# Table of Contents

BeyondTrust Remote Support Integration with Microsoft Dynamics 365 .......................... 3

Prerequisites for the BeyondTrust Remote Support Integration with Microsoft Dynamics 365 .......................................................... 4

- Applicable Versions ................................................................................. 4
- Network Considerations ......................................................................... 4
- Prerequisite Installation and Configuration ........................................ 4

Configure Microsoft Dynamics 365 for Integration with BeyondTrust Remote Support .......................... 5

Configure API Access with Azure AD .......................................................... 6

- Configure Permissions for the Application Account ............................. 6

Configure BeyondTrust Remote Support for Integration with Microsoft Dynamics 365 ................... 8

- Verify the API Is Enabled ....................................................................... 8
- Create an OAuth API Account ................................................................. 8
- Add an Outbound Event URL ................................................................ 9

Configure the Microsoft Dynamics 365 Plugin for Integration with BeyondTrust Remote Support ........................................................................ 11

- BeyondTrust Appliance B Series ............................................................ 11
- Microsoft Dynamics 365 Instance .......................................................... 12

Use Cases for the Microsoft Dynamics 365 Integration with BeyondTrust Remote Support .......................................................... 14

- Generate Session Key ........................................................................... 14
- Import BeyondTrust Session Data into Ticket ....................................... 14
BeyondTrust Remote Support Integration with Microsoft Dynamics 365

IMPORTANT!

You must purchase this integration separately for both your Remote Support software and your Microsoft Dynamics 365 solution. For more information, contact BeyondTrust sales.

Service desks and customer support organizations using Microsoft Dynamics 365 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 Microsoft Dynamics 365.

The Microsoft Dynamics 365 integration with BeyondTrust Remote Support provides the following functionality:

- A BeyondTrust session key can be generated from within a Microsoft Dynamics 365 case.
- When the BeyondTrust session ends, session data can be pushed into the case and viewed from within the case.

The integration consists of two main parts:

- Middleware which receives event notifications from the BeyondTrust Appliance B Series and pushes data into Microsoft Dynamics 365
- Two Microsoft Dynamics 365 solutions which provide customization to the Microsoft Dynamics 365 user interface
Prerequisites for the BeyondTrust Remote Support Integration with Microsoft Dynamics 365

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

Applicable Versions

- BeyondTrust Remote Support: 19.2 and newer
- Microsoft Dynamics 365

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>Microsoft Dynamics 365</td>
<td>443</td>
<td>API calls from the BeyondTrust Middleware Engine server.</td>
</tr>
<tr>
<td>BeyondTrust Middleware Engine Server</td>
<td>BeyondTrust Appliance B Series</td>
<td>443</td>
<td>API calls from the BeyondTrust Middleware Engine server.</td>
</tr>
<tr>
<td>BeyondTrust Appliance B Series</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, then this port does not have to be open.</td>
</tr>
</tbody>
</table>

Prerequisite Installation and Configuration

The Microsoft Dynamics 365 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 Microsoft Dynamics 365 for Integration with BeyondTrust Remote Support

Configuration within Microsoft Dynamics 365 consists of installing two custom solutions:

2. Ensure the appropriate environment is selected.
3. In the left menu, click Solutions.
4. Click Import.
5. From the Import a Solution pop-up, click Browse and select the provided BeyondTrust_1_x_managed.zip. Click Next.
6. When presented with Solution Information, click Import.
7. When the solution is finished importing, click Publish All Customizations.
8. Repeat the above steps to import the BeyondTrustButton_1_x_managed.zip file.
9. In the list of solutions, open the BeyondTrust Remote Support solution.
10. Open the resource in the list named bt_/javascripts/LaunchModalDialog.js.
11. Click the Text Editor button. In the editor, find the line that begins with var hostname = and change to the appropriate hostname for the Remote Support appliance. Click OK when done.
12. Click Save, and then click Publish.
Configure API Access with Azure AD

Within the Azure AD Tenant, you must create an app registration and bind an application user account to that registered app. Follow the instructions in the section titled Connect as an app in the following Microsoft guide:

Note: After creating the registration, you will create a client secret under Certificates & Secrets in the app registration. This secret will be leveraged by the integration when you configure the Middleware plugin.

Configure Permissions for the Application Account

Once you have created the app registration, custom security role, and application account, the final step is to give the account the appropriate permissions within Dynamics 365.

2. Select your environment.
3. Click Settings at the top to view the environment settings menu page.
4. Expand Users + permissions and select Security roles.
5. From the list of Security Roles, select the role created in the previous section.
6. Click the **Edit** link at the top.
7. On the **Service** tab, scroll down to the **Case** entity and assign the role **Read** and **Append To** permissions at **Organization** level (click multiple times to change to the appropriate level).

8. On the **Custom Entities** tab, scroll down to the entities that begin with **BeyondTrust** and assign all permissions at **Organization** level for these **BeyondTrust** entity types.

9. Click **Save and Close** at the top to save the new permissions.
Configure BeyondTrust Remote Support for Integration with Microsoft Dynamics 365

Several configuration changes are necessary on the BeyondTrust Appliance B Series to integrate with Microsoft Dynamics 365. 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 B Series 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 OAuth API Account

The Microsoft Dynamics 365 API account is used from within Microsoft Dynamics 365 to make Remote Support Command API calls to Remote Support.

1. In /login, navigate to Management > API Configuration.
2. Click Add.
3. Check **Enabled**.
4. Enter a name for the account.
5. **OAuth Client ID** and **OAuth Client Secret** is used during the OAuth configuration step in Microsoft Dynamics 365.
6. Under **Permissions**, check the following:
   - Command API: **Full Access**.
   - Reporting API: Allow Access to Support Session Reports and Recordings, and Allow Access to Presentation Session Reports and Recordings.
7. Click **Save** at the top of the page 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. The list of outbound events contains 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 Microsoft Dynamics 365 Plugin for Integration with BeyondTrust Remote Support

Now that you have configured Microsoft Dynamics 365 and the BeyondTrust Appliance B Series, deploy and configure the Microsoft Dynamics 365 Plugin.

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 Microsoft Dynamics 365 Plugin shows in the list of plugins. Click the clipboard icon to add a new configuration.

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.

BeyondTrust Appliance B Series

The first portion of the plugin configuration provides the necessary settings for communication between the plugin and the B Series 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 B Series Appliance. If outbound events are not being used, this value is still required, but any value may be used.
3. **BeyondTrust Appliance B Series Host Name**: The hostname of the B Series Appliance. Do not include https:// or other URL elements.
4. **BeyondTrust Integration API OAuth Client ID**: The client ID of the OAuth account.
5. **BeyondTrust Integration API OAuth Client Secret**: The client secret of the OAuth account.
6. **Locale Used for BeyondTrust API Calls**: This value directs the B Series Appliance to return session data in the specified language.
7. **Disabled**: Enable or disable this plugin configuration.
8. **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. We do not recommend this in production environments.
9. **Use Non-TLS Connections**: Leave unchecked unless it is the specific goal to use non-secure connections to the B Series 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. We strongly discourage using non-secure connections.

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

10. **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.

   - Support Session End
   - Customer Exit Survey is Completed
   - Representative Survey is Completed

11. **Polling Event Types:** If network constraints limit connectivity between the B Series Appliance and the middleware engine such that outbound events cannot be used, an alternative is to use polling. The middleware engine regularly polls the B Series 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.

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

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

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

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

**Microsoft Dynamics 365 Instance**

The remainder of the plugin configuration provides the necessary settings for communication between the plugin and the Microsoft Dynamics 365 instance. The configuration settings include:

1. **Microsoft Dynamics 365 URL:** URL of the Microsoft Dynamics 365 instance.
2. **Azure AD Tenant ID:** The Tenant ID of the Azure instance.
3. **Azure AD App Registration ID:** The ID of the app registration created for this integration.
4. **Azure AD App Registration Client Secret:** The client secret created under the app registration.
5. **Update Microsoft Dynamics 365 with all BeyondTrust sessions:** If enabled, all BeyondTrust sessions are imported into Microsoft Dynamics 365.
6. **List of Allowed Microsoft Dynamics 365 Prefixes:** If desired, enter a comma-separated list of allowed Microsoft Dynamics 365 prefixes (e.g., ABC, CBA). Only BeyondTrust sessions related to these prefixes are imported.
Note: If Update 365 with all BeyondTrust sessions is checked, the value in this field is ignored.

7. **Import Timestamp as UTC:** If enabled, any datetime values are imported as UTC times. If not enabled, datetime values are imported using the local time zone.

After saving the configuration, click the test icon next to the new plugin configuration. No restart is needed.
Use Cases for the Microsoft Dynamics 365 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 case.

Import BeyondTrust Session Data into Ticket

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

- General Information
- Chat Transcript (including files transferred, special actions, and other events)
- Session Events
- System Information (General section)
- Session Notes
- Surveys (customer and representative)