Remote Support
Password Safe Integration
# Table of Contents

BeyondTrust Remote Support Integration with Password Safe .................................. 3  
Overview .................................................................................................................... 3  
Prerequisites ............................................................................................................... 3  
Installation and Administration .................................................................................. 3  
Network Considerations ............................................................................................. 4  
**Configure Password Safe for Integration with Remote Support** ................................ 5  
Create an API Registration .......................................................................................... 5  
Grant Access to the API Registration .......................................................................... 6  
Create Global Approver .............................................................................................. 7  
Enable Managed Account for API use ......................................................................... 9  
**Configure Remote Support for Integration with Password Safe** ............................. 11  
Create an API Service Account - BeyondTrust 16.1 and Earlier ............................... 11  
Create an API Service Account - BeyondTrust 16.2 and Later .................................. 12  
**Configure the Endpoint Credential Manager Plugin for Integration with Privileged Remote Access** .......................................................... 13  
Install the Endpoint Credential Manager .................................................................... 13  
Install and Configure the Plugin ................................................................................ 14  
Test Settings ............................................................................................................... 16  
**Troubleshoot the Remote Support and Password Safe Integration** ......................... 17
BeyondTrust Remote Support Integration with Password Safe

Overview

The Endpoint Credential manager (ECM) plug-in 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, it 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 pre-configured VPN or other routing in place
- Passwords to be securely stored in Password Safe.

The BeyondTrust Endpoint Credential Manager enables communication between Password Safe and Remote Support. The ECM is deployed to a hardened Windows Server inside the firewall, typically in the same network as the Password Safe instance. Once deployed, BeyondTrust 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 passwords to be rotated 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.

Prerequisites

The following software is required:

- Endpoint Credential Manager (Current is 1.4)
- Password Safe ECM Plugin (Current is 19.2.1.19596)
- Password Safe
- Remote Support

Installation and Administration

IMPORTANT!

To complete this integration, please ensure that you have the necessary software installed and configured as indicated in this guide, along with accounting for any network considerations.
Network Considerations

<table>
<thead>
<tr>
<th>Outbound From</th>
<th>Inbound To</th>
<th>TCP Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>ECM Server</td>
<td>Secure Remote Access Appliance</td>
<td>443</td>
<td>API calls from ECM</td>
</tr>
<tr>
<td>ECM Server</td>
<td>Password Safe Server</td>
<td>443</td>
<td>ECM makes calls to Password Safe RESTful Web Services</td>
</tr>
</tbody>
</table>

For more information on installing and using the ECM plugin, please see the section on ECM installation and setup.
Configure Password Safe for Integration with Remote Support

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

- Create an API registration to be used by the integration.
- Give users access to the API registration.
- Create or identify an account with Approver permissions that can be used to automatically approve check-out requests generated by the integration.
- Enable managed account for API use.

Create an API Registration

1. In the BeyondInsight console, under Configuration > General, select API Registrations.

   Note: If an API Registration already exists that you’d like to use for the integration, select it and skip to step 4 below.

2. Click Create API Registration.

3. Provide a name for the registration, such as ECM Integration, and then click Create.
4. Click Add Authentication Rule to add source IP addresses to the registration.

5. Add the IP of the server hosting the ECM in the IP address field for the IP Rule, and then click Create Rule.

Grant Access to the API Registration

Permissions are handled at the group level. The group can be one that exists only within BeyondInsight or is managed by an outside source, such as Active Directory or LDAP. The following steps describe creating a local group within BeyondInsight, but the same can be done using an existing group:

1. In the BeyondInsight console, under Configuration > Role Based Access, select User Management.

2. Under Groups, click Create New Group, and then select Create a New Group.

3. Enter a descriptive Group Name and Description for the group, and then click Create Group.
4. Under Group Details, select Users, and then assign a user or users to the group.

5. Under Group Details, select Smart Groups, and then assign Read Only permissions on at least one smart group, such as All Managed Accounts.

![Note: Password Safe roles are not required for this access because access is based on the incoming user's permissions. However, it is acceptable to manage special access or permissions unique for users using this group.]

6. Under Group Details, select API Registrations, and then select the registration you created for the integration. This change is saved automatically and allows the integration to query the Password Safe APIs on behalf of any user added to this group.

Create Global Approver

A user with the Password Safe Approver role for All Managed Accounts is needed. This allows credentials checked out using the integration to be automatically approved. The following describes how to create the group, assign the Approver role, and add the user to the appropriate groups. The same can be accomplished with an existing group and user, as long as sufficient permissions are present.

1. In the BeyondInsight console, under Configuration > Role Based Access, select User Management.
2. Under Groups, click Create New Group, and then select Create a New Group.

3. Enter a descriptive Group Name and Description for the group, and then click Create Group.

4. Under Group Details, select Users, and then assign a user or users to the group.

5. Under Group Details, select Smart Groups, and then assign Read Only permissions on the All Managed Accounts smart group.
6. Click the More Options button for the All Managed Accounts smart group, where you granted the read only permission in above steps, and then select Edit Password Safe Roles.

7. Check the Approver role box, and then click Save Roles.

8. Assign the same user or users that were assigned to the global approvers group, to the group you created for the API registration in above steps.

Enable Managed Account 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 **More Options** button; 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**.
Configure Remote Support for Integration with Password Safe

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

Create an API Service Account - BeyondTrust 16.1 and Earlier

The API user account is used from within the integration to make BeyondTrust Command API calls to BeyondTrust.

2. Click Create New User and name it Integration or something similar.
3. Leave Must Reset Password at Next Login unchecked.
5. Set Allowed to View Support Session Reports to View All Sessions.
6. Check Allowed to view support session recordings.
7. Set Allowed to View Presentation Session Reports to View All Sessions.
8. Check Allowed to Use Reporting API and Allowed to Use Command API.
9. Scroll to the bottom and save the account.
Create an API Service Account - BeyondTrust 16.2 and Later

1. Go to Management > API Configuration and click Add to create a new API account.
2. Provide a name for the API account.
3. Under Permissions, check Full Access to the Command API.
4. For the Reporting API, check Allow Access to Support Session Reports and Recordings and Allow Access to Presentation Session Reports and Recordings.
5. Be sure to copy the values for both the OAuth Client ID and OAuth Client Secret for use in a later step.
6. Click Save to create the account.
Configure the Endpoint Credential Manager Plugin for Integration with Privileged Remote Access

**IMPORTANT!**

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

**Install the Endpoint Credential Manager**

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

- Windows Vista or newer, 64-bit only
- .NET 4.5 or newer

1. To begin, download the BeyondTrust Endpoint Credential Manager (ECM) from [BeyondTrust Support at beyondtrustcorp.service-now.com/csm](https://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.

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

4. Click **Next** on the Welcome screen.
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 Secure Remote Access Appliance. A list of the ECMs connected to the appliance site can be found at /login > **Status** > **Information** > **ECM Clients**.

**Note:** When multiple ECMs are connected to a BeyondTrust site, the Secure Remote Access Appliance routes requests to the ECM that has been connected to the 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:

<table>
<thead>
<tr>
<th>Setting Name</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoint URL</td>
<td>The full URL to the PS SDK Web Services</td>
<td>ex: https://&lt;password-safe-server-hostname&gt;/BeyondTrust/api/public/v3</td>
</tr>
<tr>
<td>API Registration Key</td>
<td>The Key for the API Registration created for the integration</td>
<td></td>
</tr>
<tr>
<td>Global Approver</td>
<td>The username for the account created to allow automated approval of requests for credentials via the integration.</td>
<td></td>
</tr>
</tbody>
</table>
Test Settings

The settings specific to Password Safe can be tested directly from the plugin configuration screen using the **Test Settings** button. Simply enter a user from whose account you’d like to retrieve credentials, an endpoint for which the user has one or more credentials, and view the resulting list.

![Test Settings Configuration](image)

**Note:** Passwords are not actually retrieved and displayed. Only a list of credentials is retrieved and displayed. The settings used for the test are the ones currently entered on the screen, not necessarily what is saved. The test user should have the **Requestor** role with access to the API.

1. Enter a user account from which to retrieve credentials.

   ![Enter a User](image)

2. Enter an endpoint for which the user account has one or more credentials.

   ![Enter an Endpoint](image)

3. View the resulting list.

   ![Found Credentials](image)
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, it is recommended to 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 restart the ECM service.

**Common Issues and Resolution Steps**

<table>
<thead>
<tr>
<th>Issue</th>
<th>Cause</th>
<th>Debugging Steps/ Possible Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>ECM Configurator cannot find or load the plugin</td>
<td>DLL files were not deployed to ECM install directory.</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>DLL files are being blocked by Windows.</td>
<td>While the build server signs assemblies to help prevent this error, some systems still block the DLLs. To unblock them, right-click on the DLL. Select Properties. In the General &gt; Security section, check the Unblock box. Click OK to save the changes. Repeat these steps with any other DLLs being paged with the plugin DLL.</td>
</tr>
<tr>
<td>No credentials are returned when using the <strong>Test Settings</strong> feature</td>
<td>ECM has been configured without the proper settings.</td>
<td>A failure to retrieve credentials using the <strong>Test Settings</strong> 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 <strong>Configurator.log</strong> 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.</td>
</tr>
</tbody>
</table>

*Note: The **Test Settings** feature does NOT communicate with BeyondTrust PRA 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.*
<table>
<thead>
<tr>
<th>Issue</th>
<th>Cause</th>
<th>Debugging Steps/ Possible Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>No credentials are returned when using the Test Settings feature</td>
<td>There is a lack of network connectivity.</td>
<td>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.</td>
</tr>
<tr>
<td>Credentials are returned via the Test Settings feature but are not available in the access console</td>
<td>ECM has been configured without the proper settings.</td>
<td>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.</td>
</tr>
<tr>
<td>Credentials are returned via the Test Settings feature but are not available in the access console</td>
<td>BeyondTrust PRA has been configured without the proper settings.</td>
<td>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.</td>
</tr>
<tr>
<td>Credentials are returned via the Test Settings feature but are not available in the access console</td>
<td>The ECM service has stopped functioning.</td>
<td>Restart the BeyondTrust ECM Service.</td>
</tr>
<tr>
<td>Credentials are returned via the Test Settings feature but are not available in the access console</td>
<td>There is a lack of network connectivity.</td>
<td>A lack of connectivity could be preventing the integration from working. In this case, the missing connection would occur between BeyondTrust PRA and the ECM server. If the ECM is unable to establish a connection to the BeyondTrust PRA, it is unable to receive requests for credentials. Try loading 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.</td>
</tr>
<tr>
<td>Credentials are returned via the Test Settings feature but are not available in the access console</td>
<td>The user mapping has failed.</td>
<td>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 PRA user is a local user, no domain information is present. The same is true for users authenticating to PRA 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.</td>
</tr>
<tr>
<td>TLS Error trying to connect to the Password Safe API</td>
<td>No trusted Certificate available</td>
<td>Add the Password Safe certificate to the ECM Servers trusted store.</td>
</tr>
</tbody>
</table>