Remote Support

BMC FootPrints 12 Integration
# Table of Contents

BeyondTrust Remote Support Integration with BMC FootPrints 12 .................................. 3

Prerequisites for the BeyondTrust Remote Support Integration with BMC FootPrints 12 .......................... 4
  Applicable Versions ................................................................. 4
  Network Considerations .......................................................... 4
  Prerequisite Installation and Configuration .................................. 4

Configure BMC FootPrints 12 for Integration with BeyondTrust Remote Support ............. 5
  Enable Web Services ............................................................... 5
  Create an API User Account ...................................................... 6

Configure BeyondTrust for the BMC FootPrints 12 Integration ...................................... 8
  Verify the API Is Enabled ............................................................ 8
  Create an API Service Account - BeyondTrust 16.1 and Earlier .................. 8
  Create an API Service Account - BeyondTrust 16.2 and Later .................. 9
  Add an Outbound Event URL ...................................................... 9
  Add a Custom Link .................................................................. 10

Configure the BMC FootPrints 12 Plugin for Integration with BeyondTrust Remote Support ........................................ 11
  Secure Remote Access Appliance ................................................. 11
  BMC FootPrints 12 Instance ...................................................... 12
  Test Settings and Generate HTML Content .................................. 13
  Report Templates .................................................................. 13

Finish Configuring BMC FootPrints 12 for Integration with BeyondTrust Remote Support ........................................ 14
  Customize Incident Form (Agent's View) ...................................... 14
  Customize Incident Form (Customers' View) .................................. 17
  Create Custom Link Page .......................................................... 18

Use Cases for the BMC FootPrints 12 Integration with BeyondTrust Remote Support ........ 19
  Generate Session Key ............................................................... 19
  Import BeyondTrust Session Data into Ticket .................................. 19
  Jump to Configuration Item ....................................................... 20
  Click-to-Chat for Self Service Users ........................................... 20
  Access Ticket from Representative Console .................................. 20
BeyondTrust Remote Support Integration with BMC FootPrints 12

**IMPORTANT!**

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

Service desks and customer support organizations using BMC FootPrints 12 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 FootPrints.

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

- A BeyondTrust support session can be initiated from the BMC FootPrints interface. This session is linked to the incident in BMC FootPrints.
- A BeyondTrust Jump session can be initiated from the BMC FootPrints interface. From within FootPrints, you can Jump to a pinned Jump Client. These sessions are linked to the incident in BMC FootPrints.
- At the end of a session, the incident can be updated with the following information:
  - Chat Transcript (including files transferred, special actions, and other events)
  - System Information (General section plus other select details such as disk, memory, and network)
  - Session Notes
  - Surveys (customer and representative)
  - Links to Session Recordings
Prerequisites for the BeyondTrust Remote Support Integration with BMC FootPrints 12

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 FootPrints: 12.x

Network Considerations

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

<table>
<thead>
<tr>
<th>Outbound From</th>
<th>Inbound To</th>
<th>TCP Port #</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>BeyondTrust Middleware Engine Server</td>
<td>BMC FootPrints</td>
<td>443</td>
<td>API calls from the BeyondTrust Middleware Engine server.</td>
</tr>
<tr>
<td>BeyondTrust Middleware Engine Server</td>
<td>Secure Remote Access Appliance</td>
<td>443</td>
<td>API calls from the BeyondTrust Middleware Engine server.</td>
</tr>
<tr>
<td>Secure Remote Access Appliance</td>
<td>BeyondTrust Middleware Engine Server</td>
<td>8180 (default)</td>
<td>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.</td>
</tr>
<tr>
<td>Secure Remote Access Appliance</td>
<td>BeyondTrust Middleware Engine Server</td>
<td>443 (optional)</td>
<td></td>
</tr>
</tbody>
</table>

Prerequisite Installation and Configuration

The BMC FootPrints integration is a BeyondTrust Middleware Engine plugin.

For more information on installing and working with the BeyondTrust Middleware Engine, please see the BeyondTrust Remote Support Middleware Engine Installation and Configuration document at www.beyondtrust.com/docs/remote-support/how-to/integrations/middleware-engine.
Configure BMC FootPrints 12 for Integration with BeyondTrust Remote Support

Enable Web Services

1. Log into FootPrints as an admin user.
2. Click the Administration tab.
4. If not already checked, check the box to **Enable availability of external API**.

5. Click **Save** to enable the external API web services.

### Create an API User Account

1. Click the **Administration** tab.
2. Under **User Management**, click **Users**.

3. Click the **New** button to open the new user form.
4. Complete the form with the following settings:
   a. **Role**: System Administrator
   b. **License Type**: Fixed
   c. **Name**: BeyondTrust Integration (example only; actual value can be anything)
   d. **User ID**: BeyondTrust_integration (example only; actual value can be anything)
   e. **Authentication Method**: FootPrints
   f. **Password**: (Create a password)
   g. **Licensing**: (Uncheck the boxes for CMDB, Mobile, and Change Approvers)
5. Under **Assign Containers to User**, select the containers to which the integration applies and select **Agent** as the **Role** for each.

6. Click **Save** to create the API user account.
Configure BeyondTrust for the BMC FootPrints 12 Integration

Several configuration changes are necessary on the Secure Remote Access Appliance to integrate with BMC FootPrints 12. You must make these changes on each appliance for which you intend to create a plugin configuration, described in "Configure the BMC FootPrints 12 Plugin for Integration with BeyondTrust Remote Support" on page 11.

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

Verify 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.

2. Click Create New User and name it Integration or something similar.
3. Leave Must Reset Password at Next Login unchecked.
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 click Add to create a new API account.
2. Provide a name for the API account.
3. Under Permissions, check Full Access to the Command API.
4. For the Reporting API, check Allow Access to Support Session Reports and Recordings and Allow Access to Presentation Session Reports and Recordings.
5. Be sure to copy the values for both the OAuth Client ID and OAuth Client Secret for use in a later step.
6. Click Save to create the account.

Add an Outbound Event URL

1. Go to /login > Management > Outbound Events.
2. In the HTTP Recipients section, click Add 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. Click Save.
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.

Add a Custom Link

BeyondTrust custom links can be configured to allow representatives to quickly access the FootPrints item that is associated with the session.

**BeyondTrust 15.1 and later**

2. Click Add.
3. Enter a name for the link, and then set the URL to 
   https://support.example.com/files/BeyondtrustCustomLink.html?
   view=1&externalKey=%SESSION.CUSTOM.EXTERNAL_KEY%
   where support.example.com is your BeyondTrust site hostname.

   **Note:** The page referenced in the custom link URL does not yet exist but is created at the end of the section "Configure the BMC FootPrints 12 Plugin for Integration with BeyondTrust Remote Support" on page 11.

4. Click Save to save the new link.
Configure the BMC FootPrints 12 Plugin for Integration with BeyondTrust Remote Support

Now that you have configured BMC FootPrints 12 and the Secure Remote Access Appliance, deploy and configure the BMC FootPrints 12 plugin.

For more information on installing and working with the BeyondTrust Middleware Engine, please see the BeyondTrust Remote Support Middleware Engine Installation and 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 FootPrints Plugin shows in the list of plugins. Click the clipboard icon to add a new configuration.

Secure Remote Access Appliance

The first portion of the plugin configuration provides the necessary settings for communication between the plugin and the Secure Remote Access 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 Secure Remote Access Appliance. If outbound events are not being used, this value is still required, but any value may be used.
3. **Secure Remote Access Appliance Host Name:** The hostname of the Secure Remote Access 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 Secure Remote Access 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 Secure Remote Access 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 Secure Remote Access 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 Secure Remote Access Appliance and the middleware engine such that outbound events cannot be used, an alternative is to use polling. The middleware engine regularly polls the Secure Remote Access 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 Secure Remote Access 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 FootPrints 12 Instance**

The remainder of the plugin configuration provides the necessary settings for communication between the plugin and the BMC FootPrints 12 instance. The configuration settings include:
1. **BMC FootPrints 12 Services URL**: The external API services URL for the BMC FootPrints 12 instance (e.g., https://footprints.example.com/footprints/servicedesk/externalapioap/ExternalApiServicePort).

2. **BMC FootPrints 12 Username**: The username of the API account.

3. **BMC FootPrints 12 Password**: The password of the above user.

4. **BMC FootPrints 12 Reports Field Name**: The name of the field created on the incident form to display the BeyondTrust session reports (standard name is BeyondTrust Reports).

Save the configuration.

### Test Settings and Generate HTML Content

Once the proper configuration has been entered and saved, use the tool’s **Test this Plugin Configuration** function to verify the settings. In addition to verifying settings for both BeyondTrust and FootPrints, the page outputs several snippets of HTML that are used in the creation of the UI elements within FootPrints.

### 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 more information on Handlebars templates, please see handlebarsjs.com.
Finish Configuring BMC FootPrints 12 for Integration with BeyondTrust Remote Support

Customize Incident Form (Agent's View)

1. Click the Administration tab.
2. On the Main tab, select your workspace to edit it.
3. Select the Record Definitions menu item, and then select the Incident type.
4. Edit the **Incident** type by clicking the **Edit** button or double-clicking the item in the **Record Definitions** view.

5. Select the **Fields** menu item, and then click the **Add** button to add a new field.

6. Complete the new field form with the following settings:
   a. **Singular Name:** BeyondTrust Reports
   b. **Field Type:** Text area
   c. **Permissions:** Optional
   d. **Validation:** None
   e. **Value Length:** Any
   f. **View in List:** [Checked]
   g. **Searchable:** [Checked]
   h. **Journaling:** [Checked]
   i. **Auto Filter:** [Unchecked]

7. Click **Save** to create the new field.

8. Select the **Forms** menu item, select the **Agent Web** form, and then click the **Edit Form** button.
9. Add a new section named **BeyondTrust** with a 3 column layout.

10. Within the new section, add an HTML/Code Control to the left-most column.
11. Copy and paste the HTML content from **Step 1** of the generated content on the plugin test page as the **Code value**.
12. Set **HTML** as the **Content Type**.

13. Add another HTML/Code Control to the right-most column.
14. Copy and paste the HTML content from **Step 2** of the generated content on the plugin test page as the **Code value**.
15. Set **HTML** as the **Content Type**.
17. Set the Width to 3 columns.
18. Add a horizontal rule tag (<hr/>) as the Code value.
19. Set HTML as the Content Type.
20. Finally, on another new row, add the BeyondTrust Reports field control with a Width of 3 columns and a Height of 10 rows.

21. Once completed, the form should look similar to the screenshot.
22. Click Save to save the new section and form controls.

**Customize Incident Form (Customers’ View)**

1. While still editing the Incident type for the workspace, select and edit the Customer Web form from the Forms menu item.
2. Add an HTML/Code Control. If the form is still in the standard layout, the new control can be added in the column to the right of the Created On field. Otherwise, choose the desired location and add the field there.
3. Copy and paste the HTML content from Step 3 of the generated content on the plugin test page as the **Code value**.

4. Set **HTML** as the **Content Type**.

5. Once complete, the form should look similar to the screen shot.

6. Click **Save** to save the form with the new control.

7. Navigate back to the root of the workspace view (where you selected **Incident** from **Record Definitions** in a previous step) and click **Save and Publish** to publish all form changes in the current workspace.

---

**Note:** Repeat the steps in the above two sections for any additional workspaces with which the integration should work.

---

**Create Custom Link Page**

1. Create an empty text file using Notepad or another text editor and copy and paste the HTML content from Step 4 of the generated content on the plugin test page into the file.

2. Save the file as **BeyondTrustCustomLink.html**.

3. Log into the BeyondTrust /login interface and upload the file to the file store under **Public Portals > File Store**.
Use Cases for the BMC FootPrints 12 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.

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)
Jump to Configuration Item

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

Click-to-Chat for Self Service Users

Self Service users can open their submitted tickets and start a chat support session directly from the FootPrints 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 FootPrints and provides the representative with any available issue details, history, or other context to help quickly resolve the issue.