Table of Contents

BeyondTrust Remote Support Integration with CA Service Desk .................................................. 3
Prerequisites for the BeyondTrust Remote Support Integration with CA Service Desk ........ 4
  Applicable Versions .................................................................................................................. 4
  Network Considerations .......................................................................................................... 4
  Prerequisite Installation and Configuration .............................................................................. 4
Configure CA Service Desk for Integration with BeyondTrust Remote Support .................... 5
  Create New Tables .................................................................................................................. 5
  Implement Web Customizations ............................................................................................... 7
  Add Web UI Elements .............................................................................................................. 9
Configure BeyondTrust for the CA Service Desk Integration ................................................ 13
  Verify the API Is Enabled ....................................................................................................... 13
  Create an OAuth API Account ................................................................................................. 13
  Add an Outbound Event URL ................................................................................................. 14
Configure the CA Service Desk Plugin for Integration with BeyondTrust Remote Support ........ 16
  BeyondTrust Appliance B Series ............................................................................................ 16
  CA Service Desk Instance ...................................................................................................... 17
  Report Templates .................................................................................................................... 18
Use Cases for the CA Service Desk 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
  Auto-Ticket Creation .............................................................................................................. 20
BeyondTrust Remote Support Integration with CA Service Desk

IMPORTANT!

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

Service desks and customer support organizations using CA Service Desk 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 CA Service Desk.

The integration between CA Service Desk and BeyondTrust Remote Support enables you to initiate a request for a support session from within your support portal as an analyst or employee, providing secure remote support capabilities for your end user community. Additionally, all aspects of the remote support session can be captured directly within your CA Service Desk support ticket, offering information to the analyst and end user in order to properly diagnose, troubleshoot, and resolve user issues.
Prerequisites for the BeyondTrust Remote Support Integration with CA Service Desk

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: 19.2 and later
- CA Service Desk: 17.x (plus any associated cumulative patches and test fixes)

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>CA Service Desk</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 CA 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 document at www.beyondtrust.com/docs/remote-support/how-to/integrations/middleware-engine.
Configure CA Service Desk for Integration with BeyondTrust Remote Support

**IMPORTANT!**

Before beginning the installation, please ensure you have backed up your CA Service Desk primary and secondary servers.

Create New Tables

1. Open the **Web Screen Painter** and log in as an administrator.
2. From within the Web Screen Painter, open **Tools > Schema Designer**.
3. Select **Add Table**, and create a table named **z_bomgar_session**.
4. Click **OK**.
5. The table info should now be displayed. Fill in the form with the following information:
   - **Name**: z_bomgar_session
   - **Display Name**: BeyondTrust Session
   - **Schema Name**: z_bomgar_session
   - **Description**: Fac_Attr_Entry z_bomgar_session
   - **Default Display Field**: bgr_session_id
   - **Foreign Key Field**: id
6. Click **Save**.
7. After creating and saving the table with the required basic information, click **Add Column** to add the following columns to the table:

<table>
<thead>
<tr>
<th>Schema Name</th>
<th>Display Name</th>
<th>Field Type</th>
<th>SREL Table or Length</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>analyst</td>
<td>analyst</td>
<td>SREL</td>
<td>SREL Table: cnt</td>
<td>No</td>
</tr>
<tr>
<td>bgr_session_id</td>
<td>bgr_session_id</td>
<td>String</td>
<td>100</td>
<td>Yes</td>
</tr>
</tbody>
</table>
### Table 1: Schema, Display Name, Field Type, SREL Table or Length, Required

<table>
<thead>
<tr>
<th>Schema Name</th>
<th>Display Name</th>
<th>Field Type</th>
<th>SREL Table or Length</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>cr_persid</td>
<td>cr_persid</td>
<td>SREL</td>
<td>SREL Table: cr</td>
<td>Yes</td>
</tr>
<tr>
<td>end_date_time</td>
<td>end_date_time</td>
<td>Date</td>
<td>n/a</td>
<td>Yes</td>
</tr>
<tr>
<td>recording_url</td>
<td>recording_url</td>
<td>String</td>
<td>1000</td>
<td>No</td>
</tr>
<tr>
<td>session_duration</td>
<td>session_duration</td>
<td>Duration</td>
<td>n/a</td>
<td>No</td>
</tr>
<tr>
<td>start_date_time</td>
<td>start_date_time</td>
<td>Date</td>
<td>n/a</td>
<td>No</td>
</tr>
<tr>
<td>support_session_detail</td>
<td>support_session_detail</td>
<td>String</td>
<td>30000</td>
<td>Yes</td>
</tr>
</tbody>
</table>

8. Once all columns have been created, select **File > Save and Publish**. When prompted to continue, click **Yes**.

9. Once again, select **Add Table**, and create a table named **zbgr_connection_type**.

10. Click **OK**.

11. The table info should now be displayed. Fill in the form with the following information:
   - **Name**: zbgr_connection_type
   - **Display Name**: BeyondTrust Connection Type
   - **Schema Name**: zbgr_connection_type
   - **Description**: Fac_Attr_Entry zbgr_connection_type
   - **Default Display Field**: connection_name
   - **Foreign Key Field**: id

12. Click **Save**.

13. After creating and saving the table with the required basic information, click **Add Column** to add the following columns to the table:

<table>
<thead>
<tr>
<th>Schema Name</th>
<th>Display Name</th>
<th>Field Type</th>
<th>SREL Table or Length</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>connection_name</td>
<td>Connection_name</td>
<td>String</td>
<td>100</td>
<td>Yes</td>
</tr>
<tr>
<td>default_connection_type</td>
<td>Default_connection_type</td>
<td>Integer</td>
<td>n/a</td>
<td>No</td>
</tr>
<tr>
<td>delete_flag</td>
<td>SRel_Attr_Entry zbgr_connection_type.delete_flag</td>
<td>SREL</td>
<td>SREL Table: Actbool</td>
<td>No</td>
</tr>
<tr>
<td>Description</td>
<td>Description</td>
<td>String</td>
<td>250</td>
<td>Yes</td>
</tr>
<tr>
<td>zjumpoint_required</td>
<td>Zjumpoint_required</td>
<td>SREL</td>
<td>SREL Table: bool (Boolean)</td>
<td>No</td>
</tr>
</tbody>
</table>

14. Once all columns have been created, select **File > Save and Publish**. When prompted to continue, click **Yes**.

15. Navigate to the **nr** table within Schema Designer.

16. Select **Add Column** and add the following fields to this table:

<table>
<thead>
<tr>
<th>Schema Name</th>
<th>Display Name</th>
<th>Field Type</th>
<th>SREL Table or Length</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>zbgr_conn_type</td>
<td>zbgr_conn_type</td>
<td>SREL</td>
<td>SREL Table: zbgr_connection_type</td>
<td>No</td>
</tr>
<tr>
<td>zbgr_jpoint</td>
<td>zbgr_jpoint</td>
<td>String</td>
<td>200</td>
<td>No</td>
</tr>
</tbody>
</table>
17. Once all columns have been created, select **File > Save and Publish**. When prompted to continue, click **Yes**.
18. Ensure all users are out of the system, and then shut down CA Service Desk services on all servers.
19. Open an administrative command prompt window and run the command **pdm_publish**.

**Implement Web Customizations**

1. If not already stopped, stop CA Service Desk services.
2. Browse to the directory where CA Service Desk is installed (e.g., C:\Program Files (x86)\CA\Service Desk Manager).
3. Copy the components package (CA_Service_Management_Integration_Components.zip) to the primary server and extract the contents to \**patches**.

**Note:** The **patches** folder is not created during CA Service Desk installation and may need to be manually created.

4. Locate **detail_in.html** in \**patches**\CA_Service_Management_Integration_Components\CA_ServiceDesk_FrontEnd_Code\site\mods\www\httmpl\web\analyst and open the file in a text editor such as Notepad.
5. Open **detail_in.html** in \**site\mods\www\httmpl\web\analyst** in a text editor.

**Note:** If you have not previously customized your Analyst Incident interface, you will not find a **detail_in.html** file located in \**site\mods\www\httmpl\web\analysts**. In this case, you need to copy the **detail_in.html** file from \**bopcfg\www\httmpl\web\analyst\** to \**site\mods\www\httmpl\web\analyst**.

6. Within the first file, from the **patches** folder, there are six code snippets that must be copied to the corresponding location in the second file. These snippets are surrounded by lines which read `<!-- Integral Customization -- Start -->` and `<!-- Integral Customization -- End -->`. Copy the code between those lines and paste them in the same locations in the second file.

**Note:** Do NOT copy the "Start" and "End" lines.

7. Save the file when complete.

**IMPORTANT!**

*If you have multiple Analyst type form groups, make sure to apply the changes to each **detail_in.html** form located in each respective Analyst type form group. An Analyst type form group is any sub-folder underneath \**site\mods\www\httmpl\web\analyst**.*
8. Copy the following files from `\patches\CA_Service_Management_Integration_Components\CA_ServiceDesk_FrontEnd_Code\site\mods\www\http\web\analyst` to `\site\mods\www\http\web\analyst`:
   - `detail_z_bomgar_session.html`
   - `detail_zbgr_connection_type.html`
   - `list_z_bomgar_session.html`
   - `list_zbgr_connection_type.html`

9. Repeat steps 4-7 above but for `cmdb_detail.html` in `\patches\CA_Service_Management_Integration_Components\CA_ServiceDesk_FrontEnd_Code\site\mods\www\http\web\employee` as the source file and `\site\mods\www\http\web\employee` as the destination. There should be two snippets that must be copied and placed in the destination file.

10. Repeat steps 4-7 above but for `nr_cmdb Harvard_worx_tab.html` in `\patches\CA_Service_Management_Integration_Components\CA_ServiceDesk_FrontEnd_Code\site\mods\www\http\web\analyst` as the source file and `\site\mods\www\http\web\employee` as the destination. There should be one snippet that must be copied and placed in the destination file.

11. Repeat steps 4-7 above but for `detail_in.html` in `\patches\CA_Service_Management_Integration_Components\CA_ServiceDesk_FrontEnd_Code\site\mods\www\http\employee` as the source file and `\site\mods\www\http\web\employee` as the destination. There should be three snippets that must be copied and placed in the destination file.

12. Copy `start_session.js` from `\patches\CA_Service_Management_Integration_Components\CA_ServiceDesk_FrontEnd_Code\site\mods\www\http\root\scripts`.

13. Copy `Bomgar.png` from `\patches\CA_Service_Management_Integration_Components\CA_ServiceDesk_FrontEnd_Code\site\mods\www\http\root\img` to `\site\mods\www\http\root\img`.

14. Open `\ns.env` in a text editor and add the following line: `@NX_bomgar_HOST=<BeyondTrust_Host>` where `<BeyondTrust_Host>` is the hostname of your BeyondTrust site (e.g., support.example.com).

15. Start the CA Service Desk Manager services.

16. Open an administrative command prompt window, change directories to `\patches\CA_Service_Management_Integration_Components\CA_ServiceDesk_FrontEnd_Code`, and run the command to load data into the `zbgr_connection_type` table: `Pdm_load -f zbgr_connection_type.txt`.

17. Verify that all files copied in this section have been copied to each primary and secondary server. Log into each primary and secondary CA Service Desk server and verify that the web changes in this section have been replicated in the following files in these locations:
   - `\site\mods\www\http\web\analyst`
     - `detail_in.html`
     - `detail_z_bomgar_session.html`
     - `detail_zbgr_connection_type.html`
     - `list_z_bomgar_session.html`
     - `list_zbgr_connection_type.html`
   - `\site\mods\www\http\web\employee`
     - `detail_in.html`
   - `\site\mods\www\http\root\scripts`
     - `start_session.js`
   - `\site\mods\www\http\root\img`
     - `Bomgar.png`
Add Web UI Elements

1. Log into CA Service Desk as an administrator.
2. Go to Administration > Security and Role Management > Role Management > Menu Trees.
3. Within the Menu Trees list, select admin_tree.

**Note:** If your admin tree is already customized, skip steps 4-6 and select your custom admin tree.

4. Select File > Copy.
5. Fill in the following values:
   a. **Menu Tree Name:** custom_admin_tree
   b. **Code:** cat
   c. **Internal:** No
   d. **Description:** Administration Tree
6. Fill in the following values:
   a. **Menu Tree Name:** custom_admin_tree
   b. **Code:** cat
   c. **Internal:** No
   d. **Description:** Administration Tree
7. Click Save.

8. Select Customize Menu.

9. Within ServiceDesk > Application Data > Codes, right-click Codes and click Create New Node.

10. Create a new node with the following information:
    a. **Node Name**: BeyondTrust Connection Type
    b. **Resource**: BeyondTrust Connection Type

   **Note**: If you do not have a BeyondTrust Connection Type resource, follow step 11 to create one. Otherwise, skip to step 12 once you have saved the record.

11. Click Save.
12. Click **Save**.

13. To create a new resource, click the blue **Resource** link, and select the **Create New** button from the displayed screen. Fill in the following information to create the BeyondTrust Connection Type resource:
   - **Name**: BeyondTrust Connection Type
   - **Description**: BeyondTrust Connection Type
   - **Resource**: OP=SEARCH+FACTORY=zbgr_connection_type+QBE.EQ.delete_flag=0

SALES: www.beyondtrust.com/contact  SUPPORT: www.beyondtrust.com/support  DOCUMENTATION: www.beyondtrust.com/docs

©2003-2021 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

TC: 9/27/2021
14. Go to Administrator > Security and Role Management > Role Management > Tabs.
15. Click on Administration tab with full menu.
16. Select the Administration link from the starting page and edit the Administration Web Form.
17. Modify the Resource section to add the following to the end of the existing value: +KEEP.tree_code=cat.
18. Restart the CA Service Desk services.
Configure BeyondTrust for the CA Service Desk Integration

Several configuration changes are necessary on the BeyondTrust Appliance B Series to integrate with CA Service Desk. You must make these changes on each appliance for which you intend to create a plugin configuration, described in “Configure the CA Service Desk Plugin for Integration with BeyondTrust Remote Support” on page 16.

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 CA Service Desk API account is used from within CA Service Desk 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 CA Service Desk.

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 CA Service Desk Plugin for Integration with BeyondTrust Remote Support

Now that you have configured CA Service Desk and the BeyondTrust Appliance B Series, deploy and configure the CA Service Desk 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 CA Service Desk 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.

**CA Service Desk Instance**

The remainder of the plugin configuration provides the necessary settings for communication between the plugin and the CA Service Desk instance. The configuration settings include:
1. **CA Service Desk Services URL:** The services URL for the CA Service Desk instance (e.g., https://caservicedesk.example.com/axis/services/USD_R11_WebService)

2. **CA Service Desk Username:** The username of the API account.

3. **CA Service Desk Password:** The password of the above user.

4. **Enable Automatic Incident Creation on Session Start (Rejoins session):** If checked, the plugin processes `support_conference_member_added` events and the external key to determine whether to create a ticket within CA Service Desk or not. The plugin attempts to create the ticket only if this setting is enabled, if the conference member joining the conference is a representative, and if the external key is either a JSON string or the literal value `CHAT`.

5. **Enable Automatic Incident Creation on Session End:** If checked, the plugin processes `support_conference_end` events as usual but also examines the external key to determine whether to create a ticket within CA Service Desk or not. The plugin attempts to create the ticket only if this setting is enabled and if the external key is empty, is a JSON string, or is the literal value `CHAT`. If the external key is any other value, it is assumed to be a valid ticket ID, and the session is processed as usual (i.e., no ticket is created).

6. **Ticket Default Data:** A JSON string containing values that can be used to prepopulate certain fields on the newly created ticket.

After saving the configuration, click the test icon next to the new plugin configuration. No restart is needed.

**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 the Handlebars website at handlebarsjs.com.**
Use Cases for the CA Service Desk 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 Service Desk ticket. The following Jump types are available:

- **Jump Client** (Pinned Client)
- **Local Jump** (Push and Start Local)
- **Remote Jump** (Push and Start Remote)
- **Remote Desktop Protocol** (RDP)
- **Shell Jump** (Remote Console)

Click-to-Chat for Self Service Users

Self Service users can open their submitted tickets and start a chat support session directly from the Service Desk 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.

Auto-Ticket Creation

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