BeyondTrust

Privileged Remote Access
ServiceNow Integration

TC:3/4/2024

Table of Contents

BeyondTrust PRA Integration with ServiceNow

IMPORTANT!

You must purchase this integration separately from your BeyondTrust Privileged Remote Access solution. For more information, contact BeyondTrust's Sales team.

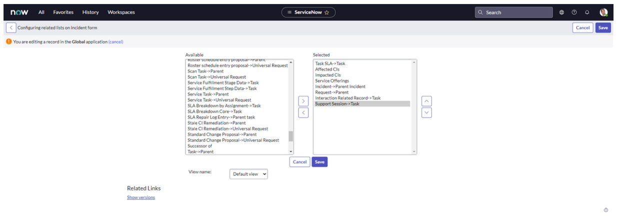
Organizations using ServiceNow can integrate with BeyondTrust PRA to provide secure privileged access to critical assets from within ServiceNow, satisfy internal and external compliance requirements with comprehensive audit trails, and integrate with change management processes.

- **Outbound Access Sessions**: Technicians can launch BeyondTrust access sessions from within ServiceNow incidents using BeyondTrust Jump Technology.
- **Session Updates:** BeyondTrust access session data is written back to ServiceNow incidents, change requests, and configuration items. This includes file transfers, system information, session notes, and session recordings.
- **Change Management Endpoint Approval:** BeyondTrust PRA can be configured to request approval from ServiceNow before a device is accessed via the BeyondTrust PRA access console.

ServiceNow Application Scope

ServiceNow supports integrations that are developed in a *global scope* and integrations that are developed in an *application scope*. This documentation covers an integration that was developed in our BeyondTrust PRA application scope.

For this integration, administrators are prompted when configuring items that live in the global scope. For example, when configuring the Form Layout of an Incident, the user is prompted with an option to **Edit this Section in Global**. The recommendation for this integration is to edit the section in the global scope, which allows the user to edit the form or record without having to switch out of our BeyondTrust application scope.


now
All
Favorites
History
Workspaces
ServiceNow
Search
Cancel
Save
Available
Roster schedule entry proposal->Parent
Roster schedule entry proposal->Universal Request
Scan Task->Parent
Scan Task->Universal Request
Service Fulfillment Stage Data->Task
Service Fulfillment Step Data->Task
Service Task->Parent
Service Task->Universal Request
SLA Breakdown by Assignment->Task
SLA Breakdown Core->Task
SLA Repair Log Entry->Parent task
Stale CI Remediation->Parent
Stale CI Remediation->Universal Request
Standard Change Proposal->Parent
Standard Change Proposal->Universal Request
Successor of
Task->Parent
Selected
Task SLA->Task
Affected CIs
Impacted CIs
Service Offerings
Incident->Parent Incident
Request->Parent
Interaction Related Record->Task
Support Session->Task
Cancel
Save
Related Links
Show versions

Configuring related lists on Incident form

You are editing a record in the **Global** application (cancel)

View name: Default view

The ServiceNow application is available at the ServiceNow Store at https://store.servicenow.com/sn_appstore_store.do#!/store/application/03b39cd74fdb7100237ca5017310c7d0/.

Requirements for the ServiceNow Integration with BeyondTrust PRA

Outlined below are requirements for the BeyondTrust PRA and ServiceNow integration. If any of the integration requirements are not yet met, they must be in place prior to starting the integration setup process unless the associated features of the integration are not required.

Review Base Integration Requirements

Base requirements are a current version of a ServiceNow release with a working Service Desk application, and a current BeyondTrust Appliance B Series (physical or virtual) with at least one usable access console.

To configure network firewall rules for this integration, do the following:

- Allow TCP 443 traffic from the B Series Appliance to the appropriate ServiceNow instance.
- Allow TCP 443 traffic from the appropriate ServiceNow instance to the B Series Appliance.
- Optionally, use ServiceNow MID Servers for this integration.

> *For more information on MID Servers, please see ServiceNow MID Server at https://docs.servicenow.com/bundle/utah-servicenow-platform/page/product/mid-server/concept/mid-server-landing.html.*

Review Additional Integration Requirements

The PRA version of BeyondTrust's ServiceNow integration has additional features which require that certain ServiceNow functions be operational in order to work correctly. If these functions are not set up or actively used, the integration can still be installed and the basic features work, but the enterprise features are not usable until the necessary ServiceNow functionality has been implemented. This can be done after the initial installation of the integration update set(s). The additional features should immediately be usable, assuming the appropriate setup steps are taken during the integration setup as described in this guide.

To successfully integrate theBeyondTrust services with ServiceNow, the following requirements must also be met and reviewed:

- A working ServiceNow configuration management database (CMDB)
- One or more ServiceNow configuration items on which BeyondTrust Jump Client services can be or have been installed

The CMDB is used to launch BeyondTrust sessions based on the hostname of the machine added to the configuration item field of an incident. If the CMDB is not populated with any available hosts, BeyondTrust Jump cannot be used to remotely access them through ServiceNow's interface. These hosts can be added after the initial setup without making any changes to the integration.

BeyondTrust's supported operating systems include all of the major modern versions of Microsoft, Apple, and Linux. One or more computers running one of these operating systems needs to be populated in ServiceNow's CMDB in order for BeyondTrust's Jump features to work through ServiceNow. As mentioned above, this can be done after initial installation of the integration.

Test the Firewall

It is important to test all requirements of the integration prior to beginning setup. Most of these can be tested by the BeyondTrust and ServiceNow administrators within their respective systems, but to test the network firewall, the BeyondTrust admin should take the following steps to confirm that the necessary rules are in place.

1. Log into a machine either external to the B Series Appliance's network or in the same VPN as the ServiceNow instance, depending on how ServiceNow is connecting to the B Series Appliance's network.
2. Log into the B Series Appliance's **/appliance** interface.
3. Browse to **Support > Utilities :: TCP Connection Test**.
4. Enter the hostname of the ServiceNow instance, enter the port number of **443**, and then click **Test**. A successful result is a *Connected* status message.

> ***Note:*** *Do not enter the protocol when entering the ServiceNow instance, for example* ***https://servicenow.example.com/****. Instead, use the fully qualified domain name only, for example* ***servicenow.example.com****. In most environments, the BeyondTrust Appliance B Series resides in a DMZ network and has a public DNS address which ServiceNow contacts over the public internet. In some environments, BeyondTrust is not publicly accessible. In these cases, contact ServiceNow about implementing a VPN connection to your internal network for ServiceNow. For more information, please see Virtual Private Network (VPN) at https://docs.servicenow.com/bundle/utah-platform-security/page/administer/encryption/concept/c_SetUpAVPN4SNowBusNet.html.*

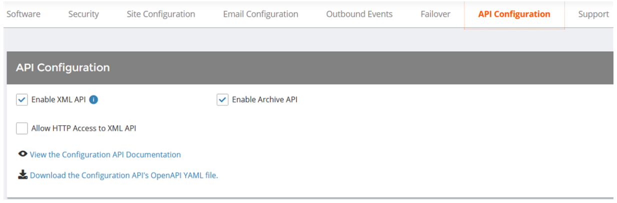
Configure BeyondTrust PRA for the ServiceNow Integration

All the steps in this section take place in the BeyondTrust **/login** administrative interface. Access your BeyondTrust interface by going to the hostname of your B Series Appliance followed by **/login** (e.g., https://support.example.com/login).

Verify the API is Enabled

The BeyondTrust integration requires the BeyondTrust XML API to be enabled. This feature is used from within the integrating software to communicate with the BeyondTrust APIs.

In **/login**, navigate to **Management > API Configuration** and verify that **Enable XML API** is checked.



API Configuration

☑ Enable XML API ☑ Enable Archive API

□ Allow HTTP Access to XML API

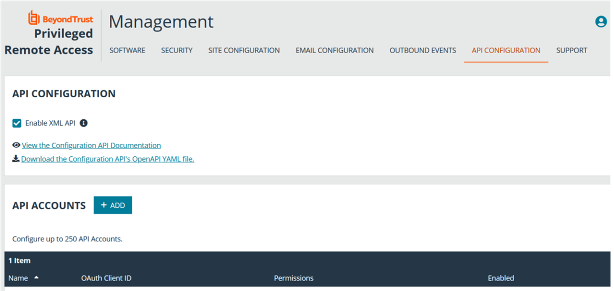
View the Configuration API Documentation

Download the Configuration API's OpenAPI YAML file.

Create an OAuth API Account

The ServiceNow API account is used from within ServiceNow to make Remote Support Command API calls to Remote Support.

1. In **/login**, navigate to **Management > API Configuration**.
2. Click **Add**.



API CONFIGURATION

☑ Enable XML API

View the Configuration API Documentation

Download the Configuration API's OpenAPI YAML file.

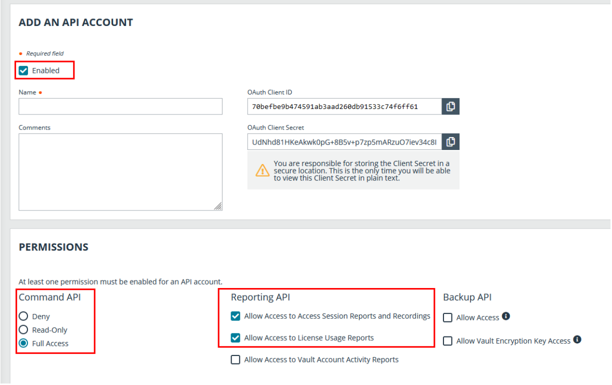
API ACCOUNTS + ADD

Configure up to 250 API Accounts.

1 Item

Name	OAuth Client ID	Permissions	Enabled

3. Check **Enabled**.
4. Enter a name for the account.
5. **OAuth Client ID** and **OAuth Client Secret** is used during the OAuth configuration step in ServiceNow.
6. Under **Permissions**, check the following:
   - Command API: **Full Access**.
   - Reporting API: **Allow Access to Access Session Reports and Recordings**, and **Allow Access to License Usage Reportsee**.
7. Click **Save** at the top of the page to create the account.



ADD AN API ACCOUNT

• *Required field*

☑ Enabled

Name •

Comments

OAuth Client ID: 70befbe9b474591ab3aad260db91533c74f6ff61

OAuth Client Secret: UdNhd81HKeAkwk0pG+8B5v+p7zp5mARzuO7iev34c8I

You are responsible for storing the Client Secret in a secure location. This is the only time you will be able to view this Client Secret in plain text.

PERMISSIONS

At least one permission must be enabled for an API account.

Command API
○ Deny
○ Read-Only
● Full Access

Reporting API
☑ Allow Access to Access Session Reports and Recordings
☑ Allow Access to License Usage Reports
□ Allow Access to Vault Account Activity Reports

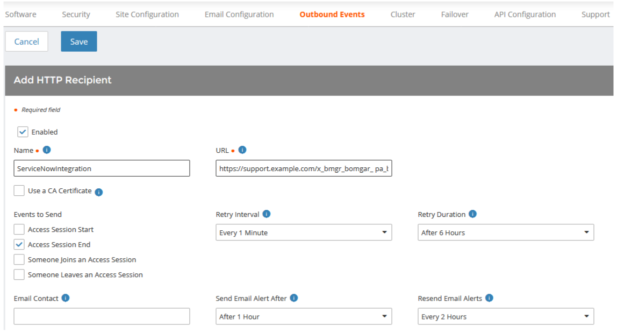
Backup API
□ Allow Access
□ Allow Vault Encryption Key Access

SALES: www.beyondtrust.com/contact SUPPORT: www.beyondtrust.com/support DOCUMENTATION: www.beyondtrust.com/docs 7
©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority. TC: 3/4/2024

Add Outbound Events

Outbound events are used to notify ServiceNow that a BeyondTrust Session has finished and is ready to be imported into ServiceNow.

1. In **/login**, navigate to **Management > Outbound Events**.
2. Click **Add**.
3. Provide a name of *ServiceNow Integration* or something similar, depending on your ServiceNow instance.
4. Set the URL to *https://example.service-now.com/api/x_bmgr_bomgar_pam/outbound_event/session_end*, where *example.service-now.com* is the ServiceNow instance name.
5. If using an outbound event token for added security, append *outbound_event_token=YOUR-TOKEN* to the end of the URL, so that the entire URL resembles *https://example.service-now.com/api/x_bmgr_bomgar_pam/outbound_event/session_end?outbound_event_token=YOUR-TOKEN*. You must also store this token with the appliance configuration record in ServiceNow.
6. For **Events to Send**, check **Access Session End**.
7. Click **Save**.



Add HTTP Recipient

• Required field

☑ Enabled

Name • : ServiceNowIntegration

URL • : https://support.example.com/x_bmgr_bomgar_ pa_l

☐ Use a CA Certificate

Events to Send

☐ Access Session Start
☑ Access Session End
☐ Someone Joins an Access Session
☐ Someone Leaves an Access Session

Retry Interval: Every 1 Minute

Retry Duration: After 6 Hours

Email Contact:

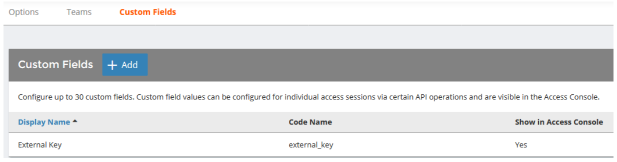
Send Email Alert After: After 1 Hour

Resend Email Alerts: Every 2 Hours

Create Custom Fields

BeyondTrust custom fields are used to map ServiceNow Tasks (incidents, change requests, problem records, and service catalog requests) and Configuration Items to BeyondTrust access sessions.

1. In **/login**, navigate to **Configuration > Custom Fields**.
2. Click **Add**.
3. Enter the following values:
   - **Display Name:** ServiceNow Task ID
   - **Code Name:** snow_task_id
4. Check the **Show in Access Console** option.
5. Click **Save** to save the new field.
6. Repeat the steps above for the following custom field values:
   - **Display Name:** ServiceNow Configuration Item ID
   - **Code Name:** snow_cmdb_ci_id
   - **Show in Access Console:** checked



Custom Fields

Configure up to 30 custom fields. Custom field values can be configured for individual access sessions via certain API operations and are visible in the Access Console.

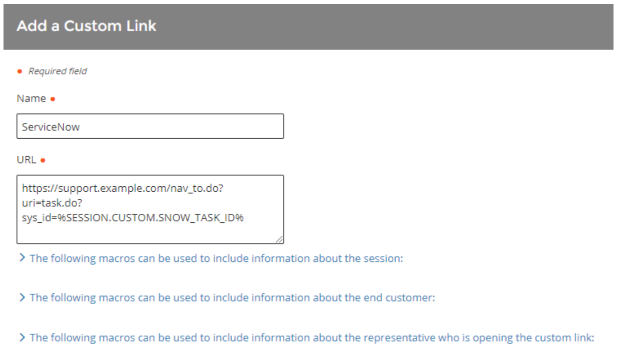
Display Name ▲	Code Name	Show in Access Console
External Key	external_key	Yes

Set Up the Custom Link

BeyondTrust custom links can be configured to allow users to quickly access the ServiceNow incident that is associated with the session.

1. In **/login**, navigate to **Access Console > Custom Links**.
2. Click **Add**.

3. Enter a name for the link, and then set the URL to *https://example.service-now.com/nav_to.do?uri=task.do?sys_id=%SESSION.CUSTOM.SNOW_TASK_ID%* where *https://example.service-now.com* is the ServiceNow instance name. If needed, you can use any of the available macros to customize the link according to your specifications.
4. Click **Save** to save the new link.



Add a Custom Link

• *Required field*

Name •

ServiceNow

URL •

https://support.example.com/nav_to.do?uri=task.do?sys_id=%SESSION.CUSTOM.SNOW_TASK_ID%

› The following macros can be used to include information about the session:

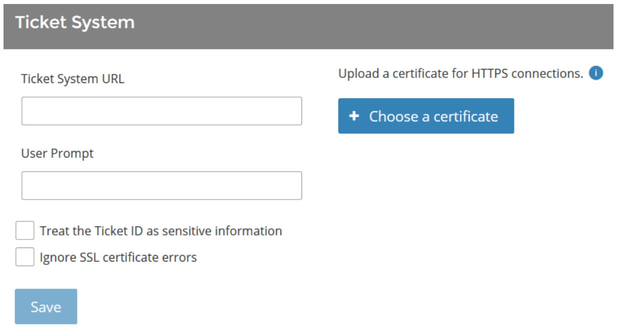
› The following macros can be used to include information about the end customer:

› The following macros can be used to include information about the representative who is opening the custom link:

Set Up Change Management Workflow

BeyondTrust change management workflow can be configured to require approval through an ITSM system before allowing access to BeyondTrust Jump Clients.

1. In **/login**, navigate to **Jump > Jump Policies**.
2. Under **Ticket System**, enter an appropriate **Ticket System URL** similar to *https://example.service-now.com/api/x_bmgr_bomgar_pam/endpoint_approval*.
3. Upload the CA certificate from the ServiceNow instance.
4. Enter the desired **User Prompt**. For example, with a change request workflow, enter **ServiceNow ChangeID Required**.
5. Click **Save**.



Ticket System

Ticket System URL

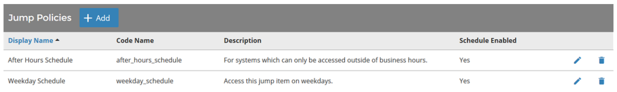
Upload a certificate for HTTPS connections.

User Prompt

□ Treat the Ticket ID as sensitive information

□ Ignore SSL certificate errors

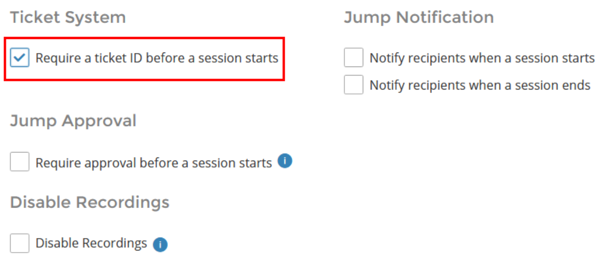
6. Next, under the **Jump Policies** section, click **Add**, or click **Edit** next to an existing Jump Policy.



Jump Policies + Add

Display Name ▴	Code Name	Description	Schedule Enabled
After Hours Schedule	after_hours_schedule	For systems which can only be accessed outside of business hours.	Yes
Weekday Schedule	weekday_schedule	Access this jump item on weekdays.	Yes

7. Under **Ticket System**, check **Require a ticket ID before a session starts**.



Ticket System

☑ Require a ticket ID before a session starts

Jump Notification

□ Notify recipients when a session starts

□ Notify recipients when a session ends

Jump Approval

□ Require approval before a session starts

Disable Recordings

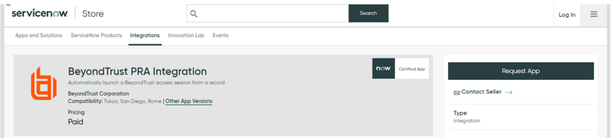
□ Disable Recordings

Configure ServiceNow for Integration with BeyondTrust PRA

Unless otherwise noted, all of the steps in this section take place in the ServiceNow interface. The development and/or test instances of ServiceNow should be used initially so that the integration can be thoroughly tested before installation in the production instance.

Install BeyondTrust Integration

The Integration must be purchased directly from BeyondTrust. After the purchase, it is installed via the ServiceNow Store. There is no mechanism to purchase the integration at the ServiceNow Store. Follow the steps below to request and install the integration.



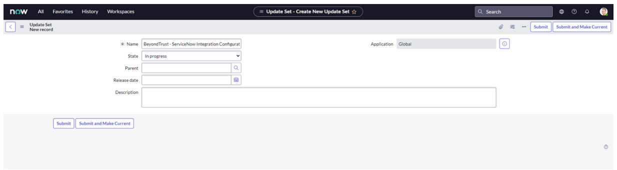
BeyondTrust PRA Integration
Automatically launch a BeyondTrust access session from a record
BeyondTrust Corporation
Compatibility: Tokyo, San Diego, Rome | Other App Versions
Pricing
Paid
Type
Integration

1. Log in to your ServiceNow platform with your corporate account. Please contact your company Now Support (HI) admin if you do not have credentials.
2. Search for BeyondTrust PRA Integration, or go to the app's page at https://store.servicenow.com/sn_appstore_store.do#!/store/application/03b39cd74fdb7100237ca5017310c7d0.
3. Click **Request App**.
4. Request Privileged Remote Access with ITSM.
5. Within a business day, BeyondTrust approves the request with a $0 purchase price, and sends a copy of these installation instructions to the requester.
6. Once you receive the confirmation, return to the app's page in the ServiceNow store.
7. Click **Complete Purchase**.
8. Review the contract details.
9. If you agree, check **Accept the Site Terms of Use**.
10. Click **Complete Purchase**.
11. The app is ready for installation on your ServiceNow instance(s).
12. Repeat the steps below for each instance.
13. Login to the ServiceNow instance on which you want to install the app.
14. Navigate to **System Applications > All Available Applications > All**.
15. Search for the app you want to install.
16. Click **Install**.

For more information on installing applications, please see ServiceNow's Help Page at https://store.servicenow.com/sn_appstore_store.do#!/store/helpcenter.

Create Local Update Set

Local update sets are used in ServiceNow to capture configuration changes. They can be used to quickly transfer these configuration changes to other environments.



* Name: BeyondTrust - ServiceNow Integration Configurat
State: In progress
Parent:
Release date:
Description:
Application: Global

1. Select **System Update Sets > Local Update Sets**, and click the **New** button above the list of update sets to create a new local

update set.

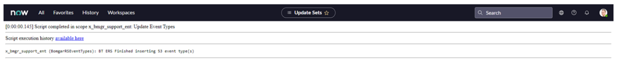
2. In the **Name** field, enter *BeyondTrust - ServiceNow Integration Configuration* (or an equivalent).
3. Click **Submit and Make Current**. This update set captures any changes you make during the configuration process. Make sure that the **BeyondTrust - ServiceNow Integration Configuration** update set is selected in ServiceNow's update set dropdown for the following steps.
4. Make sure the **Application** is set to **BeyondTrust PRA Integration**. If it is not, use the settings cog in the upper right of the screen to switch to the aforementioned scope.
5. After configuration is complete and tested, the local update set can be imported or promoted to new instances of ServiceNow (e.g., the production instance) to quickly replicate the integration. This must be done after transferring the BeyondTrust - ServiceNow retrieved update set.

> *For more information on transferring update sets, please see "Transfer the BeyondTrust PRA-ServiceNow Integration Update Sets" on page 19.*

Update BeyondTrust PRA Session Event Types

Event types are used to control which BeyondTrust events are processed with a BeyondTrust session import. This step updates the database with all the available event types.

1. Select **BeyondTrust PRA > Update Event Types**.
2. This loads all the available BeyondTrust session event types into the database, so that unwanted events can be filtered out in a subsequent step when setting up your B Series Appliances.



[0:00:00.145] Script completed in scope x_bmgr_support_ent: Update Event Types

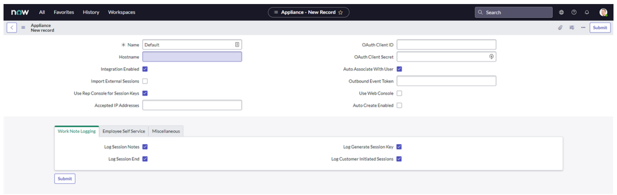
Script execution history available here

```
x_bmgr_support_ent (BomgarRSEventTypes): BT ERS Finished inserting 53 event type(s)
```

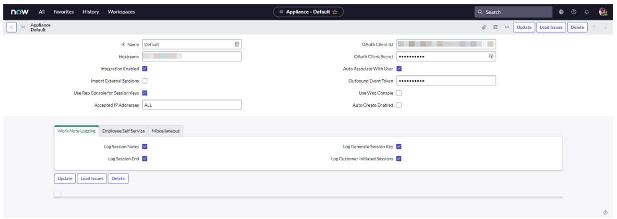
Set Up B Series Appliance

B Series Appliances are set up in ServiceNow to connect ServiceNow with a B Series Appliance.

1. Select **BeyondTrust PRA > Appliances**.
2. Click **New** to add a new BeyondTrust Appliance B Series and enter the following values:



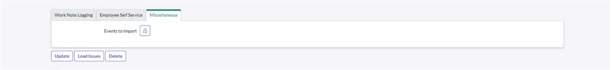
* Name	Default	OAuth Client ID	
Hostname		OAuth Client Secret	
Integration Enabled	☑	Auto Associate With User	☑
Import External Sessions	☐	Outbound Event Token	
Use Rep Console for Session Keys	☑	Use Web Console	☐
Accepted IP Addresses		Auto Create Enabled	☐
Log Session Notes	☑	Log Generate Session Key	☑
Log Session End	☑	Log Customer Initiated Sessions	☑



* Name	Default	OAuth Client ID	[redacted]
Hostname	[redacted]	OAuth Client Secret	••••••••••
Integration Enabled	☑	Auto Associate With User	☑
Import External Sessions	☐	Outbound Event Token	••••••••••
Use Rep Console for Session Keys	☑	Use Web Console	☐
Accepted IP Addresses	ALL	Auto Create Enabled	☐
Log Session Notes	☑	Log Generate Session Key	☑
Log Session End	☑	Log Customer Initiated Sessions	☑

- **Name:** Must be **Default**.
- **Hostname:** Hostname of the BeyondTrust Appliance B Series.
- **OAuth Client ID/ OAuth Client Secret:** the OAuth client id and Client Secret that are used to authenticate to B Series Appliance. This is obtained in a previous step, Create a ServiceNow OAuth API Account.
- **Outbound Event Token:** The token that is used as an added security measure to confirm outbound events are coming from the B Series Appliance that is sending the same token. If left blank, this outbound event token process is ignored. However, if a value is provided, the same value must be sent from all outbound events coming from BeyondTrust as a parameter named **outbound_event_token**.
- **Integration Enabled:** Turns the integration on and off.

- **Import External Sessions:** If checked, session reports for sessions that are started external to ServiceNow are imported into ServiceNow.
- **Accepted IP Addresses:** A comma-separated list of IP addresses from which this integration accepts outbound events.
- **Auto Associate With User:** If checked, when the session report is imported, the integration attempts to associate a ServiceNow user with the session. The lookup is based on the session's primary user's username.
- **Auto Associate With Config Item:** If checked, when the session report is imported, the integration attempts to associate a ServiceNow config item with the session.
- **Events to Import:** A list of BeyondTrust session events to process when importing a BeyondTrust session.



> ***Note:*** *You cannot configure this setting until after the B Series Appliance has been saved.*

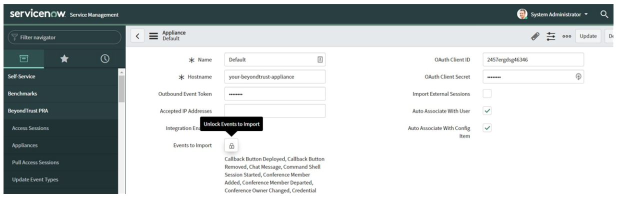
Configure Events to Import

Event types are used to control which BeyondTrust events are processed with a BeyondTrust session import. This step defines which events are processed for each BeyondTrust session import.

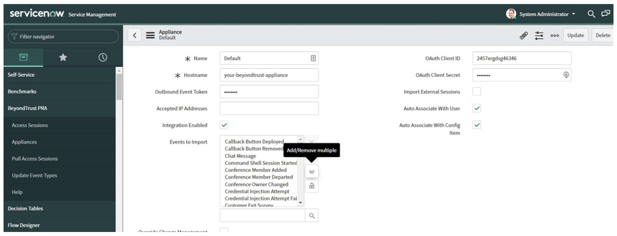
1. Select **BeyondTrust PRA > Appliances**.
2. Click the name of your B Series Appliance.
3. Click the **Edit Events to Import** button (the lock icon).
4. Click the **Add/Remove multiple** button (the group of people icon) located on the right side of the field.
5. Select the events you want from the **Collection** field on the left and use the arrows to move the events to the **List** field on the right.

> ***Tip:*** *You can use CTRL+A to select all events.*

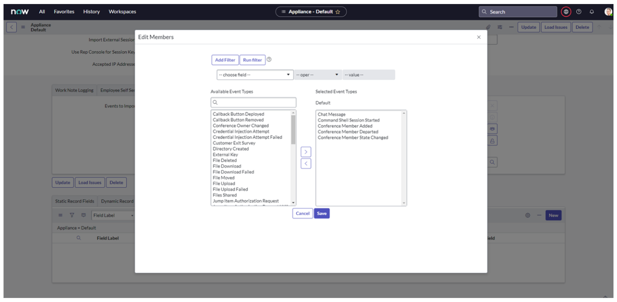
6. Click the **Save** button when you are finished.



Name: Default
Hostname: your-beyondtrust-appliance
Outbound Event Token: ••••••••
Accepted IP Addresses:
Events to Import: Callback Button Deployed, Callback Button Removed, Chat Message, Command Shell Session Started, Conference Member Added, Conference Member Departed, Conference Owner Changed, Credential
OAuth Client ID: 2457ergdsg46346
OAuth Client Secret: ••••••••
Import External Sessions ☐
Auto Associate With User ☑
Auto Associate With Config Item ☑



Name: Default
Hostname: your-beyondtrust-appliance
Outbound Event Token: ••••••••
Accepted IP Addresses:
Integration Enabled ☑
Events to Import:
Callback Button Deployed
Callback Button Removed
Chat Message
Command Shell Session Started
Conference Member Added
Conference Member Departed
Conference Owner Changed
Credential Injection Attempt
Credential Injection Attempt Fai
Customer Exit Survey
OAuth Client ID: 2457ergdsg46346
OAuth Client Secret: ••••••••
Import External Sessions ☐
Auto Associate With User ☑
Auto Associate With Config Item ☑

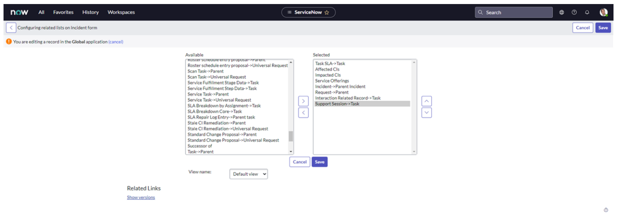


Available Event Types:
Callback Button Deployed
Callback Button Removed
Conference Owner Changed
Credential Injection Attempt
Credential Injection Attempt Failed
Customer Exit Survey
Directory Created
External Key
File Deleted
File Download
File Download Failed
File Moved
File Upload
File Upload Failed
Files Shared
Jump Item Authorization Request

Selected Event Types
Default
Chat Message
Command Shell Session Started
Conference Member Added
Conference Member Departed
Conference Member State Changed

Configure BeyondTrust Session Related Lists

Related lists are used to provide a list of BeyondTrust sessions that are associated with a task (incident, change request, service catalog, etc.) or configuration item.



Configuring related lists on Incident form

You are editing a record in the **Global** application (cancel)

Available:

- Roster schedule entry proposal->Parent
- Roster schedule entry proposal->Universal Request
- Scan Task->Parent
- Scan Task->Universal Request
- Service Fulfillment Stage Data->Task
- Service Fulfillment Step Data->Task
- Service Task->Parent
- Service Task->Universal Request
- SLA Breakdown by Assignment->Task
- SLA Breakdown Core->Task
- SLA Repair Log Entry->Parent task
- Stale CI Remediation->Parent
- Stale CI Remediation->Universal Request
- Standard Change Proposal->Parent
- Standard Change Proposal->Universal Request
- Successor of
- Task->Parent

Selected:

- Task SLA->Task
- Affected CIs
- Impacted CIs
- Service Offerings
- Incident->Parent Incident
- Request->Parent
- Interaction Related Record->Task
- Support Session->Task

View name: Default view

Task Configuration

1. Select **Incident** or the desired task type.
2. Click **Open** to see a list of open tasks.
3. Select an incident by clicking the **Task Number**.
4. Right-click the title bar and select **Configure > Related Lists**.
5. Ensure that **Access Session > Task** has been moved to the **Selected** column.
6. Click the **Save** button.
7. The BeyondTrust sessions list appears towards the bottom of the form once these steps are complete.

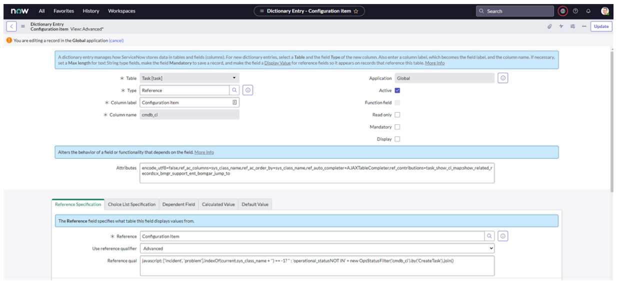
CMDB Configuration

1. Select **Configuration > Servers**.
2. Click **All** to see a list of servers.
3. Select a server by clicking the **Name** of a server.
4. Right-click the Incident title bar and select **Configure > Related Lists**.
5. Ensure that **Access Session > Configuration Item** has been moved to the **Selected** column.
6. Click the **Save** button.
7. The BeyondTrust sessions list appears towards the bottom of the configuration item form once these steps are complete.

Configure Incident CMDB Jump Macros

BeyondTrust Jump technology can be used for unattended access to devices through the B Series Appliance.

1. Select **Incident** or the desired task type.
2. Click **Open** to see a list of open tasks.
3. Select an incident by clicking the **Incident Number**.
4. Populate the **Configuration Item** field by clicking the magnifying glass icon, and then selecting an item in the list.
5. Once the Configuration Item is populated, click the **Update** button on the title bar. This takes you back to the list.
6. Click the name of the task you just updated.
7. Right-click the **Configuration Item Label**, and then click **Configure Dictionary**.
8. Locate the **Attributes** field and take note of the part of the value that reads **ref_contributions=task_show_ci_map;show_related_records**.



Dictionary Entry
Configuration item View: Advanced*

You are editing a record in the **Global** application (cancel)

A dictionary entry manages how ServiceNow stores data in tables and fields (columns). For new dictionary entries, select a **Table** and the field **Type** of the new column. Also enter a column label, which becomes the field label, and the column name. If necessary, set a **Max length** for text String type fields, make the field **Mandatory** to save a record, and make the field a Display Value for reference fields so it appears on records that reference this table. More Info

* Table	Task [task]	Application	Global
* Type	Reference	Active	☑
* Column label	Configuration item	Function field	□
* Column name	cmdb_ci	Read only	□
		Mandatory	□
		Display	□

Alters the behavior of a field or functionality that depends on the field. More Info

Attributes: encode_utf8=false,ref_ac_columns=sys_class_name,ref_ac_order_by=sys_class_name,ref_auto_completer=AJAXTableCompleter,ref_contributions=task_show_ci_map;show_related_records;x_bmgr_support_ent_bomgar_jump_to

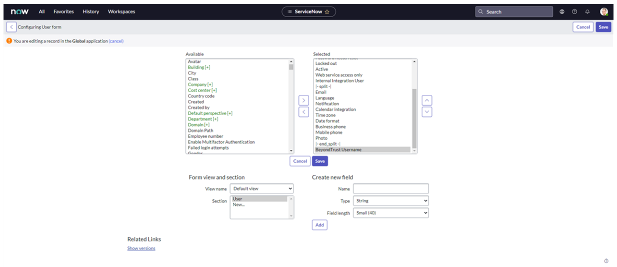
The **Reference** field specifies what table this field displays values from.

* Reference: Configuration Item
Use reference qualifier: Advanced
Reference qual: javascript: ['incident', 'problem'].indexOf(current.sys_class_name + '') == -1 ? '' : 'operational_statusNOT IN' + new OpsStatusFilter('cmdb_ci').by('CreateTask').join()

9. Add the **Jump To** value of **x_bmgr_bomgar_pam_bomgar_pam_jump_to** or **x_bmgr_bomgar_pam_bomgar_pam_jump_to_web** as a semicolon-separated item in **ref_contributions** (e.g., **ref_contributions=x_bmgr_bomgar_pam_bomgar_pam_jump_to;task_show_ci;show_related_records**).
10. Click **Update** to save your changes.

Configure BeyondTrust Username and Authentication

1. Log into your BeyondTrust **/login** interface with the same credentials as a ServiceNow user who is expected to be using Privileged Remote Access.



You are editing a record in the **Global** application (cancel)

View name: Default view

Section: User, New...

Name:

Type: String

Field length: Small (40)

2. Download and install a BeyondTrust access console from the **/login > My Account** tab.

Troubleshoot Login Failure

- Make sure that BeyondTrust and ServiceNow are checking credentials against the same LDAP server(s), if appropriate. Check the LDAP server in the BeyondTrust interface under **/login > Users & Security > Security Providers**.
- If LDAP authentication is not being used, log in to ServiceNow. Select **User Administration > Users**, and then select the user to be used for testing and focus on the **BeyondTrust Username** field.
- If this field does not exist while viewing a user, hover over the icon next to **User** on the title bar, and then select **Configure > Form Layout** and move the **BeyondTrust Username** field from the **Available** list to the **Selected** list. Once done, enter the name of a known-working BeyondTrust user account in this field and save.

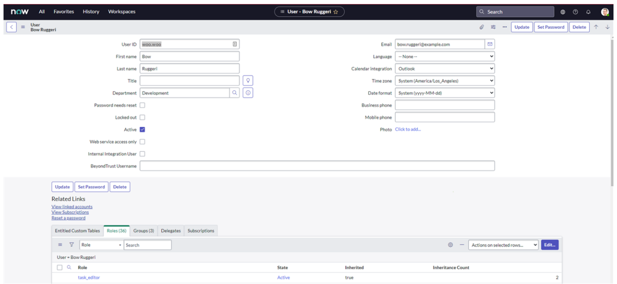
For more information on how to check the LDAP server for ServiceNow, please see LDAP Integration at https://docs.servicenow.com/bundle/utah-platform-security/page/integrate/ldap/concept/c_LDAPIntegration.html.

Assign Users Appropriate Roles

Give the appropriate roles to ITIL users who provide technical support using this integration, those who need to review session information, and those who will manage the app's configuration.

> ***Note:*** *You must elevate the admin's role in order to make the following change.*

1. Select **User Administration > Users**.
2. Select a user.
3. Find the **Roles** tab and click the **Edit** button.

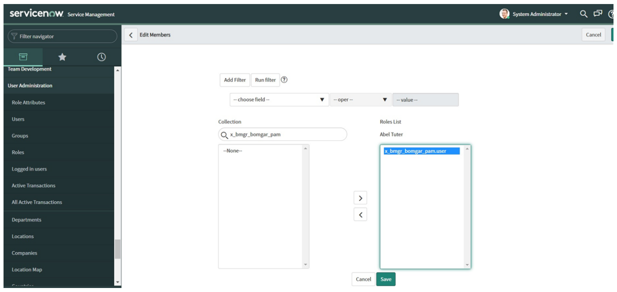


User ID: woo.woo
First name: Bow
Last name: Ruggeri
Title:
Department: Development
Password needs reset ☐
Locked out ☐
Active ☑
Web service access only ☐
Internal Integration User ☐
BeyondTrust Username:
Email: bow.ruggeri@example.com
Language: -- None --
Calendar integration: Outlook
Time zone: System (America/Los_Angeles)
Date format: System (yyyy-MM-dd)
Business phone:
Mobile phone:
Photo: Click to add...

User = Bow Ruggeri

Role	State	Inherited	Inheritance Count
task_editor	Active	true	2

4. Add the appropriate role or roles from the **Collection** list to the **Roles** list. The available roles are:
   - **x_bmgr_bomgar_pam.app_admin**: Users assigned this role can view and manage the application's configuration.
   - **x_bmgr_bomgar_pam.data_viewer**: Users assigned this role can view data created by the application (i.e., Access sessions and their ancillary records).
   - **x_bmgr_bomgar_pam.jump_user**: Users assigned this role can leverage the application's UI actions and macros to initiate a BeyondTrust Privileged Remote Access session to an existing Jump Item either from a ticket with a Configuration Item or directly from the CMDB record.



Collection: x_bmgr_bomgar_pam
--None--

Roles List
Abel Tuter
x_bmgr_bomgar_pam.user

5. Click **Save**.

Deprecated User Role

The existing user role **x_bmgr_bomgar_pam.user** is deprecated and will be removed in a later version. Users with only this role are able to use the application and view data as before, but they are no longer able manage its configuration.

> ***Note:*** *If you can no longer see and edit the app configuration, please assign the user role* ***new x_bmgr_bomgar_pam.app_admin*** *to users who require this access.*

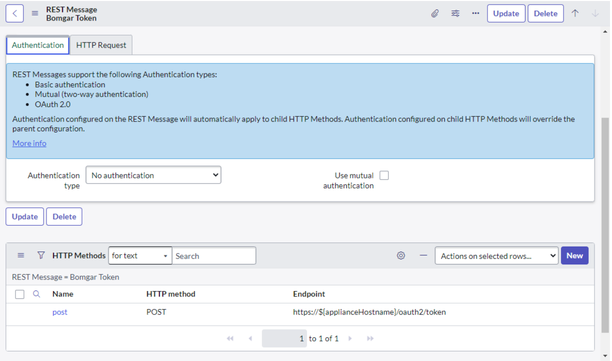
Transition all users to the new roles based on the access they require. There is no hierarchy to these roles. For example, a user with the role **x_bmgr_bomgar_pam.app_admin** can only manage configuration and cannot use the application's Jump To functionality or view session data without being assigned one of the other roles as well.

Use the ServiceNow MID Server Option

It is possible to avoid direct connection between ServiceNow and Privileged Remote Access by using a MID server for internal Privileged Remote Access deployments.

To configure the integration to use a MID server for API requests to a Privileged Remote Access site, specify the MID server to use on the individual outbound REST messages:

1. In ServiceNow, navigate to **System Web Services > Outbound > REST Message**.
2. Filter to show only messages for the BeyondTrust application being configured.
3. Click the **Name** of one of the messages to edit its properties.
4. In the **HTTP Methods** related list at the bottom, select the **Name** of the method (typically **post**).


REST Message
Bomgar Token

REST Messages support the following Authentication types:

- Basic authentication
- Mutual (two-way authentication)
- OAuth 2.0

Authentication configured on the REST Message will automatically apply to child HTTP Methods. Authentication configured on child HTTP Methods will override the parent configuration.

More info

Authentication type: No authentication

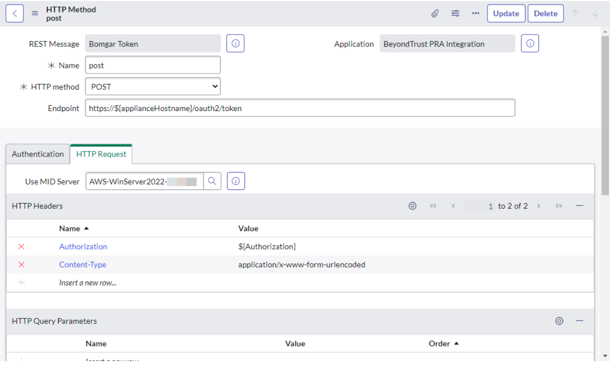
Use mutual authentication: □

REST Message = Bomgar Token

Name	HTTP method	Endpoint
post	POST	https://${applianceHostname}/oauth2/token

1 to 1 of 1

5. On the resulting form, select the **HTTP Request** tab and select your MID server in the **Use MID Server** field.
6. Click **Update** to save the changes.


HTTP Method
post

REST Message: Bomgar Token

Application: BeyondTrust PRA Integration

* Name: post

* HTTP method: POST

Endpoint: https://${applianceHostname}/oauth2/token

Use MID Server: AWS-WinServer2022-[redacted]

HTTP Headers — 1 to 2 of 2

Name ▲	Value
Authorization	${Authorization}
Content-Type	application/x-www-form-urlencoded
Insert a new row...	

HTTP Query Parameters

Name	Value	Order ▲

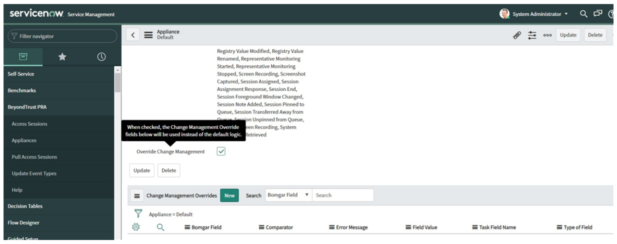
Repeat these steps for each outbound REST message that is a part of the application.

> *For more information on MID Servers, please see ServiceNow MID Server at https://docs.servicenow.com/bundle/utah-servicenow-platform/page/product/mid-server/concept/mid-server-landing.html.*

Set Up Change Management Workflow

BeyondTrust change management workflow works out of the box with a default Servicenow configuration. The configuration can be customized, if necessary.

The **Default Approval Processing** list includes the checks that are made when a ticket approval request is processed in ServiceNow.



Appliance
Default

Registry Value Modified, Registry Value Renamed, Representative Monitoring Started, Representative Monitoring Stopped, Screen Recording, Screenshot Captured, Session Assigned, Session Assignment Response, Session End, Session Foreground Window Changed, Session Note Added, Session Pinned to Queue, Session Transferred Away from Queue, Session Unpinned from Queue, ...een Recording, System ... Retrieved

When checked, the Change Management Override fields below will be used instead of the default logic.

Override Change Management ☑

Appliance = Default

Bomgar Field	Comparator	Error Message	Field Value	Task Field Name	Type of Field

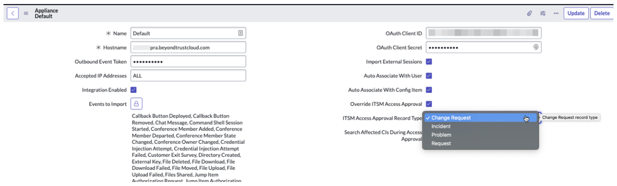
1. **Find the Ticket (aka Task):** Searches for the task based on **task number**. If not found by number, searches by task **sys_id**. If the task is not found, a failure response is sent back to BeyondTrust.
2. **Match the Rep:** Checks to make sure the rep username matches the task **assigned_to** field user's **user_name** (User Id) or BeyondTrust PRA **username** field. If the reps do not match, a failure response is sent back to BeyondTrust.

3. **Match the Computer Name:** Ensures the task's **cmdb_ci** name matches the computer name being Jumped to in BeyondTrust. If the computer names do not match, a failure response is sent back to BeyondTrust.
4. **Ensure Task Approval:** Ensures the task's **approval** field is **approved**. If the task is not approved, a failure response is sent back to BeyondTrust.
5. **Ensure Field State:** Ensures the task's **state** field is not **closed**, **cancelled**, or **resolved** (value is less than 3). If the state is not less than 3, a failure response is sent back to BeyondTrust.

Override Change Management

Change Management Override allows you to change the Change Management Workflow type. For most applications, this should be changed to **Change Request**.

1. Go to the **Appliance** screen and check the **Override Change Management** option.
2. For **ITSM Access Approval Record Type**, select **Change Request**.

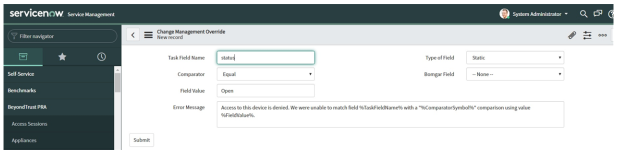


Name: Default
Hostname: [redacted]pra.beyondtrustcloud.com
Outbound Event Token: ••••••••••
Accepted IP Addresses: ALL
Integration Enabled: ☑
Events to Import: Callback Button Deployed, Callback Button Removed, Chat Message, Command Shell Session Started, Conference Member Added, Conference Member Departed, Conference Member State Changed, Conference Owner Changed, Credential Injection Attempt, Credential Injection Attempt Failed, Customer Exit Survey, Directory Created, External Key, File Deleted, File Download, File Download Failed, File Moved, File Upload, File Upload Failed, Files Shared, Jump Item Authorization Request, Jump Item Authorization

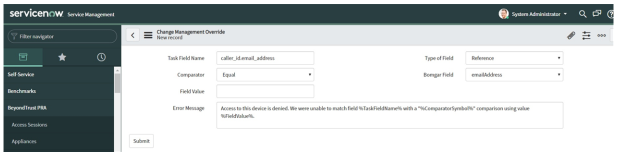
OAuth Client ID: [redacted]
OAuth Client Secret: ••••••••••
Import External Sessions: ☑
Auto Associate With User: ☑
Auto Associate With Config Item: ☑
Override ITSM Access Approval: ☑
ITSM Access Approval Record Type: ✓ Change Request | Incident | Problem | Request
Search Affected CIs During Access Approval

Privileged Remote Access Change Management Override provides an administrator a way to customize the **Approval Process** without the burden of manual coding.

1. Go to the **Appliance** screen and check the **Override Change Management** option.
2. Click on the **New** button next to the **Change Management Overrides Table**.
3. The goal of this record is to compare a **Task** field value with data provided by the B Series Appliance or a value defined by the user. Here is brief description of all the information:



Task Field Name: status
Comparator: Equal
Field Value: Open
Error Message: Access to this device is denied. We were unable to match field %TaskFieldName% with a "%ComparatorSymbol%" comparison using value %FieldValue%.
Type of Field: Static
Bomgar Field: -- None --



Task Field Name: caller_id.email_address
Comparator: Equal
Field Value:
Error Message: Access to this device is denied. We were unable to match field %TaskFieldName% with a "%ComparatorSymbol%" comparison using value %FieldValue%.
Type of Field: Reference
Bomgar Field: emailAddress

- **Task Field Name:** This is the name of the **Field** inside the **ServiceNow Task Table**. A comprehensive list of the important Task table fields can be found at Important Task Table Fields at https://docs.servicenow.com/bundle/utah-application-development/page/administer/task-table/reference/r_ImportantTaskTableFields.html.
- **Comparator:** The kind of evaluation performed. It can be an **Equal**, **Lesser than** or **Greater than** comparison.
- **Type of Field:** If the **Static** option is selected, whatever value entered by the user in the **Field Value** is used. On the other hand, if the **Reference** option is marked, the value selected in the **Bomgar Field** dropdown is selected.
- **Field Value:** A hard-coded value entered by the user.
- **Bomgar Field** : A list of all the information sent by the B Series Appliance that the user can select.
- **Error Message:** In case that the comparison between the **ServiceNow Task Field Value** and the **Field** value, or **Bomgar Field** selected by the user is negative, the **Error Message** value is returned to the B Series Appliance along with a deny access to the Jump. There are 3 reserved words that can be used inside the **Error Message** that leverage the outcome result:
  - **%TaskFieldName%:** The actual value returned by ServiceNow of the **Task Field Name** chosen.
  - **%ComparatorSymbol%:** The symbol related to the option selected in the **Comparator**. Possible results are **>**, **=**, or **<**.

- **%FieldValue%:** The value used in the conditional logic, regardless of the option selected.

Transfer the BeyondTrust PRA-ServiceNow Integration Update Sets

The steps below are typically used after the integration has been imported and configured in a test/development instance of ServiceNow and is being transferred to a production instance. However, they are also applicable to transferring the integration between any ServiceNow instances.

Transfer Update Set

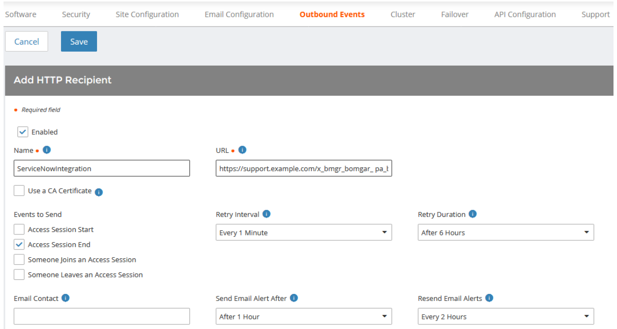
1. Follow the steps in the ServiceNow documentation to transfer the **BeyondTrust - ServiceNow Integration** update set(s) into the destination instance of ServiceNow.

> ***Note:** This is typically done by retrieving the update sets from the destination instance or by exporting the update sets from the original instance as XML files. For details, please see Export and Import XML files at https://docs.servicenow.com/bundle/utah-platform-administration/page/administer/development-best-practices/concept/c_ExportAndImportXMLFiles.html.*

2. Follow the same steps to transfer the **BeyondTrust - ServiceNow Integration Configuration** update set.

Configure Production Outbound Event

1. In the BeyondTrust interface, go to **/login > Management > Outbound Events**.
2. Copy the URL of the event for the original ServiceNow instance.
3. Click **Add**.
4. In the URL field, paste and replace the name of the original ServiceNow instance with that of the new one such that **/x_bmgr_bomgar_ pam_bomgar_ post.do** is preserved at the end. The result should be similar to **https://example.service-now.com/x_bmgr_bomgar_ pam_bomgar_ post.do**, as opposed to **https://example-dev.service-now.com/x_bmgr_bomgar_ pam_bomgar_ post.do**.
5. Under **Events to Send**, check **Access Session End**.
6. Click **Save**.
7. Locate the outbound event created during testing and then click **Edit**.
8. Uncheck **Enabled** and then click **Save**.



Add HTTP Recipient

• *Required field*

☑ Enabled

Name • : ServiceNowIntegration

URL • : https://support.example.com/x_bmgr_bomgar_ pa_l

☐ Use a CA Certificate

Events to Send

☐ Access Session Start
☑ Access Session End
☐ Someone Joins an Access Session
☐ Someone Leaves an Access Session

Retry Interval: Every 1 Minute

Retry Duration: After 6 Hours

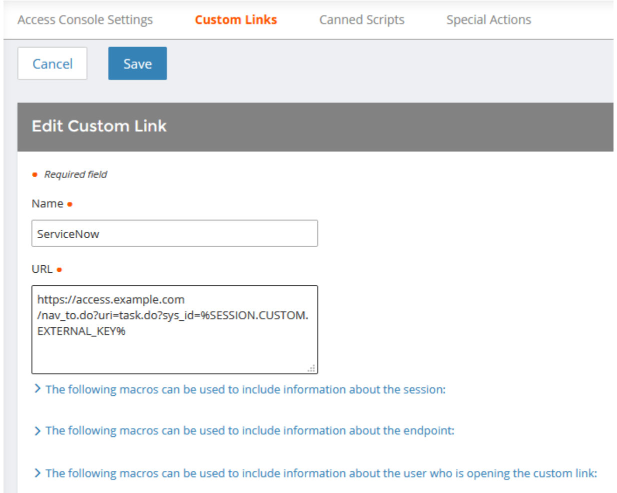
Email Contact:

Send Email Alert After: After 1 Hour

Resend Email Alerts: Every 2 Hours

Configure Custom Link

1. Go to **Access Console > Custom Links**.
2. Click **Edit** for the ServiceNow link, and then update the ServiceNow URL to direct to the destination instance of ServiceNow. Be careful to preserve **/nav_to.do?uri=task.do?sys_id=%SESSION.CUSTOM.EXTERNAL_KEY%** at the end.
3. Click **Save**.
4. Test the integration setup in its new location following the same steps used to test the original instance.



Edit Custom Link

• Required field

Name •

ServiceNow

URL •

https://access.example.com
/nav_to.do?uri=task.do?sys_id=%SESSION.CUSTOM.EXTERNAL_KEY%

> The following macros can be used to include information about the session:

> The following macros can be used to include information about the endpoint:

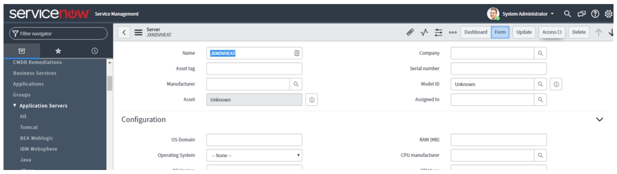
> The following macros can be used to include information about the user who is opening the custom link:

For more information on testing the integration, please see "Test the Setup of the BeyondTrust PRA and ServiceNow Integration" on page 21.

Test the Setup of the BeyondTrust PRA and ServiceNow Integration

The following steps take place in ServiceNow and BeyondTrust and are provided to ensure that the integration is working properly. Troubleshooting suggestions are provided with each step in case of failure.

Test Access Configuration Item Button



Server
JXNDVHEAT

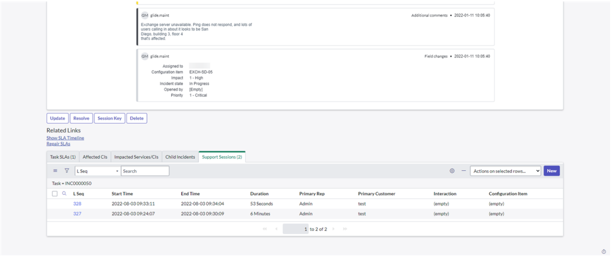
Name: JXNDVHEAT
Asset tag:
Manufacturer:
Asset: Unknown
Company:
Serial number:
Model ID: Unknown
Assigned to:

Configuration

OS Domain:
Operating System: -- None --
RAM (MB):
CPU manufacturer:

1. Log into the BeyondTrust access console, and then log into ServiceNow with the same account. If BeyondTrust and ServiceNow use different authentication systems, manually assign your BeyondTrust user to your ServiceNow user as described in "Configure BeyondTrust Username and Authentication" on page 14.
2. Open a configuration item in ServiceNow that has a corresponding Jump Client in BeyondTrust, and make sure the **Access CI** button shows up.
3. Click the **Access CI** button. It should launch the BeyondTrust access console. In case of failure, make sure the following are true:
   - The ServiceNow user account is mapped to a BeyondTrust user account as described in this guide.
   - The ServiceNow API User Connection test completes successfully.
   - The BeyondTrust **Hostname**, **Username**, and **Password** fields are set correctly in ServiceNow under **BeyondTrust PRA > Appliances**. These should match the API User Connection test.

Test BeyondTrust Session Import



glide.maint — Additional comments • 2022-01-11 10:05:40

Exchange server unavailable. Ping does not respond, and lots of users calling in about it looks to be San Diego, building 3, floor 4 that's affected.

glide.maint — Field changes • 2022-01-11 10:05:40

Assigned to: [redacted]
Configuration item: EXCH-SD-05
Impact: 1 - High
Incident state: In Progress
Opened by: [Empty]
Priority: 1 - Critical

Task = INC0000050

L Seq	Start Time	End Time	Duration	Primary Rep	Primary Customer	Interaction	Configuration Item
328	2022-08-03 09:33:11	2022-08-03 09:34:04	53 Seconds	Admin	test	(empty)	(empty)
327	2022-08-03 09:24:07	2022-08-03 09:30:09	6 Minutes	Admin	test	(empty)	(empty)

1 to 2 of 2

1. Log into ServiceNow as an ITIL user or an admin.
2. Use the **Access CI** button as described above to start a BeyondTrust session.
3. End the session from the access console and close any session end messages on the user and/or customer sides of the session.
4. Refresh the ServiceNow incident from which the session key was generated, scroll to the bottom of the page, and check the **BeyondTrust Sessions** list. There should be an entry for the recent session. If not, make sure the following are true:
   - The API User Connection test works correctly as described above.
   - There are no BeyondTrust errors reported for your ServiceNow instance in the BeyondTrust Outbound Events list. Your BeyondTrust admin can check this in BeyondTrust from the **/login** web interface under **Management > Outbound Events**.
   - The IP address is set up correctly, following the steps below:
     - Log into ServiceNow as an admin.
     - Browse to **System Logs > Transactions**, remove all existing filters, and add a URL filter of **/x_bmgr_bomgar_ pam_bomgar_ post.do**.

- Click one of the results and make sure the originating IP address of the transaction is included in the **B Series Appliance IP Address** field of the integration B Series Appliance settings under **BeyondTrust PRA > Appliances > Default**.

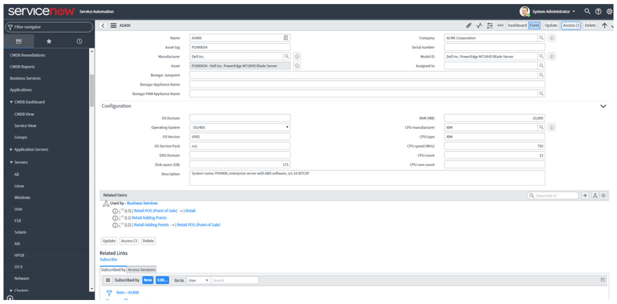
Use Cases for the ServiceNow Enterprise Integration with BeyondTrust Privileged Remote Access

Organizations using ServiceNow can integrate with BeyondTrust PRA to provide secure, privileged access to critical assets from within ServiceNow. This satisfies internal and external compliance requirements while maintaining comprehensive audit trails and integrating with change management processes.

Jump to Configuration Item

Technicians can leverage BeyondTrust Jump Technology to access a configuration item associated with an incident directly from the incident. Additionally, this same technology can be leveraged directly from within a configuration item, even if it is not associated with an incident.

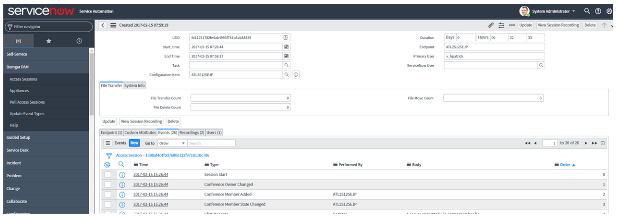
Once the session ends, a detailed report of the session is imported into ServiceNow and associated with the incident or configuration item record from which it originated.



Import BeyondTrust Session Data into a ServiceNow Record

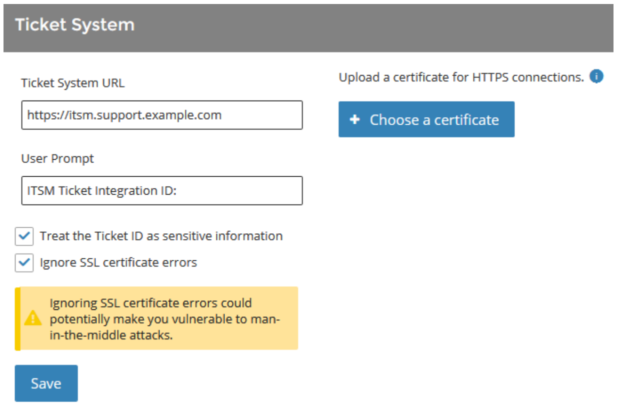
Once the BeyondTrust access session ends, ServiceNow is automatically updated with information gathered during the session, including:

- File Transfer Information
- Endpoint System Information
- Users Involved
- Endpoint Details
- Access Session Recordings



Change Management Workflow

BeyondTrust access requests can require a ServiceNow incident ID to be entered as part of the access request process. Once entered, the request is sent to ServiceNow where it can be programmatically denied or allowed using the BeyondTrust API.



Ticket System

Ticket System URL: https://itsm.support.example.com

User Prompt: ITSM Ticket Integration ID:

☑ Treat the Ticket ID as sensitive information

☑ Ignore SSL certificate errors

Ignoring SSL certificate errors could potentially make you vulnerable to man-in-the-middle attacks.

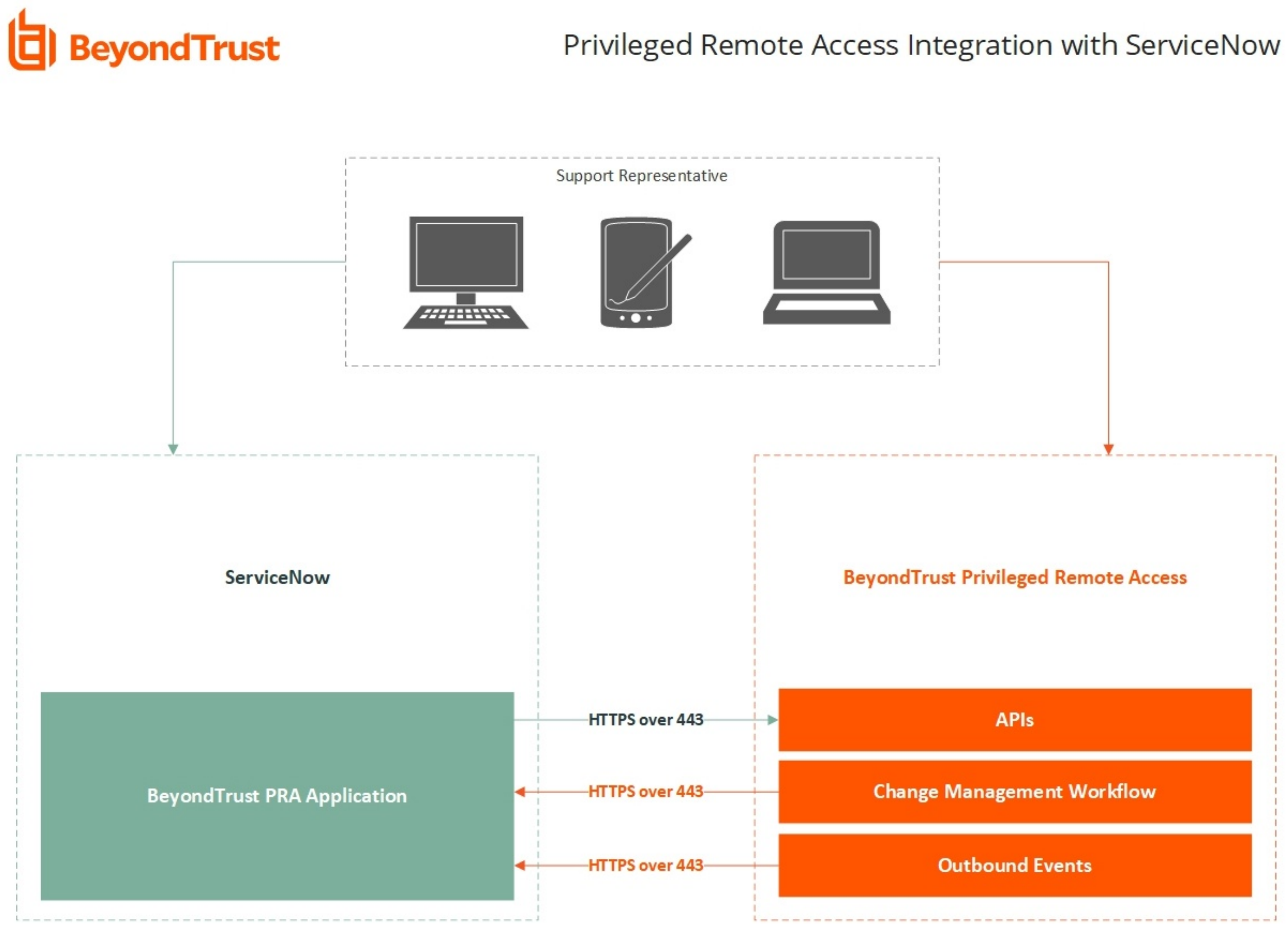
Upload a certificate for HTTPS connections.

Access ServiceNow Records from Access Console

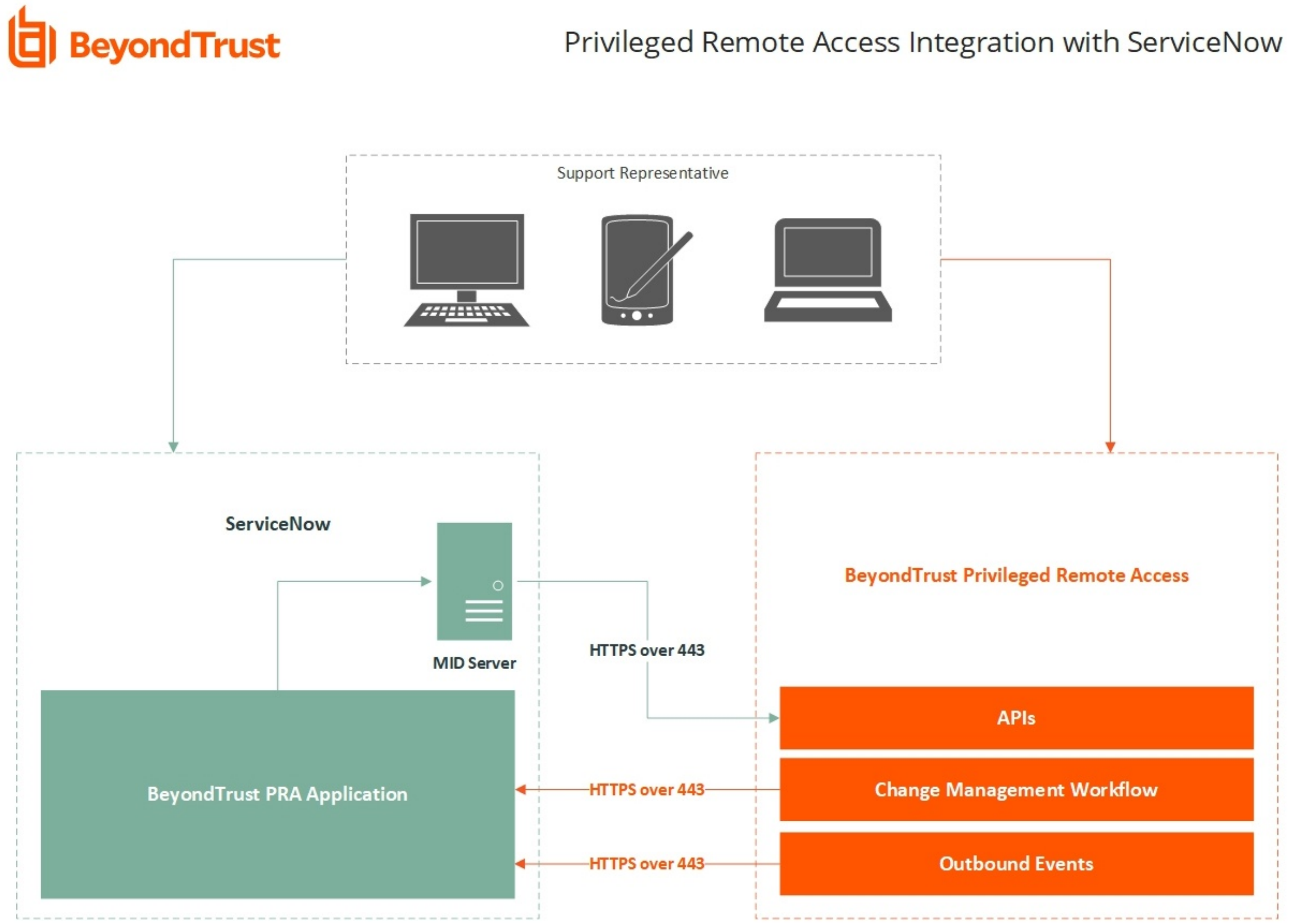
Using BeyondTrust's custom link ability, a user can access the associated ServiceNow record directly from within the access console. This saves time searching for the record in ServiceNow and provides the user with any available session details, history, or other context to help resolve issues quickly.

ServiceNow PRA Integration Architecture Diagrams

Network Diagram


BeyondTrust
Privileged Remote Access Integration with ServiceNow
Support Representative
ServiceNow
BeyondTrust PRA Application
BeyondTrust Privileged Remote Access
APIs
Change Management Workflow
Outbound Events
HTTPS over 443
HTTPS over 443
HTTPS over 443

Network with Mid Server Diagram


BeyondTrust
Privileged Remote Access Integration with ServiceNow
Support Representative
ServiceNow
MID Server
BeyondTrust PRA Application
HTTPS over 443
HTTPS over 443
HTTPS over 443
BeyondTrust Privileged Remote Access
APIs
Change Management Workflow
Outbound Events