BeyondTrust

BeyondInsight and Password Safe ServiceNow Integration Guide 6.9

TC:6/2/2019

Table of Contents

Configure BeyondInsight and Password Safe with ServiceNow **3**
Configure ServiceNow Asset Import Connector **4**
Create ServiceNow Import Connector 4
Create a Smart Group 4
Change the Batch Size Limit for Import File 5
Configure ServiceNow Export Connector **6**
Create ServiceNow Export Connector 6
Field Mappings for Exporting Assets Only 6
Field Mappings for Exporting Vulnerabilities Only 7
Field Mappings for Exporting Both Assets and Vulnerabilities 8
Create a Smart Group 8
Change the Data Export Processing Frequency 9
Configure ServiceNow with Password Safe Ticket System **10**
Create ServiceNow Ticket System Connector 10
Create a Functional Account in Password Safe 10
Create a ServiceNow Ticket System in Password Safe 11

Configure BeyondInsight and Password Safe with ServiceNow

BeyondInsight allows you to import and export data between the BeyondInsight database and your ServiceNow instance using connectors. You can configure connectors to import assets from ServiceNow and to export assets and vulnerabilities into ServiceNow.

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 Asset Importer
- ServiceNow Export Connector
- ServiceNow Ticket System

Configure ServiceNow Asset Import Connector

To configure the ServiceNow asset import connector, 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) that will be imported to ServiceNow. After the smart rule is created, the data in the rule will be 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 Import Connector

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 may 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.*

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

1. Select **Configuration > General > Connectors**.
2. In the **Connectors** pane, click **+**.
3. Select **ServiceNow Asset Importer**.
4. Enter a connector name. The connector name can be any name.
5. 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.
6. Enter the ServiceNow URL.
7. Enter the information for the ServiceNow tables that you want to import to BeyondInsight. The default values are IP address and FQDN.
8. Leave the **Active** box checked. Asset data is only imported from ServiceNow when the check box is selected.
9. Set the scheduling options to synchronize ServiceNow with the BeyondInsight database.
10. Click **Test** to ensure the connection to the ServiceNow instance is working.
11. Click **Update** to save the settings.

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 the **Asset Selection** criteria, **ServiceNow Assets**, as shown:

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 the check box is checked.

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

To configure a ServiceNow export connector, you must do the following:

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

Create ServiceNow Export Connector

1. Select **Configuration > General > Connectors**.
2. In the **Connectors** pane, click **+**.
3. Select **ServiceNow Export Connector**.
4. Enter a connector name, and a ServiceNow username and password.
    - The connector name can be any name.
    - The credentials for the ServiceNow system must provide access to the web service and be able to create requests.
5. If you are using an older version of ServiceNow and you are using update sets, check the **Using Update Set** box.
6. Leave the **Active** box checked. Data is only exported when the check box is selected.
7. Check **Export Assets** or **Export Vulnerabilities**, or both.
8. For the export options, enter the following information:
    - **Web Service URL:** Enter the URL to the ServiceNow instance.
    - **Extended Field Mappings:** Enter the field mappings according to which export options you selected. Available fields and suggested field mappings are detailed in sections below.
9. Click **Test** to ensure the connection to the ServiceNow instance is working.
10. Click **Update** to save the settings.

Field Mappings for Exporting Assets Only

- **AssetID** must be mapped to a ServiceNow field
- Mapping the BeyondInsight **VulnerabilityID** field on the asset web service configuration will result in an asset record being created in ServiceNow for each vulnerability that it is associated with that asset.
- The ServiceNow field **name** must be mapped if assets are being exported.

BeyondInsight Asset Fields Available for Export

- AssetID
- AssetName
- AssetRisk
- DateAdded
- DnsName
- IpAddress
- OperatingSystem

- SmartGroupName
- VulnerabilityID
- Workgroup

Suggested Field Mappings

ServiceNow Field	Data Type	Asset Field	Literal Value
correlation_id or custom correlation_id field	String	AssetID	
correlation_display or custom correlation_display field	String	(Literal Value)	BeyondInsight Asset
name	String	AssetName	
ip_address	String	IpAddress	
Os	String	OperatingSystem	
Map other fields as determined by user requirements.			

Field Mappings for Exporting Vulnerabilities Only

- Only vulnerabilities in the selected audit group will be exported.
- All vulnerabilities for all assets will be exported if no audit group is selected.
- The ServiceNow **field correlation_id** must be mapped if vulnerabilities are being exported.

BeyondInsight Vulnerability Fields Available for Export

- AssetID
- Category
- CCEIds
- CVEIds
- FirstOccurred
- LastOccurred
- Severity
- VulnerabilityID
- VulnerabilityName
- VulnerabilityDescription

Suggested Field Mappings

ServiceNow Field	Data Type	Vulnerability Field	Literal Value
correlation_id or custom correlation_id field	String	VulnerabilityID	
correlation_display or custom correlation_display field	String	(Literal Value)	BeyondInsight Vulnerability
short_description	String	VulnerabilityName	
Work_notes	String	VulnerabilityDescription	
Impact	String	Severity	
Map other fields as determined by user requirements.			

Field Mappings for Exporting Both Assets and Vulnerabilities

The following connector configuration will export data once for each smart rule for each asset, and will export the list of vulnerabilities one by one for each asset. The **VulnerabilityID** must ***not*** be present on the asset portion of the connector.

Suggested Field Mappings for Assets

ServiceNow Field	Data Type	Asset Field	Literal Value
correlation_id or custom correlation_id field	String	AssetID	
correlation_display or custom correlation_display field	String	(Literal Value)	BeyondInsight Asset
name	String	AssetName	
ip_address	String	IpAddress	
Os	String	OperatingSystem	
Map other fields as determined by user requirements.			

Suggested Field Mappings for Vulnerabilities

ServiceNow Field	Data Type	Vulnerability Field	Literal Value
correlation_id or custom correlation_id field	String	AssetID	
correlation_display or custom correlation_display field	String	(Literal Value)	BeyondInsight Vulnerability
short_description	String	VulnerabilityName	
Work_notes	String	VulnerabilityDescription	
Impact	String	Severity	
Determined by user	String	VulnerabilityID	
Map other fields as determined by user requirements.			

Create a Smart Group

Assets and vulnerabilities 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.*

1. Configure the smart group as usual.
2. In the **Perform Actions** area, select **Export Data**.

3. Select the name of the connector.
4. Select an audit group from the list. Only vulnerabilities in the selected audit group will be exported. All vulnerabilities for all assets will be exported if no audit group is selected.
5. Enter the expiration period in days, and then click **Save**.

Note: *Assets and vulnerabilities (depending on what is defined in the collector details) are only exported once in the defined expiration period. However, an asset or vulnerability 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 creating smart groups and rules, please see the *BeyondInsight User Guide* at https://www.beyondtrust.com/docs/password-safe/beyondinsight.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 **refere nceTime** 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>
```

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 to your ServiceNow instance is located in the following installation directory:

%\Program Files(x86)\eEye Digital Security\Retina CS\ServiceNow

For more information on transferring update sets in ServiceNow, please visit ServiceNow's website at http://wiki.servicenow.com/index.php?title=Transferring_Update_Sets .

Configure ServiceNow with Password Safe Ticket System

The user configuring the ServiceNow and Password Safe integration needs the **passwordsafe_ticket_system** role. The unique name for this role is **x_bets_bi_integrat.passwordsafe_ticket_system**.

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

- 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.*

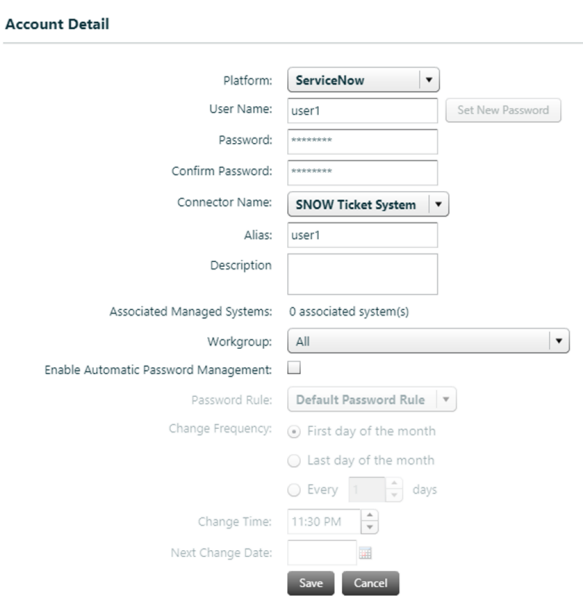
Create ServiceNow Ticket System Connector

1. Select **Configuration > General > Connectors**.
2. In the **Connectors** pane, click **+**.
3. Select **ServiceNow Ticket System**.
4. Enter the following details for your ServiceNow system:
    - **Ticket System Name:** Enter a name for the ticket system.
    - **Instance URL:** Provide the URL for the ServiceNow environment.
    - **Username & 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.
    - **Enable State Validation:** (optional) Check this option if you want tickets with a certain status available to Password Safe. You then must select the table name and status types that you want to whitelist. Depending on your requirements, you might want only active tickets available to Requestors accessing the ticket system through an RDP session. For example, you can check **Active** on the **State List** to add the table name to the **Valid State Mappings** table.
    - **Table Name:** Enter the name of a ticket table in the ServiceNow system, and then click **Search**. If the table name is valid and exists in ServiceNow, the **State List** is populated.
    - **State List:** Select a state, and then click **Add**. The **Valid State Mappings** table displays the ServiceNow table name and the status fields that you selected.
5. Click **Test** to ensure connectivity to your ServiceNow server is successful.
6. Click **Update**.

Create a Functional Account in Password Safe

1. In the console, click **Configuration**.
2. Under **Privileged Access Management**, click **Password Safe**.
3. In the **System Configuration** pane, click **Functional & Login Accounts**.
4. In the **Account Alias** pane, click **+ (Add New Account)**.

5. Enter the username and credentials for ServiceNow. The credentials are the same credentials used when entering ticket details in ServiceNow.
6. Select **SNow Ticket System** from the **Connector Name** list.
7. Click **Save**.



Create a ServiceNow Ticket System in Password Safe

1. In the console, click **Configuration**.
2. Under **Privileged Access Management**, click **Password Safe**.
3. In the **System Configuration** pane, click **Ticket Systems**.
4. In the **Ticket Systems** pane, click **+ (Create New Ticket System)**.
5. Select **ServiceNow Ticket System** from the **Platform** list.
6. Select the functional account.
7. Check the boxes for the remaining options.
8. Click **Update**.