Privileged Remote Access Integration with BeyondInsight and Password Safe

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

TC:3/4/2024

Table of Contents

BeyondTrust Privileged Remote Access Integration with Password Safe 3

Overview 3

Prerequisites 3

Configure Privileged Remote Access for Integration with Password Safe 5

Create an OAuth API Account 5

Configure Password Safe for Integration with Privileged Remote Access 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

Configure the Endpoint Credential Manager Plugin for Integration with Privileged Remote Access 9

Install the Endpoint Credential Manager 9

Install and Configure the Plugin 11

Test Plugin Settings 13

Search External Jump Items Using Privileged Remote Access Consoles 17

Prerequisites and Limitations 17

Enable External Jump Items Search 17

Search for External Jump Items 18

Configure Database Connection to Enable Privileged Remote Access Dashboard in BeyondInsight 19

Overview 19

Prerequisites 19

Network Considerations 19

Configure Database to Enable Privileged Remote Access Integration 19

View the Privileged Remote Access Dashboard in BeyondInsight 20

Database Recommendation 21

Troubleshoot the Privileged Remote Access and Password Safe Integration 22

Common Issues and Resolution Steps 22

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

BeyondTrust Privileged Remote Access 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. 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 desktop and web access consoles.

The integration enables:

- One-click password injection and session spawning
- Credentials never to 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 Privileged Remote Access. 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. Privileged Remote Access 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 BeyondTrustPrivileged Remote Accessand Password Safe.

For more information on installing and using the ECM plugin, please see "Configure the Endpoint Credential Manager Plugin for Integration with Privileged Remote Access" on page 9.

Prerequisites

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

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

- 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.

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

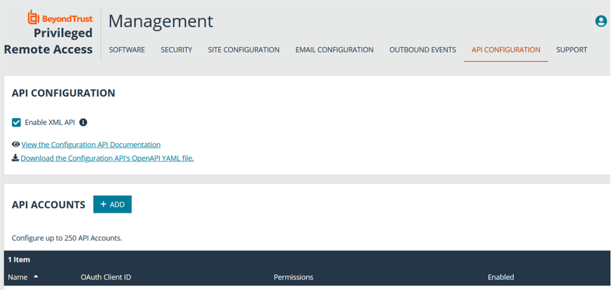
Configure Privileged Remote Access for Integration with Password Safe

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 Privileged Remote Access Command API calls to Privileged Remote Access.

1. In **/login**, navigate to **Management > API Configuration**.
2. Click **Add**.



API CONFIGURATION

☑ Enable XML API

View the Configuration API Documentation

Download the Configuration API's OpenAPI YAML file.

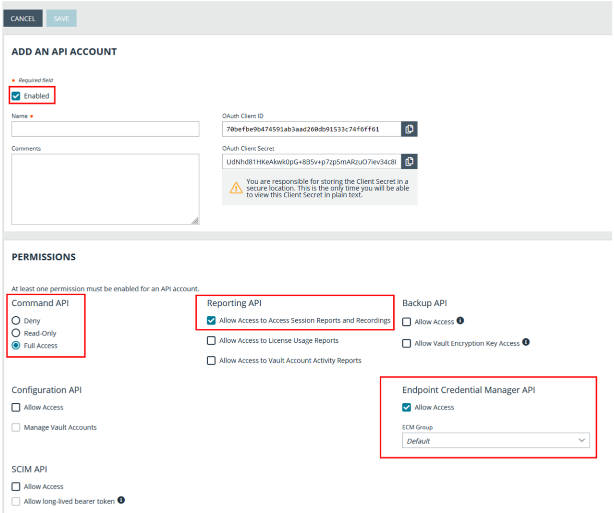
API ACCOUNTS

Configure up to 250 API Accounts.

1 Item

Name	OAuth Client ID	Permissions	Enabled

3. Check **Enabled**.
4. Enter a name for the account.
5. **OAuth Client ID** and **OAuth Client Secret** are used during the OAuth configuration step 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**.



ADD AN API ACCOUNT

• Required field

☑ Enabled

Name •

OAuth Client ID: 70befbe9b474591ab3aad260db91533c74f6ff61

Comments

OAuth Client Secret: UdNhd81HKeAkwk0pG+8B5v+p7zp5mARzuO7iev34c8l

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.

Command API
○ Deny
○ Read-Only
● Full Access

Reporting API
☑ Allow Access to Access Session Reports and Recordings
☐ Allow Access to License Usage Reports
☐ Allow Access to Vault Account Activity Reports

Backup API
☐ Allow Access
☐ Allow Vault Encryption Key Access

Configuration API
☐ Allow Access
☐ Manage Vault Accounts

Endpoint Credential Manager API
☑ Allow Access
ECM Group: Default

SCIM API
☐ Allow Access
☐ Allow long-lived bearer token

> ***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** at the top of the page to create the account.

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

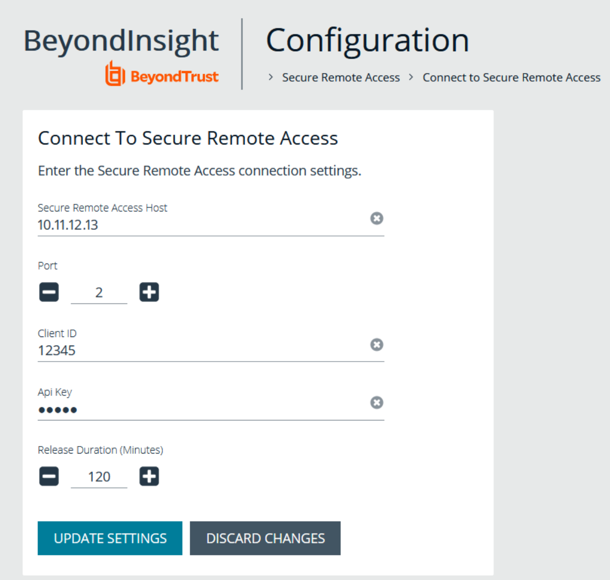
Configure Password Safe for Integration with Privileged Remote Access

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 Privileged Remote Access instance.
3. Obtain the **OAuth Client ID** and **OAuth Client Secret** for the API account you created in Privileged Remote Access, 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**.



Connect To Secure Remote Access

Enter the Secure Remote Access connection settings.

Secure Remote Access Host
10.11.12.13

Port
2

Client ID
12345

Api Key
●●●●●

Release Duration (Minutes)
120

Upon completion of this form, BeyondInsight does the following:

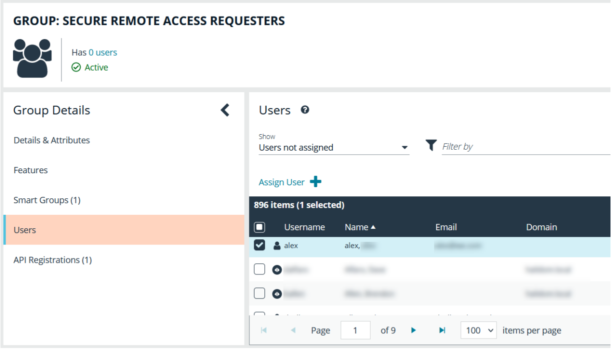
- Creates an all-day auto-approve access policy called **Secure Remote Access Approval Policy**
- Creates an API registration called **Secure Remote Access Integration**
- Creates a group called **Secure Remote Access Requesters** that uses the **Secure Remote Access Approval Policy** and the **Secure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

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

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.



GROUP: SECURE REMOTE ACCESS REQUESTERS

Has 0 users
Active

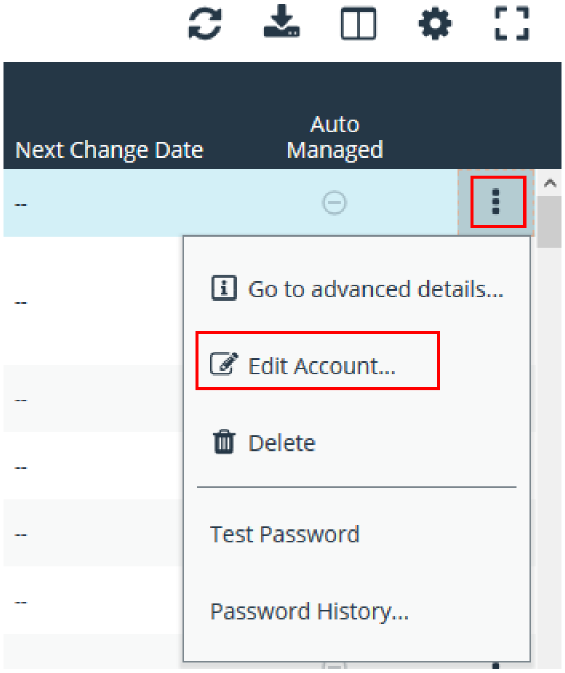
896 items (1 selected)

□	Username	Name ▲	Email	Domain
☑	alex	alex, [redacted]	[redacted]	
□	[redacted]	[redacted]		[redacted]
□	[redacted]	[redacted]		[redacted]

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.

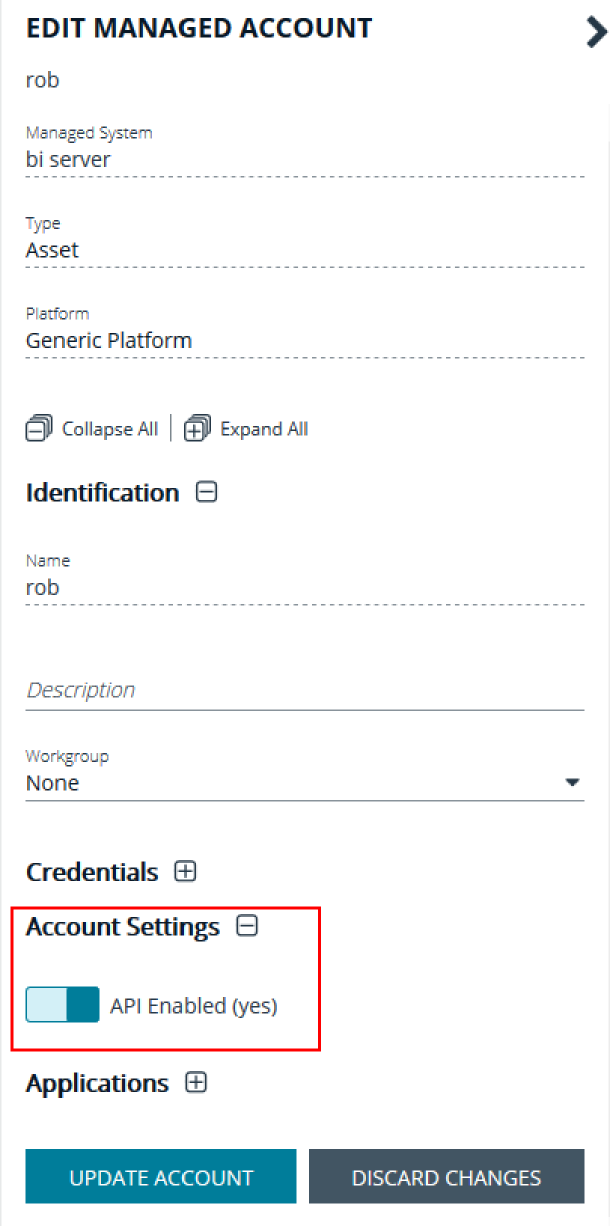
1. In the BeyondInsight Console, select **Managed Accounts**.
2. Select the managed account, and then click the vertical ellipsis button.
3. Select **Edit Account**.



©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

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

Identification

Name: rob

Description

Workgroup: None

Account Settings

API Enabled (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 Privileged Remote Access using credentials stored in Password Safe .

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

Configure the Endpoint Credential Manager Plugin for Integration with Privileged Remote Access

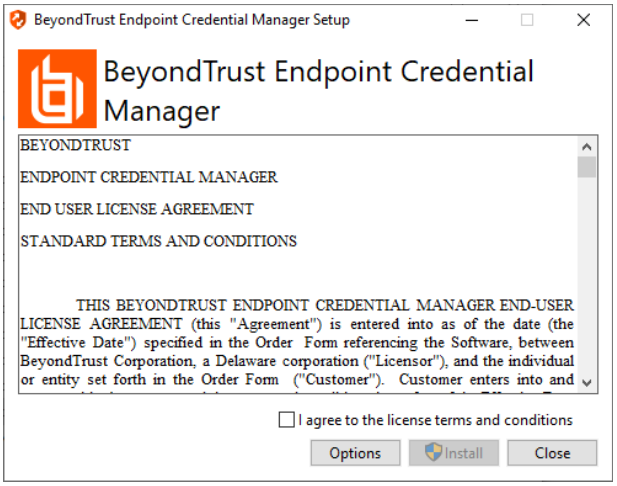
The ECM must be installed on a system with the following requirements:

- 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 at beyondtrustcorp.service-now.com/csm.
2. Start the BeyondTrust Endpoint Credential Manager Setup Wizard.
3. Agree to the EULA terms and conditions. Check the box 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.



BeyondTrust Endpoint Credential Manager Setup
BeyondTrust Endpoint Credential Manager
□ I agree to the license terms and conditions
Options
Install
Close

BEYONDTRUST

ENDPOINT CREDENTIAL MANAGER

END USER LICENSE AGREEMENT

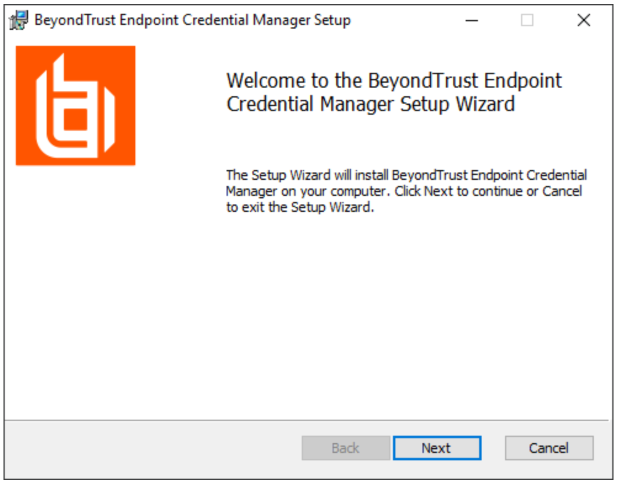
STANDARD TERMS AND CONDITIONS

THIS BEYONDTRUST ENDPOINT CREDENTIAL MANAGER END-USER LICENSE AGREEMENT (this "Agreement") is entered into as of the date (the "Effective Date") specified in the Order Form referencing the Software, between BeyondTrust Corporation, a Delaware corporation ("Licensor"), and the individual or entity set forth in the Order Form ("Customer"). Customer enters into and

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

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

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

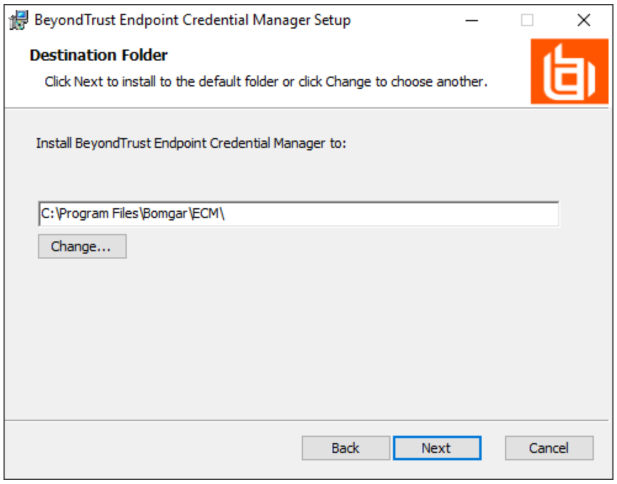


BeyondTrust Endpoint Credential Manager Setup

Welcome to the BeyondTrust Endpoint Credential Manager Setup Wizard

The Setup Wizard will install BeyondTrust Endpoint Credential Manager on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

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.



BeyondTrust Endpoint Credential Manager Setup

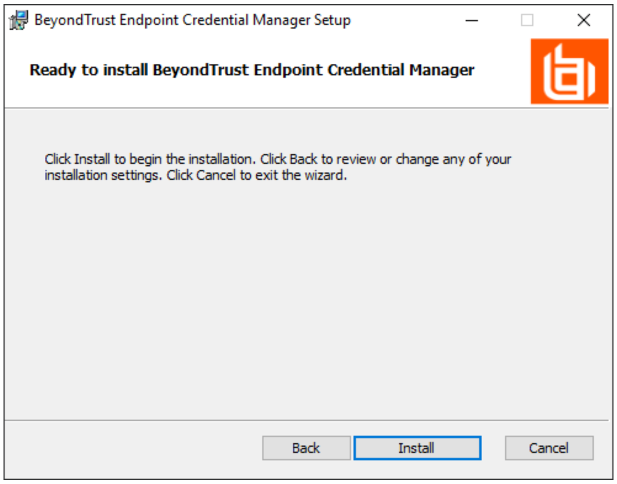
Destination Folder

Click Next to install to the default folder or click Change to choose another.

Install BeyondTrust Endpoint Credential Manager to:

C:\Program Files\Bomgar\ECM\

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



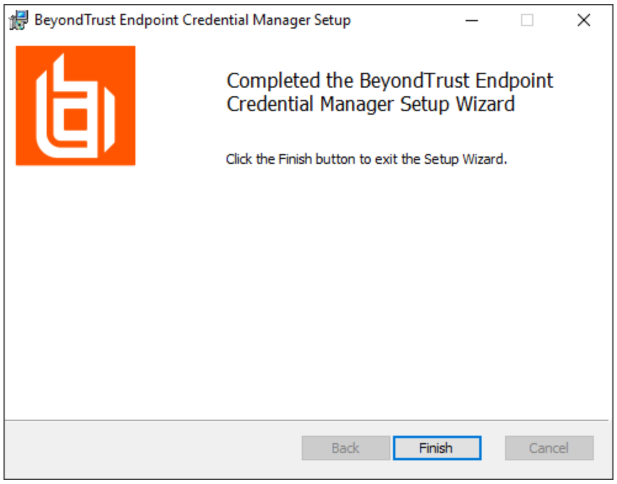
BeyondTrust Endpoint Credential Manager Setup

Ready to install BeyondTrust Endpoint Credential Manager

Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

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



Completed the BeyondTrust Endpoint Credential Manager Setup Wizard

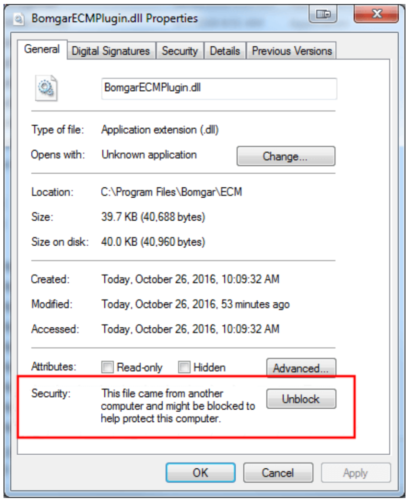
Click the Finish button to exit the Setup Wizard.

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

> ***Note:*** *When ECMs are connected in a high availability configuration, the BeyondTrust Appliance B Seriesroutes requests to the ECM in the ECM Group 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.



BomgarECMPlugin.dll

Type of file: Application extension (.dll)

Opens with: Unknown application

Location: C:\Program Files\Bomgar\ECM

Size: 39.7 KB (40,688 bytes)

Size on disk: 40.0 KB (40,960 bytes)

Created: Today, October 26, 2016, 10:09:32 AM

Modified: Today, October 26, 2016, 53 minutes ago

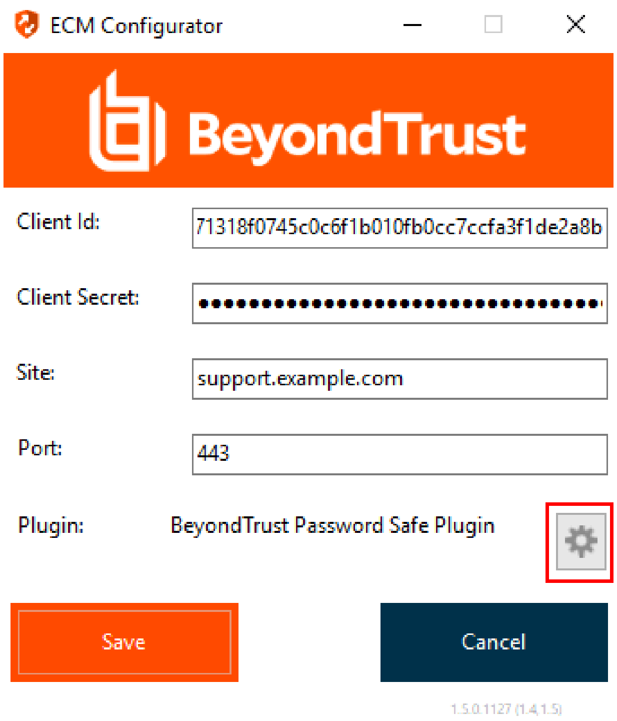
Accessed: Today, October 26, 2016, 10:09:32 AM

Attributes: □ Read-only □ Hidden

Security: This file came from another computer and might be blocked to help protect this computer.

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

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



Client Id: 71318f0745c0c6f1b010fb0cc7ccfa3f1de2a8b

Client Secret: ●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●

Site: support.example.com

Port: 443

Plugin: BeyondTrust Password Safe Plugin

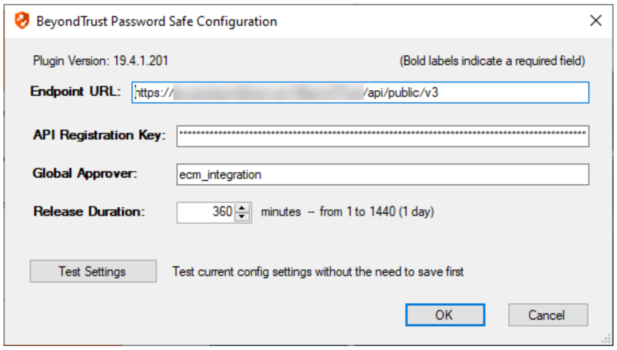
©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

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: https://[redacted]/api/public/v3

API Registration Key: ••

Global Approver: ecm_integration

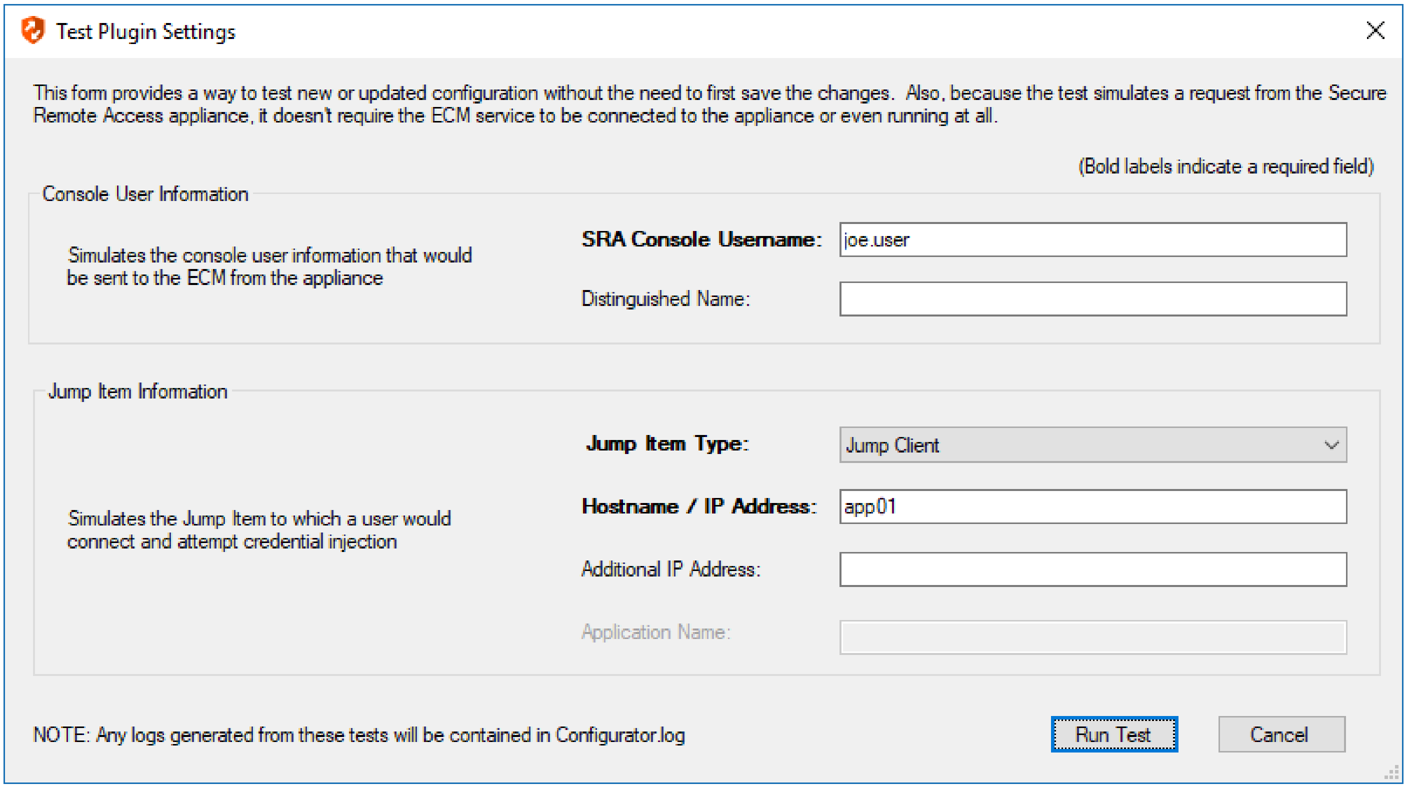
Release Duration: 360 minutes -- from 1 to 1440 (1 day)

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 access 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.*

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.



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: joe.user

Distinguished Name:

Jump Item Information

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

Jump Item Type: Jump Client

Hostname / IP Address: app01

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.

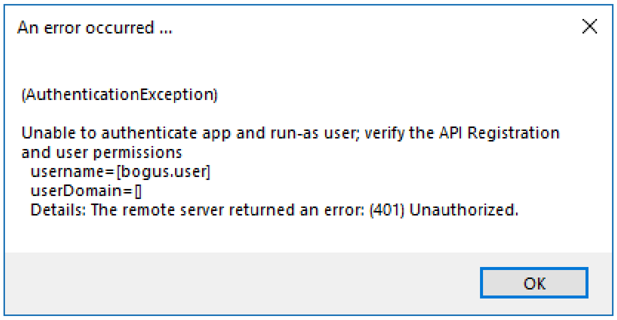
> ***Note:*** *The Jump Client type should be used to simulate Remote Jump and Local Jump items as well.*

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

- **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.



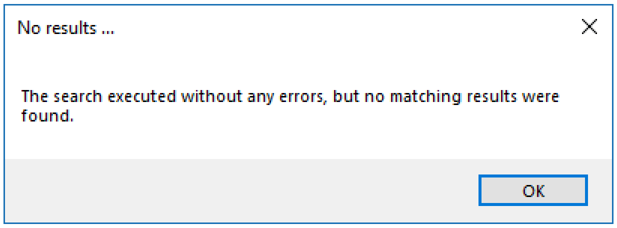
An error occurred ...

(AuthenticationException)

Unable to authenticate app and run-as user; verify the API Registration and user permissions
 username=[bogus.user]
 userDomain=[]
 Details: The remote server returned an error: (401) Unauthorized.

> ***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.

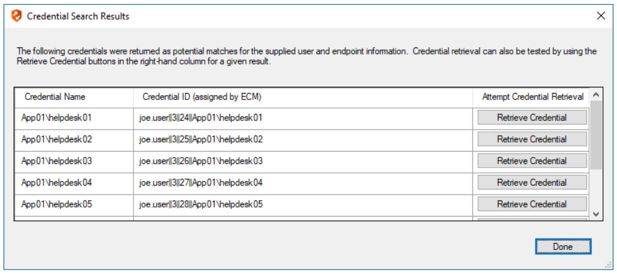


No results ...

The search executed without any errors, but no matching results were found.

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.



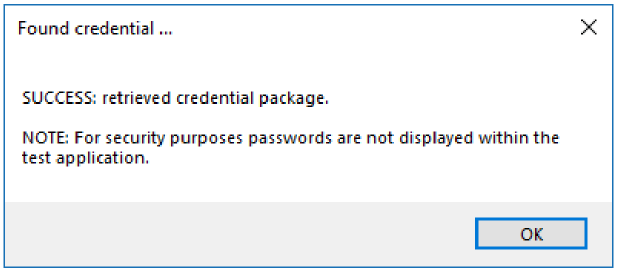
Credential Search Results

The following credentials were returned as potential matches for the supplied user and endpoint information. Credential retrieval can also be tested by using the Retrieve Credential buttons in the right-hand column for a given result.

<table>
<tr><th>Credential Name</th><th>Credential ID (assigned by ECM)</th><th>Attempt Credential Retrieval</th></tr>
<tr><td>App01\helpdesk01</td><td>joe.user||3||24||App01\helpdesk01</td><td>Retrieve Credential</td></tr>
<tr><td>App01\helpdesk02</td><td>joe.user||3||25||App01\helpdesk02</td><td>Retrieve Credential</td></tr>
<tr><td>App01\helpdesk03</td><td>joe.user||3||26||App01\helpdesk03</td><td>Retrieve Credential</td></tr>
<tr><td>App01\helpdesk04</td><td>joe.user||3||27||App01\helpdesk04</td><td>Retrieve Credential</td></tr>
<tr><td>App01\helpdesk05</td><td>joe.user||3||28||App01\helpdesk05</td><td>Retrieve Credential</td></tr>
</table>

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

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



Found credential ...

SUCCESS: retrieved credential package.

NOTE: For security purposes passwords are not displayed within the test application.

***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.*

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

Search External Jump Items Using Privileged Remote Access Consoles

Prerequisites and Limitations

The Password Safe and ECM integration must be fully configured before Managed Systems can be searched and accessed from PRA Consoles. The Password Safe installation must use the same user authentication method as Privileged Remote Access.

Searching and accessing Password Safe Managed Systems requires a deployed Jumpoint in PRA, as all sessions started from External Jump Items are performed using a Jumpoint. A Jumpoint must be positioned on the network to have connectivity to potentially any of the External Jump Items returned by the ECM. In the case where multiple Jumpoints are deployed on endpoints across segmented networks, the Jumpoint used may be selected automatically by matching against an External Jump Item's Network ID.

This feature is available for Managed RDP and shell systems. Web Jump is not available, but is planned for a future release.

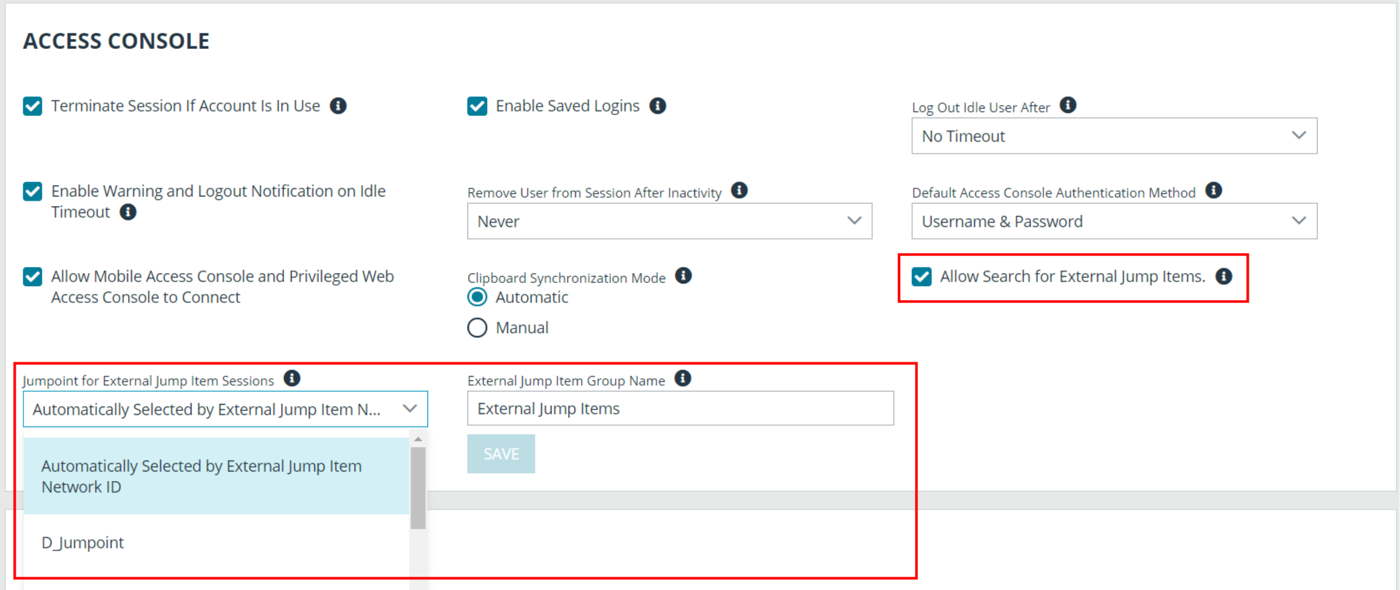
Clustered Jumpoints can be used, and external Jump Items do not count toward the endpoint license count.

Enable External Jump Items Search

Search for External Jump Items must be enabled before use.

1. In **/login**, navigate to **Management > Security**.
2. Scroll down to **Access Console** section.
3. Check **Allow Search for External Jump Items**.
    - This setting does not take effect until the software is restarted.
    - A pop-up window provides the option to restart now by clicking **Yes** or to restart later by clicking **No**. If you click **No**, you can restart PRA later from the **Status** page in /login.
4. Select the **Jumpoint for External Jump Item Sessions** from the dropdown list of available Jumpoints, or leave the default selection of **Automatically Selected by External Jump Item Network ID** to allow PRA to determine which Jumpoint handles the session.
    - This setting is available only when **Allow Search for External Jump Items** is checked.
    - The **External Jump Item Network ID** is an attribute you must set on the Jumpoint from **Jump > Jumpoint** in /login. It is equivalent to the **Workgroup** attribute on managed systems in Password Safe. Its value is matched against the **Network ID** property for external Jump Items returned by the ECM to determine the Jumpoint to handle a session.
5. Optionally, enter an **External Jump Item Group Name**, or leave the default of **External Jump Items**.
    - This setting is available only when **Allow Search for External Jump Items** is checked.
    - This name displays as the Jump Group name when viewing Jump Items in the Access Console or the Web Access Console.
    - Click **Save** if you have modified the default group name.

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.



ACCESS CONSOLE

☑ Terminate Session If Account Is In Use

☑ Enable Saved Logins

Log Out Idle User After: No Timeout

☑ Enable Warning and Logout Notification on Idle Timeout

Remove User from Session After Inactivity: Never

Default Access Console Authentication Method: Username & Password

☑ 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: Automatically Selected by External Jump Item N...

Automatically Selected by External Jump Item Network ID

D_Jumpoint

External Jump Item Group Name: External Jump Items

Search for External Jump Items

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

1. From the console, view the list of Jump Items.
2. Select the Jump Group for external Jump Items. The name of this group is the name provided when you enabled external Jump Items 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 (endpoint) include the **Hostname/IP**, **Jump Method** (RDP or shell), and **Comments**. Click the Jump Item (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 Item Sessions** has not been selected when enabling external Jump Items search.*

4. Once a Jump Item (endpoint) has been accessed, it is available in the **Recently Used** group.

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

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 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.

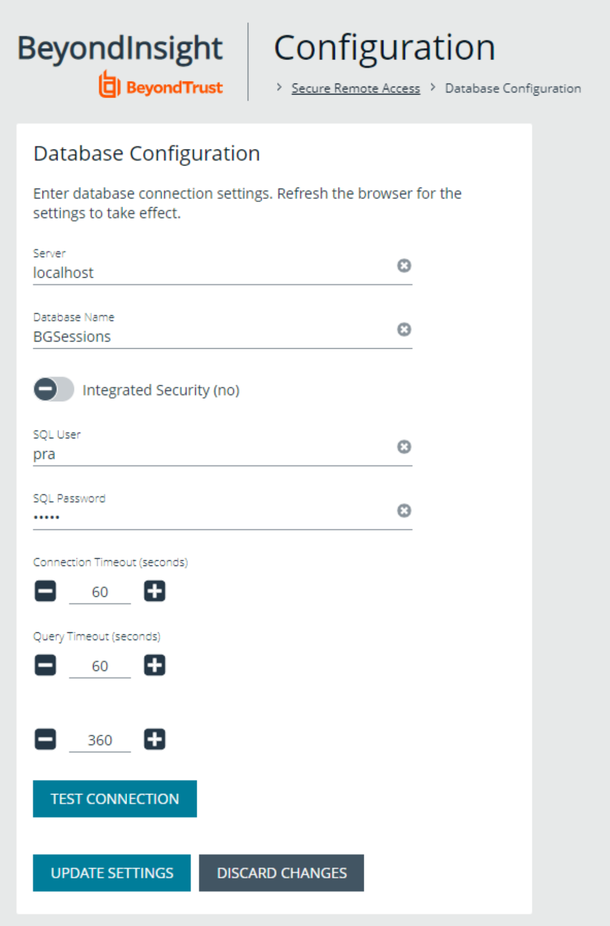
- The BeyondTrust Integration Client uses port 443 to make API calls to Privileged Remote Access.
- The BeyondTrust Integration Client uses port 1433 to store Privileged Remote Access session data in the **BGSessions** SQL server database.
- BeyondInsight uses port 1433 to query the **BGSessions** SQL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

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

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**.



Database Configuration

Enter database connection settings. Refresh the browser for the settings to take effect.

Server: localhost

Database Name: BGSessions

Integrated Security (no)

SQL User: pra

SQL Password: •••••

Connection Timeout (seconds): 60

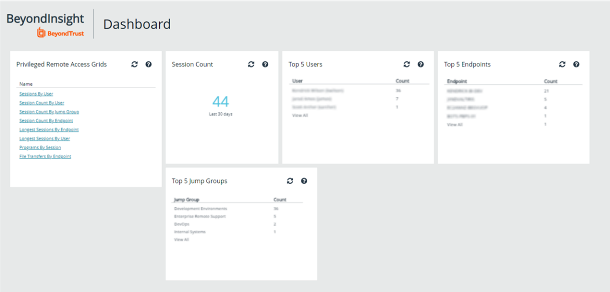
Query Timeout (seconds): 60

360

***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.



Privileged Remote Access Grids

Name
Sessions By User
Session Count By User
Session Count By Jump Group
Session Count By Endpoint
Longest Sessions By Endpoint
Longest Sessions By User
Programs By Session
File Transfers By Endpoint

Session Count: 44 Last 30 days

Top 5 Users

User	Count
[illegible]	36
[illegible]	7
[illegible]	1
View All	

Top 5 Endpoints

Endpoint	Count
[illegible]	21
[illegible]	5
[illegible]	4
[illegible]	1
View All	1

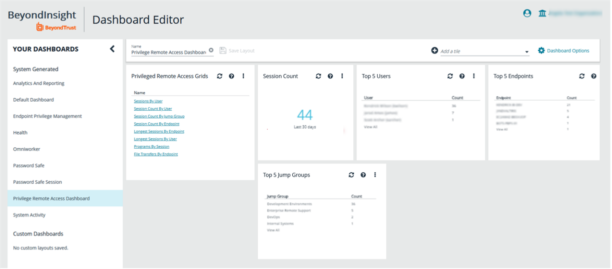
Top 5 Jump Groups

Jump Group	Count
Development Environments	36
Enterprise Remote Support	5
DevOps	2
Internal Systems	1
View All	

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

***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);
```

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

Troubleshoot the Privileged Remote Access 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: 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. ***Note:** The **Test Settings** feature does **NOT** communicate with BeyondTrust PRA at any point. It 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.*

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

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 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 PRA 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.
Credentials are returned via the **Test Settings** feature but are not available in the access 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 PRA 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 access 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 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.
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.

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.