Remote Support
Microsoft Dynamics CRM Integration
# Table of Contents

- **BeyondTrust Remote Support Integration with Microsoft Dynamics CRM** .......................... 3
- **Prerequisites for the BeyondTrust Remote Support Integration with Microsoft Dynamics CRM** ........................................... 4
  - Applicable Versions ............................................................................. 4
  - Network Considerations ...................................................................... 4
  - Prerequisite Installation and Configuration ......................................... 4
- **Configure Microsoft Dynamics CRM for Integration with BeyondTrust Remote Support** ................................................................. 5
- **Configure BeyondTrust Remote Support for Integration with Microsoft Dynamics CRM** ................................................................. 6
  - Verify the API Is Enabled .................................................................... 6
  - Create an API Service Account - BeyondTrust 16.1 and Earlier ............... 6
  - Create an API Service Account - BeyondTrust 16.2 and Later .................. 7
  - Add an Outbound Event URL ................................................................. 7
- **Configure the Microsoft Dynamics CRM Plugin for Integration with BeyondTrust Remote Support** ......................................................... 9
  - Secure Remote Access Appliance ......................................................... 9
  - Microsoft Dynamics CRM Instance ....................................................... 10
- **Use Cases for the Microsoft Dynamics CRM Integration with BeyondTrust Remote Support** ............................................................. 12
  - Generate Session Key ......................................................................... 12
  - Import BeyondTrust Session Data into Ticket ....................................... 12
BeyondTrust Remote Support Integration with Microsoft Dynamics CRM

IMPORTANT!

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

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

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

- A BeyondTrust session key can be generated from within a Microsoft Dynamics CRM 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 Secure Remote Access Appliance and pushes data into Microsoft Dynamics CRM.
- Two Microsoft Dynamics CRM solutions which provide customization to the Microsoft Dynamics CRM user interface.
Prerequisites for the BeyondTrust Remote Support Integration with Microsoft Dynamics CRM

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: 14.x and newer
- Microsoft Dynamics CRM: 2016

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 CRM</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) 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 CRM 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 CRM for Integration with BeyondTrust Remote Support

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

1. Log into Microsoft Dynamics CRM as an administrator.
2. Expand the menu next to Microsoft Dynamics CRM and click Settings.
3. Under Customization, click Solutions.
4. Click Import.
5. From the Import Solution popup, click Choose File and select the provided bomgar_1_1.zip. Click Next.
6. When presented with Solution Information, click Next.
7. When presented with Import Options, leave the Post Import Action selected and click Import.
8. When the solution is finished importing, click Publish All Customizations.
9. Repeat the above steps to import the Support Button zip file. The only difference is that there is no Import Options step.
10. In the list of solutions, open the BeyondTrust solution.
11. Open the resource in the list that starts with bom_/javascripts/LaunchModalDialog.
12. Click the Text Editor button. In the editor, find the line that begins with var hostname = and change to the appropriate hostname. Click OK when done.
13. Click Save, and then click Publish.
Configure BeyondTrust Remote Support for Integration with Microsoft Dynamics CRM

Several configuration changes are necessary on the Secure Remote Access Appliance to integrate with Microsoft Dynamics CRM. 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.
Configure the Microsoft Dynamics CRM Plugin for Integration with BeyondTrust Remote Support

Now that you have configured Microsoft Dynamics CRM and the Secure Remote Access Appliance, deploy and configure the Microsoft Dynamics CRM 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 Microsoft Dynamics CRM 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.

**Microsoft Dynamics CRM Instance**

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

1. **Microsoft Dynamics CRM URL**: URL of the Microsoft Dynamics CRM instance.
2. **Microsoft Dynamics CRM Domain**: Domain of the Microsoft Dynamics CRM instance.
3. **Microsoft Dynamics CRM User Name**: Username used to connect to Microsoft Dynamics CRM.
4. **Microsoft Dynamics CRM Password**: Password of the above user.
5. **Update Microsoft Dynamics CRM with all BeyondTrust sessions**: If enabled, all BeyondTrust sessions are imported into Microsoft Dynamics CRM.

6. **List of Allowed Microsoft Dynamics CRM Prefixes**: If desired, enter a comma-separated list of allowed Microsoft Dynamics CRM prefixes (e.g., ABC, CBA). Only BeyondTrust sessions related to these prefixes are imported.

```
Note: If Update CRM 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 CRM 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)