BeyondTrust

Privileged Remote Access
Thycotic Secret Server Integration

TC:5/14/2019

Table of Contents

BeyondTrust Privileged Remote Access Integration with Thycotic Secret Server

IMPORTANT!

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

BeyondTrust's Privileged Remote Access plugin integration to Thycotic 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 Thycotic 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 pre-configured VPN or other routing in place
- Passwords always stored securely in Thycotic Secret Server

The BeyondTrust Endpoint Credential Manager (ECM) enables the communication between Thycotic 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.

Thycotic 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 Thycotic 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). 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 Thycotic Secret Server Plugin for Integration with BeyondTrust Privileged Remote Access" on page 9.

Applicable Versions

- BeyondTrust Privileged Remote Access: 15.x and newer
- Thycotic Secret Server: 8.9.0 and newer

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	443	ECM calls to the BeyondTrust API.
ECM Server	Thycotic Secret Server	443	ECM calls to Secret Server web services.

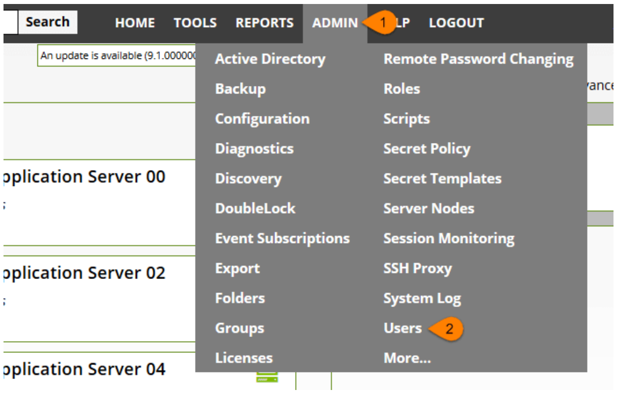
***Note:** The ECM can be obtained only with a paid BeyondTrust integration service.*

Configure Thycotic Secret Server for Integration with BeyondTrust Privileged Remote Access

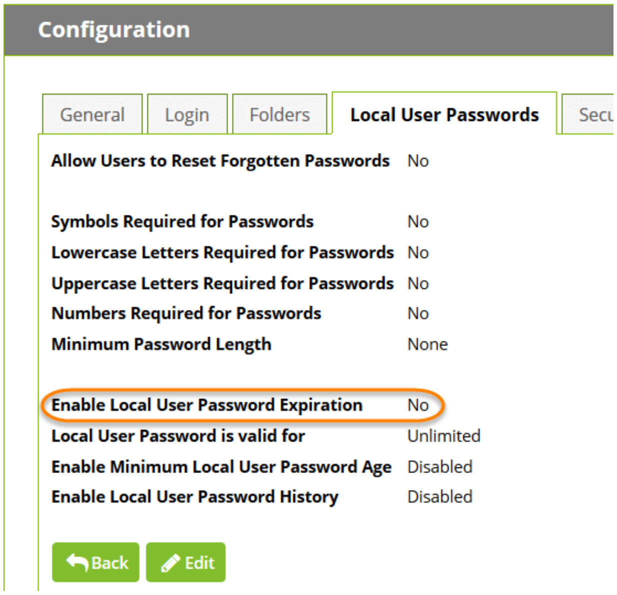
Sign into Secret Server as an administrative user.

Create API Account

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

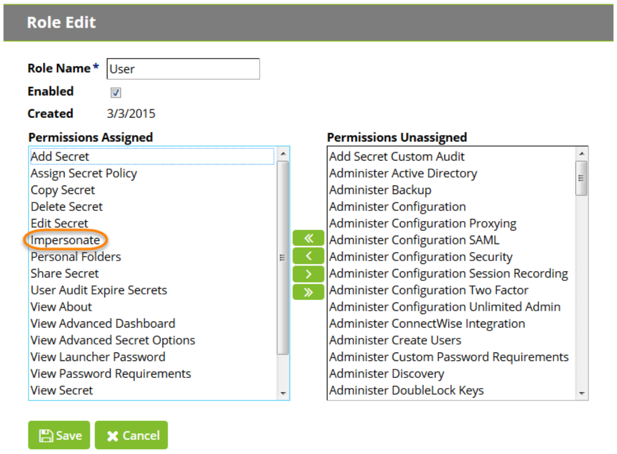


2. If the API account is the only local account, it is recommended to disable local user password expiration so the ECM plugin integration does not break each time the password expires or changes. This setting is found under **Admin > Configuration > Local User Passwords**.



Allow Users to Reset Forgotten Passwords	No
Symbols Required for Passwords	No
Lowercase Letters Required for Passwords	No
Uppercase Letters Required for Passwords	No
Numbers Required for Passwords	No
Minimum Password Length	None
Enable Local User Password Expiration	No
Local User Password is valid for	Unlimited
Enable Minimum Local User Password Age	Disabled
Enable Local User Password History	Disabled

3. 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.
4. Ensure that the permission **Web Services Impersonate** (sometimes listed as just **Impersonate**) is added to the **Permissions Assigned** list.
5. Click **Save** to update the role permissions.



Role Edit

Role Name*	User
Enabled	☑
Created	3/3/2015

Permissions Assigned

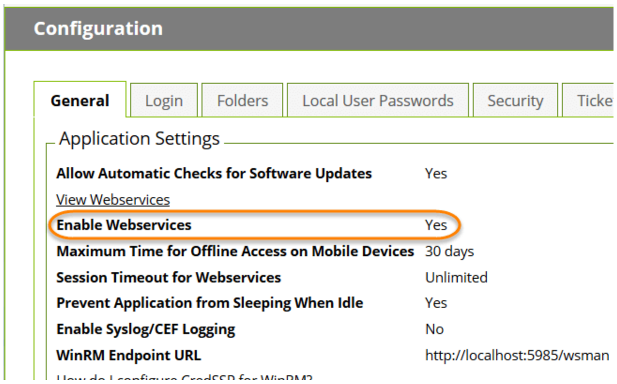
Add Secret
Assign Secret Policy
Copy Secret
Delete Secret
Edit Secret
Impersonate
Personal Folders
Share Secret
User Audit Expire Secrets
View About
View Advanced Dashboard
View Advanced Secret Options
View Launcher Password
View Password Requirements
View Secret

Permissions Unassigned

Add Secret Custom Audit
Administer Active Directory
Administer Backup
Administer Configuration
Administer Configuration Proxying
Administer Configuration SAML
Administer Configuration Security
Administer Configuration Session Recording
Administer Configuration Two Factor
Administer Configuration Unlimited Admin
Administer ConnectWise Integration
Administer Create Users
Administer Custom Password Requirements
Administer Discovery
Administer DoubleLock Keys

Enable Web Services

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



Configuration

Application Settings

Allow Automatic Checks for Software Updates	Yes
View Webservices	
Enable Webservices	Yes
Maximum Time for Offline Access on Mobile Devices	30 days
Session Timeout for Webservices	Unlimited
Prevent Application from Sleeping When Idle	Yes
Enable Syslog/CEF Logging	No
WinRM Endpoint URL	http://localhost:5985/wsman
How do I configure CredSSP for WinRM?	

Configure BeyondTrust Privileged Remote Access for Integration with Thycotic Secret Server

Several configuration changes are necessary on the BeyondTrust 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 BeyondTrust Appliance followed by /login (e.g., **https://access.example.com/login**).

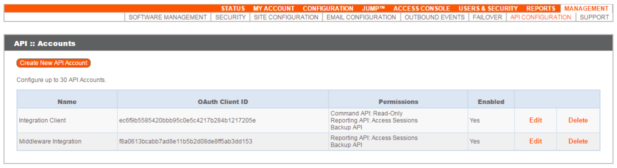
Create an API Service Account - BeyondTrust 16.1 and Earlier

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

1. Go to **/login > Users & Security > Users**.
2. Click **Create New User** and name it **Integration** or something similar.
3. Leave **Must Reset Password at Next Login** unchecked.
4. Set **Password Expires On** to **Never Expires**.
5. Check **Administrator**.
6. Scroll to the bottom and save the account.

Create an API Service Account - BeyondTrust 16.2 and Later

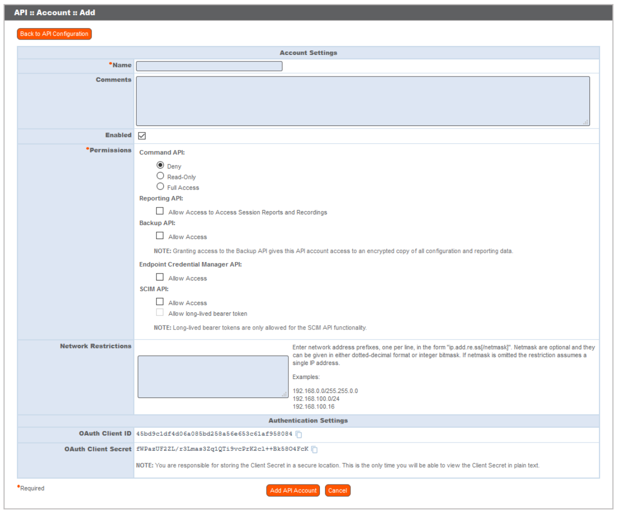
1. Go to **Management > API Configuration** and create a new API account.



Configure up to 30 API Accounts.

Name	OAuth Client ID	Permissions	Enabled		
Integration Client	ec6f9b5585420bbb95c0e5c4217b284b1217205e	Command API: Read-Only Reporting API: Access Sessions Backup API	Yes	Edit	Delete
Middleware Integration	f8a0613bcabb7ad8e11b5b2d08de8ff5ab3dd153	Reporting API: Access Sessions Backup API	Yes	Edit	Delete

2. Under **Permissions**, check **Full Access** to the **Command API**.
3. For the **Reporting API**, check **Allow Access to Support Session Reports and Recordings** and **Allow Access to Presentation Session Reports and Recordings**. Also be sure to copy the values for both the **OAuth Client ID** and **OAuth Client Secret** for use in a later step.



•Name	
Comments	
Enabled	☑
•Permissions	Command API: ● Deny ○ Read-Only ○ Full Access Reporting API: ☐ Allow Access to Access Session Reports and Recordings Backup API: ☐ Allow Access NOTE: Granting access to the Backup API gives this API account access to an encrypted copy of all configuration and reporting data. Endpoint Credential Manager API: ☐ Allow Access SCIM API: ☐ Allow Access ☐ Allow long-lived bearer token NOTE: Long-lived bearer tokens are only allowed for the SCIM API functionality.
Network Restrictions	Enter network address prefixes, one per line, in the form "ip.add.re.ss[/netmask]". Netmask are optional and they can be given in either dotted-decimal format or integer bitmask. If netmask is omitted the restriction assumes a single IP address. Examples: 192.168.0.0/255.255.0.0 192.168.100.0/24 192.168.100.16
OAuth Client ID	45bd9c1df4d06a085bd258a56e653c61af958084
OAuth Client Secret	fWPazUF2ZL/r3Lmas3Zq1QTi9vcPrK2cl++Bk5804FcK NOTE: You are responsible for storing the Client Secret in a secure location. This is the only time you will be able to view the Client Secret in plain text.

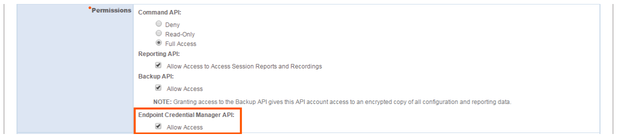
•Required

4. Click **Add API Account** to create the account.

Allow ECM Connections

PRA 17.1 and Later

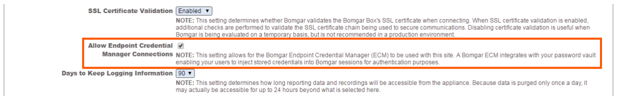
1. Go to **/login > Management > API Configuration**.
2. Add or edit an API account.
3. For **Endpoint Credential Manager API**, check **Allow Access**.



•Permissions	Command API: ○ Deny ○ Read-Only ● Full Access Reporting API: ☑ Allow Access to Access Session Reports and Recordings Backup API: ☑ Allow Access NOTE: Granting access to the Backup API gives this API account access to an encrypted copy of all configuration and reporting data. Endpoint Credential Manager API: ☑ Allow Access

Prior to PRA 17.1

1. Go to **Management > Security**.
2. Ensure the box **Allow Endpoint Credential Manager Connections** is checked.



SSL Certificate Validation	Enabled ▾ NOTE: This setting determines whether Bomgar validates the Bomgar Box's SSL certificate when connecting. When SSL certificate validation is enabled, additional checks are performed to validate the SSL certificate chain being used to secure communications. Disabling certificate validation is useful when Bomgar is being evaluated on a temporary basis, but is not recommended in a production environment.
Allow Endpoint Credential Manager Connections	☑ NOTE: This setting allows for the Bomgar Endpoint Credential Manager (ECM) to be used with this site. A Bomgar ECM integrates with your password vault enabling your users to inject stored credentials into Bomgar sessions for authentication purposes.
Days to Keep Logging Information	90 ▾ NOTE: This setting determines how long reporting data and recordings will be accessible from the appliance. Because data is purged only once a day, it may actually be accessible for up to 24 hours beyond what is selected here.

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

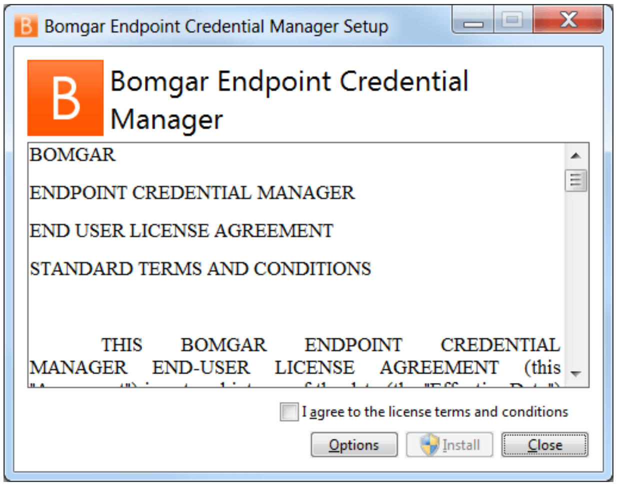
Install the Endpoint Credential Manager

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**

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

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



Bomgar Endpoint Credential Manager Setup

Bomgar Endpoint Credential Manager

BOMGAR

ENDPOINT CREDENTIAL MANAGER

END USER LICENSE AGREEMENT

STANDARD TERMS AND CONDITIONS

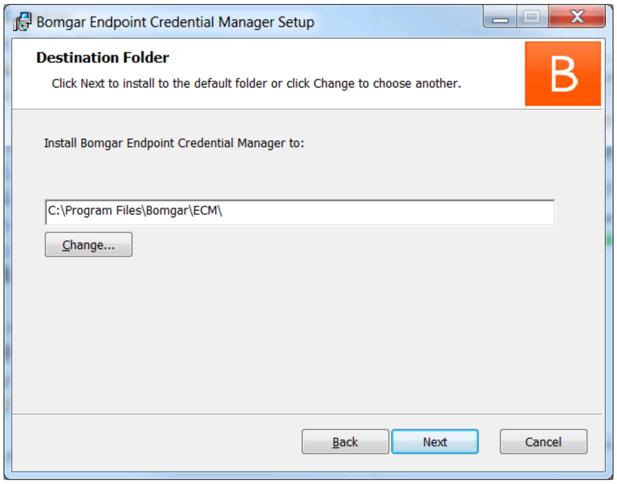
THIS BOMGAR ENDPOINT CREDENTIAL MANAGER END-USER LICENSE AGREEMENT (this

□ I agree to the license terms and conditions

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

1. Click **Install**.

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



Bomgar Endpoint Credential Manager Setup

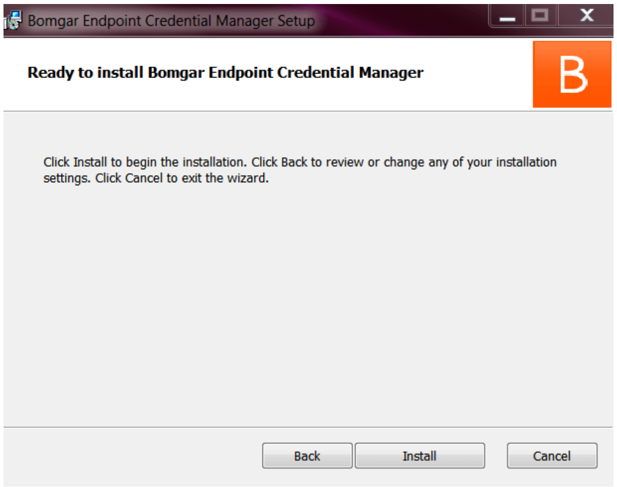
Destination Folder

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

Install Bomgar Endpoint Credential Manager to:

C:\Program Files\Bomgar\ECM\

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

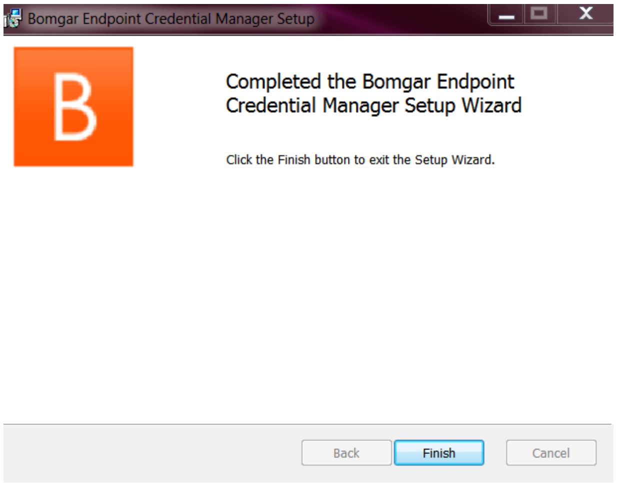


Bomgar Endpoint Credential Manager Setup

Ready to install Bomgar 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.

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



Bomgar Endpoint Credential Manager Setup

Completed the Bomgar Endpoint Credential Manager Setup Wizard

Click the Finish button to exit the Setup Wizard.

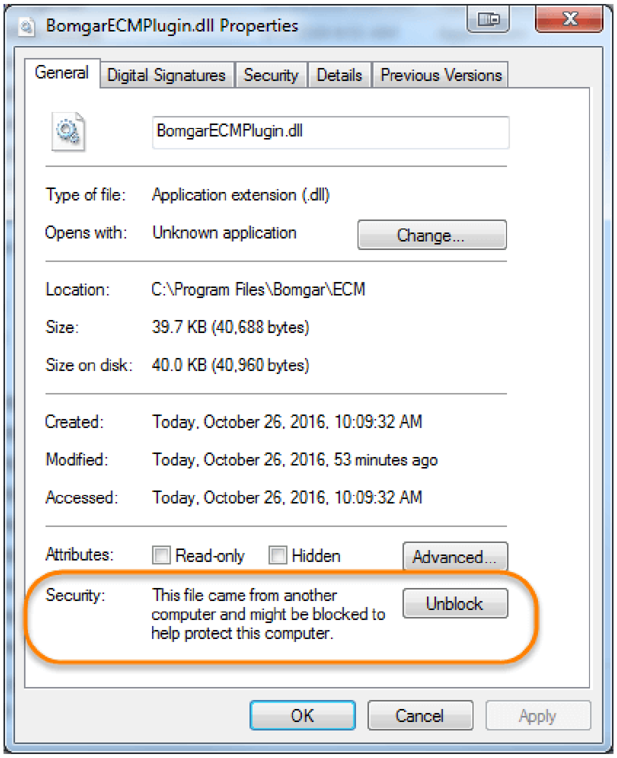
Note: *To ensure optimal up-time, administrators can install up to five ECMs on different Windows machines to communicate with the same site on the PRA Appliance. A list of the ECMs connected to the appliance site can be found at* ***/login > Status > Information > ECM Clients****.*

Note: *When multiple ECMs are connected to a BeyondTrust site, the PRA 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:
    a. First, ensure that the DLL is not blocked. Right-click on the DLL and select **Properties**.
    b. On the **General** tab, look at the bottom of the pane. If there is a **Security** section with an **Unblock** button, click the button.
    c. Repeat these steps for any other DLLs packaged with the plugin.
    d. In the Configurator, click the **Choose Plugin** button and browse to the location of the plugin DLL **ThycoticSecretServerPlugin.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.

4. After selecting the DLL, click the gear icon in the Configurator window to configure plugin settings.

5. The following settings are available:

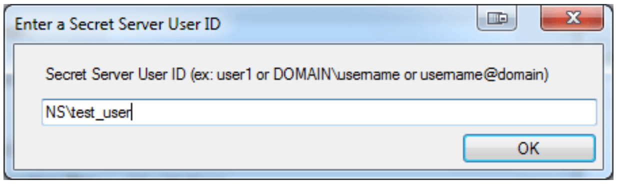
Setting Name	Description	Notes	Required
Endpoint URL	The full URL to the Secret Server web services	e.g., https://<thycotic-server-hostname>/SecretServer/webservices/SSWebservice.asmx	Yes
API User	Username of the API account created in Secret Server		Yes
API Password	Password of the above user		Yes
API 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
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

Setting Name	Description	Notes	Required
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

Test Settings

The settings specific to Secret Server can be tested directly from the plugin configuration screen using the **Test Settings** button.

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

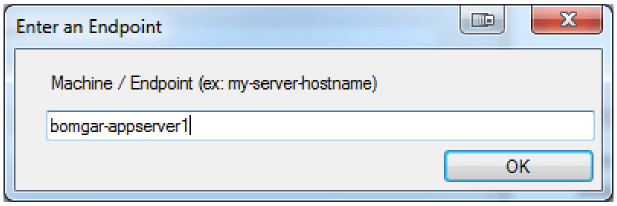


Enter a Secret Server User ID

Secret Server User ID (ex: user1 or DOMAIN\username or username@domain)

NS\test_user

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



Enter an Endpoint

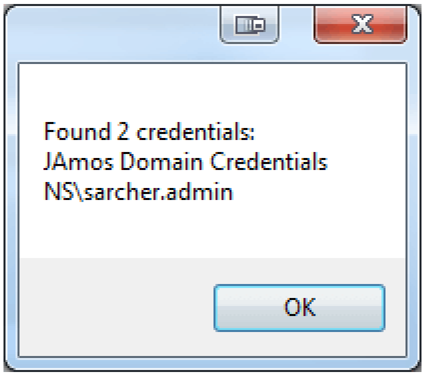
Machine / Endpoint (ex: my-server-hostname)

bomgar-appserver1

3. View the resulting list.

> ***Note:*** *No actual passwords are retrieved or displayed, only the list of credentials.*

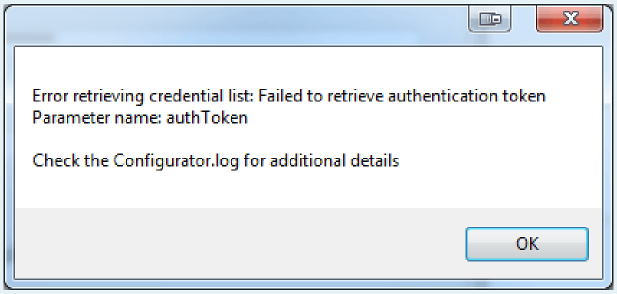
> ***Note:*** *The settings used for the test are the ones currently entered on the screen, not necessarily what is saved.*


Found 2 credentials:
JAmos Domain Credentials
NS\sarcher.admin

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. The user can either approve the request, granting API user access to their credentials for future sessions, or they can deny the request. 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.*


Error retrieving credential list: Failed to retrieve authentication token
Parameter name: authToken

Check the Configurator.log for additional details

The ***Configurator.log*** *should indicate that authentication was successful but that permission to access that user's secrets is pending approval.*

Clear Token Cache

To avoid excessive authentication calls to Thycotic, the plugin caches (in an encrypted form) authentication tokens for users as they attempt to retrieve secrets through the integration. Subsequent calls use the cached token until it expires. At that point, a new authentication token is retrieved and cached. The **Clear Token Cache** button allows an admin to clear all cached authentication tokens if such action becomes necessary for maintenance, testing, etc.