LDI ServiceNow Integration Guide

Release Version: 2   **Release Date: 3 June 2023**

Contents

1   ServiceNow Integration

The Lenovo Device Intelligence (LDI) ServiceNow Integration Guide helps you setup LDI ServiceNow Plugin so that ServiceNow platform can connect to device(s) in the LDI organization account through LDI external API.

1.1   Audience

IT Administrators, Analysts, and Managers.

1.2   Prerequisites

- Establish parity between LDI and ServiceNow Platforms.
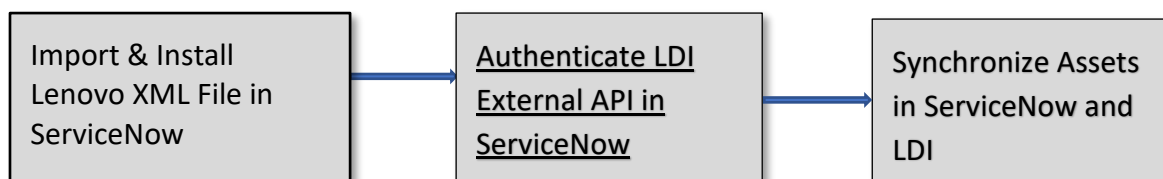
> **Note**:
>
> A physical device like laptop, desktop, server, etc. is referred to as a Device in LDI application and as an Asset in the ServiceNow application.

You must synchronize devices in LDI with the Assets or configuration items in the ServiceNow application for the proper working of the LDI ServiceNow plugin. Therefore, you must fulfil the following conditions:

   o The name of the LDI device must be the same as the name of the Asset in the ServiceNow application
   o The Serial number of the LDI device and Asset serial number must be the same.

- Requisite Roles and Rights required for LDI and ServiceNow accounts.

Application	Roles and Rights
Lenovo Device Intelligence (LDI)	You must have an Organization Administrative account to generate API credentials - Client ID and Secret. The API credentials are required for API integration between LDI and ServiceNow so that the LDI ServiceNow plugin can work.
ServiceNow	Administrator account

Disclaimer – The LDI ServiceNow plugin was developed and tested in a clear and empty ServiceNow Instance. Any change done by ServiceNow in their platform can affect the LDI ServiceNow plugin.

| Import & Install Lenovo XML File in ServiceNow	→	Authenticate LDI External API in ServiceNow	→	Synchronize Assets in ServiceNow and LDI

1.2.1   Import and Install Lenovo XML File in ServiceNow

Application Remote Update Set is an XML file that you can import into ServiceNow Instance. The file contains configuration and scripts developed by Lenovo.
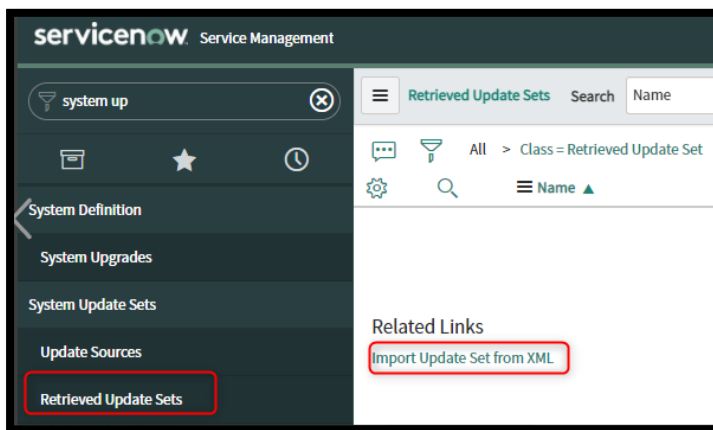
> **Note**: It is mandatory to have an administrative account in ServiceNow application.

Follow these steps to import and install Lenovo XML file:

1. Sign in to the ServiceNow dashboard.
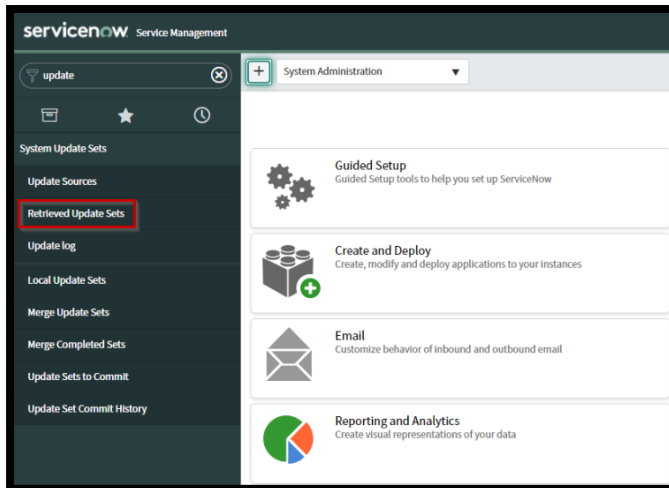
2. Enter **update** in the search box. The **System Update Sets** menu appears.

3. Click **Retrieved Update Sets**. In the Related Links, Import Update Set from XML link appears.
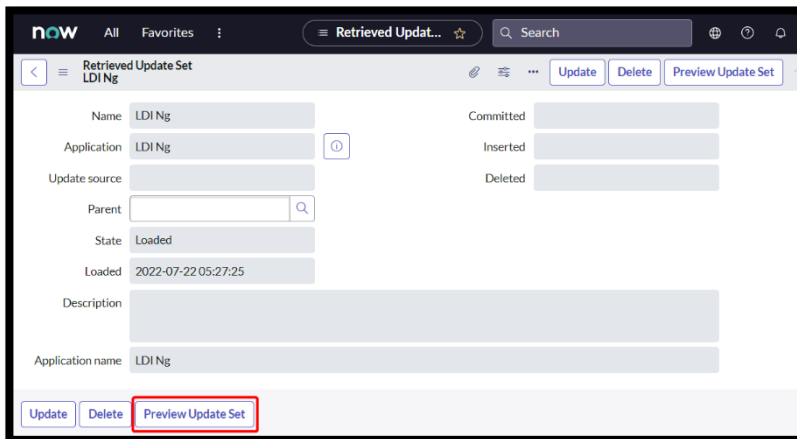

4. Request the ServiceNow XML file via email to ldisupport@lenovo.com and once received click Import Update Set from XML.

5. Click **Choose file**, and then click **Upload.** After the file is imported, the LDI Ng application appears in the list.
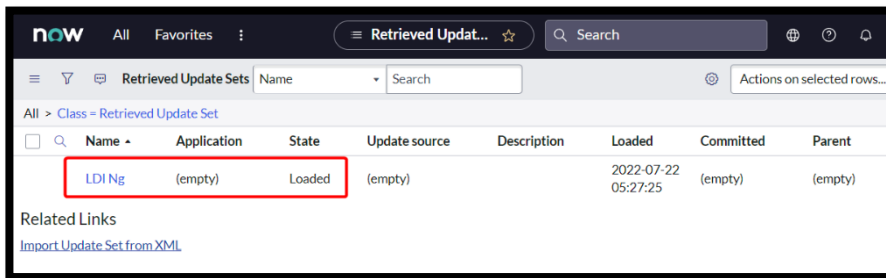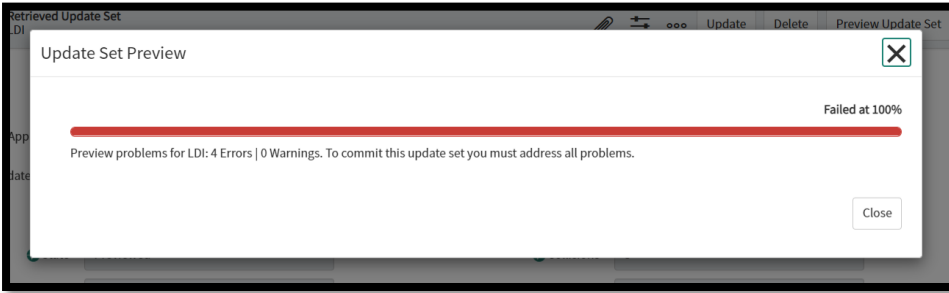

6. Click **LDI Ng**. The LDI record appears in the ServiceNow application.
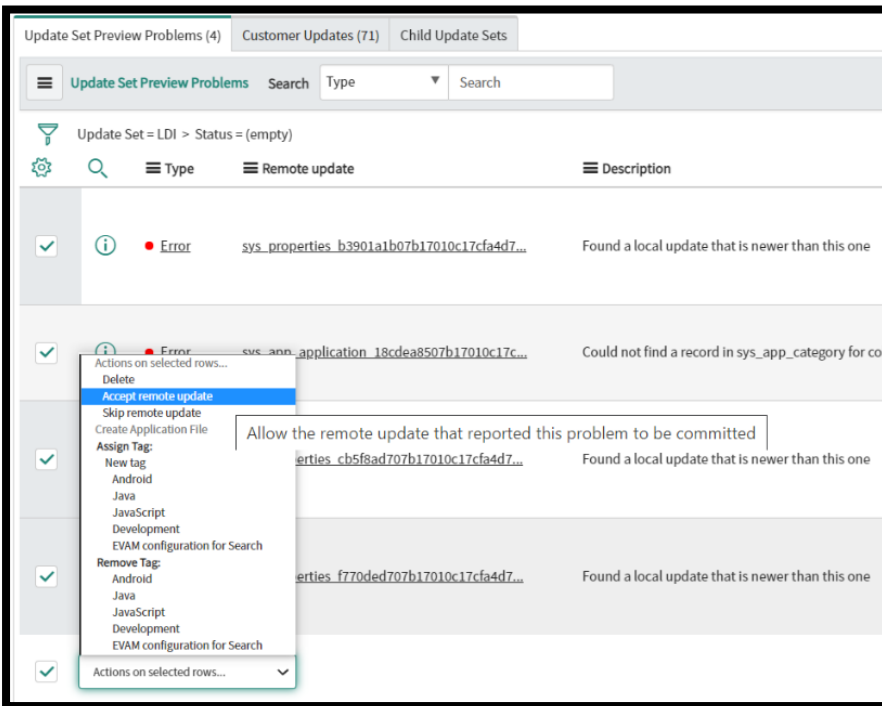

Note: You can update, delete, or get a preview of the LDI update sets.
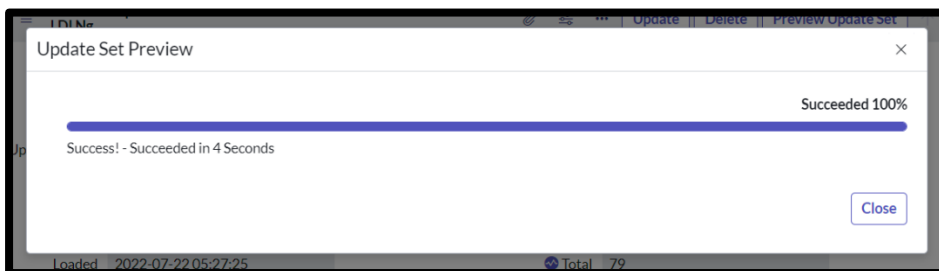
7. Click Preview Update Set.

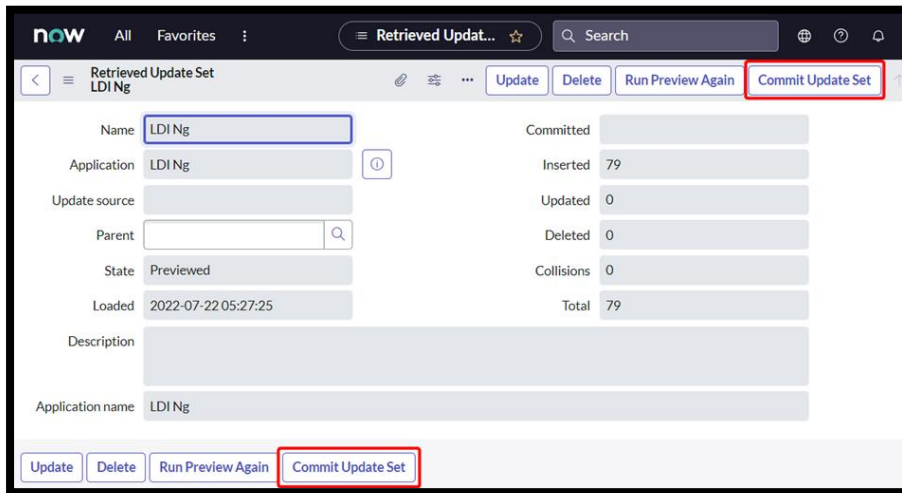**Note**: The preview fails if there are errors during import of LDI XML file.

8. To resolve the errors, select all errors in the tab, click **Update Set Preview Problems.**
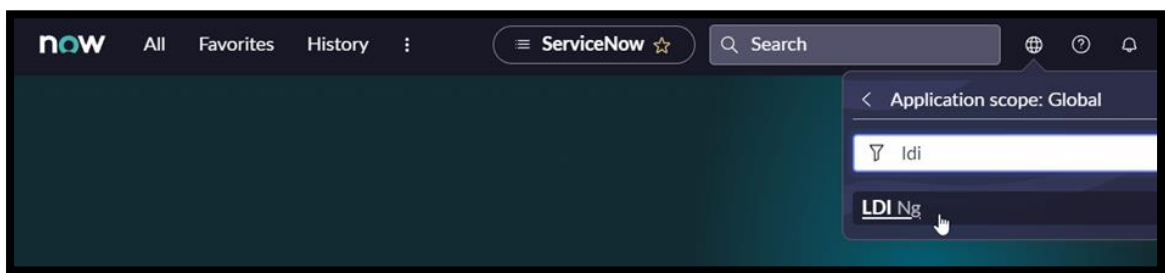

9. Click Accept remote update.

10. Click **Commit Update Set**. The update set is successfully commited.
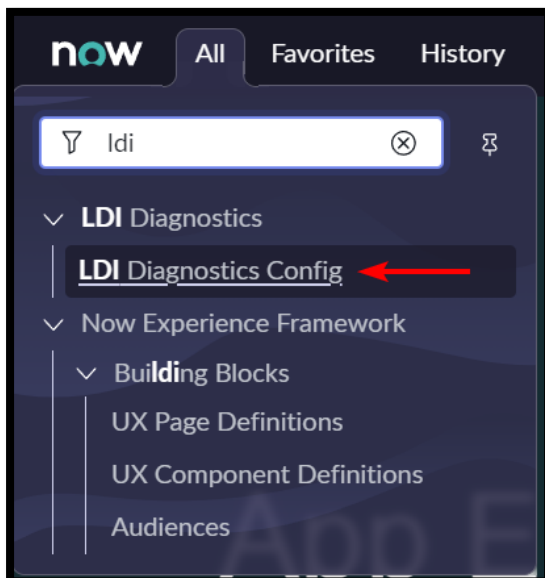

1.2.2   Authenticate LDI API Credentials in ServiceNow

This section explains how to add the LDI API credential in the ServiceNow instance to setup LDI ServiceNow plugin.

1. We recommend switching to the context of the newly committed LDI Ng application

2. In the search box, enter **LDI**. The **LDI Diagnostics Config** tab appears.

3. Click **LDI Config**. The **Properties** page appears. In this page, enter credentials of LDI API to establish connection between ServiceNow and LDI platform.

7

Properties

Insert properties values to establish connection to LDI API

LDI External API url link in format https://... ⓘ

Authentication URL to get LDI API token ⓘ

External API client id ⓘ

External API client secret ⓘ

Save

4. Enter the External API URL and Authentification URL for your LDI portal's region as denoted below:

| LDI API URLs |
| --- |
| 1. NA |
| External API: https://api.naea1.uds.lenovo.com
Authentication: https://auth.naea1.uds.lenovo.com |
| 2. EU |
| External API: https://api.euwe1.uds.lenovo.com
Authentication: https://auth.euwe1.uds.lenovo.com |
| NA is North American Region and EU is European Union Region. |

Note: For more information, refer to the LDI API Guide.

5. Enter LDI API Client ID and Client Secret. These can be sourced in the LDI portal by navigating to the Profile dropdown and selecting Organization Settings → API Credentials.
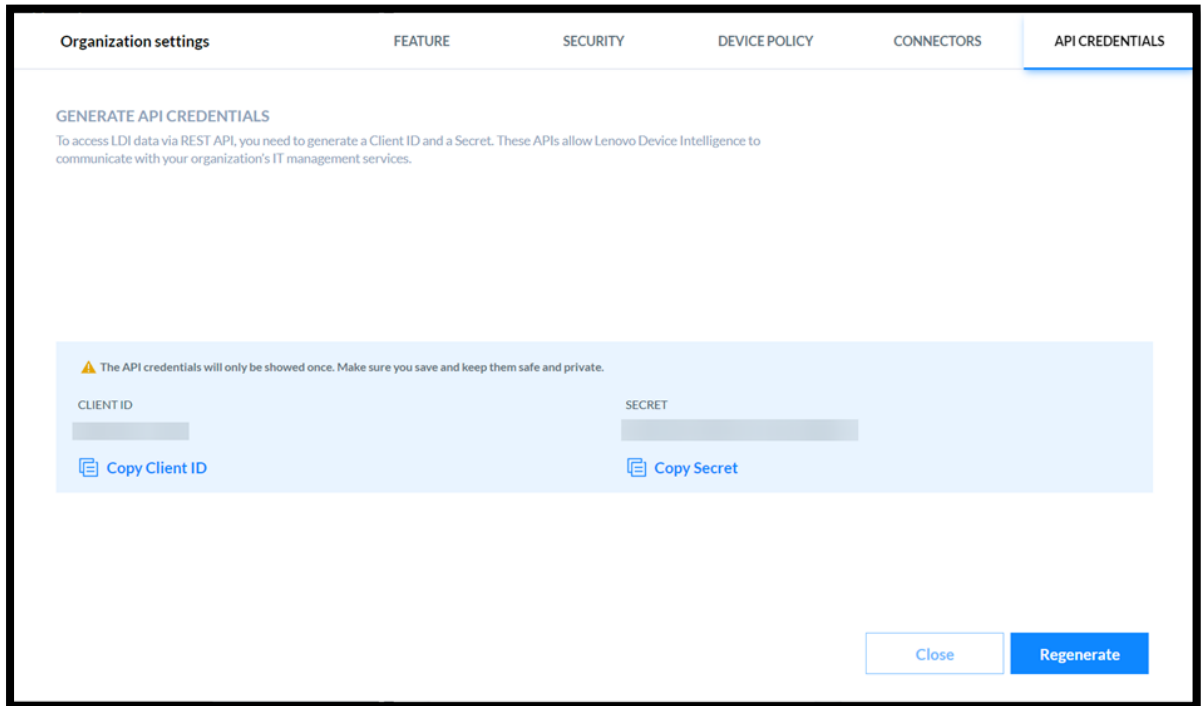
Note: After you generate a new pair of Client ID and Secret key, the older pair gets invalid.
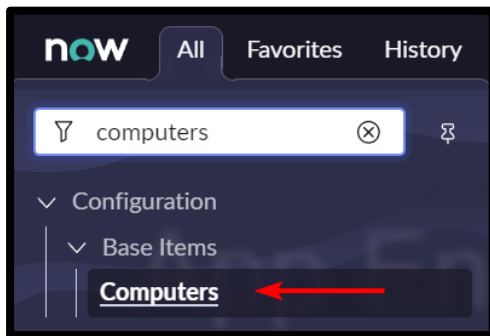
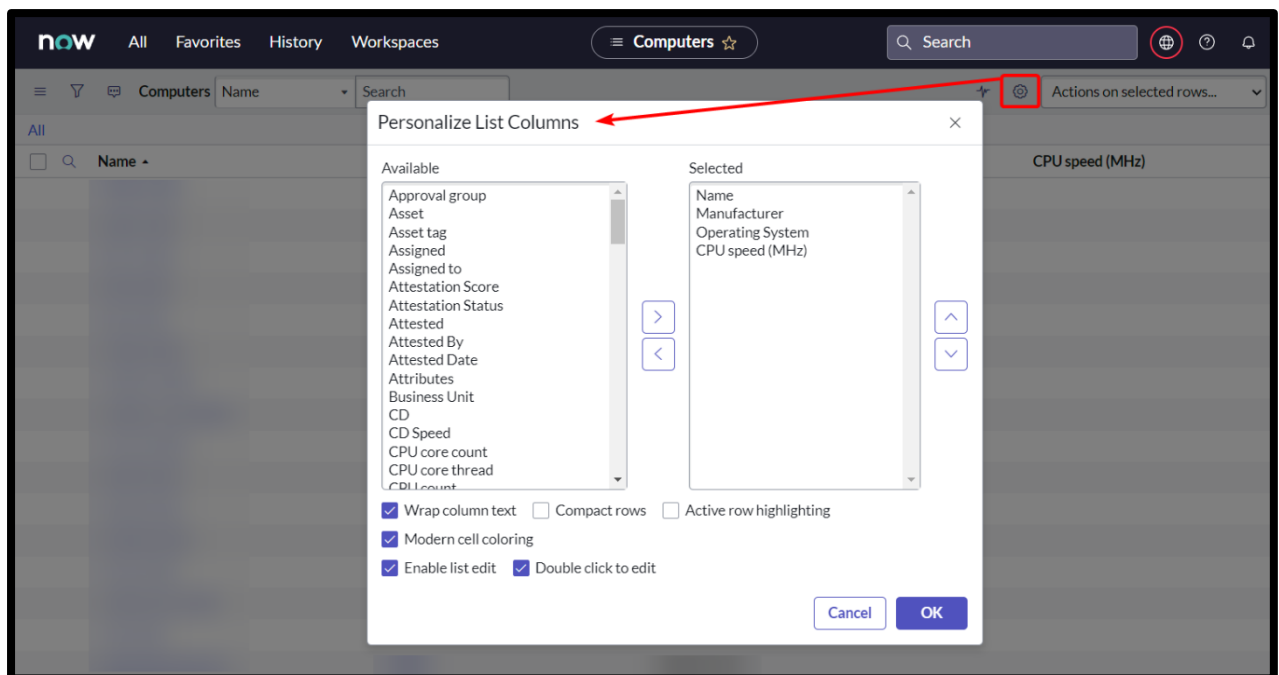6.   Now select save once the fields are completed.
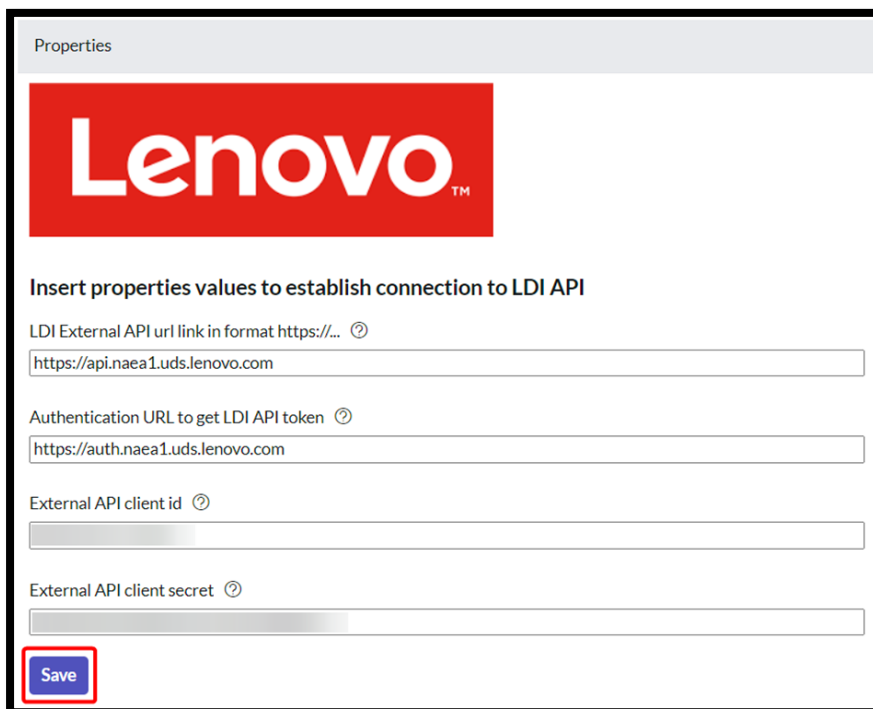
1.2.3 Synchronize Assets in ServiceNow and LDI

Refer [Prerequisites](#) section before proceeding ahead.

1. Log in to ServiceNow instance.

2. In the search box, enter **computers**. Click the **Computers** tab that appears in the navigation menu.
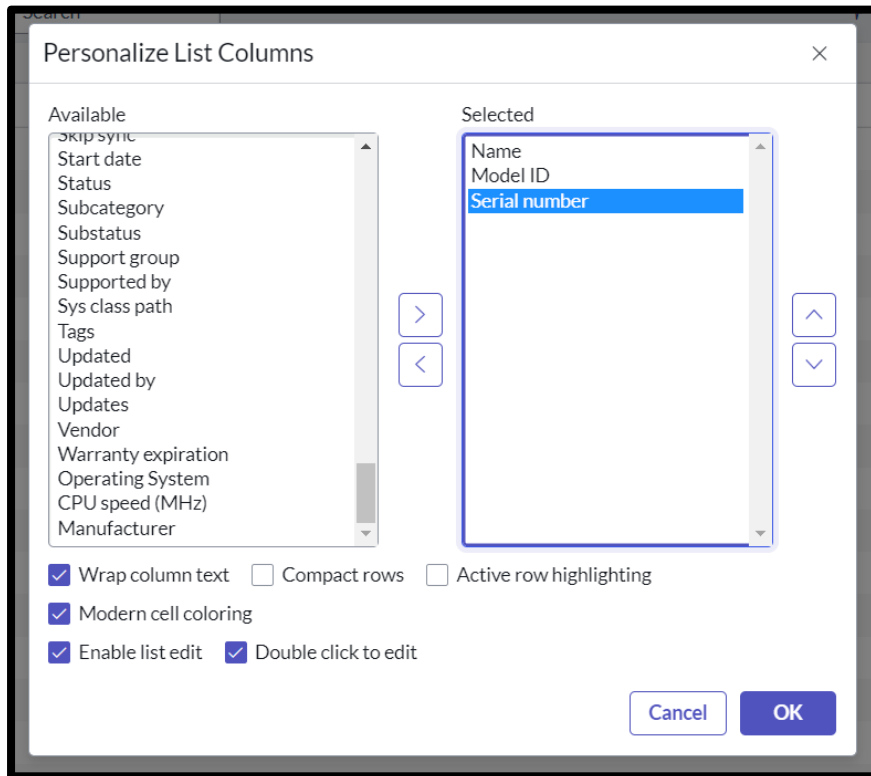

3. Click the **Settings** ⚙ icon so that the **Personalize List Columns** window appears.

**Note:** The checkboxes shown in the screenshot are marked by default.

1. Name of the Asset. For example, EPUAKYIW0FCA

2. Model ID of the Asset – HP EliteBook 850G7 Notebook

3. Serial Number of the Asset – 5CG1092

You can search an asset by the Name, Model ID, or Serial Number. Choose assets you want to synchronize by using filters.

Important Note: Do not apply filter if you want to synchronize all.
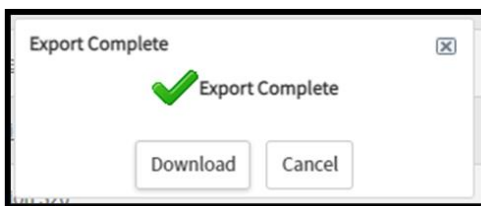
4. Mark the checkboxes to select Assets(s) that you want to synchronize with LDI platform.
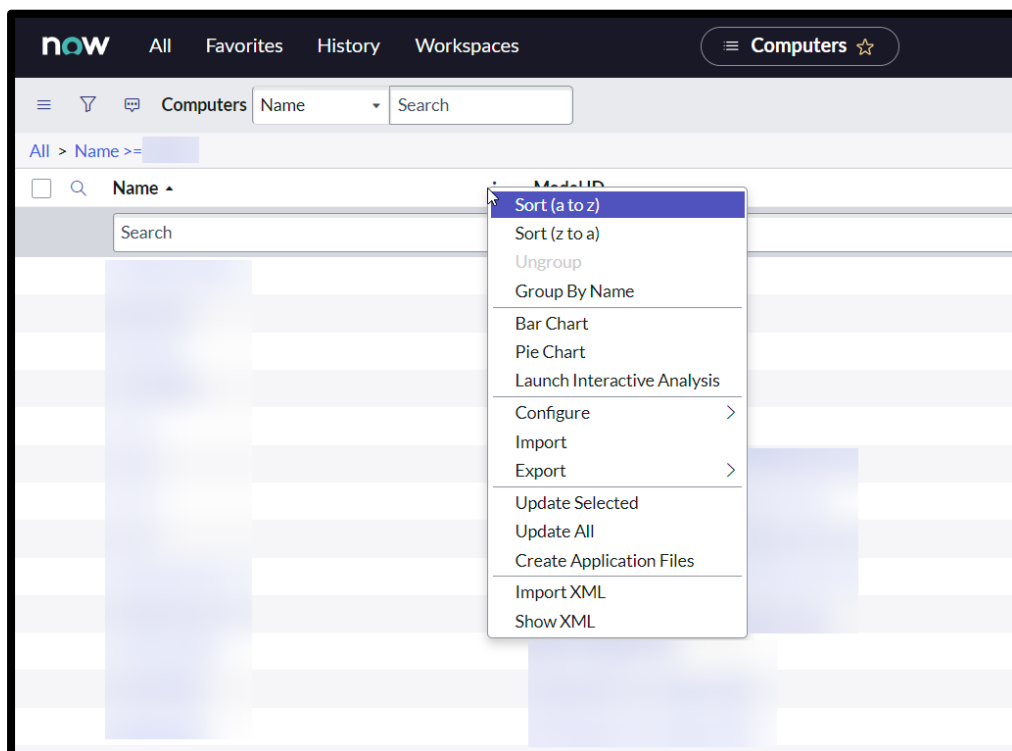
5. Right-click the **Export** tab. In the context menu, choose **Export → CSV**.
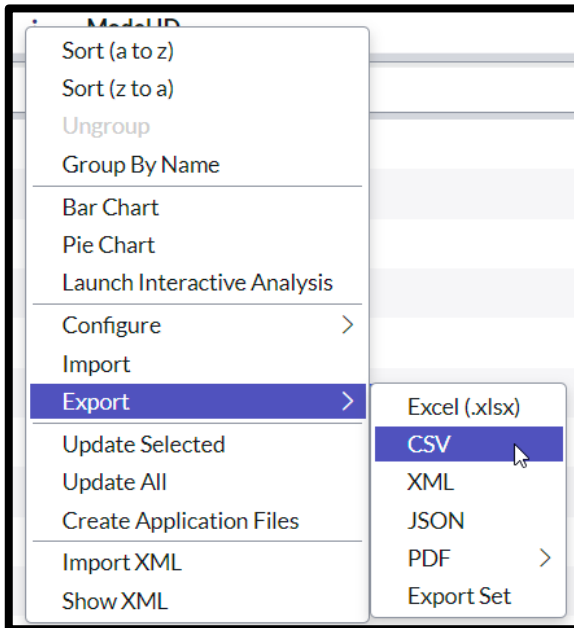
6. Select the type of format of the file to be exported. For example, CSV.

7. Click **Download.** The file is downloaded on the device.

   The format of the ServiceNow file is:

   ```
   "name","model_id","serial_number"
   "EPUAKYIW0FCA","HP HP EliteBook 850 G7 Notebook PC","5CG1092PLB"
   ```

   ```
   DEVICE NAME, MACHINE TYPE, SERIAL NUMBER, GROUP
   EPUAKYIW0FCA, HP EliteBook 850 G7 Notebook PC,5CG1092PLB,
   EPBYMINW150E,HP EliteBook 850 G7 Notebook PC,5CG1092PMP,Office1
   ```

1.2.4   Mandatory Requirements for LDI CSV Format

If the name of a device in LDI and ServiceNow is different, then the device name can be changed automatically using the CSV file.
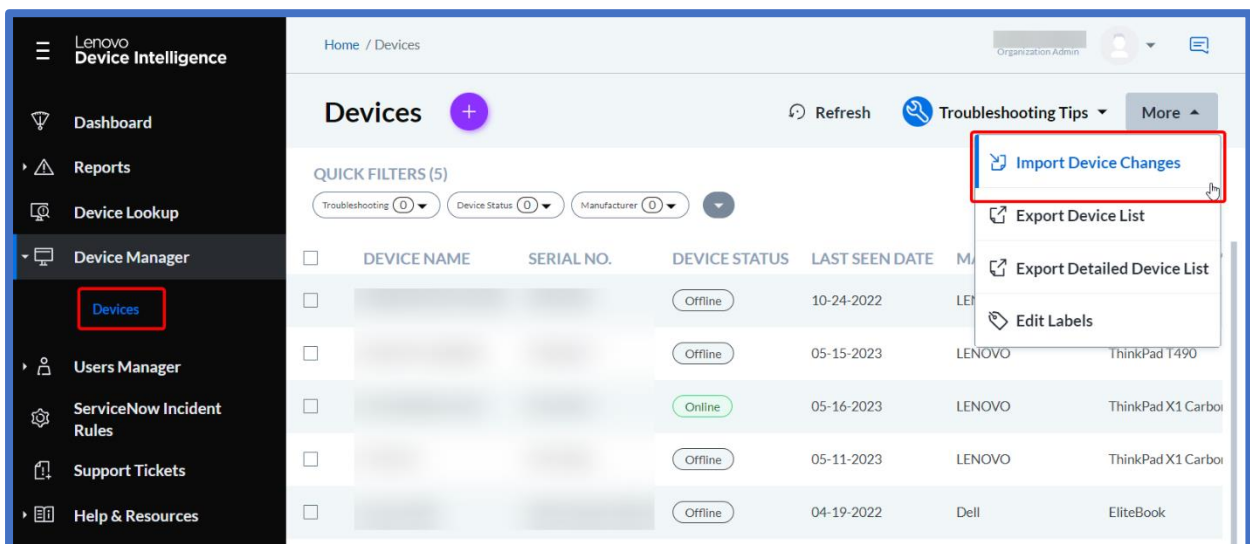
Important Notes:

- Only underscore (_) and dash (-) symbols are allowed.
- To upgrade DEVICE NAME automatically, MACHINE TYPE must be model_id, and SERIAL NUMBER must be equal to serial_number
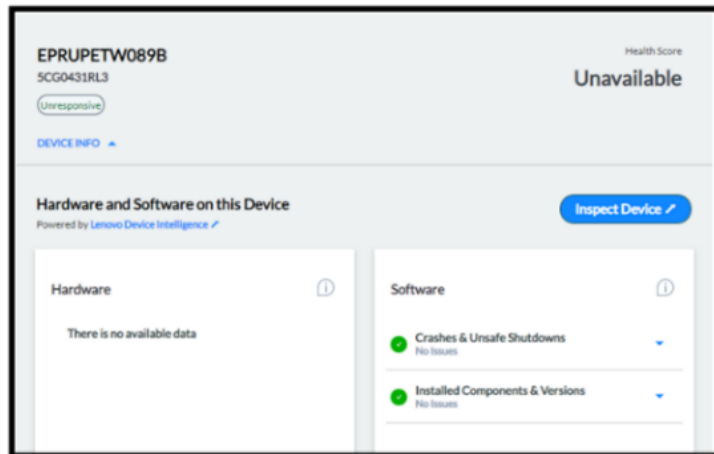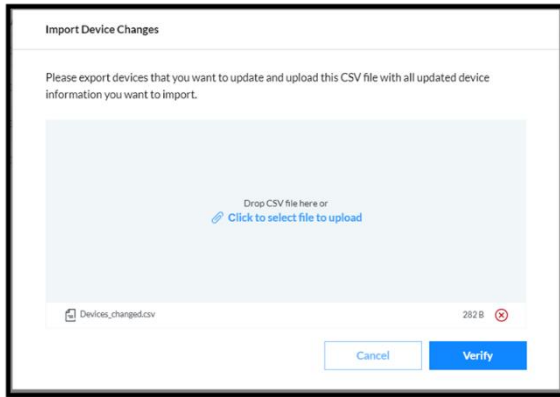

1.2.5   Update Asset Information from ServiceNow to LDI Account

1. Log in your LDI portal.
2. Click **Devices** in the navigation menu. The **Devices** pane appears.

3. Click **More**. The drop-down window appears.
4. Click **Import Device Changes**.

5. Select the file. For example, the CSV file of Assets exported from ServiceNow.

6. Click **Verify**. The file is verified.

7. Click **Yes.** The device information is updated in LDI, and you receive a confirmation email at your registered email ID. ServiceNow receives data of specific device(s) and renders it in the Plugin tab. The LDI ServiceNow plugin is set up.
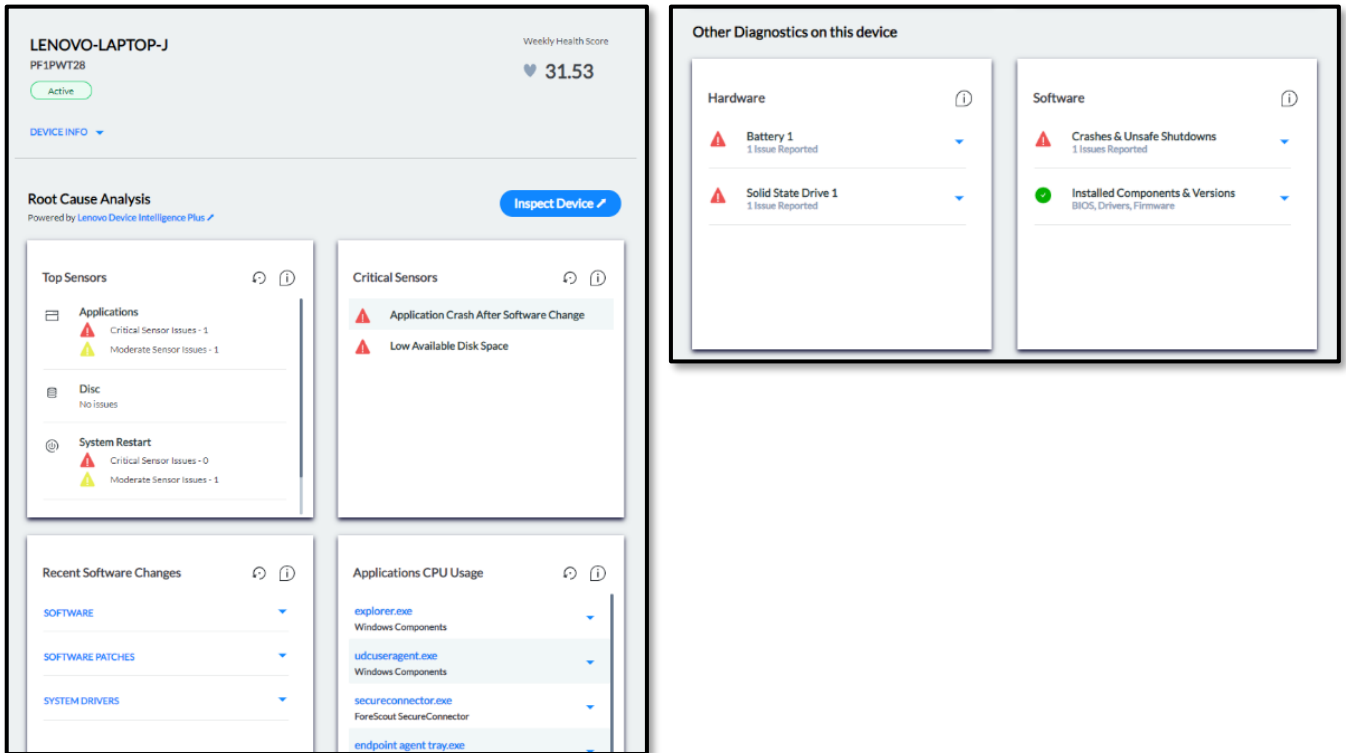
1.2.6   Integrate ServiceNow into LDI

This feature allows the system to raise a ticket and assign it to the LDI Support team when an incident occurs. It includes tasks such as configuring connection to ServiceNow portal, creating rules that includes sensor management, etc.

Communication between servicenow-integration-service and ServiceNow API occurs using basic authentication. Thus, ServiceNow user credentials are stored in the servicenow-integration-service database and provided each time the API is called.

There is a possibility to use a more secure mechanism - OAuth authentication, when a limited-time token is obtained from OAuth API by credentials and is used in the API calls.

Follow this procedure to support the OAuth authentication:

1. The Organization Admin must create a user in ServiceNow for User ID and Password and a client for Client ID and Client Secret. For example, the user could be called **ldiservice**.
2. To do this, begin by searching in your ServiceNow portal for **organization** and select **Users**.
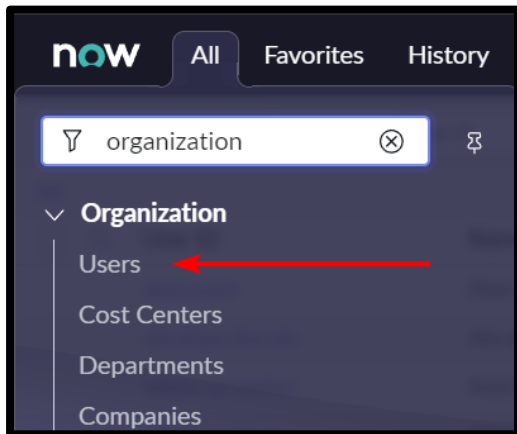
3. Inside the Users page, click on New and create a new user such as ldiservice and generate a password for the user. Take note of the username and password for step 10.

4. The user must also have roles specified: Admin, Asset, App_service_user, etc. With this set of roles, there is an issue with setting high impact and urgency through the API. When High is requested, Medium is set in the incident

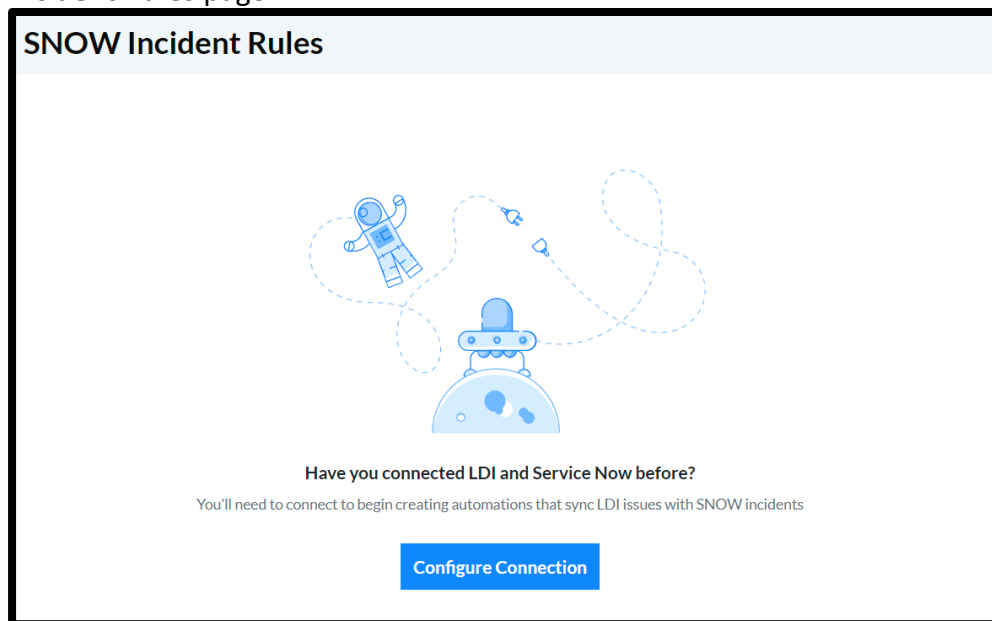5. In the search box type **application registry** and select Application Registry.
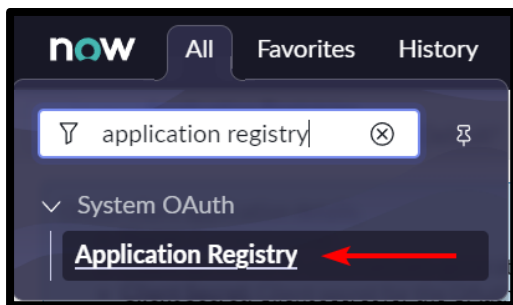
6. Once in the Application Registry page, select the ldi-service-connect.

7. Within the ldi-service-connect Application Registry, take note of the Client ID and Client Secret for step 10.
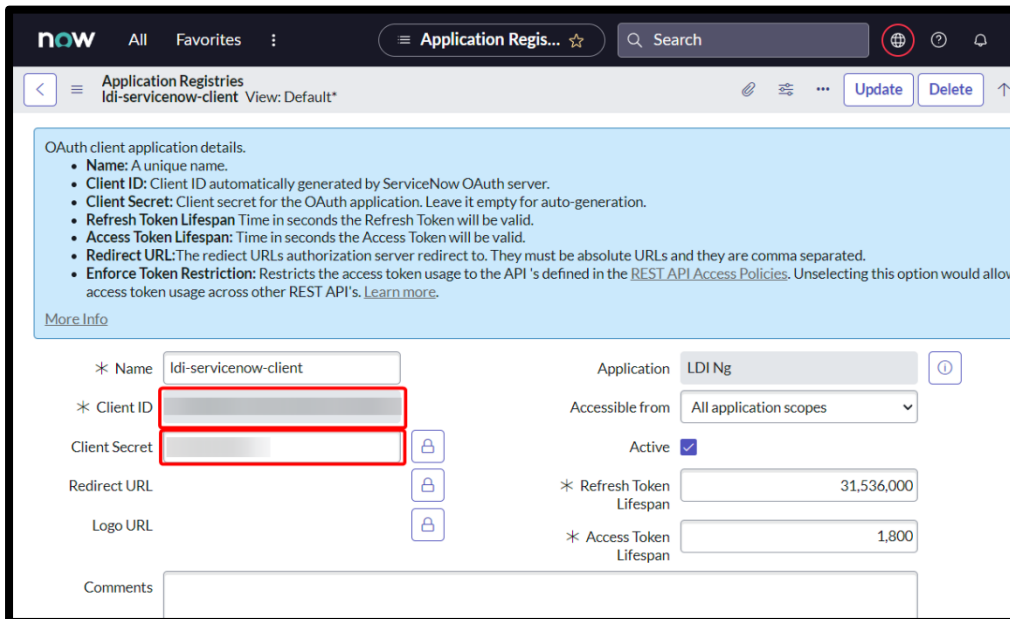
8. Now in another browser window, navigate to your LDI Portal and open the **SNOW Incident Rules** page.

9. We're now going to enter the ServiceNow API fields into the LDI portal so click **Configure Connection**.

10. Complete the Configuration form with the fields collected in the past few steps

Note: If you've done this previously and need to update the credentials you can click on the Config Status and choose **Edit Configuration**.
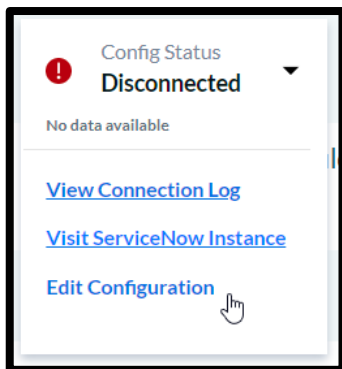

11. Fill-in Instance URL.

12. Enter the values for these fields:

- User ID or Admin Credentials
- Password
- Client ID
- Client Secret

13. Click **Connect to ServiceNow**. All the filled-in credentials are stores in the database afterward. This way it's possible to receive tokens whenever it's needed.
Note: This option requires saving user and password, but this user can be controlled at ServiceNow side.
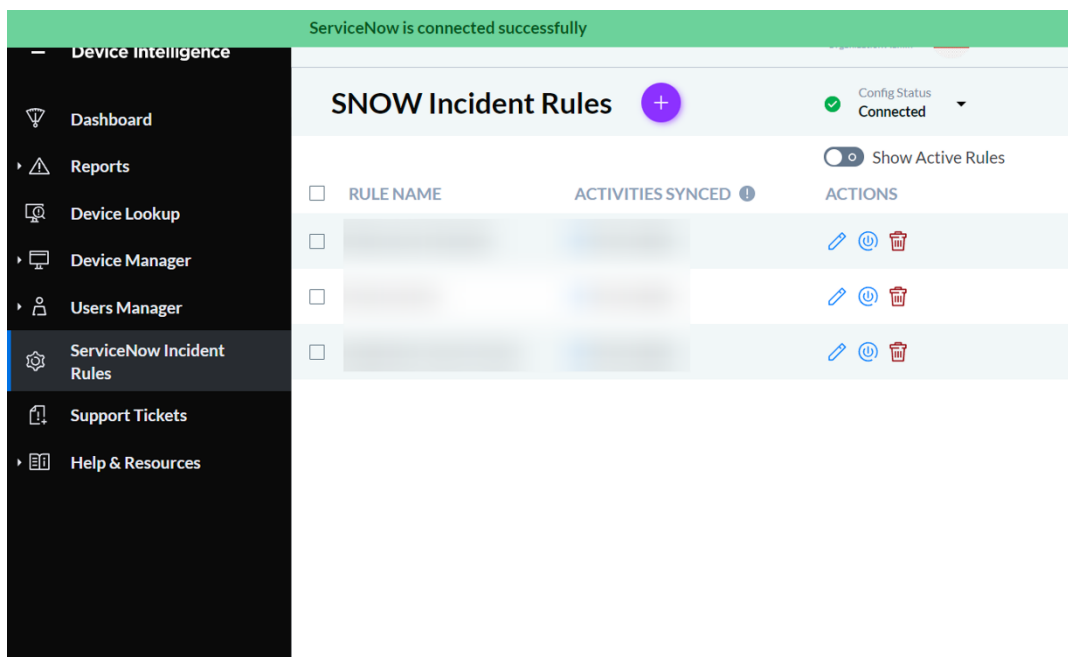
Note: You must have an LDI Admin access privileges to configure and create a rule.

1. Log in to LDI portal.

2. Select the ServiceNow Incident Rules page.

3. Click the **Config Status** drop-down on top-right in the page.

4. Select Edit Configuration. The Configure Connection to ServiceNow page appears.

5. In the **Add Instance Credentials** section, enter the ServiceNow Instance URL, ServiceNow User ID, and ServiceNow Password.

6. In the **Add Client Credentials** section, enter the ServiceNow Client ID and ServiceNow Client Secret.

   Note: All are mandatory fields.

7. Click Connect ServiceNow.

1.2.7   Create a ServiceNow Incident Rule

Note: You need to configure ServiceNow in LDI before creating an incident rule. Refer to Integrate ServiceNow Into LDI for more details.
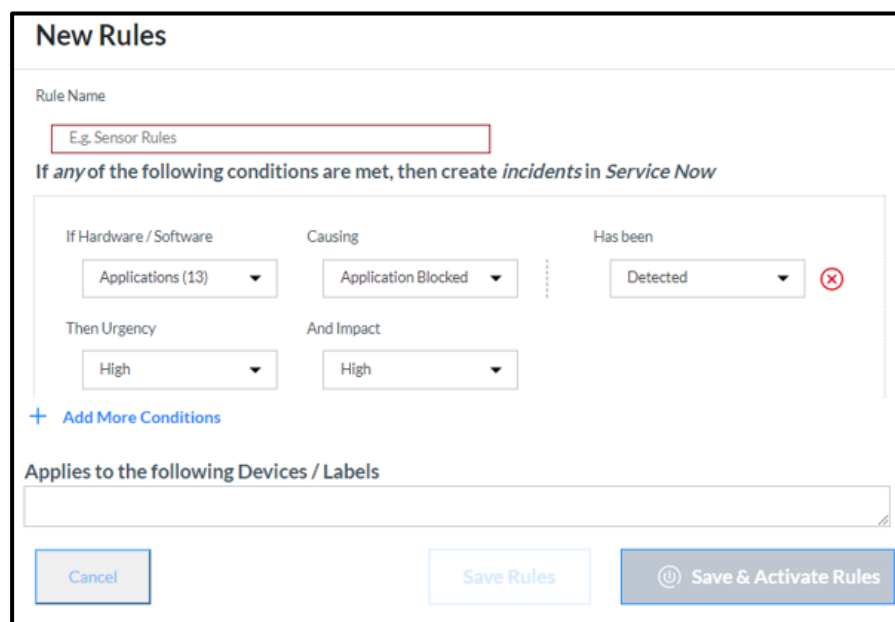
The following table displays the fields in the SNOW Incident Rules page:

Field Name	Field Description
Rule Name	The Name of the ServiceNow rule.
Activities Synced	The activities logged by LDI automation. Activities synced displays the number of incidents created when this rule is applied. When the rule is deactivated, this field is not updated.
Actions	- Click the ✎ icon to edit a rule. - Click the ⏻ icon to activate a rule. - Click the ⏻ icon to deactivate a rule. - Click the 🗑 icon to delete a rule.

Note: You can also click the ⬤◯ Show Active Rules toggle button on top of the page to display all the active rules for the ServiceNow devices.

To create a rule:

1. In the **SNOW Incident Rules** page, click the ⊕ icon. The **New Rules** page appears.

2. Enter the name you want to give to a new rule.

3. Select the conditions from the dropdowns.

4. Enter the device name or label to which the new rule is applicable.

5. Click **Save Rules**.

1.2.8　Handle an Incident in ServiceNow

The following page displays all the related details of an event created due to occurrence of an incident.

Note: When you create an incident, the details are updated in the **LDI Diagnostics** tab. You can see this tab at the bottom of the page. This tab helps you to take appropriate actions.

If the connection of ServiceNow is broken with the LDI device for more than 24 hours, you are unable to see the updated issue resolution details.