



# BeyondTrust

## **BeyondInsight and Password Safe ServiceNow Integration Guide**

## Table of Contents

---

<b>Configure BeyondInsight and Password Safe with ServiceNow</b> .....	<b>3</b>
Configure ServiceNow Scan Target Collector .....	4
Configure ServiceNow Export Connector .....	6
Configure ServiceNow with Password Safe Ticket System .....	9

# Configure BeyondInsight and Password Safe with ServiceNow

BeyondInsight allows you to import and export asset data between the BeyondInsight database and your ServiceNow instance using connectors.

You can also configure integration between ServiceNow and the Password Safe Ticket System to allow for ticket validation prior to users gaining access to privileged passwords and sessions. This integration includes options to auto-approve ticket validation, and break glass functionality for emergency approval in the case where ServiceNow is unavailable.

The following connectors can be created in BeyondInsight to connect to your ServiceNow server:

- ServiceNow Export Connector
- ServiceNow Scan Target Collector
- ServiceNow Ticket System

## Configure ServiceNow Scan Target Collector

To configure the ServiceNow Scan Target Collector, you must do the following:

- Create a connection to your ServiceNow instance.
- Create a Smart Group with parameters configured to include the assets (host and IP address) to import from ServiceNow. After the Smart Rule is created, the data in the rule is refreshed and exported based on the **Smart Rule Action expiration period**, which is every hour by default.



**Note:** *BeyondInsight supports only ServiceNow Cloud Solutions.*

## Create ServiceNow Scan Target Collector

After the connector is tested and saved, each scheduled run retrieves ServiceNow data from the defined table that has an entry in one of the defined fields (valid IP address or DNS defined).



**Tip:** *There might be a large number of records to import from ServiceNow. You can change the default value in the `RemManagerSvc.ece.config` file. For more information, please see ["Change the Batch Size Limit for Import File" on page 5](#).*

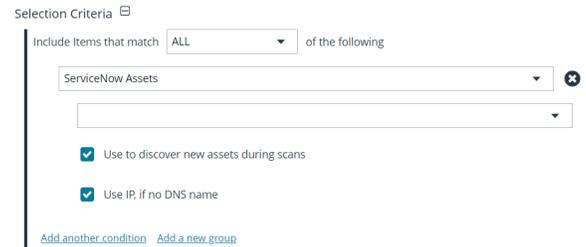
After the data is retrieved, the data is stored in the BeyondInsight database.

1. In BeyondInsight, go to **Configuration > General > Connectors**.
2. From the **Connectors** pane, click **Create New Connector**.
3. Enter a name for the connector.
4. Select **ServiceNow Scan Target Collector** from the **Connector Type** dropdown list.
5. Click **Create Connector**.
6. Select the applicable **Organization** from the dropdown list.
7. Leave **Active** enabled. Asset data is imported from ServiceNow only when the connector is active.
8. Enter a ServiceNow **Username** and **Password**. The credentials for the ServiceNow system must provide access to the web service and be able to create requests.
9. Enter the ServiceNow **instance URL**.
10. Enter the **Source Table**. The default value is `cmdb_ci_computer`.
11. Enter the information from the ServiceNow table that you want to import to BeyondInsight. The default values are `ip_address` and `fqdn`.
12. Set the scheduling options to synchronize ServiceNow with the BeyondInsight database. Time period options change depending on the **Frequency**.
13. Enter the **Start** date and time for synchronization to begin.
14. Click **Test Connector** to ensure the connection to the ServiceNow instance is working.
15. Enable **Run immediately After Save** if desired.
16. Click **Create Connector**.

## Create a Smart Group

Once the data is in the BeyondInsight database, you can create a smart group based on the ServiceNow assets. When creating the smart group, ensure you select **ServiceNow Assets** from the dropdown in the **Selection Criteria**.

When the Smart Group processes, the DNS name is always used when it exists. The IP address is used to determine assets in the Smart Group when that option is enabled.



Selection Criteria ⊞

Include items that match **ALL** of the following

ServiceNow Assets ⊕

Use to discover new assets during scans

Use IP, if no DNS name

[Add another condition](#) [Add a new group](#)

## Change the Batch Size Limit for Import File

Depending on the environment, there may be a large number of records to import. You can set the **importBatchLimit** value in the **RemManagerSvc.exe.config** file, located in the BeyondInsight installation directory. The default limit set in the file is **5000**. You cannot enter a value greater than **10000**.

```
<!-- ServiceNow Imports -->  
<Process name="servicenowimportshandler" assembly="" order="17" active="true"  
accessType="internal">  
<Handlers>  
<Handler name="ServiceNowImportsHandler" handlerType="1" runFrequency="3" frequencyType="m"  
referenceTime="1:00" namespace="" order="0" active="true" importBatchLimit="5000"></Handler>  
</Handlers>  
</Process>
```

## Configure ServiceNow Export Connector

There are two steps to configure a ServiceNow export connector:

- Create a connection to your ServiceNow instance.
- Create a Smart Group with parameters configured to include the assets (and data) to export to ServiceNow. After the Smart Rule is created, the data in the rule is refreshed and exported based on the **Smart Rule Action expiration period**, which is every hour by default.

### Create ServiceNow Export Connector

Follow the steps below to create the connector:

1. In BeyondInsight, go to **Configuration > General > Connectors**.
2. From the **Connectors** pane, click **Create New Connector**.
3. Enter a name for the connector.
4. Select **ServiceNow Export Connector** from the **Connector Type** dropdown list.
5. Click **Create Connector**.
6. Select the applicable **Organization** from the dropdown list.
7. Leave **Active** enabled. Asset data is imported from ServiceNow only when the connector is active.
8. Enter a ServiceNow **Username** and **Password**. The credentials for the ServiceNow system must provide access to the web service and be able to create requests.
9. If you are using an older version of ServiceNow and you are using update sets, enable the **Using Update Set** option.
10. Enable **Asset Export Active**.
11. Enter the URL to the ServiceNow instance in **Asset Web Service URL** box.
12. Select desired **Extended Field Mappings** from the list.
13. Click **Create Mapping** and enter the field mappings according to which export options you selected. Available fields and suggested field mappings are detailed in sections below or the export options, enter the following information:
14. Click **Test Connector** to ensure the connection to the ServiceNow instance is working.
15. Click **Create Connector**.

### Create Field Mappings for Exporting Assets

When creating field mappings, the following must be considered:

- **Asset ID** must be mapped to a ServiceNow field.
- The ServiceNow field **name** must be mapped if assets are being exported.

These BeyondInsight asset fields are available for export:

- Asset ID
- Asset Name
- Dns Name
- Ip Address
- Operating System

- Workgroup
- SmartGroup Name
- Date Added
- Last Updated
- Literal Value (Enter **Literal Value**)

## Suggested Field Mappings

ServiceNow Field	Data Type	Asset Field	Literal Value
correlation_id or custom correlation_id field	String	Asset ID	
correlation_display or custom correlation_display field	String	(Literal Value)	BeyondInsight Asset
name	String	Asset Name	
ip_address	String	IP Address	
Os	String	Operating System	
Map other fields as determined by user requirements.			

## Create a Smart Group

Assets exported are defined in the Smart Group. After the Smart Group is created, the data in the rule is processed and exported every hour.



**Tip:** You can change the processing time in the *RemManagerSvc.exe.config* file. For more information, please see "[Change the Data Export Processing Frequency](#)" on page 8.

1. From the **Smart Rules** page in BeyondInsight, configure a Smart Group as usual.
2. In the **Actions** area, select **Export Data**.
3. Select the name of the connector.
4. Select an audit group from the list.
5. Enter the expiration period in days..

Actions ⊟

Export Data ⊕

ServiceNow ⊟

Expiration period (in days) ⊖ 30 ⊕

Show asset as Smart Group ⊕

View assets in a standard asset grid ⊟

[Add another action](#)

Create Smart Rule Discard



**Note:** Assets (depending on what is defined in the collector details) are only exported once in the defined expiration period. However, an asset may be exported more than once if, for any reason, the item is excluded from the smart group but is re-included later. After the expiration period passes, if that asset or vulnerability remains in the smart group, it is exported again.



For more information on working with Smart Rules, please see the [BeyondInsight User Guide](https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/index.htm) at <https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/index.htm>.

## Change the Data Export Processing Frequency

You can set the data export processing frequency value in the **RemManagerSvc.exe.config** file, located in the BeyondInsight installation directory, by changing the **referenceTime** value.

```
<!-- Data export processor. This exports Assets and/or Vulnerabilities to external systems such as BMC Remedy. -->
<Process name="DataExportProcessor" assembly="" order="13" active="true" accessType="internal">
<Handlers>
<Handler name="DataExportHandler" handlerType="1" runFrequency="1" frequencyType="h"
referenceTime="1:00" namespace="" order="0" active="true"></Handler>
</Handlers>
</Process>
```



**Note:** For BeyondInsight version 21.2 and later releases, the data export processor does not export vulnerabilities.

## Import the BeyondInsight Update Set

The update set provides the BeyondInsight modules and menus in your ServiceNow instance. The BeyondInsight update set file you must import into your ServiceNow instance is located in the following installation directory on Windows 2022 appliances:

**%Program Files (x86)%\BeyondTrust\BeyondInsight\ServiceNow**



**Note:** For Windows 2016 appliances, the installation directory is **%Program Files(x86)\eEye Digital Security\Retina CS\ServiceNow**.



For more information on transferring update sets in ServiceNow, please see [Update set transfers](https://docs.servicenow.com/bundle/rome-application-development/page/build/system-update-sets/reference/update-set-transfers.html) at <https://docs.servicenow.com/bundle/rome-application-development/page/build/system-update-sets/reference/update-set-transfers.html>.

## Configure ServiceNow with Password Safe Ticket System

The process to configure ServiceNow with Password Safe is as follows:

- Create the integration user in ServiceNow. This integration user is used to configure the connector and functional account in the next steps.
- Assign the user the **itil** role in ServiceNow.
- Create a ServiceNow ticket system connector in BeyondInsight to your ServiceNow instance.
- Create a functional account and associate that with the ServiceNow connector.
- Add the ServiceNow ticket system to Password Safe.



**Note:** For any tickets being verified, you must ensure the **Requestor** is populated in the **Assigned To** field in the ServiceNow web portal. The **User ID** here must match the Password Safe **User ID**. Tickets must also be associated with a ticket table extending from the **Task** table.

## Create ServiceNow Ticket System Connector

Follow these steps to create the connector:

1. In BeyondInsight, go to **Configuration > General > Connectors**.
2. From the **Connectors** pane, click **Create New Connector**.
3. Enter a name for the connector.
4. Select **ServiceNow Ticket System** from the **Connector Type** dropdown list.
5. Click **Create Connector**.
6. Enter the following details for your ServiceNow system:
  - **Instance URL:** Provide the URL for the ServiceNow environment.
  - **Table Name (Optional):** If applicable, enter the appropriate table name.
  - **User ID Mapping:** Select the User ID format used in the ServiceNow instance. This validates users in Password Safe are assigned to the ticket in ServiceNow. The options are:
    - **User Name**
    - **User Principal Name**
    - **Email Address**
  - **Username and Password:** Provide credentials to be used to authenticate with ServiceNow. The credentials are used only on this configuration page. The user must be a member of a role containing an ACL for the **sys\_choice** table value field with **Read** access.
  - **Ticket Field Mappings:** Add field mappings to further validate tickets. You can map against Password Safe checkout start and end date and the system being accessed, as well as literal values, which is useful for validating the tickets state. Username is validated separately.
7. Click **Test Connector** to ensure connectivity to your ServiceNow server is successful.
8. Click **Create Connector**.

## Create a Functional Account in Password Safe

Once you have created the connector, follow these steps to create the functional account:

1. In BeyondInsight, go to **Configuration > Privileged Access Management > Functional Accounts**.
2. Click **Create New Functional Account**.
3. Select **Ticket System** from the **Entity Type** dropdown.
4. Select **ServiceNow** from the **Platform** dropdown.
5. Enter the **Username** and **Password** for ServiceNow. The credentials are the same used when entering ticket details in ServiceNow.
6. From the **Search Connectors** dropdown, select the ServiceNow connector (created using the process above).
7. Enter an **Alias** and, if required, a **Description** for the account.
8. Click **Create Functional Account**.

## Create a ServiceNow Ticket System in Password Safe

With the connector and functional account created, follow these steps:

1. In BeyondInsight, go to **Configuration > Privileged Access Management > Ticket Systems**.
2. From the **Ticket Systems** pane, click **Create New Ticket System**.
3. Select **ServiceNow Ticket System** from the **Platform** dropdown menu.
4. Select the functional account from the dropdown menu (created using the process above).
5. Enter a **Name** for the system.
6. If desired, enter a **Description**, **Access Policy Certificate Code Name**, and **Access Policy Code**.
7. Enable the options for features you want. Options are:
  - **Auto Approve on Ticket Number Validation**
  - **Enable Emergency Approval Without Ticket Number**
  - **Make Ticket System the Default**
8. Click **Create Ticket System** when done.



**Note:** The **Access Policy Certificate Common Name** and **Access Policy Code** fields are not used.