NOZOMI NETWORKS

ServiceNow Vulnerability Response
Integration Guide

SVR v1.2.1 — 2024-09-13

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 guide gives an overview of the ServiceNow Vulnerability Response integration with Nozomi Networks. It outlines the steps needed to prepare and configure your application, focusing on entering key credentials and selecting the appropriate server for seamless operation.

> **Note:**
> This guide updates and replaces the **Scoped Application Installation and Configuration Guide** - **Nozomi Integration for Vulnerability Response.**

This guide will help you prepare your instance to make sure that your application operates correctly. It also describes a clear process to let you configure your certified application after installation.

The **ServiceNow Vulnerability Response** integration is mostly pre-configured. This means that you only need to:

- Enter your **Nozomi URL**
- Enter your **username**
- Enter your **password**
- Select a *Management, Instrumentation, and Discovery (MID)* server

Chapter 2. Requirements

Requirements

This section outlines the requirements for integrating ServiceNow Vulnerability Response with Nozomi Networks. It will help you make sure that the necessary plug-ins are enabled, verify compatibility with supported ServiceNow versions (Utah, Vancouver, Washington DC), and confirm that your Nozomi Networks platform meets the specified version criteria.

Plug-ins

- Vulnerability Response
- Vulnerability Response Integration with NVD

ServiceNow

- Utah
- Vancouver
- Washington DC

Nozomi Networks platforms

- *Central Management Console (CMC)* version 24.2.0, or later
- Vantage

Chapter 3. Configuration

Configure the application

Learn how to configure the Nozomi Networks integration within ServiceNow, including setup, connection parameters, and testing configurations, to ensure seamless vulnerability management. Follow these detailed steps to establish and verify connections with your Nozomi Networks platform.

Before you begin

Make sure that the **Vulnerability Response Integration with NVD** application has been run at least once.

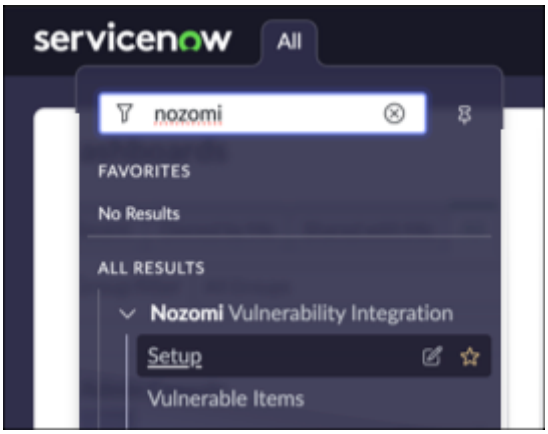
About this task

To make sure that you get the most accurate information, Nozomi Networks recommends that you populate the *Common Vulnerabilities and Exposures (CVE)* library before you import Nozomi Networks data.

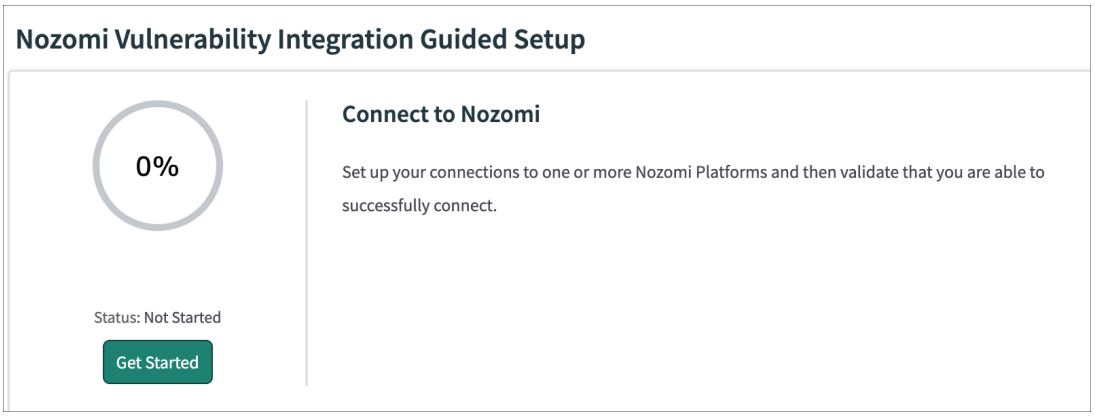
For more details about the **Vulnerability Response Integration with NVD**, see the ServiceNow documentation.

Procedure

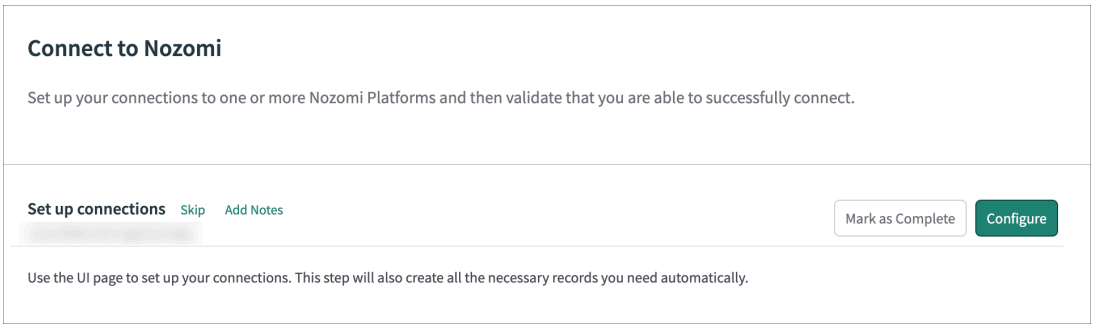
1. Go to ServiceNow.
2. Go to **Nozomi Vulnerability Integration > Setup**



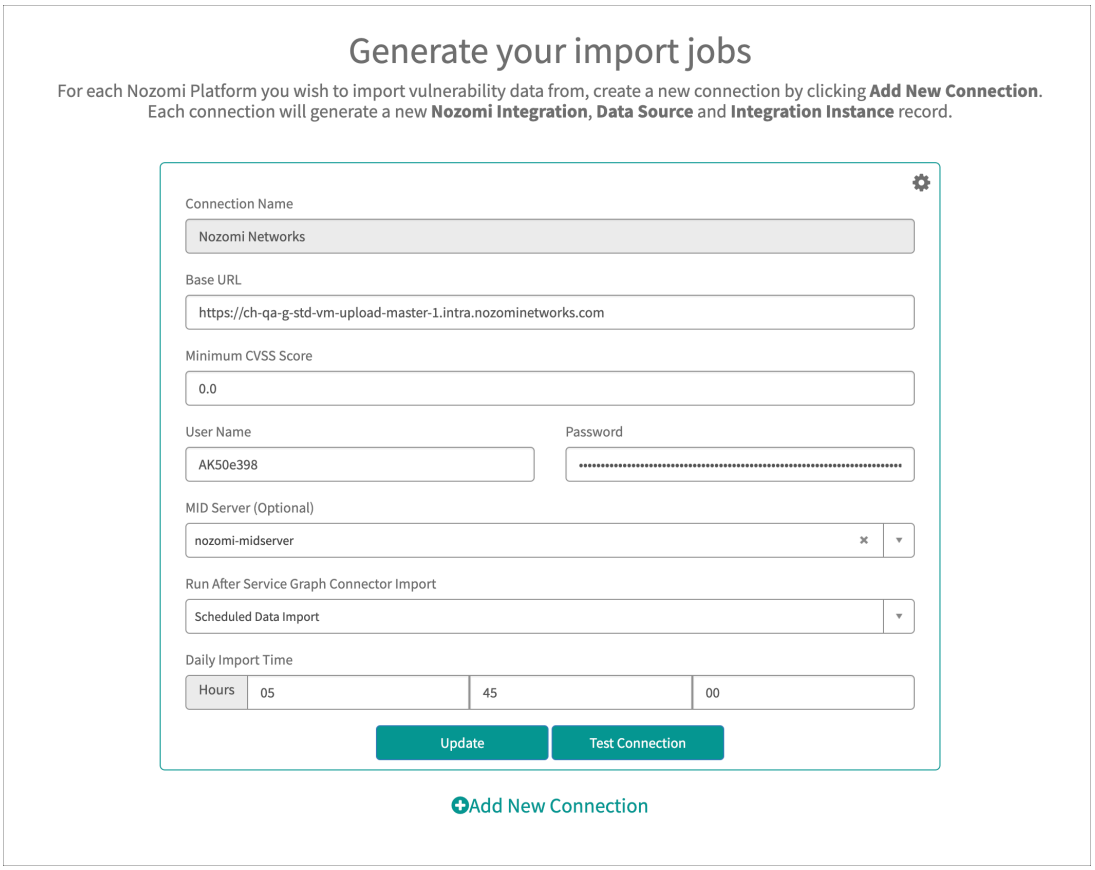
3. In the **Connect to Nozomi** section, select **Get Started**.



4. To the right of **Set up connections**, select **Configure**.



5. Enter the applicable details.



The **Connection Manager** lets you connect one or more Nozomi Networks platform instances. By default, a single connection exists that is named **Nozomi**. You can add additional connections to other Nozomi Networks platform instances as required. Each connection has the following parameters:

- **Connection Name**
- **Base URL** (of the Nozomi instance)
- **Minimum CVSS Score**

> **Note:**
> This specifies the minimum threshold, inclusive of vulnerabilities, that will be imported. For example, if set to 8.0, only vulnerabilities with a *Common Vulnerability Scoring System (CVSS)* of 8.0 or higher will be imported

- **User Name**
- **Password**
- **MID server (Optional)**
- **Run After Service Graph Connector Import**
- **Daily Import Time**

6. To verify the parameters that you have entered, select **Test Connection**.

Result: If the test connection is successful, you will see the **Test Connection** button temporarily show **Results: 200**

7. **Optional:** Add additional connections.
   a. Select **Add New Connection**.

   b. Do steps 1 (on page 15) thru 6 (on page 18) again.

Configure the integration parameters

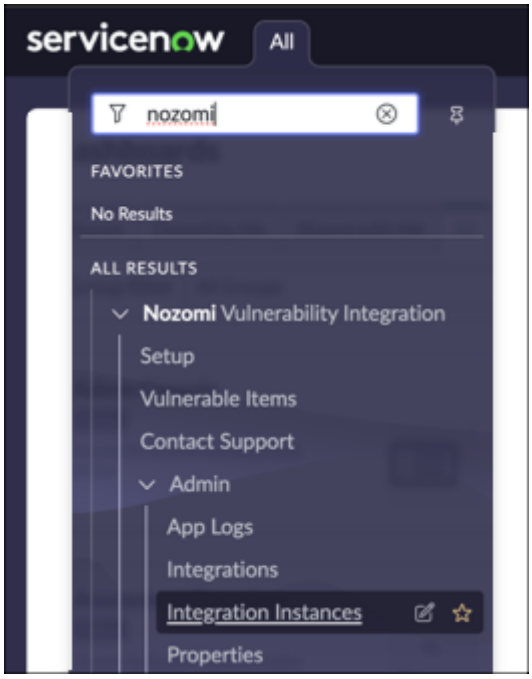
Learn how to configure integration parameters for Nozomi Vulnerability Integration in ServiceNow. Read how to adjust the number of records retrieved for each Application Programming Interface (API) call, which will ensure efficient data handling during the Node Common Vulnerabilities and Exposures (CVE) integration process.

About this task

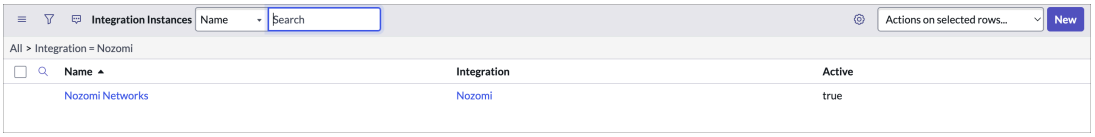
For each Nozomi Integration record that is created, there is an additional parameter not shown in the **Setup Assistant**. The `node_cve_api_page_size` parameter lets you to specify how many records are pulled in for each *application programming interface (API)* call for the Node *CVE*s integration.

Procedure

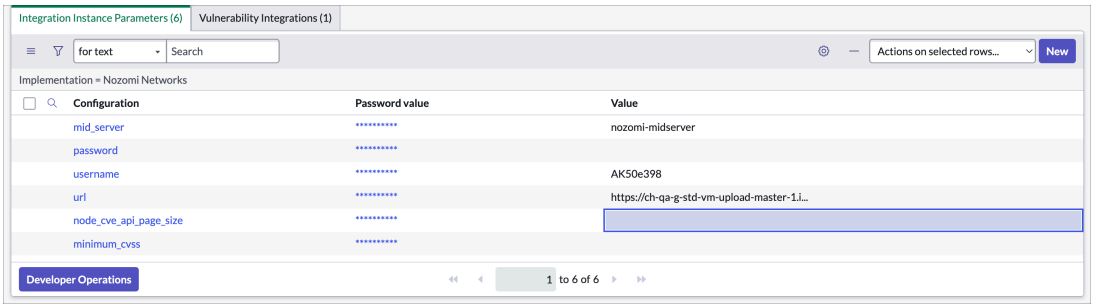
1. Go to **Nozomi Vulnerability Integration > Integration Instances**.



2. Select **Nozomi Networks**.



3. In **Integration Instance Parameters**, change the `node_cve_api_page_size` value as required.



The default behavior is to retrieve 500 records at a time. If the value of the parameter is blank, the default number of records will be 500, or the value of the `detection_integration_page_size` of the system properties. For more details, see System properties (on page 22). If you increase the value of this parameter, more data will be imported with each *API* call, which will result in fewer *API* calls to Nozomi for each integration run. If you decrease the value of the parameter, there will be more *API* calls to *Nozomi*, as the data will be imported in smaller chunks. The default value of 500 should be sufficient for most use cases and environments.

System properties

Explore essential system properties for optimizing Nozomi Vulnerability Integration in ServiceNow. Read how to view, adjust, and manage settings related to data import duration, batch size, and timing buffers to ensure accurate and efficient vulnerability detection integration.

The values of these properties have been set for optimal performance without additional configuration. However, if necessary, users with the **x_none_nozomi_vr.admin** role can modify them. To view these properties, got to **Nozomi Vulnerability Integration > Admin > Properties**.

detection_integration_delta_days_default

By default, a Nozomi Asset CVEs Integration (which pulls in vulnerability detections) will initially import data reaching back `(VALUE)` days. The default value is `90`.

If you wish to import more than 90 days of data on the initial integration run, for example if you wanted to import the past 6 months of data, you would change this value to `180`.

You can also got to the related Nozomi Integration Record **Nozomi Vulnerability Integration > Integrations** and manually change the `Start time` field to the desired date/time.

detection_integration_page_size

When importing vulnerability detections, the data will be pulled from the *API (VALUE)* records *at a time*. The default value is 500.

If you increase the value of this property, more data will be imported with each *API* call, which will result in fewer *API* calls to *Nozomi* for each integration run. If you decrease the value of the property, there will be more *API* calls to Nozomi, as the data will be imported in smaller chunks.

node_cve_integration_start_time_buffer

When doing a delta import for Node CVE Integration, the `Start time` sent to the *API* will be *{VALUE}* hours before the `Start time` on the integration record, to make sure that we get any new records from the *API* that may have been created during the previous integration run.

The default value is 4.

The integration uses a *buffer* to make sure that no records are missed from Nozomi, if vulnerability detection records are created in *Nozomi* while the ServiceNow integration is running.

Example:

Nozomi Vulnerability Integration is set to run every day at 2:00 AM.

The integration starts at 2:00 AM.

The integration ends at 3:00 AM.

The `Start time` for the next integration run is 3:00 AM.

It is possible that some vulnerability detections were created in Nozomi between 2:00 AM and 3:00 AM.

The value of the `node_cve_integration_start_time_buffer` is 4 (hours).

The next time the integration runs (2:00 AM), the *API* call will pull in data from the `Start time` (3:00 AM), minus the buffer hours (4 hours by default). So the integration will pull data from Nozomi that has been created/updated since 11:00 PM the previous day.

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

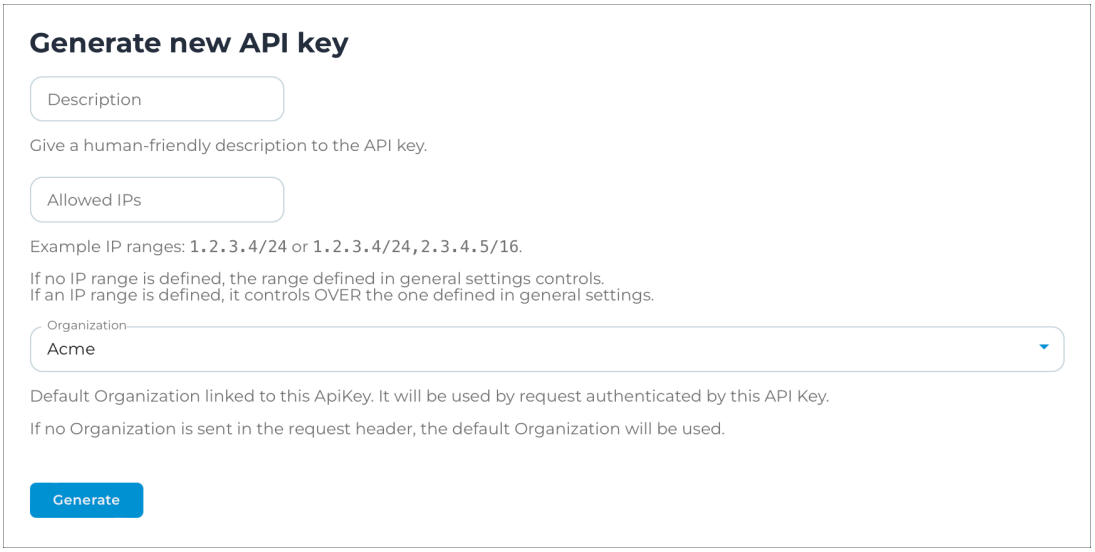
About this task

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.



> **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.

> **Note:**
> For these settings, you must use comma-delimited entries, in format. Values here will override the values in the **SECURITY** section on the **General** page.

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

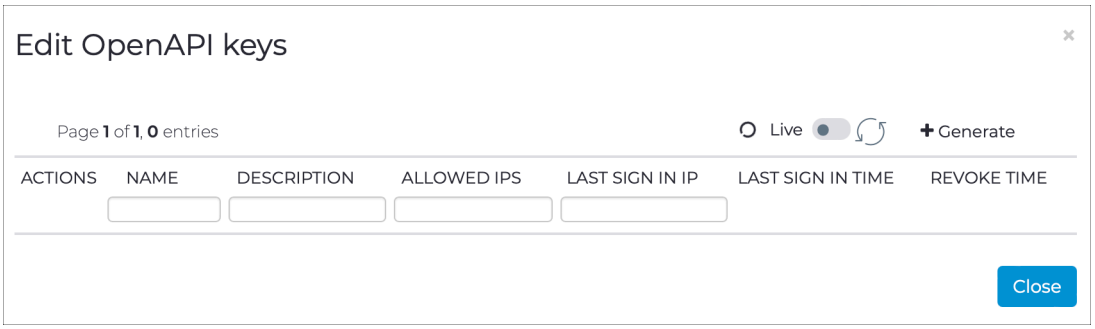
1. In the top navigation bar, select

   Result: A menu shows.

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

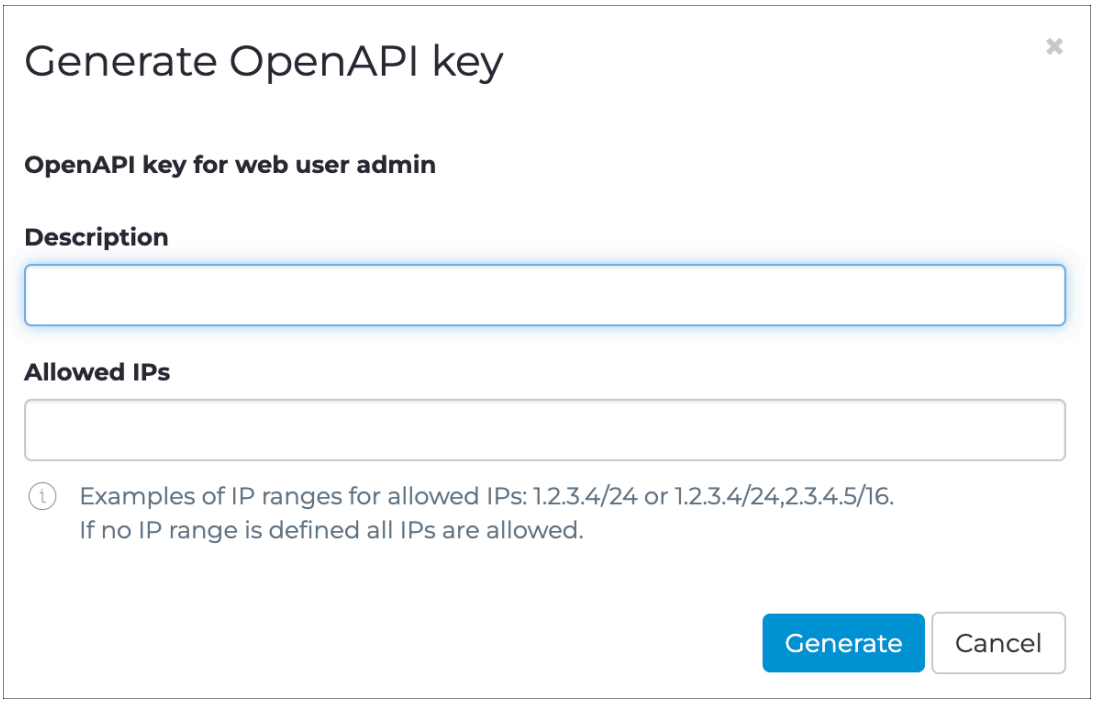
   Result: A dialog shows.

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. Troubleshooting

Troubleshooting

This section provides solutions for common issues with the ServiceNow Vulnerability Response integration with Nozomi Networks. It covers configuration checks, MID server connections, log analysis, handling import queues, resolving script failures, and offers guidance on when to contact customer support, and what information you should provide.

Configuration details

The **ServiceNow Vulnerability Response** integration is mostly pre-configured. This means that you only need to:

- Enter your **Nozomi URL**
- Enter your **username**
- Enter your **password**
- Select a *MID* server

If the **ServiceNow Vulnerability Response** is not working correctly, make sure that the above details have been entered correctly.

MID server connection

If you cannot connect to your Nozomi Networks environment from ServiceNow through the *MID* server, make sure that:

- The *MID* server is on the same network as the Nozomi Networks platform
- You can ping the Nozomi Networks instance from the *MID* server

Logs and error messages

If necessary, read the log messages. You can find the log messages in **System Logs** from the source: `x_none_nozomi_vr` Additional log messages from the source `sn_vul` might also show.

Error messages might show in:

- The `notes` field of the Vulnerability Integration Run, or
- The `state` and `notes` fields of the Vulnerability Integration Process

Import Queue table

The `sn_vul_ds_import_q_entry` of the **Import Queue** table will contain all of the pending transformation requests. To see what is currently being executed, you can filter this table to only show items that have a status of **Processing**.

Potential Failures of the VR-Register Discovery Source for Nozomi Fix Script

During the installation process, you might encounter instances where the **VR-Register Discovery Source for Nozomi** script fails to execute successfully. In such cases, you can follow the steps below to address the issue:

Examine the installation logs for error messages related to the **VR-Register Discovery Source for Nozomi** Fix Script. These logs can provide valuable insights into the cause of the failure, such as:

```
Application error in system log JavaScript evaluation error on:
var source_name = 'VR-Nozomi';
```

```
var dsUtil = new global.CMDBDataSourceUtil();
dsUtil.addDataSource(source_name);
```

Try the Fix Script again.

> **Note:**
> If the script fails during the initial installation attempt, you can run it again once the overall installation process has finished.

Customer support

If none of the previous solutions work, please contact our Customer Support team.

To help us resolve your problems as quickly as possible, please provide detailed information about the error messages and all the relevant logs.

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.

Common Vulnerabilities and Exposures

CVEs give a reference method information-security vulnerabilities and exposures that are known to the public. The United States' National Cybersecurity FFRDC maintains the system.

Common Vulnerability Scoring System

CVSS is a standardized framework used in cybersecurity to assess the severity of software vulnerabilities. It provides a numerical score to help prioritize risk management and response efforts.

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.