Remote Support

BMC Remedy Integration

Table of Contents

BeyondTrust Integration with BMC Remedy

IMPORTANT!

You must purchase this integration separately from both your BeyondTrust software and your BMC Remedy solution. For more information, contact BeyondTrust sales.

Service desks and customer support organizations using BMC Remedy can integrate with BeyondTrust to improve service levels, centralize support processes, and strengthen compliance. This document describes the installation and configuration of the BeyondTrust Remote Support integration with BMC Remedy.

The BMC Remedy integration with BeyondTrust Remote Support provides the following functionality:

- A BeyondTrust support session can be initiated from the context of a BMC Remedy ticket.
- A BeyondTrust Jump session can be initiated to a computer system Configuration Item associated with a ticket.
- At the end of a session, the incident can be updated with the session information.

Prerequisites for the BeyondTrust Remote Support Integration with BMC Remedy

To complete this integration, please ensure that you have the necessary software installed and configured as indicated in this guide, accounting for any network considerations.

Applicable Versions

- BeyondTrust Remote Support: 14.x and newer
- BMC Remedy: 8.x and newer

Network Considerations

The following network communication channels must be open for the integration to work properly.

Outbound From	Inbound To	TCP Port #	Purpose
BeyondTrust Middleware Engine Server	BMC Remedy	443	API calls from the BeyondTrust Middleware Engine server.
BeyondTrust Middleware Engine Server	BeyondTrust Appliance	443	API calls from the BeyondTrust Middleware Engine server.
BeyondTrust Appliance	BeyondTrust Middleware Engine Server	8180 (default) 443 (optional)	The BeyondTrust Middleware Engine server receives outbound events from the appliance. However, if polling is used instead of outbound events, then this port does not have to be open.

Prerequisite Installation and Configuration

The BMC Remedy integration is a BeyondTrust Middleware Engine plugin. To install the BeyondTrust Middleware Engine, follow the instructions in the BeyondTrust Middleware Engine Configuration document at www.beyondtrust.com/docs/remote-support/how-to/integrations/middleware-engine. The BeyondTrust Middleware Engine Configuration document is also useful to understand how to work with the middleware engine.

Configure BMC Remedy for Integration with BeyondTrust Remote Support

Integration between BMC Remedy and BeyondTrust Remote Support requires importing a collection of custom objects into the BMC Remedy environment. These include Filters, Active Links, Web Services, etc. The following steps outline this import and configuration process.

Initially, some manual steps must be taken before the bulk of the AR System items can be imported.

Import Forms

1. Open BMC Remedy Developer Studio.
2. From the main menu, select **File > Import**.
3. Expand **BMC Remedy Developer Studio**.
4. Select **Object Definitions** and click **Next**.
5. Select the appropriate server and click **Next**.
6. Select the **bomgar_Remedy_Int_With_Incident_Vx.x.xml** file from the appropriate location and click **Next**.
7. From the XML file, add the following forms, removing all other items:
   a. **COL:BGR:SessionDetail:Staging**
   b. **COL:BGR:Configuration:Params**
   c. **COL:BGR:Form:Setup_Template**
8. Select the following options:
   a. **Replace Objects on the Destination Server**
   b. **Delete Excess Views**
   c. **Replace Application Owner**
   d. **Handle Conflicting Types: Display Conflict Error**
9. Click **Finish**.
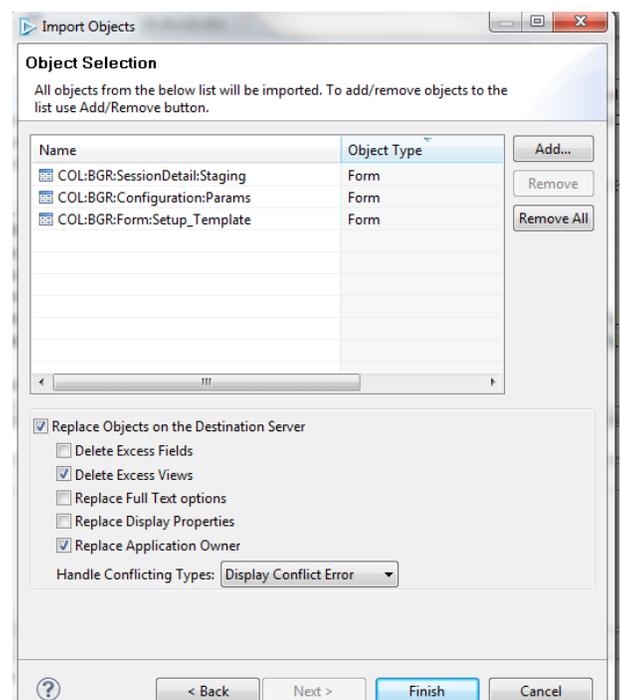
> 📌 *Note: The import process may take several minutes to complete. Upon successful completion, the above forms will have been imported into the AR System.*

Update Existing Forms - HPD:Help Desk

> **Note:**
>
> *Before this operation, determine in which views the fields will be visible. To save time, it may be a good idea to set the Remedy Administrator preferences (in the **Windows > Preferences** menu) so that fields are not automatically added to all views. This way, fields are added only to the views to which they are pasted. Also, make sure to back up the Incident Form.*
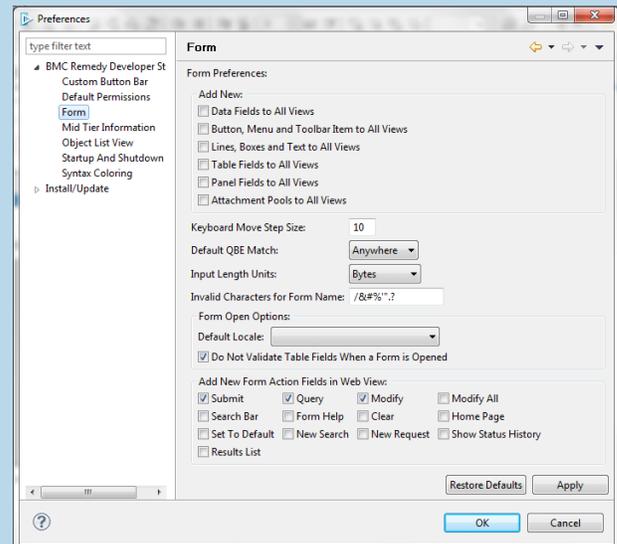
1. Open the **Incident** form (**HPD:Help Desk**) in the **Best Practices** view in Developer Studio.

2. Also open the newly imported **COL:BGR:Form:Setup_Template**.

3. If the **Incident** form does not already have an overlay, select **Forms > Create View Overlay** from the menu.

4. Add a new Panel with the following properties:

    a. **ID:** 800000001

    b. **Name:** COL_Pnl_BeyondTrust_Sessions

    c. **Label:** BeyondTrust Sessions

    d. **Visible:** False

    e. **Permission:** Public

5. Copy and paste the following fields from the **Setup_Template** form to the new panel on the **Incident** form.

    a. **800000002:** COL_Tbl_Session_Summary

    b. **800000003:** COL_Col_Session_ID

    c. **800000004:** COL_Col_Start_Time

    d. **800000005:** COL_Col_End_Time

    e. **800000006:** COL_Col_Duration

    f. **800000007:** COL_Col_File_Count

    g. **800000008:** COL_Col_Representative

    h. **800000009:** COL_Ctrl_BeyondTrust_Logo

    i. **800000010:** COL_Char_Support_Session_Details

6. Once complete, the **BeyondTrust Sessions** panel should look similar to the screen shot. Save the form.
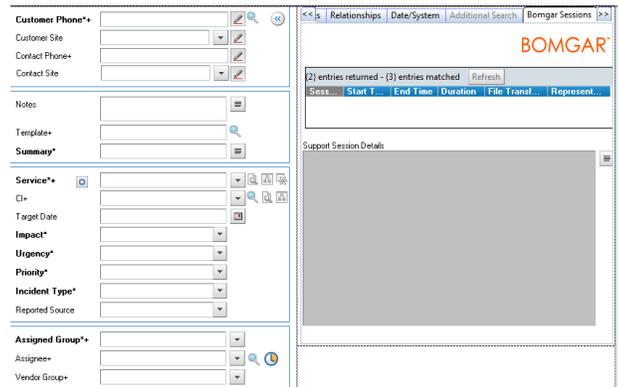
Add "Launch BeyondTrust Session Key" Link to Left Navigation

1. Add the left navigation **z2NF_LeftNavigation** to the overlay and save it.
2. Select the left navigation from the outline window and right-click it.
3. Select **Edit Menu / Navigation Items**.
4. In the **Edit** window, expand the **Functions** items to add a new item under this menu.
5. Select the **Functions** menu and click **Add Item**.
6. Once the item is added, select it and edit its properties to match the following:
   a. **ID:** 900370918
   b. **Name:** COL_z2NI_LaunchBomgarSession()
   c. **Label:** Launch BeyondTrust Session Key
   d. **Visible:** True
   e. **Permission:** Public
7. Save the **Incident** form.
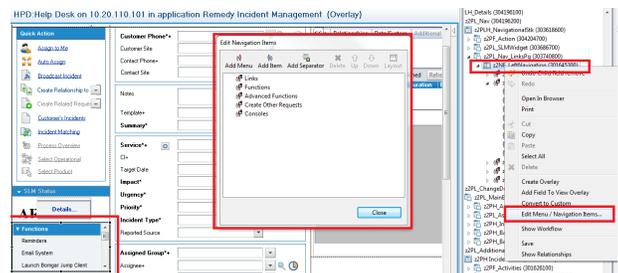
Add Display-Only Fields

1. Copy the following display-only fields from the **Setup_Template** form to the bottom area of the **Incident** form:
   a. **900070914:** z2tmp_LaunchURL
   b. **900070917:** z2tmp_Launch_CI
   c. **900270919:** z2tmp_SessionURL
2. Save the form.
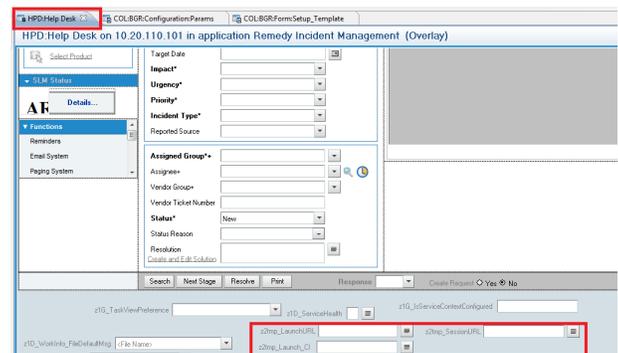
Add "Launch BeyondTrust Jump Client" Link to Left Navigation

1. Select the left navigation from the outline window and right-click it.
2. Select **Edit Menu / Navigation Items**.
3. In the **Edit** window, expand the **Functions** items to add a new item under this menu.
4. Select the **Functions** menu and click **Add Item**.
5. Once the item is added, select it and edit its properties to match the following:
    a. **ID:** 908970913
    b. **Name:** COL_z2NI_Launch BeyondTrust CI
    c. **Label:** Launch BeyondTrust Jump Client
    d. **Visible:** True
    e. **Permission:** Public
6. Save the **Incident** form.

Update Existing Forms - SRS:RequestDetail

1. Open the **Service Request Console** form (**SRS:RequestDetail**) in **SRS User** view in **Developer Studio**.
2. Also open the newly imported **COL:BGR:Form:Setup_Template (SRM-RQC View)**.
3. If the **Service Request** form does not already have an overlay, select **Forms > Create View Overlay** from the menu.
4. Copy and paste the following fields from the **Setup_Template** form to the new panel on the **Service Request** form.
    a. **800000600:** COL_Btn_Get_Support_Now
    b. **800000601:** COL_VF_Launch_Support_Window
    c. **800000602:** COL_Char_Mid-Tier_URL
    d. **800000603:** COL_Char_Incident_Number
5. Once complete, the request details should look similar to the screen shot. Save the form.
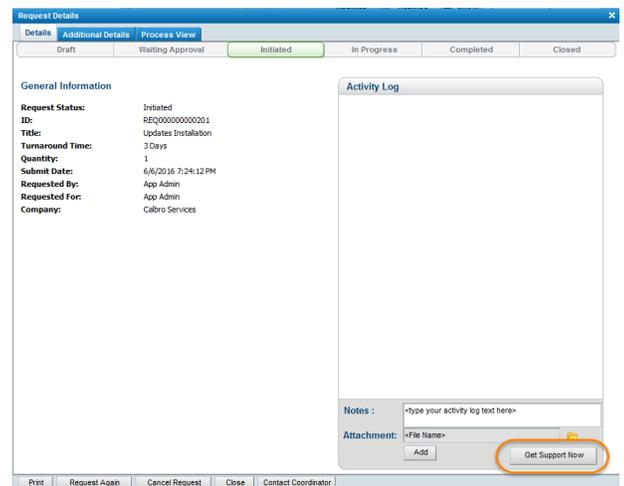
Import Remaining Items

Once the manual steps above have been completed, the remainder of the package can be imported.

1. From the main menu, select **File > Import**.
2. Expand **BMC Remedy Developer Studio**.
3. Select **Object Definitions** and click **Next**.
4. Select the appropriate server and click **Next**.
5. Select the **bomgar_Remedy_Int_With_Incident_Vx.x.xml** file from the appropriate location and click **Next**.
6. Import all objects, making sure to select **Replace Objects on the Destination Server**.
7. Click **Finish**.

> **Note:** *The import process may take several minutes to complete. Upon successful completion, the required forms, workflows, and web services will have been imported into the AR System.*

8. Flush the Mid-Tier and browser caches, located at **<protocol>://<mid-tier-server>:<port>/arsys/shared/config/config.jsp**.

Configure the Integration

1. In a browser, open the **Configuration Params** form (**<protocol>://<mid-tier-server>:<port>/arsys/forms/<AR-server-name>/COL:BGR:Configuration:Params**).
2. Add attribute details for the **BeyondTrust Server** attribute for both the **Launch Session** and **Launch BeyondTrust CI (Jump Client)** items.
3. The **Attribute Value** should be **https://<BeyondTrust-site-hostname>**.
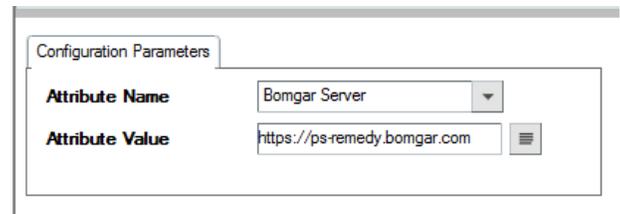

> **Note:** *Access to the **BeyondTrust Sessions** tab as well as the **Session Key** and **Jump to CI** functions are controlled by users' group memberships. Any user who should have access to these items should be added to a new Group in Remedy named "BeyondTrust Users".*

Configure Smart IT for the Integration between BMC Remedy and BeyondTrust Remote Support
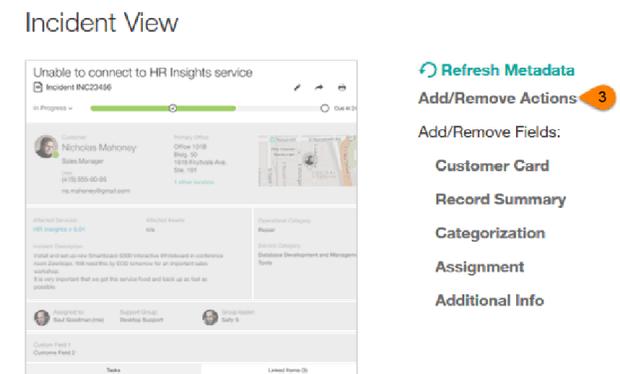
If your environment has Smart IT available, there are a few use cases that can be implemented within Smart IT.

Generate BeyondTrust Session Key

1. Log into Smart IT as an admin user (**<protocol>://<mid-tier-server>:<port>/ux/smart-it/#/**).
2. Navigate to **Configuration > Screen Configuration**.
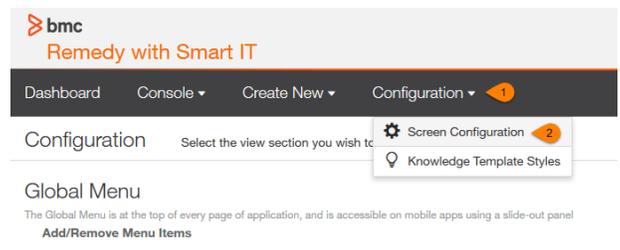
3. In the **Incident View** section, select **Add/Remove Actions**.

4. Create a new action with the following settings:
   a. **Action Type:** Client-side URL
   b. **Supported Platforms:** Desktop Web (UC)
   c. **URL/URI:** `https://<BeyondTrust-hostname>/api/client_script?public_portal_hostname=<BeyondTrust-public-portal-hostname>&type=rep&operation=generate&action=generate_session_key&session.custom.external_key=[id]`
   d. **Open Behavior:** New Browser Window
   e. **Default Label Text:** Generate BeyondTrust Session Key
5. Save the action.
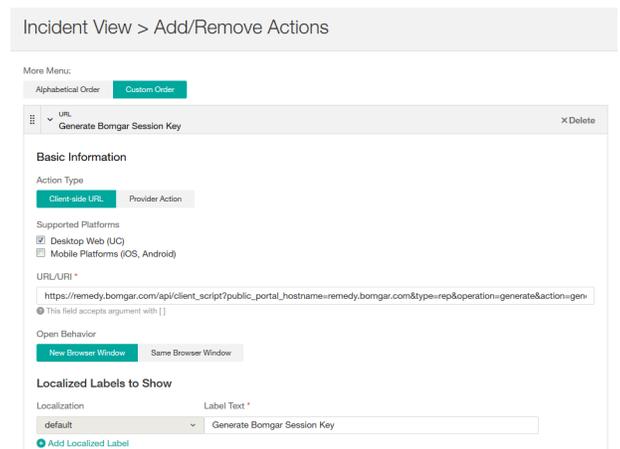
Leverage SmartRecorder to Create Incidents

BeyondTrust 15.1 and later

1. Log into the BeyondTrust /login interface as an admin user.

2. Browse to **Rep Console > Custom Links**.

3. Under **Rep Console :: Custom Links**, click **Create New Custom Link**.

4. Create a link with the following settings:

   a. **Name:** Create Incident via BMC Smart IT

   b. **URL:** `<protocol>://<mid-tier-server>:<port>/ux/smart-it/#/create/smart-recorder?customer=%CUSTOMER.NAME%&desc=%SESSION.DETAILS%`

5. Click **Add Custom Link** to save the new link.

BeyondTrust 15.0 and earlier

1. Log into the BeyondTrust /login interface as an admin user.

2. Browse to **Configuration > Options > Representative Console :: Custom Link**.

3. Set the URL to `<protocol>://<mid-tier-server>:<port>/ux/smart-it/#/create/smart-recorder?customer=%CUSTOMER.NAME%&desc=%SESSION.DETAILS%`

4. Click **Save**.

Configure BeyondTrust for the BMC Remedy Integration

Several configuration changes are necessary on the BeyondTrust Appliance to integrate with BMC Remedy. You must make these changes on each appliance for which you intend to create a plugin configuration, described in "Configure the BMC Remedy Plugin for Integration with BeyondTrust Remote Support" on page 16.

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

Verify That the API Is Enabled

This integration requires the BeyondTrust XML API to be enabled. This feature is used by the BeyondTrust Middleware Engine to communicate with the BeyondTrust APIs.
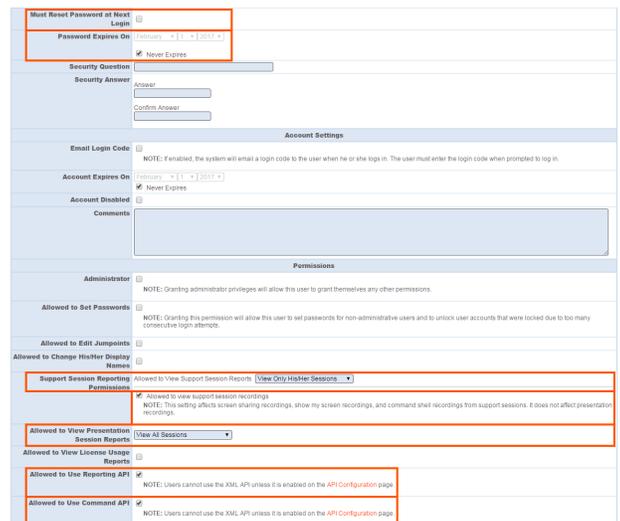
Go to **/login > Management > API Configuration** and verify that **Enable XML API** is checked.

## Create an API Service Account - BeyondTrust 16.1 and Earlier

The API user account is used from within the integration to make BeyondTrust Command API calls to BeyondTrust.

1. Go to **/login > Users & Security > Users**.
2. Click **Create New User** and name it **Integration** or something similar.
3. Leave **Must Reset Password at Next Login** unchecked.
4. Set **Password Expires On** to **Never Expires**.
5. Set **Allowed to View Support Session Reports** to **View All Sessions**.
6. Check **Allowed to view support session recordings**.
7. Set **Allowed to View Presentation Session Reports** to **View All Sessions**.
8. Check **Allowed to Use Reporting API** and **Allowed to Use Command API**.
9. Scroll to the bottom and save the account.

Create an API Service Account - BeyondTrust 16.2 and Later

1. Go to **Management > API Configuration** and create a new API account.

2. Under **Permissions**, check **Full Access** to the **Command API**.

3. For the **Reporting API**, check **Allow Access to Support Session Reports and Recordings** and **Allow Access to Presentation Session Reports and Recordings**.

4. Be sure to copy the values for both the **OAuth Client ID** and **OAuth Client Secret** for use in a later step.
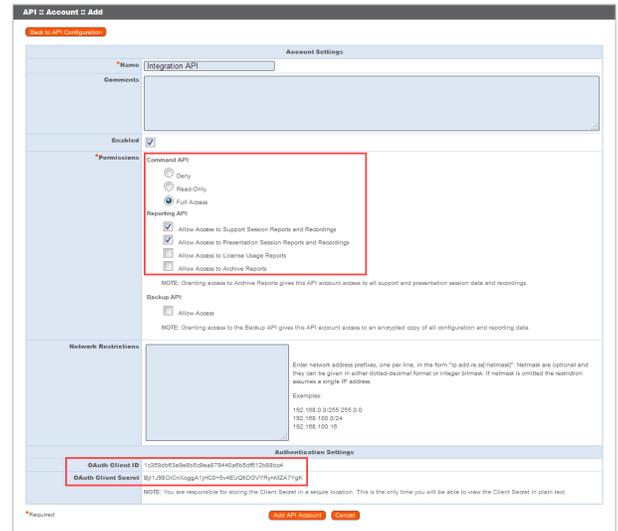
5. Click **Add API Account** to create the account.

Add an Outbound Event URL

1. Go to **/login > Management > Outbound Events**.

2. Click **Add New HTTP Recipient** and name it **Integration** or something similar.

3. Enter the URL to use:

   - If using an appliance ID of "default": `http://<middleware-host>:<port>/ERSPost`. The default port is `8180`.

   - If using an appliance ID other than "default": `http://<middleware-host>:<port>/ERSPost?appliance=<appliance-id>` where `<middleware-host>` is the hostname where the BeyondTrust Middleware Engine is installed. The default port is `8180`. The `<appliance-id>` is an arbitrary name, but note the value used, as it is entered later in the plugin configuration. This name accepts only alphanumeric values, periods, and underscores.

4. Scroll to **Events to Send** and check the following events:

   - **Support Session End**
   - **Customer Exit Survey is Completed**
   - **Representative Survey is Completed**
   - **Someone Joins a Support Session** (Optional)

5. Scroll to the bottom and click **Add Recipient**.
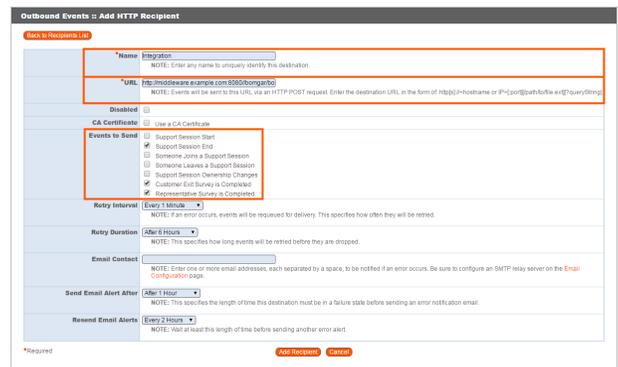
6. Now, the list of outbound events should contain the event just
    added. The **Status** column displays a value of **OK** if
    communication is working. If communication is not working, the
    Status column displays an error which you can use to repair
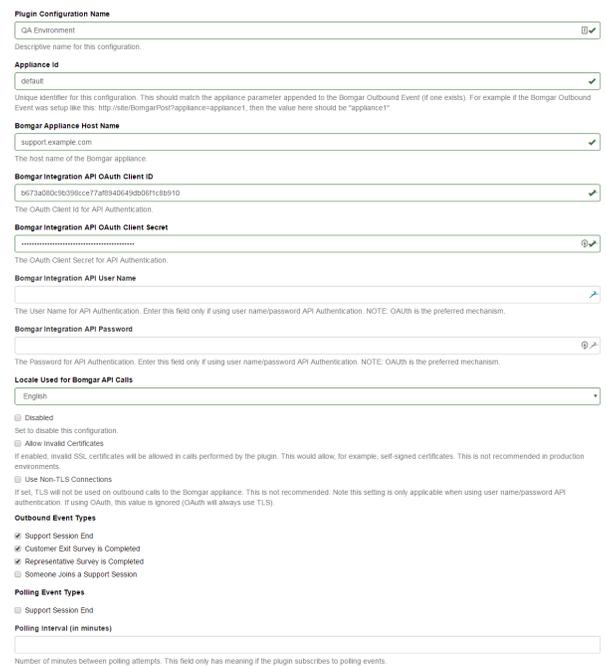   communication.

Configure the BMC Remedy Plugin for Integration with BeyondTrust Remote Support

Now that you have configured BMC Remedy and the BeyondTrust Appliance, deploy and configure the BMC Remedy plugin. For additional information about working with the BeyondTrust Middleware Engine, please see the BeyondTrust Middleware Engine Configuration document at www.beyondtrust.com/docs/remote-support/how-to/integrations/middleware-engine.

1. Copy the provided plugin zip file to the server hosting the BeyondTrust Middleware Engine.
2. Extract the plugin zip file to the **Plugins** folder in the directory where the BeyondTrust Middleware Engine is installed.
3. Restart the BeyondTrust Middleware Engine Windows service.
4. From the server, launch the middleware administration tool. The default URL is **http://127.0.0.1:53231**.
5. The **BMC Remedy Plugin** shows in the list of plugins. Click the clipboard icon to add a new configuration.

BeyondTrust Appliance

The first portion of the plugin configuration provides the necessary settings for communication between the plugin and the BeyondTrust Appliance. The configuration sections include:

1. **Plugin Configuration Name:** Any desired value. Because multiple configurations can be created for a single plugin, allowing different environments to be targeted, provide a descriptive name to indicate how this plugin is to be used.
2. **Appliance Id:** This can be left as **Default** or can be given a custom name. This value must match the value configured on the outbound event URL in the BeyondTrust Appliance. If outbound events are not being used, this value is still required, but any value may be used.
3. **BeyondTrust Appliance Host Name:** The hostname of the BeyondTrust Appliance. Do not include `https://` or other URL elements.
4. **BeyondTrust Integration API OAuth Client ID**: When using API accounts in BeyondTrust Remote Support 16.2.1 or newer, this field should contain the Client ID of the OAuth account.
5. **BeyondTrust Integration API OAuth Client Secret:** When using API Accounts available in BeyondTrust Remote Support 16.2.1 or newer, this field should contain the client Secret of the OAuth account.
6. **BeyondTrust Integration API User Name:** If using a BeyondTrust Remote Support version prior 16.2.1, this field should contain the username of the API service account created on the BeyondTrust Appliance.
7. **BeyondTrust Integration API Password:** If using a BeyondTrust Remote Support version prior 16.2.1, this field should contain the password of the above user.
8. **Locale Used for BeyondTrust API Calls:** This value directs the BeyondTrust Appliance to return session data in the specified language.
9. **Disabled:** Enable or disable this plugin configuration.

10. **Allow Invalid Certificates:** Leave unchecked unless there is a specific need to allow. If enabled, invalid SSL certificates are allowed in calls performed by the plugin. This would allow, for example, self-signed certificates. This is not recommended in production environments.

11. **Use Non-TLS Connections:** Leave unchecked unless it is the specific goal to use non-secure connections to the BeyondTrust Appliance. If checked, TLS communication is disabled altogether. If non-TLS connections are allowed, HTTP access must be enabled on the BeyondTrust **/login > Management > API Configuration** page. Using non-secure connections is discouraged.

> 📌 **Note:** *When using OAuth authentication, TLS cannot be disabled.*

12. **Outbound Events Types:** Specify which events the plugin processes when received by the middleware engine. Keep in mind that any event types selected here must also be configured to be sent in BeyondTrust. The middleware engine receives any events configured to be sent in BeyondTrust but passes them off to the plugin only if the corresponding event type is selected in this section.

    a. **Support Session End**

    b. **Customer Exit Survey is Completed**

    c. **Representative Survey is Completed**

13. **Polling Event Types:** If network constraints limit connectivity between the BeyondTrust Appliance and the middleware engine such that outbound events cannot be used, an alternative is to use polling. The middleware engine regularly polls the BeyondTrust Appliance for any sessions that have ended since the last session was processed. At this time, only the **Support Session End** event type is supported.

> 📌 **Note:** *One caveat to polling behavior versus the use of outbound events is that if a session has ended but the customer exit survey has not yet been submitted within the same polling interval, the customer exit survey is not processed. This does not apply to representative surveys since the session is not considered to be complete if a representative survey is still pending.*

14. **Polling Interval:** Enter only if polling is used. This determines how often the middleware engine polls the BeyondTrust Appliance for sessions that have ended.

15. **Retry Attempt Limit:** Enter the number of retries that can be attempted if the plugin fails to process an event.

16. **Retry Outbound Event Types:** Specify which outbound events the plugin retries if it fails to process the event.

17. **Retry Polling Event Types:** Specify which polling events the plugin retries if it fails to process the event.

BMC Remedy Instance

The remainder of the plugin configuration provides the necessary settings for communication between the plugin and the BMC Remedy instance. The configuration settings include:

1. **BMC Remedy Services URL:** URL of the AR Service for the BMC Remedy instance (e.g., `https://remedy.example.com/arsys/services/ARService`).

2. **BMC Remedy Username:** The username of the API account.

3. **BMC Remedy Password:** The password of the above user.

4. **BMC Remedy AR Server:** The name of the AR/app server instance.

5. **Session Reports Storage:** Populate the session reports into the BeyondTrust Sessions tab, as a Work Note, or both.

    The following settings apply only if **Session Reports Storage** is set to **Work Notes** or **Both**:

a. **Work Info Source:** The default value for the Source field on the Work Note (e.g., Email, Phone, Web, Other, etc.).

b. **Work Info Type:** The default value for the Type field on the Work Note. The name should contain no spaces or other non-alpha characters (e.g., CustomerCommunication, GeneralInformation, IncidentTaskAction, etc.).

c. **Publish as Public Notes:** Specifies whether to publish the notes as public or not.

d. **Lock Log:** Specifies whether to lock the work log or not.

After saving the configuration, click the test icon next to the new plugin configuration. No restart is needed.

Report Templates

On the BeyondTrust Middleware Engine server, in the **<install dir>\Plugins\<integration>\Templates** folder, there are multiple files ending with ***.hbs**. These files are used by the plugin to format the textual session report and exit surveys that are added to the corresponding ticket each time a BeyondTrust session ends or each time a survey is submitted. The templates can be edited if desired.

> **Note:** *If changes need to be made to a template, it is a good idea to first back up the original in case the changes ever need to be reverted.*

For additional information on Handlebars templates, see handlebarsjs.com.

Use Cases for the BMC Remedy Integration with BeyondTrust Remote Support

Generate Session Key

Support staff can generate a session key that can be given to the end user over the phone or via email to initiate a support session that is automatically associated with the selected ticket.
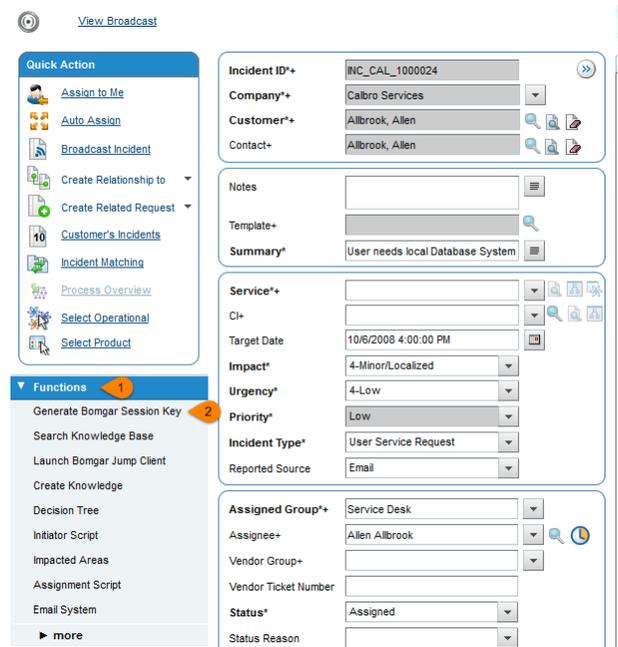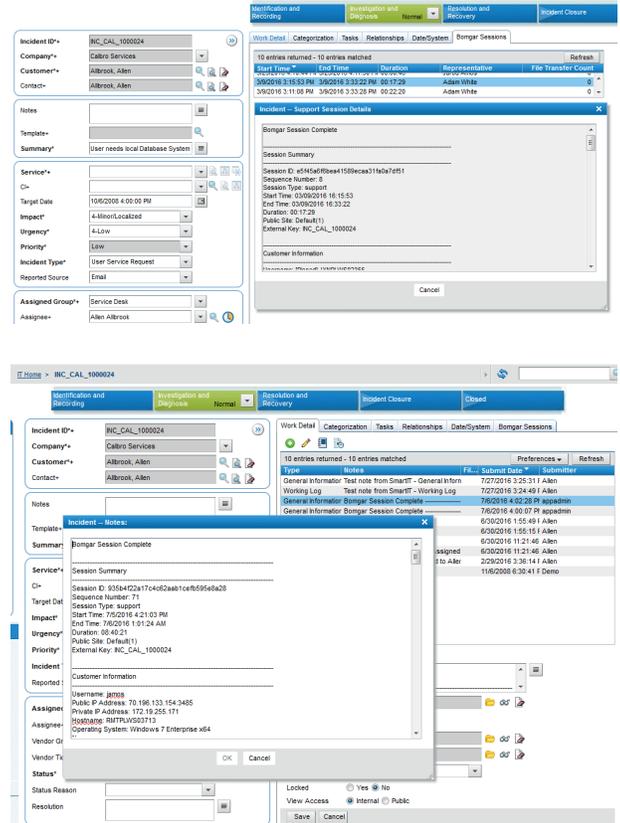

This can be done from within Smart IT.
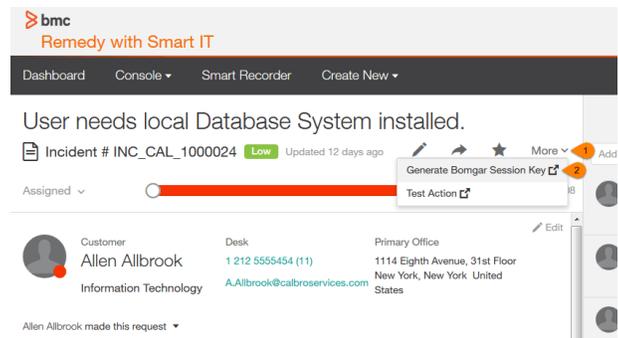
Import BeyondTrust Session Data into Ticket

Once the session ends, the ticket is automatically updated with information gathered during the session, including:

- **Chat Transcript** (including files transferred, special actions, and other events)
- **System Information** (the General section plus other select details such as disk, memory, and network)
- **Session Notes**
- **Surveys** (customer and representative)

To be flexible in meeting varying needs, session data can be displayed within a custom BeyondTrust Sessions tab on the Incident form, added as a Work Note, or both.

Jump to Configuration Item

Support staff can leverage BeyondTrust Jump Technology to access a configuration item associated with a ticket directly from the BMC Remedy ticket.

Click-to-Chat for Self Service Users

Self Service users can open their submitted requests in the SRM Request Entry Console and start a chat support session directly from the BMC Remedy ticket. This allows the user the quickest path to resolution while also providing the representative with the necessary context to assist the user. Sessions can be elevated to full support sessions if enabled and when necessary.
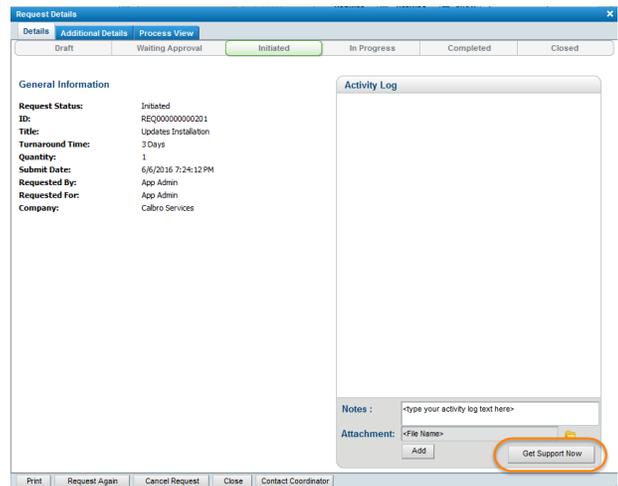
Access Ticket from Representative Console

Using BeyondTrust's custom links ability, a representative can access the associated ticket directly from within the representative console. This saves time searching for the ticket in BMC Remedy and provides the representative with any available \issue details, history, or other context to help quickly resolve the issue.

Create Ticket via Smart IT

Using the Smart Recorder in Smart IT for BMC Remedy and BeyondTrust's custom links, a ticket can be created from within the representative console with a single click when the representative is in session. The customer name and issue description from the BeyondTrust session are automatically passed into the new ticket. If available, this can save time and unnecessary clicks for support staff.