



BeyondTrust

Privileged Remote Access Delinea Secret Server Integration

Table of Contents

Integrate BeyondTrust Privileged Remote Access with Delinea Secret Server	3
Prerequisites for the BeyondTrust Privileged Remote Access Integration with Delinea Secret Server	4
Applicable Versions	4
Network Considerations	4
Configure Delinea Secret Server for Integration with BeyondTrust Privileged Remote Access	5
Create API Account	5
Enable Web Services	6
Configure BeyondTrust Privileged Remote Access for Integration with Delinea Secret Server	7
Create an OAuth API Account	7
Allow ECM Connections	8
Configure the Delinea Secret Server Plugin for Integration with BeyondTrust Privileged Remote Access	9
Install the Endpoint Credential Manager	9
Install and Configure the Plugin	11

Integrate BeyondTrust Privileged Remote Access with Delinea Secret Server

IMPORTANT!

You must purchase this integration separately from your BeyondTrust Privileged Remote Access solution. For more information, contact BeyondTrust's Sales team.

BeyondTrust's Privileged Remote Access plugin integration to Delinea Secret Server enables automatic password injection to authorized systems through encrypted BeyondTrust connections, removing the need to share and expose credentials to privileged accounts. In addition to machine-specific credentials, the integration also has the ability to retrieve domain credentials that are not machine-specific, giving domain admins and other privileged users access to those credentials for use on endpoints on a domain.

The integration between BeyondTrust and Delinea enables:

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

The BeyondTrust Endpoint Credential Manager (ECM) enables the communication between Delinea Secret Server and BeyondTrust Privileged Remote Access. The ECM is deployed to a hardened Windows Server inside the firewall, typically in the same network as Secret Server. Once the ECM is 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 an access session, and the user is automatically logged in, having never seen the username/password combination.

Delinea Secret Server handles all elements of securing and managing the passwords, so policies that require the password to be rotated after use are supported. BeyondTrust Privileged Remote Access handles creating and managing access to the endpoint and then recording the session and controlling the level of access granted to the user, including what the user can see and do on that endpoint.

Prerequisites for the BeyondTrust Privileged Remote Access Integration with Delinea Secret Server

To complete this integration, please ensure that you have the necessary software installed and configured as indicated in this guide, accounting for any network considerations. The integration is provided in the form of a plugin (ZIP archive containing the necessary DLL files and other supporting files) for use within BeyondTrust's Endpoint Credential Manager (ECM).



Note: Please ensure you have acquired the proper version of the ECM to be compliant with the version of BeyondTrust Privileged Remote Access in use, and install the ECM according to the instructions in "[Configure the Delinea Secret Server Plugin for Integration with BeyondTrust Privileged Remote Access](#)" on page 9.

Applicable Versions

- BeyondTrust Privileged Remote Access: 15.x and later
- Delinea Secret Server: 8.9.0 and later

Network Considerations

The following network communication channels must be open for the integration to work properly.

Outbound From	Inbound To	TCP Port #	Purpose
ECM Server	BeyondTrust Appliance B Series	443	ECM calls to the BeyondTrust API.
ECM Server	Delinea Secret Server	443	ECM calls to Secret Server web services.



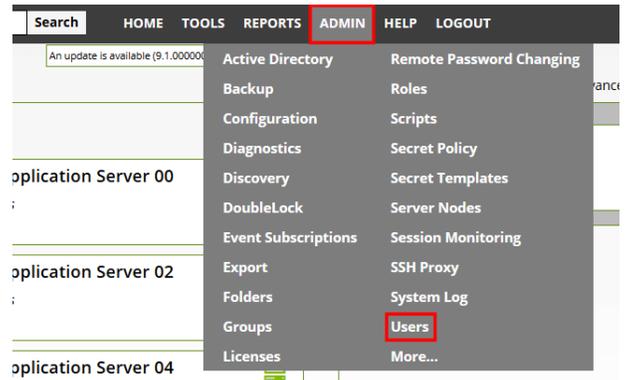
Note: The ECM can be obtained only with a paid BeyondTrust integration service.

Configure Delinea Secret Server for Integration with BeyondTrust Privileged Remote Access

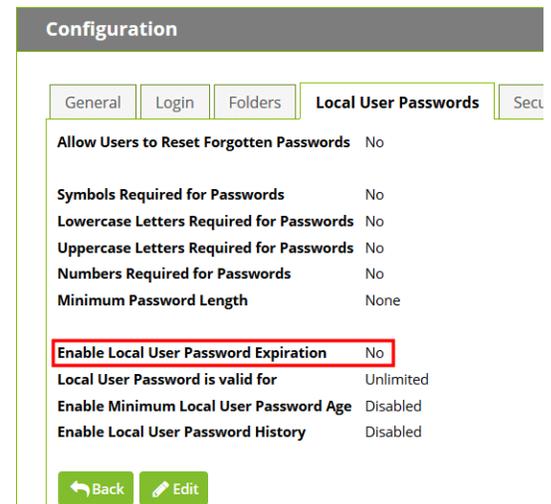
Sign in to Secret Server as an administrative user.

Create API Account

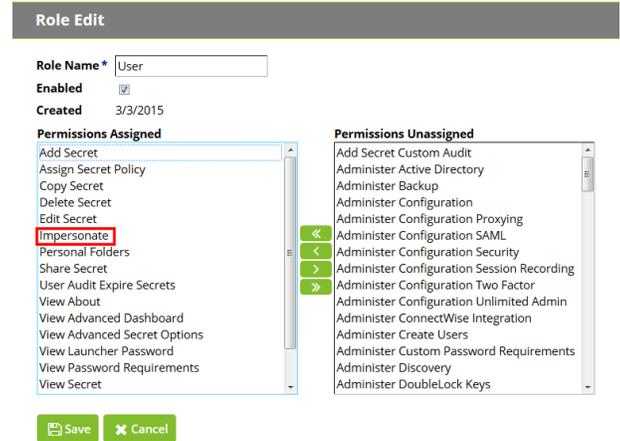
1. Under **Admin > Users**, click **Create New** to create a local user for API calls.



2. If the API account is the only local account, we recommend you disable local user password expiration so the ECM plugin integration does not break each time the password expires or changes. This setting is found under **Admin > Configuration > Local User Passwords**.

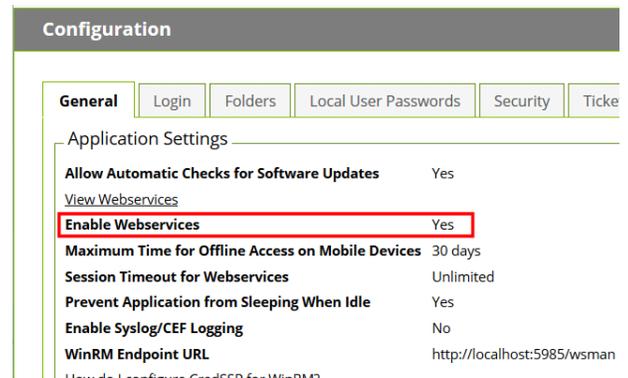


- Under **Admin > Roles**, edit the role in which the API account is a member (typically the **User** role). Click the role name in the list to view it, and then click the **Edit** button at the bottom of the page below the **Permissions** list.
- Ensure that the permission **Web Services Impersonate** (sometimes listed as just **Impersonate**) is added to the **Permissions Assigned** list.
- Click **Save** to update the role permissions.



Enable Web Services

- Under **Admin > Configuration**, click the **General** tab.
- In the **Application Settings** section, ensure the **Enable Webservices** setting is set to **Yes**.
- If not already enabled, click **Edit** at the bottom of the page, check the box to enable the services, and save the settings.



Configure BeyondTrust Privileged Remote Access for Integration with Delinea Secret Server

Several configuration changes are necessary on the B Series Appliance to integrate with Secret Server.

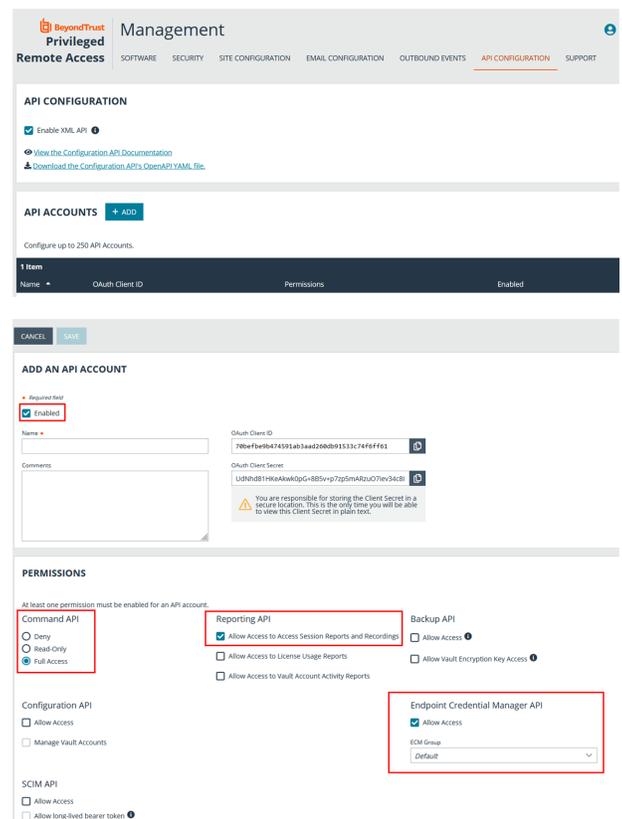
All of the steps in this section take place in the BeyondTrust `/login` administrative interface. Access your BeyondTrust interface by going to the hostname of your B Series Appliance followed by `/login`, for example: <https://access.example.com/login>.

Create an OAuth API Account

The Thycotic Secret Server API account is used from within Thycotic Secret Server to make Privileged Remote Access Command API calls to Privileged Remote Access.

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** are used during the OAuth configuration step in Thycotic Secret Server.
6. Set the following **Permissions**:
 - **Command API**: Full Access.
 - **Reporting API**: Allow Access to Access Session Reports and Recordings.
 - **Endpoint Credential Manager API**: Allow Access.
 - If ECM groups are enabled on the site, select which **ECM Group** to use. ECMs that are not associated with a group come under **Default**.



The screenshot shows the 'ADD AN API ACCOUNT' form in the BeyondTrust Management console. The 'Enabled' checkbox is checked. The 'Name' field is empty. The 'OAuth Client ID' field contains '7b0e7d0474591a83aed3f0b091533c74ff6f61'. The 'OAuth Client Secret' field contains 'LjDn8B1H6a8M4nG-r85v4p7z5m4Bzu07bc343f'. A warning message states: '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.' The 'PERMISSIONS' section shows 'Command API' with 'Full Access' selected, 'Reporting API' with 'Allow Access to Access Session Reports and Recordings' selected, and 'Endpoint Credential Manager API' with 'Allow Access' selected and 'ECM Group' set to 'Default'.

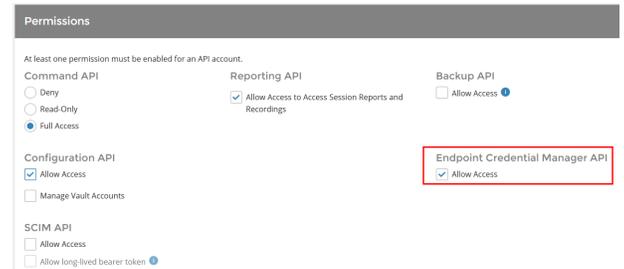
 **Note:** The ECM Group feature is only present if enabled when your site is built. If it is not present, please contact your site administrator.

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

Allow ECM Connections

PRA 20.1 and later

1. Go to `/login > Management > API Configuration`.
2. Add or edit an API account.
3. Under **Permissions**, check **Allow Access** for **Endpoint Credential Manager API**.



Permissions

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

Command API	Reporting API	Backup API
<input type="radio"/> Deny	<input checked="" type="checkbox"/> Allow Access to Access Session Reports and Recordings	<input type="checkbox"/> Allow Access
<input type="radio"/> Read-Only		
<input checked="" type="radio"/> Full Access		
Configuration API		Endpoint Credential Manager API
<input checked="" type="checkbox"/> Allow Access		<input checked="" type="checkbox"/> Allow Access
<input type="checkbox"/> Manage Vault Accounts		
SCIM API		
<input type="checkbox"/> Allow Access		
<input type="checkbox"/> Allow long-lived bearer token		

Configure the Delinea Secret Server Plugin for Integration with BeyondTrust Privileged Remote Access

Install the Endpoint Credential Manager

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

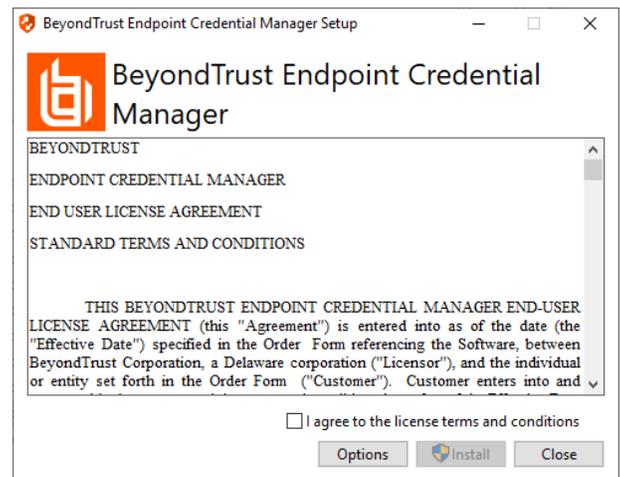
- Windows Vista or newer, 64-bit only
- .NET 4.5 or newer
- Processor: 2GHz or faster
- Memory: 2GB or greater
- Available Disk Space: 80GB or greater

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**.

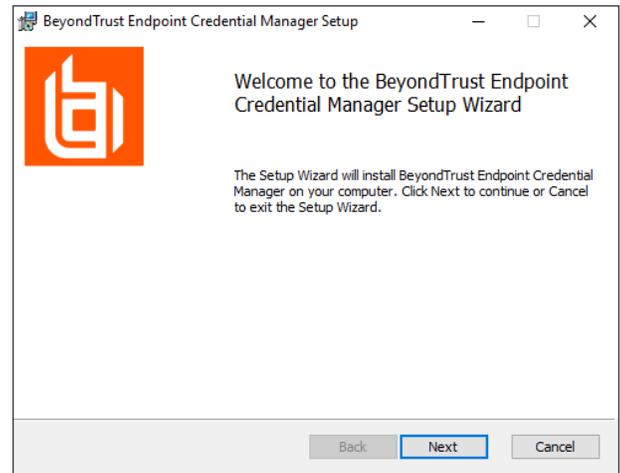
If you need to modify the ECM installation path, click the **Options** button to customize the installation location.



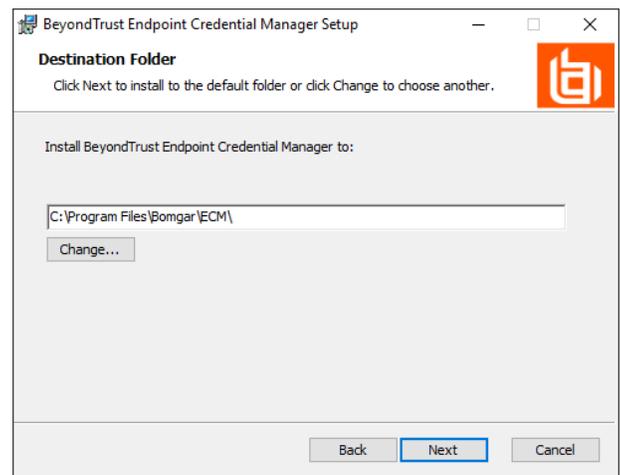
Note: You are not allowed to proceed with the installation unless you agree to the EULA.



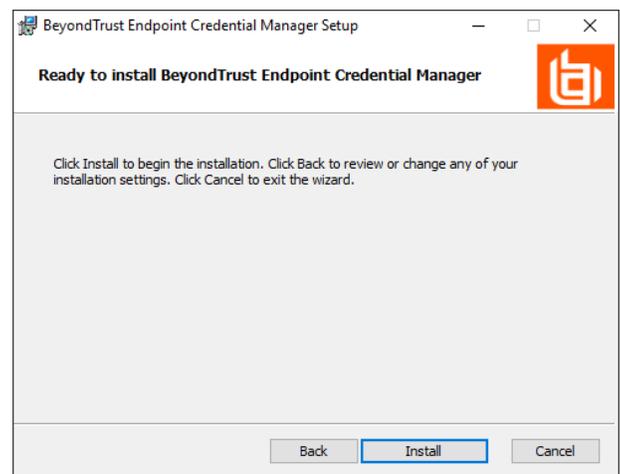
4. Click **Next** on the Welcome screen.



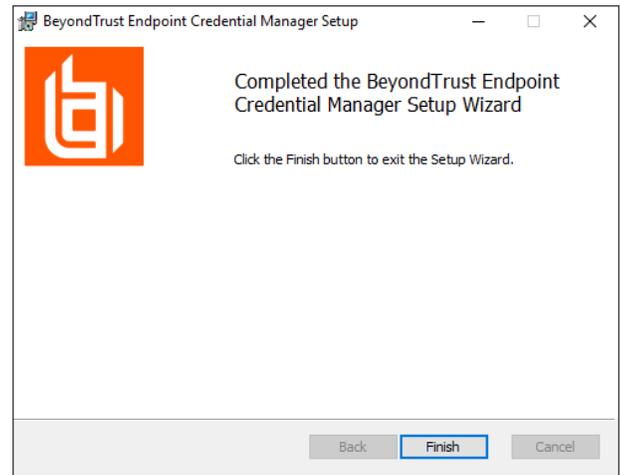
5. Choose a location for the credential manager, and then click **Next**.
6. On the next screen, you can begin the installation or review any previous step.



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



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

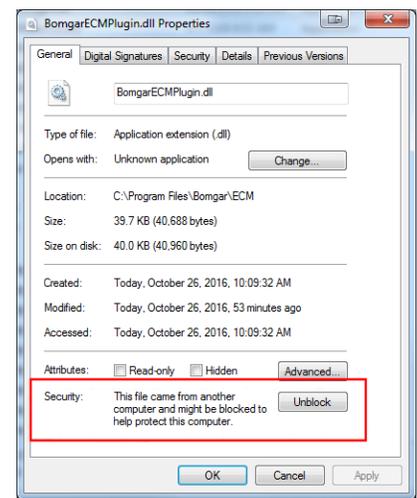


Note: To ensure optimal up-time, administrators can install up to three ECMs on different Windows machines to communicate with the same credential store. A list of the ECMs connected to the appliance site can be found at **/login > Status > Information > ECM Clients**.

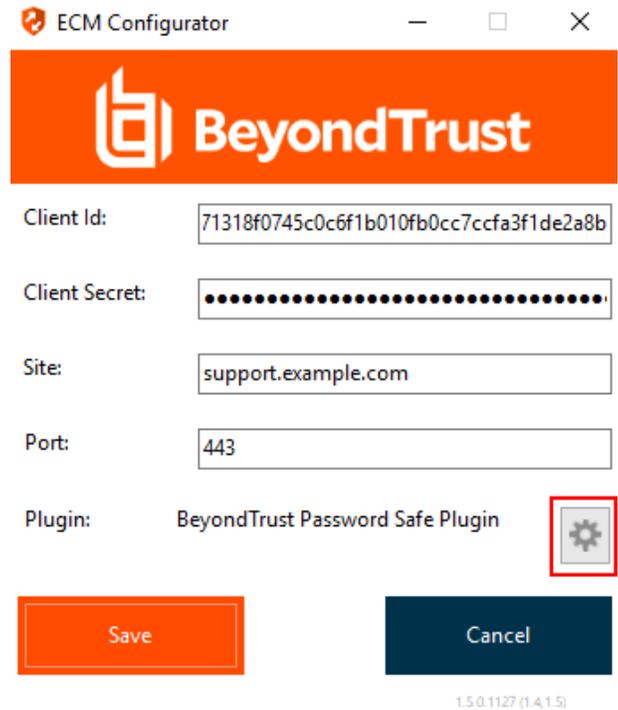
Note: When ECMs are connected in a high availability configuration, the BeyondTrust Appliance B Series routes requests to the ECM in the ECM Group that has been connected to the appliance the longest.

Install and Configure the Plugin

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



ECM Configurator

BeyondTrust

Client Id:

Client Secret:

Site:

Port:

Plugin: BeyondTrust Password Safe Plugin 

1.5.0.1127 (1.4.1.5)

5. The following settings are available:

Setting Name	Description	Notes	Required
Endpoint URL	The full URL to the Secret Server web services	e.g., https://<delinea-server-hostname>/SecretServer/webservices/SSWebservice.asmx	Yes
API User	Username of the API account created in Secret Server		Yes
API Password	Password of the above user		Yes
API Domain	Domain of the API account created in Secret Server	Used only if the API account is not a local user in Secret Server	No
API Organization	Organization of the API account created in Secret Server	Not typically used for such accounts	No
Include domain credentials for	When checked, in addition to retrieving machine-specific credentials for the select endpoint, it also retrieves domain credentials where the domain field (configured below) matches one of the configured domains	This field can contain multiple domains separated with commas	No

Setting Name	Description	Notes	Required
Domain Field	API web service field containing domain names	The default value of Domain should be left unless an organization is using another field to store this information on domain secrets	Yes
Machine Field	API web service field containing machine names	The default value of Machine should be left unless an organization is using another field to store this information on machine-specific secrets	Yes
Default Domain for Local BeyondTrust Users	When a value is supplied, the plugin initially attempts to retrieve credentials for the user with the username from BeyondTrust and the configured default domain	This setting is necessary if some or all BeyondTrust users are local users but the corresponding accounts in Secret Server are domain accounts with the same username portion	No
Enable fall-back to local account if domain account not found	When checked, the plugin first attempts to retrieve credentials for the user as a domain user and then, if no match is found, makes a second attempt without the domain	This setting is necessary if some or all BeyondTrust users are domain users but the corresponding accounts in Secret Server are domain accounts with the same username portion	No
Include default organization	If enabled, the supplied organization is included when querying for a matching Secret Server user		No

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.

 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.

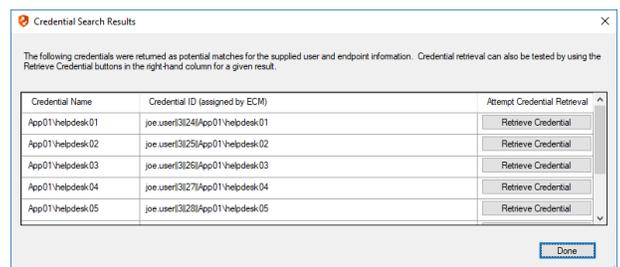
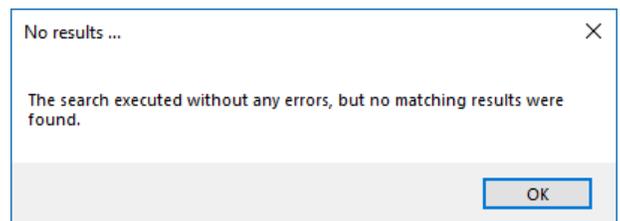
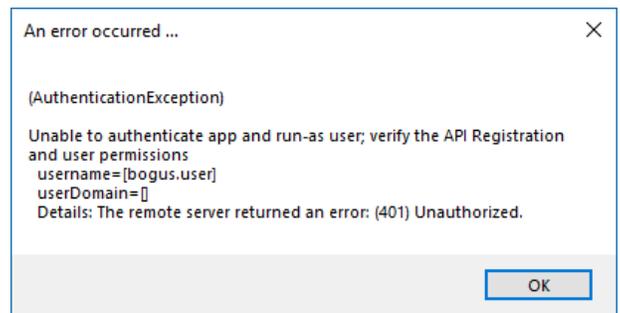


Note: *It's important to note that, either way, the same information is included in the **Configurator.log**, along with more detail as to exactly what point in the execution the failure occurred.*

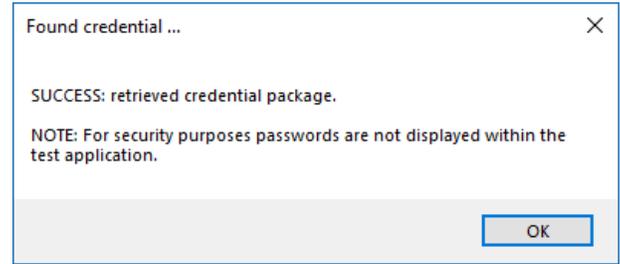
It's possible that the test succeeds in that it doesn't encounter any errors and yet it doesn't return any credentials. Because this is a perfectly valid result, it is not treated as an error.

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.



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.

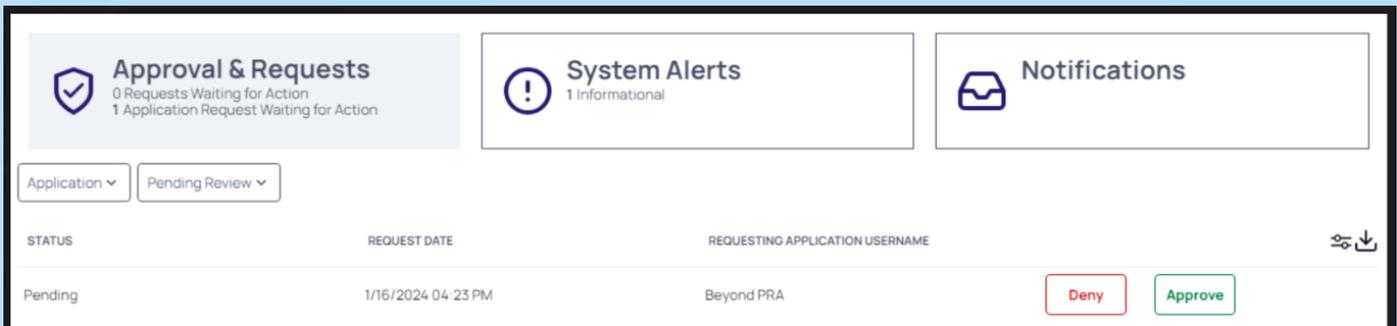


IMPORTANT!

Access to individual Secret Server user secrets is handled by a delegated trust feature built into Secret Server. This means that a user can grant access to their secrets to an API user.

The first time a user attempts to access an endpoint via the BeyondTrust access console, a request for this access is generated, and an email is sent to the user, stating "An Application, BeyondTrust PRA, is requesting access to [SecretServer] on your behalf."

The user must click the link in the email, and approve or deny the request in the Delinea web UI. Approving the requests grants the API user access to their credentials for future sessions.



This access can be revoked by the user at any time. If for some reason the email is not received, the page to manage this access is available to all Secret Server users under **Tools > Manage Applications**.

When using the **Test Settings** button to test the retrieval of secrets for a user who has NOT approved access for the API account, the resulting dialog for the test is similar to the screen shot below.

