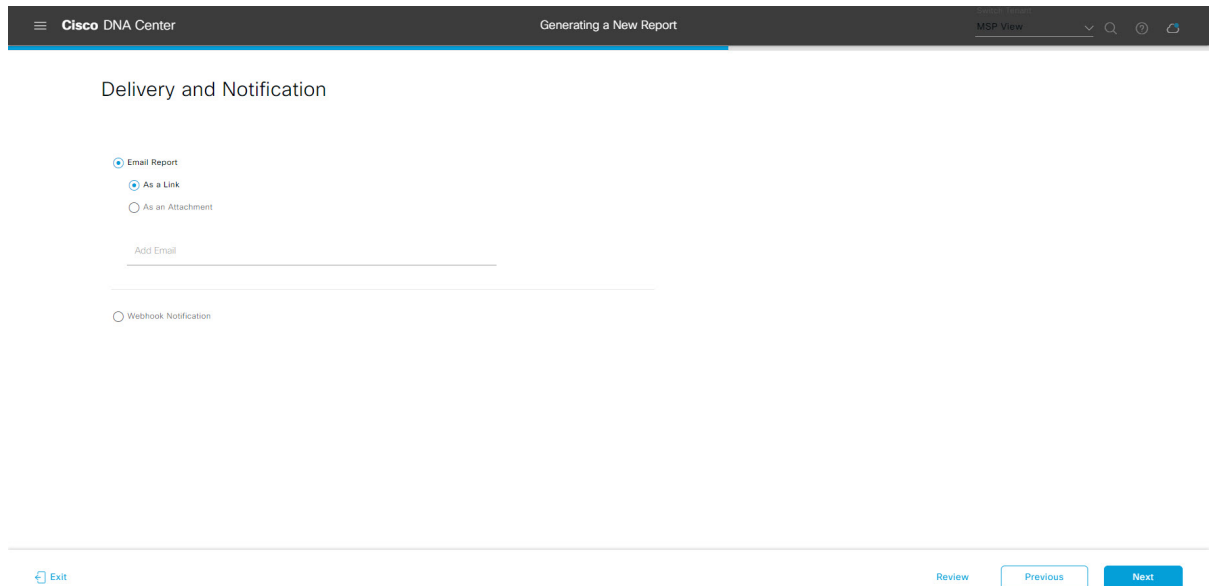
Click **Next**. The **Summary** window opens.

Step 12   In the **Summary** window, review the configuration and if necessary edit any of the files.

Figure 95: Summary

Click **Next**.

After the report is generated, a success window appears.

Step 13   Click the **View the Generated Reports** link.

The **Generated Reports** window opens with instance details of the report that was scheduled.

Figure 96: Generated Reports

What to do next

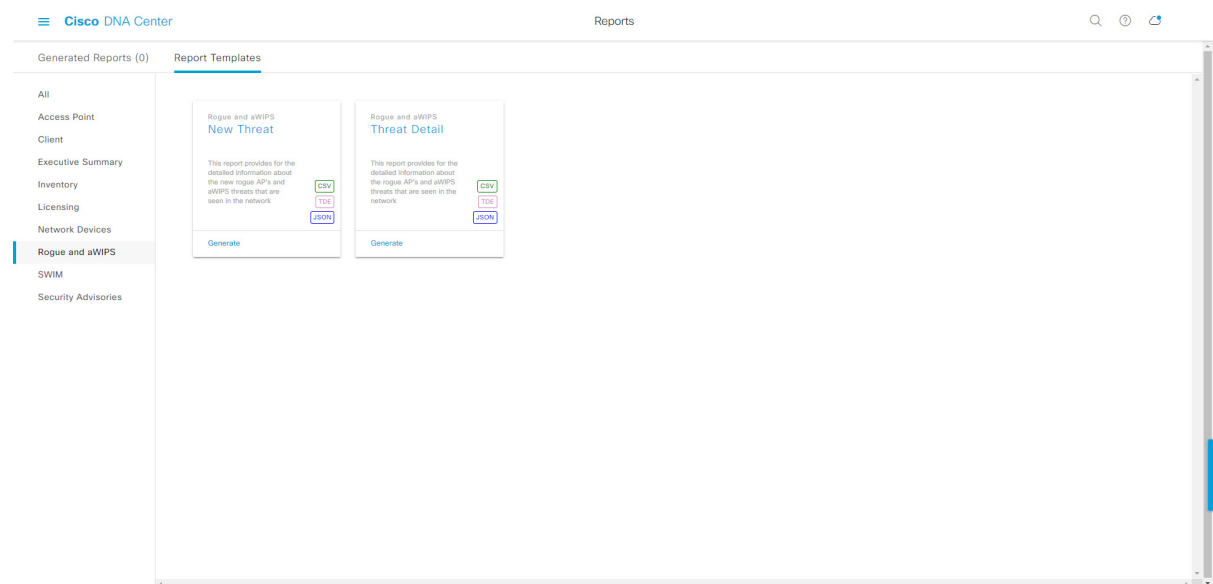Review your report instance in **Generated Reports** window.

> **Note** You can download, review, edit, duplicate, or delete the report in the **Generated Reports** window. For additional information, see View Generated Reports, on page 133.

Run a Rogue and aWIPS Report

Perform this procedure to configure **Rogue and aWIPs** reports for your network. You can configure **Rogue and aWIPS** reports using the **Reports** window in the Cisco DNA Center GUI.

Figure 97: Rogue and aWIPS Reports

Before you begin

Run a successful **Discovery** job in Cisco DNA Center. You can check whether a **Discovery** job is successful in **Device Inventory**. Click the menu icon (☰) and choose **Provision** > **Inventory** to view the results.

Step 1 Click the menu icon (☰) and choose **Reports** > **Report Templates**.

The **Report Templates** window opens and displays the supported reporting categories. A link represents each category. Click a link to view only the supported reports for that category.

For this release, reporting is supported for the following categories:

- **Access Point**: Reports that provide data about Access Points and Access Point Radios.

- **Client**: Reports that help with analyzing how the clients are performing in the network.

• **Executive Summary**: Report that helps with analyzing how devices, applications, and clients are performing in the network.

• **Inventory**: Report listing devices discovered by Cisco DNA Center.

• **Licensing**: Reports that lists devices that noncompliant devices and the reasons for noncompliance.

• **Network Devices**: Reports that provide data about the devices within your network.

• **Rogue and aWIPS**: Reports that provide data about threats within your network.

• **SWIM**: Report listing all the devices in network with software and versioning.

• **Security Advisories**: Report that provides Cisco security advisory information on the network devices.

Note   The Access Point, Client, and Executive Summary reports support up to 90 days of data retention.

Step 2   After clicking a link, review the **Report Templates** window for that selected category.

Figure 98: Reports Templates Window
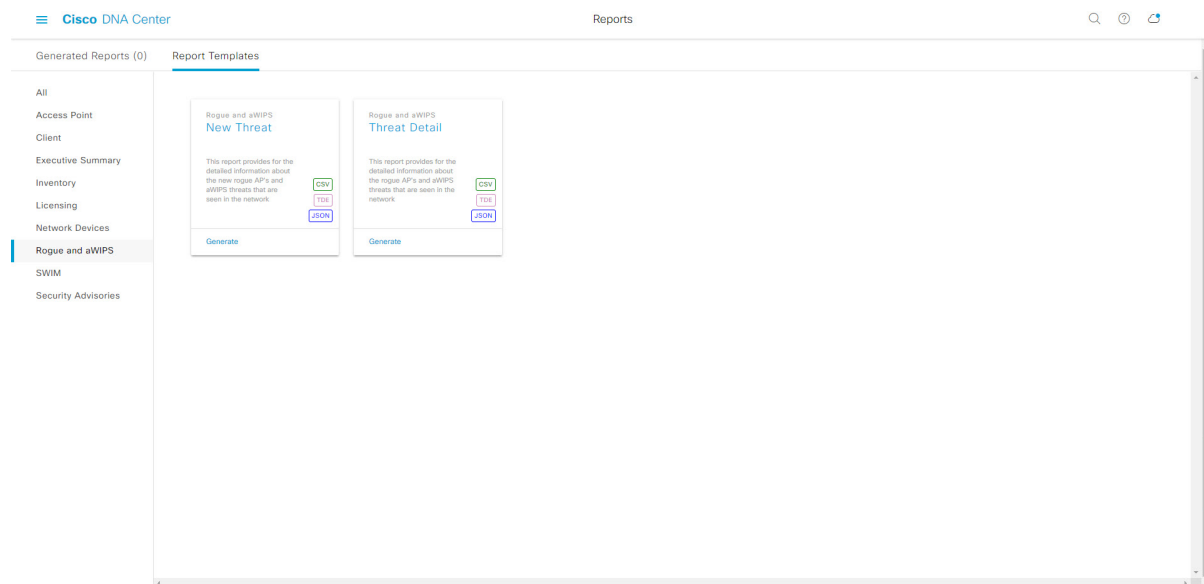
The **Report Templates** window displays supported report templates. Each template is represented by a tile and contains information about the report and links to configure (generate) a report. Determine which template you wish to use to generate a report. For example, for a **Rogue and aWIPs** report you can create a **New Threat** or **Thread Detail** report. Within the tile are also icons that represent the supported file types for the reports (CSV, TDE, or JSON).

Step 3   In the tile, click the header to view a sample report.

A window appears for the sample report. Use the side bar in the window to scroll down and review the entire sample report. The following data is presented:

• Applied filters (data filters that were used to build the report).

• Data metrics and summaries

• Graphical representation of the data (including line, bar, and pie graphs).

• Tables that assist you in analyzing the data.

Note   You can use the sample report to plan how you want your report to look.

Step 4   Click **X** to close the preview.

Step 5   In the tile, click the **Generate** link to configure parameters to build a report.

The **Generate** window opens where you can select a format type for the report, apply data filters for your reports, as well as set up schedules for the actual report generation.

Step 6   In the **Generate a New Report** window, click **Let's Do It** to get started.

Figure 99: Generate a New Report

The **Select Report Template** window opens.

Step 7   In the **Select Report Template** window, select the template for the report.

Choose the **Template** from the drop-down lists.

Note   The **Template** consists of the individual report types within the categories for the release.

You can review an autogenerated sample in the same window.

Figure 100: Setup Report Template

Click **Next**. The **Setup Report Scope** window opens.

Step 8 In the **Setup Report Scope** window, name the report and select the scope.

Enter a report name in the **Report Name** field and click in the **Scope** field to display the available filter. Click the filter options that you want for the report.

Note The **Setup Report Scope** options change depending upon the selected **Template**.

Figure 101: Setup Report Scope
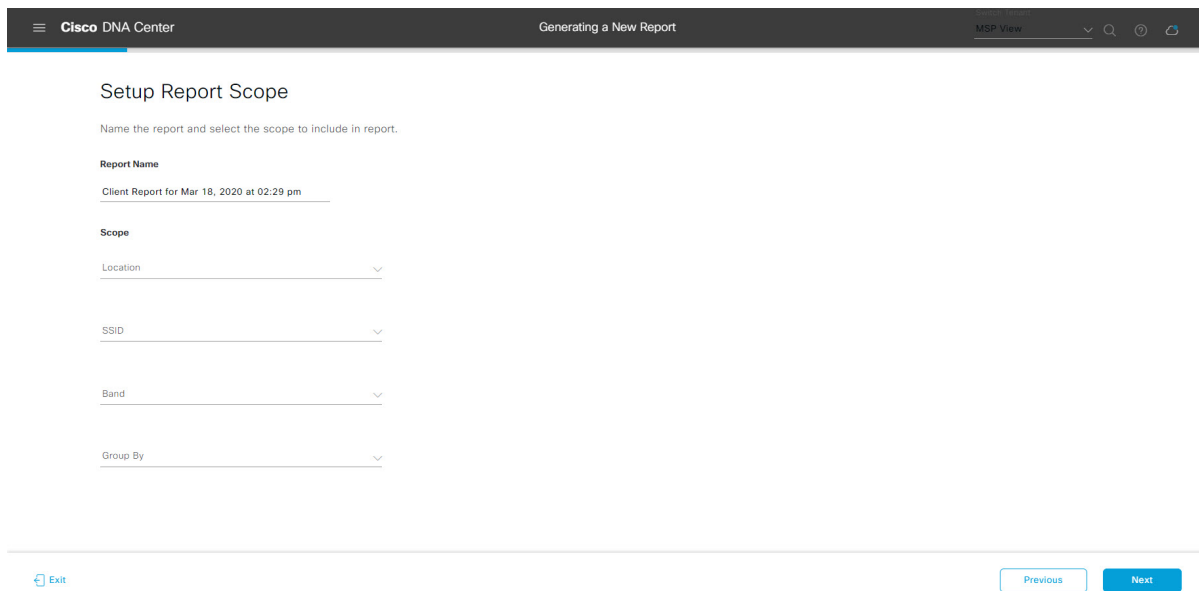
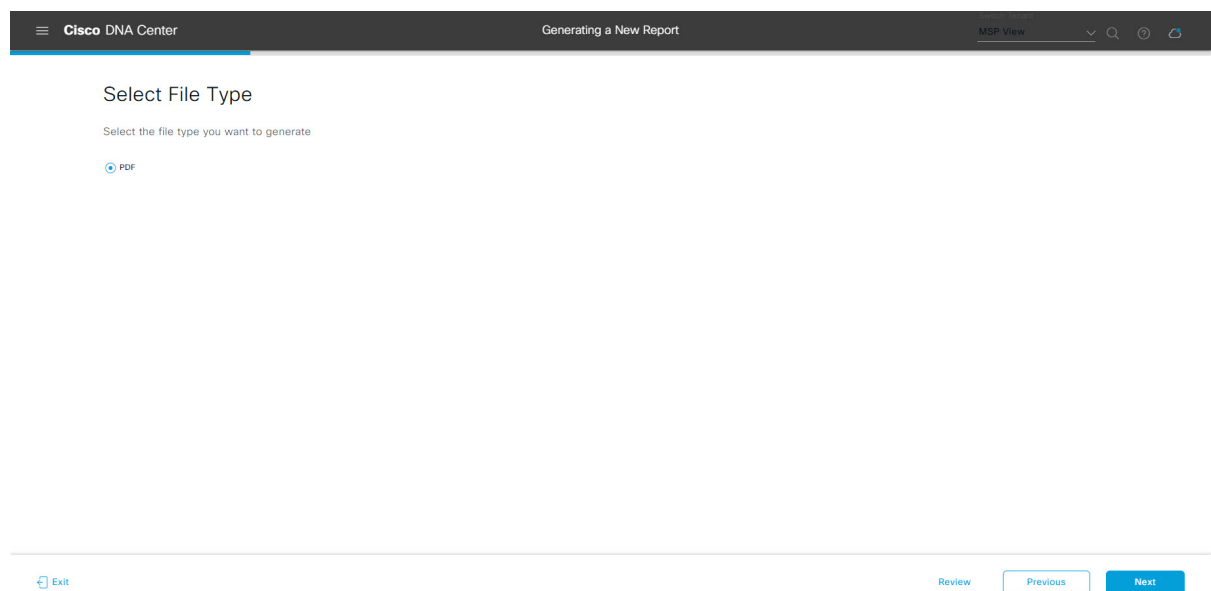Click **Next**. The **Select File Type** window opens.

Step 9 In the **Select File Type** window, select the file type for the report.

Depending upon the report that you are creating, the following **File Type** options may be available:

- **PDF**
- **CSV**
- **Tableau Data Extract**
- **JSON**

For the **CSV**, **JSON**, and **Tableau Data Extract** file types, a **Fields** option displays that permits you to select attributes (additional fields) for the CSV, JSON, and Tableau Data Extract results.

Figure 102: Select File Type

Click **Next**. The **Schedule Report** window opens.

Step 10 In the **Schedule Report** window, select the time range and schedule for the report.

The following **Time Range** options are available:

- **Last 3 hours**
- **Last 24 hours**
- **Last 7 days**
- **Custom**

  Note Clicking **Custom** opens up fields where you can choose the date and time interval per the specific report type, as well as the time zone (GMT) for the time range.
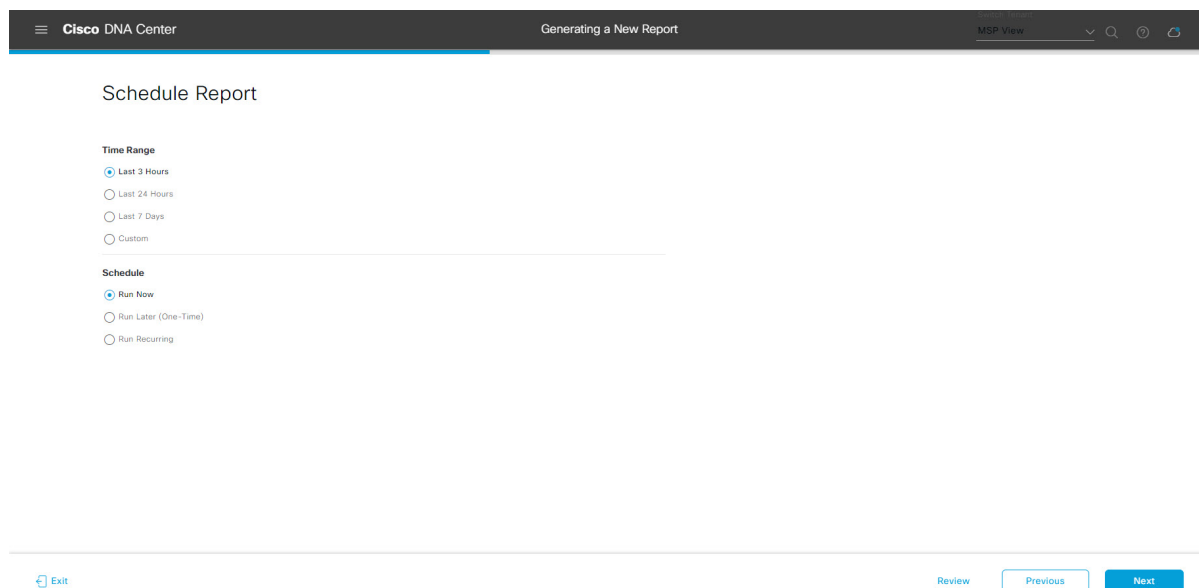
The following **Schedule** options are available:

- **Run Now**

　　　　　　　• **Run Later**

　　　　　　　• **Run Recurring**

You can also select a time zone for the report when configuring with the following **Schedule** options:

　　　　　　　• **Custom**

　　　　　　　• **Run Later (One Time)**

　　　　　　　• **Run Recurring**

Figure 103: Schedule Report

Click **Next**. The **Delivery and Notification** window opens.

Step 11　　In the **Delivery and Notification** window, select the Delivery mechanism for the report.

The options include:

　　　　　　　• **Email Report**: Email report is sent as a link or attachment.

　　　　　　　Note　　　　If you have not yet configured an SMTP server for the emails, you will be prompted to configure one. Follow the prompts to the **Email** tab in the GUI to configure an SMTP server. Click **System** > **Settings** > **External Services** > **Destinations** > **Email**.

　　　　　　　　　　• **Link**: The email notification of a successfully compiled report has a link back to itself and the **Generated Reports** page under **Reports**. You can view and download the report from this link and location.

　　　　　　　　　　Note　　　　Email notifications with embedded links to reports support up to 20 email addresses. To add multiple email addresses, you need to add each email address separately and press **Enter** (on your keyboard) after each addition. Cisco DNA Center platform validates the email addresses and notifies you if the syntax is incorrect.

　　　　　　　　　　• **Attachment**: Report is attached to the email notification.

Note	PDF reports support email notification attachments of up to 20-MB in size and up to 10 email addresses. To add multiple email addresses, you need to add each email address separately and press **Enter** (on your keyboard) after each addition. Cisco DNA Center platform validates the email addresses and notifies you if the syntax is incorrect.

Cisco DNA Center sends the following email notifications for the report:

- Report is in the queue waiting to be processed.

- Report processing is in progress.

- Report has successfully been compiled and is completed.

- **Webhook Notification**: Notification is sent as a webhook to the configured webhook URL address (callback URL). Select a webhook from the drop-down list **(Subscription Profile** field).

Note	If you have not yet created a webhook, you will be prompted to create one. Follow the prompts to the **Webhook** tab in the GUI to configure a webhook. In general, to configure a webhook, click **System** > **Settings** > **External Services** > **Destinations** > **Webhook** tab.

You will receive status webhook notifications for the report. For example, you will receive "In Queue", "In Progress", and "Success" webhook notifications. You will also be able to view these notifications in the GUI.

Figure 104: Delivery and Notification

Click **Next**. The **Summary** window opens.

Step 12 In the **Summary** window, review the configuration and if necessary edit any of the files.

Run a Rogue and aWIPS Report

Figure 105: Summary

Click **Next**.

After the report is generated, a success window appears.

Step 13   Click the **View the Generated Reports** link.

The **Generated Reports** window opens with instance details of the report that was scheduled.

Figure 106: Generated Reports

What to do next

Review your report instance in **Generated Reports** window.
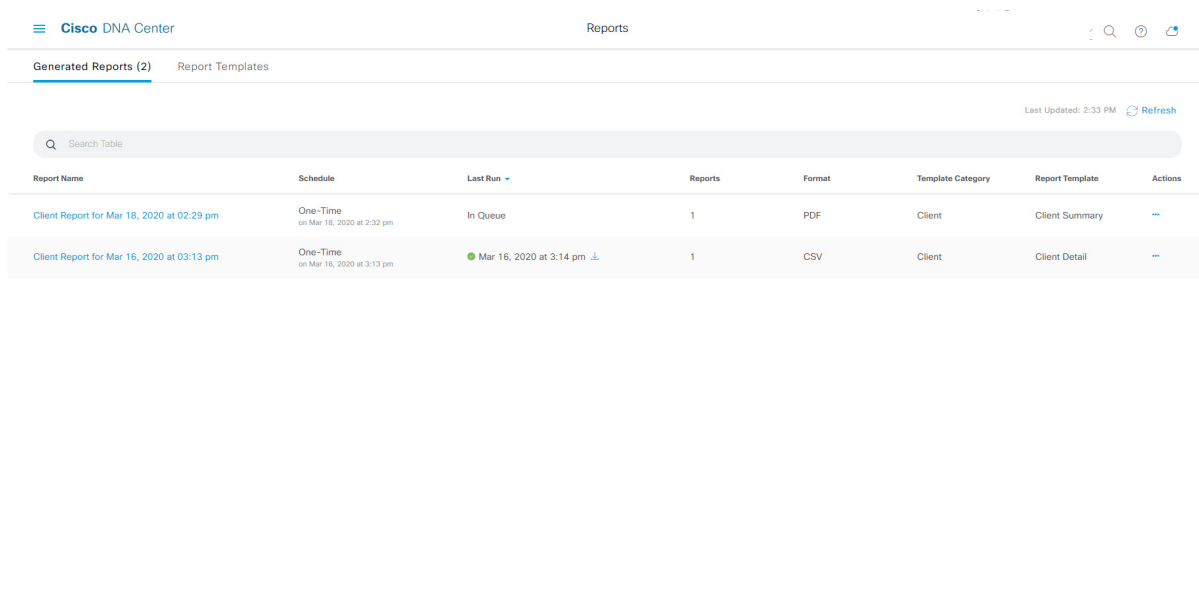
Note   You can download, review, edit, duplicate, or delete the report in the **Generated Reports** window. For additional information, see View Generated Reports, on page 133.

Run an ROI Report

The Cisco DNA Center platform ROI Insights report is a customized report that shows the productivity improvement of network operations with Cisco DNA Center and comparative ROI insights with a traditional NMS.

The following procedure describes how to configure an ROI report for a network operation.

Step 1   Click the menu icon (≡) and choose **Reports** > **Usage Insights**.

The **Usage Insights** window displays the following information:

- **SAVINGS**: Displays the time and cost saved on network operation with Cisco DNA Center for a selected time range.

- **ROI Insights**: Lists the ROI Insights report that is created based on **Features**, **Time Saved**, **Cost Saved**, **Usage KPI**, **Traditional NMS** time, **Cisco DNA Center** time, and **Actions**.

- **Savings Trends**: Displays the savings trend of **Cost** and **Time** for an ROI Insights report.

    Note   The **Savings Trends** area appears only if the selected time range is more than a month.

Step 2   In the **Campus Network Assurance**, **Network Device Onboarding**, **Campus Software Image Management**, and **Campus Network Segmentation** areas, enter the time savings in the **Hours** and **Minutes** name fields for a traditional NMS and Cisco DNA Center.

- Traditional NMS: Average time to detect and resolve an issue in the network without Cisco DNA Center.

- Cisco DNA Center: Average time to detect and resolve an issue in the network with Cisco DNA Center.

Step 3   To modify the **Cost Inputs** and **IT Inputs**, click **Customize ROI Insights** and make the changes.

The **Customize ROI Insights** area displays the preconfigured **Avg. Cost per IT Staff**, **Currency**, **No. of IT Staff**, and **Avg. Annual Hrs Worked**.

Step 4   To edit the time savings for a feature, click the corresponding **Edit** link under the **Actions** column and update the time in the subsequent pop-up window.

Step 5   To choose the time range for which you want to see the ROI report, click the time range drop-down list below the **Customize ROI Insights** pane and click a time range radio button.

a)   Choose from the available time range options: **1 Month**, **3 Months**, **6 Months**, and **1 Year**.

b)   To customize the time range of ROI reports, click the time range drop-down list, click **Custom**, and define the **Start Date** and **End Date**.

Figure 107: Usage Insights Report Dashboard
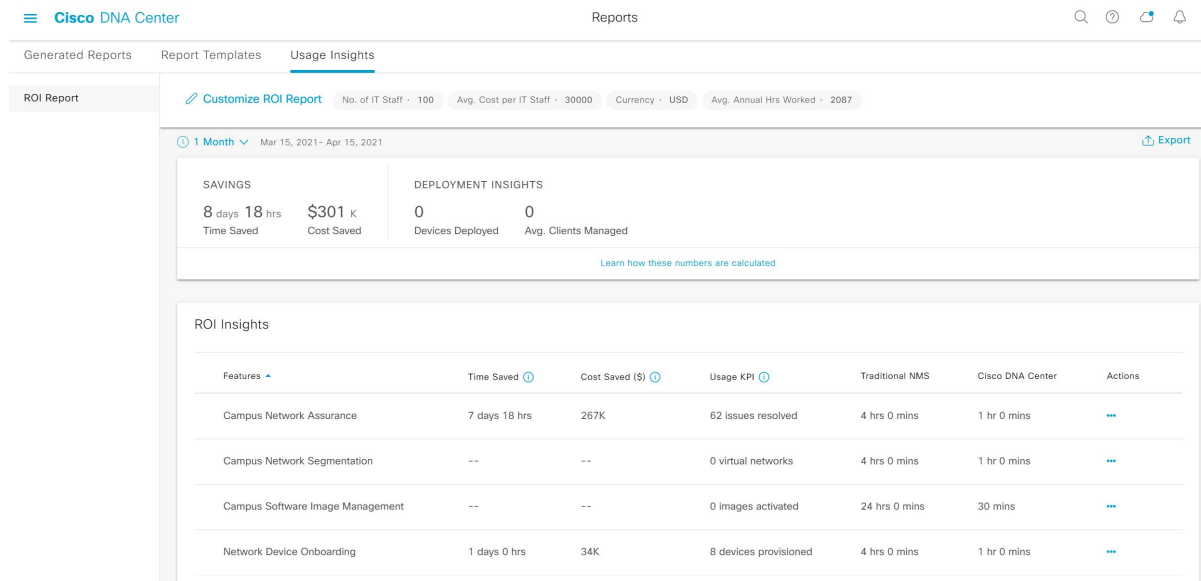
Step 6   Click **Learn how these numbers are calculated** above the **ROI Insights** table in the middle pane to see the calculation details.

The **Calculation Details** window shows how to calculate **Time Saved** and **Cost Saved**.

Step 7   To export the ROI report, click **Export**.

The supported file types for the reports are PDF and CSV.

Run a Security Advisories Report

Perform this procedure to configure a **Security Advisories** report about your network. You can configure a **Security Advisories** report using the **Reports** window in the Cisco DNA Center GUI.

Figure 108: Security Advisories Report

Before you begin

Run a successful **Discovery** job in Cisco DNA Center. You can check whether a **Discovery** job is successful in **Device Inventory**. Click the menu icon (☰) and choose **Provision** > **Inventory** to view the results.

Step 1   Click the menu icon (☰) and choose **Reports** > **Report Templates**.

The **Report Templates** window opens and displays the supported reporting categories. A link represents each category. Click a link to view only the supported reports for that category.

For this release, reporting is supported for the following categories:

- **Access Point**: Reports that provide data about Access Points and Access Point Radios.

- **Client**: Reports that help with analyzing how the clients are performing in the network.

- **Executive Summary**: Report that helps with analyzing how devices, applications, and clients are performing in the network.

- **Inventory**: Report listing devices discovered by Cisco DNA Center.

- **Licensing**: Reports that lists devices that noncompliant devices and the reasons for noncompliance.

- **Network Devices**: Reports that provide data about the devices within your network.

- **Rogue and aWIPS**: Reports that provide data about threats within your network.

- **SWIM**: Report listing all the devices in network with software and versioning.

- **Security Advisories**: Report that provides Cisco security advisory information on the network devices.

Note   The Access Point, Client, and Executive Summary reports support up to 90 days of data retention.

Step 2 After clicking on a link, review the **Report Templates** window for that selected category.

Figure 109: Report Templates Window
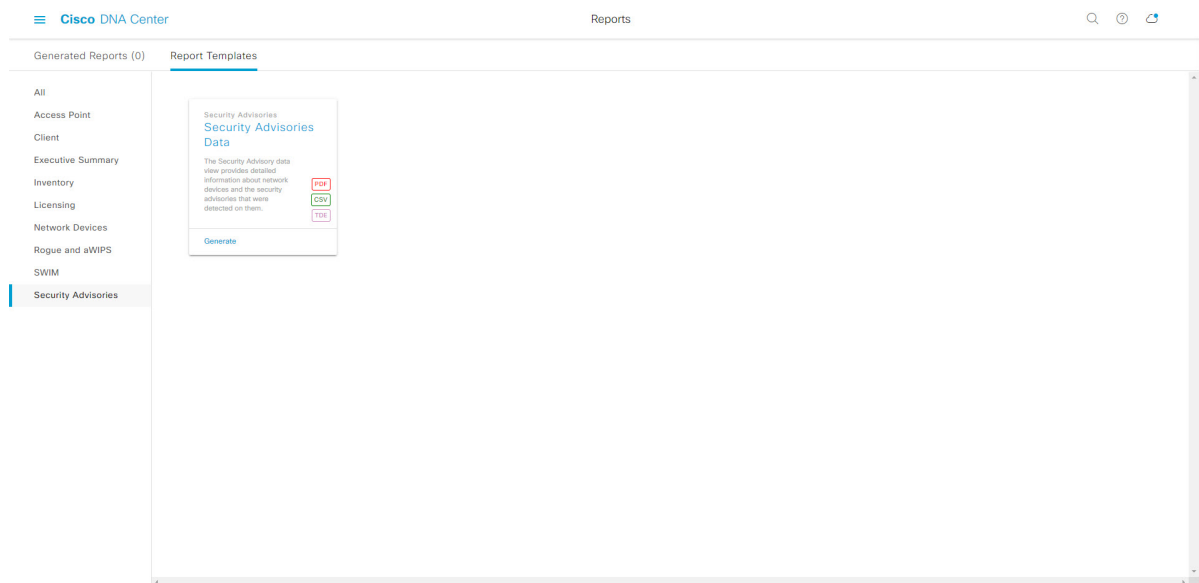
The **Report Templates** window displays supported report templates. Each template is represented by a tile and contains information about the report and links to configure (generate) a report. Determine which template you wish to use to generate a report. For example, for a **Security Advisories** report you can create a **Security Advisories Data** report. Within the tile are also icons that represent the supported file types for the reports (PDF, CSV, or TDE).

Step 3 In the tile, click the header to view a sample report.

A window appears for the sample report. Use the side bar in the window to scroll down and review the entire sample report. The following data is presented:

- Applied filters (data filters that were used to build the report).

- Data metrics and summaries

- Tables that assist you in analyzing the data.

Note   You can use the sample report to plan how you want your report to look.

**Step 4** Click **X** to close the preview.

Step 5 In the tile, click the **Generate** link to configure parameters to build a report.

The **Generate** window opens where you can select a format type for the report, apply data filters for your reports, as well as set up schedules for the actual report generation.

Step 6 In the **Generate a New Report** window, click **Let's Do It** to get started.

Figure 110: Generate a New Report
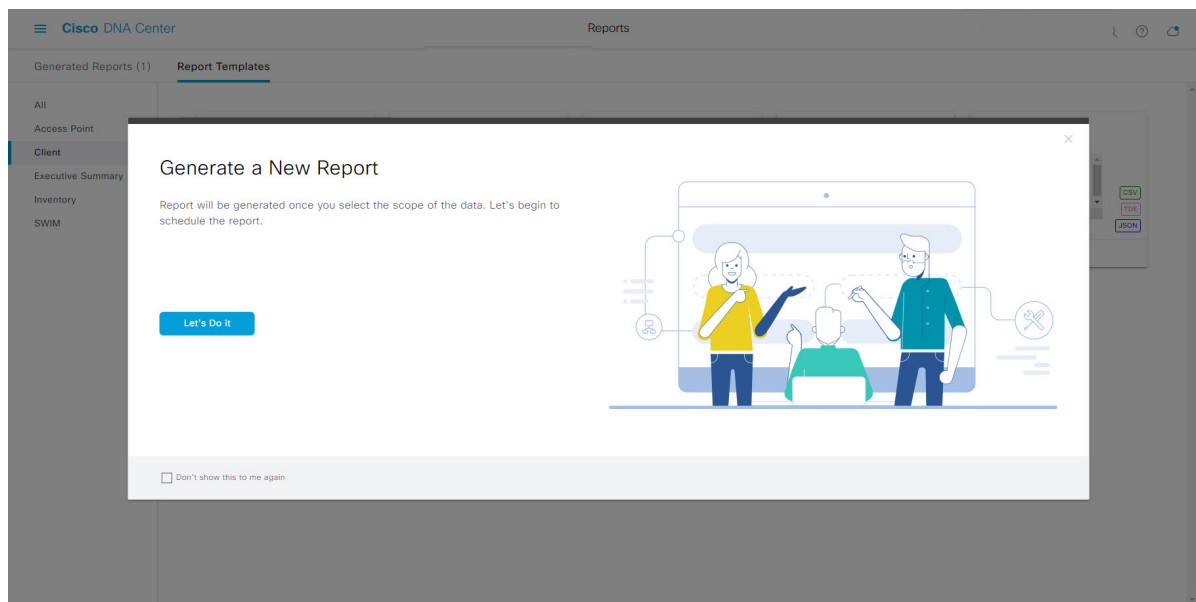
The **Select Report Template** window opens.

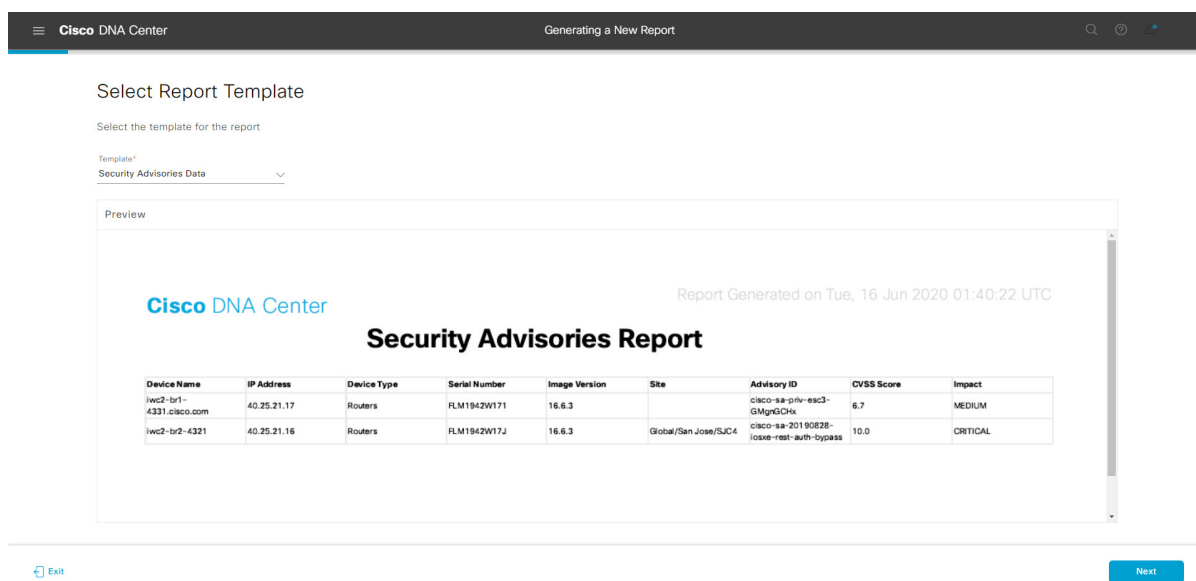**Step 7**   In the **Select Report Template** window, select the template for the report.

Choose the **Template** from the drop-down lists.

Note   The **Template** consists of the individual report types within the categories for the release.

You can review an autogenerated sample in the same window.

Figure 111: Select Report Template

Click **Next**. The **Setup Report Scope** window opens.

Step 8   In the **Setup Report Scope** window, name the report and select the scope.

Enter a report name in the **Report Name** field and click in the **Scope** field to display the available filter. Click the filter options that you want for the report.

Note   The **Setup Report Scope** options change depending upon the selected **Template**.

Figure 112: Setup Report Scope

Click **Next**. The **Select File Type** window opens.

Step 9   In the **Select File Type** window, select the file type for the report.

Depending upon the report that you are creating, the following **File Type** options may be available:

- **PDF**
- **CSV**
- **Tableau Data Extract**
- **JSON**

For the **CSV**, **JSON**, and **Tableau Data Extract** file types, a **Fields** option displays that permits you to select attributes (additional fields) for the CSV, JSON, and Tableau Data Extract results.

Figure 113: Select File Type

Click **Next**. The **Schedule Report** window opens.

Step 10 In the **Schedule Report** window, select the time range and schedule for the report.

The following **Time Range** options are available:

- **Last 3 hours**
- **Last 24 hours**
- **Last 7 days**
- **Custom**

  Note Clicking **Custom** opens up fields where you can choose the date and time interval per the specific report type, as well as the time zone (GMT) for the time range.
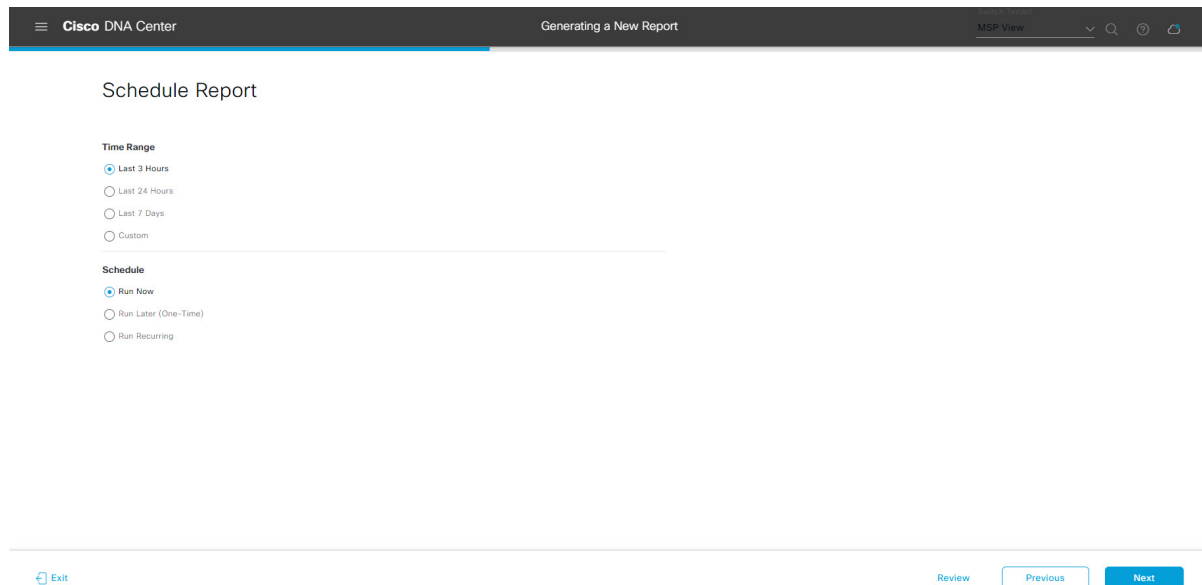
The following **Schedule** options are available:

- **Run Now**
- **Run Later**
- **Run Recurring**

You can also select a time zone for the report when configuring with the following **Schedule** options:

- **Custom**
- **Run Later (One Time)**
- **Run Recurring**

Figure 114: Schedule Report

Click **Next**. The **Delivery and Notification** window opens.

Step 11   In the **Delivery and Notification** window, select the Delivery mechanism for the report.

The options include:

- **Email Report**: Email report is sent as a link or attachment.

  Note   If you have not yet configured an SMTP server for the emails, you will be prompted to configure one. Follow the prompts to the **Email** tab in the GUI to configure an SMTP server. Click **System** > **Settings** > **External Services** > **Destinations** > **Email**.

  - **Link**: The email notification of a successfully compiled report has a link back to itself and the **Generated Reports** page under **Reports**. You can view and download the report from this link and location.

    Note   Email notifications with embedded links to reports support up to 20 email addresses. To add multiple email addresses, you need to add each email address separately and press **Enter** (on your keyboard) after each addition. Cisco DNA Center platform validates the email addresses and notifies you if the syntax is incorrect.

  - **Attachment**: Report is attached to the email notification.

    Note   PDF reports support email notification attachments of up to 20-MB in size and up to 10 email addresses. To add multiple email addresses, you need to add each email address separately and press **Enter** (on your keyboard) after each addition. Cisco DNA Center platform validates the email addresses and notifies you if the syntax is incorrect.

  Cisco DNA Center sends the following email notifications for the report:

  - Report is in the queue waiting to be processed.

  - Report processing is in progress.

• Report has successfully been compiled and is completed.

• **Webhook Notification**: Notification is sent as a webhook to the configured webhook URL address (callback URL). Select a webhook from the drop-down list **(Subscription Profile** field).

Note	If you have not yet created a webhook, you will be prompted to create one. Follow the prompts to the **Webhook** tab in the GUI to configure a webhook. In general, to configure a webhook, click **System** > **Settings** > **External Services** > **Destinations** > **Webhook** tab.

You will receive status webhook notifications for the report. For example, you will receive "In Queue," "In Progress," and "Success" webhook notifications. You will also be able to view these notifications in the GUI.

Figure 115: Delivery and Notification

Click **Next**. The **Summary** window opens.

Step 12   In the **Summary** window, review the configuration and if necessary edit any of the files.

Figure 116: Summary

Click **Next**.

After the report is generated, a success window appears.

Step 13   Click the **View the Generated Reports** link.

The **Generated Reports** window opens with instance details of the report that was scheduled.

Figure 117: Generated Reports

What to do next

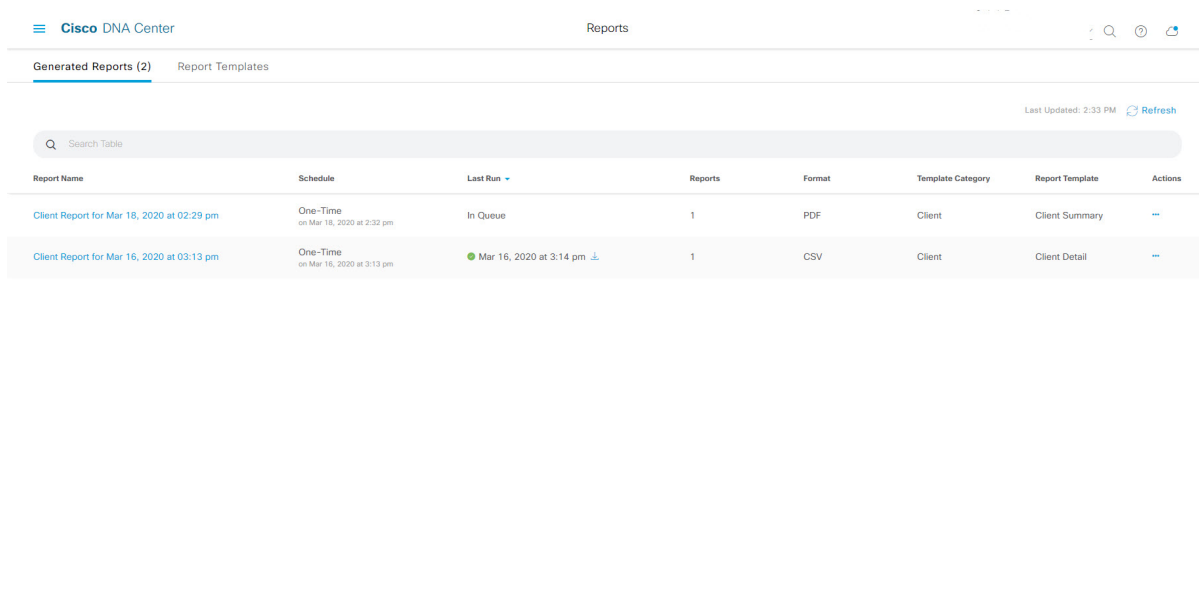Review your report instance in **Generated Reports** window.

Note	You can download, review, edit, duplicate, or delete the report in the **Generated Reports** window. For additional information, see View Generated Reports, on page 133.

Run a SWIM Report

Perform this procedure to configure **SWIM** reports about your network. You can configure **SWIM** reports using the **Reports** window in the Cisco DNA Center GUI.

Figure 118: SWIM Reports

Before you begin

Run a successful **Discovery** job in Cisco DNA Center. You can check whether a **Discovery** job is successful in **Device Inventory**. Click the menu icon (☰) and choose **Provision** > **Inventory** to view the results.

Step 1   Click the menu icon (☰) and choose **Reports** > **Report Templates**.

The **Report Templates** window opens and displays the supported reporting categories. A link represents each category. Click a link to view only the supported reports for that category.

For this release, reporting is supported for the following categories:

- **Access Point**: Reports that provide data about Access Points and Access Point Radios.

- **Client**: Reports that help with analyzing how the clients are performing in the network.

- **Executive Summary**: Report that helps with analyzing how devices, applications, and clients are performing in the network.

- **Inventory**: Report listing devices discovered by Cisco DNA Center.

- **Licensing**: Reports that lists devices that noncompliant devices and the reasons for noncompliance.

- **Network Devices**: Reports that provide data about the devices within your network.

- **Rogue and aWIPS**: Reports that provide data about threats within your network.

- **SWIM**: Report listing all the devices in network with software and versioning.

- **Security Advisories**: Report that provides Cisco security advisory information on the network devices.

Note The Access Point, Client, and Executive Summary reports support up to 90 days of data retention.

Step 2 After clicking a link, review the **Report Templates** window for that selected category.

Figure 119: Report Templates Window
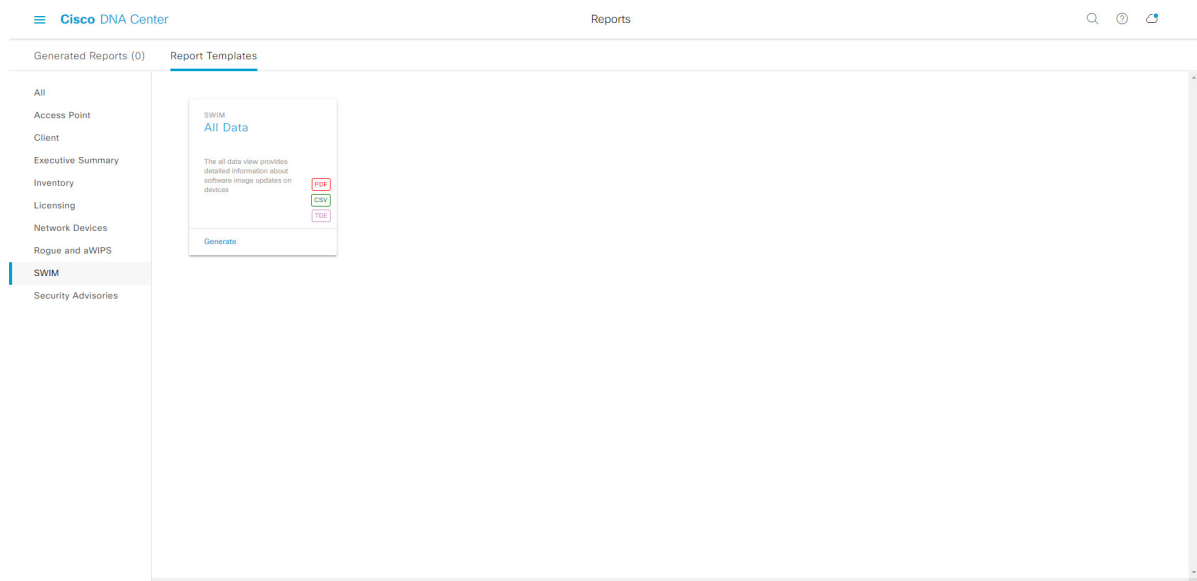
The **Report Templates** window displays supported report templates. Each template is represented by a tile and contains information about the report and links to configure (generate) a report. Determine which template you wish to use to generate a report. For example, for a **SWIM** report you can create an **All Data** report. Within the tile are also icons that represent the supported file types for the reports (PDF, CSV, or TDE).

Step 3 In the tile, click the header to view a sample report.

A window appears for the sample report. Use the side bar in the window to scroll down and review the entire sample report. The following data is presented:

- Applied filters (data filters that were used to build the report).

- Data metrics and summaries

- Tables that assist you in analyzing the data.

Note You can use the sample report to plan how you want your report to look.

Step 4 Click **X** to close the preview.

Step 5 In the tile, click the **Generate** link to configure parameters to build a report.

The **Generate** window opens where you can select a format type for the report, apply data filters for your reports, as well as set up schedules for the actual report generation.

Step 6 In the **Generate a New Report** window, click **Let's Do It** to get started.

Figure 120: Generate a New Report
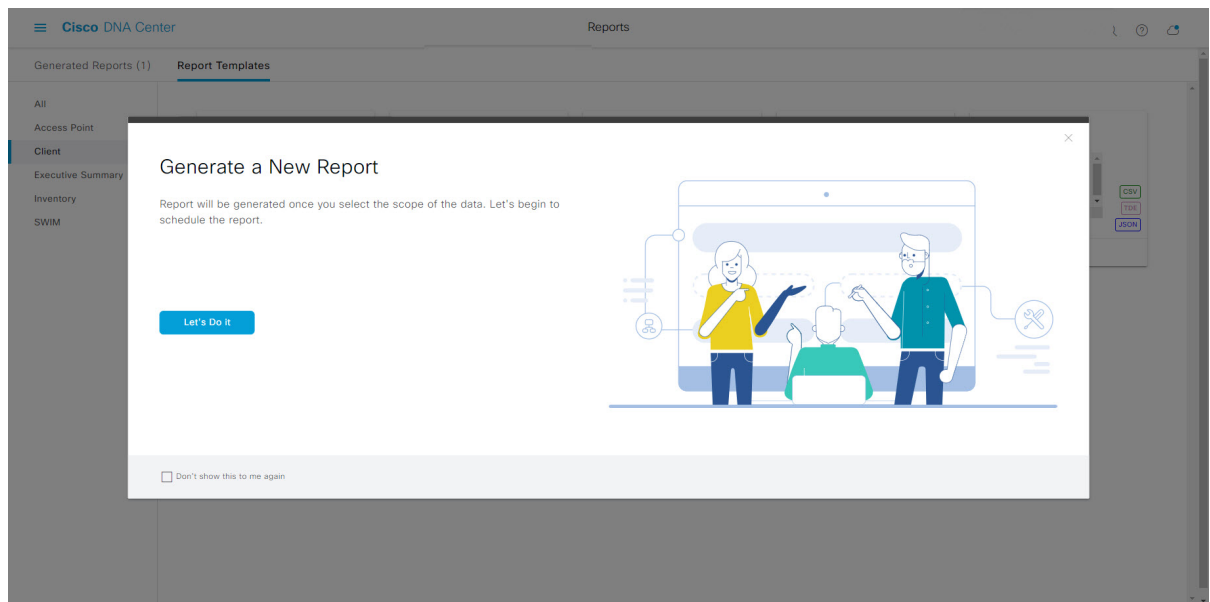
The **Select Report Template** window opens.

Step 7 In the **Select Report Template** window, select the template for the report.

Choose the **Template** from the drop-down lists.

Note The **Template** consists of the individual report types within the categories for the release.

You can review an autogenerated sample in the same window.

Figure 121: Setup Report Template

Click **Next**. The **Setup Report Scope** window opens.

Step 8 In the **Setup Report Scope** window, name the report and select the scope.

Enter a report name in the **Report Name** field and click in the **Scope** field to display the available filter. Click the filter options that you want for the report.

Note The **Setup Report Scope** options change depending upon the selected **Template**.

Figure 122: Setup Report Scope

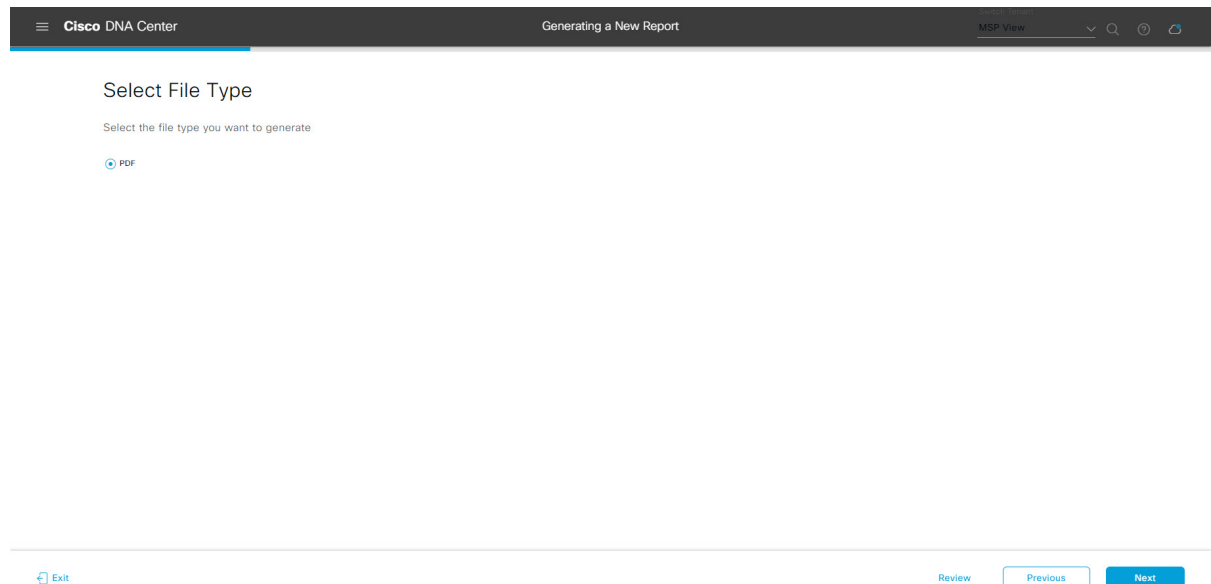Click **Next**. The **Select File Type** window opens.

Step 9 In the **Select File Type** window, select the file type for the report.

Depending upon the report that you are creating, the following **File Type** options may be available:

- **PDF**

- **CSV**

- **Tableau Data Extract**

- **JSON**

For the **CSV**, **JSON**, and **Tableau Data Extract** file types, a **Fields** option displays that permits you to select attributes (additional fields) for the CSV, JSON, and Tableau Data Extract results.

Figure 123: Select File Type

Click **Next**. The **Schedule Report** window opens.

Step 10 In the **Schedule Report** window, select the time range and schedule for the report.

The following **Time Range** options are available:

- **Last 3 hours**

- **Last 24 hours**

- **Last 7 days**

- **Custom**

Note Clicking **Custom** opens up fields where you can choose the date and time interval per the specific report type, as well as the time zone (GMT) for the time range.

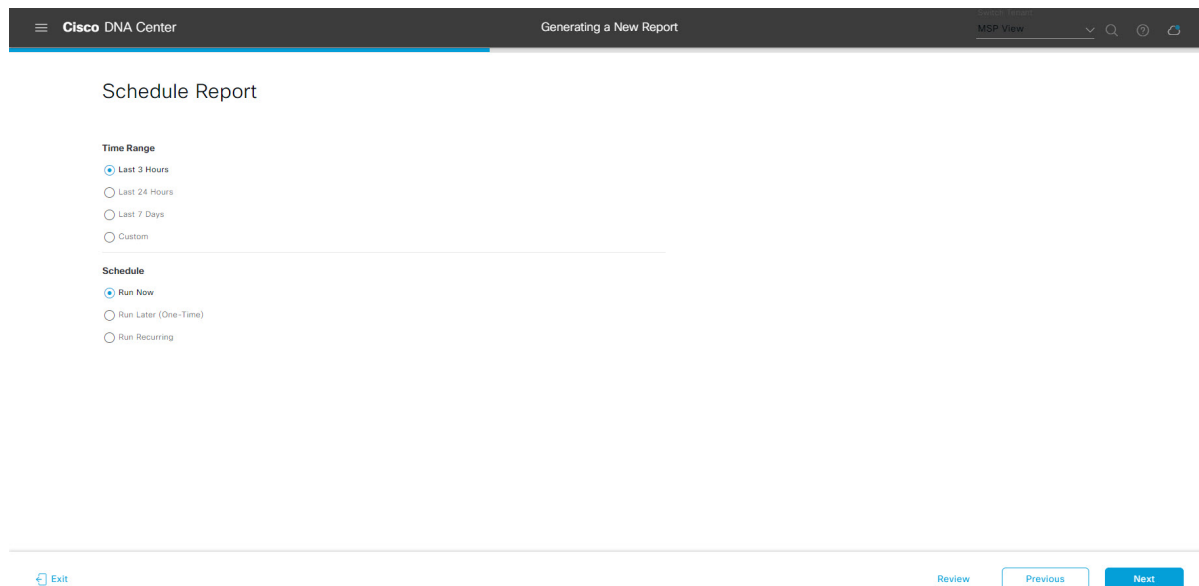The following **Schedule** options are available:

- **Run Now**

- **Run Later**

- **Run Recurring**

You can also select a time zone for the report when configuring with the following **Schedule** options:

- **Custom**

- **Run Later (One Time)**

- **Run Recurring**

Figure 124: Schedule Report

Click **Next**. The **Delivery and Notification** window opens.

Step 11   In the **Delivery and Notification** window, select the Delivery mechanism for the report.

The options include:

- **Email Report**: Email report is sent as a link or attachment.

  Note   If you have not yet configured an SMTP server for the emails, you will be prompted to configure one. Follow the prompts to the **Email** tab in the GUI to configure a SMTP server. Click **System** > **Settings** > **External Services** > **Destinations** > **Email**.

  - **Link**: The email notification of a successfully compiled report has a link back to itself and the **Generated Reports** page under **Reports**. You can view and download the report from this link and location.

    Note   Email notifications with embedded links to reports support up to 20 email addresses. To add multiple email addresses, you need to add each email address separately and press **Enter** (on your keyboard) after each addition. Cisco DNA Center platform validates the email addresses and notifies you if the syntax is incorrect.

  - **Attachment**: Report is attached to the email notification.

Note	PDF reports support email notification attachments of up to 20-MB in size and up to 10 email addresses. To add multiple email addresses, you need to add each email address separately and press **Enter** (on your keyboard) after each addition. Cisco DNA Center platform validates the email addresses and notifies you if the syntax is incorrect.

Cisco DNA Center sends the following email notifications for the report:

- Report is in the queue waiting to be processed.

- Report processing is in progress.

- Report has successfully been compiled and is completed.

- **Webhook Notification**: Notification is sent as a webhook to the configured webhook URL address (callback URL). Select a webhook from the drop-down list **(Subscription Profile** field).

Note	If you have not yet created a webhook, you will be prompted to create one. Follow the prompts to the **Webhook** tab in the GUI to configure a webhook. In general, to configure a webhook, click **System** > **Settings** > **External Services** > **Destinations** > **Webhook** tab.

You will receive status webhook notifications for the report. For example, you will receive "In Queue," "In Progress," and "Success" webhook notifications. You will also be able to view these notifications in the GUI.

Figure 125: Delivery and Notification

Click **Next**. The **Summary** window opens.

Step 12 In the **Summary** window, review the configuration and if necessary edit any of the files.

Figure 126: Summary

Click **Next**.

After the report is generated, a success window appears.

Step 13   Click the **View the Generated Reports** link.

The **Generated Reports** window opens with instance details of the report that was scheduled.

Figure 127: Generated Reports
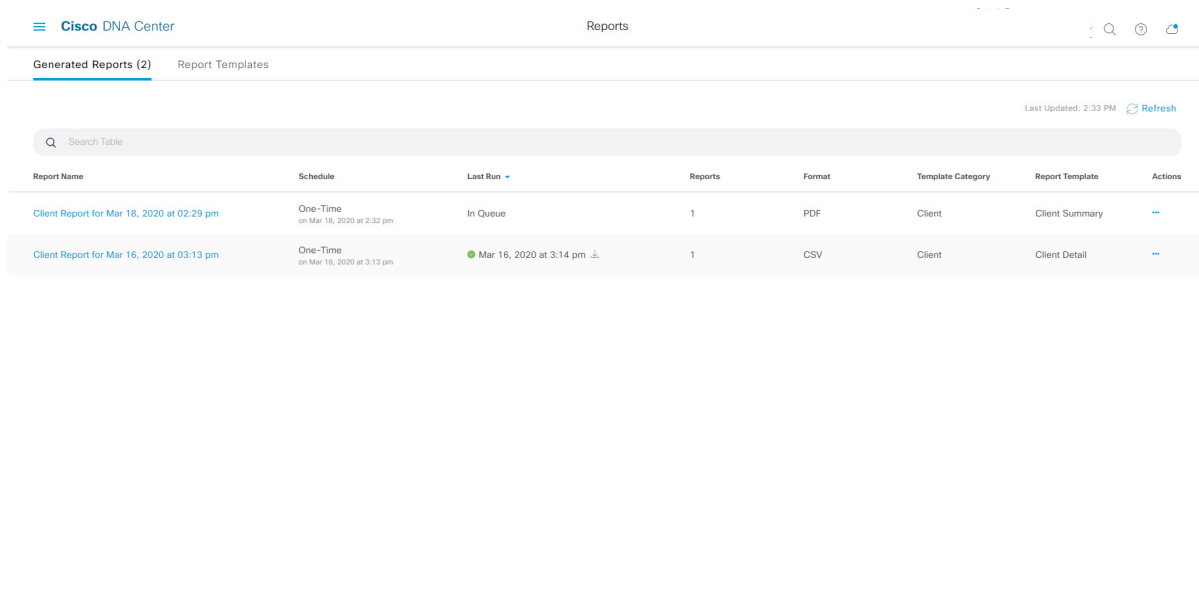
What to do next

Review your report instance in the **Generated Reports** window.

> **Note** You can download, review, edit, duplicate, or delete the report in the **Generated Reports** window. For additional information, see View Generated Reports, on page 133.

View Generated Reports

Perform this procedure to download, review, edit, duplicate, or delete a previously generated report.

Figure 128: Generated Reports

Before you begin

• Run a successful **Discovery** job in Cisco DNA Center. You can check whether a **Discovery** job is successful in **Device Inventory**. Click the menu icon (≡) and choose **Provision** > **Inventory** to view the results.

• Create a report using the **Schedule** functionality in the **Catalog**.

Step 1 Click the menu icon (≡) and choose **Reports**.

Step 2 Click the **Generated Reports** tab.

The following information is displayed:

• **Report Name**: Name of the report.

- If you did not give the report a name, a default name is given to the report that contains the report type with the date and time of the report.

  Note   With this release, the report name becomes a link that opens up a view of the report itself within the **Generated Reports** window. Also, there is a **Download** link that is provided to download a copy of the report.

- **Schedule**: One-time generated report or reoccurring report. Also, there is a brief description of the schedule that generated the report.

- **Last Run**: Displays report execution status and details. The following report execution status types may be displayed:

  - **Not Initiated**: Report scheduled but not yet started.

  - **In Queue**: Report scheduled and in the processing queue to be executed.

  - **In Progress**: Report currently being executed.

  - **Completed**: Report execution completed displaying the date and time.

    Clicking on the icon (downward pointing arrow) downloads the last generated report.

  - **Expired**: Report expired and no longer available in Cisco DNA Center.

  - **Error**: Report execution failed.

- **Reports**: Number of reports up to a total of 7.

  Hover (mouse) over the displayed report number and **View Report List** appears. Click **View Report List** to display a reports dialog box. The reports dialog box lists all the report executions, their status (**Not Initiated**, **In Queue**, **In Progress**, **Completed**, **Expired**, and **Error**) and a **Download** button to download a copy. Clicking **Error** displays any errors and warnings for the report execution.

  Important   Cisco DNA Center retains a total of 7 reports. Specifically, Cisco DNA Center retains the last 7 reports that are executed, as well as the last 7 reports executed over the last 7 days (week). For example, if you run 8 reports in a single day, Cisco DNA Center will only retain the last 7 reports. If you schedule 1 report for each day, Cisco DNA Center will only keep the most recent 7 reports over the last 7 days (week). You can also export the reports in their various formats from the Cisco DNA Center and archive them to a safe location.

- **Format**: File format type, for example a PDF or CSV file format.

- **Template Category**: Type of report based on the catalog options (Client, Executive Summary, SWIM, or Inventory).

- **Report Template**: Template used when generating the report.

- **Actions**: List of tasks you can perform with the reports.

You can adjust the downloads that are displayed in the GUI by clicking the **Filter** icon and using the filter, or entering a keyword in the **Find** field.

Step 3   Click **Actions** to perform one or more of the following tasks:

- **View Config**: Opens a window where the configured parameters for the report are displayed (including the schedule). You can review the configured report parameters in this window. You cannot make any changes to the report configuration in this window. This is a read-only view. If you must edit the configuration, click **Edit**. You can both view and edit a report configuration by clicking **Edit**.

- **Edit**: Opens a window where configured parameters for the report are displayed (including the schedule). You can review the parameters and also edit them in this window. Click **Save** after making any edits to the report.

Important	After you edit and update the report configuration, any future report executions reflect this new configuration. This is important if reports are being generated on a reoccurring schedule. Also, if you edit and update a report configuration, all the previous reports in Cisco DNA Center will be deleted. The GUI displays a warning about the deletion when clicking the **Save** button in the window. You do not have to make any edits in the configuration to click the **Save** button and delete all previous reports.

- **Duplicate**: Opens the **Duplicate** window where you can either view or configure the parameters for the report. Click **Generate Report** to generate the report again.

Note	If you want to create a new report based on an existing report and its configuration, use the **Duplicate** option and make changes to the configuration. This permits you to create a new report similar to the existing one, while retaining the existing report and its configuration. If you want to discard the existing report and completely replace it with a new report, use the **View Config** and **Edit** options as described previously.

- **Run Now**: Starts the process to execute the report. A Success message appears after a successful report execution.

Note	If you try to execute a report and there are seven previous reports, the GUI displays a warning that only the last seven reports are saved. You use the **Run Now** option when you must generate a report outside of an existing schedule for the reports.

- **Delete**: Deletes the report. You are prompted to confirm that this action before the report is deleted.

Developer Toolkit GUI

About Developer Toolkit

The Cisco DNA Center platform provides you with the following software developer tools to access and program with Cisco DNA Center, as well as to integrate Cisco DNA Center with other applications:

- **APIs**: Available APIs organized within categories by functionality (for example, **Operational Tasks** or **Site Management** APIs).

- **Integration Flows**: Available integration flows organized by category type. Currently, only IT Service Management (ITSM) is available.

- **Events**: Provides a window to view and subscribe to specific events that may occur in your network.

Work with APIs

Perform this procedure to review available APIs, generate example code for using the APIs, and try out the APIs interactively on the Cisco DNA Center platform. You accomplish these tasks using the **APIs** window in the Cisco DNA Center GUI.

Figure 129: Cisco DNA Center Platform APIs Window

The Cisco DNA Center GUI displays documentation about each API call, including the request method and URL, query parameters, request header parameters, responses, and schema, and ways to preview or test the request.

Before you begin

- Ensure that you have met the supported programming language and authentication prerequisites, as described in the previous section. For more information, see API Prerequisites, on page 7.

- You must first enable the **Rogue and aWIPS** bundle to view these specific APIs. Click the menu icon (≡) and choose **Platform** > **Manage** > **Bundles** > **Rogue and aWIPS** > **Enable**. After enabling this bundle, you can view the APIs within the bundle under the **Contents** tab, or choose **Platform** > **Developer Toolkit** > **APIs** > **Know Your Network** > **Devices**.

Step 1   Click the menu icon (≡) and choose **Platform** > **Developer Toolkit** > **APIs**.

Step 2   Review the APIs displayed by the GUI.

At any point in time, you will see a list of supported APIs for your release version.

If necessary, click the **>** icon to display the API subdomains.

Step 3   Choose an API from the domains and subdomains.

> **Note**   The APIs are organized based on the Cisco DNA Center platform as a platform capabilities model. For example, APIs are grouped as **Authentication**, **Know Your Network**, **Site Management**, **Connectivity**, **Operational Tools**, **Policy**, **Event Management**, and **Ecosystem Integrations**.

After choosing an API, the following information is displayed in columns:

- **Method**: Supported methods include GET, POST, PUT, and DELETE.

- **Name**: Link to access the slide-in pane and additional information, including description, features, tags, parameters, responses, model schemas, and so on.

- **Description**: Brief description of method.

- **URL**: URL value for the method.

- Icon (**...**): Accesses links to create a code preview snippet or **Try It** option.

Note   A blue color-coded message may appear stating that the specific API configuration is still in progress and to check back at a later time. The screen will auto refresh when the API is registered and you may proceed with your API activity. In the highly unlikely event that a red color-coded message appears stating that the API cannot be configured, contact your Cisco DNA Center administrator to contact Cisco for assistance in resolving the issue.

Step 4   Click the name (link) of an API method.

The following information about the API method is displayed:

- **DESCRIPTION**: Brief description of API.

- **FEATURES**: Method and URL information.

- **TAGS**: API identifiers, including where and under what circumstances you would use the API. Note that some APIs may not have tags.

- **PARAMETERS**: Parameters of API, including description, data type (Boolean or string), default value, and required value.

- **RESPONSES**: Possible HTTP responses.

- **MODEL SCHEMAS**: Presents response as a data model (**Model** tab) or JSON format of the actual response (**Model Schema** tab). Sample code is available from the **Code Preview** button.

- **POLICIES**: An API rate limiting feature, where policies are applied to certain APIs. These policies set the number of API calls per time interval per client IP address.

Step 5   (Optional) Generate a code preview by clicking **Code Preview**.

Note   If you are creating your own program, you can cut and paste the code preview sample into your own program.

Step 6   (Optional) In the **Code Preview** window, choose a language from the drop-down to generate the code.

The following languages are supported:

- **Shell**

- **Node - HTTP**

- **Node - Unirest**

- **Node - Request**

- **Python**

- **Ruby**

- **JavaScript**

> • **JQuery**
>
> • **PHP**
>
> • **Go**
>
> • **Ansible**

After reviewing or copying the code preview sample for use, click **Close**.

Step 7   (Optional) Try the method by clicking **Try It**.

Step 8   (Optional) In the **Try It** window, fill in the requested values (for example, URL address or value) and click **Run**.

After reviewing the response and/or error code, click **Close**.

When Cisco DNA Center returns a 202 (Accepted) HTTP status code, the result body includes a task ID and a URL that you can use to query for more information about the asynchronous task that your original request spawned. For example, you can use this information to determine whether a lengthy task has completed. For more information, see Getting Information about Asynchronous Operations.

Note   The response is a live response from Cisco DNA Center itself, and the results reflect the actual state of your network. In contrast, the code previews are static and contain placeholders for values that you must supply.

Work with Integration Flows

An integration flow defines the interaction between Cisco DNA Center platform and a third-party system, such as an ITSM system that is used to track, troubleshoot, and resolve network issues.

Cisco DNA Center platform supports schedule-based integration flows. This type of integration flow runs on a schedule, performs a task, and pushes the information to a REST endpoint or other vendor-specific destination. Schedule-based integration flows can be edited in the GUI using the **Integration Flows** window to specify the schedule on which they execute.

Note   The integration flows available in the **Developer Toolkit** are used by various bundles in **Manage** > **Bundles**. Bundles are used to integrate your own applications with Cisco DNA Center or to enhance the performance of Cisco DNA Center itself. You can view the integration flows used in a bundle by clicking the bundle in **Manage** and clicking the **Contents** tab. Integration flows for the bundle are listed under the **Contents** tab.

Figure 130: Cisco DNA Center Platform Integration Flows Window

Before you begin

Ensure that you have enabled and scheduled the integration flows that you will review and manage in the **Integration Flows** window.

Note   Before you can view and manage integration flows in the **Integration Flows** window, you must enable them. You enable integration flows from the individual bundles in the Cisco DNA Center platform. For example, click the menu icon (☰) and choose **Platform** > **Developer Toolkit** > **Manage** > **Bundles** > **Basic ITSM (ServiceNow) CMDB synchronization**. Click the **Contents** tab and then click **Enable**.

Step 1   Click the menu icon (☰) and choose **Platform** > **Developer Toolkit** > **Integration Flows**.

Step 2   Review the integration flows displayed by the GUI.

   Note   Available integration flows are organized by group. For this release, the only group available is ITSM Integration.

Step 3   Choose an integration flow from the ITSM Integration group.

The following information is displayed:

   • **Name**: Name of the integration flow and link to access a slide-in pane where additional information is available.

   If the integration flow is a REST based trigger type, after you click the integration flow name additional data such as description, tags, parameters, responses, model schemas, and policies appear.

   If the integration flow is a schedule based trigger type, after you click the integration flow name a slide-in pane for setting the schedule appears. This slide-in pane displays **DESCRIPTION**, **TAGS**, and **HOW TO USE THIS FLOW** content.

- **Description**: Brief description of integration flow.

- **Trigger**: REST-based or Schedule based.

- Icon (**…**): Accesses links to create a code preview or the **Try It** option. If the integration flow is schedule based, this icon accesses a **Schedule Flow** option.

Step 4   For a REST-based integration flow, click on the name (link) of the integration flow.

A slide-in pane opens with details about the REST-based integration flow, You can review the details and then close the slide-in pane.

Step 5   For a REST-based integration flow, generate a code preview snippet by mousing over the Icon (**…**) and clicking **Generate Code Preview**.

These choices appear only for REST-based triggered integration flows. Schedule based integration flows provide a Schedule Flow menu item on hover.

Step 6   In the **Code Preview** window, choose a programming language from the drop-down to generate the code.

After reviewing or copying the code for use, click **Close**.

Step 7   To try a REST request path interactively, mouse over the Icon (**…**) and click **Try It**.

Step 8   In the **Try It** window, fill in the requested values (for example, URL address or value) and click **Run**.

After trying the method, review the response and/or error code within the **Try It** window, and click **Close**.

When Cisco DNA Center returns a 202 (Accepted) HTTP status code, the result body includes a task ID and a URL that you can use to query for more information about the asynchronous task that your original request spawned. For example, you can use this information to determine whether a lengthy task has completed. For more information, see Getting Information about Asynchronous Operations.

Note   For responses, Cisco DNA Center APIs use a task-based response architecture so that multiple requests and responses can be sent concurrently. Therefore, all PUT, POST, and DELETE requests have a task-based response. To view more details about the response, send a GET request to the task URL (either from a script or as a URL). For error codes, the Cisco DNA Center APIs follow the standard HTTP status codes.

Step 9   For the schedule based integration flow, mouse over the Icon (**…**) and click **Schedule Flow**.

Step 10   Review the following displayed data:

- **DESCRIPTION**: Description and purpose of integration flow.

- **TAGS**: Tags indicate what the Cisco DNA Center component is used for or affected by the bundle.

- **HOW TO USE THIS FLOW**: Schedule configuration options.

You can schedule the integration flow using the GUI.

Step 11   Configure a schedule for the integration flow using the following GUI options:

- **Run Now**: Choose **Run Now** and then click the **Schedule** button to run the integration flow.

- **Run Later**: Choose **Run Later** and then enter a date, time, and time zone. Click the **Schedule** button to run the integration flow at the specified date, time, and time zone.

- **Recurring**: Choose **Recurring** and then configure the following options:

    - **Repeats**: Choose daily or weekly repeating occurrences for the integration flow

• **Run at Interval**: Set the time interval between integration flows.

• **Set Schedule Start**: Set a start date.

• **Set Schedule End**: Set an end date.

Click the **Schedule** button to run the integration at the configured times.

Work with Event Notifications

You can associate a notification to specific events that may occur in your network. After the notification is associated with event and even if the event does occur, you receive a notification by REST API or email. You associate a notification to an event by using the **Events Notifications** window in the Cisco DNA Center platform GUI.

Before you begin

• For a REST API notification, you configured the webhook destination in the **Webhook** tab in Cisco DNA Center. To access the **Webhook** tab, click the menu icon (☰) and choose **System** > **Settings** > **External Services** > **Destinations** > **Webhook**. For detailed information about configuring a webhook destination, see Configure a Webhook Destination, on page 39.

• For email notification of events, you configured the email destination in the **Email** tab in Cisco DNA Center. To access the **Email** tab, click the menu icon (☰) and choose **System** > **Settings** > **External Services** > **Destinations** > **Email**. For detailed information about configuring an email destination, see Configure an Email Destination, on page 42.

• For a syslog server notification of events, you configured the syslog server destination in the **Syslog** tab in Cisco DNA Center. To access the **Syslog** tab, click the menu icon (☰) and choose **System** > **Settings** > **External Services** > **Destinations** > **Syslog**. For detailed information about configuring a syslog server destination, see Configure a Syslog Server Destination, on page 44.

• For an SNMP trap notification of events, you configured the SNMP trap destination in the **Trap** tab in Cisco DNA Center. To access the **Trap** tab, click the menu icon (☰) and choose **System** > **Settings** > **External Services** > **Destinations** > **Trap**. For detailed information about configuring a trap destination, see Configure a Trap Notification, on page 46.

• You have accessed the **Event Settings** window and reviewed or edited the list of events that may occur within your network for ITSM integration and can be captured by Cisco DNA Center. To access the **Event Settings** window, click the menu icon (☰) and choose **Platform** > **Manage** > **Configurations** > **Event Settings**.

Step 1   Click the menu icon (☰) and choose **Platform** > **Developer Toolkit** > **Event Notifications**.

The **Events Notifications** window appears.

Step 2   Click the **Notifications** tab to view the notification tiles.

Each notification is represented by a tile and contains link to view notification details.

Step 3 From the **CHANNELS** area in the left pane, click the radio button next to the channels for which you want to view the respective notification tiles.

The supported channels are **REST**, **PAGERDUTY**, **SNMP**, **SYSLOG**, **WEBEX** and **EMAIL**.

Note	• You must create a notification for an event with respective channels and trigger the notification. For more information, see **Create an Event Notification** in the Cisco DNA Center User Guide.
	• One event notification supports more than one channel.

Step 4 Click a notification tile link for which you want to view the notification details.

The **Notification Details** slide in pane displays the following notification details based on the selected channel:

- **Name**: Name of the event.

- **Description**: Event description

- **Sites**

- **Events**

- **REST**: Appears only when you want to view REST notification details. The **REST** area shows the following information:

    - **URL**: URL address of the REST API endpoint that event will be sent to.

    - **Method**: Either the PUT or POST method.

    - **Trust certificate**: Whether a trust certificate is required for REST API endpoint notification.

    - **Headers**: The **Header Name** and **Header Value**.

- **PAGERDUTY**: Appears only when you want to view PAGERDUTY notification details. The **PAGERDUTY** area shows the following information:

    - PagerDuty Events API URL

    - PagerDuty Integration Key

    - PagerDuty Events API Version

- **SNMP**: Appears only when you want to view **SNMP** notification details.

- **SYSLOG**: Appears only when you want to view **SYSLOG** notification details.

- **WEBEX**: Appears only when you want to view **WEBEX** notification details.

- **EMAIL**: Appears only when you want to view **EMAIL** notification details. The **EMAIL** area shows the email recipients **From** and **To** along with email **Subject**.

Step 5 In the **Notification Details** slide-in pane, click the toggle button at the top-right corner to enable or disable the respective notification.

Step 6 To edit a particular notification, click the **Actions** drop-down list and choose **Edit**.

Step 7 In the **EDIT NOTIFICATION** window, configure the following based on the selected channel:

    a. In the **Name** name field, enter a unique name.

    b. In the **Description** name field, enter the description of respective event.

    c. Expand the **Site and Events** and choose a site from the Select a site drop-down list.

    d. Click the plus icon next to an event, or click **Add All** to add all the events to the respective notification.

    e. To remove an event from the notification, click the cross icon next to an event that you want to remove, or click **Remove All** to remove all events from the respective notification.

    f. Expand **Configuration** to edit the configuration of the selected notification channel.

        To specify the details in the **Configuration** area, see **Create an Event Notification** in the Cisco DNA Center User Guide.

        Note In the **Configuration** area, the fields shown depend on the type of selected notification channel.

Step 8 Click the toggle button at the top-right corner to toggle between the tile view and list view.

Step 9 Click the **Event Catalog** tab to view the list of created events.

    Note You can adjust the events that are displayed by entering a keyword in the **Find** field.

Step 10 Review the data on an individual event within the table.

The following **Event Details** tab data is displayed:

- **Description**: Brief description of the event and how it is triggered.

- **Event ID**: Identification number of the event.

- **Version**: Version number of the event.

- **Namespace**: Namespace of the event.

- **Severity**: 1 through 5.

    Note Severity 1 is the most important or critical priority and should be assigned for this type of an event.

- **Domain**: REST API domain to which the event belongs.

- **Sub Domain**: Subgroup under the REST API domain to which the event belongs.

- **Category**: Error, Warn, Info, Alert, Task Progress, Task Complete.

- **Note**: Additional information about the event or to assist in further understanding the event.

- **Event Link**: Event broadcast using REST URL.

- **Tags**: Tags indicate what Cisco DNA Center component is affected by the event. The default value for tags for this release is ASSURANCE with additional syntax for the specific Assurance issue.

- **Supported Endpoints**: What endpoint types are supported for the event notifications (email, REST API, or SNMP trap, and webex).

- **Model Schema**: Presents model schema about the event:

  - **Details**: Example of model schema detail for the event.

  - **REST Schema**: REST schema format for the event.

Step 11   Click the **Notifications** tab to view the active notification associated to respective event.

When you associate a notification to an event, a **Try-It Now** button appears in the **Event Catalog** tab. To run an event notification simulation, click **Try-It Now**. For information, Work with Event Notification Simulations.

Work with Event Notification Simulations

Cisco DNA Center platform supports event simulation, which lets you test an event's subscription (email, REST API, SNMP trap notification, syslog server, or Webex). After running an event simulation, the results (success or failure) are displayed in the GUI.

Before you begin

- For a syslog server notification of events, you configured the syslog server destination in the **Syslog** tab in Cisco DNA Center. To access the **Syslog** tab, click the menu icon (☰) and choose **System** > **Settings** > **External Services** > **Destinations** > **Syslog**. For detailed information about configuring a syslog server destination, see Configure a Syslog Server Destination, on page 44.

- For an email notification, you configured the email destination in the **Email** tab in Cisco DNA Center. To access the **Email** tab, click the menu icon (☰) and choose **System** > **Settings** > **External Services** > **Destinations** > **Email**. For detailed information about configuring an email destination, see Configure an Email Destination, on page 42.

- For a REST API notification, you configured the webhook destination in the **Webhook** tab in Cisco DNA Center. To access the **Webhook** tab, click the menu icon (☰) and choose **System** > **Settings** > **External Services** > **Destinations** > **Webhook**. For detailed information about configuring a webhook destination, see Configure a Webhook Destination, on page 39.

- You have accessed the **Event Settings** window and reviewed or edited the list of events that may occur within your network for ITSM integration and can be captured by Cisco DNA Center. To access the **Event Settings** window, click the menu icon (☰) and choose **Platform** > **Manage** > **Configurations** > **Event Settings**.

Step 1   Click the menu icon (☰) and choose **Platform** > **Developer Toolkit** > **Event Notifications**.

Step 2   In the **Event Notifications** window, review the events table that is displayed.

Note   You can adjust the events that are displayed by entering a keyword in the **Find** field.

Step 3   In the **Event Catalog** tab, click an event. The slide-in pane shows a **Try-It Now** button if Cisco DNA Center is subscribed to that event. Click **Try-It Now**.

The following data is displayed; you can edit only the **Details** field:

- **Event Name**: Cisco DNA Center system name for the event.

- **Event ID**: Identification number of the event.

- **Instance ID**: Identification number of the event's instance.

- **Name**: Name of the event.

- **Description**: Brief description of the event and how it is triggered.

- **Namespace**: Namespace of the event.

  For this release, the default value for all events is ASSURANCE.

- **Context**: Event context field.

  The default value is EXTERNAL.

- **Source**: Source field.

  The default value is EXTERNAL.

- **Type**: **Network**, **App**, **System**, **Security**, or **Integrations** type of event.

- **Category**: **Error**, **Warn**, **Info**, **Alert**, **Task Progress**, **Task Complete**.

- **Severity**: 1 through 5.

- **Domain**: REST API domain to which the event belongs.

- **Sub Domain**: Subgroup under the REST API domain to which the event belongs.

- **Details**: Field for additional user detail about the event.

Step 4   Click **X** to exit from the field.

Step 5   Click **Publish** to run the event simulation and review results.

The following results are displayed:

- **Subscription Name**: User-created subscription name.

- **Connector Type**: Email, REST API, SNMP trap, or Syslog.

- **Status**: Loading, Success, or Fail.

- **Message**: For a REST connector type (REST API subscription), an HTTPS response appears.

Runtime Dashboard

About Runtime Dashboard

The **Runtime Dashboard** provides you with a quick review of the following summaries:

- **API Summary**: Summary of recent API calls, results, and performances. Click **View Details** to open a slide-in pane with information about individual API call counts and call durations.

 The **Runtime Dashboard** only displays data from a Cisco DNA Center-to-ServiceNow API integration.

- **Event Summary**: Cisco DNA Center events involving REST endpoints or integration flows. Click an event name (link) to open a slide-in pane with additional detailed event information.

- **CMDB Synchronization Summary**: Summary that displays the Configuration Management Database (CMDB) synchronization status of devices selected from **Inventory**.

- **Integration Flow Summary**: Summary of integration flow instances, results, and performances. Click the appropriate tab to view additional detailed information about either the REST-based or schedule-based integration flows.

Review the Event Summary

Perform this procedure to review the Cisco DNA Center platform **Event Summary**. The **Event Summary** displays the total number of events published to external systems, based on the type of event. You can use the **Event Summary** to assist in monitoring and troubleshooting the Cisco DNA Center platform and its integration with other systems.

You review the **Event Summary** in the **Runtime Dashboard** window in the Cisco DNA Center GUI.

*Figure 131: Cisco DNA Center Platform Runtime Dashboard Window*
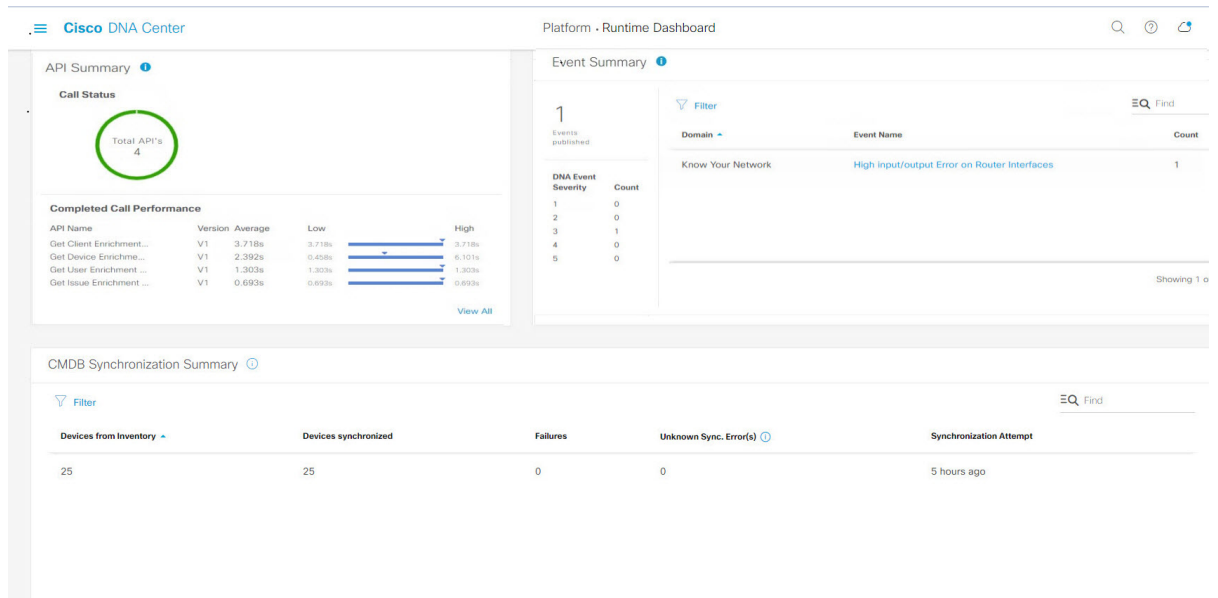
Before you begin

For the **Event Summary** field to display events, you need to enable, configure, and activate the bundles in **Bundles**. Additionally, you need to enable associated event notifications for the bundles in **Event Settings**. For information about **Bundles**, see Bundle Features, on page 14. For information about **Event Settings**, see Configure Event Settings, on page 33.

Step 1 Click the menu icon ( ) and choose **Platform** > **Runtime Dashboard**.

Step 2 Choose a time interval for the event summary by clicking on **Last 1 Week** at the upper right side of the GUI menu bar.

You can view the event summary for the last 6, 12, and 24 hour period or for the week.

Step 3 Review the **Event Summary** field in the **Runtime Dashboard** window.

Figure 132: Events Summary Field
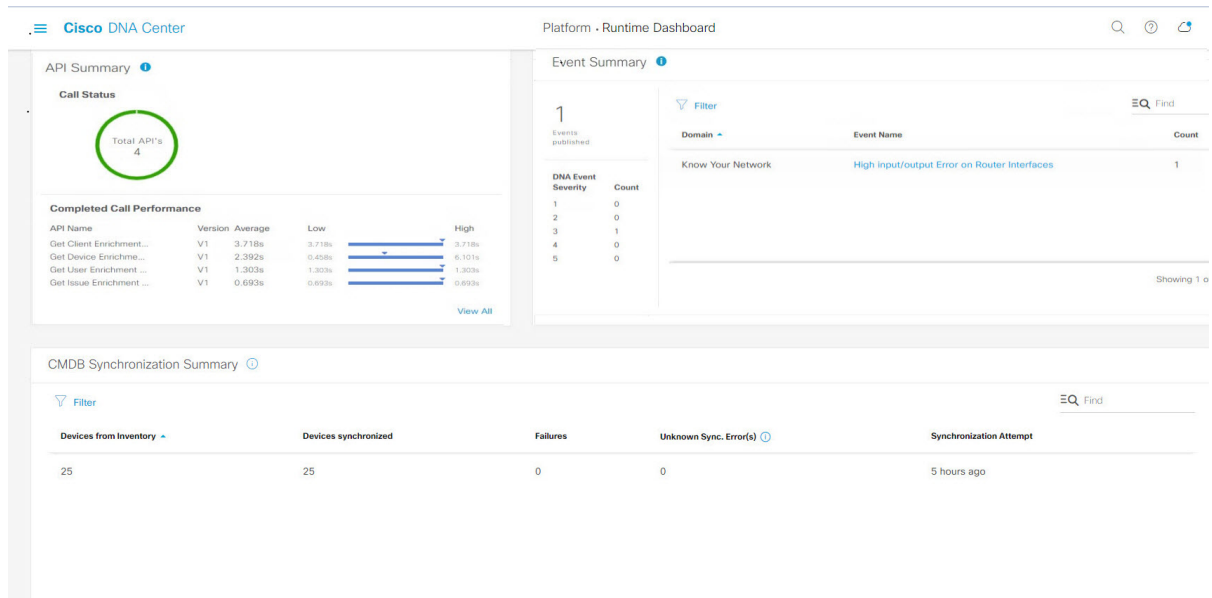
The following information is displayed for any current events:

- **Events Published**: Total number of events that are captured and published (displayed in the GUI) by the Cisco DNA Center platform.

- **Event Severity**: Event totals by severity number (1 through 5).

- **Count**: Number of events.

- **Events**: List of events by domain (category), event name (links), and count (number of events).

Note   Scroll down to view the entire list by using the scroll bar at the right of the field.

Step 4   Click an event name (link) to view additional detailed data.

As an example, if the events **Router Unreachable** or **BGP Tunnel Connectivity** exist in your GUI window click the link.

After clicking an event name (link), a slide-in pane opens.

Step 5   Review a list of this type of event (history) in the slide-in pane.

Figure 133: Event History
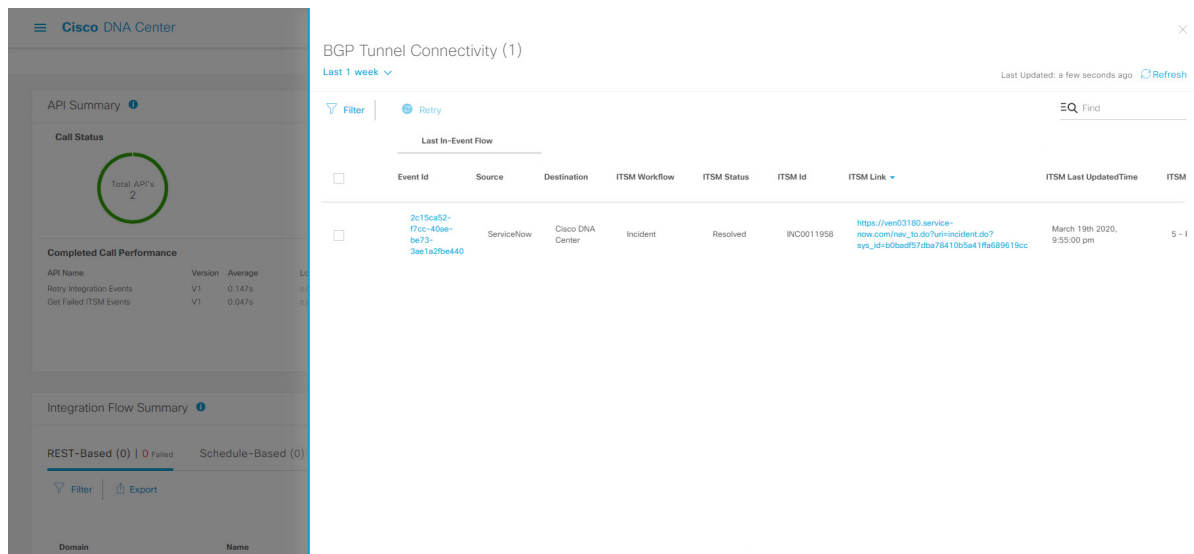
Individual events are listed displaying the following information:

- **Event ID**: Cisco DNA Center event identification number generated by Cisco DNA Center .

- **Source**: Location from where event originated. For example, the Cisco DNA Center platform (DNACP) or an ITSM system (ServiceNow).

- **Destination**: Location for where the event was directed to. For example, the Cisco DNA Center platform (Cisco DNA Center) or an ITSM system (ServiceNow).

- **ITSM Workflow**: Type of ITSM workflow (for example, an **Incident** or **Problem**).

- **ITSM Status**: Current status of the event. For example, an event can have a status of **Open**, **New**, **Closed**, or **N/A**.

- **ITSM ID**: ITSM event identification number generated by the ITSM (ServiceNow).

- **ITSM Link**: Link to ITSM server for the ITSM event.

- **ITSM Last Updated Time**: Last date and time of event update.

- **ITSM Entity Severity/Priority**: ITSM severity or priority assigned to the event.

- **Event Severity**: Cisco DNA Center severity assigned to the event (1 through 5).

You can adjust the events that are displayed in the table by clicking the **Filter** icon and using the filter, or by entering a keyword in the **Find** field.

Step 6 Click an event ID number (link) to view only data associated with that specific event.

After clicking an event ID number (link), a slide-in pane opens.

Step 7 Review the event ID data in the slide-in pane.

Figure 134: Event ID Data

The following information is displayed about that single event:

- **Source**: Location from where event originated (for example, the Cisco DNA Center platform or DNACP).

- **Destination**: Location for where the event was directed to. For example, the REST Endpoint.

- **ITSM Workflow**: Type of ITSM workflow (for example, an **Incident** or **Problem**).

- **ITSM Status**: Current status of the event. For example, an event can have a status of **Open**, **New**, or **Resolved**.

- **ITSM ID**: ITSM event identification number.

- **ITSM Link**: Link to the ITSM (ServiceNow).

- **ITSM Last Updated Time**: Last date and time of event update.

- **ITSM Entity Severity/Priority**: ITSM severity or priority assigned to the event.

- **Event Severity**: Cisco DNA Center severity assigned to the event (1 through 5).

To close the slide-in pane and return to the previous window, click the event link at the top left of the window.

To close the slide-in pane in the new window and return to the **Runtime Dashboard**, click the link at the top left again.

Step 8 (Optional) Click the **ITSM Link** to open up and access the ITSM program (ServiceNow Service Management GUI) and specific incident.

Figure 135: ServiceNow Incident

> **Note** For the **Runtime** event link to ITSM program to be operational, you must follow the procedures to set up the Cisco DNA Center platform to ServiceNow integration as described in the *Cisco DNA Center ITSM Integration Guide*.

Step 9 (Optional) Click the **Cisco DNA** tab in the ServiceNow Service Management GUI to review details about the event.

Figure 136: Cisco DNA Tab

The following information is available from the **Cisco DNA** tab:

- **Cisco DNA Network UserID**

- **Cisco 360 View**

- **Cisco DNA Network Details**

> • **Cisco DNA Event Domain**
>
> • **Cisco DNA Event Details and Suggested Actions**
>
> • **Cisco DNA Event ID**
>
> • **Approval Status**

What to do next

Review the additional Cisco DNA Center platform data displayed in the **Runtime Dashboard**.

Retry an ITSM Event

You can retry (resend and reprocess) an ITSM event from the Cisco DNA Center platform to an ITSM (ServiceNow). You retry an individual ITSM event in the **Event Summary** fields of the Cisco DNA Center GUI.

Figure 137: Retry Icon Within ITSM Event

The **Event Summary** window in **Runtime Dashboard** displays the total number of events that are published to external systems, based on the type of event. You use the **Event Summary** to help monitoring and troubleshooting the Cisco DNA Center platform and its integration with other systems.

Before you begin

For the **Event Summary** field to display events, you must enable, configure, and activate the bundles in **Bundles**. Also, you must enable associated event notifications for the bundles in **Event Settings**.

Step 1 Click the menu icon (☰) and choose **Platform** > **Runtime Dashboard**.

Step 2 Choose a time interval for the event summary by clicking **Last 1 Week** at the upper right side of the GUI menu bar.

You can view the event summary for the last 6, 12, and 24-hour period or for the week.

Step 3   Review the **Event Summary** field in the **Runtime Dashboard** window.

The following information is displayed for any current events:

- **Events Published**: Total number of events that are captured and published (displayed in the GUI) by the Cisco DNA Center platform.

- **Event Severity**: Event totals by severity number (1–5).

- **Count**: Number of events.

- **Events**: List of events by domain (category), event name (links), and count (number of events).

Note   Scroll down to view the entire list by using the scroll bar at the right of the field.

Step 4   Click an ITSM event name (link) to view more detailed data.

As an example, if the ITSM event **SWIM Upgrade Request Creation Image Activation** exists in your GUI window click the link.

After clicking an event name (link), a slide-in pane opens.

Step 5   Review a list of this type of event (history) in the slide-in pane.

Figure 138: Event History

Individual events are listed displaying the following information:

- **Event ID**: Cisco DNA Center event identification number generated by Cisco DNA Center .

- **Source**: Location from where event originated. For example, the Cisco DNA Center platform (DNACP) or an ITSM system (ServiceNow).

- **Destination**: Location for where the event was directed to. For example, the Cisco DNA Center platform (Cisco DNA Center) or an ITSM system (ServiceNow).

- **ITSM Workflow**: Type of ITSM workflow (for example, an **Incident** or **Problem**).

- **ITSM Status**: Current status of the event. For example, an event can have a status of **Open**, **New**, **Closed**, **N/A** or, **Resolved**.

- **ITSM ID**: ITSM event identification number generated by the ITSM (ServiceNow).

- **ITSM Link**: Link to ITSM server for the ITSM event.

- **ITSM Last Updated Time**: Last date and time of event update.

- **ITSM Entity Severity/Priority**: ITSM severity or priority that is assigned to the event.

- **Event Severity**: Cisco DNA Center severity that is assigned to the event (1–5).

You can adjust the events that are displayed in the table by clicking the **Filter** icon and using the filter, or by entering a keyword in the **Find** field.

Step 6   Determine what ITSM events must be resent and reprocessed.

If an ITSM event displays **N/A** as a value for **ITSM Workflow**, **ITSM Status**, or **ITSM ID** (and the source of the event is ServiceNow and the destination of the event is Cisco DNA Center), this indicates an issue that would require a retry attempt. Also, a check box appears under the **Filter** column for an ITSM event that requires a retry attempt.

Step 7   Check the check box in the **Filter** column to select an ITSM event and enable the **Retry** button.

Step 8   Click **Retry**.

Figure 139: Retry ITSM Event Icon

After the event is resent to the ITSM destination, one of the following occurs:

- Retry Success: Appropriate values display in the **ITSM Workflow**, **ITSM Status**, and **ITSM ID** columns for the event. For example, *RFC* in the **ITSM Workflow** column, *New* in the **ITSM Status** column, and an alphanumeric ID for the **ITSM ID**.

- Retry Failure: If the event retry fails, then the ITSM event will still display **N/A** as a value for **ITSM Workflow**, **ITSM Status**, or **ITSM ID**. See the following step for working with a second retry failure.

Step 9   (Optional) After another retry failure, in the Cisco DNA Center GUI, click the menu icon (☰) and choose **Platform** > **Developer Toolkit** > **APIs** > **Ecosystem Integrations** > **ITSM** > **Get Failed ITSM Events**.

Access this API method to retrieve information about the ITSM integration failure.

Step 10   Click **Try It** and enter the instance ID (**instanceId**) of the failed event from the **Runtime Dashboard**.

Step 11   Click **Run**.

The following response data can be retrieved using this API:

- **eventStatus**: ITSM (ServiceNow) event status

- **errorCode**: ITSM (ServiceNow) event error code

- **errorDescription**: Description of the ITSM (ServiceNow) event error

- **responseReceivedFromITSMSystem**: ITSM (ServiceNow) response

Use the information retrieved by the API to understand and correct the event failure.

What to do next

Retry (resend and reprocess) any other ITSM events, if necessary.

Review the API Summary

Perform this procedure to review the Cisco DNA Center platform **API Summary**. The **API Summary** displays the total number of API calls, API call duration, and API call status. You can use this data to assist in monitoring performance of the Cisco DNA Center platform APIs. This information can be helpful when monitoring or troubleshooting Cisco DNA Center platform and its integration with other systems.

You review the **API Summary** using the **Runtime Dashboard** window in the Cisco DNA Center GUI.

Figure 140: Cisco DNA Center Platform Runtime Dashboard Window
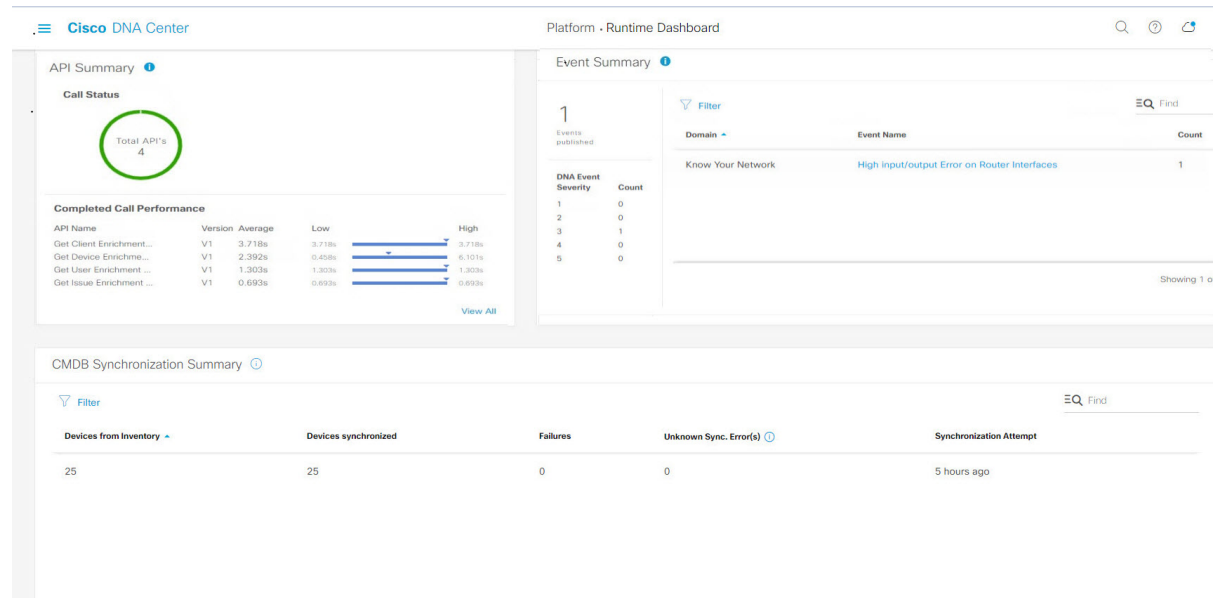
Before you begin

For the **API Summary** field to display events, you need to enable, configure, and activate the bundles that provide the events to monitor in **Bundles**. For information about **Bundles** see Bundle Features, on page 14.

Step 1	Click the menu icon (≡) and choose **Platform** > **Runtime Dashboard**.
Step 2	Choose a time interval for the API summary by clicking **Last 1 Week** at the upper right side of the GUI menu bar.
	You can view the API summary for the last 6, 12, and 24 hour period or for the week.
Step 3	Review the **API Summary** field.
	The **API Summary** field displays the following information:

- **Call Status**: Total number of API calls and status display. The color green represents the successful API calls and the color red represents the unsuccessful API calls.

- **Completed Call Performance**: List of API calls in alphabetical order with completed call performance in seconds (Low, Average, High).

- **View Details**: Link to view additional API details.

Step 4	Click **View Details** to review additional details about the APIs.
	The **All APIs calls** slide-in pane opens.
Step 5	Review the information in the **All APIs calls** slide-in pane.
	The following information is displayed:

- API by name

- API version

- API call count table, that includes the total number of API calls, number of successful API calls (green icon), and number of unsuccessful API calls (red icon).

- API call duration table that includes minimum, maximum, and average duration.

You can adjust the APIs that are displayed in the tables by clicking the **Filter** icon and using the filter, or by entering a keyword in the **Find** field.

What to do next

Review the additional Cisco DNA Center platform data displayed in the **Runtime Dashboard**.

Review the CMDB Synchronization Summary

Perform this procedure to review the Cisco DNA Center platform **CMDB Synchronization Summary**. The **CMDB Synchronization Summary** displays the synchronization status of inventory device data to ServiceNow. You can use the summary to help monitor and troubleshoot device data synchronization with ServiceNow.

You review the **CMDB Synchronization Summary** using the **Runtime Dashboard** window in the Cisco DNA Center GUI.

Figure 141: Cisco DNA Center Platform Runtime Window
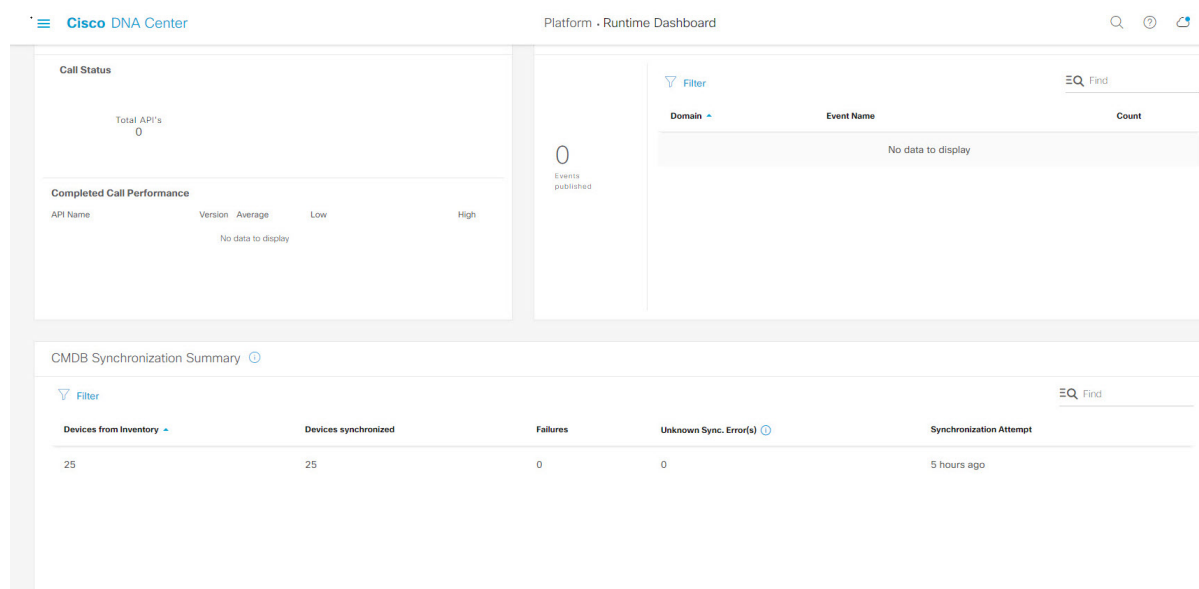
Before you begin

For the **CMDB Synchronization Summary** field to display events, you must enable, configure, and activate the bundles in **Bundles**. Additionally, you must enable associated event notifications for the bundles in **Event Settings**. For information about **Bundles**, see Bundle Features, on page 14. For information about **Event Settings**, see Configure Event Settings, on page 33.

Step 1   Click the menu icon (☰) and choose **Platform** > **Runtime Dashboard**.

Step 2   Review the **CMDB Synchronization Summary** field, which displays the following information:

- **Devices from inventory**: Total number of devices from **Inventory** collected from Cisco DNA Center.

- **Devices synchronized**: List of devices that were successful synchronized with ServiceNow.

- **Failures**: Number of failed synchronization attempts between Cisco DNA Center and ServiceNow.

     Click **Learn More...** for additional information.

- **Unknown Synch Errors**: Number of partially successful synchronization attempts between Cisco DNA Center and ServiceNow

     Click **Learn More...** for additional information.

- **Synchronization Attempt**: When the last synchronization attempt was made between Cisco DNA Center and ServiceNow.

Step 3   (Optional) Click the **Learn More** link for any synchronization failure.

Step 4   Review the displayed data about the synchronization failure for the device.

The following information is displayed in a table:

- **Device ID**: Device identification number.

- **Host Name**: Name of the host to which the device is connected to.

- **Device Type**: Type of device, such as a switch, router, or AP.

- **MAC Address**: MAC address of the device.

- **Management IP Address**: Device's management address that can be used to access and troubleshoot the device.

- **Serial Number:** Serial number of the device.

Step 5   Click the **DeviceID** link to review additional information about the device in the **Inventory** window.

What to do next

Review the data displayed by Cisco DNA Center to troubleshoot any synchronization issues between the device and ServiceNow.

Review the additional Cisco DNA Center platform data displayed in the **Runtime Dashboard**.

Review the Integration Flow Summary

Perform this procedure to review the Cisco DNA Center platform **Integration Flow Summary**. You can use the **Integration Flow Summary** to assist in monitoring performance of the Cisco DNA Center platform integration flows. This information can be helpful when monitoring or troubleshooting Cisco DNA Center platform and its integration with other systems.

You review the **Integration Flow Summary** using the **Runtime Dashboard** window in the Cisco DNA Center GUI.

Figure 142: Cisco DNA Center Platform Runtime Dashboard Window
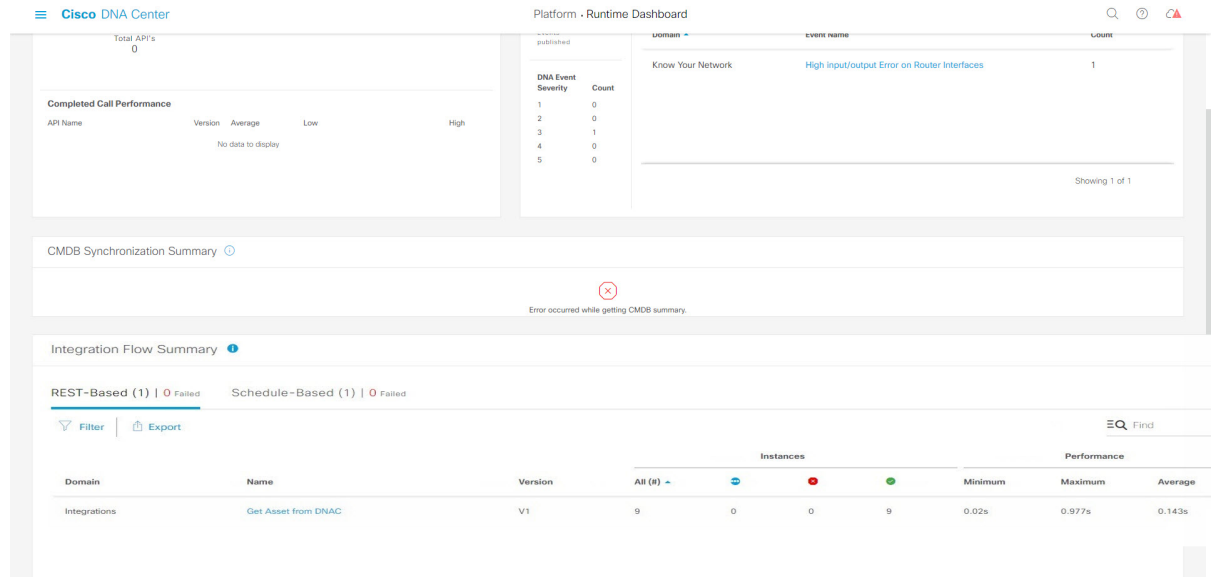
Before you begin

For the **Integration Flow Summary** fields (two tabs) to display data, you need to enable, configure, and activate the bundles that provide the events to monitor in **Bundles**. For information about **Bundles**, see Bundle Features, on page 14.

Step 1   Click the menu icon (≡) and choose **Platform** > **Runtime Dashboard**.

Step 2   Choose a time interval for the integration flow summary by clicking **Last 1 Week** at the upper right side of the GUI menu bar.

You can view the integration flow summary for the last 6, 12, 24 hour period or for the week.

Step 3   Review the **Integration Flow Summary** field, which displays the following information:

- **REST-Based**: Domain, integration flow name and link, version, instance totals, instance status (successful [green], fail [red], in progress [blue]), and performances (minimum, maximum, and average call performance times, in milliseconds).

- **Schedule-Based**: Domain, integration flow name and link, version, instance totals, instance status (successful [green], fail [red], in progress [blue]), and performances (minimum, maximum, and average call performance times, in milliseconds).

Step 4   For a summary of the data generated by REST-based integration flows, click the **REST-Based** tab.

Step 5   Review the **REST-Based** data.

Click an integration flow name (link) to view additional information about the instances. The following additional information appears in a slide-in pane:

- **Instance ID**: Identification number (and link) of the instance to the integration flow. You can configure an instance to more than one integration flow.

- **Status**: Status of the instance (success or fail).

- **Start Time**: Start date and time of the instance call.

- **End Time**: End date and time of the instance call.

- **Duration**: Duration of call, in seconds.

Step 6   Click an individual instance ID (link) to view detailed information about it.

The following additional information appears in a slide-in pane:

- **RUN SUMMARY**: Start and end times and dates, time taken, status.

- **ERRORS**: Error responses (if any).

- **LOGS**: Log entries (if available).

Click the **X** icon to close the slide-in pane and return to the previous window.

Step 7   For a summary of the data generated by schedule-based integration flows, click the **Schedule-Based** tab.

Step 8   Review the **Schedule-Based** data.

Click an integration flow name (link) to view additional information about the instances. The following additional information appears in a slide-in pane:

- **Instance ID**: Identification number of the instance within the integration flow.

- **Status**: Status of the instance (success or fail).

- **Start Time**: Start date and time of the instance call.

- **End Time**: End date and time of the instance call.

- **Duration**: Duration of call, in seconds.

Step 9   Click an individual instance ID (link) to view detailed information about it.

The following additional information appears in a slide-in pane:

- **RUN SUMMARY**: Start and end times and dates, time taken, status.

- **ERRORS**: Error responses (if any).

- **LOGS**: Log entries (if available).

Click the **X** icon to close the slide-in pane and return to the previous window.

What to do next

Review the additional Cisco DNA Center platform data displayed in the **Runtime Dashboard**.