Remote Support

JIRA Integration
# Table of Contents

- BeyondTrust Remote Support Integration with JIRA Service Desk ........................................... 3
- Prerequisites  .............................................................................................................................. 4
  - Applicable Versions ..................................................................................................................... 4
- Configure JIRA Service Desk for Integration with BeyondTrust Remote Support ............... 5
- Configure BeyondTrust Remote Support for Integration with JIRA Service Desk .............. 7
  - Verify 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
  - Create a Custom Link .................................................................................................................. 9
- Configure the JIRA Service Desk Plugin for Integration with BeyondTrust Remote Support ................................................................. 10
  - Secure Remote Access Appliance ........................................................................................... 10
  - JIRA Service Desk Server Instance ........................................................................................ 11
  - Report Templates ....................................................................................................................... 12
- JIRA Service Desk and BeyondTrust Remote Support Use Cases ...................................... 13
  - Generate Session Key ............................................................................................................... 13
  - Import BeyondTrust Session Date into an Issue .................................................................... 13
  - Jump to Configuration Item ..................................................................................................... 14
  - User-Initiated Session on Existing Issue in Customer Portal ................................................. 14
  - Access an Issue from the Representative Console ............................................................... 14
  - Auto-Issue Creation .................................................................................................................. 15
BeyondTrust Remote Support Integration with JIRA Service Desk

IMPORTANT!

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

This document describes the installation and configuration of the BeyondTrust Remote Support and JIRA Service Desk Server integration. The integration consists of two main parts:

- **Middleware**: This receives event notifications from the Secure Remote Access Appliance and pushes data into JIRA Service Desk.
- **Service Desk add-on**: This modifies the JIRA Service Desk user interface with BeyondTrust components.

The JIRA Service Desk integration with BeyondTrust Remote Support provides the following functionality:

- A BeyondTrust session key can be generated from within a JIRA Service Desk issue.
- When the BeyondTrust session ends, session data is pushed into JIRA Service Desk and can be viewed from within the issue. Also, when the session ends, a work log entry can be created.
- An agent can type a machine name into a field on the screen and Jump to the device using BeyondTrust Jump technology.
- While in a BeyondTrust session, the representative can edit the external key and can associate the session with a particular JIRA Service Desk issue.
- Customers can request help on an existing issue via the JIRA Service Desk Customer Portal.
- Customers can request help outside of an existing issue via the JIRA Service Desk Customer Portal. When the session starts, an issue is created automatically in JIRA Service Desk.
- A custom link in the BeyondTrust representative console can be used to open an issue in JIRA Service Desk.
Prerequisites

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

Applicable Versions

- BeyondTrust Remote Support: 15.x and later
- JIRA Service Desk Server: 3.2 and later

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>JIRA Service Desk Server</td>
<td>443</td>
<td>JIRA Service Desk REST API calls.</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) 443 (optional)</td>
<td>The BeyondTrust Middleware Engine server receives outbound events from the appliance. However, if polling is used instead of outbound events, this port does not have to be open.</td>
</tr>
</tbody>
</table>

Prerequisite Installation and Configuration

The JIRA Service Desk 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](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](http://www.beyondtrust.com/docs/remote-support/how-to/integrations/middleware-engine).
Configure JIRA Service Desk for Integration with BeyondTrust Remote Support

Configuration of JIRA Service Desk for the integration with BeyondTrust Remote Support consists of installing the add-on and using the add-on’s configuration screen to customize the behavior.

To install the add-on:

1. Log into JIRA Service Desk as an administrator.
2. Under the JIRA Administration menu, choose Add-ons.
3. Click Manage add-ons.
4. Click Upload add-on.
5. Browse to and select the provided add-on .jar file.

To configure the add-on:

1. From the Add-ons screen, expand the BeyondTrust Enterprise Remote Support Integration add-on section.
2. Click Configure.
3. There are four tabs to configure:
   - On the General tab, enter the hostname of the Secure Remote Access Appliance.
   - On the Agent View tab, select whether to show the BeyondTrust Session Key button as a menu item or as a button. Also, select which Jump Options to show.
On the Customer Portal Request View tab, enable, disable, and/or customize the ways a user can start a BeyondTrust session on an existing issue. This can be configured individually for each JIRA Service Desk.

On the Customer Portal View tab, enable, disable, and customize the ways a user can start a BeyondTrust session outside of an existing issue (auto issue creation). This can be configured individually for each JIRA Service Desk.
Configure BeyondTrust Remote Support for Integration with JIRA Service Desk

Several configuration changes are necessary on the Secure Remote Access Appliance.

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.

![Note: The Someone Joins a Support Session event is optional. This event is needed when using auto issue creation functionality.]

**Create a Custom Link**

Under Rep Console > Custom Links, create a new custom link:

**URL:** https://<jira server>/browse/%SESSION.CUSTOM.EXTERNAL_KEY%

![Note: In the URL above, replace <jira server> with the hostname of your JIRA Service Desk Server instance.]
Configure the JIRA Service Desk Plugin for Integration with BeyondTrust Remote Support

Now that you have configured JIRA Service Desk and the Secure Remote Access Appliance, deploy and configure the JIRA Service Desk 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. Unzip 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 JIRA Service Desk 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.

    **Note**: If using polling, this integration is not able to push customer exit survey data into Service Desk.

### JIRA Service Desk Server Instance

The remainder of the plugin configuration provides the necessary settings for communication between the plugin and the JIRA Service Desk instance. The configuration settings include:

- **JIRA Service Desk URL**: The services URL for the JIRA Service Desk instance (e.g., https://myjiraserver.domain.net/). If the JIRA Service Desk instance has a context path, please include it (e.g.,
https://myjiraserver.domain.net/jira/).

- **JIRA Service Desk Username** - User that can connect to JIRA Service Desk. This user needs to be an administrator of the service desk(s).
- **JIRA Service Desk Password** - Password for above user.
- **Update Work Log** - If enabled, a work log entry is created at the end of the support session in the associated JIRA Service Desk issue.
- **BeyondTrust rep field used to map to JIRA Service Desk user** - This is used for auto issue creation. The integration takes this value and attempts to find a corresponding JIRA Service Desk user. This value must match a JIRA username, display name, or email address.
- **Assign Issue to Rep on Issue Creation** - If enabled, when an issue is auto-created, it is assigned to the representative working the session.

### Report Templates

On the BeyondTrust Middleware Engine server, in the `<install dir>`\Plugins\<integration>\Templates folder, there are multiple files ending with ".hbs." The templates can be edited to suit the needs of each client. Please note that the JIRA Service Desk integration only uses the `WorkLog.hbs` file from the distribution.

---

**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.

---

**i** For more information on Handlebars templates, please see [handlebarsjs.com](http://handlebarsjs.com).
JIRA Service Desk and BeyondTrust Remote Support Use Cases

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 issue.

Import BeyondTrust Session Date into an Issue

On the support session ends, the issue is automatically updated with information gathered during the session.

- Summary
- Customer
- Rep(s)
- Chat
- File Transfers
- Session Notes
- Recording Links
- Exit Surveys (Customer and Rep)
Jump to Configuration Item

Support staff can Jump to a machine from the Service Desk issue. Please note JIRA Service Desk does not have a configuration item type functionality, so the machine name must be typed in manually. The following Jump types are available:

- Pinned Jump Client
- Local Jump
- Remote Jump
- RDP
- Shell Jump

User-Initiated Session on Existing Issue in Customer Portal

Users can open submitted issues and start a chat support session directly from the Service Desk issue. This provides the rep with necessary context to assist the user, while also providing the user a quick resolution. If enabled and when necessary, sessions can be elevated to full remote support sessions.

Access an Issue from the Representative Console

Using BeyondTrust's Custom Links ability, a representative can access an associated issue directly from within the rep console. This saves time when searching for the issue in Service Desk and provides the rep with any issue details, history, or other context needed to help quickly resolve the issue.
Auto-Issue Creation

For previously unreported issues or questions, the end user can submit a simple issue description to immediately begin a support session. Meanwhile, the integration takes the submitted information from the session and creates a new Service Desk issue. This saves time and unnecessary steps for the end user and support staff.