



BeyondTrust

Remote Support BMC FootPrints 11 Integration

Table of Contents

BeyondTrust Integration with BMC FootPrints 11	3
Prerequisites for the BeyondTrust Remote Support Integration with BMC FootPrints 11	4
Applicable Versions	4
Network Considerations	4
Prerequisite Installation and Configuration	4
Configure BMC FootPrints 11 for Integration with BeyondTrust Remote Support	5
Enable Web Services	5
Create an API User Account	5
Configure BeyondTrust for the BMC FootPrints 11 Integration	7
Verify That the API Is Enabled	7
Create an API Service Account - BeyondTrust 16.1 and Earlier	7
Create an API Service Account - BeyondTrust 16.2 and Later	8
Add an Outbound Event URL	8
Configure the BMC FootPrints 11 Plugin for Integration with BeyondTrust Remote Support	10
Secure Remote Access Appliance	10
BMC FootPrints 11 Instance	11
Test Settings and Generate HTML Content	12
Report Templates	12
Finish Configuring BMC FootPrints 11 for Integration with BeyondTrust Remote Support	13
Create BeyondTrust Form	13
Add the Generate Session Key Button	14
Add the Jump to Pinned Client Button	14
Add the Push and Start Local Button	15
Add the BeyondTrust Data Field	16
Publish the Form	16
Use Cases for the BMC FootPrints 11 Integration with BeyondTrust Remote Support	17
Generate Session Key	17
Import BeyondTrust Session Data into Ticket	17
Jump to Configuration Item	18

BeyondTrust Integration with BMC FootPrints 11

IMPORTANT!

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

Service desks and customer support organizations using BMC FootPrints 11 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 or perform a Local Jump. 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 11

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: 11.x

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 FootPrints	443	API calls from the BeyondTrust Middleware Engine server.
BeyondTrust Middleware Engine Server	Secure Remote Access Appliance	443	API calls from the BeyondTrust Middleware Engine server.
Secure Remote Access 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.

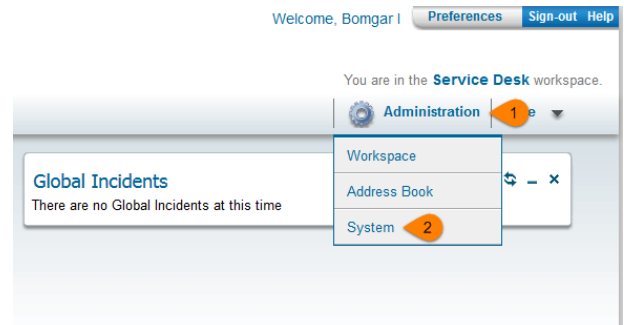
Prerequisite Installation and Configuration

The BMC FootPrints 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.

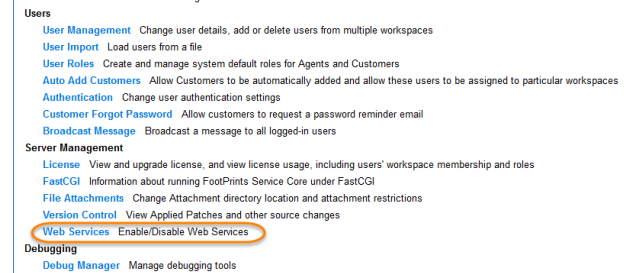
Configure BMC FootPrints 11 for Integration with BeyondTrust Remote Support

Enable Web Services

1. Log into FootPrints as an admin user.
2. Click **Administration > System**.

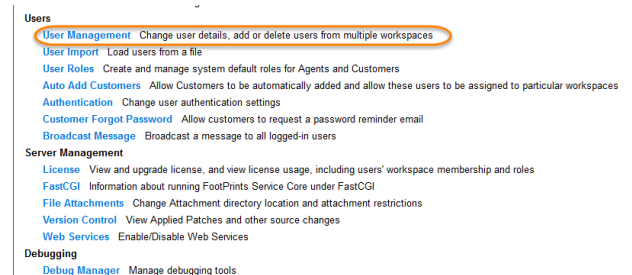


3. Under **Server Management**, click **Web Services**.
4. On the **Web Services Setup** screen, click the radio button next to **Enabled**.
5. Enter your password and click **Save** to enable web services.



Create an API User Account

1. Click **Administration > System**.
2. Under **Users**, click **User Management**.



3. Fill in all required fields, adding the user to the **Service Desk** workspace.
4. For the workspace **Role**, select **System Administrator**.
5. Click **Save** and enter your password to create the user.
6. Select the **Fixed** license type and click **Save** again.

Create or Edit User
Add Users to Workspaces

This interface allows you to add a new user or edit an existing user in a single or multiple Footprints Service Core workspaces. Select the radio button below corresponding to the action you wish to perform.

Create New User
 Edit User

Mandatory fields for all users

User ID

New Password New Password Again

Passwords properly match ✔

Fields for Agents only

Name Primary Email Address

Wireless Address Pager Address

Accessibility Enable If enabled, Footprints Service Core is optimized to be used with JAWS and other text-to-speech browsers.

Available Workspaces

- Change and Release M...
- Customer Support Wor...
- Problem Management
- Service Desk
- Service Portfolio

Selected Workspaces

- Service Desk

Default Workspace	Address Book	Role	Supervisor
Service Desk	Integration Address Book (1)	System Administrator	None

Configure BeyondTrust for the BMC FootPrints 11 Integration

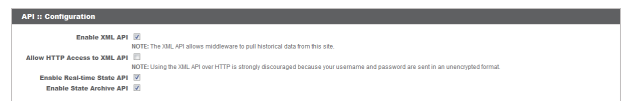
Several configuration changes are necessary on the Secure Remote Access Appliance to integrate with BMC FootPrints 11. You must make these changes on each appliance for which you intend to create a plugin configuration, described in "[Configure the BMC FootPrints 11 Plugin for Integration with BeyondTrust Remote Support](#)" on page 10.

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 Secure Remote Access 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.

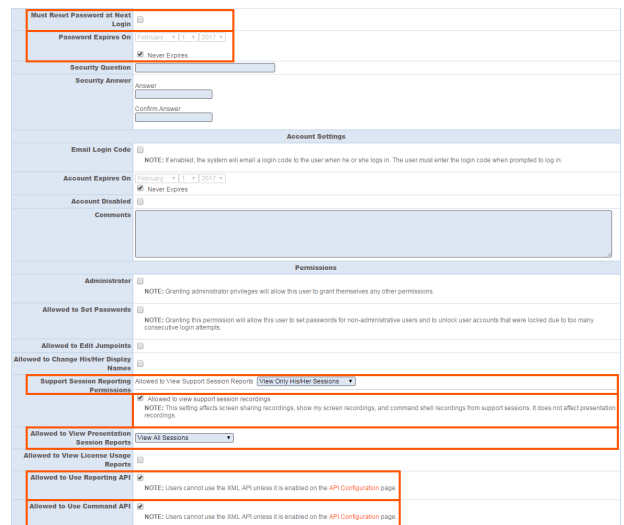
Go to **/login > Management > API Configuration** and verify that **Enable XML API** is checked.



Create an API Service Account - BeyondTrust 16.1 and Earlier

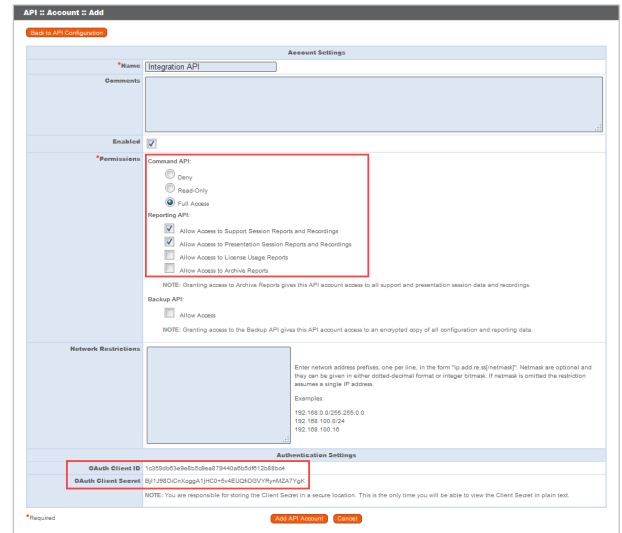
The API user account is used from within the integration to make BeyondTrust Command API calls to BeyondTrust.

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

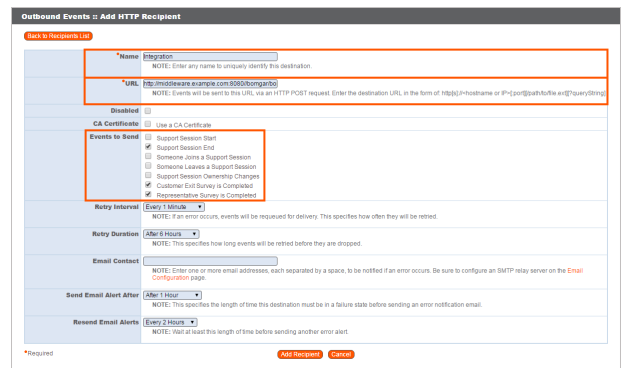
1. Go to **/login > Management > Outbound Events**.
2. Click **Add New HTTP Recipient** and name it **Integration** or something similar.
3. Enter the URL to use:

- 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**.



- 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.

Outbound Events :: HTTP Recipients						
Add New HTTP Recipient						
Configure up to 10 external HTTP servers that will be notified when certain session events occur. These servers must respond to each event with HTTP 200 in order to be considered successful.						
Name	Disabled	URL	Events to Send	Status	Actions	
Session Counter	Yes	http://bmc.example.com/session	Support Session Start	OK	Edit	Delete
Survey Page	Yes	http://bmc.example.com/survey	Customer Exit Survey is Completed Representative Survey is Completed	OK	Edit	Delete

Configure the BMC FootPrints 11 Plugin for Integration with BeyondTrust Remote Support

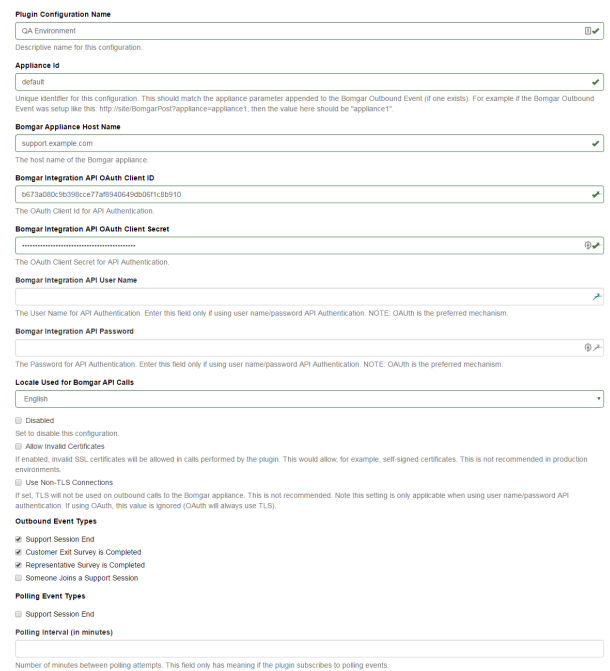
Now that you have configured BMC FootPrints 11 and the Secure Remote Access Appliance, deploy and configure the BMC FootPrints 11 plugin. For additional information about working with the BeyondTrust Middleware Engine, please see the [BeyondTrust Middleware Engine Configuration](http://www.beyondtrust.com/docs/remote-support/how-to/integrations/middleware-engine) 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.



Plugin Configuration Name
QA Environment

Appliance Id
default

Bomgar Appliance Host Name
support.example.com

Bomgar Integration API OAuth Client ID
5d73a300-3c38ace77a894d549b00f1c8910

Bomgar Integration API OAuth Client Secret

Bomgar Integration API User Name

Bomgar Integration API Password

Locale Used for Bomgar API Calls
English

Disabled
Set to disable this configuration.

Allow Invalid Certificates
If enabled, invalid SSL certificates will be allowed in calls performed by the plugin. This would allow, for example, self-signed certificates. This is not recommended in production environments.

Use Non-TLS Connections
If set, TLS will not be used on outbound calls to the Bomgar appliance. This is not recommended. Note this setting is only applicable when using user name/password API authentication. If using OAuth, this value is ignored (OAuth will always use TLS).

Outbound Event Types

- Support Session End
- Customer Exit Survey is Completed
- Representative Survey is Completed
- Someone Joins a Support Session


Polling Event Types

- Support Session End


Polling Interval (in minutes)
1

Number of minutes between polling attempts. This field only has meaning if the plugin subscribes to polling events.

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 11 Instance

The remainder of the plugin configuration provides the necessary settings for communication between the plugin and the BMC FootPrints 11 instance. The configuration settings include:

1. **BMC FootPrints 11 Services URL:** The MRWebServices URL for the BMC FootPrints 11 instance (e.g., `https://footprints.example.com/MRcgi/MRWebServices.pl`).
2. **BMC FootPrints 11 Username:** The username of the API account.
3. **BMC FootPrints 11 Password:** The password of the above user.



The screenshot shows a configuration form with three fields:

- BMC FootPrints 11 Services URL:** A text input field containing the URL `https://footprints.example.com/MRcgi/MRWebServices.pl`. Below it is a small text label: "The services URL for the BMC FootPrints 11 instance (ex: https://footprints.example.com/MRcgi/MRWebServices.pl)".
- BMC FootPrints 11 Username:** A text input field containing the username `api_user`. Below it is a small text label: "The username for API calls to the BMC FootPrints 11 instance".
- BMC FootPrints 11 Password:** A password input field with masked characters. Below it is a small text label: "The password for the user account for API calls to the BMC FootPrints 11 instance".

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, JavaScript, and CSS 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.



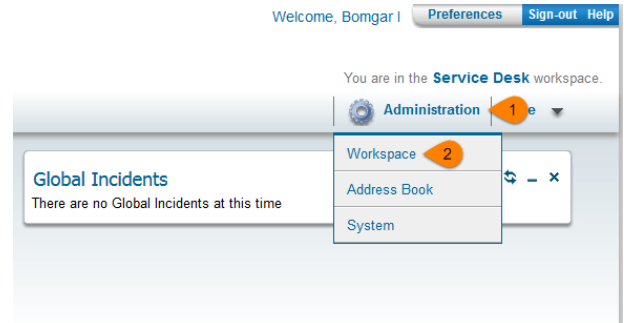
Note: *If changes need to be made to a template, it is a good idea to first back up the original in case the changes ever need to be reverted.*

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

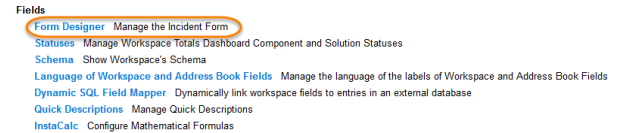
Finish Configuring BMC FootPrints 11 for Integration with BeyondTrust Remote Support

Create BeyondTrust Form

1. Click **Administration > Workspace**.

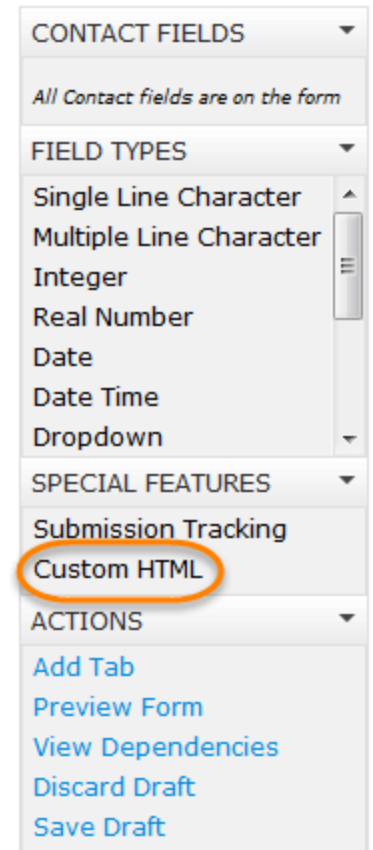


2. Under **Fields**, click **Form Designer**.
3. In the form designer, click the green plus symbol on the left side of the screen to create a new tab.
4. Give the new tab the title of **BeyondTrust**.
5. Click the button to select a **3 column layout**.



Add the Generate Session Key Button

1. From the **Special Features** menu located on the right side of the screen, drag a **Custom HTML** field to the first column in the editor.
2. In the Custom HTML dialog, configure the field with the following settings:
 - a. **Name:** Generate Session Key
 - b. **Width:** 1 column
 - c. **Rich Text Mode:** Unchecked
 - d. **Content:** See below



3. Return to the BeyondTrust Middleware Administration tool and go to the plugin test page. Select and copy the HTML in the section labeled **Step 2: FootPrints Assets**.
4. Paste the HTML into the **Content** section of the **Customer HTML** field.
5. Press **Enter** a few times to add some blank lines after the HTML you just pasted.
6. Select and copy the HTML from the next section of the plugin test labeled **Step 3: Generate Session Key**.
7. Paste the HTML into the **Content** section of the **Custom HTML** field at the end, after the previously pasted HTML.
8. Click **Save**.

Step 2: FootPrints Assets - Must be placed in the page BEFORE the first Bomgar button

```
<style type="text/css">
.bomgar-btn_ .bomgar-btn.hover {
background: #ff5722;
border: 1px solid #e14713;
border-radius: 4px;
font-size: 14px;
padding: 10px 16px;
color: #fff;
cursor: pointer;
display: inline-block;
```

Step 3: Generate Session Key

```
<a id="bomgar_link" class="bomgar-btn">Generate Session Key</a>
<script type="text/javascript">
var bgStuff = new BgFootprints("https://footprints.ps.bomgar.com/");
bgStuff.loadDataFromPage();
bgStuff.setGenerateSessionKeyOnClick(document.getElementById("bomgar_link"));
</script>
```

Add the Jump to Pinned Client Button

1. From the **Special Features** menu located on the right side of the screen, drag a **Custom HTML** field to the second column in the editor.

2. In the **Custom HTML** dialog, configure the field with the following settings:
 - a. **Name:** Jump to Pinned Client
 - b. **Width:** 1 column
 - c. **Rich Text Mode:** Unchecked
 - d. **Content:** See below
3. Return to the BeyondTrust Middleware Administration tool and go to the plugin test page. Select and copy the HTML in the section labeled **Step 4: Jump to Pinned Client**.
4. Paste the HTML into the **Content** section of the **Custom HTML** field.
5. Click **Save**.

Step 4: Jump to Pinned Client

```
<div class="combo-btn">
<input type="text" id="bg-searchstring" placeholder="Enter a search string..." onclick="this.select();" />
<a id="bomgar_jump" class="bomgar-btn">Jump To Pinned Client</a>
</div>
<script type="text/javascript">
var bgStuff = new BgFootprints("https://footprints.ps.bomgar.com");
bgStuff.loadDataFromPage();
bgStuff.setJumpToOnClick(document.getElementById('bomgar_jump'), document.getElementById('bg-searchstring'));
</script>
```

Add the Push and Start Local Button

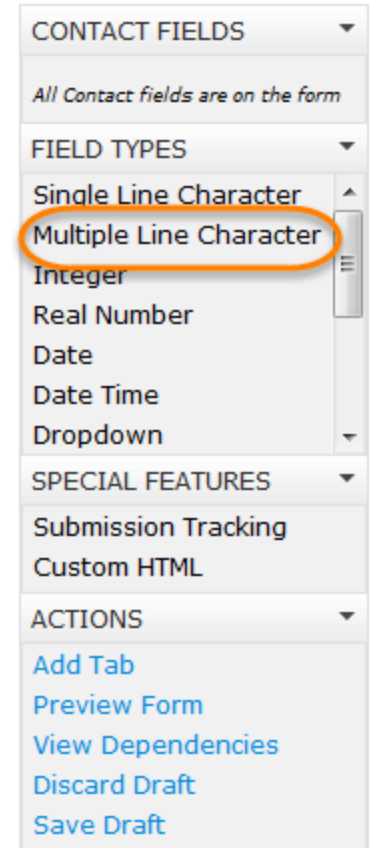
1. From the **Special Features** menu located on the right side of the screen, drag a **Custom HTML** field to the third column in the editor.
2. In the **Custom HTML** dialog, configure the field with the following settings:
 - a. **Name:** Push and Start Local
 - b. **Width:** 1 column
 - c. **Rich Text Mode:** Unchecked
 - d. **Content:** See below
3. Return to the BeyondTrust Middleware Administration tool and go to the plugin test page. Select and copy the HTML in the section labeled **Step 5: Push and Start Local**.
4. Paste the HTML into the **Content** section of the **Custom HTML** field.
5. Click **Save**.

Step 5: Push and Start Local

```
<div class="combo-btn">
<input type="text" id="bg-hostname" placeholder="Enter a hostname..." onclick="this.select();" />
<a id="bomgar_push_start_local" class="bomgar-btn">Push and Start Local</a>
</div>
<script type="text/javascript">
var bgStuff = new BgFootprints("https://footprints.ps.bomgar.com");
bgStuff.loadDataFromPage();
bgStuff.setPushStartLocalOnClick(document.getElementById('bomgar_push_start_local'), document.getElementById('bg-
</script>
```

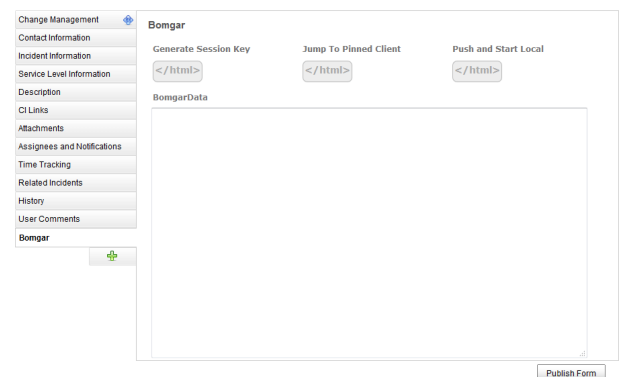
Add the BeyondTrust Data Field

- From the **Field Types** menu located on the right side of the screen, drag a **Multiple Line Character** field to the editor just below the buttons you just added.
- In the **Multiple Line Character** dialog, configure the field with the following settings:
 - Name:** BeyondTrustData
 - Length:** 30 rows
 - Add timestamp:** Checked
 - Width:** 3 columns
 - Input Size:** Long
 - Rich Text Mode:** Unchecked
- Click **Save**.



Publish the Form

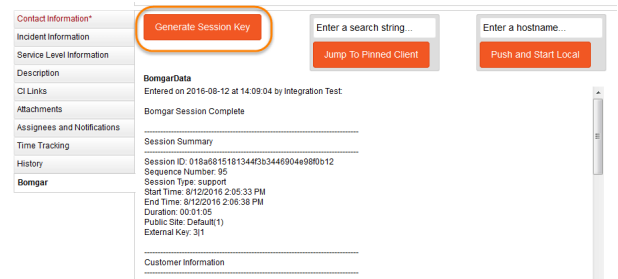
- When finished, the form should look similar to the screen shot.
- Click **Publish Form**.
- Click **Yes** when prompted to publish the form.



Use Cases for the BMC FootPrints 11 Integration with BeyondTrust Remote Support

Generate Session Key

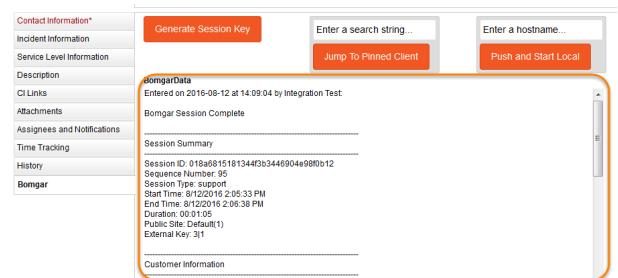
Support staff can generate a session key that can be given to the end user over the phone or via email to initiate a support session that is automatically associated with the selected ticket.



Import BeyondTrust Session Data into Ticket

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

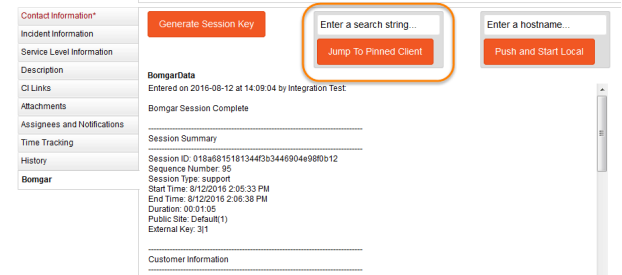
- **Chat Transcript** (including files transferred, special actions, and other events)
- **System Information** (the General section plus other select details such as disk, memory, and network)
- **Session Notes**
- **Surveys** (customer and representative)



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.

Jump to Pinned Client:



Push and Start Local:

