



NOZOMI
NETWORKS

ServiceNow Service Graph Connector Integration Guide

SGC v1.4.8 – 2025-03-18

Legal notices

Information about the Nozomi Networks copyright and use of third-party software in the Nozomi Networks product suite.

Copyright

Copyright © 2013-2024, Nozomi Networks. All rights reserved. Nozomi Networks believes the information it furnishes to be accurate and reliable. However, Nozomi Networks assumes no responsibility for the use of this information, nor any infringement of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent, copyright, or other intellectual property right of Nozomi Networks except as specifically described by applicable user licenses. Nozomi Networks reserves the right to change specifications at any time without notice.

Third Party Software

Nozomi Networks uses third-party software, the usage of which is governed by the applicable license agreements from each of the software vendors. Additional details about used third-party software can be found at <https://security.nozominetworks.com/licenses>.

Contents

Chapter 1. Introduction.....	5
Overview.....	7
Chapter 2. Requirements.....	9
Requirements.....	11
Chapter 3. Configuration.....	13
Local user integration in CMC.....	15
Add a local user.....	15
Local user integration in Vantage.....	17
Invite a user in Vantage.....	17
Service Graph Connector configuration.....	19
Install the Service Graph Connector application.....	20
Guided Setup for the Service Graph Connector.....	22
Configure table permissions.....	23
Configure assets import.....	25
Configure incidents import.....	33
Validate data flow.....	38
Mapping to custom CMDB tables in ServiceNow.....	39
Map Nozomi Networks data with IntegrationHub ETL.....	40
Map Nozomi Networks data with IntegrationHub ETL - example.....	43
System properties configuration.....	45
Add a new column to asset select query.....	46
Generate an API key in Vantage.....	49
Generate an OpenAPI key in a sensor.....	51
Chapter 4. Additional configuration.....	53
Configure an MID server.....	55
Add a trusted certificate.....	56
Add a non-trusted certificate.....	57
Chapter 5. Frequently Asked Questions.....	59
How to change which Nozomi assets get targeted to which ServiceNow classes?.....	61
How can I add additional or custom fields from the Nozomi API into my integration?.....	62
Why am I seeing duplicates after the first import?.....	63
Chapter 6. Troubleshooting.....	65
Service Graph Connector application is no longer working.....	67
Cross-scope access-policy error shows.....	68

Glossary.....71

Chapter 1. Introduction



Overview

*This documentation describes the **ServiceNow Service Graph Connector for Nozomi Networks (Service Graph Connector)** integration with the Nozomi Networks platform.*

General

This integration includes the following information:

- What information is being exchanged and the direction of flow
- How to configure the **Service Graph Connector** application in a ServiceNow instance

The integration is a two-way integration between the Nozomi Networks platform and the ServiceNow instance. The administrator of the **Service Graph Connector** application sets a schedule to pull data from the instance that is connected to Nozomi Networks. In addition, incidents that are pulled from a Nozomi Network instance, and closed in ServiceNow, result in an update of the status, and subsequent closure, in the Nozomi Networks instance.

Scope and limitations

The documentation provides guidance on how to configure this Nozomi Networks ServiceNow application.

The application is designed to extract and display data from Nozomi Networks solutions within the ServiceNow platform.

Throughout this section, you will find screenshots that show the interface for this Nozomi Networks application as they show inside the ServiceNow environment. Nozomi Networks has tested and validated these configurations.

Support scope

Nozomi Networks Support is available to assist with the configuration and troubleshooting of this application. This includes the data integration from Nozomi Networks products in ServiceNow and all functions that the Nozomi Networks screens and workflows provide.

Out of scope

Items that are not directly connected to this Nozomi Networks application, are out of scope of the Nozomi Networks Support team. This means that Nozomi Networks Support does not cover troubleshooting or support for other:

- ServiceNow-native features
- ServiceNow third-party integrations
- ServiceNow components

Nozomi Networks Support does not cover screens or processes that only display or use data from Nozomi Networks integrations, when they are not part of this Nozomi Networks application. For these issues, you should contact [ServiceNow Support](#).



Chapter 2. Requirements



Requirements

A description of the requirements for the use of the **Service Graph Connector** application.

ServiceNow requirements

ServiceNow Tokyo, or later.

Supported Nozomi Networks platforms

- [Central Management Console \(CMC\)](#) - release 22.4, or higher (the incidents closure feature requires [Nozomi Networks Operating System \(N2OS\) 24.4.0](#))
- Vantage

Connectivity

Make sure that the ServiceNow instance has connectivity to your Nozomi Networks appliance. The Nozomi Networks appliance will send queried data to the ServiceNow instance so connectivity must be established.

Make sure that there is a path from the Nozomi Networks appliance to your ServiceNow instance.



Note:

Connectivity through the ServiceNow [Management, Instrumentation, and Discovery \(MID\)](#) server does not require additional configuration items in the application. Make sure that the connectivity from all on-premises ServiceNow instances is correctly configured to connect with the Nozomi Networks instance via the [MID](#) server. For more details, see [Configure an MID server \(on page 55\)](#).

Package dependencies

In the instance that will run the **Service Graph Connector**, you **MUST** install these packages:

- Integration Commons for [Configuration Management Database \(CMDB\)](#), minimum version 2.4.1
- System import Sets, minimum version 1.0.0
- [Information Technology Operations Management \(ITOM\)](#) Discovery License
- [ITOM](#) Licensing
- IntegrationHub [Extract Transform Load \(ETL\)](#) (2.1.0)
- [CMDB Configuration Item \(CI\)](#) Class Models (1.32.0)
- Data Stream Actions (com.glide.hub.action_type.datastream)

If a plug-in is missing in your ServiceNow instance it **MUST** be installed as it is a dependency that the Service Graph Connector for Nozomi Networks requires. For help with plug-ins, see the [ServiceNow documentation](#).

**Note:**

If you are using an on-premises (self-hosted) instance of ServiceNow, you will need to contact ServiceNow support to get the necessary credentials to perform the activation of the required plug-ins.

Chapter 3. Configuration



Local user integration in CMC

To connect to Nozomi Networks, you need to configure a local user.

When you integrate a local user in [CMC](#), make sure that the user belongs to a group that has these permissions:

- Queries and exports
- Assets
- Alerts, and
- Sensors




Note:

If you use the Vulnerability Response application, you also need to provide the Vulnerabilities permission.

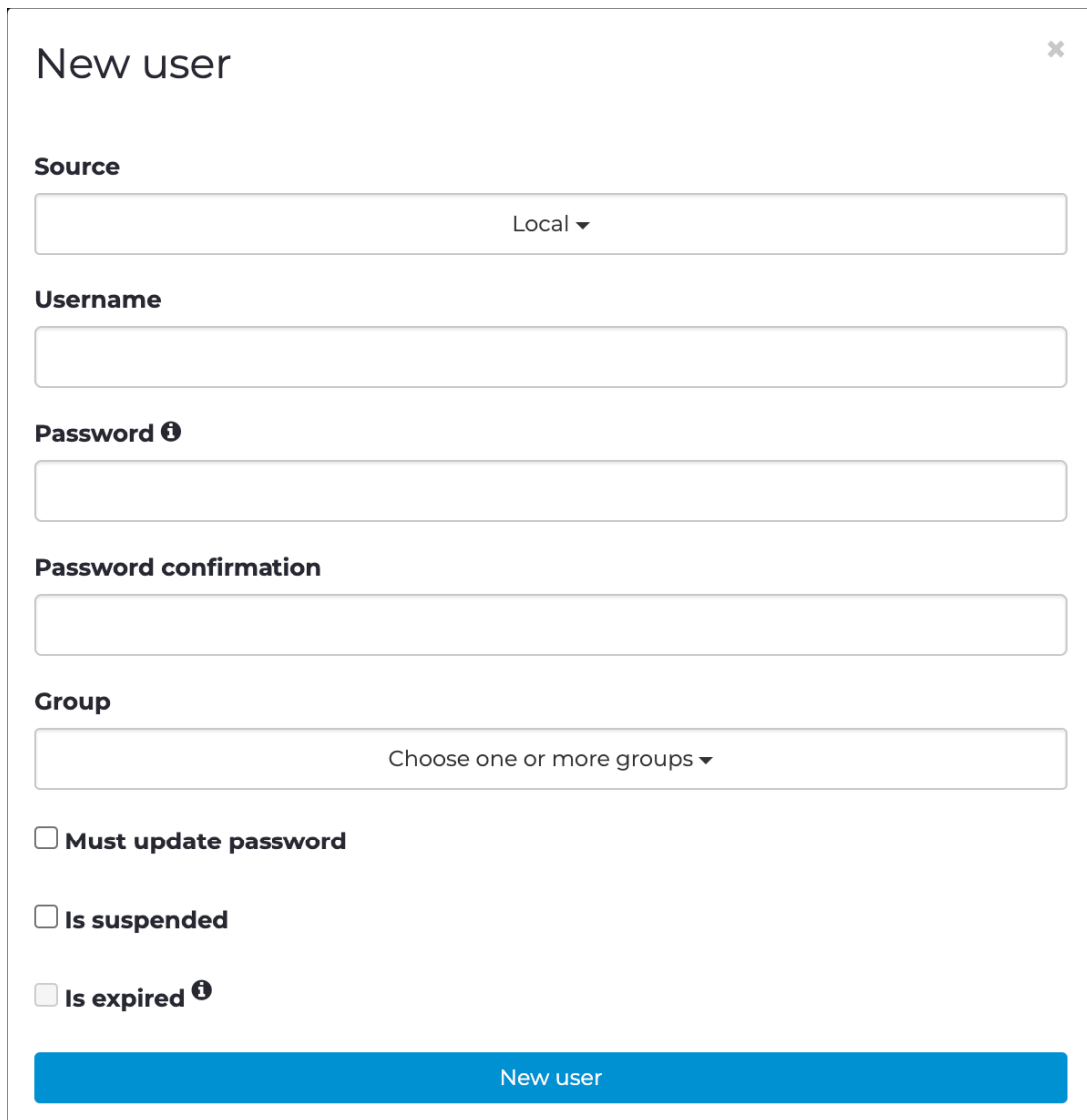
Add a local user

The **Users** page lets you add a new user.

Procedure

1. In the top navigation bar, select 
Result: The administration page opens.
2. In the **Settings** section, select **Users**.
Result: The **Users management** page opens.
3. In the top right section, select **Users**.
Result: The **Users** page opens.
4. In the top right section, select **+Add**.
Result: A dialog shows.

5. From the **Source** dropdown, select **Local**.



New user ✕

Source

Local ▼

Username

Password ⓘ

Password confirmation

Group

Choose one or more groups ▼

Must update password

Is suspended

Is expired ⓘ

New user

6. In the **Username** field, enter a value.

7. In the **Password** field, enter a password.

8. In the **Password confirmation** field, enter the password again.

9. From the **Group** dropdown, select a group for the user.

10. Select **New user**.

Results

The user has been added.

Local user integration in Vantage

To connect to Nozomi Networks, you need to configure a local user.

When you integrate a local user in Vantage, make sure that the user belongs to a group that has these permissions:

- Assets
- Alerts


**Note:**

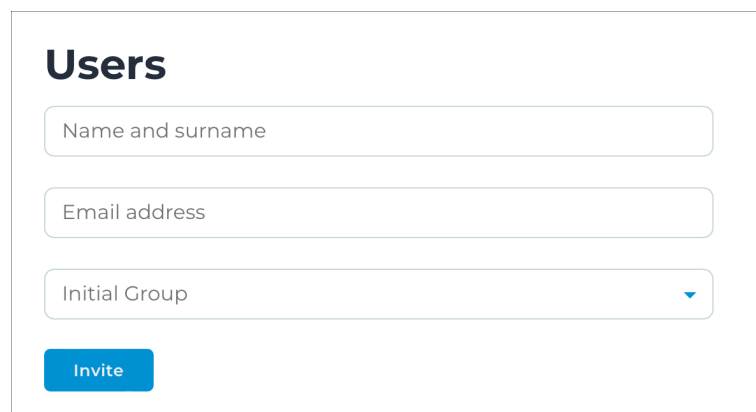
If you use the Vulnerability Response application, you also need to provide the Vulnerabilities permission.

Invite a user

You can use the **Users** page to send an email invite to someone to add them as a new user in Vantage.

Procedure

1. In the top navigation bar, select 
Result: The administration page opens.
2. In the **Teams** section, select **Users**.
Result: The **Users** page opens.
3. Select **Invite**.
Result: Data entry fields show.
4. In the **Name and surname** field, enter the details as necessary.



Users

Name and surname

Email address

Initial Group ▼

Invite

5. In the **Email address** field, enter an email address for the user.
6. Select the **Initial Group** dropdown, and select an option.
7. Select **Invite**.

Results

The email invitation has been sent.

Service Graph Connector configuration

*A description of the necessary procedures that you need to do to configure the **Service Graph Connector** application.*

To configure the **Service Graph Connector** application, do these procedures:

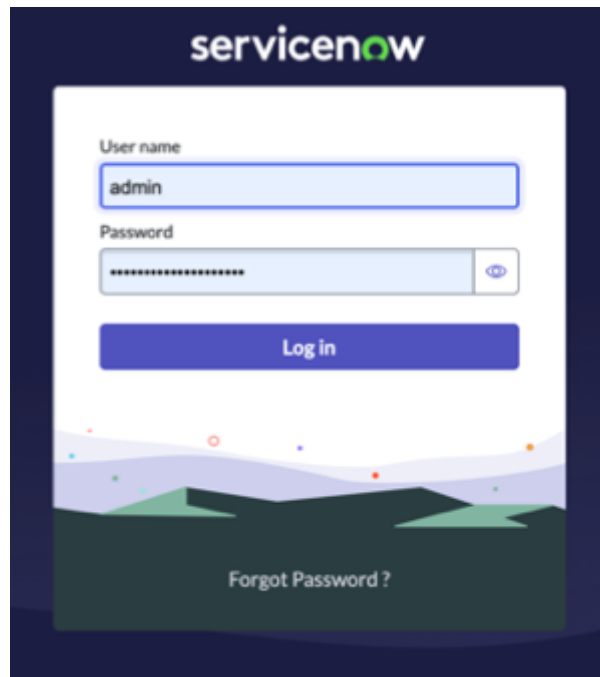
- [Install the Service Graph Connector application \(on page 20\)](#)
- [Guided Setup for the Service Graph Connector \(on page 22\)](#)

Install the Service Graph Connector application

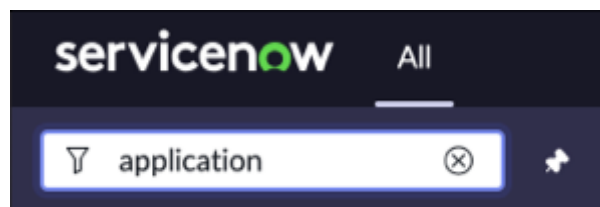
Learn how to install the Service Graph Connector application on your ServiceNow instance, to enable integration with the Nozomi Networks software.

Procedure

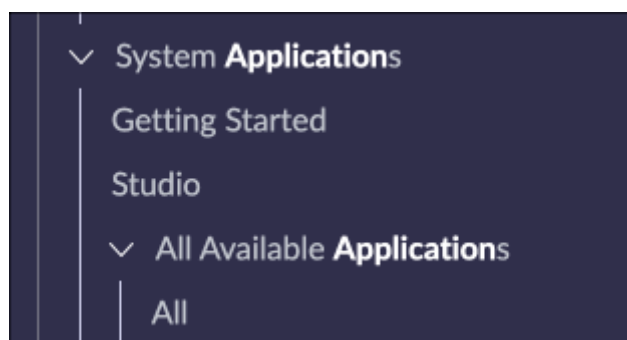
1. Log in to the ServiceNow instance.



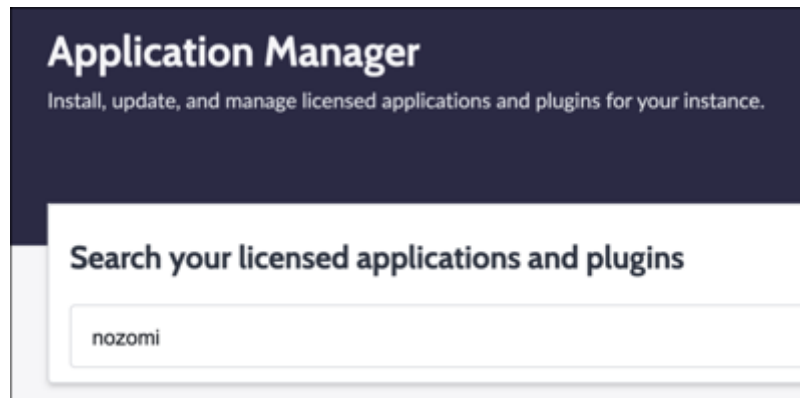
2. In the left sidebar, search for application.



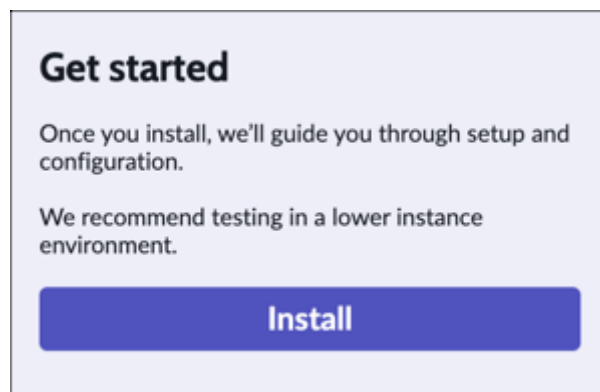
3. In the left sidebar, look for **All Available Applications**.



4. Select **All**.
5. In the search field, enter **nozomi** and press enter.

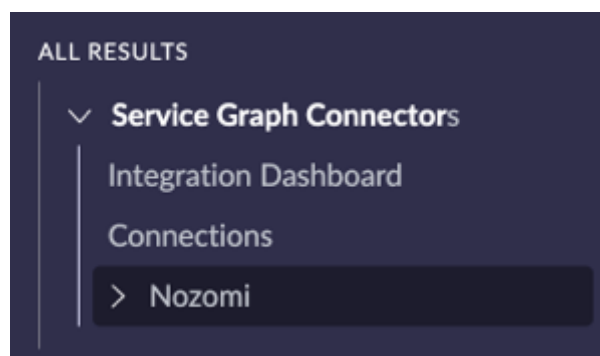


6. Select the application and in the top right section, select **Install**.



7. Wait for the installation procedure to finish.
8. Refresh the instance.

After installing and refreshing your instance, you should see the **Nozomi** application under **Service Graph Connectors** in the left side bar.

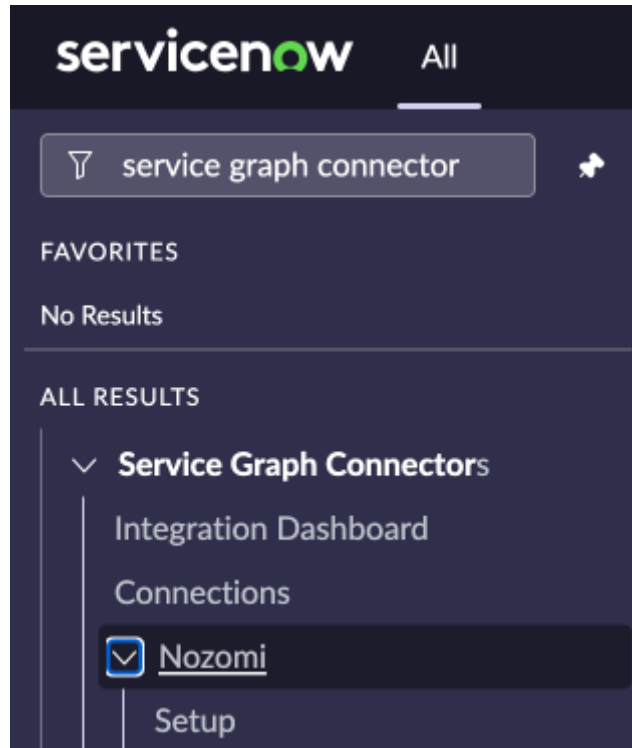


Guided Setup for the Service Graph Connector

Follow the step-by-step guided setup process to configure the **Service Graph Connector for Nozomi** application within your ServiceNow instance. There are three sections to the guided setup: **Table permissions**, **Incidents**, and **Assets**. This procedure takes you through each of these sections.

Procedure

1. In the left sidebar, under **Nozomi**, select **Setup**.



This takes you to the Guided Setup page for the **Service Graph Connector**.

2. In the top right section, select **Get Started**.

0%
Complete

Service Graph Connector for Nozomi Networks

Getting started Get Started

This Guided Setup will walk you through configuration of the Service Graph Connector for Nozomi Networks. You will need the username / password of a valid user with API permissions for each Nozomi Networks CMC instance you want to import from. ServiceNow Admin role is required to configure most steps. Click "Get Started" to begin!

Usage of this Service Graph Connector requires a subscription to the IT Operations Management (ITOM) Visibility application. Managed IT Resources (as defined in [Section 1.1 of the ServiceNow Subscription Unit Overview](#)) created or modified in the CMDB by this Service Graph Connector, but not yet managed by ITOM Visibility, will increase Subscription Unit consumption within ITOM Visibility. Customers should review their current ITOM Visibility Subscription Unit consumption to ensure available capacity.

Get going

Get Service Graph Connector for Nozomi Networks up and running, quickly and easily.

>

Learn

Learn about the common configuration tasks that integrate Nozomi with CMDB.

>

Feel empowered

Feel empowered to customize Nozomi integration with CMDB.

Configure table permissions

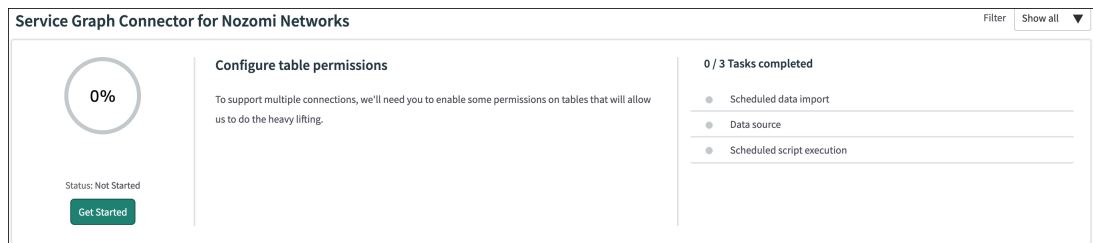
Learn how to configure table permissions within the **Service Graph Connector for Nozomi** application.

About this task

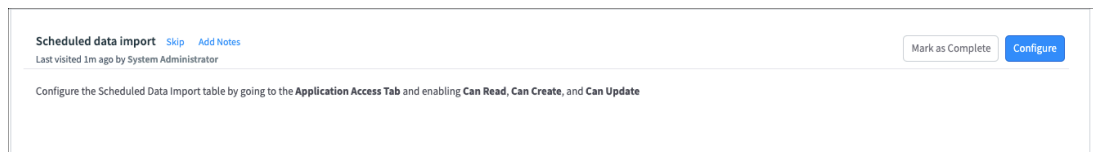
You should have the ServiceNow Admin role to install and configure table permissions.

Procedure

1. In the filter navigator, go to **Service Graph Connector for Nozomi > Setup**
2. Select **Get Started**.
3. Select **Configure table permissions**
4. Select **Get Started**.
5. In the **Configure table permissions** section, select **Scheduled data import**.



6. In the **Scheduled data import** section, select **Configure**.



7. Select **Application Access**.

Columns	Controls	Application Access
Accessible from		
All application scopes		
Can read	<input checked="" type="checkbox"/>	Allow access to this table via web services <input checked="" type="checkbox"/>
Can create	<input checked="" type="checkbox"/>	Allow configuration <input type="checkbox"/>
Can update	<input checked="" type="checkbox"/>	
Can delete	<input type="checkbox"/>	

8. Select these options:

- **Can read**
- **Can create**
- **Can update**

9. Select **Mark as Complete**.10. In the **Data source** section, select **Configure**.

11. Do steps 8 (on page 24) and 9 (on page 24) again.

12. In the **Scheduled script execution** section, select **Configure**.

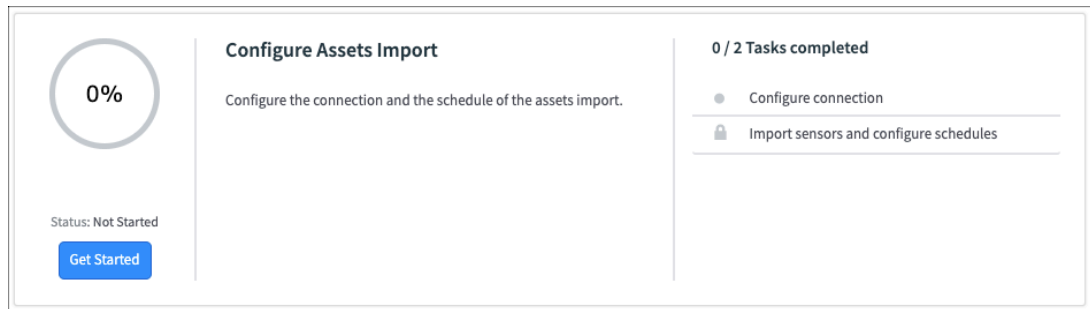
13. Do steps 8 (on page 24) and 9 (on page 24) again.

Configure assets import

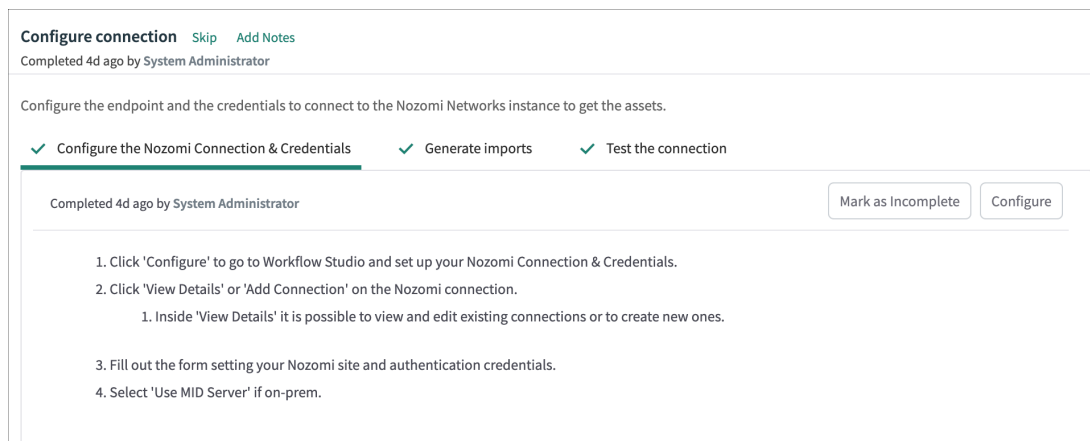
Discover the detailed process of configuring asset imports within the **Service Graph Connector** application. This includes setting up connections, validating sensors, configuring schedules, and executing data imports, to ensure seamless integration and data synchronization for efficient network asset management.

Procedure

1. In the **Configure Assets Import** section, select **Get Started**.



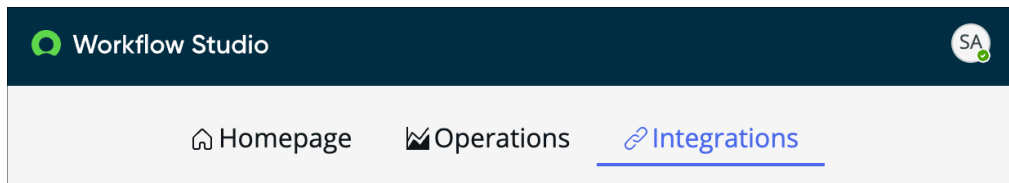
2. Select **Configure connection**
3. In **Configure The Nozomi Connection & Credentials**, select **Configure**.



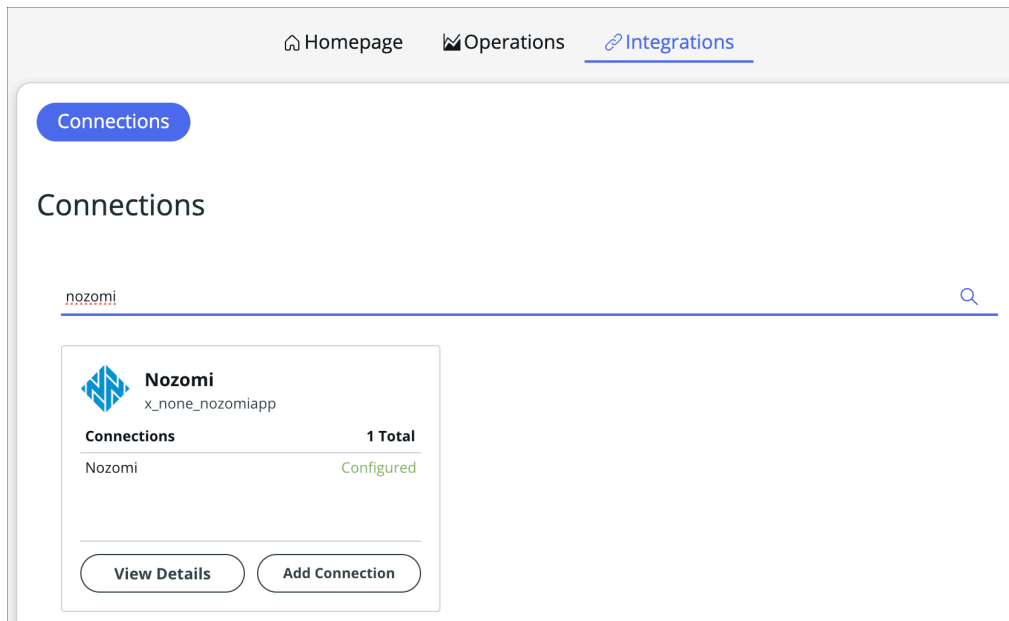
Result: A new tab opens.

4. If your ServiceNow instance have been updated to Washington, do these extra steps:

a. When **Workflow studio** opens in a new page, select **Integrations**.



b. In the search field, search for **Nozomi**.



5. Select **Add Connection**.

6. Enter your site information.

7. **Optional:** If necessary, select **Use MID server**.

CMC: Use the username and password for the local user account

Vantage: Use an *application programming interface (API)* Key Name and *API* Key Token for **User name** and **Password**, respectively. For more details on how to generate an *API* key, see the Vantage documentation.

8. If you have other Nozomi Networks instances that you would like to connect to, add additional connections.

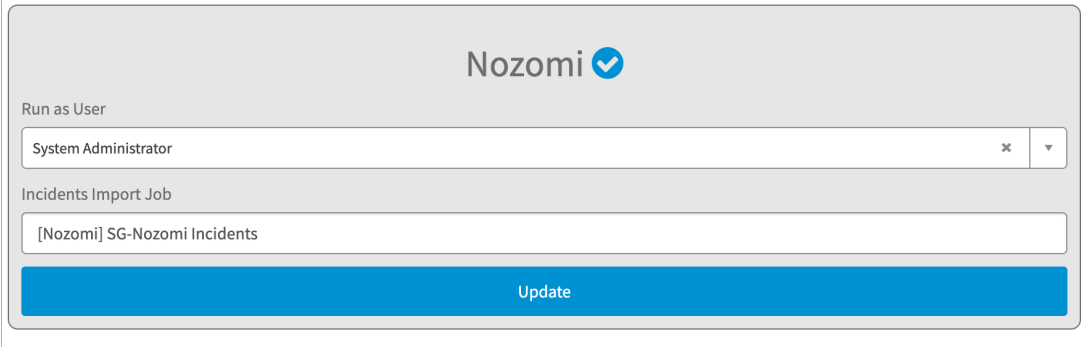
9. Go back to the **Configure connections** section in the guided setup, and select **Mark as Complete**.

10. In the **Configure connections** section, select **Generate imports**.

11. Select **Configure**.

12. On the **Custom UI** page, review each connection that you just created. If necessary, change the details for names.

13. For each connection, select **Generate**.



The screenshot shows a configuration window for Nozomi. At the top, the Nozomi logo is displayed with a blue checkmark. Below the logo, there are two input fields. The first is labeled 'Run as User' and contains the text 'System Administrator'. The second is labeled 'Incidents Import Job' and contains the text '[Nozomi] SG-Nozomi Incidents'. At the bottom of the window, there is a large blue button labeled 'Update'.

14. If the connection is successful, a blue checkmark shows next to the connection name.

You can update these values to make changes in the future.

15. Select **Mark as Complete**.
16. Go back to the guided setup.
17. Select **Test the connection**.
18. Select **Configure**.
- For each connection there should be one Service Graph Connection.
19. Open each Service Graph Connection.
20. To test the connection, select **Test Connection**.
21. Go back to the guided setup, select **Mark as Complete**.
22. Select **Import sensors and configure schedules**.

23. Select **Import sensors**.

Import sensors and configure schedules [Skip](#) [Add Notes](#)

Last visited 5m ago by System Administrator

After successfully connecting to the Nozomi Networks API, you'll need to import Nozomi sensors (appliances) to the NIDS class, add metadata (owner, site, etc) and validate the NIDS, then set up the scheduled jobs.

● **Import sensors** 🔒 Validate sensors ● Configure schedules

Last visited 5m ago by System Administrator [Mark as Complete](#) [Configure](#)

Before importing all of your Nozomi assets, we need need to import all of your sensors (Nozomi appliances).

1. Open each of the Nozomi appliance scheduled data import jobs.
2. Manually execute the scheduled data import by clicking the Execute Now button.
3. Once the scheduled job is completed, you will be able to see them in the [Network Intrusion Detection Systems \[cmdb_ci_nids\]](#) table.

24. Select **Configure**.

25. For each connection there should be one scheduled data import related to Appliances, select it.

Name	Active	Class	Updated
[Nozomi] SG-Nozomi Appliances	false	Scheduled Data Import	01-12 02:05

26. To manually execute the scheduled data import, select **Execute Now**.

Scheduled Data Import
[Nozomi] SG-Nozomi Appliances

Name: [Nozomi] SG-Nozomi Appliances Application: Service Graph Connector for Nozomi N

Data source: [Nozomi] SG-Nozomi Appliances Run: Daily

Run as: Conditional:

Note: You can also select **Execute Full Import** which will force a full import of Nozomi Networks data, regardless of the last import execution time.

27. Go back to the guided setup and select **Mark as Complete**.

28. Select **Validate sensors**.

Import sensors and configure schedules [Skip](#) [Add Notes](#)

Last visited just now by System Administrator

After successfully connecting to the Nozomi Networks API, you'll need to import Nozomi sensors (appliances) to the NIDS class, add metadata (owner, site, etc) and validate the NIDS, then set up the scheduled jobs.

Import sensors
 Validate sensors
 Configure schedules

Last visited 19h ago by System Administrator

Once the scheduled data imports have finished, you can now validate each sensor (appliance) that was discovered by the integration. Any metadata that you add to the NIDS (such as owner, site, etc) will also be inherited by OT Assets imported into the CMDB.

NOTE: Nozomi CI and OT Asset data *will not* be imported until its parent sensor has been validated using the Validate UI Action on the NIDS form.

1. Click configure and go through each Nozomi NIDS.
2. It is recommended that you populate NIDS metadata such as location, owner, and network type. This information will be cascaded down to any child OT Assets that are detected by this sensor. OT Assets will only be created if network type is defined as OT.
3. If the network type is set to OT, then Nozomi assets that are detected by this sensor will have manufacturing OT Assets created.
4. After configuring the sensor, click the Validate UI action.

After validating the sensors, Nozomi CI's and OT Assets will now be able to import into the CMDB when the scheduled import runs.

29. Select **Configure**.

30. It will open the [Network Intrusion Detection Systems \(NIDS\)](#) showing all the appliances the integration has discovered.

Network Intrusion Detection Systems							
Name	Manufacturer	Model ID	Validated	Firmware version	NIDS network type	NIDS assignment site	NIDS
3a52372b604e	Nozomi Networks	Nozomi Networks Container	false	22.5.0-10042129_C32FA	OT	(empty)	SG-N

Here is where you can also configure the assignment site and all metadata.

31. Once you have completed the configuration, select **Validate** on the related link at the bottom of the form.

32. After all the *NIDS* have been validated, select **Mark as Complete**.

33. Select **Configure schedules** and select **Configure**.

34. Open each appliance import scheduled job.

35. The run as user should be set based on what you selected during the **Generate imports** step.

36. Set the Active checkbox to true and adjust the runtime frequency.

The screenshot shows a configuration form for a job. The fields are as follows:

- Name:** [CMC] SG-Nozomi Appliances
- Application:** Service Graph Connector for Nozomi
- Data source:** [CMC] SG-Nozomi Appliances
- Run as:** Erik Anderson
- Run:** Daily
- Time:** Hours 00 00 00
- Active:**
- Conditional:**

37. Scroll to the bottom of the form and confirm that the Assets import job is listed child job. Set this job to active as well.

The screenshot shows a table of jobs. The table has columns for Name, Active, and Order. The 'Assets import' job is highlighted, and its 'Active' checkbox is checked.

Name	Active	Order
[CMC] SG-Nozomi Assets	<input checked="" type="checkbox"/>	100

38. Once you have completed configuring all the jobs, you can either wait for the scheduled job to run, or you can select **Execute Now** to manually execute the job on the **Appliance Scheduled Data Import Job**.



Note:

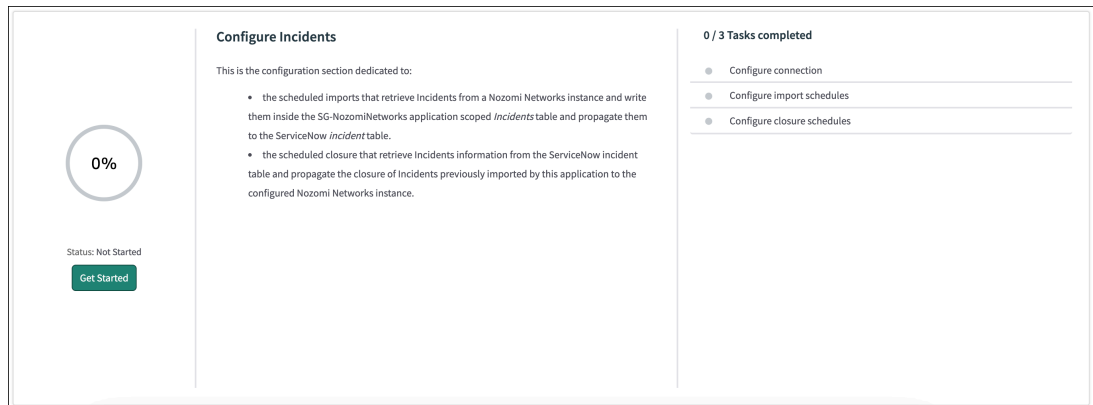
You can also select **Execute Full Import**, which will force a full import of Nozomi Networks data, regardless of the last import execution time.

Configure incidents import

Explore the step-by-step process of configuring incident imports within the **Service Graph Connector for Nozomi** application. This procedure covers connection setup, validation, schedule configuration, and manual execution, to ensure seamless integration and management of incident data for enhanced operational efficiency.

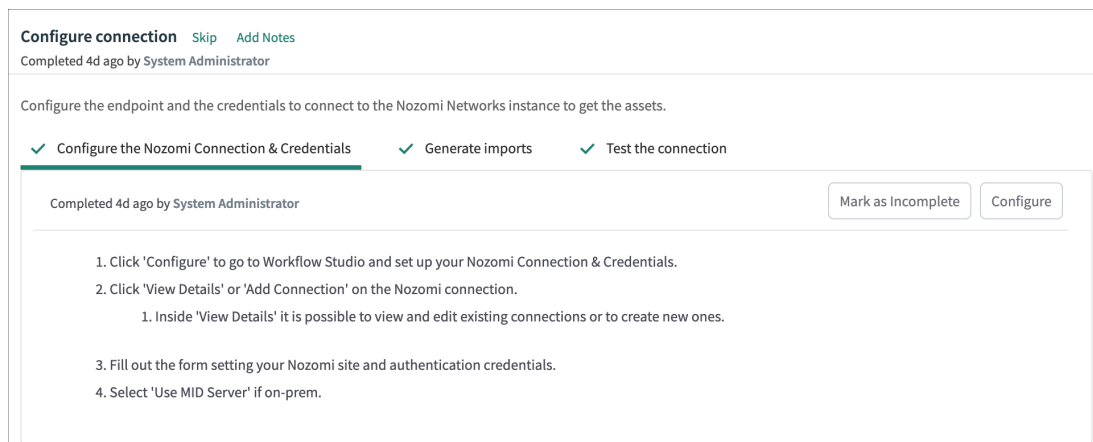
Procedure

1. In the **Configure Incidents** section, select **Get Started**.



2. Select **Configure connection**.

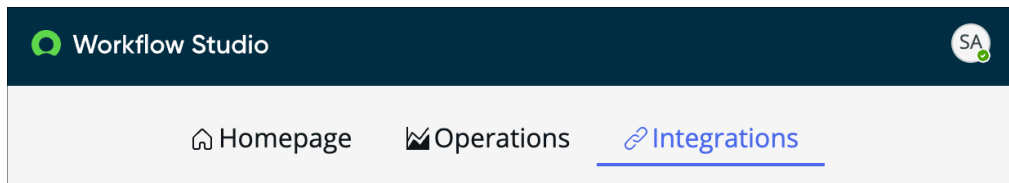
3. In **Configure The Nozomi Connection & Credentials**, select **Configure**.



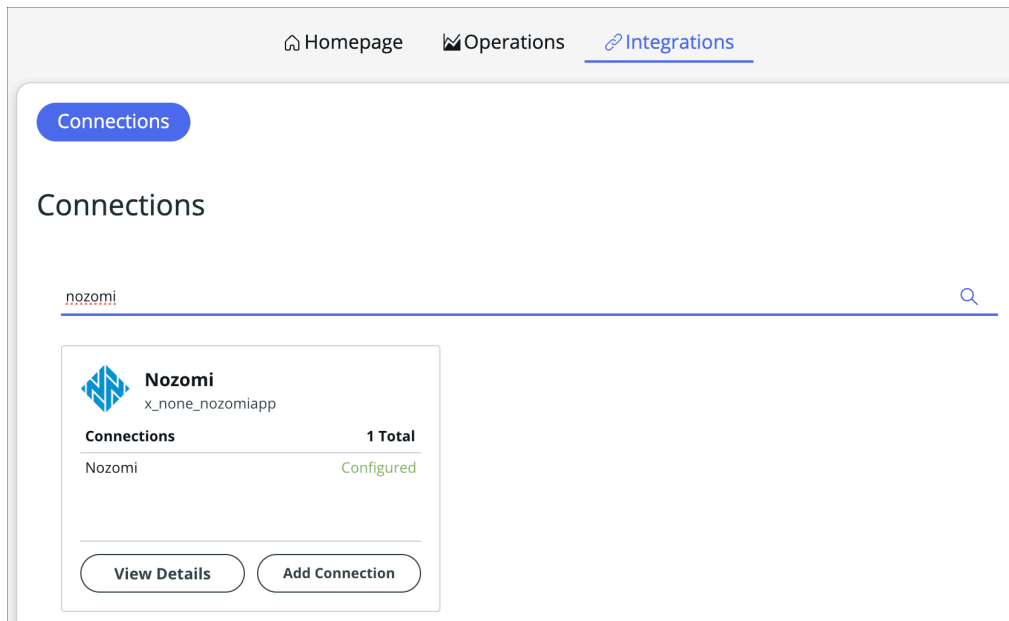
Result: A new tab opens.

4. If your ServiceNow instance have been updated to Washington, do these extra steps:

a. When **Workflow studio** opens in a new page, select **Integrations**.



b. In the search field, search for **Nozomi**.



5. Select **Add Connection**.

6. Enter your site information.

7. Select **Configure**.

8. On the **Custom UI** page, review each connection that you just created. If necessary, change the details for names.

9. For each connection, select **Generate**.

10. If the connection is successful, a blue checkmark shows next to the connection name.

You can update these values to make changes in the future.

11. Select **Mark as Complete**.

12. Go back to the guided setup.

13. Select **Test the connection**.

14. Select **Configure**.

For each connection there should be one Service Graph Connection.

15. Open each Service Graph Connection.

16. To test the connection, select **Test Connection**.

17. Go back to the guided setup, select **Mark as Complete**.

18. Select **Configure schedules**.

Configure schedules [Add Notes](#) Mark as Complete Configure

Last visited 3m ago by System Administrator

By default, the Incidents scheduled job is disabled.

On the **Scheduled Data Import** form:

- Select **Active** to activate the scheduled job.
- Select **Daily** for the job to run once each day and set the time each day the job should run.
- Scroll to the bottom of the page and activate the Asset Scheduled Data Imports that are set to run after.
- Either wait for the integration to run naturally on its scheduled starting time or you can click the Execute Now button to kick off the import immediately.

Note: If you have multiple connections try to schedule them at different times so that you don't have multiple imports executing at once.

19. Select **Configure**.

20. Open each incident import scheduled job.

Name	Active	Class	Updated
*Incidents	Search	=Scheduled Data Import	Search
[Nozomi] SG-Nozomi Incidents	false	Scheduled Data Import	01-12 02:03

21. The run as user should be set based on what you selected during the **Generate imports** step.

22. Select the **Active** checkbox, and adjust the runtime frequency.

Scheduled Data Import
[Nozomi] SG-Nozomi Incidents

Name: Application: Service Graph Connector for Nozomi N

Data source: Run: Daily


Run as: Conditional:

Active:

23. Once you have completed configuring all the jobs, you can either wait for the scheduled job to run, or you can select **Execute Now** to manually execute the job on the **Incidents Scheduled Data Import Job**.

24. Go back to the guided setup and select **Mark as Complete**.

25. Select **Configure closure schedules**.

 **Note:**
This option is only available in Vantage, or [N2OS 24.4.0](#), or higher.

26. Select **Configure**.

Configure closure schedules [Skip](#) [Add Notes](#) [Mark as Complete](#) [Configure](#)

Last visited 2m ago by System Administrator

By default, the Incidents closure scheduled job is disabled.

On the **Scheduled Incidents Closure** form:

- Select **Active** to activate the scheduled script.
- Select **Daily** for the script to run once each day and set the time each day the script should run.
- Either wait for the integration to run naturally on its scheduled starting time or you can click the Execute Now button to kick off the script immediately.

Note: If you have multiple connections try to schedule them at different times so that you don't have multiple imports / closures executing at once.

27. Open each scheduled script execution.

Name	Active	Class	Updated
[Nozomi] SG-Nozomi Incidents Closure	false	Scheduled Script Execution	2024-09-17 07:05:08

28. Select **Active**, and modify the runtime frequency.

Scheduled Script Execution
[Nozomi] SG-Nozomi Incidents Closure

Name: [Nozomi] SG-Nozomi Incidents Closure

Active:

Application: Service Graph Connector for Nozomi Networks

Conditional:

For scheduled job types that require an entered time, you have the option to enter an associated time zone. If no time zone is selected, the job will run at the entered time in time zone of the user who entered the time. If 'Use System Time Zone' is selected, the entered time will run in the time zone of the instance running the job.

Run: Daily

29. Once you have completed the configuration of all the jobs, you can:

Choose from:

- Wait for the scheduled job to run, or
- Select **Execute Now** to manually execute the job on the **Incidents Closure Scheduled Script Execution**

Validate data flow

You now need to validate that the data is flowing from the configured Nozomi Networks instance to the ServiceNow instance. To do this, you need to look at the applicable tables in ServiceNow.

Procedure

1. On the left side bar, in the main **ServiceNow** search box, search for the **Incidents** table.



2. View the **Nozomi created at** column.

Name	Ack	Appliance host	Description	Import set run	IP dst	IP src	Mac dst	Mac src	Nozomi created at	Correlation id
Eng operations	false	Network Sensor 1	A Eng operations made on device 10.0.42.	TH0001166	10.0.42.115	10.0.42.221	00:09:91:03:a7:8a	00:50:56:a6:be:7b	1711490559396	161ded37-aea4-4e77-9e88-43edd6557f45

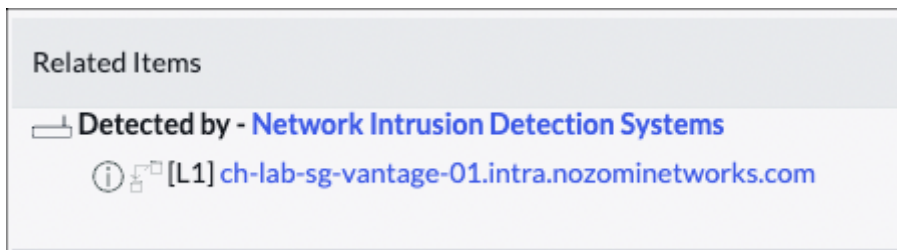
This indicates that the **Service Graph Connector** application is retrieving incident information that Nozomi Networks has generated.

3. On the left side bar, in the main ServiceNow search box, search for the Nozomi Networks hardware.

Name	Location	IP Address	Class
192.168.231.43	(empty)		OT Control System

When data is visible in this table, it indicates that the **Service Graph Connector** application is retrieving asset information from Nozomi Networks.

You can open the asset to show the related **NIDS**.



Mapping to custom CMDB tables in ServiceNow

A description of how to customize Configuration Management Database (CMDB) tables in ServiceNow with your own data model.

If you have created bespoke *operational technology (OT)* tables to represent your *OT* assets, they might not match the Nozomi Networks model. If this is the case, you will need to map this into your framework.

The recommended method for mapping newly integrated Nozomi Networks data into custom *CMDB* tables is to use the IntegrationHub *ETL* functionality. This lets you:

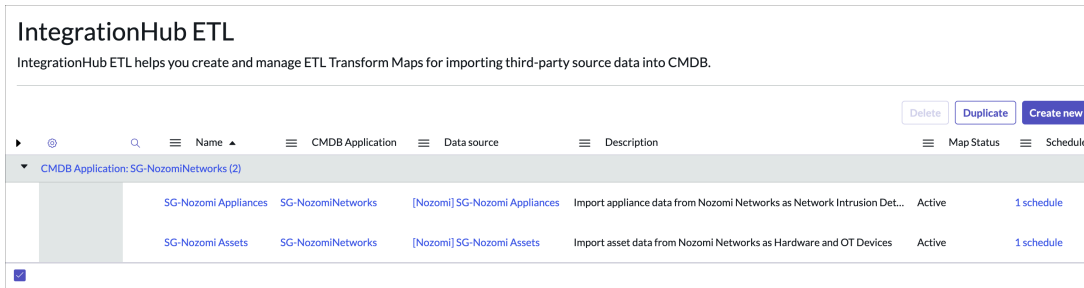
- Map the fields of the Nozomi Networks source tables with your custom tables
- Conditionally Import data into your custom tables
- Transform imported data, if required

Map Nozomi Networks data with IntegrationHub ETL

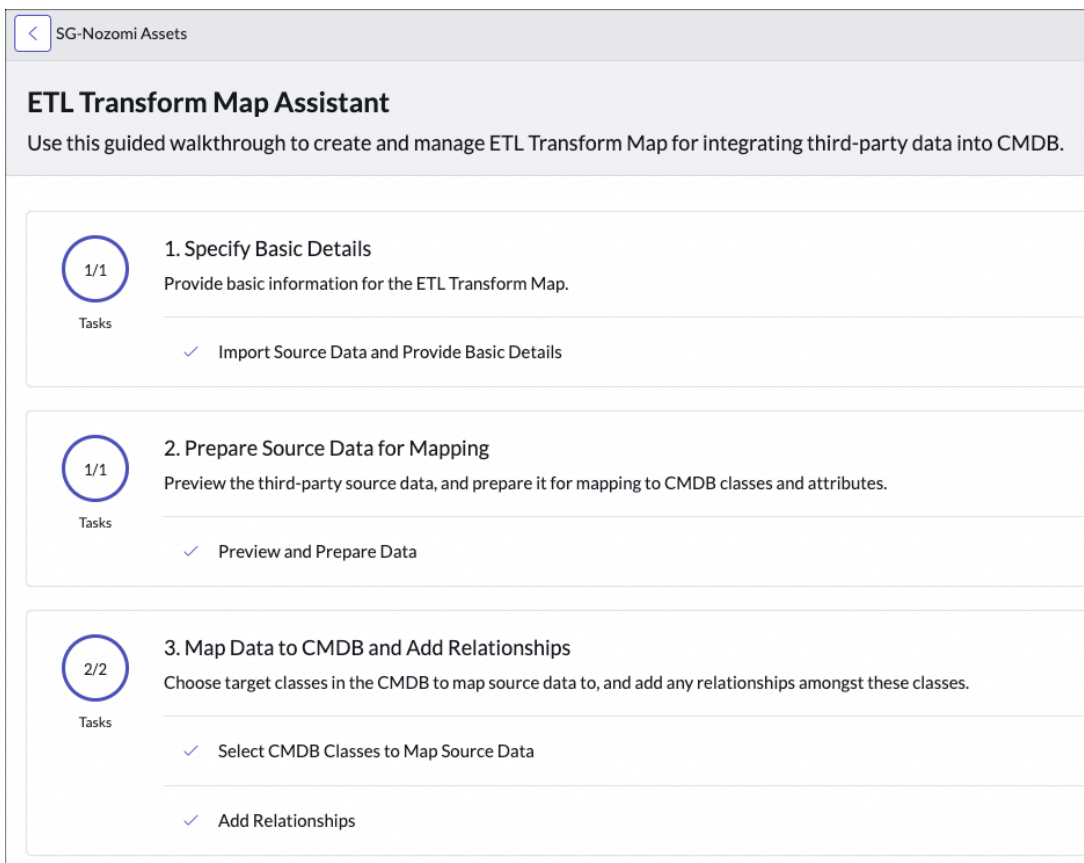
Discover how to use IntegrationHub ETL to map data from the **Service Graph Connector** application. to custom tables in ServiceNow.

Procedure


1. Search for **IntegrationHub ETL** in the navigation bar, to make sure that it is installed in your ServiceNow instance.



2. To start the configuration procedure to import data from the Nozomi Networks Service Graph connector to your custom tables, select **SG-Nozomi Assets**.



- To specify a sample import set to be used to edit the ETL Transform Map, select **Import Source Data and Provide Basic Details**.


 **Note:**
This requires the application to be run at least once.


- To go back to the previous menu, select the back arrow.

Specify Basic Details



← **Provide Basic Information for the ETL Transform Map**


Provide the template with some basic properties, and select a data source to map to CMDB.


* CMDB Application 


* Name 

Description

* Data Source  

Sample Import Set 

Preview Size Override 

Load Complete Schema 

- Select **Preview and Prepare Data**.

Prepare Source Data for Mapping

← **Preview and Prepare Data**

Nested Data Structure

Tree Collection

- object
- object(1)
- object(2)

The column schema is based on existing transform columns and 100 preview import set records. You can load complete schema in [Specify Basic Details](#) step. The table below displays raw source data. Click a column's action menu (☰) for specific data transformation options. You can also set columns to be ignored in mapping.

Show data structure

object	☰	☰	☰	☰	☰
appliance_hosts_json					
are_all_nodes_confirmed					
capture_device					
created_at					
description					

Here you can see existing transformations, and edit or create new ones.

6. To go back to the previous menu, select the back arrow.

7. Select **CMDB Classes to Map Source Data**.

The screenshot shows a configuration interface for mapping source data to CMDB classes. The page title is "Map Data to CMDB and Add Relationships" with a sub-header "Select CMDB Classes to Map Source Data". A "Mark as Complete" button is in the top right. Below the header, there is a descriptive text: "Set target class to map your source data. To set specific rules for how source data should map to classes, add a conditional class." Two buttons, "Add Class" and "Add Conditional Class", are provided. The main content area lists three classes:

- Conditional Class: Computer**
cmdb_ci_computer
If object.target_class_data_entity=cmdb_ci_computer
Buttons: Edit Class (toggle on), Edit Mapping
- Conditional Class: Network Gear**
cmdb_ci_netgear
If object.target_class_data_entity=cmdb_ci_netgear
Buttons: Edit Class (toggle on), Edit Mapping
- Basic Class: Hardware**
cmdb_ci_hardware
Buttons: Edit Class, Edit Mapping (toggle on)

Here you can see existing mapping from staging tables data to your custom **CMDB** tables. It is possible to modify:

- Existing mapping
- Create mapping to new classes
- Create mapping to new conditional classes

Map Nozomi Networks data with IntegrationHub ETL - example

An example of Nozomi Networks discovered Voice over Internet Protocol (VoIP) phones. These devices will be categorized in the **SG-Nozomi Assets** import set table as `voip_phone` under the `type` field. We will then map these devices into the ServiceNow Internet of Things (IoT) Device Configuration Management Database (CMDB) table.

About this task


You can add whatever conditions are required to correctly map the Nozomi Computers data to your own custom ServiceNow [CMDB](#) tables on this screen.

Procedure


1. Follow the [Map Nozomi Networks data with IntegrationHub ETL](#) (on page 40) procedure up to and including step 7 (on page 42)
2. Select **Add Conditional Class**.

Add Conditional Class

Use the condition builder to set how source column values will correlate to CMDB classes.

Collection 

If



Then

Else

3. Add conditions as necessary to correctly map the SG-Nozomi Assets data to your own custom ServiceNow [CMDB](#).

Add Conditional Class ✕

Use the condition builder to set how source column values will correlate to CMDB classes.

Collection object ▼

If

object.type ▼ is ▼ voip_phone ⊖ OR AND

Then

Class is IoT Device ▼

New Criteria

Else

Class is -- Select one -- ▼

Cancel Delete Class Save

4. When you have finished, select **Save**.

The new Conditional Class table shows as **IoT Device 1**.

Conditional Class Edit Class

IoT Device 1

cmdb_ci_iot
If object.type=voip_phone

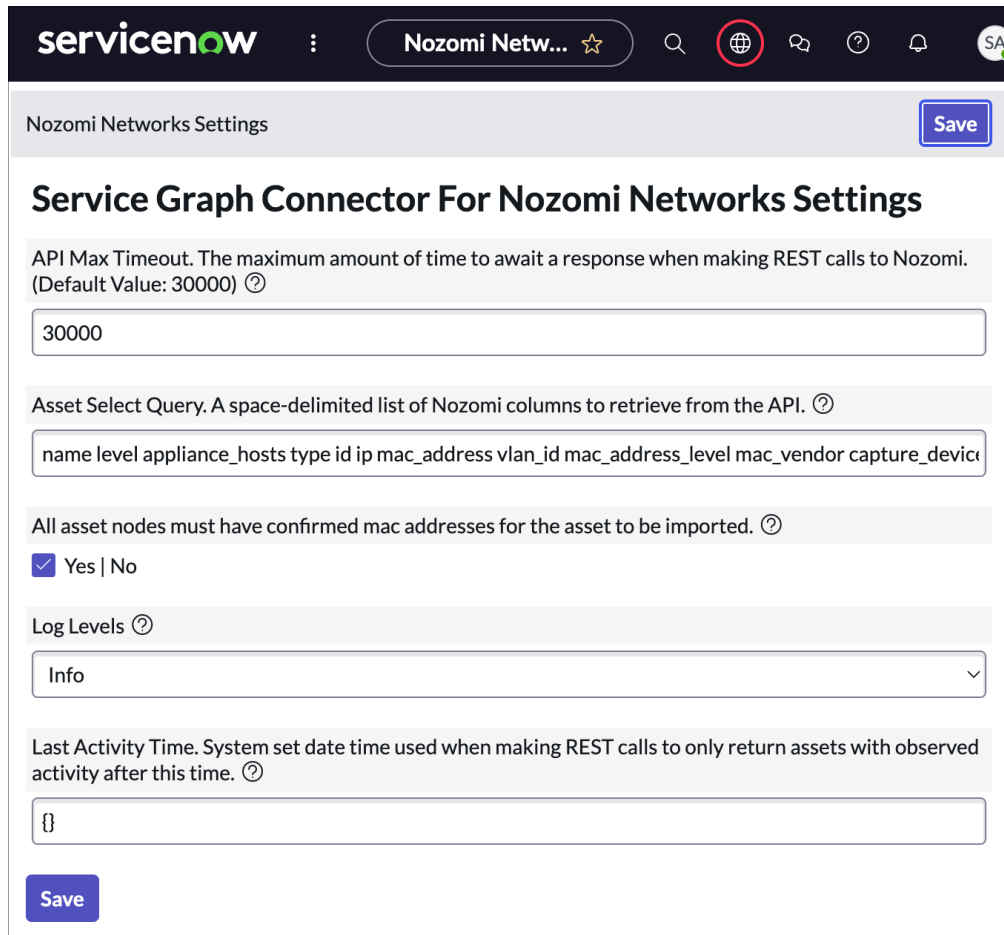
Set Up Mapping

Now, when the **Service Graph Connector** does a scheduled run, the data from the **SG-Nozomi Assets** table will be mapped into the ServiceNow [CMDB IoT Device](#) table.

System properties configuration

A description of how you can adjust additional settings through the system properties.

You can adjust additional settings through the system properties module in **Service Graph Connector for Nozomi > Admin > System Properties**. This is where you can make various adjustments to the Service Graph Connector import behaviors.



The screenshot shows the ServiceNow interface for configuring system properties. The breadcrumb trail is "Nozomi Networks Settings > Admin > System Properties". The page title is "Service Graph Connector For Nozomi Networks Settings". There are two "Save" buttons, one at the top right and one at the bottom left. The configuration includes:

- API Max Timeout:** A text input field containing "30000". Description: "The maximum amount of time to await a response when making REST calls to Nozomi. (Default Value: 30000)".
- Asset Select Query:** A text input field containing "name level appliance_hosts type id ip mac_address vlan_id mac_address_level mac_vendor capture_device". Description: "A space-delimited list of Nozomi columns to retrieve from the API."
- Mac Address Requirement:** A checkbox labeled "All asset nodes must have confirmed mac addresses for the asset to be imported." which is checked. The options are "Yes | No".
- Log Levels:** A dropdown menu currently set to "Info".
- Last Activity Time:** A text input field containing "{}". Description: "System set date time used when making REST calls to only return assets with observed activity after this time."

Figure 1. System properties

Add a new column to asset select query

When you add a new column to the asset select query, it is necessary to do some additional steps in order to have the new column available in the system.

About this task

Once a new column, such as **column_foo** has been added, you need to augment the data stream action that imports data into the staging table.

Procedure

1. To open Flow Designer, go to **All > Flow Designer**.

Result: A new page opens.

2. Select **Actions**.
3. In the **Search** field, search for the term **Get Nozomi Assets**.
4. Open the action and enter the **Script Parser** step.

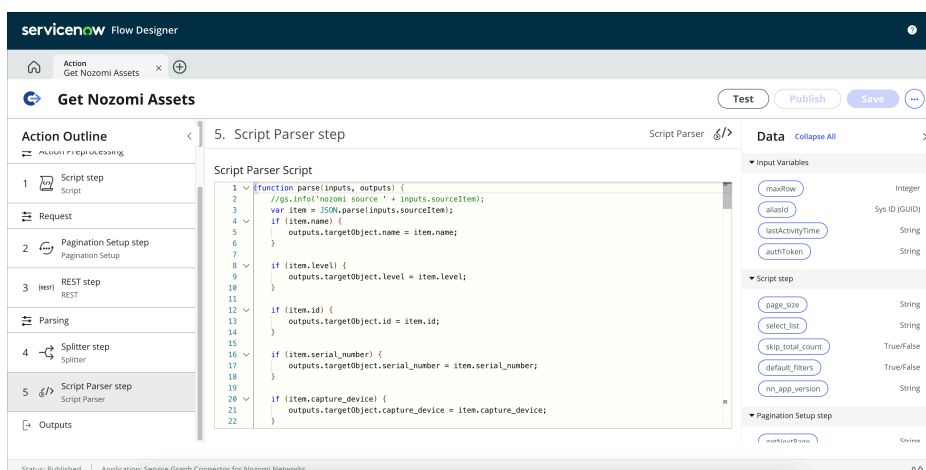
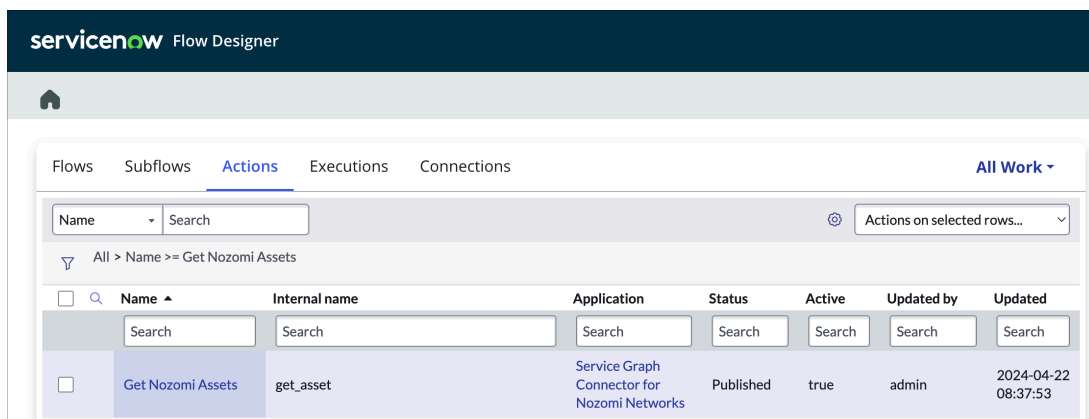


Figure 2. Script Parser step

This is where the script that parses the response live.

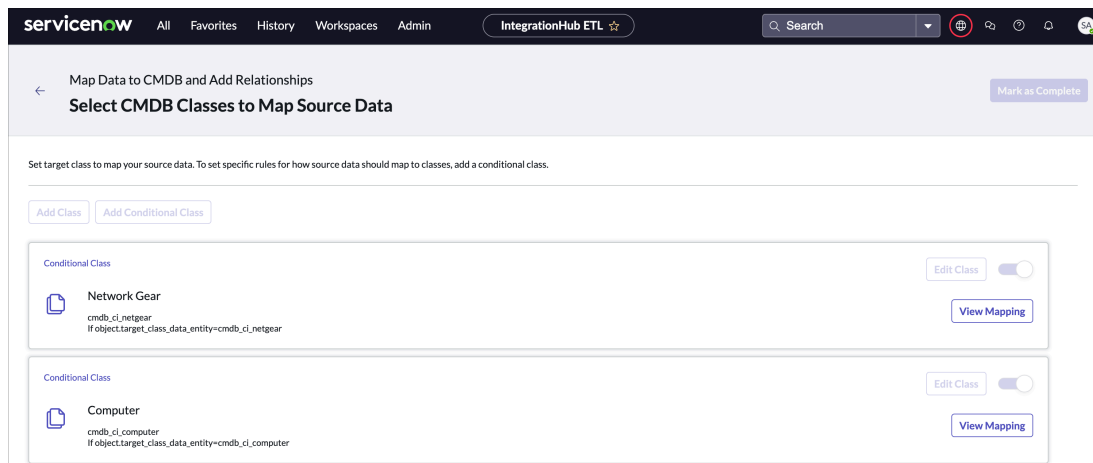
5. Immediately after `outputs.targetObject.custom_fields = tmpArray;` around line 180, add this code:

```
if (item.column_foo) {  
    outputs.targetObject.column_foo = item.column_foo;  
}
```

**Note:**

Where `column_foo` is the name of the new column. For each new column you will need to add similar code to that shown above.

6. To map our new data field into ServiceNow **CMDB** tables, open the **IntegrationHub ETL**.



Depending on where you want to map the new data, you might need to change existing classes, such as `Computer`, or add new ones.

7. For example, to add new data to `Computer`, in the right of the **Computer** section, select **View Mapping**.

Result: A new page opens.

8. On the left, available attributes for the selected class show. On the right, all the data fields available for the specific data source show.

Map to Computer View Class Details

Map to CMDB Transform Data

The column schema is based on existing transform columns and 100 preview import set records. You can load complete schema in [Specify Basic Details](#) step. Required attributes for this class are shown by default. Start mapping by dragging source data columns or transformed data columns to their CMDB class attributes

[Add Attribute](#)

Mapping to Computer (cmdb_ci_computer)
From collection: object

▼ Source Native Key ⓘ
Source Column **object-id_unique** ⓘ

▼ Source Recency Timestamp ⓘ
Source Column ⓘ

▼ Name ⓘ
Source Column ⓘ

▼ Serial number ⓘ
Source Column ⓘ

Data

- object
 - appliance_hosts_json
 - are_all_nodes_confirmed
 - capture_device
 - created_at
 - description
 - firmware_version
 - id
 - id_unique
 - id_unique_ot
 - ip_addresses_json
 - is_networkgear
 - last_activity_time

**Note:**

Some attributes might be missing. You can select **Add attribute** to add them.

9. For more details on **IntegrationHub ETL** and its possible customizations, see the [ServiceNow documentation](#).

Generate an API key

Before you can use an API key, you must generate one.

Before you begin


Before you do this procedure, make sure that you have:

- Created a user to associate with your third-party application
- Assigned the user a role that grants the necessary permissions and scope within Vantage

About this task

Once an [API](#) key has been created, you cannot edit it. You can only revoke it.

Procedure

1. Log into Vantage as the user who will own the [API](#) key.
2. In the top navigation bar, select  > **Profile**.
3. Select **API Keys**.

Result: The **API Keys** page opens.

4. In the **Description** field, enter a description for the [API](#) key.

Generate new API key

Give a human-friendly description to the API key.

Example IP ranges: 1.2.3.4/24 or 1.2.3.4/24, 2.3.4.5/16.
If no IP range is defined, the range defined in general settings controls.
If an IP range is defined, it controls OVER the one defined in general settings.

Organization
Acme

Default Organization linked to this ApiKey. It will be used by request authenticated by this API Key.
If no Organization is sent in the request header, the default Organization will be used.



Note:

Nozomi Networks recommends that the description includes the name of the application that will connect with the [API](#) key.

5. **Optional:** Enter a range of allowed addresses in the **Allowed IPs** field. Only applications within this range will be permitted to connect with this key.

6. In the **Organization** field, select the organization that will be the default for this [API](#) key.


**Note:**

If an [API](#) request that uses this key doesn't include an organization, the default organization is used.

7. Select **Generate**.

Result: Vantage generates a key and displays its:

- Key name
- Key token
- Allowed ips
- Linked organization

8.  **Important:**

You will need some of these values when you configure your third-party application. While the name is shown in the Vantage after this point, the token is not shown again. If you lose this data, you must generate a new [API](#) key.

Record these details:

- Key name
- Key token
- Allowed ips

Generate an OpenAPI key

The profile settings menu lets you generate an OpenAPI key.

Procedure

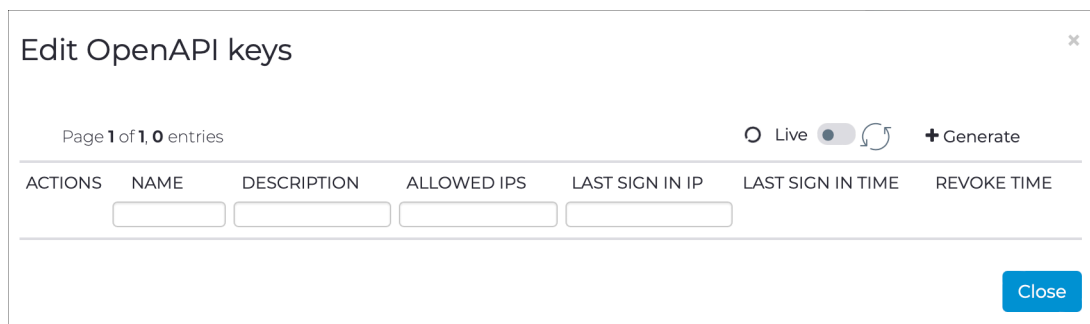
1. In the top navigation bar, select 

Result: A menu shows.

2. Select **Other actions**.
3. Select **Edit OpenAPI keys**.

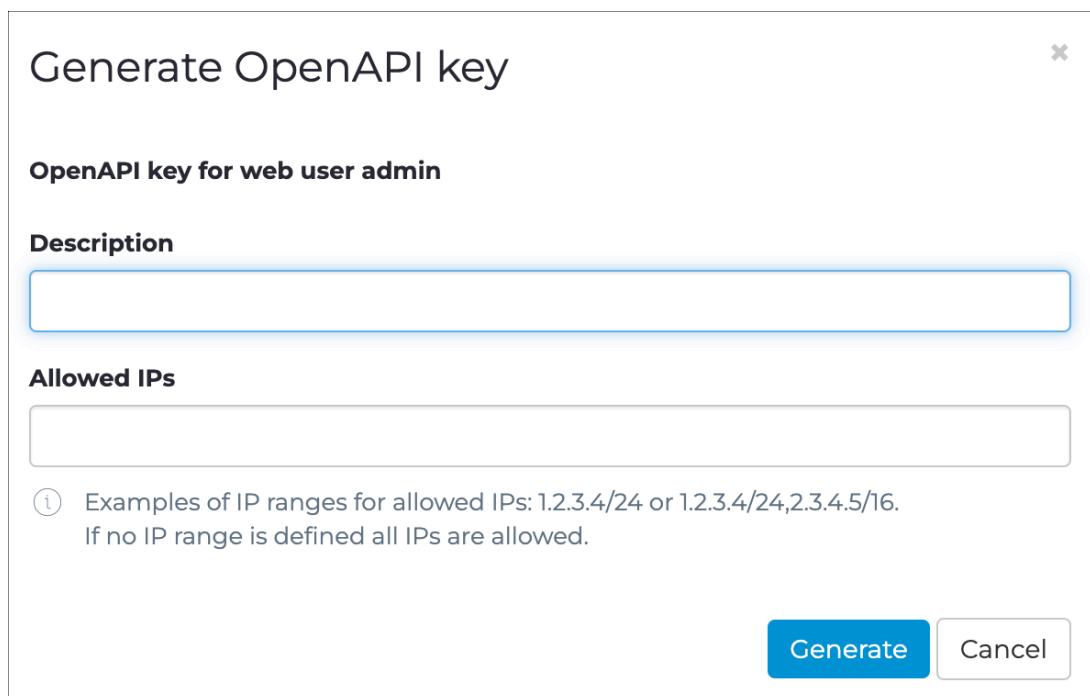
Result: A dialog shows.

4. In the top right, select **+ Generate**.



Result: A dialog shows.

5. In the **Description** field, enter a description for the OpenAPI key.



6. In the **Allowed IPs** field, enter the details of the allowed addresses.
7. Select **Generate**.

Results

Your OpenAPI key has been generated.

Chapter 4. Additional configuration



Configure an MID server

To use a Management, Instrumentation, and Discovery (MID) server with the **Service Graph Connector** application, you will need to configure your ServiceNow instance.

Procedure

1. Go to the filter navigator in the upper left.
2. Search for **MID Server > Servers**.

Name	Host name	Status	Validated	Version	Last refreshed	Started	Stopped	Router	Logged in user
		Down	Yes	quebec-12-09-2020_patch9-10-28-2021_11...	2021-12-06 08:04	2021-12-02 12:37	2021-12-02 12:37		midserveruser

A list of existing **MID** Servers and their status shows.

3. Select **New**.

Version compatibility could not be determined. Verify that the MID Server is configured as expected. [More Info](#)

The MID Server facilitates communication between the ServiceNow platform and external applications, data sources, and services. Add MID Server configuration parameters and capabilities here. Read about [configuring the MID Server](#) or find assistance with [MID Server troubleshooting](#).

Name:
 Status:
 Validated: Rekey
 Validated At:
 Validated By:
 Version:
 Last refreshed:
 Started:
 Stopped:
 Time zone:
 Idle Since:
 Logged in user:
 Container ID:
 Profile ID:
 Host name:
 IP address:
 Router:
 Network:
 Host OS:
 Windows domain:
 Unresolved issues:
 Is using a custom certificate:
 Is using mutual authentication:
 Purpose:
 Invalidated At:
 Invalidated By:

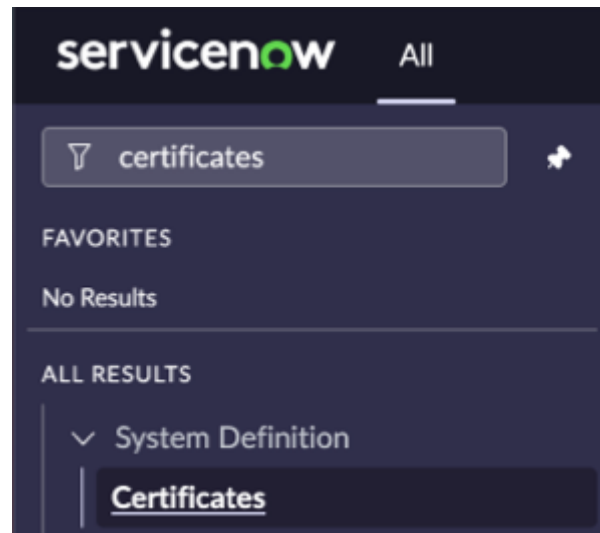
4. Enter the necessary information in the fields as necessary.
5. Select **Submit**.

Add a trusted certificate

If Nozomi Networks system has a trusted certificate, you have to import it.

Procedure

1. In the left sidebar, enter **certificates** and press enter.



2. Under **System Definition**, select **Certificates**.
3. In the top right corner, select **New**.

Result: A dialog shows.

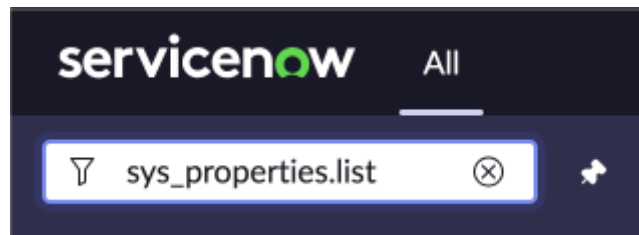
4. Enter the details as necessary.
5. Select **Submit**.

Add a non-trusted certificate

If Nozomi Networks system has a non-trusted certificate, you will need to add two system properties before you can add a certificate.

Procedure

1. Under **System Definition**, select **All**
2. In the left sidebar, enter `sys_properties.list` and press enter.



Result: A list shows.

3. In the top left section, in the search field, enter `com.glide.communications.httpClient.verify_hostname`
4. Press enter.
5. If the file does not exist, create it.
 - a. Select **Create**.
 - b. Enter the details as necessary.
 - c. Select **Submit**.
6. In the **Value** column, set the value to `false`
7. In the top left section, in the search field, enter `com.glide.communications.httpClient.verify_revoked_certificate`
8. Press enter.
9. If the file does not exist, create it.
 - a. Select **Create**.
 - b. Enter the details as necessary.
 - c. Select **Submit**.
10. In the **Value** column, set the value to `false`
11. **Optional:** In the top left section, in the search field, enter `com.glide.communications.trustmanager_trust_all`
12. Press enter.
13. If the file does not exist, create it.
 - a. Select **Create**.
 - b. Enter the details as necessary.
 - c. Select **Submit**.

14. In the **Value** column, set the value to `true`
15. Do the [Add a trusted certificate \(on page 56\)](#) procedure.

Chapter 5. Frequently Asked Questions



How to change which Nozomi assets get targeted to which ServiceNow classes?

A description of how you can change which Nozomi Networks assets get targeted to which ServiceNow classes.

To determine which ServiceNow class and [OT](#) asset type best fits each asset, the **Service Graph Connector** integration uses a combination of:

- Type
- Roles
- [operating system \(OS\)](#)

This logic is in the **SGNozomiClassCalculator**. To make customizations to the default behavior of the class modeling, you can create an extension point script that lets users make final adjustments to the target class data for each asset before the [ETL](#) imports the source data.

You can use the filter navigator, to go to **Service Graph Connector for Nozomi > Admin > Extension Points**. You can then open the **SGNozomiClassCalculatorExtension** extension point record.

A built-in example will show with a `getTargetClass` function that the main import flow will execute.

You can select the **create implementation** related link to generate a new script include. Now you can adjust the items that you want to.

How can I add additional or custom fields from the Nozomi API into my integration?

A description of how you can add additional, or custom fields, from the Nozomi Networks application programming interface (API) into your ServiceNow integration.

The integration will pre-process and flatten the [API](#) data before importing it to the staging table. For both asset and appliance imports, extension points have been provided in which the flattened item that has been processed so far and the raw [API](#) item returned from the data stream action are passed through. This lets users make additional changes to the data before importing to the staging table.

You can use the filter navigator, to go to **Service Graph Connector for Nozomi > Admin > Extension Points**. You can then open either the records for:

- **SGNozomiAssetsExtension**, or
- **SGNozomiAppliancesExtension**

A built-in example will show that has a process function where the flattened item built by the integration prior and the [API](#) item returned from the data stream action are passed through.

You can select the **create implementation** related link to generate a new script include. You can now adjust the flattened Item object and return it so that it will be included in the transforms.

Why am I seeing duplicates after the first import?

A description of why it is possible that you will see duplicate items even though the network adapter media access control (MAC) addresses match.

The **Service Graph Connector** application uses the *Identification and Reconciliation Engine (IRE)* to rely on successfully identifying and updating existing *CMDB* data based on identification rules. One of the primary identification rules that the integration relies on is the Network Adapter lookup rule in the **Hardware** table.

You can go to **Under Configuration > CI Class Manager** to search for the hardware class and open the **Identification rule** section. There should be a Network adapter lookup rule.

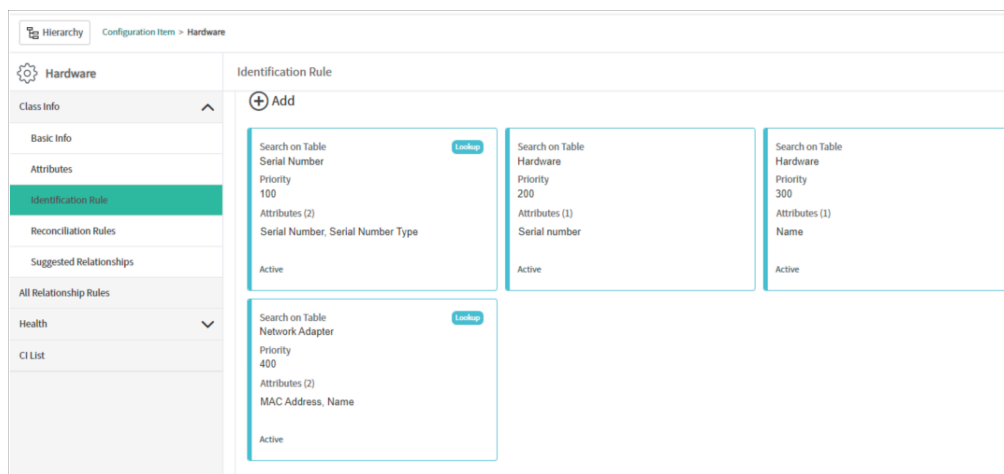


Figure 3. Identification Rule

The network adapter lookup identification rule looks for matching network adapters based on the **Name** and **MAC address** values. Other sources of data populate the network adapter with a name with another value, but *Service Graph Connectors* populate the name value with the *media access control (MAC)* address as well. If this is causing problems with your *CMDB* data, consider removing the **Name** from the network adapter lookup.

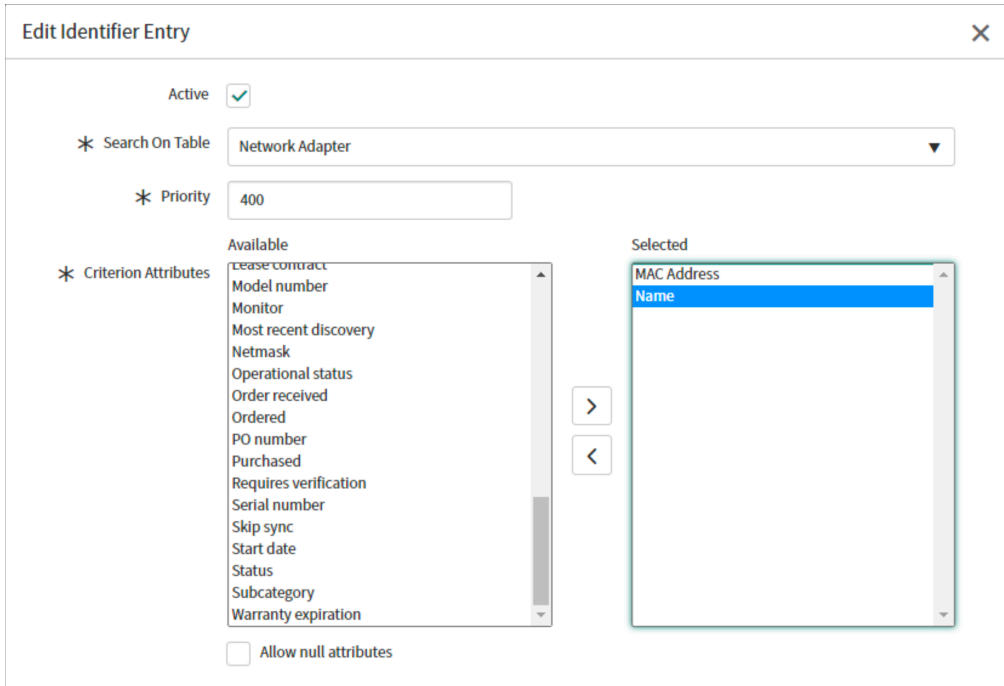


Figure 4. Edit Identifier Entry

The network adapter lookup identification rule by default requires an exact count match of network adapters to pass the check. This means that if the Nozomi Networks asset being imported has two **MAC** addresses and during the lookup only one of the **MAC** addresses matches with an existing **CMDB** record, the check will fail. This will result in a duplicate. To disable this feature, on the network adapter lookup rule, you can open the advanced options and disable the **Enforce exact count match** setting. This will allow identification in the case where a **CI** in ServiceNow only has one **MAC** address, but the Nozomi Networks asset has Multiple.

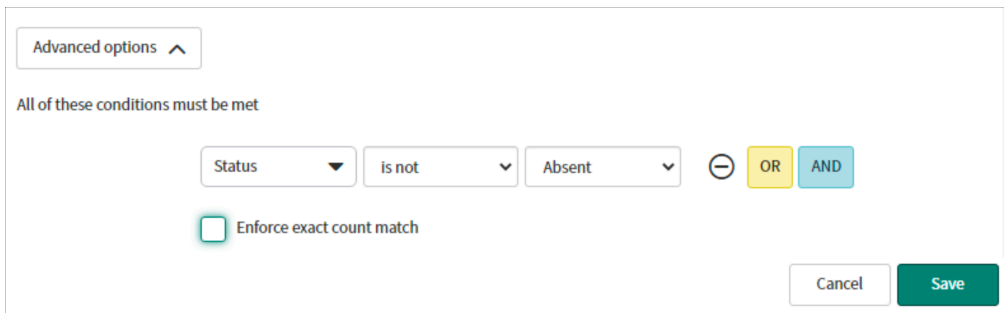


Figure 5. Edit Identifier Entry

Chapter 6. Troubleshooting



Service Graph Connector application is no longer working

Possible cause

A communication, or connectivity, problem has caused the application to stop working.

Procedure

Verify connectivity is permitted from the Nozomi Networks appliance to the ServiceNow instance.

Procedure

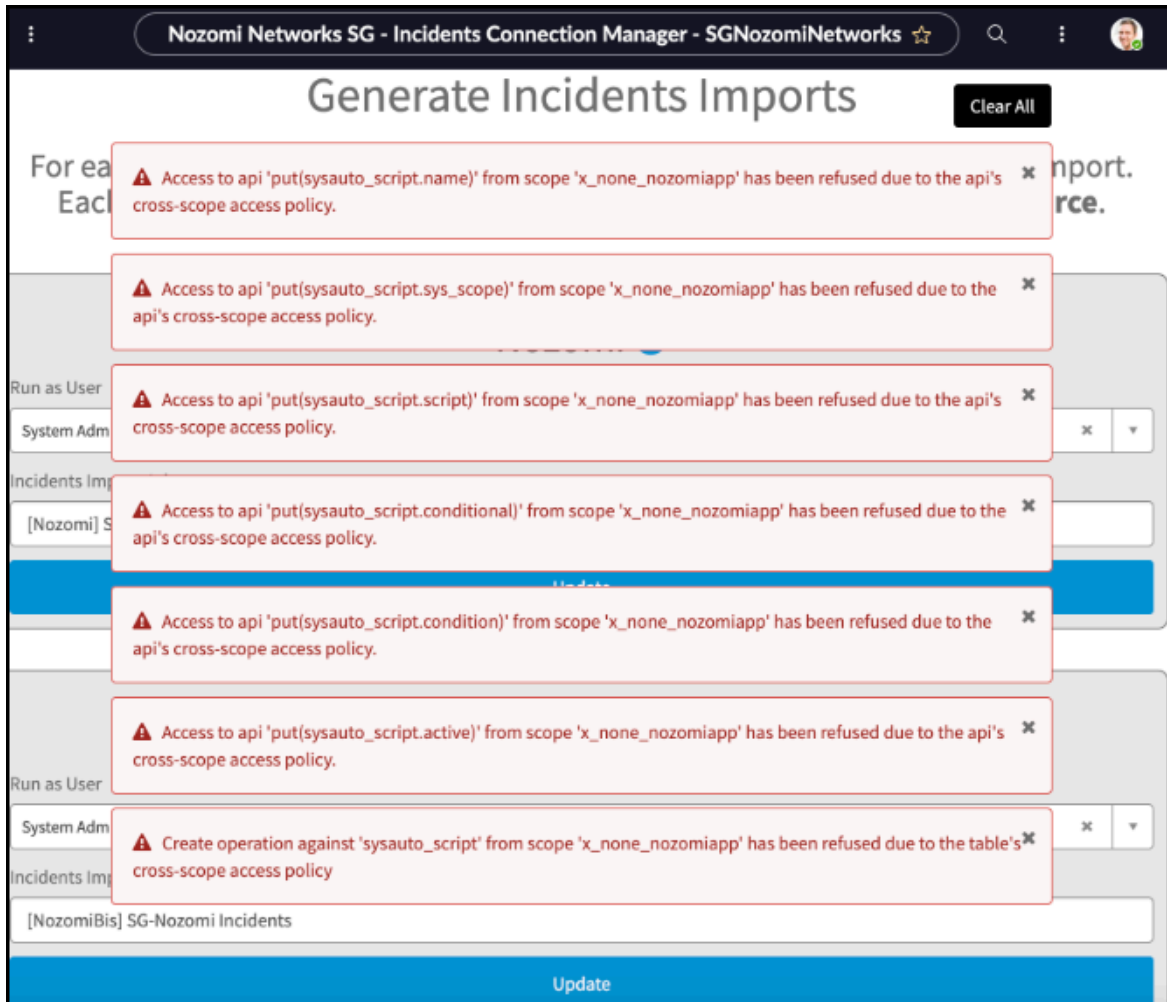
Make sure that if there is a *MID* server in use is properly configured to permit communications.

If none of the previous solutions work, please contact our [Customer Support](#) team.

Cross-scope access-policy error shows

When you generate incidents imports, you might see an error message. This can happen even if you have followed the guided set-up, and set the cross-scope privileges correctly.

About this task



Procedure

1. Go to the table definition record in the **Scheduled Script Execution Table** [sysauto_script].
2. Select the **Application Access** tab.

The screenshot shows the 'Application Access' configuration for the 'Scheduled Script Execution' table. The 'Application' is set to 'Global'. Under the 'Application Access' tab, the 'Accessible from' dropdown is set to 'All application scopes'. The 'Can read' checkbox is checked. The 'Can create' and 'Can update' checkboxes are checked and highlighted with a red box. The 'Can delete' checkbox is unchecked. There are also options for 'Allow access to this table via web services' (checked) and 'Allow configuration' (unchecked).

3. Make sure that these checkboxes are selected:
 - **Can create**
 - **Can update**
4. Select the **Controls** tab.
5. Select the **Live feed** checkbox.

The screenshot shows the 'Controls' configuration for the 'Scheduled Script Execution' table. The 'Label' is 'Scheduled Script Execution', the 'Name' is 'sysauto_script', and it 'Extends table' 'Scheduled Job'. The 'Extensible' checkbox is checked. The 'Live feed' checkbox is unchecked and highlighted with a red box. The 'Columns', 'Controls', and 'Application Access' tabs are visible at the top.

6. Select **Save**.
7. Deselect **Live feed** checkbox.
8. Select **Save** again.

What to do next

Do the [Configure incidents import \(on page 33\)](#) procedure again.

Glossary



Application Programming Interface

An API is a software interface that lets two or more computer programs communicate with each other.

Central Management Console

The Central Management Console (CMC) is a Nozomi Networks product that has been designed to support complex deployments that cannot be addressed with a single sensor. A central design principle behind the CMC is the unified experience, that lets you access information in the similar method to the sensor.

Configuration Item

A CI is any computer, device, software, or service in the CMDB. A CI's record will include all of the relevant data, such as manufacturer, vendor, location, etc. Configuration items can be created or maintained either using tables, lists, and forms within the platform, or using the Discovery application.

Configuration Management Database

The CMDB in ServiceNow helps you track not only the configuration items (CIs) within your system, but also the relationships between those items.

Extract Transform Load

ETL definitions extract data from a source table, transform the data as desired, and load the data into one or more target tables. ETL definitions also support nested data structures.

Identification and Reconciliation Engine

IRE is an underlying key component in Identification and Reconciliation, providing a centralized framework to perform identification and reconciliation processes across different data sources. IRE uses identification rules, reconciliation rules, and IRE data source rules when processing incoming data before inserting that data to the CMDB.

Information Technology Operations Management

ServiceNow ITOM is a suite of cloud-based tools and solutions designed to help organizations streamline and optimize their IT operations. It provides capabilities for monitoring, managing, and automating various aspects of IT infrastructure and services. ServiceNow ITOM aims to enhance visibility, improve service delivery, and increase the overall efficiency of IT operations within an organization.

Internet of Things

The IoT describes devices that connect and exchange information through the internet or other communication devices.

Management, Instrumentation, and Discovery

The Management, Instrumentation, and Discovery (MID) Server is a Java application that runs as a Windows service or UNIX daemon on a server in your local network. The ServiceNow® MID Server enables communication and the movement of data between a ServiceNow instance and external applications, data sources, and services.

Media Access Control

A MAC address is a unique identifier for a network interface controller (NIC). It is used as a network address in network segment communications. A common use is in most IEEE 802 networking technologies, such as Bluetooth, Ethernet, and Wi-Fi. MAC addresses are most commonly assigned by device manufacturers and are also referred to as a hardware address, or physical address. A MAC address normally includes a manufacturer's organizationally unique identifier (OUI). It can be stored in hardware, such as the card's read-only memory, or by a firmware mechanism.

Network Intrusion Detection Systems

A NIDS is a security mechanism designed to monitor and analyze network traffic for signs of unauthorized access, misuse, or other malicious activity. NIDS are an integral part of network security infrastructure and are used to protect networks from various threats such as hacking attempts, malware infections, denial-of-service (DoS) attacks, and data breaches.

Nozomi Networks Operating System

N2OS is the operating system that the core suite of Nozomi Networks products runs on.

Operating System

An operating system is computer system software that is used to manage computer hardware, software resources, and provide common services for computer programs.

Operational Technology

OT is the software and hardware that controls and/or monitors industrial assets, devices and processes.

Voice over Internet Protocol

VoIP is a technology for making voice calls using the internet instead of traditional phone lines. VoIP converts voice signals into digital data packets and transmits them over the internet to recipients, offering advantages like cost savings and flexibility.