



BeyondTrust

Remote Support HaloPSA or HaloITSM Integration

Table of Contents

BeyondTrust Remote Support Integration with HaloPSA or HaloITSM	3
BeyondTrust Remote Support / HaloPSA Benefits	3
Use Case	3
Problem	3
Solution	3
Integration Overview	3
Prerequisites	4
Halo Requirements	4
Create Client ID and Client Secret in Remote Support	5
Configure Remote Support in HaloPSA	7
Add HaloPSA Webhook to Remote Support	11
Send Invitations and Link Sessions	13
Live Chat	13
Ticket Details	14
Actions	14
New Ticket	15
Link Session	15
Custom Button to Open the Device Automatically	16

BeyondTrust Remote Support Integration with HaloPSA or HaloITSM

BeyondTrust Remote Support enables you to remotely access and fix nearly any device, running any platform, located anywhere in the world. Support professionals can work on multiple systems simultaneously, chat with multiple end-users at once, and work with other reps in the same session to fix problems faster.

With the BeyondTrust Remote Support / HaloPSA or HaloITSM integration, users can streamline support and improve performance. End users are able to initiate Remote Support via the self-service portal for quick resolutions. Support technicians are able to launch a secure remote support session from a ticket to immediately start resolving issues. This enables an increase in first call resolution rates, shortens ticket response times and negates the need for on-site visits.

BeyondTrust Remote Support / HaloPSA Benefits

- Automatic updates to the ticket to provide detailed analysis and visibility.
- Support technicians can remotely support multi-platforms such as laptops, desktops, POS systems, kiosks and more.
- Secure remote support from any browser with no downloads required.
- Track performance and log session activity for security, compliance and training.
- Choose from on-premise and cloud deployment.

Use Case

Problem

An employee isn't receiving any emails and thinks his Outlook has stopped working. He tries to resolve this himself however the Knowledge Base articles can't help him. Therefore, he raises a ticket in HaloPSA so someone from the support team can help him.

Solution

The ticket is picked up by the support team. They run initial checks but can't see what the problem is and realize they need to access the employees computer. With the Remote Support / Autotask, The support team can start a remote session from within HaloPSA. They let the employee know and click on the link within the ticket. They can then easily solve the issue remotely and the employee's emails work again.

Integration Overview

This guides provides details of the following steps to create and use the integration:

- Review Prerequisites
- Create Client ID and Client Secret in Remote Support.
- Configure Remote Support in HaloPSA or HaloITSM.
- Add HaloPSA or HaloITSM Webhook to Remote Support
- Using the HaloPSA or HaloITSM with Remote Support.

This guide refers to HaloPSA, but the instructions also apply to HaloITSM.

Should you need any assistance, please log into the [Customer Portal](https://beyondtrustcorp.service-now.com/csm) at <https://beyondtrustcorp.service-now.com/csm> to chat with Support.

Prerequisites

A supported version of BeyondTrustRemote Support is required. To confirm your version is supported, contact support or refer to the [BeyondTrust End of Life Policy](https://www.beyondtrust.com/eos-eol) at <https://www.beyondtrust.com/eos-eol>.

Halo Requirements

Application	Minimum Version
Halo Service Desk	v2.06
HaloITSM	v2.06
HaloPSA	v2.06
HaloCRM	v2.06
NHServer	v12.78.38

Create Client ID and Client Secret in Remote Support

Follow these steps to create a new API account in Remote Support, and generate a new Client ID and Client Secret.

1. Go to **/login > Management > API Configuration**.
2. Click **Enable XML API**.
3. Click **Add** to create a new API account. Name it *HaloPSA* or something similar.
4. Set **Command API** to **Full Access**.
5. Under **Reporting API**, check **Allow Access to Support Session Reports and Recording**.
6. Under Configuration API, check **Allow Access**.
7. Make a note of the **OAuth Client ID** and **OAuth Client Secret** and store this information in secure location. These are used later in configuring the integration.
8. Click **Save**.

- Status
- Consoles & Downloads
- My Account
- Configuration
- Jump
- Vault
- Console Settings
- Users & Security
- Reports
- Public Portals
- Reports
- Public Portals
- Reports
- Public Portals
- Reports
- Public Portals
- Reports
- Localization
- Management

Management

SOFTWARE SECURITY SITE CONFIGURATION EMAIL CONFIGURATION OUTBOUND EVENTS FAILOVER API CONFIGURATION

Q

CANCEL
SAVE

ADD AN API ACCOUNT

• Required field

Enabled

Name •

Comments

OAuth Client ID

OAuth Client Secret

⚠ You are responsible for storing the Client Secret in a secure location. This is the only time you will be able to view this Client Secret in plain text.

PERMISSIONS

At least one permission must be enabled for an API account.

<p style="font-size: 0.8em; margin: 0;">Command API</p> <p><input type="radio"/> Deny</p> <p><input type="radio"/> Read-Only</p> <p><input checked="" type="radio"/> Full Access</p>	<p style="font-size: 0.8em; margin: 0;">Reporting API</p> <p><input checked="" type="checkbox"/> Allow Access to Support Session Reports and Recordings</p> <p><input type="checkbox"/> Allow Access to Presentation Session Reports and Recordings ⚠</p> <p><input type="checkbox"/> Allow Access to License Usage Reports</p> <p><input type="checkbox"/> Allow Access to Archive Reports ⓘ</p> <p><input type="checkbox"/> Allow Access to Vault Account Activity Reports</p> <p><input type="checkbox"/> Allow Access to Syslog Reports</p>	<p style="font-size: 0.8em; margin: 0;">Backup API</p> <p><input type="checkbox"/> Allow Access ⓘ</p> <p><input type="checkbox"/> Allow Vault Encryption Key Access ⓘ</p>
<p style="font-size: 0.8em; margin: 0;">Configuration API</p> <p><input type="checkbox"/> Allow Access</p> <p><input type="checkbox"/> Manage Vault Accounts</p>	<p style="font-size: 0.8em; margin: 0;">Real-Time State API</p> <p><input type="checkbox"/> Allow Access</p>	<p style="font-size: 0.8em; margin: 0;">Endpoint Credential Manager API</p> <p><input type="checkbox"/> Allow Access</p>

Configure Remote Support in HaloPSA

There are two places which you can enable the Remote Support integration in Halo.

- You can go to **Configuration > Integrations**.
- You can go to the Remote Support module, and enable it from within here. This is the recommended method, as configuration changes are required here regardless of where the integration is enabled.

Follow these steps to install and configure the Remote Support app in HaloPSA:

1. Log in to HaloPSA, and go to the report support module.
2. Navigate to **General Settings**.
3. Select *General User* as the **Default User**. Most remote session data either matches a Live Chat or a Ticket ID, which almost always has a corresponding user assigned. If you are using Live Chat on the end-user portal on the login screen, the chat is not linked to a user. Also, if you are accepting remote session data from remote sessions that weren't generated from Halo, then there is no associated user. It is in these circumstances that the remote session data is linked to the default user specified here.
4. Check **Allow Agents to invite Users to Remote Sessions for other Agents**. This allows agents to invite users to remote sessions for agents other than themselves, or one of the configured BeyondTrust teams. There is more information about this below.
5. Check **Allow Agents to send quick Remote Session invites from the Ticket screen** if this is desired. This option should not be checked if you want to force technicians to use a specific action to send the invites, or if you are restricting who has the ability to send the invites.

General Settings

Default User

Remote Sessions that do not have a valid User will be saved against this User.

- Allow Agents to invite Users to Remote Sessions for other Agents
- Allow Agents to send quick Remote Session invites from the Ticket screen

6. Scroll down to **Remote Session Invitations** and set these options:
 - **Canned Text for Remote Session Invitations for email template** This variable is \$REMOTEINVITE. If you are using this variable in one of your templates, use either the \$LINKTOREMOTE or \$REMOTESSESSIONCODE variables so that a code/URL for the remote session gets populated. You do not need to use \$REMOTEINVITE in your templates – you can just use \$LINKTOREMOTE or \$REMOTESSESSIONCODE directly in the email template should you wish to do so.
 - **Email and Live Chat Templates** Below the \$REMOTEINVITE option, you configure the email and live chat templates. The email template loads the usual email template editor screen that you should be familiar with. The Live Chat invitation works differently. You must enter the HTML manually, as shown below.

This template will be used when inviting Users to join a Remote Session via Live Chat. It should contain the variable \$LINKTOREMOTE, which will be replaced with a URL generated by your chosen Remote Support Integration.

We would like to have a remote session to look at this issue with you.

 Please click here and select Download Remote Support and run the file.

7. Go the BeyondTrust module in your Halo instance.
8. The first set of options is **Setup**.
9. Enter the **Application URL**, *https://your-domain.beyondtrustcloud.com*.
10. Enter the **Client ID**, and **Client Secret**. These are **OAuth Client ID** and **OAuth Client Secret** obtained from BeyondTrust Remote Support.
11. Click Test Configuration to ensure the information entered is correct.

Setup



Application URL

A Client ID and Client Secret are required to generate and retrieve Session Keys/Remote Session URLs from Beyond Trust. You can obtain these values by creating an API account on the Login > Management > API Configuration page in Beyond Trust.

Client ID

Client Secret

Test Configuration

12. Go to the Teams and Agents options.
13. Enable the integration for any Agent who you would like to use it, and assign their BeyondTrust display name to their Agent account. This must be done per agent by going to the **Configuration > Agents > Choose Agent > Details** tab.

Teams and Agents



Session Keys/URLs can be generated for any Agent that is logged in to the Beyond Trust console. This feature can be enabled for each Agent on the details tab of the Agent Configuration screen in HaloPSA.

To detect when an Agent is logged in to the Beyond Trust console, the Agent's Beyond Trust username is also required.

View Agents

Beyond Trust

Allow Beyond Trust Session Keys/URLs to be generated for this Agent

Yes

Beyond Trust Display Name

Administrator



Note: The BeyondTrust username field is used for matching when session details are sent to Halo. The name field must match the Agents public or private display name value set in BeyondTrust, otherwise the session data will not be processed.

14. Configuring Teams is optional, but we recommend configuring at least one team.
15. Teams can be added manually by clicking **Add**, or imported from BeyondTrust by clicking **Get Teams**.
16. The list of teams shows the name of the team in BeyondTrust, the name displayed to Halo users, and status information.
17. Below the **Get Teams** button (not shown below), there is an option to generate a session for the default team if the chosen agent is not available. This means that instead of failing and returning an *Agent Unavailable* message when the chosen Agent is not logged into BeyondTrust, a remote session code/URL is generated for the default team.

Users can be invited to join a queue for Remote Support for different Teams in Beyond Trust. Teams can be added manually, or imported from Beyond Trust below.

Beyond Trust Teams

Name	Display Name	Default	Enabled	
General	General	No	No	
Team A	Team A	Yes	No	
Team B	Team B	No	Yes	

Add

Previous

Page 1 of 1

Next

18. To edit a team, click the pencil icon.
19. The display name of the team can be changed, if desired.

20. We recommend one team be selected as the default team. The default team is used in multiple scenarios, such as if no Team or Agent is chosen when sending a remote invite, or the chosen Agent is not available. With no default Team chosen, the \$REMOTELINK and \$REMOTESSESSIONCODE variables are blank. Selecting a default team provides Halo with a fallback option to generate a new remote session code/URL.
21. Each team must be enabled.

Add Teams



Name

Team B

Display Name

Default

Enabled

Save

Cancel

Add HaloPSA Webhook to Remote Support

The last stage of integrating HaloPSA and BeyondTrust Remote Support is to create an outbound event, or webhook, in Remote Support. Follow these steps:

1. In HaloPSA, view the Remote Session Data and note the outbound event URL.
2. Below the highlighted URL, there is an option that, when enabled, only allows the Halo API to process requests from BeyondTrust when the remote session code/URL for that session was generated in Halo. Regardless, the Halo API only processes requests from BeyondTrust when the remote session was attended by a technician that exists in Halo. The matching process looks at the Public, Private and Display name of the technicians who attended the session in BeyondTrust, and looks for a match against an Agent name in Halo.

Remote Session Data ^

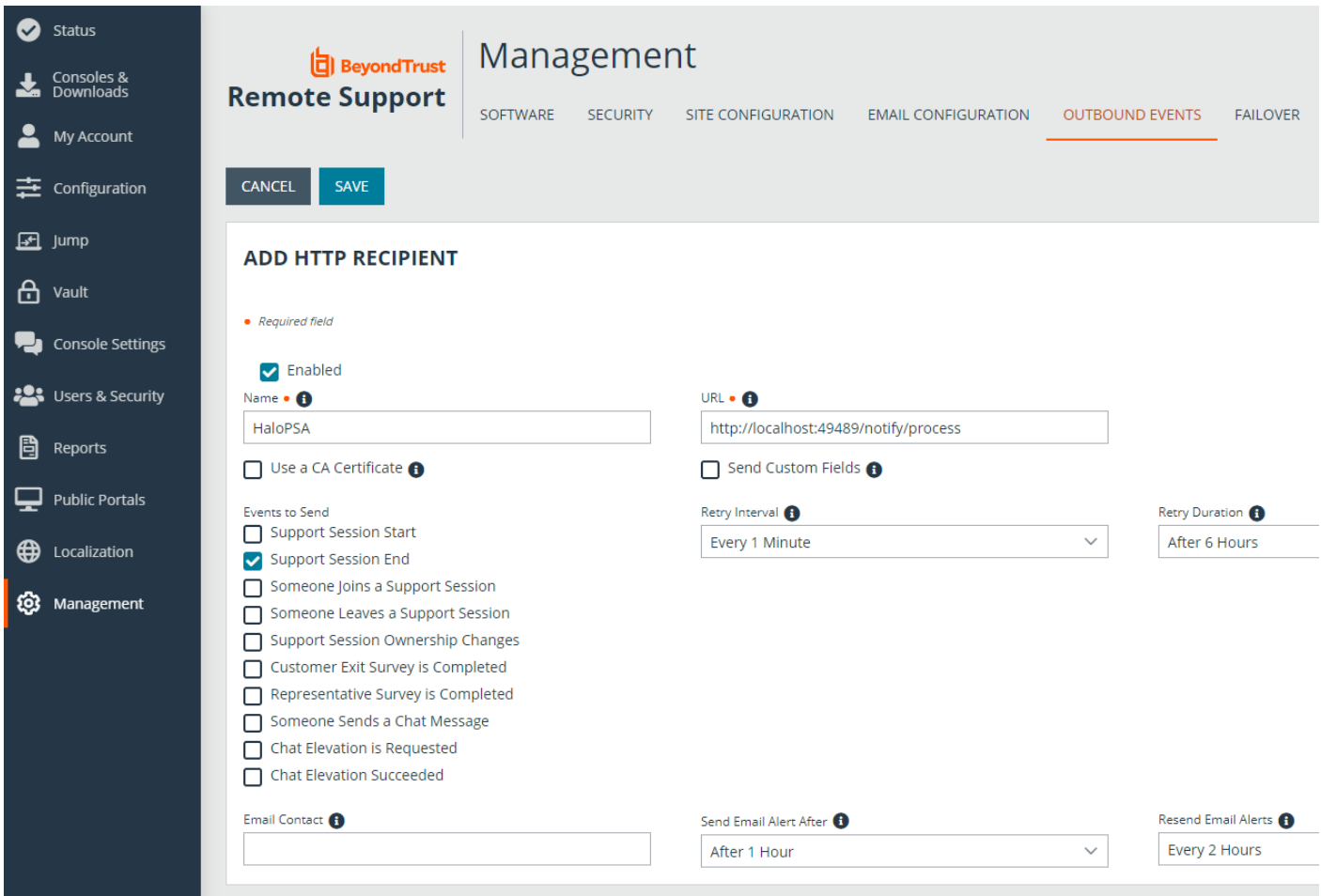
Details from a Remote Session can be sent from Beyond Trust to Halo Service Desk. If the invitation to the Remote Session was sent from Halo Service Desk, an Action will automatically be added to the Ticket from which the invitation was sent.

To enable this functionality, add an Outbound Event in Beyond Trust for the Support Session End event and for the following URL:

`http://localhost:49489/notify/process`

Only accept Remote Session Data from Beyond Trust if the session was generated from Halo Service Desk

3. In BeyondTrust Remote Support, click **Management** on the left menu.
4. Click the **Outbound Events** tab.
5. Click **Add** under **HTTP Recipients**.
 - Enter a name for the event.
 - Paste the copied Webhook URL to the **URL** field.
 - Check **Support Session End** under **Events to send**
 - Click **Save**.



Management

SOFTWARE SECURITY SITE CONFIGURATION EMAIL CONFIGURATION **OUTBOUND EVENTS** FAILOVER

CANCEL SAVE

ADD HTTP RECIPIENT

Required field

Enabled

Name

URL

Use a CA Certificate

Send Custom Fields

Events to Send

- Support Session Start
- Support Session End
- Someone Joins a Support Session
- Someone Leaves a Support Session
- Support Session Ownership Changes
- Customer Exit Survey is Completed
- Representative Survey is Completed
- Someone Sends a Chat Message
- Chat Elevation is Requested
- Chat Elevation Succeeded

Retry Interval

Retry Duration

Email Contact

Send Email Alert After

Resend Email Alerts

Once configured, every time a support session ends in BeyondTrust, a request is sent to the Halo API with the details of this request.

If the request is accepted, one of the following events occurs:

- If the session is linked to a ticket, then the remote session details are automatically added to the ticket as an action. The chat log from the session is added as the note of the action.
- If the session is linked to a live chat which is linked to a ticket, then the remote session details are added to the ticket as described above.
- If the session is linked to a live chat which is not linked to a ticket, and the live chat is still open, then the chat log from the remote session is added to the live chat as a message. It is also stored so you can link it to a ticket manually if you wish. If the chat has ended, then the remote session data is also stored so it can be appended to a ticket manually.
- In all other cases, the remote session data is stored so it can be appended to a ticket manually.

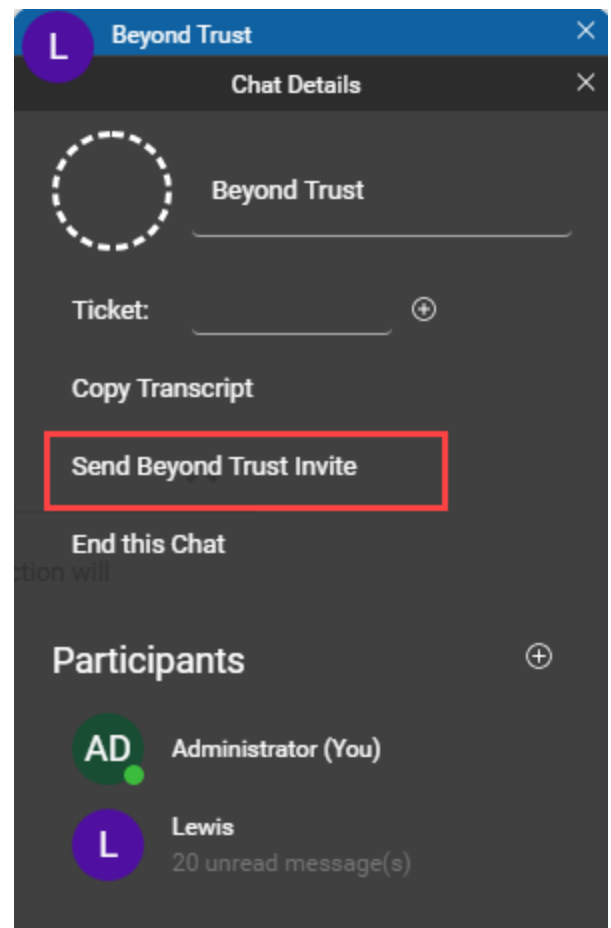
Send Invitations and Link Sessions

There are three ways to send Remote Session invitations:

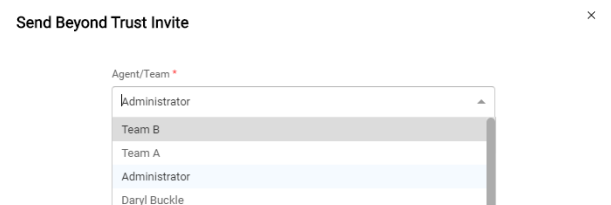
- live chat
- from the ticket details
- automatically with a new ticket

Live Chat

On the chat details page of a chat window, there is an option to send a BeyondTrust invite.



Clicking this option opens a window that allows you to choose which technician or team you would like to send the invite for. This list is all agents who have access to the integration, along with any teams you have configured. The option you choose here is used to generate the URL/code for the remote session. This means that if you chose Administrator, then when the user follows the URL, they will be placed into Administrator's private queue in BeyondTrust. Click save on this screen to post the message to the chat.



If the invitation is successful, a tick mark appears next to the button, and you can switch back to the main chat windows to view this. Should the invitation fail for any reason, an X appears next to the button, along with an error message explaining what failed.

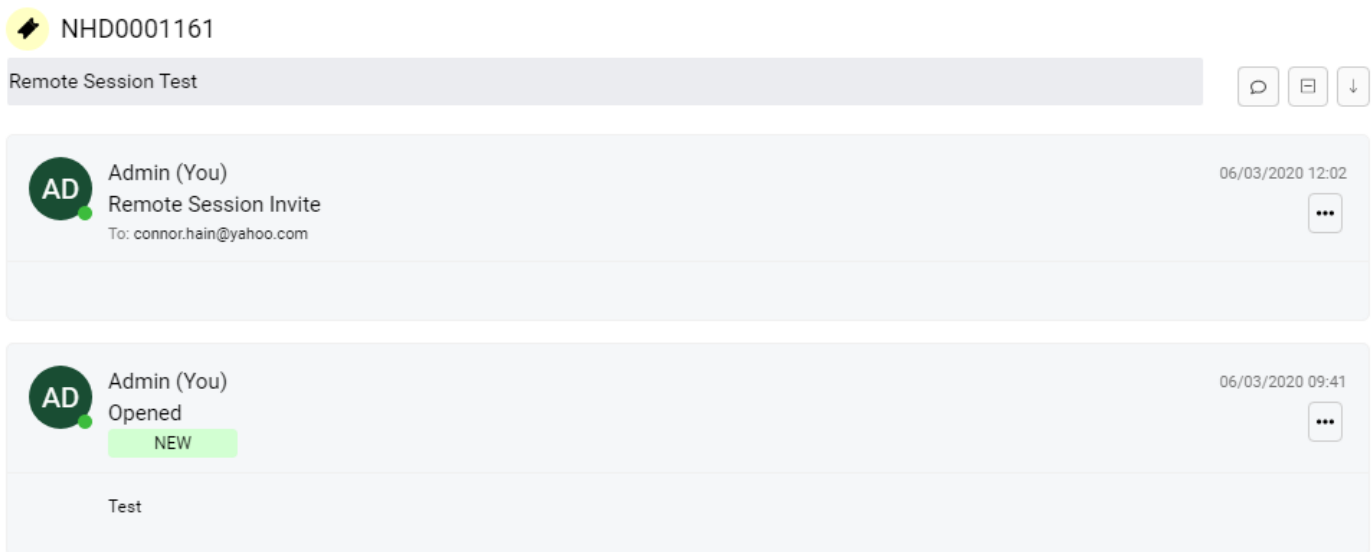
If the technician is not logged in to BeyondTrust and you have not chosen to automatically switch to the default team, then you see a TECHUNAVAILABLE message next to the invite button. Try again and send the invite to a different agent or team.

When the session ends, if your live chat is still active and you have correctly configured the Outbound Event in BeyondTrust, the details of the remote session are posted to the chat for both you and the user to see.

Ticket Details

The second option is from within the ticket itself, without using a configured action. If you open a ticket, and hover over the three dots in the top right corner, you will see an option for **Send Beyond Trust Invite**. Click this option to open a screen allowing you to choose who the session should be generated for, and also an email address to send the invite too.

Once you have submitted this, an action is added for audit purposes, so that it is clear the invitation was sent.



NHD0001161

Remote Session Test

Admin (You) Remote Session Invite
To: connor.hain@yahoo.com
06/03/2020 12:02

Admin (You) Opened
NEW
06/03/2020 09:41

Test

When the session data is sent back to Halo, the content of this is added to the ticket as an action for the technician who took the session. Should you wish to disable this option, please review general configuration for HaloPSA.

Actions

You can create a specific action that uses the Remote Invitation Template to send the invite. To do this, go to the action configuration screen and set the system use for your chosen action to **Remote Session Invitation**.

Then go to the field list tab, and add the **Remote Session Technician/Channel** field. This field allows you to choose which technician or team the invite should be generated for. If you don't want to use this field, or if the value is left blank, then Halo will use the default Team, if you have one specified. If not, then the email will be sent without a url/code.

When the session data is sent back to Halo, the content of this is added to the ticket as an action for the technician who took the session.

New Ticket

The final option available to you is to automatically send the invite when a new ticket is logged. You can specify this at request type level, on the defaults tab.

Send Remote Session Invitation

 ✕ ▾

On the end user portal, if this field is set to send an invite by default, an invitation is always sent when the user logs a ticket of this type. The default team is used to generate a code/URL. It is recommended to combine the new ticket template with the remote support template if you are using this functionality. This invitation will be added as a system action to the ticket.





In addition to this, there are a couple of fields that can be made visible on the Agent new ticket screen that allow you to choose each time whether to send the invite, and which technician or team the invite should be generated for. To configure this, on the field list tab, add the following two fields:

Remote Session Technician/Channel

Send Remote Session Invitation

Fields

The following Fields or Groups of Fields will be available for this Ticket Type.
[Click here](#) to add or modify Field Groups.*

Remote Session Technician/Channel	 
Send Remote Session Invitation	 



The **Send Remote Session Invitation** field defaults to the default value specified for the ticket type. If the invitation is sent, it gets added as an action for the technician who is logging the ticket. When the session data is sent back to Halo, the content of this is added to the ticket as an action for the technician who took the session.

Link Session

There are a few scenarios where a remote session may not link to a ticket. In these scenarios, the data is still saved to the Halo database, but the details must be manually linked to a ticket.

To do this, open a ticket and hover over the three dots in the top right-hand corner of the ticket. There is an option for **Link Remote Session**. Click this option to open a search screen.

The name of the remote session is set to the name of the chat it was generated from, if the name was set. Otherwise, it displays as **Remote Session**, as shown below.



Remote Session

Admin

26/02/2020 16:26

Batley Refreshments/Reason Avenue/Connor Hain

You can choose one remote session at a time to link to the ticket. When confirming the session, the details of this session are added as an action to the ticket.

Custom Button to Open the Device Automatically

You can create a custom button by going to **Configuration > Custom Objects > Custom Buttons > adjust the entity to Asset > Create a new Custom button.**

Use the following URL to automatically open the device in BeyondTrust. Replace [YourBeyondTrust] with your BeyondTrust URL.

```
https://[YourBeyondTrust]/api/client_script?type=rep&operation=generate&action=start_pinned_client_session&search_string=${INVENTORY_NUMBER}
```

Should you need any assistance, please log into the [Customer Portal](https://beyondtrustcorp.service-now.com/csm) at <https://beyondtrustcorp.service-now.com/csm> to chat with Support.