NOZOMI NETWORKS

ServiceNow Service Graph Connector
Integration Guide

SGC v1.4.4 — 2024-09-09

Legal notices

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

Copyright

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

Overview

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

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 one-way integration from the Nozomi Networks platform to the ServiceNow instance. Data is pulled from the Nozomi Networks connected instance on a schedule that the administrator of the **Service Graph Connector** application sets.

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 21.7, or higher
- 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 51).

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.

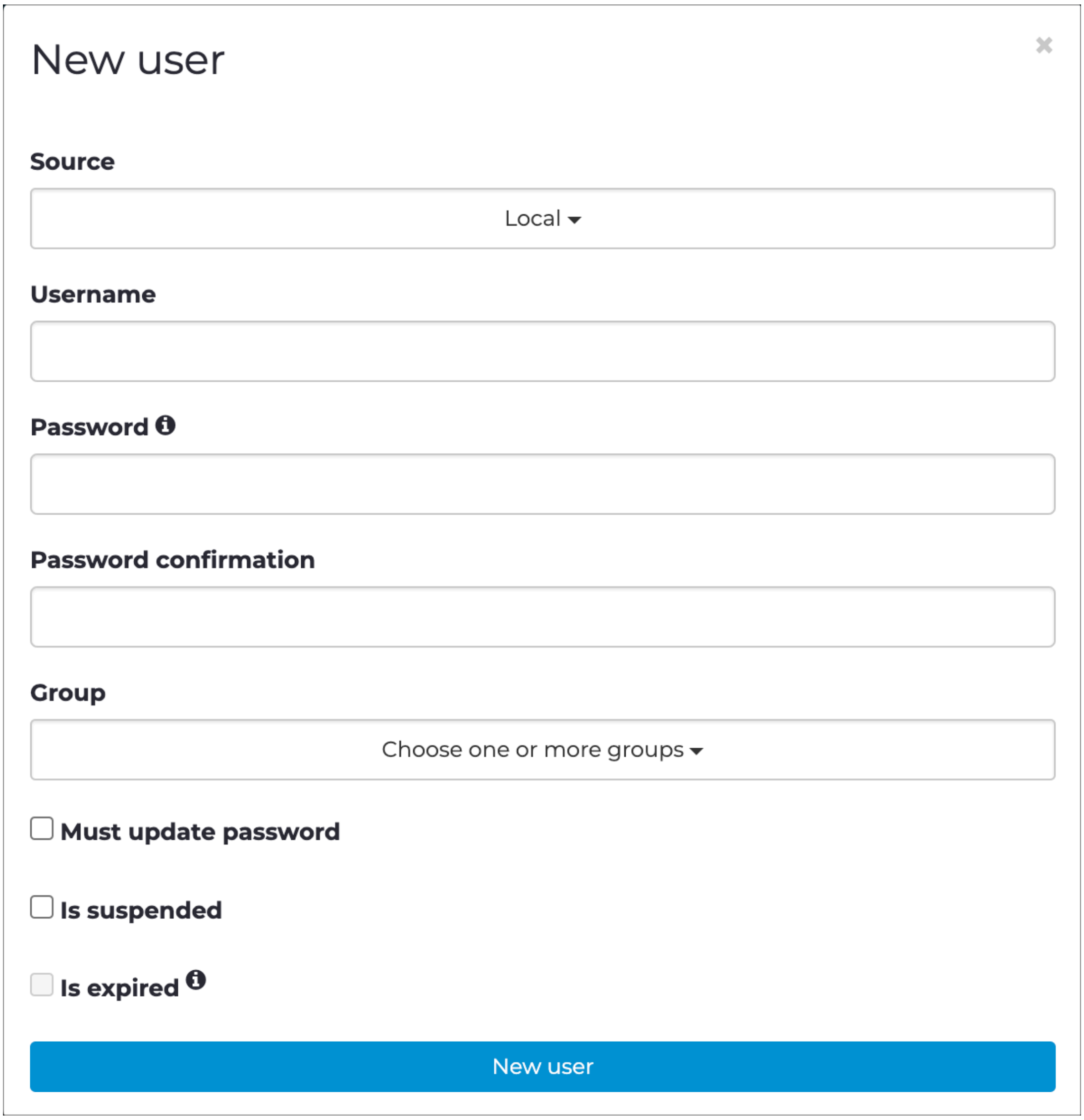
3. In the top right section, select **Users**.

   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

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.

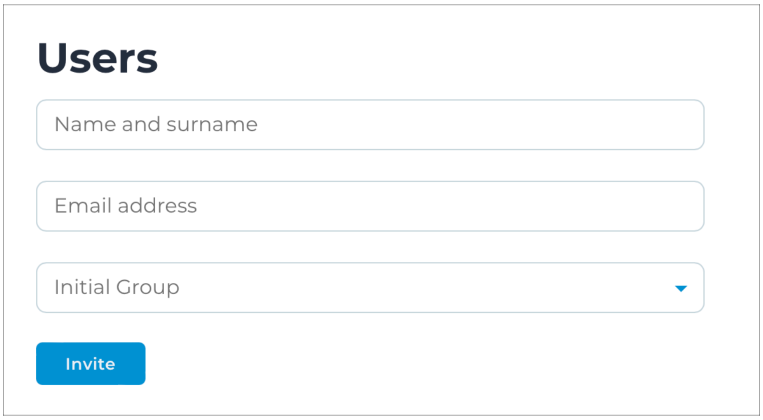
2. In the **Teams** section, select **Users**.

   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.



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:

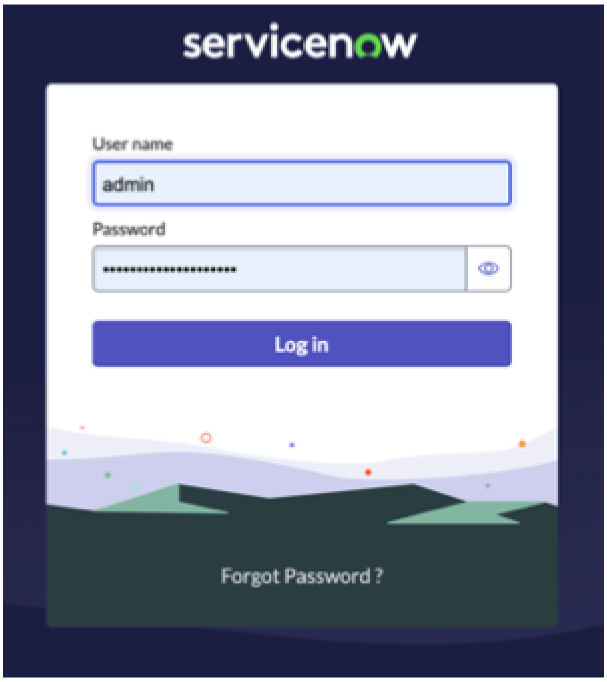
- Install the Service Graph Connector application (on page 20)
- Guided Setup for the Service Graph Connector (on page 22)

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.

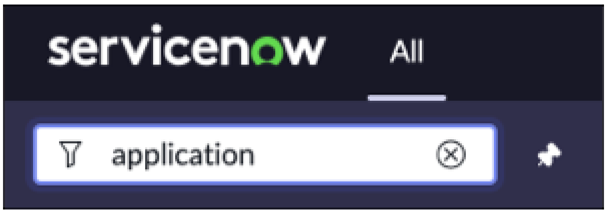


User name

admin

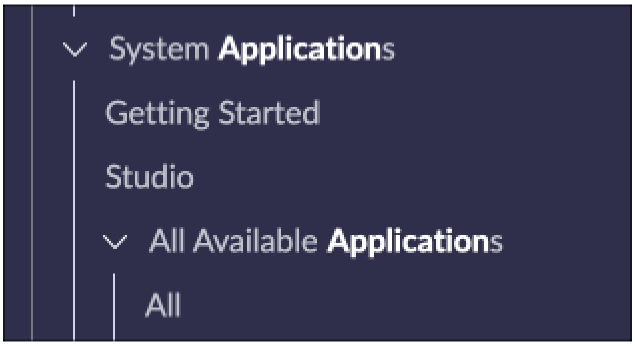
Password

2. In the left sidebar, search for application.

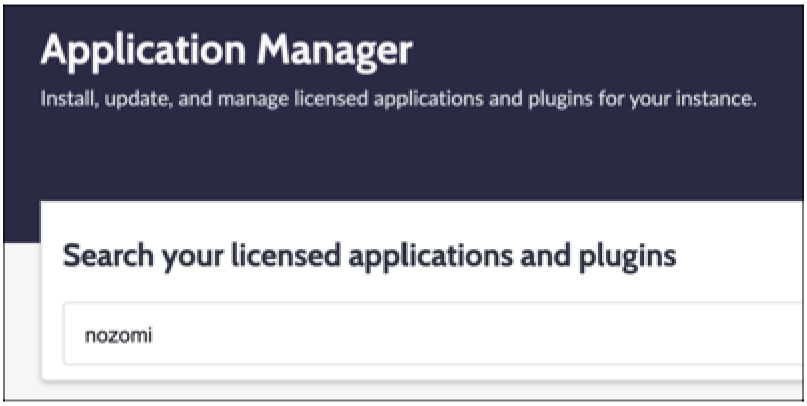


application

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



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



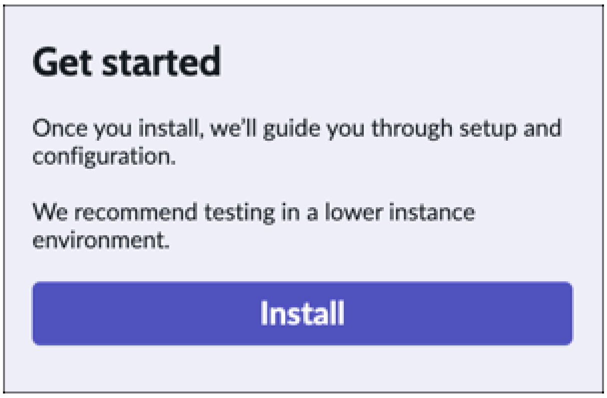
Application Manager

Install, update, and manage licensed applications and plugins for your instance.

Search your licensed applications and plugins

nozomi

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



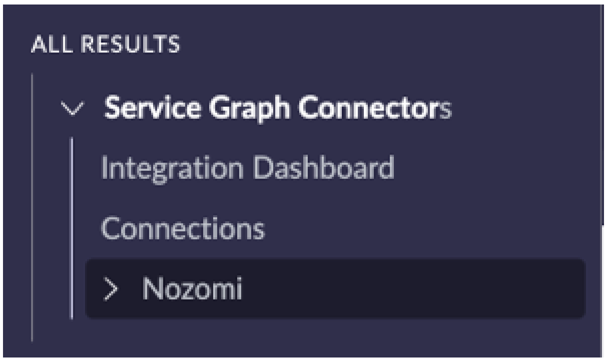
Get started

Once you install, we'll guide you through setup and configuration.

We recommend testing in a lower instance environment.

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.

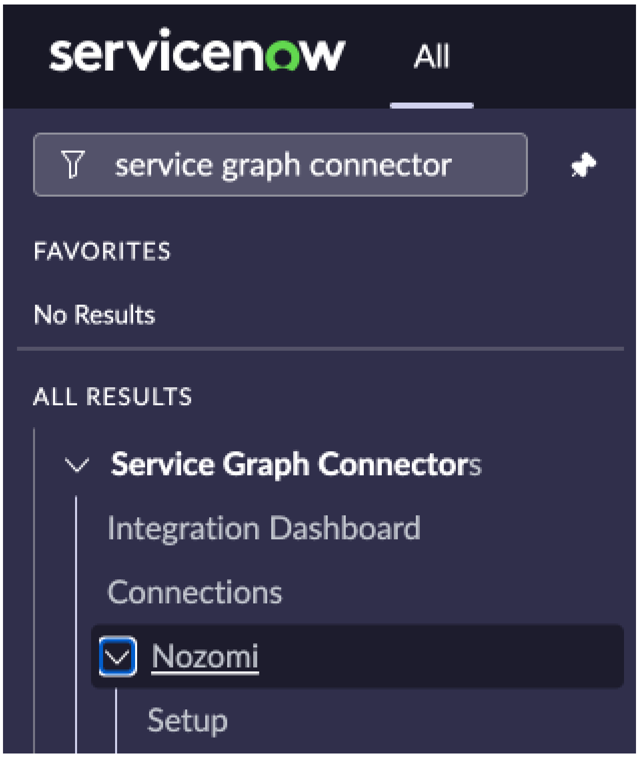


Guided Setup for the Service Graph Connector

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.*

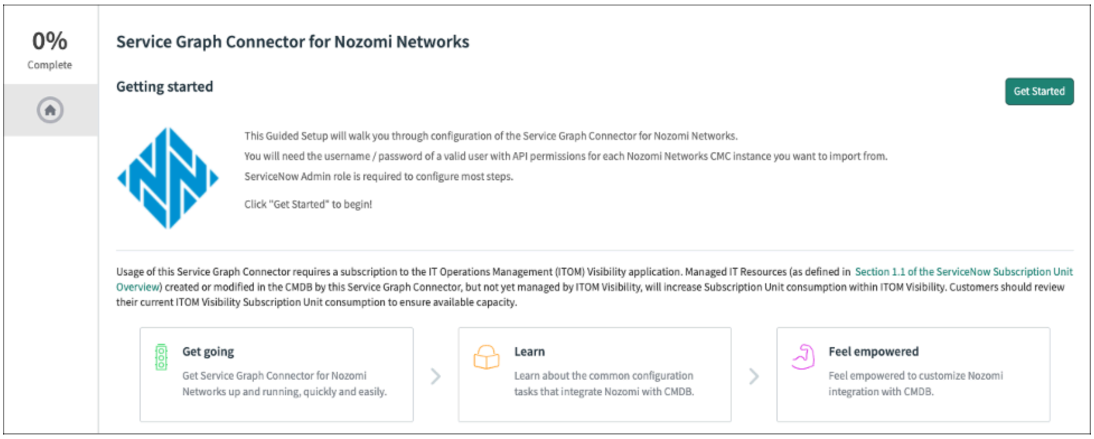
Procedure

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**.



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

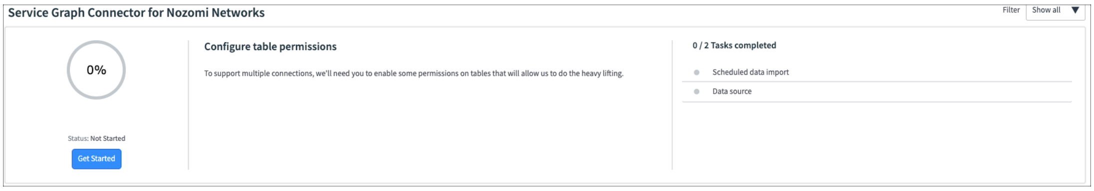
*Learn how to configure table permissions within the **Service Graph Connector for Nozomi** application.*

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**.



Service Graph Connector for Nozomi Networks

Status: Not Started

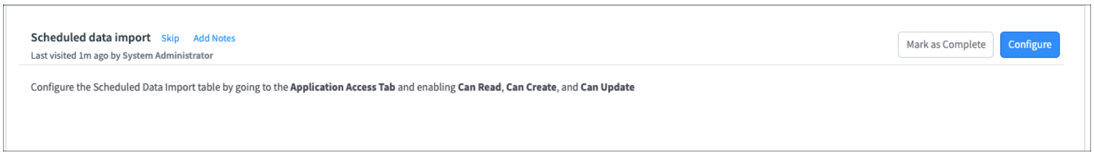
Configure table permissions

To support multiple connections, we'll need you to enable some permissions on tables that will allow us to do the heavy lifting.

0 / 2 Tasks completed

- Scheduled data import
- Data source

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

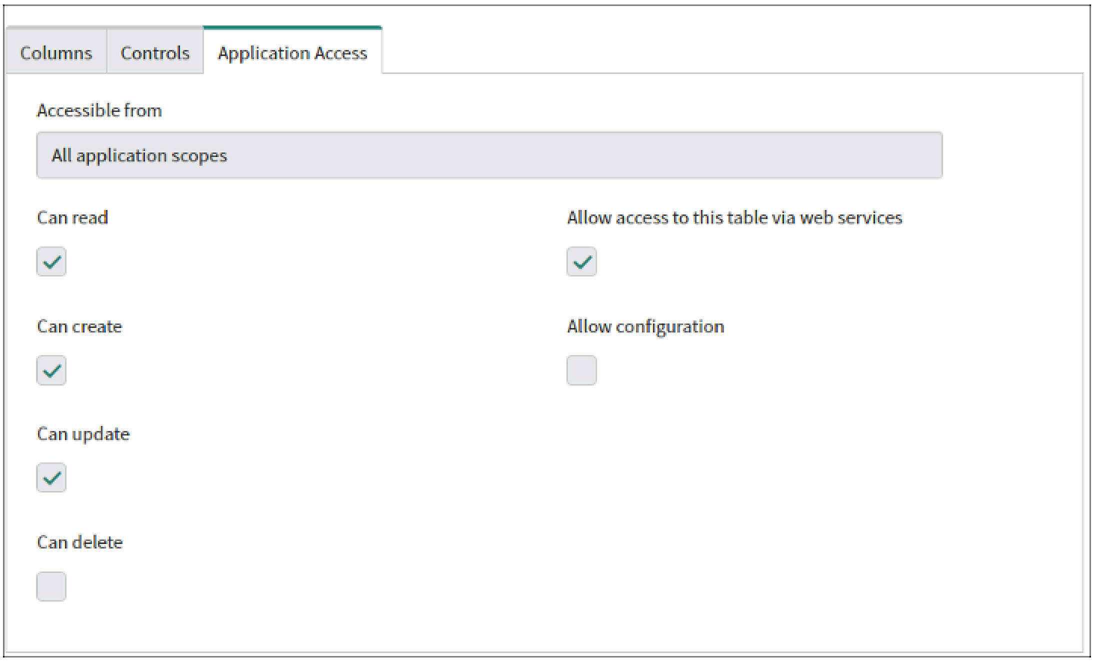


Scheduled data import

Last visited 1m ago by System Administrator

Configure the Scheduled Data Import table by going to the **Application Access Tab** and enabling **Can Read**, **Can Create**, and **Can Update**

7. Select **Application Access**.



Accessible from: All application scopes

Can read ☑

Can create ☑

Can update ☑

Can delete ☐

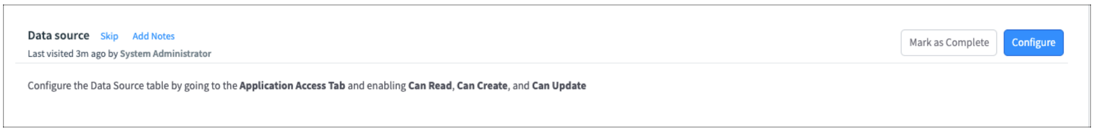
Allow access to this table via web services ☑

Allow configuration ☐

8. Select these options:
    - **Can read**
    - **Can create**
    - **Can update**

9. Select **Mark as Complete**.

10. In the **Data source** section, select **Configure**.



Last visited 3m ago by System Administrator

Configure the Data Source table by going to the **Application Access Tab** and enabling **Can Read**, **Can Create**, and **Can Update**

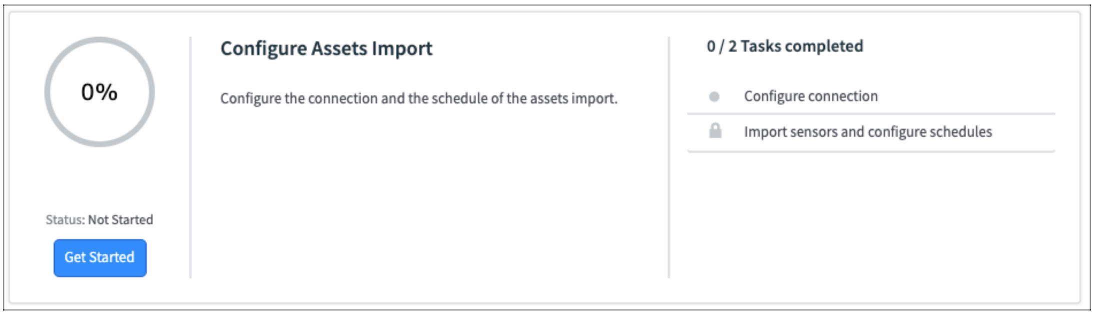
11. Do steps 8 (on page 24) and 9 (on page 24) again.

Configure assets import

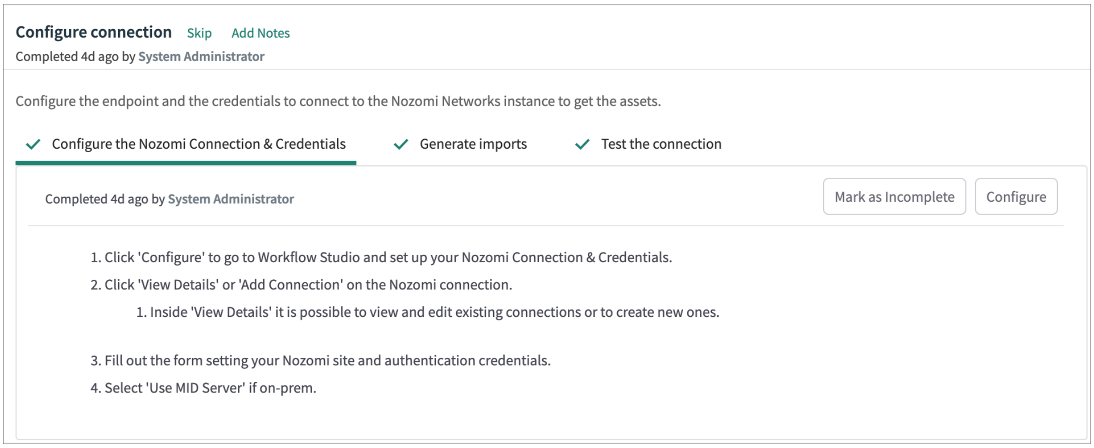
*Discover the detailed process of configuring asset imports within the **Service Graph Connector** application. This includes setting up connections, validating sensors, configuring schedules, and executing data imports, to ensure seamless integration and data synchronization for efficient network asset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

Procedure

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


0%
Status: Not Started
Get Started
Configure Assets Import
Configure the connection and the schedule of the assets import.
0 / 2 Tasks completed
Configure connection
Import sensors and configure schedules

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

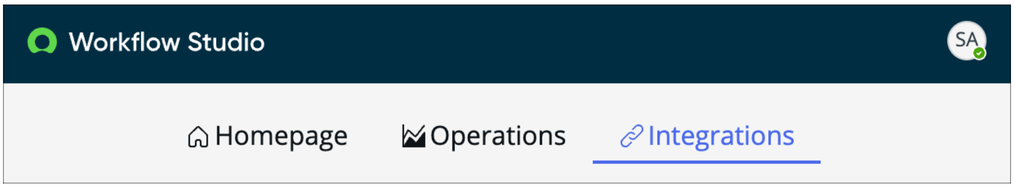

Configure connection
Skip
Add Notes
Completed 4d ago by System Administrator
✓ Configure the Nozomi Connection & Credentials
✓ Generate imports
✓ Test the connection
Completed 4d ago by System Administrator
Mark as Incomplete
Configure

Configure the endpoint and the credentials to connect to the Nozomi Networks instance to get the assets.

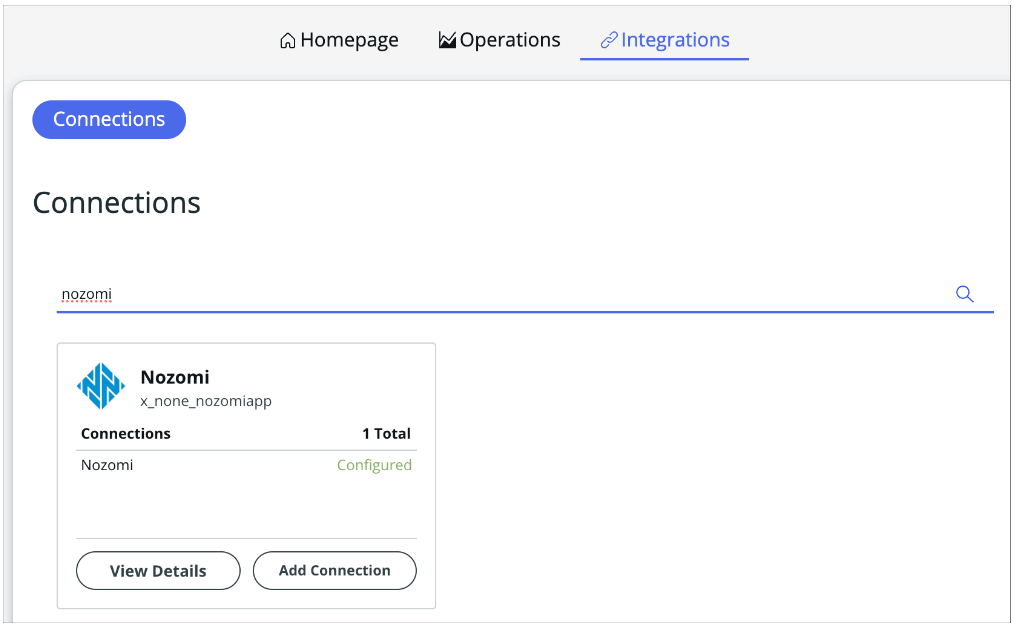
1. Click 'Configure' to go to Workflow Studio and set up your Nozomi Connection & Credentials.
2. Click 'View Details' or 'Add Connection' on the Nozomi connection.
   1. Inside 'View Details' it is possible to view and edit existing connections or to create new ones.
3. Fill out the form setting your Nozomi site and authentication credentials.
4. Select 'Use MID Server' if on-prem.

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**.

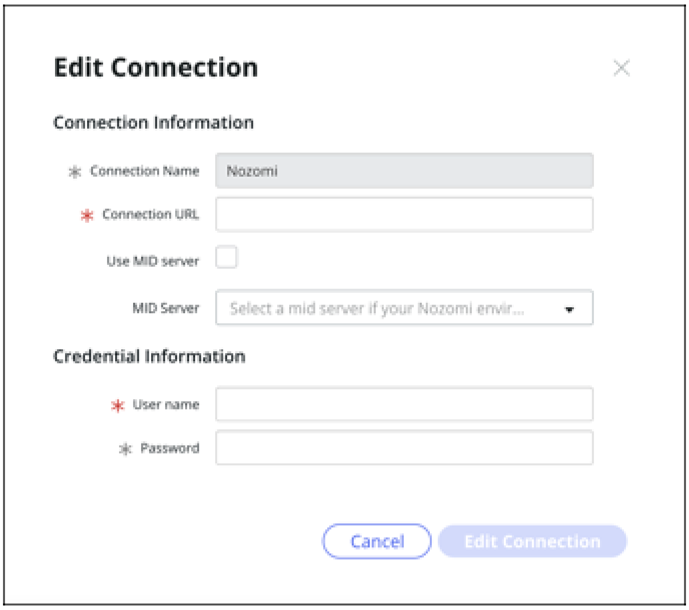


   b. In the search field, search for **Nozomi**.



5. Select **Add Connection**.

6. Enter your site information.



Edit Connection

Connection Information

* Connection Name: Nozomi

* Connection URL:

Use MID server: □

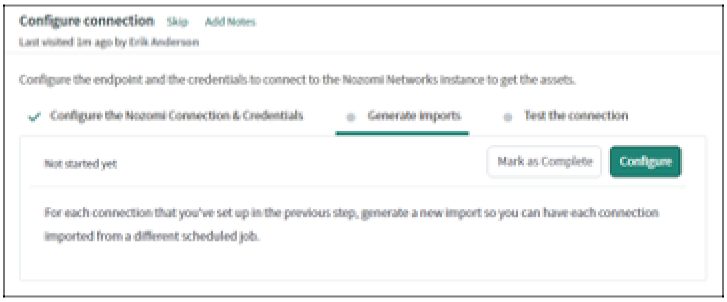
MID Server: Select a mid server if your Nozomi envir...

Credential Information

* User name:

* Password:

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**.



Configure connection

Last visited 1m ago by Erik Anderson

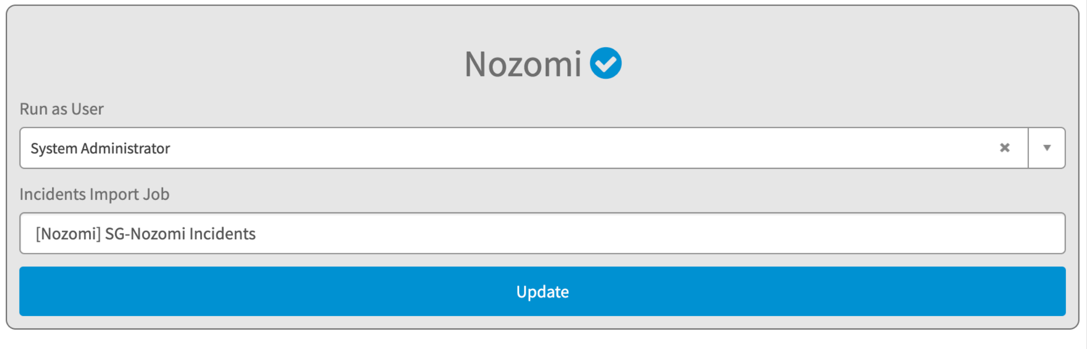
Configure the endpoint and the credentials to connect to the Nozomi Networks instance to get the assets.

Not started yet

For each connection that you've set up in the previous step, generate a new import so you can have each connection imported from a different scheduled job.

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**.



Nozomi

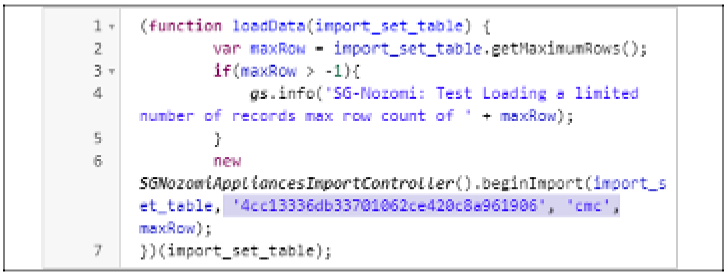
Run as User: System Administrator

Incidents Import Job: [Nozomi] SG-Nozomi Incidents

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**.

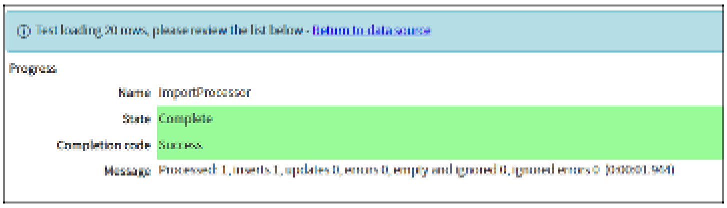
    For each connection there should be two different data sources. One for **Appliances** and one for **Assets**.
19. Open each data source and review the data loader script.



```
(function loadData(import_set_table) {
        var maxRow = import_set_table.getMaximumRows();
        if(maxRow > -1){
            gs.info('SG-Nozomi: Test Loading a limited number of records max row count of ' + maxRow);
        }
        new SGNozomiAppliancesImportController().beginImport(import_set_table, '4cc13336db33701062ce420c8a961906', 'cmc', maxRow);
})(import_set_table);
```

The connection alias `sys_id` and connection name should be listed as parameters.

20. To test the connection, in the related links, select **test load 20**.
21. You should see a successful connection like shown below. If you get a connection error, review your connection and credentials from previous steps.



ⓘ Test loading 20 rows, please review the list below - Return to data source

Progress

Name: ImportProcessor

State: Complete

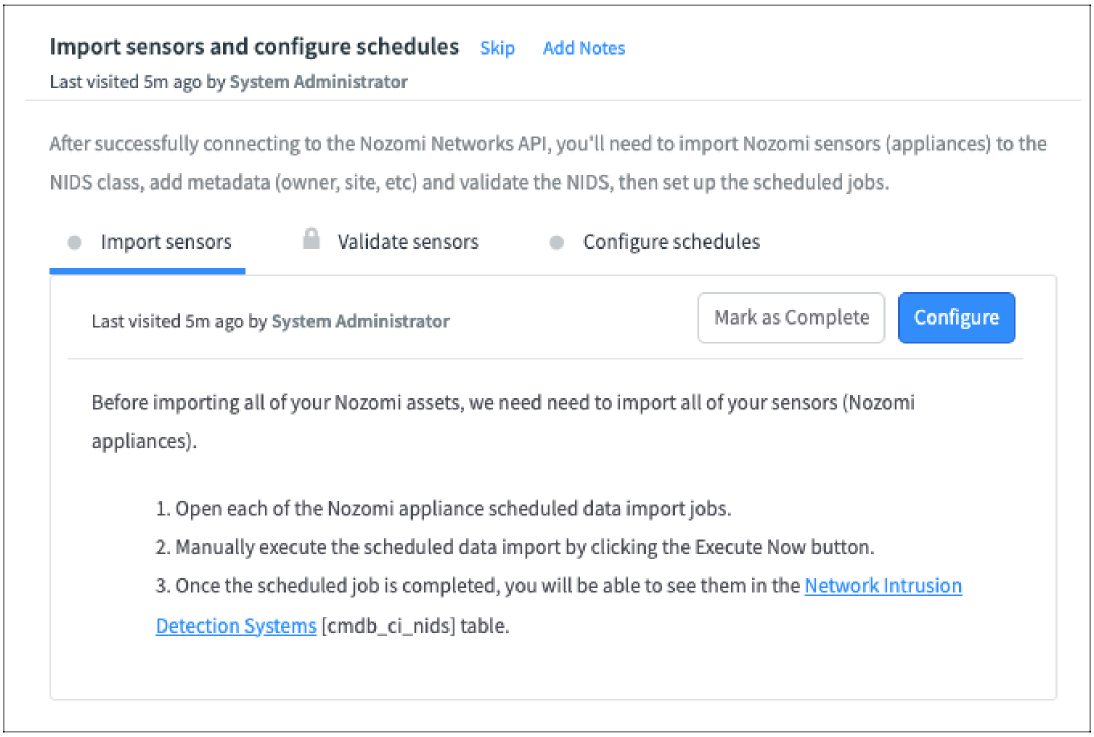
Completion code: Success

Message: Processed: 1, inserts 1, updates 0, errors 0, empty and ignored 0, ignored errors 0 (00:00:01.984)

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

23. Select **Import sensors and configure schedules**.

24. 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.

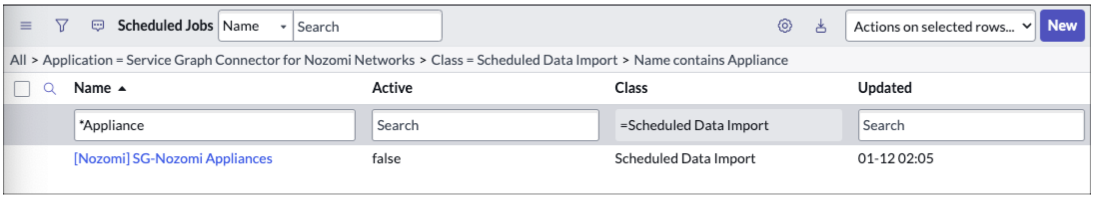
Last visited 5m ago by System Administrator

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.

25. Select **Configure**.

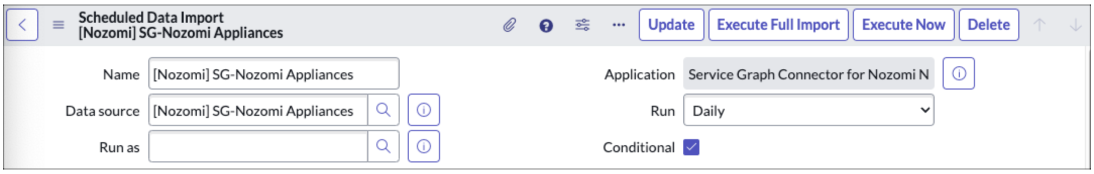
26. For each connection there should be one scheduled data import related to Appliances, select it.



All > Application = Service Graph Connector for Nozomi Networks > Class = Scheduled Data Import > Name contains Appliance

Name ▲	Active	Class	Updated
*Appliance	Search	=Scheduled Data Import	Search
[Nozomi] SG-Nozomi Appliances	false	Scheduled Data Import	01-12 02:05

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



Scheduled Data Import
[Nozomi] SG-Nozomi Appliances

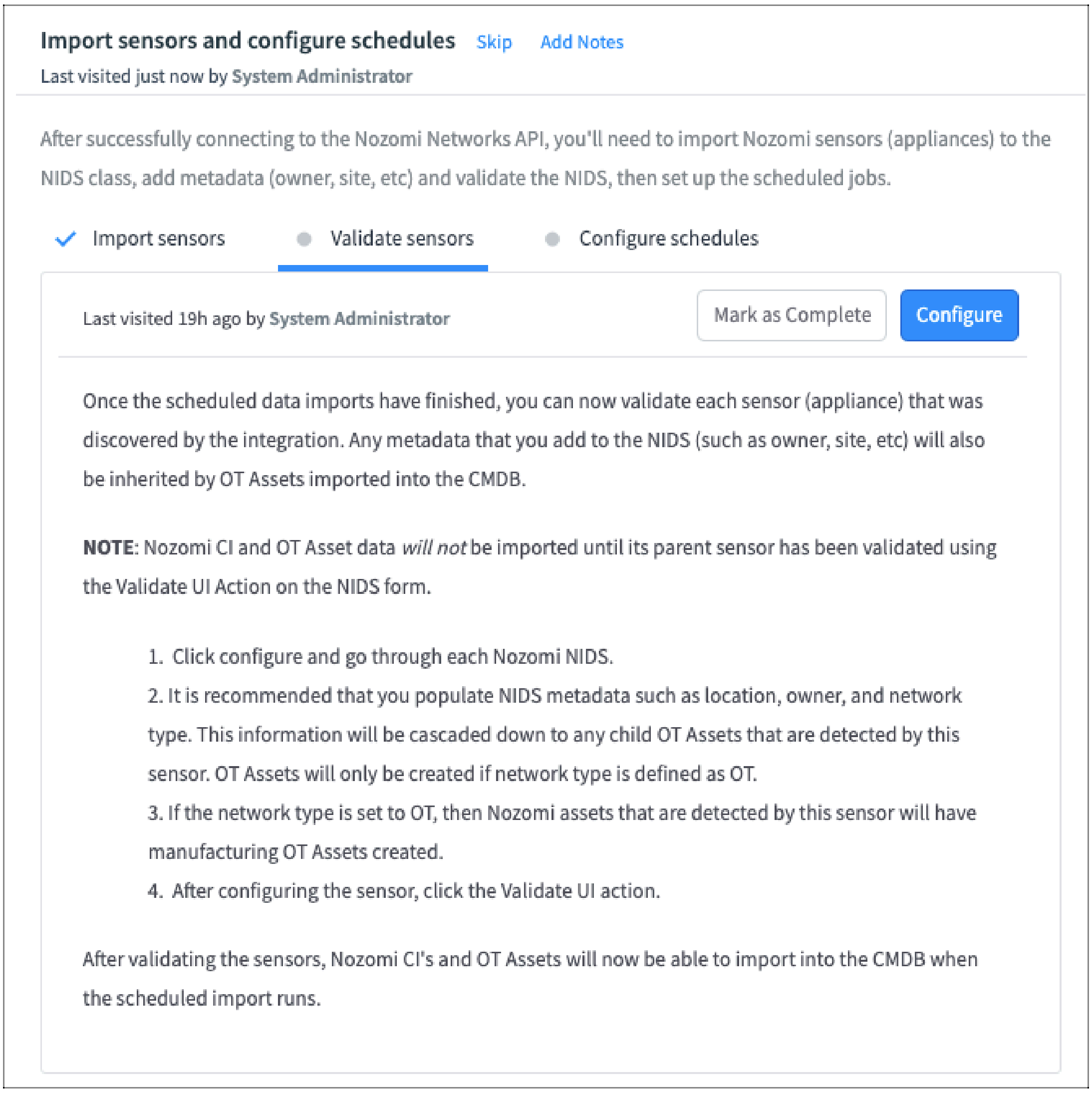
Name	[Nozomi] SG-Nozomi Appliances	Application	Service Graph Connector for Nozomi N
Data source	[Nozomi] SG-Nozomi Appliances	Run	Daily
Run as		Conditional	☑

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.

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

29. 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.

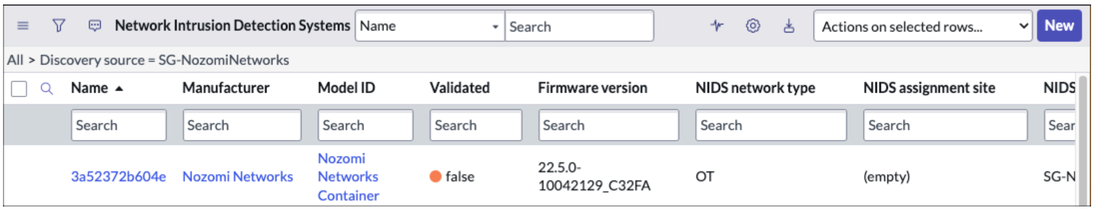
NOTE: Nozomi CI and OT Asset data *will not* be imported until its parent sensor has been validated using the Validate UI Action on the NIDS form.

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.

30. Select **Configure**.

31. It will open the *Network Intrusion Detection Systems (NIDS)* showing all the appliances the integration has discovered.



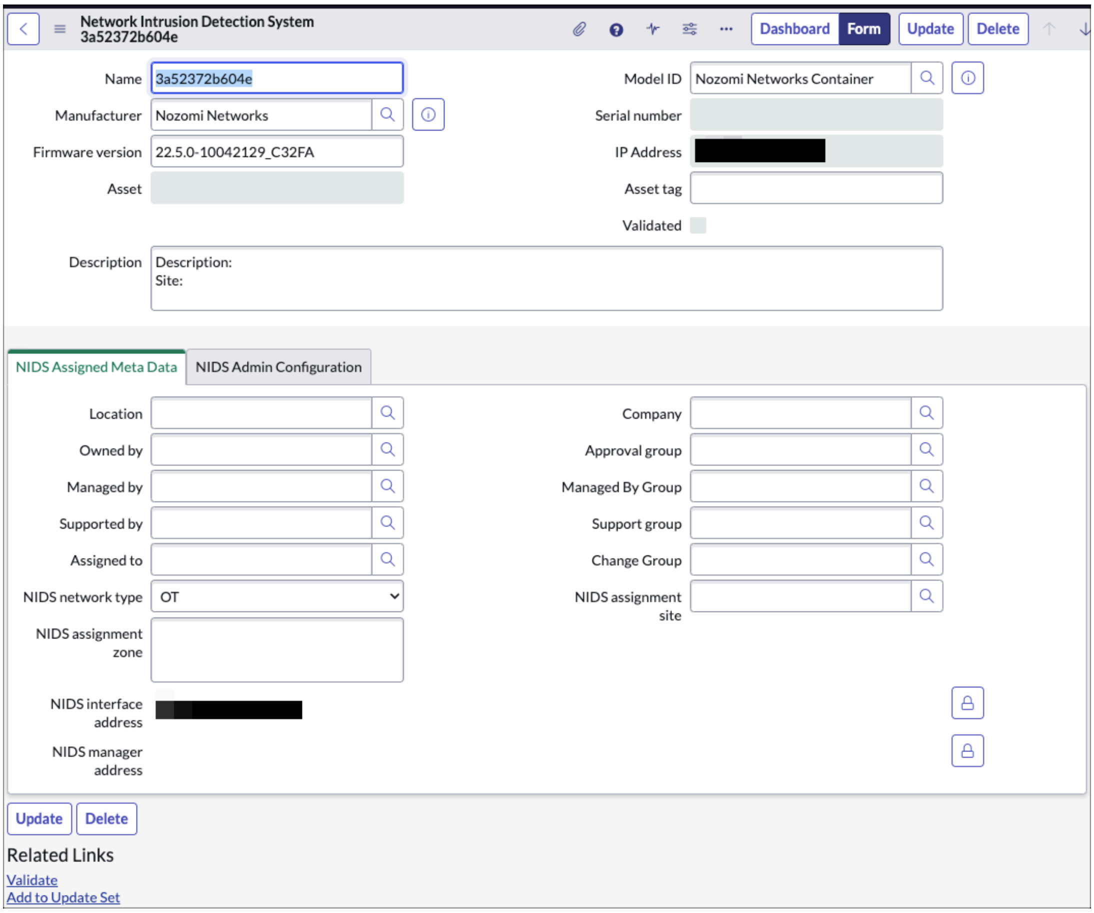
Network Intrusion Detection Systems
Name
Search
Actions on selected rows...
New

All > Discovery source = SG-NozomiNetworks

Name ▲	Manufacturer	Model ID	Validated	Firmware version	NIDS network type	NIDS assignment site	NIDS
Search	Search	Search	Search	Search	Search	Search	Sear
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.

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



Network Intrusion Detection System
3a52372b604e

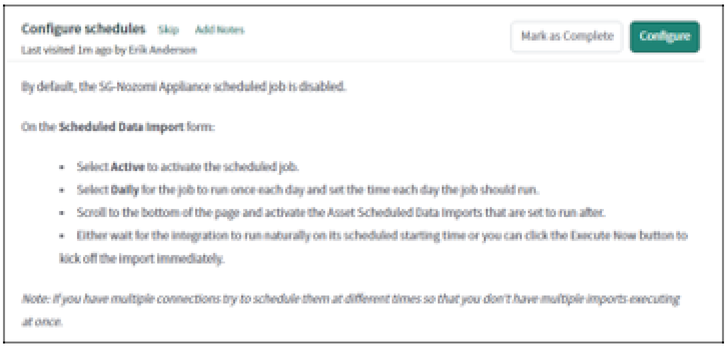
Name	3a52372b604e	Model ID	Nozomi Networks Container
Manufacturer	Nozomi Networks	Serial number	
Firmware version	22.5.0-10042129_C32FA	IP Address	[redacted]
Asset		Asset tag	
		Validated	□
Description	Description: Site:		

Location		Company	
Owned by		Approval group	
Managed by		Managed By Group	
Supported by		Support group	
Assigned to		Change Group	
NIDS network type	OT	NIDS assignment site	
NIDS assignment zone			
NIDS interface address	[redacted]		
NIDS manager address			

Related Links
Validate
Add to Update Set

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

34. Select **Configure schedules** and select **Configure**.



Configure schedules
Last visited 1m ago by Erik Anderson

By default, the SG-Nozomi Appliance scheduled job is disabled.

On the **Scheduled Data Import** form:

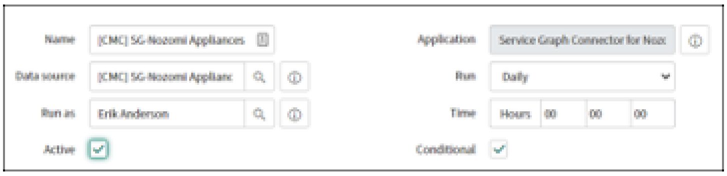
- Select **Active** to activate the scheduled job.
- Select **Daily** for the job to run once each day and set the time each day the job should run.
- Scroll to the bottom of the page and activate the Asset Scheduled Data imports that are set to run after.
- Either wait for the integration to run naturally 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.

35. Open each appliance import scheduled job.

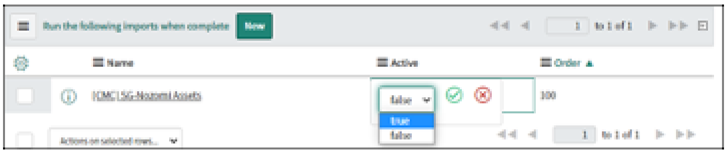
36. The run as user should be set based on what you selected during the **Generate imports** step.

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



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

38. 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.



Run the following imports when complete
New
1 to 1 of 1
Actions on selected rows...
true
false

Name	Active	Order ▲
[CMC] SG-Nozomi Assets	false	100

39. 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**.

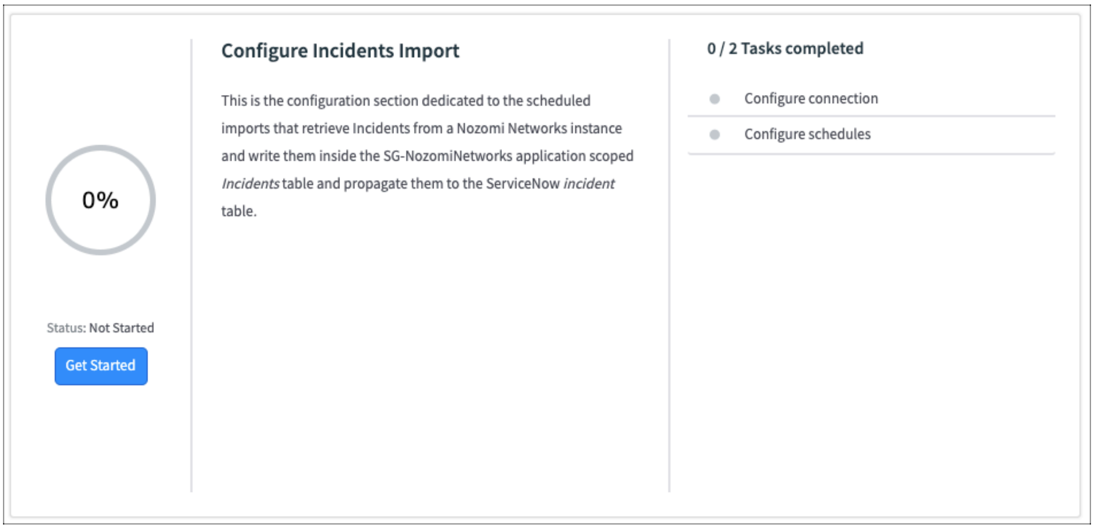
> **Note:**
> You can also select **Execute Full Import**, which will force a full import of Nozomi Networks data, regardless of the last import execution time.

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 Import**, select **Get Started**.



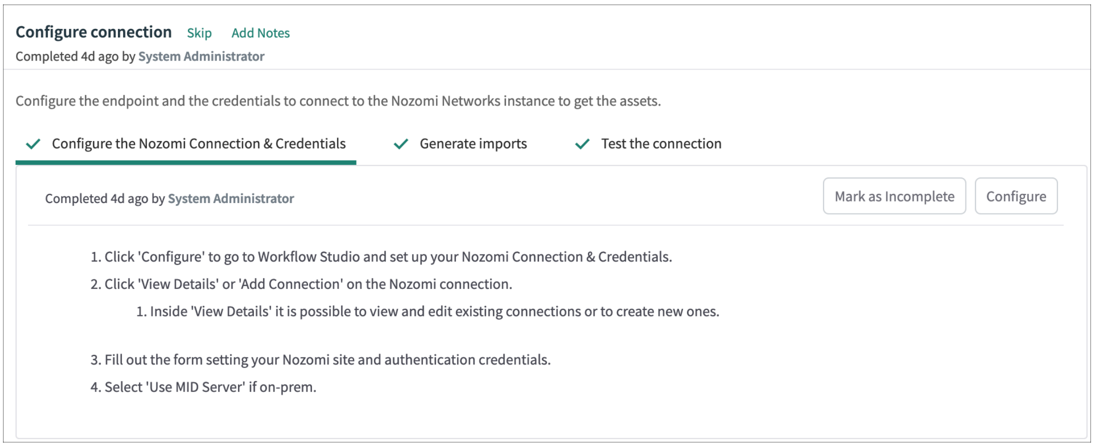
Configure Incidents Import

This is the configuration section dedicated to the scheduled imports that retrieve Incidents from a Nozomi Networks instance and write them inside the SG-NozomiNetworks application scoped *Incidents* table and propagate them to the ServiceNow *incident* table.

0 / 2 Tasks completed

- Configure connection
- Configure schedules

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



Completed 4d ago by System Administrator

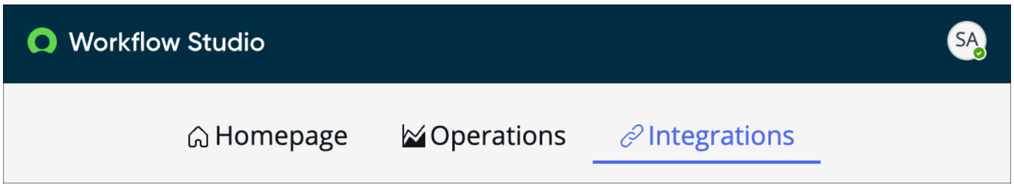
Configure the endpoint and the credentials to connect to the Nozomi Networks instance to get the assets.

Completed 4d ago by System Administrator

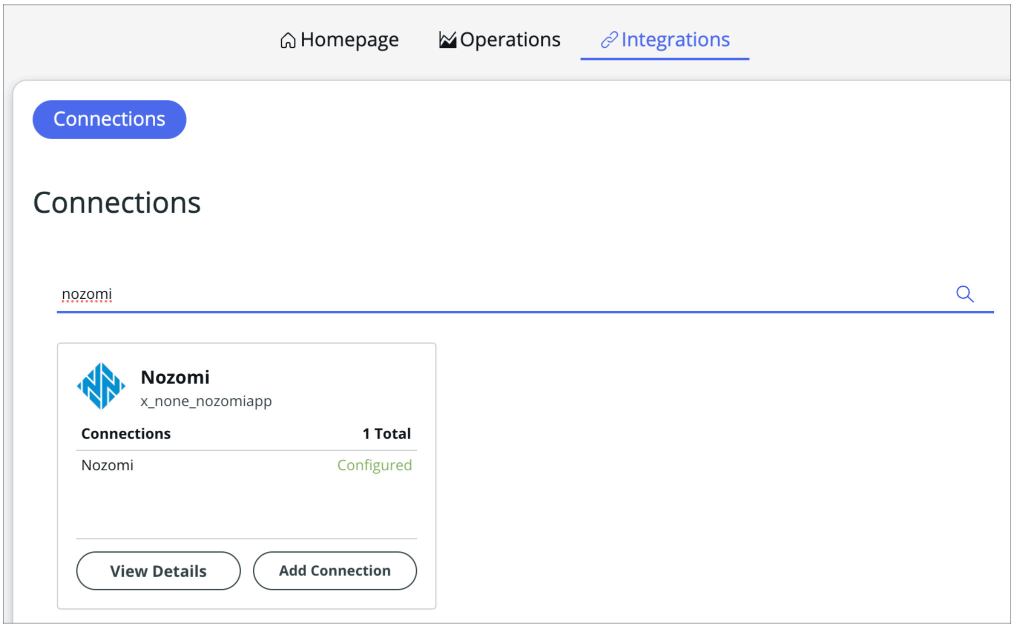
1. Click 'Configure' to go to Workflow Studio and set up your Nozomi Connection & Credentials.
2. Click 'View Details' or 'Add Connection' on the Nozomi connection.
   1. Inside 'View Details' it is possible to view and edit existing connections or to create new ones.
3. Fill out the form setting your Nozomi site and authentication credentials.
4. Select 'Use MID Server' if on-prem.

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**.

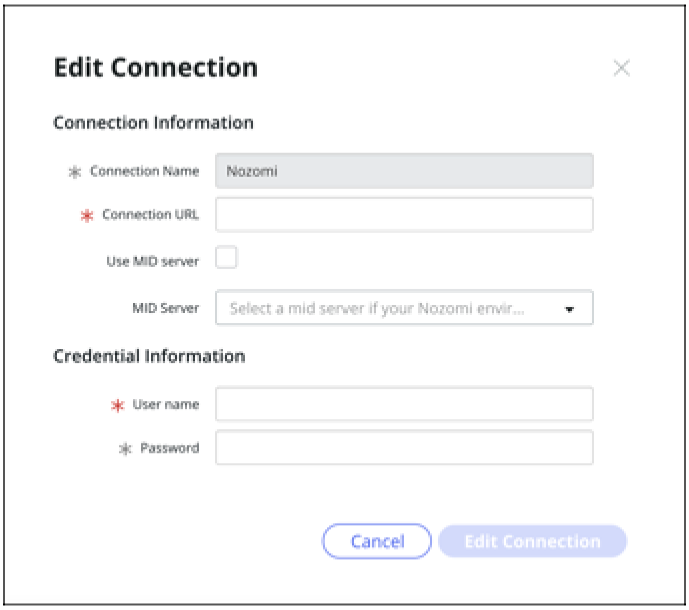


   b. In the search field, search for **Nozomi**.



5. Select **Add Connection**.

6. Enter your site information.



Edit Connection

Connection Information

* Connection Name: Nozomi

* Connection URL:

Use MID server: □

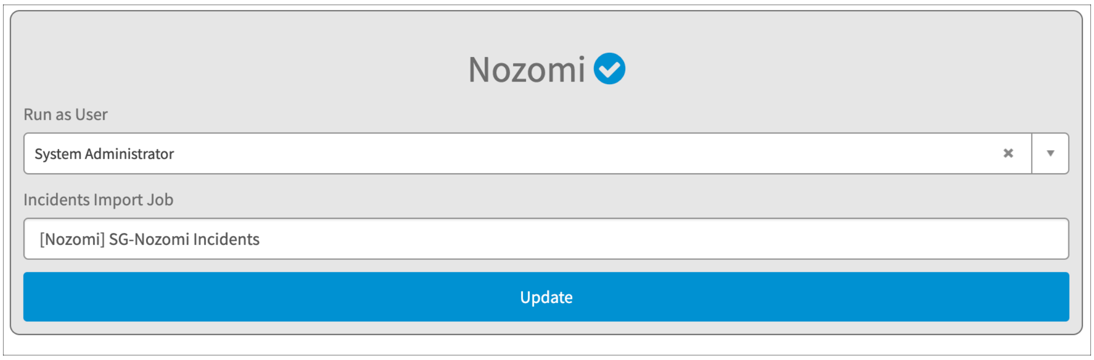
MID Server: Select a mid server if your Nozomi envir...

Credential Information

* User name:

* Password:

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.



Nozomi ✓

Run as User: System Administrator

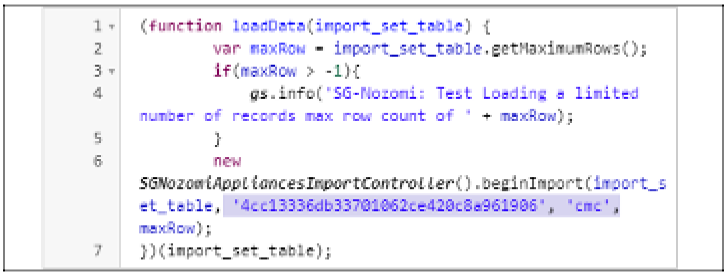
Incidents Import Job: [Nozomi] SG-Nozomi Incidents

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 an Incidents data source.

15. Open each data source and review the data loader script.

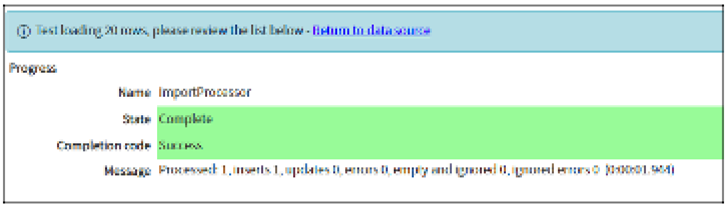


```
(function loadData(import_set_table) {
        var maxRow = import_set_table.getMaximumRows();
        if(maxRow > -1){
            gs.info('SG-Nozomi: Test Loading a limited number of records max row count of ' + maxRow);
        }
        new SGNozomiAppliancesImportController().beginImport(import_set_table, '4cc13336db33701062ce420c8a961906', 'cmc', maxRow);
})(import_set_table);
```

The connection alias `sys_id` and connection name should be listed as parameters.

16. To test the connection, in the related links, select **test load 20**.

17. You should see a successful connection like shown below. If you get a connection error, review your connection and credentials from previous steps.



ⓘ Test loading 20 rows, please review the list below - Return to data source

Progress

Name ImportProcessor

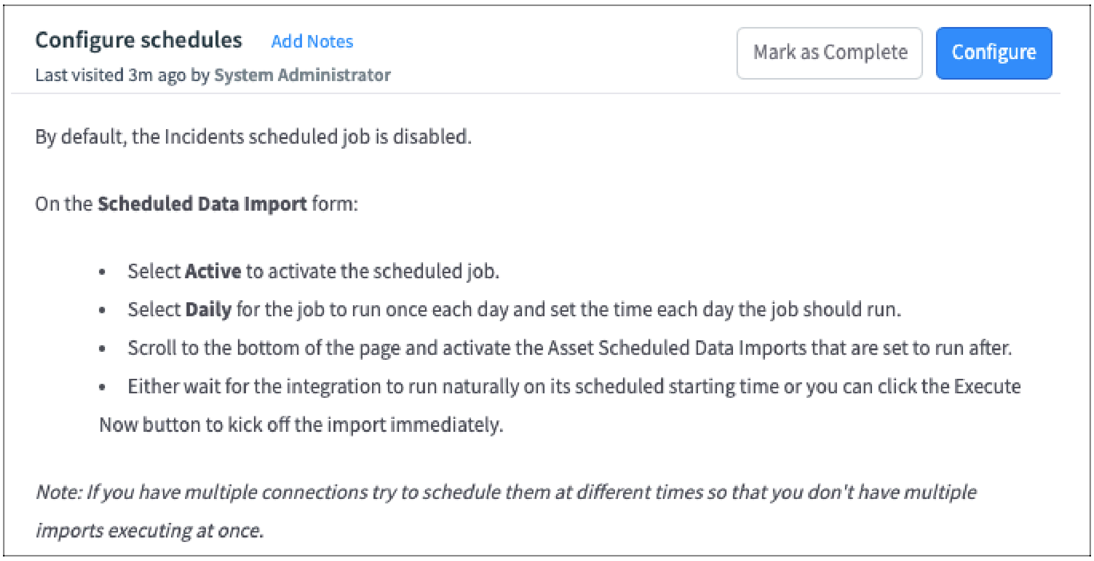
State Complete

Completion code Success

Message Processed: 1, inserts 1, updates 0, errors 0, empty and ignored 0, ignored errors 0 [0:00:01.984]

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

19. Select **Configure schedules**.



By default, the Incidents scheduled job is disabled.

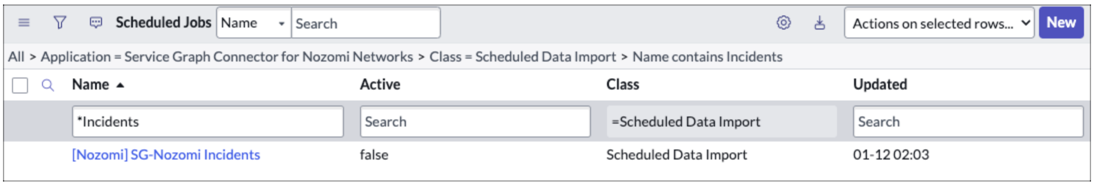
On the **Scheduled Data Import** form:

- 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.

20. Select **Configure**.

21. Open each incident import scheduled job.



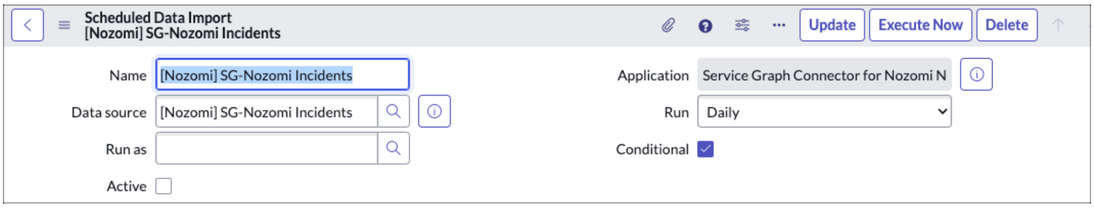
Scheduled Jobs | Name | Search | Actions on selected rows... | New

All > Application = Service Graph Connector for Nozomi Networks > Class = Scheduled Data Import > Name contains Incidents

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

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

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



Scheduled Data Import
[Nozomi] SG-Nozomi Incidents

Update | Execute Now | Delete

Name	[Nozomi] SG-Nozomi Incidents	Application	Service Graph Connector for Nozomi N
Data source	[Nozomi] SG-Nozomi Incidents	Run	Daily
Run as		Conditional	☑
Active	□		

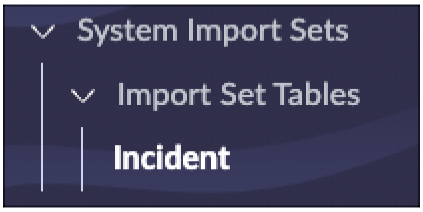
24. Once you have completed configuring all the jobs, you can either wait for the scheduled job to run, or you can select **Execute Now** to manually execute the job on the **Incidents Scheduled Data Import Job**.

Validate data flow

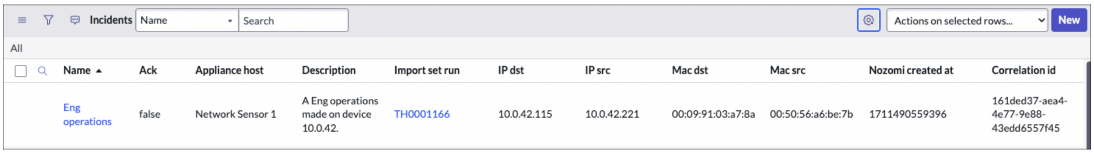
You now need to validate that the data is flowing from the configured Nozomi Networks instance to the ServiceNow instance. To do this, you need to look at the applicable tables in ServiceNow.

Procedure

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



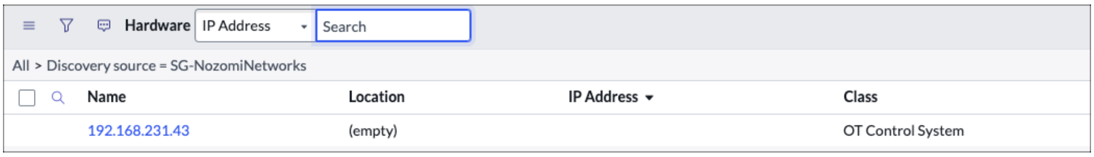
2. View the **Nozomi created at** column.



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.

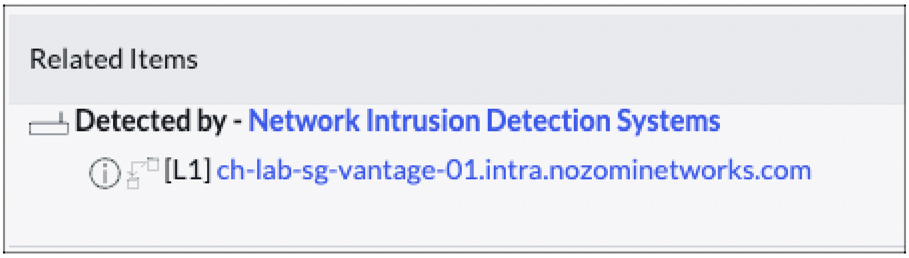


All > Discovery source = SG-NozomiNetworks

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*.


Related Items

Detected by - Network Intrusion Detection Systems

[L1] ch-lab-sg-vantage-01.intra.nozominetworks.com

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:

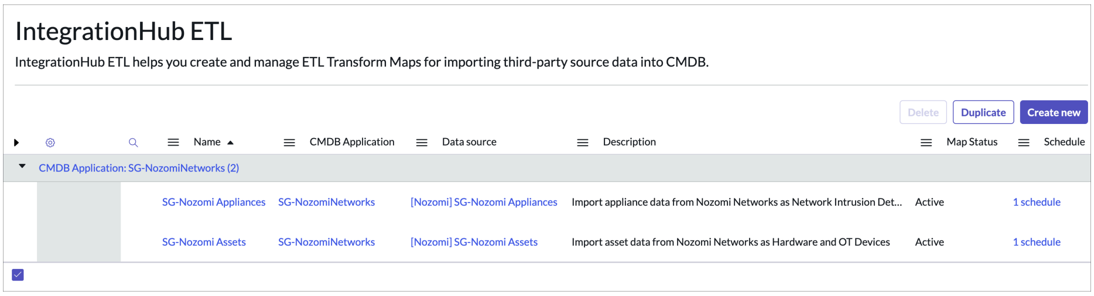
- Map the fields of the Nozomi Networks source tables with your custom tables
- Conditionally Import data into your custom tables
- Transform imported data, if required

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.



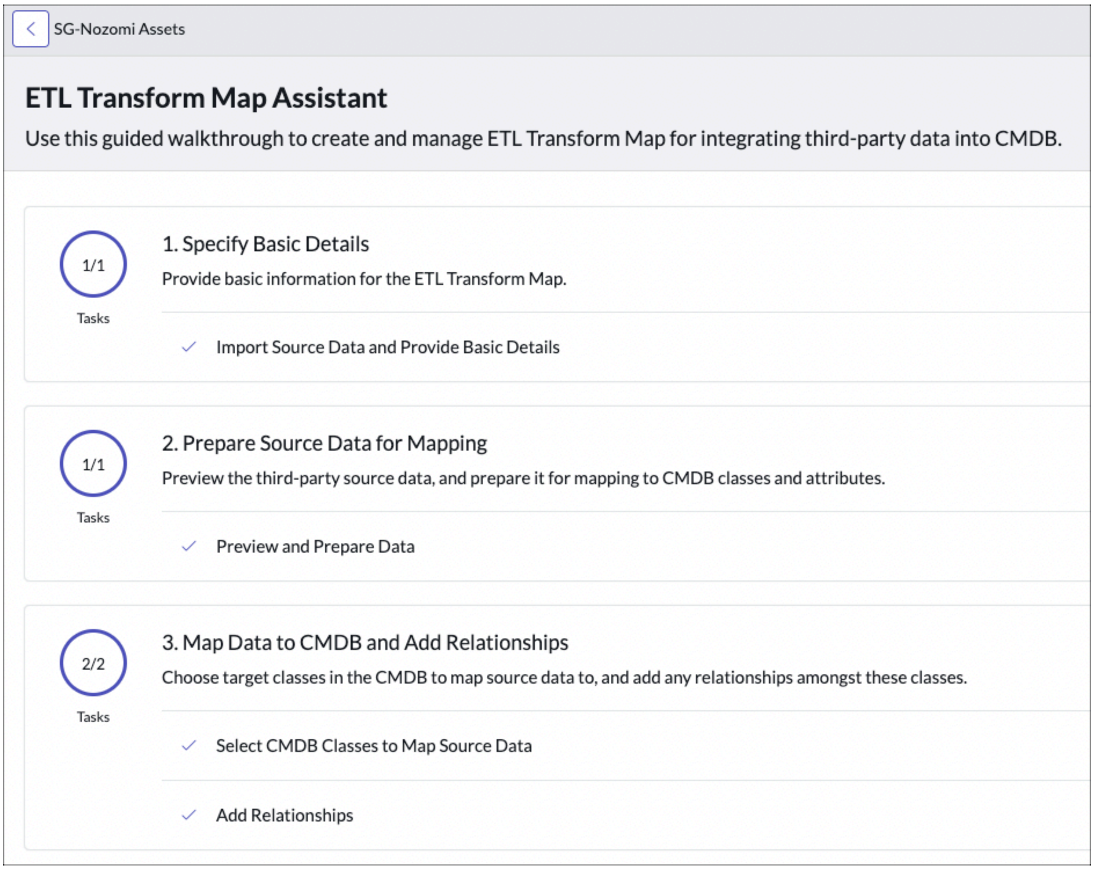
IntegrationHub ETL

IntegrationHub ETL helps you create and manage ETL Transform Maps for importing third-party source data into CMDB.

CMDB Application: SG-NozomiNetworks (2)

Name	CMDB Application	Data source	Description	Map Status	Schedule
SG-Nozomi Appliances	SG-NozomiNetworks	[Nozomi] SG-Nozomi Appliances	Import appliance data from Nozomi Networks as Network Intrusion Det...	Active	1 schedule
SG-Nozomi Assets	SG-NozomiNetworks	[Nozomi] SG-Nozomi Assets	Import asset data from Nozomi Networks as Hardware and OT Devices	Active	1 schedule

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



SG-Nozomi Assets

ETL Transform Map Assistant

Use this guided walkthrough to create and manage ETL Transform Map for integrating third-party data into CMDB.

1/1 Tasks

1. Specify Basic Details

Provide basic information for the ETL Transform Map.

✓ Import Source Data and Provide Basic Details

1/1 Tasks

2. Prepare Source Data for Mapping

Preview the third-party source data, and prepare it for mapping to CMDB classes and attributes.

✓ Preview and Prepare Data

2/2 Tasks

3. Map Data to CMDB and Add Relationships

Choose target classes in the CMDB to map source data to, and add any relationships amongst these classes.

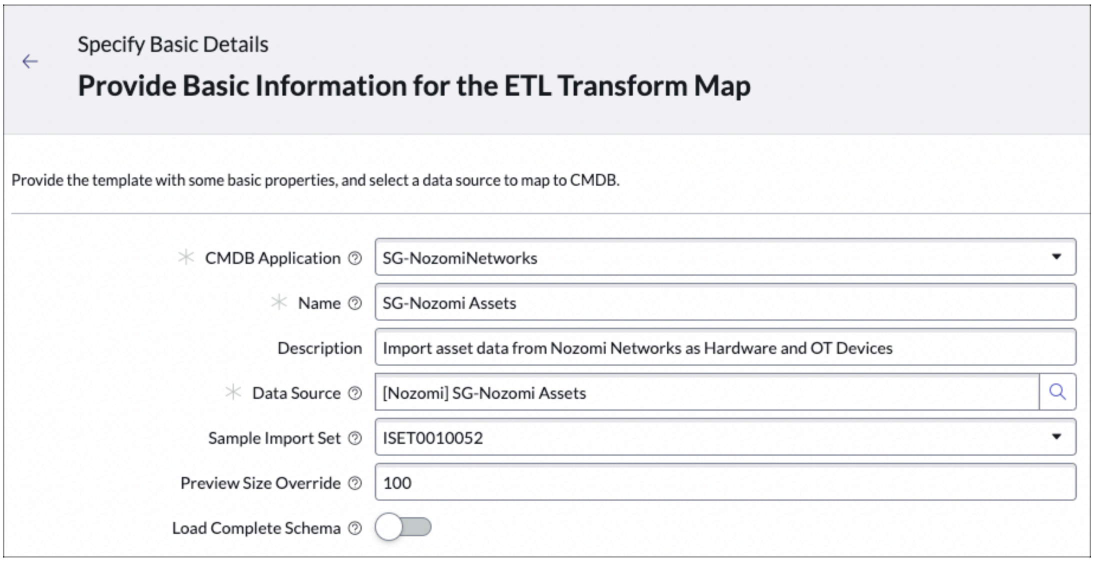
✓ Select CMDB Classes to Map Source Data

✓ Add Relationships

3. 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.

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



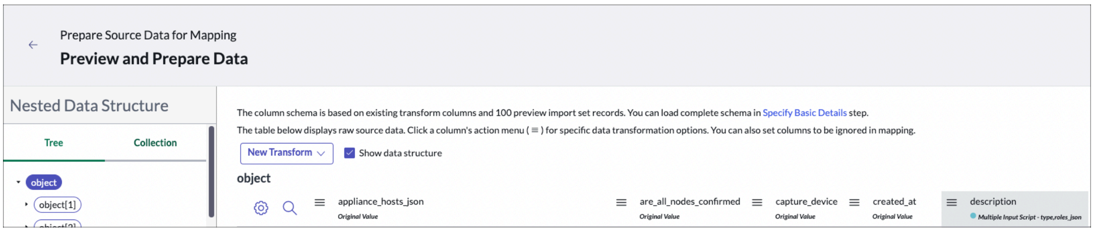
Specify Basic Details

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	SG-NozomiNetworks
* Name	SG-Nozomi Assets
Description	Import asset data from Nozomi Networks as Hardware and OT Devices
* Data Source	[Nozomi] SG-Nozomi Assets
Sample Import Set	ISET0010052
Preview Size Override	100
Load Complete Schema	○

5. Select **Preview and Prepare Data**.



Prepare Source Data for Mapping

Preview and Prepare Data

Nested Data Structure

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.

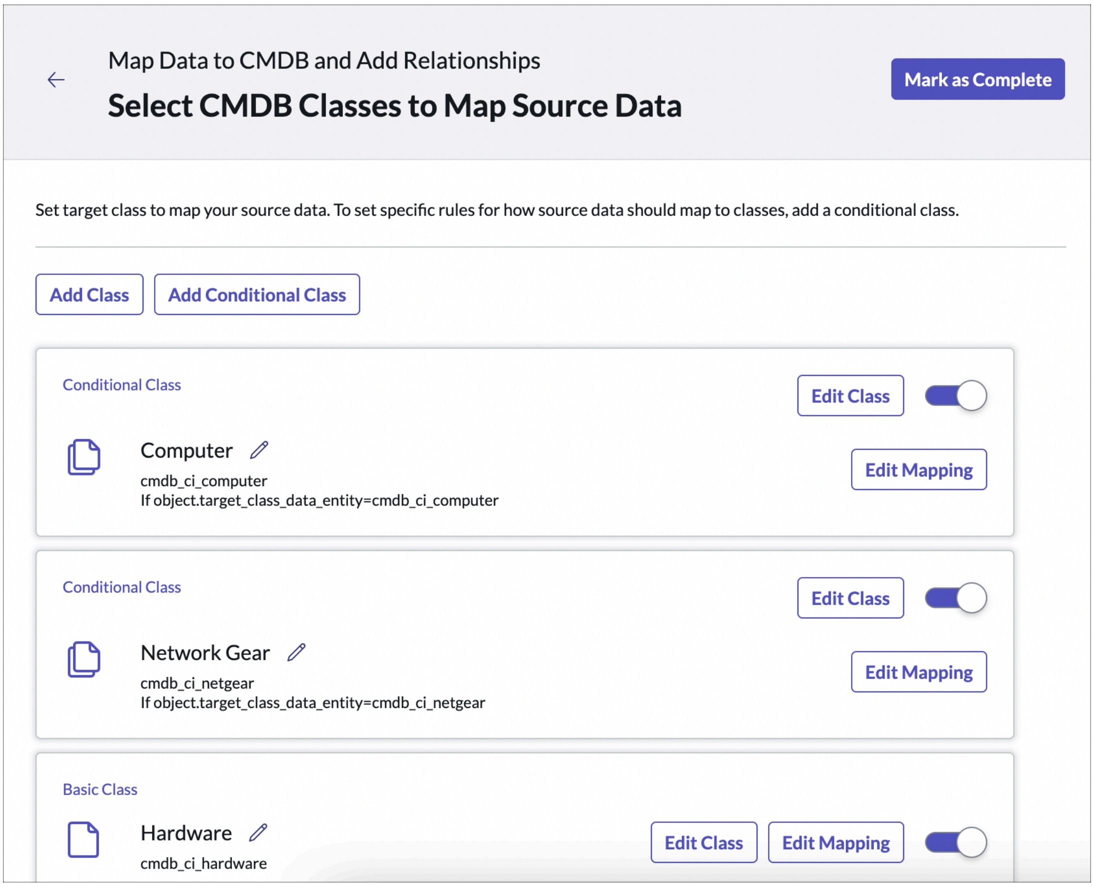
The table below displays raw source data. Click a column's action menu (≡) for specific data transformation options. You can also set columns to be ignored in mapping.

☑ Show data structure

object

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**.



Map Data to CMDB and Add Relationships

Select CMDB Classes to Map Source Data

Set target class to map your source data. To set specific rules for how source data should map to classes, add a conditional class.

Conditional Class

Computer

cmdb_ci_computer

If object.target_class_data_entity=cmdb_ci_computer

Conditional Class

Network Gear

cmdb_ci_netgear

If object.target_class_data_entity=cmdb_ci_netgear

Basic Class

Hardware

cmdb_ci_hardware

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

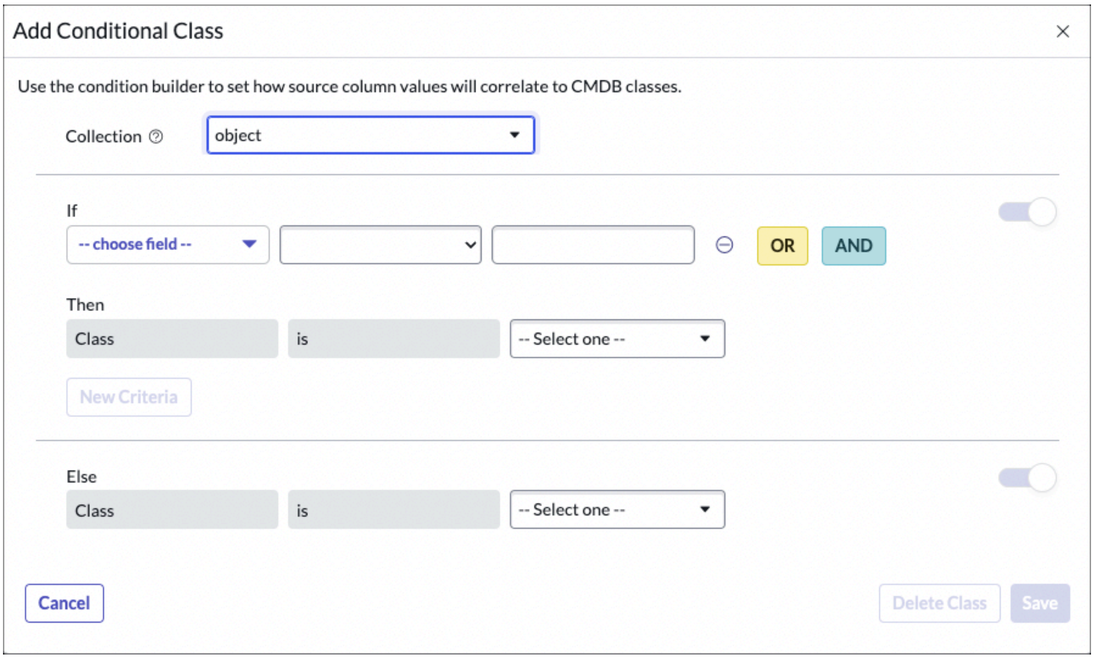
An example of Nozomi Networks discovered Voice over Internet Protocol (VoIP) phones. These devices will be categorized in the ***SG-Nozomi Assets*** *import set table as* `voip_phone` *under the* `type` *field. We will then map these devices into the ServiceNow Internet of Things (IoT) Device Configuration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

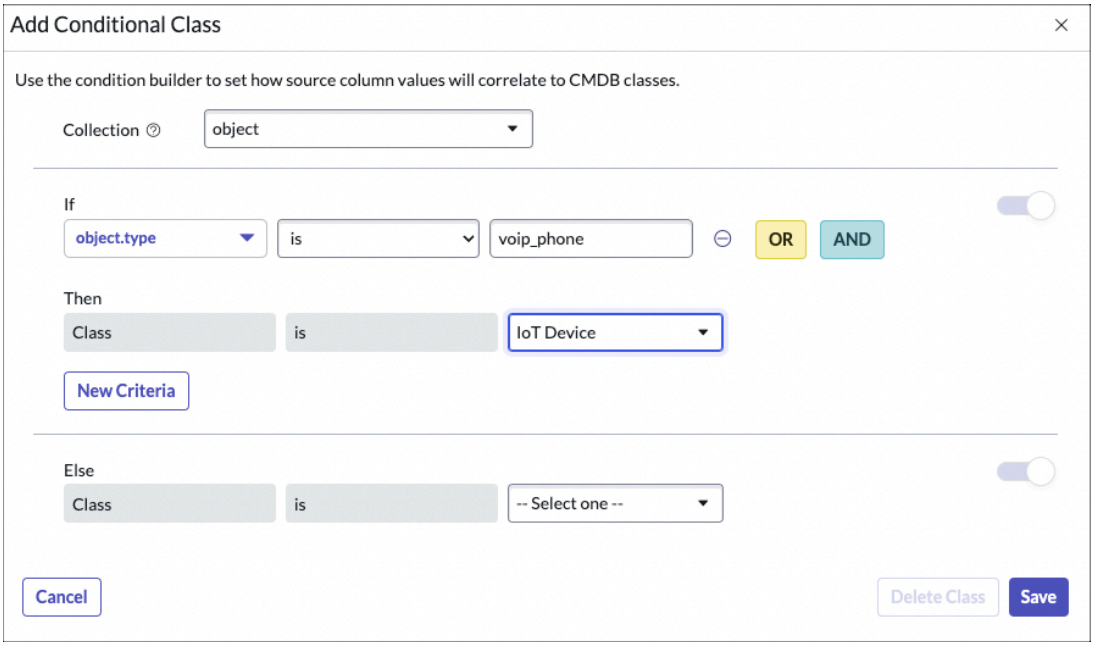


Add Conditional Class

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

Collection: object

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.

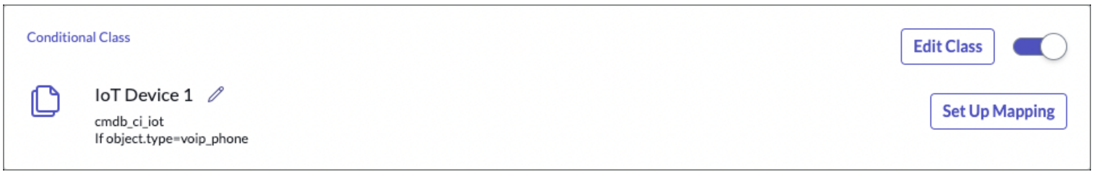
Collection: object

If: object.type | is | voip_phone

Then: Class | is | IoT Device

Else: Class | is | -- Select one --

4. When you have finished, select **Save**.
   The new Conditional Class table shows as **IoT Device 1**.



Conditional Class

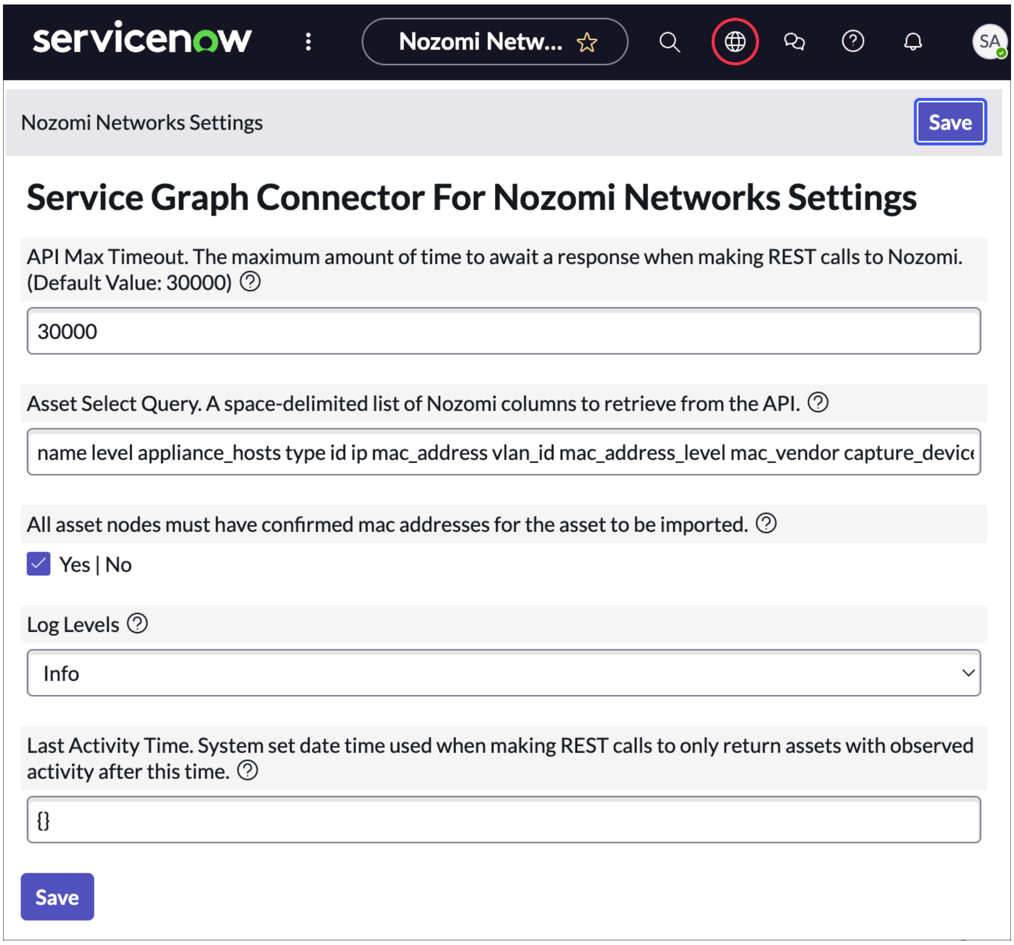
IoT Device 1
cmdb_ci_iot
If object.type=voip_phone

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.



Service Graph Connector For Nozomi Networks Settings

API Max Timeout. The maximum amount of time to await a response when making REST calls to Nozomi. (Default Value: 30000)

30000

Asset Select Query. A space-delimited list of Nozomi columns to retrieve from the API.

name level appliance_hosts type id ip mac_address vlan_id mac_address_level mac_vendor capture_devic

All asset nodes must have confirmed mac addresses for the asset to be imported.

☑ Yes | No

Log Levels

Info

Last Activity Time. System set date time used when making REST calls to only return assets with observed activity after this time.

{}

Save

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

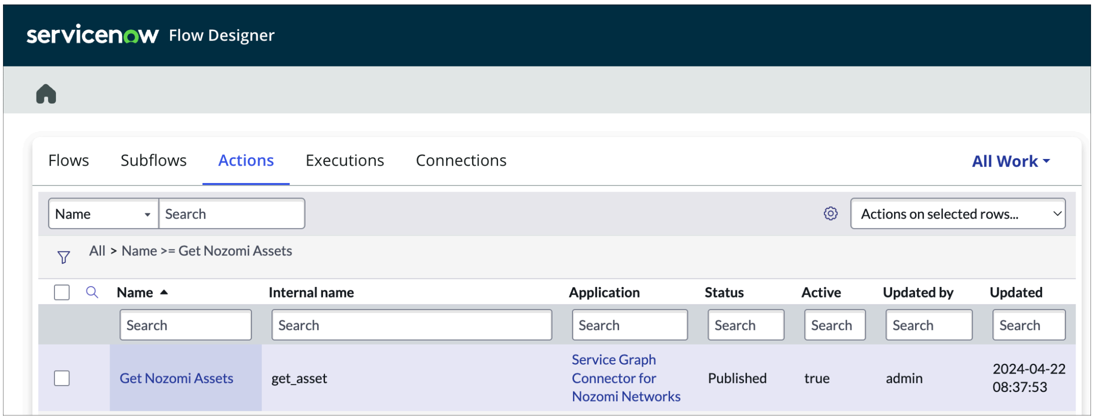
Once a new column, such as **column_foo** has been added, you need to augment the data stream action that imports data into the staging table.

Procedure

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

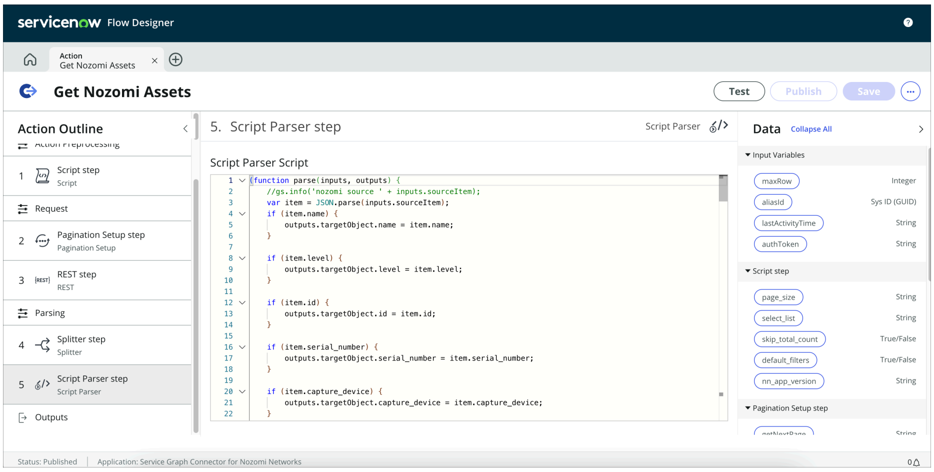
   Result: A new page opens.

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**.



All > Name >= Get Nozomi Assets

□	Name ▲	Internal name	Application	Status	Active	Updated by	Updated
	Search	Search	Search	Search	Search	Search	Search
□	Get Nozomi Assets	get_asset	Service Graph Connector for Nozomi Networks	Published	true	admin	2024-04-22 08:37:53



Script Parser Script

```
(function parse(inputs, outputs) {
    //gs.info('nozomi source ' + inputs.sourceItem);
    var item = JSON.parse(inputs.sourceItem);
    if (item.name) {
        outputs.targetObject.name = item.name;
    }

    if (item.level) {
        outputs.targetObject.level = item.level;
    }

    if (item.id) {
        outputs.targetObject.id = item.id;
    }

    if (item.serial_number) {
        outputs.targetObject.serial_number = item.serial_number;
    }

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

Input Variables

maxRow	Integer
aliasId	Sys ID (GUID)
lastActivityTime	String
authToken	String

Script step

page_size	String
select_list	String
skip_total_count	True/False
default_filters	True/False
nn_app_version	String

Pagination Setup step

getNextPage	String

Figure 2. Script Parser step

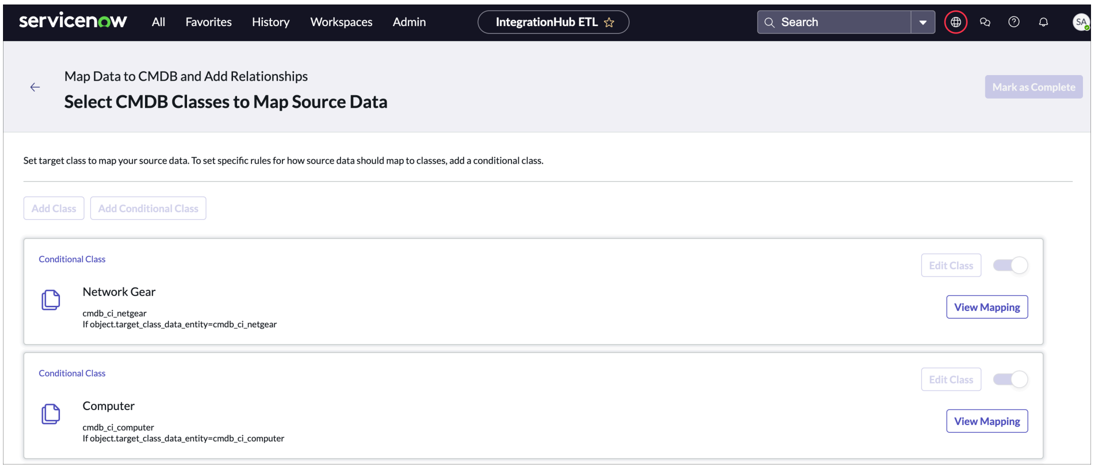
This is where the script that parses the response live.

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**.



Map Data to CMDB and Add Relationships

Select CMDB Classes to Map Source Data

Set target class to map your source data. To set specific rules for how source data should map to classes, add a conditional class.

Conditional Class

Network Gear

cmdb_ci_netgear

If object.target_class_data_entity=cmdb_ci_netgear

Conditional Class

Computer

cmdb_ci_computer

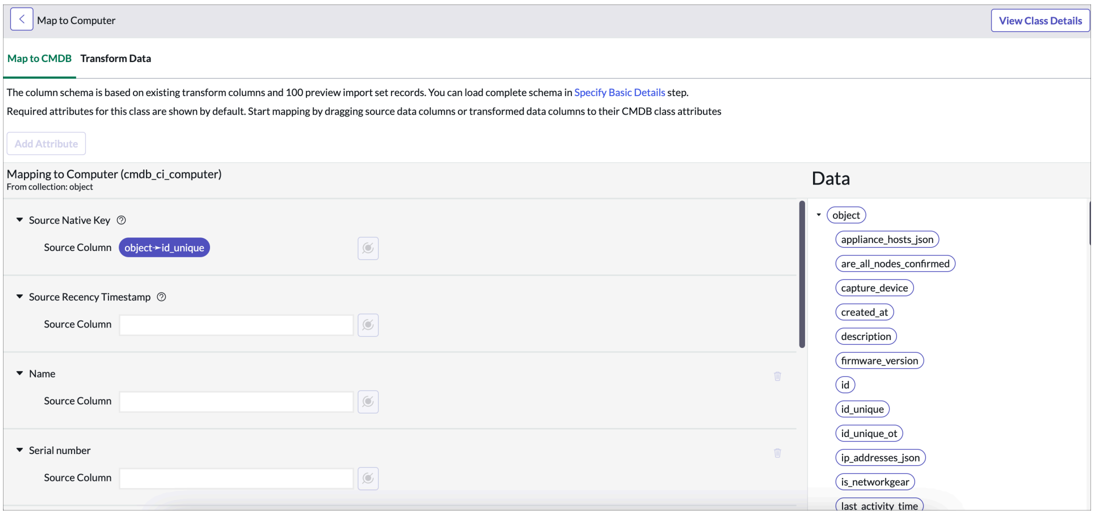
If object.target_class_data_entity=cmdb_ci_computer

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.



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

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:

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.

Chapter 4. Additional configuration

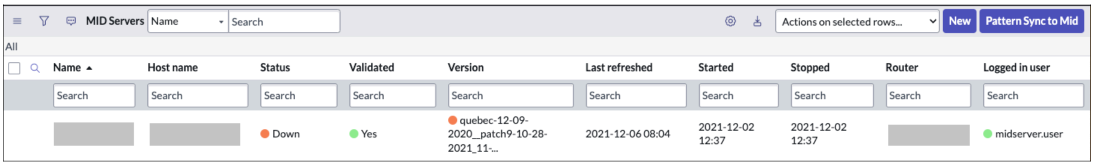
Configure an MID server

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.

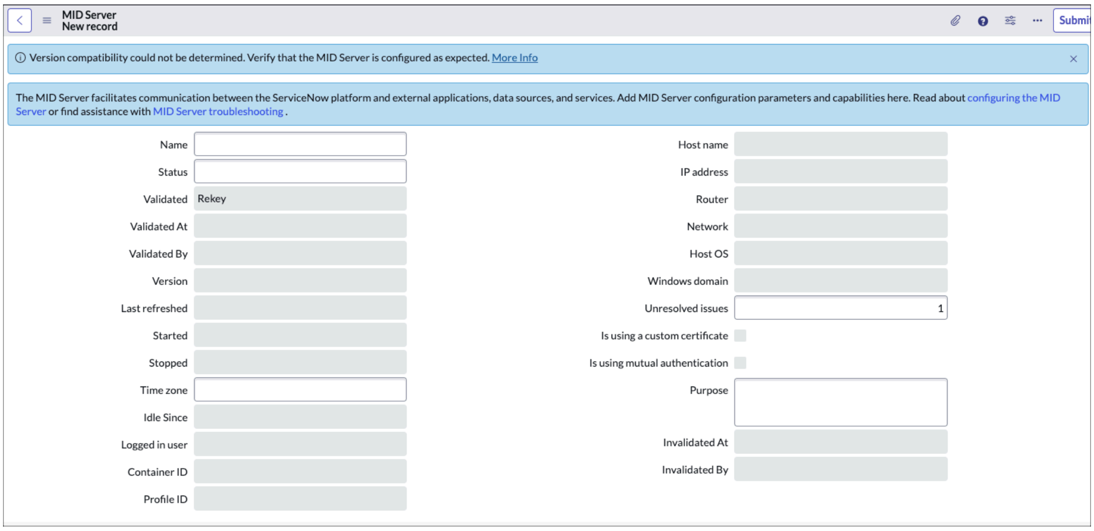
2. Search for **MID Server > Servers**.



Name ▲	Host name	Status	Validated	Version	Last refreshed	Started	Stopped	Router	Logged in user
Search	Search	Search	Search	Search	Search	Search	Search	Search	Search
[redacted]	[redacted]	● 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	[redacted]	● midserver.user

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		Host name	
Status		IP address	
Validated	Rekey	Router	
Validated At		Network	
Validated By		Host OS	
Version		Windows domain	
Last refreshed		Unresolved issues	1
Started		Is using a custom certificate	□
Stopped		Is using mutual authentication	□
Time zone		Purpose	
Idle Since			
Logged in user		Invalidated At	
Container ID		Invalidated By	
Profile ID			

4. Enter the necessary information in the fields as necessary.

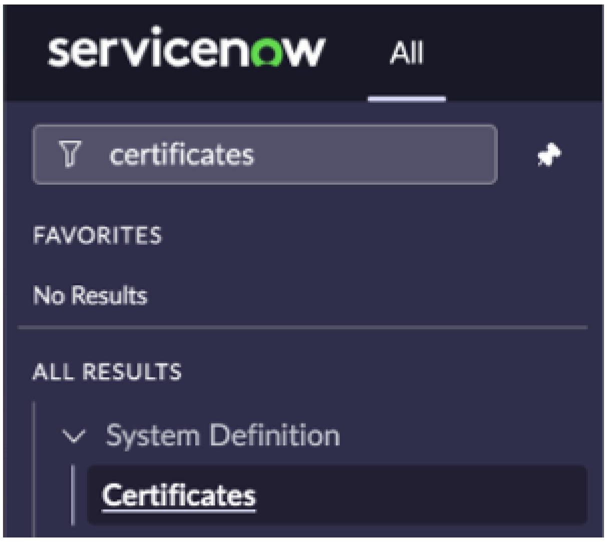
5. Select **Submit**.

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.

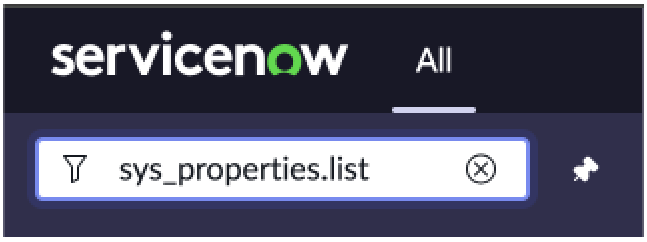
4. Enter the details as necessary.
5. Select **Submit**.

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.

   sys_properties.list

   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 52) 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**

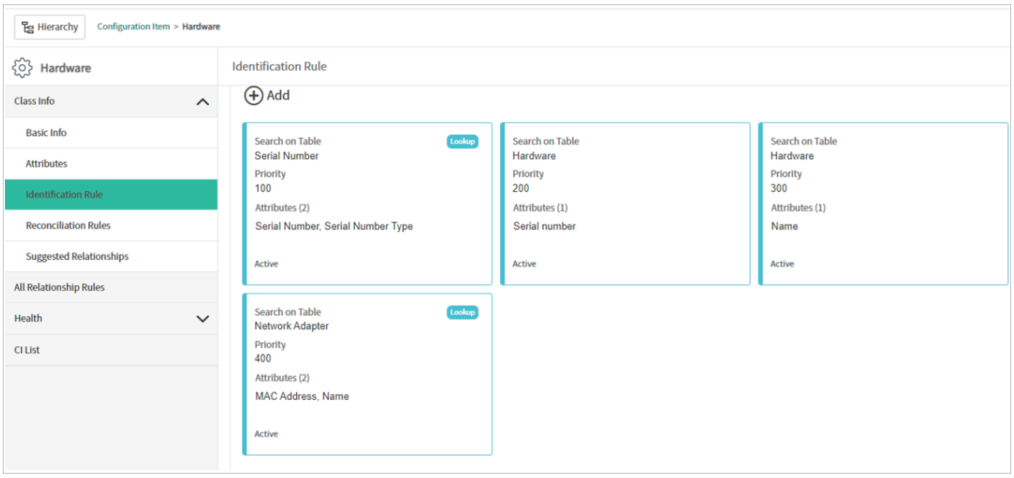
A built-in example will show that has a process function where the flattened item built by the integration prior and the *API* item returned from the data stream action are passed through.
You can select the **create implementation** related link to generate a new script include. You can now adjust the 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.



Search on Table
Serial Number
Priority
100
Attributes (2)
Serial Number, Serial Number Type
Active

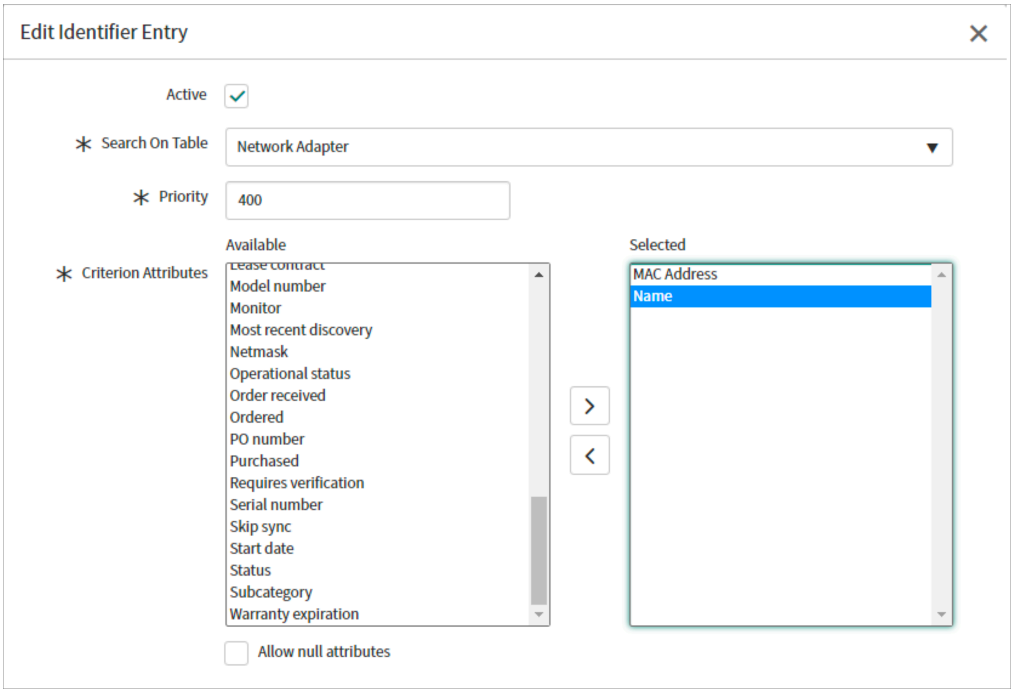
Search on Table
Hardware
Priority
200
Attributes (1)
Serial number
Active

Search on Table
Hardware
Priority
300
Attributes (1)
Name
Active

Search on Table
Network Adapter
Priority
400
Attributes (2)
MAC Address, Name
Active

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.



Edit Identifier Entry

☑ Active

* Search On Table: Network Adapter

* Priority: 400

* Criterion Attributes

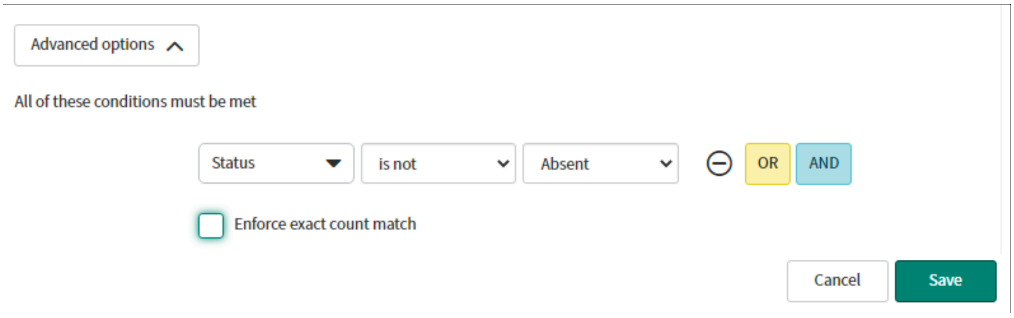
Available:
Lease contract
Model number
Monitor
Most recent discovery
Netmask
Operational status
Order received
Ordered
PO number
Purchased
Requires verification
Serial number
Skip sync
Start date
Status
Subcategory
Warranty expiration

Selected:
MAC Address
Name

□ Allow null attributes

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.



Advanced options

All of these conditions must be met

Status | is not | Absent

□ Enforce exact count match

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 it 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.

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.

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.