



BeyondTrust

Remote Support Password Safe Integration

Table of Contents

BeyondTrust Remote Support Integration with Password Safe	3
Overview	3
Prerequisites	3
Configure Password Safe for Integration with Remote Support	4
Configure the Secure Remote Access Connection	4
Add Users to the Secure Remote Access Requesters Group	5
Enable Managed Accounts for API Use	5
Configure Remote Support for Integration with Password Safe	7
Create an OAuth API Account	7
Configure the Endpoint Credential Manager Plugin for Integration with Remote Support	8
Install the Endpoint Credential Manager	8
Install and Configure the Plugin	9
Test Plugin Settings	11
Troubleshoot the Remote Support and Password Safe Integration	15
Common Issues and Resolution Steps	15

BeyondTrust Remote Support Integration with Password Safe

Overview


The Endpoint Credential Manager (ECM) service integration with Password Safe enables automatic password injection to authorized systems through an encrypted BeyondTrust connection and 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.

The 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

The BeyondTrust ECM service enables communication between Password Safe and Remote Support. 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. Remote Support 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 Remote Support and Password Safe.

 For more information on installing and using the ECM plugin, please see ["Configure the Endpoint Credential Manager Plugin for Integration with Remote Support" on page 8.](#)

Prerequisites

The following software is required:

- Password Safe Cloud or On-premises 21.2 or later release
- Remote Support
- TCP Port 443 must be open for communication between the Password Safe API and the Remote Support API

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.

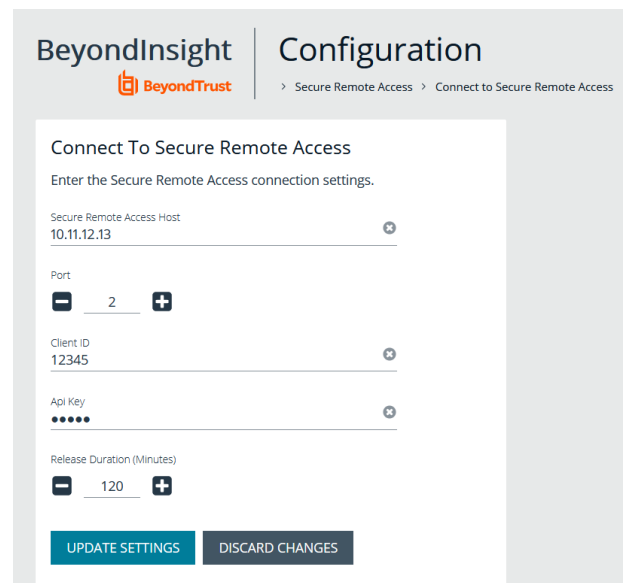
Configure Password Safe for Integration with Remote Support

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 Remote Support instance.
3. Obtain the **OAuth Client ID** and **OAuth Client Secret** for the API account you created in Remote Support, 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 'Connect to Secure Remote Access' configuration form in the BeyondInsight console. The form is titled 'Connect To Secure Remote Access' and includes the instruction 'Enter the Secure Remote Access connection settings.' The fields are: 'Secure Remote Access Host' (10.11.12.13), 'Port' (2), 'Client ID' (12345), 'API Key' (masked with dots), and 'Release Duration (Minutes)' (120). There are 'UPDATE SETTINGS' and 'DISCARD CHANGES' buttons at the bottom.

Upon completion of this form, BeyondInsight does the following:

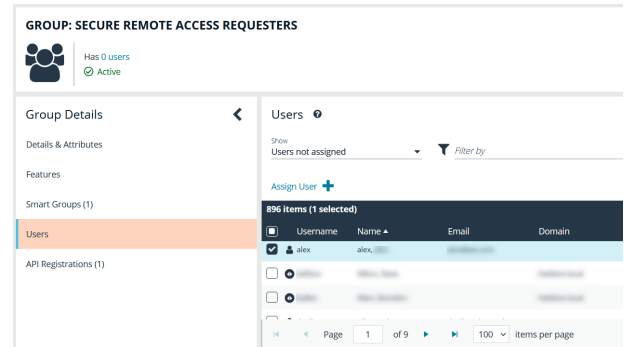
- Creates an all-day auto-approve access policy called **Secure Remote Access Approval Policy**
- Creates an API registration called **Secure Remote Access Integration**
- Creates a group called **Secure Remote Access Requesters** that uses the **Secure Remote Access Approval Policy** and the **Secure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

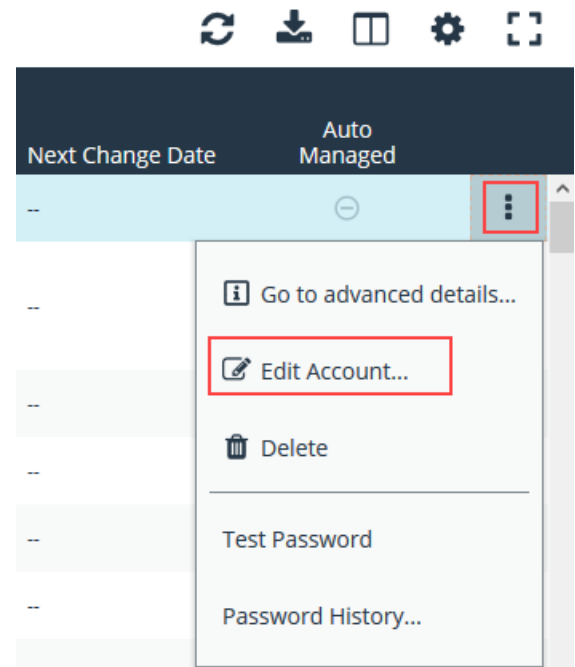
1. In the BeyondInsight Console, under **Role Based Access**, click **User Management**.
2. Locate the **Secure Remote Access Requesters** group and click the vertical ellipsis button for the group.
3. Select **View Group Details**.
4. Under **Group Details**, select **Users**, and then assign users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



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

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 Remote Support using credentials stored in Password Safe.

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

Configure Remote Support for Integration with Password Safe

Minimal configuration is necessary on the BeyondTrust Appliance B Series, as follows:

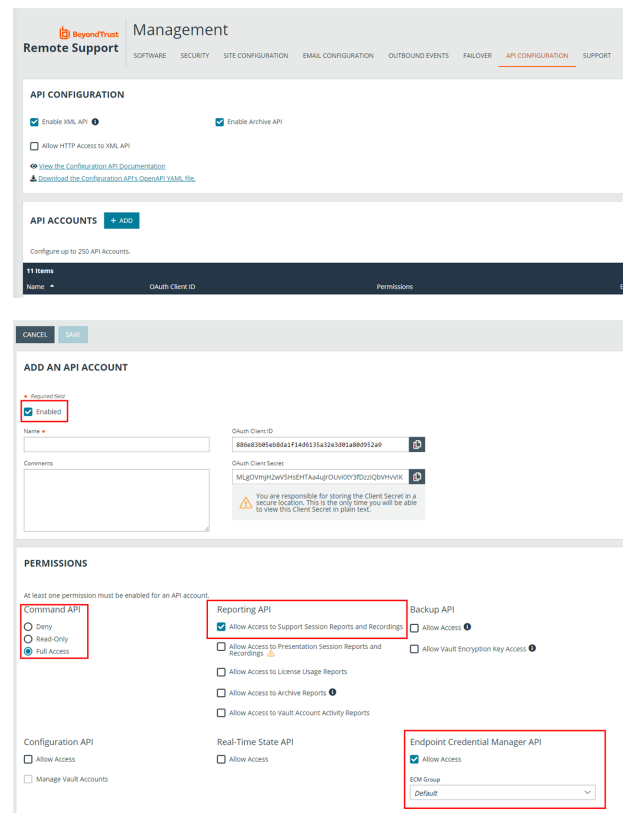
Create an OAuth API Account




The Password Safe API account is used from within Password Safe 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 Autotask.
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**.



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

7. Click **Save** at the top of the page to create the account.

Configure the Endpoint Credential Manager Plugin for Integration with Remote Support

! IMPORTANT!

You must purchase this integration separately from both your BeyondTrust Remote Support and Password Safe solutions. For more information, contact BeyondTrust sales.

The Endpoint Credential Manager (ECM) must be installed on a system with the following requirements:

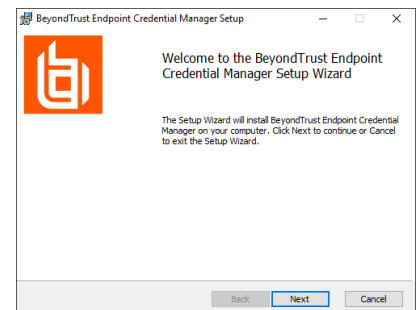
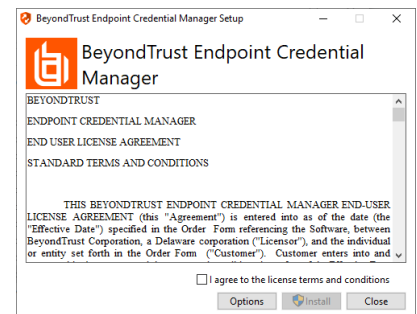
System Requirements

- Windows Vista or newer, 64-bit only
- .NET 4.5 or newer
- Processor: 2GHz or faster
- Memory: 2GB or greater
- Available Disk Space: 80GB or greater

Install the Endpoint Credential Manager

1. To begin, download the BeyondTrust Endpoint Credential Manager (ECM) from [BeyondTrust Support](https://beyondtrustcorp.service-now.com/csm) at beyondtrustcorp.service-now.com/csm
2. Start the BeyondTrust Endpoint Credential Manager Setup Wizard.
3. Agree to the EULA terms and conditions. Mark the checkbox if you agree, and then click **Install**.

If you need to modify the ECM installation path, click the **Options** button to customize the installation location.

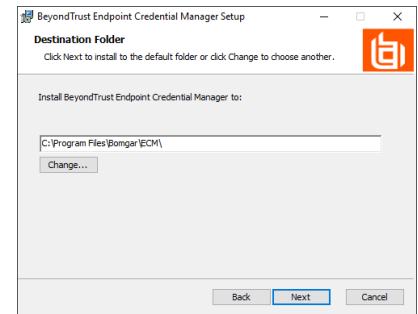


4. Click **Next** on the Welcome screen.

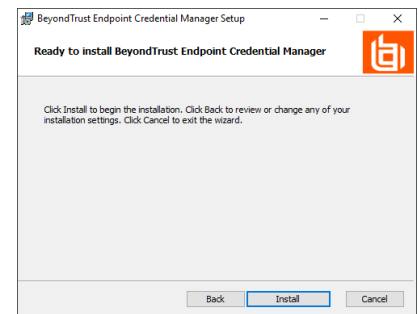


Note: You are not allowed to proceed with the installation unless you agree to the EULA.

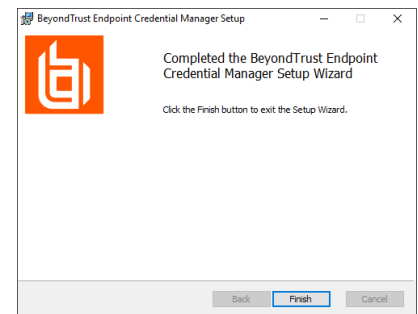
5. Choose a location for the credential manager, and then click **Next**.
6. On the next screen, you can begin the installation or review any previous step.





7. Click **Install** when you are ready to begin.



8. The installation takes a few moments. On the **Completed** screen, click **Finish**.



 **Note:** To ensure optimal up-time, administrators can install up to five ECMs on different Windows machines to communicate with the same site on the BeyondTrust Appliance B Series. A list of the ECMs connected to the B Series Appliance site can be found at **/login > Status > Information > ECM Clients**.

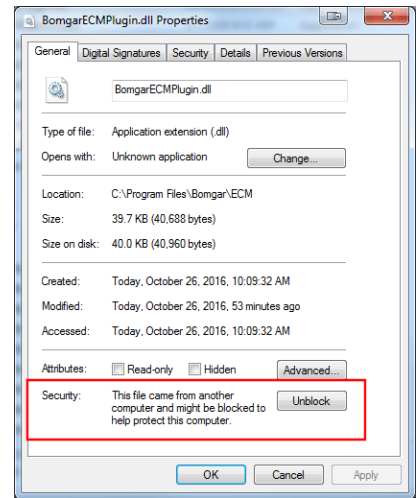
 **Note:** When multiple ECMs are connected to a BeyondTrust site, the B Series Appliance routes requests to the ECM that has been connected to the B Series Appliance the longest.

Install and Configure the Plugin

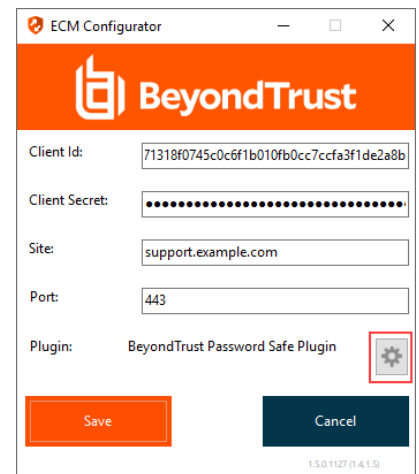
1. Once the BeyondTrust ECM is installed, extract and copy the plugin files to the installation directory (typically **C:\Program Files\Bomgar\ECM**).
2. Run the **ECM Configurator** to install the plugin.

3. The Configurator should automatically detect the plugin and load it. If so, skip to step 4 below. Otherwise, follow these steps:

- First, ensure that the DLL is not blocked. Right-click on the DLL and select **Properties**.
- On the **General** tab, look at the bottom of the pane. If there is a **Security** section with an **Unblock** button, click the button.
- Repeat these steps for any other DLLs packaged with the plugin.
- In the Configurator, click the **Choose Plugin** button and browse to the location of the plugin DLL.



4. Click the gear icon in the Configurator window to configure plugin settings.

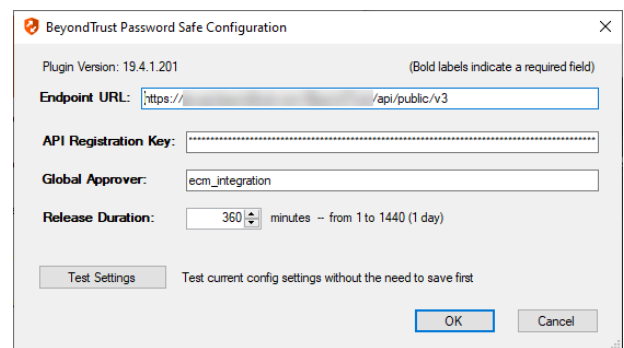


5. The following settings are available:

Setting Name	Description	Notes
Endpoint URL	The full URL to the PS SDK Web Services.	example: https://<password-safe-server-hostname>/BeyondTrust/api/public/v3
API Registration Key	The Key for the API Registration created for the integration.	
Global Approver	The username for the account created to allow automated approval of requests for credentials via the integration.	
Release Duration	The number of minutes for which the generated release request is valid and can be used to retrieve the credential.	Default is 360 minutes.

Test Plugin Settings

You can test the settings specific to Password Safe directly from the plugin configuration screen using the **Test Settings** button.



BeyondTrust Password Safe Configuration

Plugin Version: 19.4.1.201 (Bold labels indicate a required field)

Endpoint URL:


API Registration Key:


Global Approver:

Release Duration: minutes - from 1 to 1440 (1 day)

Test current config settings without the need to save first

The test functionality allows you to test new or updated configuration without the need to go through the representative console or to save the changes first. The form collects information to simulate a request from the B Series Appliance to the ECM. This means you can test the settings without having the ECM service running or connected to the B Series Appliance.

 **Note:** While the test does simulate a request from the B Series Appliance to the ECM, it does not in any way test configuration or connectivity to the B Series Appliance. It is used only for configuration, connectivity, permissions, etc., related to the password vault system.

 Test Plugin Settings
✕

This form provides a way to test new or updated configuration without the need to first save the changes. Also, because the test simulates a request from the Secure Remote Access appliance, it doesn't require the ECM service to be connected to the appliance or even running at all.

(Bold labels indicate a required field)

Console User Information

Simulates the console user information that would be sent to the ECM from the appliance

SRA Console Username:

Distinguished Name:

Jump Item Information

Simulates the Jump Item to which a user would connect and attempt credential injection

Jump Item Type:

Hostname / IP Address:

Additional IP Address:

Application Name:

NOTE: Any logs generated from these tests will be contained in Configurator.log

Console User Information

The fields collected in this section simulate the information that is sent to the ECM about the user logged into the console and requesting credentials from the password vault.

- **SRA Console Username:** The username of the console user. Depending on the type of security provider and how it is configured, this might be username-only (**joe.user**), which is the most common format, or it might include other information and in other formats, such as down-level domain info (**ACME\joe.user**) or email / UPN (**joe.user@acme-inc.com**).
- **Distinguished Name:** For LDAP Security Providers, the provider often populates the Distinguished Name of the user in addition to the username. The Distinguished Name includes domain information which is extracted by the integration and used to help identify the matching account in the password vault. An example DN is: **uid=joe.user,ou=HelpDesk,dc=acme-inc,dc=com**.

Jump Item Information

The fields collected in this section simulate the information that is sent to the ECM about the endpoint or Jump Item to which the console user may connect.

- **Jump Item Type:** Because different Jump Items result in different pieces of information being sent to the ECM, as well as how the ECM may query the password vault for applicable credentials, it is important to identify the type of Jump Item you wish to simulate as part of the test process.



Note: The Jump Client type should be used to simulate Remote Jump and Local Jump items as well.

- **Hostname / IP Address:** For most types of Jump Items, the primary piece of information used to find credentials in the password vault is the endpoint's hostname or IP address.
- **Website URL:** For Web Jump items, rather than a hostname, the ECM is provided with the URL to which the item points. This field validates that the supplied string appears to be an actual URL.
- **Additional IP Address:** For Jump Client items, in addition to the machine's name, the installed client also makes the machine's public and private IP addresses available to the ECM. Some integrations use this information to query for credentials in addition to or even instead of those which match the hostname value.
- **Application Name:** For testing credential retrieval for injection into an application via an RDP + SecureApp item, the ECM is provided with both a value to identify the endpoint (Hostname / IP Address) and one to identify the specific application. The required value for Application Name may vary across integrations. The integration specific installation guides should contain more information on possible values.

Test Results

If the test fails for any reason, error information is displayed to assist in diagnosing the cause of the failure. In most cases these errors are handled and then assigned a type, such as an authentication-related error, and then displayed with the inputs as well as any specific error messages. However, there may still be some instances where a particular error might not be anticipated, so the information is displayed in a more raw form.

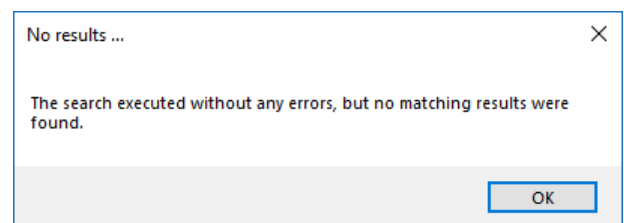
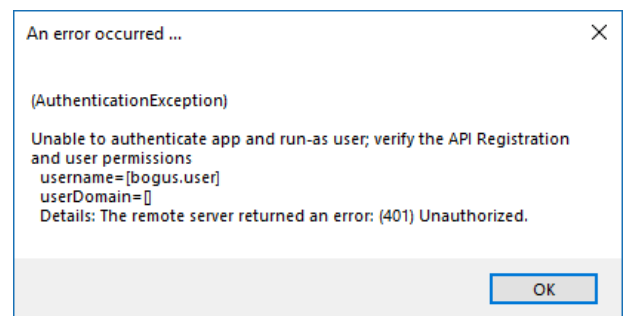
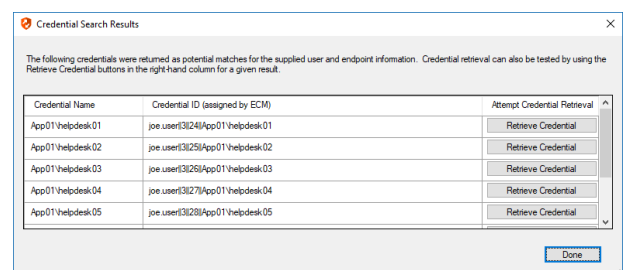


Note: It's important to note that, either way, the same information is included in the **Configurator.log**, along with more detail as to exactly what point in the execution the failure occurred.

It's possible that the test succeeds in that it doesn't encounter any errors and yet it doesn't return any credentials. Because this is a perfectly valid result, it is not treated as an error.

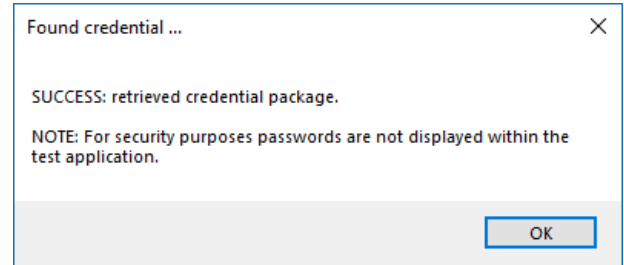
In either case, if the test succeeds but the results do not match what is expected, it's important to make note of the inputs which led to those results and verify permissions and access to credentials within the password vault.

When the search does yield one or more matching credentials, the test does allow for one additional level of verification by allowing a tester to retrieve a specific credential as would occur if it were selected for injection within the console. The tester simply clicks the **Retrieve Credential** button in the right column of the results list, and the integration then attempts to retrieve that credential on behalf of the supplied user.

Credential Name	Credential ID (assigned by ECM)	Attempt Credential Retrieval
App01\helpdesk-01	joe.user\3124\App01\helpdesk-01	Retrieve Credential
App01\helpdesk-02	joe.user\3125\App01\helpdesk-02	Retrieve Credential
App01\helpdesk-03	joe.user\3126\App01\helpdesk-03	Retrieve Credential
App01\helpdesk-04	joe.user\3127\App01\helpdesk-04	Retrieve Credential
App01\helpdesk-05	joe.user\3128\App01\helpdesk-05	Retrieve Credential

The test displays the result of the attempt to retrieve the credential, but for security reasons no password is ever displayed in clear text.



Note: Only credentials are retrieved; no actual passwords are retrieved or displayed. The settings used for the test are the ones currently entered on the screen, not necessarily what is saved.


Troubleshoot the Remote Support and Password Safe Integration

To assist you, a list of common issues experienced during the integration process has been provided and steps for resolving these issues are noted.

For any issues that involve the ECM service, we recommend you enable **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.

Common Issues and Resolution Steps

Issue	Cause	Debugging Steps/ Possible Solutions
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 being 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 on 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 being paged with the plugin DLL.
No credentials are returned when using the Test Settings feature.	ECM has been configured without the proper settings.	A failure to retrieve credentials using the Test Settings feature in the ECM Configurator is usually a result of some configuration setting being entered incorrectly. First, double-check the endpoint URL and API registration key entered. 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. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">  <p>Note: The Test Settings feature does NOT communicate with BeyondTrust Remote Support 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>

Issue	Cause	Debugging Steps/ Possible Solutions
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 may require a network administrator to open ports to allow communication.
No credentials are returned when using the Test Settings feature.	Missing permissions or invalid configuration within Password Safe.	Ensure the user is a member of a group with permissions to use the API Registration and the registration includes an authentication rule with the correct IP address to allow requests from the system running the ECM / Configurator.
Credentials are returned via the Test Settings feature but are not available in the Representative 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 Remote Support 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 Representative Console.	BeyondTrust Remote Support 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 Representative Console.	The ECM service has stopped functioning.	Restart the BeyondTrust ECM Service.
Credentials are returned via the Test Settings feature but are not available in the Representative Console.	There is a lack of network connectivity.	A lack of connectivity could prevent the integration from working. In this case, the missing connection occurs between BeyondTrust Remote Support and the ECM server. If the ECM is unable to establish a connection to the B Series Appliance, it is unable to receive requests for credentials. 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.
Credentials are returned via the Test Settings feature but are not available in the representative console.	The user mapping has failed.	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 representative console, it is possible for the domain portion to be different or missing altogether. If the Remote Support user is a local user, no domain information is present. The same is true for users authenticating to Remote Support via certain security providers like RADIUS. Check the ECM.log to make sure the values passed to the password vault match what is expected. If the test is successful, note the information used.
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.