



BeyondTrust

BeyondInsight and Password Safe Secure Remote Access Integration

Table of Contents

BeyondTrust Secure Remote Access Integration with Password Safe	3
Overview	3
Prerequisites	3
Configure the Secure Remote Access Appliance for Integration with Password Safe ...	5
Create an OAuth API Account	5
Configure Password Safe for Integration with a Secure Remote Access Appliance	6
Configure the Secure Remote Access Connection	6
Add Users to the Secure Remote Access Requesters Group	7
Enable Managed Accounts for API Use	7
Search and Access Managed Systems from PRA Consoles	9
Prerequisites and Limitations	9
Enable External Search in Privileged Remote Access /login	9
Search	10
Configure Database Connection to Enable Privileged Remote Access Dashboard in BeyondInsight	11
Overview	11
Prerequisites	11
Network Considerations	11
Configure Database to Enable Privileged Remote Access Integration	11
View the Privileged Remote Access Dashboard in BeyondInsight	12
Database Recommendation	13
Troubleshoot the Secure Remote Access and Password Safe Integration	14
Possible Issues and Resolution Steps	14

BeyondTrust Secure Remote Access Integration with Password Safe

Overview

The Secure Remote Access integration with Password Safe enables automatic password injection to authorized systems through an encrypted BeyondTrust connection, which removes the need to share and expose credentials to privileged accounts. In addition to the automatic rotation and retrieval of managed local accounts, Password Safe can also retrieve linked accounts, giving domain admins and other privileged users access to those credentials on the targeted system. If enabled within the Privileged Remote Access /login administrative software, Password Safe Managed RDP and shell systems can be searched and accessed from the Privileged Remote Access access consoles.

The Secure Remote Access integration enables:

- One-click password injection and session spawning
- Credentials to never be exposed to authorized users of BeyondTrust
- Access to systems on or off the network with no preconfigured VPN or other routing in place
- Passwords to be securely stored in Password Safe

Password Safe uses the BeyondTrust Endpoint Credential Manager (ECM) service to communicate with the Secure Remote Access Appliance. The ECM service is pre-installed with Password Safe, and configuring Secure Remote Access in Password Safe configures the API user, group, and registration. Once a Secure Remote Access connection is configured within Password Safe, users see a list of administrator-defined credentials for the endpoints they are authorized to access. A set of these credentials can be selected when challenged with a login screen during a remote session, and the user is automatically logged in, having never seen the username/password combination.

Password Safe handles all elements of securing and managing the passwords, so policies that require password rotation after use are inherently supported. The Secure Remote Access Appliance handles creating and managing the access to the endpoint, as well as recording and controlling the level of access granted to the user. This includes what the user can see and do on that endpoint.



Note: In the case where you need to deploy the ECM plugin separately, as opposed to using the ECM service that is bundled with Password Safe, the ECM is deployed to a hardened Windows Server inside the firewall, typically in the same network as the Password Safe instance.

If you are not using the bundled ECM plugin, Contact Support for assistance integrating BeyondTrust Secure Remote Access and Password Safe.

Prerequisites

- Password Safe Cloud or On-premises 21.2 or later release
- A Secure Remote Access Appliance
- TCP Port 443 must be open for communication between the Password Safe API and the Secure Remote Access Appliance API
- Searching and accessing Password Safe Managed Systems from the PRA access consoles requires:
 - A deployed Jumpoint in PRA.
 - The Password Safe installation must use the same user authentication method as Privileged Remote Access.

- The Endpoint Credential Manager software must be version 1.6 or higher.

For integrations with Password Safe Cloud, a resource broker can be installed on the same server as the Jumpoint. For large scale deployments, these services may need dedicated systems.

Configure the Secure Remote Access Appliance for Integration with Password Safe

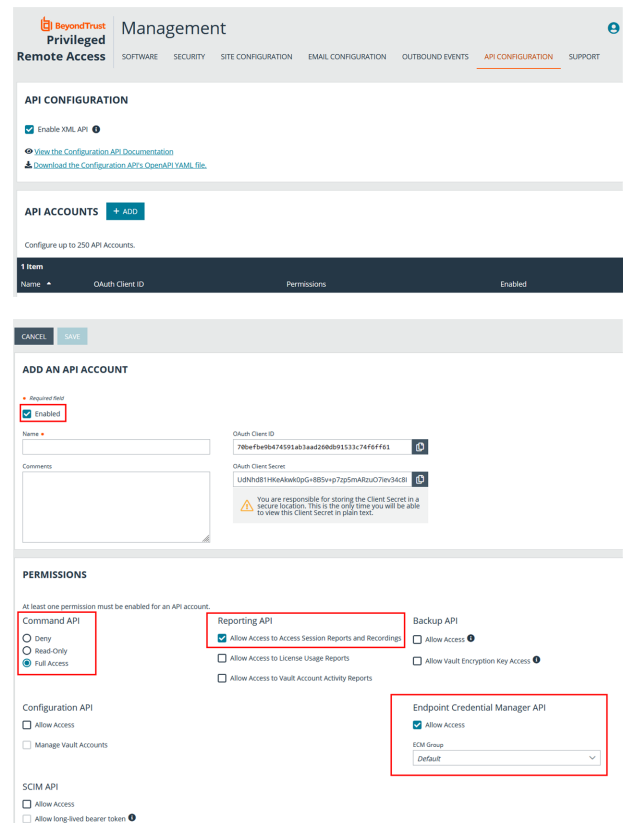
Minimal configuration is necessary on the BeyondTrust Secure Remote Access Appliance, as follows:

Create an OAuth API Account


Create an API account to be used within Password Safe to make command API calls to the Secure Remote Access Appliance.

1. Navigate to `/login > Management > API Configuration`.
2. Click **Add**.

3. Check **Enabled**.
4. Enter a name for the account.
5. Copy the **OAuth Client ID** and **OAuth Client Secret**, as these are required when configuring the **Secure Remote Access** connection settings in Password Safe.
6. Set the following **Permissions**:
 - **Command API**: Full Access.
 - **Reporting API**: Allow Access to Access Session Reports and Recordings.
 - **Endpoint Credential Manager API**: Allow Access.
 - If ECM groups are enabled on the site, select which **ECM Group** to use. ECMs that are not associated with a group come under **Default**.



The screenshot shows the 'Management' console for 'BeyondTrust Privileged Remote Access'. The 'API CONFIGURATION' section has 'Enable XML API' checked. Under 'API ACCOUNTS', there is a '+ ADD' button. The 'ADD AN API ACCOUNT' form is open, showing a table with one item. The 'PERMISSIONS' section has a note: 'At least one permission must be enabled for an API account.' The 'Command API' section has 'Full Access' selected. The 'Reporting API' section has 'Allow Access to Access Session Reports and Recordings' checked. The 'Endpoint Credential Manager API' section has 'Allow Access' checked and 'Default' selected in the 'ECM Group' dropdown.

 **Note:** The ECM Group feature is only present if enabled when your site is built. If it is not present, please contact your site administrator.

7. Click **Save** to create the account.

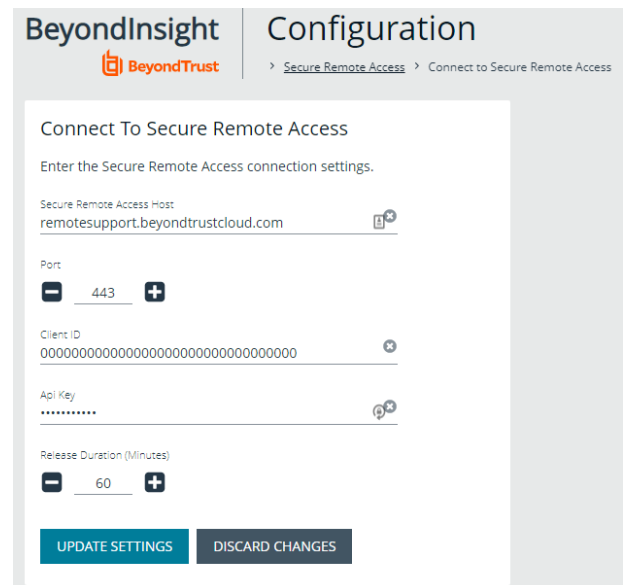
Configure Password Safe for Integration with a Secure Remote Access Appliance

The integration requires minimal setup within Password Safe and is designed to work with your existing data as it stands. The following steps are required:

- Configure the **Secure Remote Access** connection settings to use Password Safe as a credential source.
- Add users to the auto-created **Secure Remote Access Requesters** group.
- Enable managed accounts for API use.

Configure the Secure Remote Access Connection


1. In the BeyondInsight Console, navigate to **Configuration > Secure Remote Access > Connect to Secure Remote Access**.
2. Provide the **Host** and **Port** information to connect to your Secure Remote Access Appliance. The host is the URL of the Secure Remote Access site.
3. Obtain the **OAuth Client ID** and **OAuth Client Secret** for the API account you created in your Secure Remote Access Appliance, and enter these into the **Client ID** and **API Key** fields.
4. Set the number of minutes for the **Release Duration**.
5. Click **Update Settings**.



The screenshot shows the 'BeyondInsight Configuration' interface. The breadcrumb trail is 'Configuration > Secure Remote Access > Connect to Secure Remote Access'. The main heading is 'Connect To Secure Remote Access'. Below this, it says 'Enter the Secure Remote Access connection settings.' The form contains the following fields: 'Secure Remote Access Host' with the value 'remotesupport.beyondtrustcloud.com'; 'Port' with the value '443'; 'Client ID' with a long alphanumeric string; 'API Key' with a masked value '.....'; and 'Release Duration (Minutes)' with the value '60'. At the bottom of the form are two buttons: 'UPDATE SETTINGS' and 'DISCARD CHANGES'.

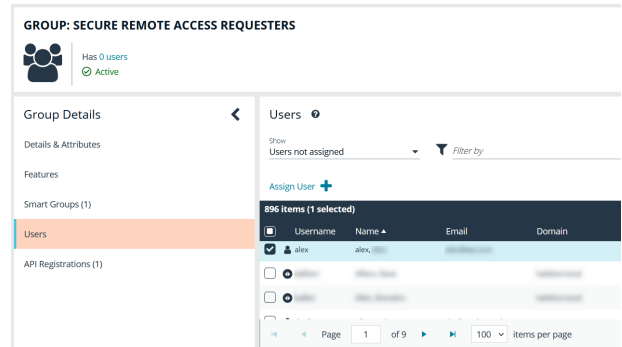
Upon completion of this form, BeyondInsight does the following:

- Creates an all-day auto-approve access policy called **Secure Remote Access Approval Policy**
- Creates an API registration called **Secure Remote Access Integration**
- Creates a group called **Secure Remote Access Requesters** that uses the **Secure Remote Access Approval Policy** and the **Secure Remote Access Integration** API registration
- Configures the ECM application with the **Secure Remote Access Integration** API registration

 **Note:** Although BeyondInsight creates a default access policy, API registration, and group to use for Secure Remote Access integration to simplify your configuration steps, you may use groups, access policies, and API registrations that you manually create, or you may modify these auto-generated ones to suit your needs.

Add Users to the Secure Remote Access Requesters Group

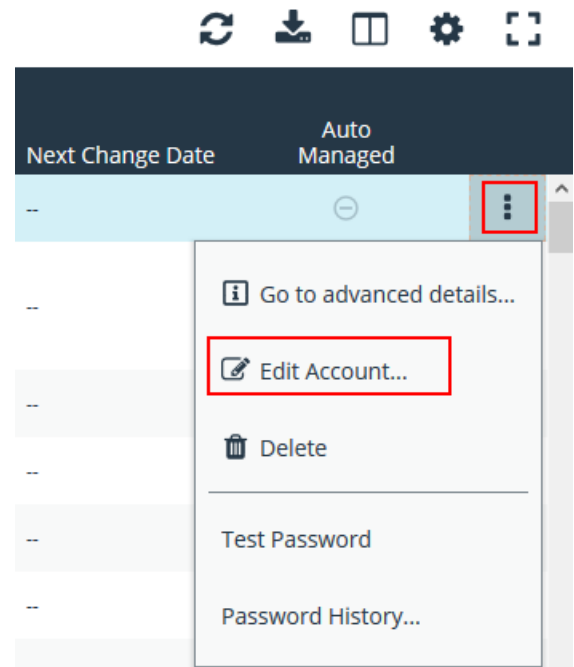
1. In the BeyondInsight Console, under **Role Based Access**, click **User Management**.
2. Locate the **Secure Remote Access Requesters** group and click the vertical ellipsis button for the group.
3. Select **View Group Details**.
4. Under **Group Details**, select **Users**, and then assign users to the group.



Enable Managed Accounts for API Use

By default, managed accounts are not accessible via the API. The accounts need to be configured to allow access through the integration.

1. In the BeyondInsight Console, select **Managed Accounts**.
2. Select the managed account, and then click the vertical ellipsis button.
3. Select **Edit Account**.



4. Under **Account Settings**, toggle the slider to **API Enabled (yes)**.
5. Click **Update Account**.



Tip: Admins also have the option to automate this step by adding **Manage Account Settings** under **Actions** in the Smart Rule, and setting the **API Enabled** option to **yes**.

EDIT MANAGED ACCOUNT ➤

rob

Managed System
bi server

Type
Asset

Platform
Generic Platform

Collapse All | Expand All

Identification

Name
rob

Description

Workgroup
None ▼

Credentials

Account Settings

API Enabled (yes)

Applications

UPDATE ACCOUNT **DISCARD CHANGES**

Once Secure Remote Access is successfully configured and your managed accounts are enabled for API use within Password Safe, you can then access systems within your Secure Remote Access Appliance using credentials stored in Password Safe.

Search and Access Managed Systems from PRA Consoles

Prerequisites and Limitations

The Password Safe and Secure Remote Access integration must be fully configured before Managed Systems can be searched and accessed.

Searching and accessing Password Safe Managed Systems requires a deployed Jumpoint in PRA. In addition, the Password Safe installation must use the same user authentication method as Privileged Remote Access.

This feature is available for Managed RDP and shell systems. Web Jump and multiple Jumpoints (network) are not available, but are planned for future releases.

Clustered Jumpoints can be used, and external Jump items do not count toward the endpoint license count.

Enable External Search in Privileged Remote Access /login

External Jump must be enabled before use.

1. In **/login**, navigate to **Management > Security**.
2. Scroll down to **Access Console**.
3. Check **Allow Search for External Jump Items**.
 - The setting does not take effect until the software is restarted.
 - A pop-up window provides the options to **Restart Now** or **Restart Later**. If you are also changing the External Jump Group Name, you can select **Restart Later**.
4. Select the **Jumpoint for External Jump Sessions** from the dropdown list of available Jumpoints.
 - This field is available only when **Allow Search for External Jump Items** is checked.
 - All sessions started from external Jump items are performed through the Jumpoint selected here. This Jumpoint must be positioned on the network to have connectivity to any of the external Jump items that are potentially returned by the ECM.
5. Enter an **External Jump Item Group Name**.
 - This field is available only when **Allow Search for External Jump Items** is checked.
 - The default is **External Jump Items**.
 - This name displays when viewing Jump Groups in the Access Console or the Web Access Console.
6. Click **Save**.
7. A pop-up window provides the options to **Restart Now** or **Restart Later**. Click **Restart Now** to enable external search or apply other changes made.

ACCESS CONSOLE

Terminate Session If Account Is In Use ⓘ

Enable Saved Logins ⓘ

Log Out Idle User After ⓘ

Enable Warning and Logout Notification on Idle Timeout ⓘ

Remove User from Session After Inactivity ⓘ

Default Access Console Authentication Method ⓘ

Allow Mobile Access Console and Privileged Web Access Console to Connect

Clipboard Synchronization Mode ⓘ
 Automatic
 Manual

Allow Search for External Jump Items. ⓘ

Jumpoint for External Jump Item Sessions ⓘ

External Jump Item Group Name ⓘ

Search

Once configured and enabled, external Jumpoints can be searched in the Access Console and the Web Access Console .

1. Go to the console, and view the list of Jump Groups.
2. Select the group for external Jump items. The name of this group is the name provided when you enabled external search.



Tip: You can skip this step and run the search from the default **My Jump Groups**, as the search includes external Jump items with other results.

3. No entries appear in this group until a search is run. Enter a search term or characters to see available endpoints found in Password Safe.
 - In the Access Console, details displayed about each Jump item include the **Hostname/IP**, **Jump Method** (RDP or shell), and **Comments**. Click the Jump Item or Endpoint for additional information and the option to Jump.
 - In the Web Access Console, details displayed also include **Status** and **Last Accessed**. Click the **i** icon at the right end of the row for additional information and the option to Jump.



Note: Jump items may display but not be available, and show the comment **Jumpoint for External Jump Items not configured**. This occurs when an appropriate **Jumpoint for External Jump Sessions** has not been selected when enabling external search.

4. Once a Jump item or endpoint has been accessed, it is available in the **Recently Used** group.

Configure Database Connection to Enable Privileged Remote Access Dashboard in BeyondInsight

Overview

Administrators can leverage the Privileged Remote Access Dashboard in the BeyondInsight console to view session details and reports of Privileged Remote Access sessions. Administrators who utilize the existing reporting functionality of /login can continue to view session details, reports, and session recordings in the /login interface.

The Privileged Remote Access integration with BeyondInsight relies on the BeyondTrust Integration Client for session reporting data. **BeyondInsight** interacts with the Integration Client's **BGSessions** database directly.

A username and password are required to access the Integration Client's **BGSessions** database, and this user must have access to the **BGSessions** tables. We recommend this user have read-only access. Once the username and password are setup, review the below prerequisites and network considerations, and then follow the steps to configure the database connection in BeyondInsight.



For more information on the BeyondTrust Integration Client, please see the [Integration Client Guide](https://www.beyondtrust.com/docs/privileged-remote-access/how-to/integrations/ic/index.htm) at <https://www.beyondtrust.com/docs/privileged-remote-access/how-to/integrations/ic/index.htm>.

Prerequisites

The following software is required:

- BeyondTrust Integration Client (version 1.7.0 or later)
- BeyondInsight (version 6.10 or later)
- Privileged Remote Access (version 19.2.1 or later)

Network Considerations

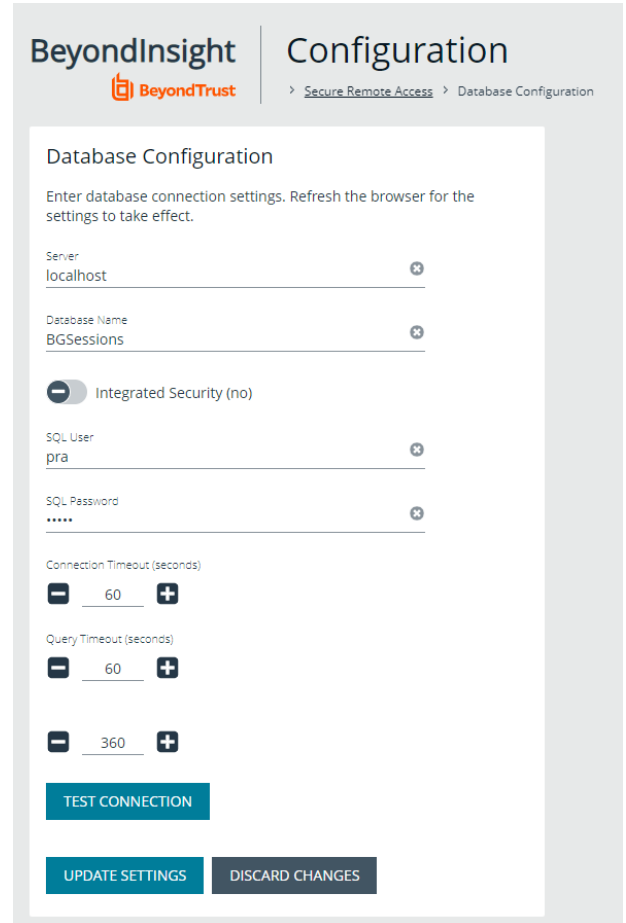
TCP ports 443 and 1433 must be open.


- The BeyondTrust Integration Client uses port 443 to make API calls to Privileged Remote Access.
- The BeyondTrust Integration Client uses port 1433 to store Privileged Remote Access session data in the **BGSessions** SQL server database.
- BeyondInsight uses port 1433 to query the **BGSessions** SQL server database to retrieve Privileged Remote Access session data.

Configure Database to Enable Privileged Remote Access Integration

1. From the home page or left menu in BeyondInsight, click **Configuration**.
2. Under **Secure Remote Access**, click **Database Configuration**.

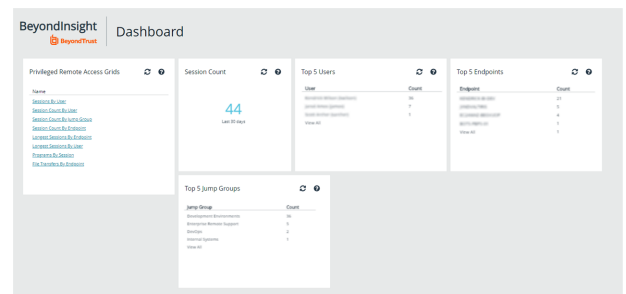
3. Provide the settings to connect to your Integration Client's **BGSessions** database where the Privileged Remote Access session data is stored:
 - **Server:** Hostname or IP address for the SQL Server hosting the Integration Client's **BGSessions** database.
 - **Database Name:** Name of the database that contains the Privileged Remote Access session data. **BGSessions** is default.
 - **Integrated Security:** If toggled to **yes**, the current Windows account credentials are used for authentication. If toggled to **no**, the username and password are specified in the connection.
 - **SQL User:** Username used to the access the **BGSessions** database.
 - **SQL Password:** Password for the SQL User.
 - **Connection Timeout:** Timeout in seconds to wait for a connection to open.
 - **Query Timeout:** Timeout in seconds to wait for the command to execute.
4. Click **Test Connection** to verify connectivity to the database.
5. Click **Update Settings**.



 **Note:** After initial setup, you must refresh your browser for the Privileged Remote Access option to display in the left menu in BeyondInsight. Clicking the Privileged Remote Access option brings you to the Privileged Remote Access Dashboard.

View the Privileged Remote Access Dashboard in BeyondInsight

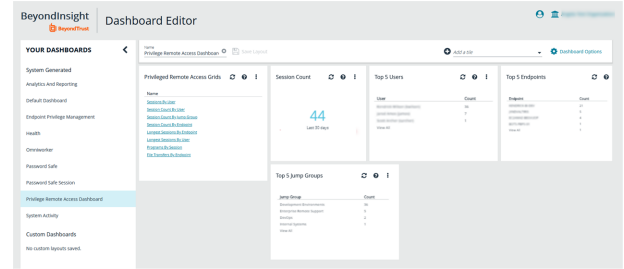
1. From the left menu in BeyondInsight, click **Privileged Remote Access**.
2. In the **Dashboard**, you can quickly view a summary of **Privileged Remote Access** session data in each card.
3. Click the items within each card to review the specific records for that item in a grid view, which can be sorted, filtered, and exported as required.





Tip: You can customize the Privileged Remote Access Dashboard by adding and removing tiles, and rearranging tiles from the **Dashboard Editor** page in BeyondInsight.

To access the **Dashboard Editor**, click **Dashboard (Preview)** the left menu in BeyondInsight, and then select **Privileged Remote Access Dashboard** from the **Your Dashboards** list.



Database Recommendation

To assist with troubleshooting potential performance issues between the Privileged Remote Access Dashboard and the **BGSessions** database, the following indexes are recommended in the **BGSessions** database:

```
create index session__start_time_ndx on session(start_time);
```

```
create index session__host_name_ndx on session(host_name);
```

```
create index session__host_name_ndx on session(host_name);
```

```
create index session__jump_group_name_ndx on session(jump_group_name);
```

```
create index session__lsid_ndx on session(lsid);
```

```
create index session_event__type_performed_by_type_ndx on session_event(type, performed_by_type);
```

```
create index session_event__session_id_ndx on session_event(session_id);
```

```
create index session_event__type_destination_ndx on session_event(type, destination);
```

```
create index session_event__type_performed_by_ndx on session_event(type, performed_by);
```

```
create index session_event_data__session_event_id_ndx on session_event_data(session_event_id);
```

```
create index session_event_data__name_ndx on session_event_data(name);
```

Troubleshoot the Secure Remote Access and Password Safe Integration


In the rare case, if you experience any issues during the integration process, a list of potential issues and steps for resolving these issues are indicated below to assist you with troubleshooting. These are applicable only for Password Safe on-premises installations, and are not applicable for Password Safe Cloud.

For any issues that involve the ECM service, we recommend enabling **DEBUG level logging**.

1. Open the **BeyondTrust-ECMService.exe** config file in a text editor.
2. Edit the file by changing the line `<level value="INFO"/>` to `<level value="DEBUG"/>`.
3. Save the file, and then restart the ECM service.

Possible Issues and Resolution Steps

Issue	Cause	Debugging Steps/ Possible Solutions
TLS Error trying to connect to the Password Safe API	No trusted certificate available.	Add the Password Safe certificate to the ECM Servers trusted store.
ECM Configurator cannot find or load the plugin	DLL files were not deployed to ECM install directory.	Copy ALL files included with the plugin into the ECM install directory, typically C:\Program Files\BeyondTrust\ECM . Close and re-open the ECM Configurator .
ECM Configurator cannot find or load the plugin	DLL files are blocked by Windows.	While the build server signs assemblies to help prevent this error, some systems still block the DLLs. To unblock them: <ol style="list-style-type: none"> 1. Right-click the DLL. 2. Select Properties. 3. In the General > Security section, check the Unblock box. 4. Click OK to save the changes. Repeat these steps with any other DLLs paged with the plugin DLL.

Issue	Cause	Debugging Steps/ Possible Solutions
No credentials are returned when using the Test Settings feature	ECM has been configured without the proper settings.	<p>A failure to retrieve credentials using the Test Settings feature in the ECM Configurator is usually a result of a configuration setting entered incorrectly.</p> <p>First, double-check the endpoint URL and API registration key entered.</p> <p>Next, check the logs in Configurator.log to see if the integration is providing any information as to why the test failed. Possible causes include: entering incorrect URL or port information, authentication failures, or network connectivity issues. The logs may also reveal a perceived failure was not a failure after all. Instead, no matches may have been found, and an empty list was provided. An empty list is still considered a valid result.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">  <p>Note: The Test Settings feature does NOT communicate with BeyondTrust Secure Remote Access Appliance at any point. It simply tests the settings related to the password vault system. Also, remember that the test uses the currently entered values and settings whether the settings have been saved or not. This allows you to test different configurations without overwriting existing settings.</p> </div>
No credentials are returned when using the Test Settings feature	There is a lack of network connectivity.	There is a lack of network connectivity between the ECM server and the password vault system. The resolution could be as simple as adding a rule to the Windows Firewall, or it might require a network administrator to open ports to allow communication.
Credentials are returned via the Test Settings feature but are not available in the access console	ECM has been configured without the proper settings.	The settings on the initial screen of the ECM Configurator tell the ECM service which BeyondTrust PRA instance to connect to and the account to use for authentication. Double-check these and review the logs in ECM.log , if necessary.
Credentials are returned via the Test Settings feature but are not available in the access console	BeyondTrust Secure Remote Access Appliance has been configured without the proper settings.	It is possible ECM connections have not been enabled or the API account being used does not have permission to access the Endpoint Credential Manager API.
Credentials are returned via the Test Settings feature but are not available in the access console	The ECM service has stopped functioning.	Restart the BeyondTrust ECM Service.

Issue	Cause	Debugging Steps/ Possible Solutions
Credentials are returned via the Test Settings feature but are not available in the access console	There is a lack of network connectivity.	<p>A lack of connectivity could prevent the integration from working. In this case, the missing connection occurs between BeyondTrust Secure Remote Access Appliance and the ECM server. If the ECM is unable to establish a connection to the BeyondTrust Secure Remote Access Appliance, it is unable to receive requests for credentials.</p> <p>Load the /login page in a browser running on the ECM server. If the browser cannot connect, the ECM will also be unable to connect. If the browser test passes, check the ECM.log to see if a connection was successfully established when starting the service.</p>
Credentials are returned via the Test Settings feature but are not available in the access console	The user mapping has failed.	<p>This issue commonly occurs (particularly with domain accounts) when a test is run with a user entered as domain\user or a similar format. However, when connecting through the access console, it is possible for the domain portion to be different or missing altogether. If the Secure Remote Access Appliance user is a local user, no domain information is present. The same is true for users authenticating to the Secure Remote Access Appliance via certain security providers like RADIUS.</p> <p>Check the ECM.log file to make sure the values passed to the password vault match what is expected. If the test is successful, note the information used.</p>