BeyondTrust

Privileged Remote Access Vault Whitepaper

TC:2/8/2019

Table of Contents

BeyondTrust Vault Whitepaper

Whether a vendor, database administrator, network engineer, or privileged insider, you can rely on BeyondTrust Vault to securely store credentials needed to access your critical business systems. BeyondTrust Vault fits seamlessly into your privileged session workflow because it is integrated directly with the Privileged Remote Access solution. Users do not need to learn to use another tool or even exit BeyondTrust to retrieve passwords. With just one click in the BeyondTrust access console, users can simply select the correct credential from the dropdown and log directly into the endpoint - without ever having to know or even see the actual password.

In this document, we will cover the following topics:

- **Vault Configuration:** Enable the user permissions needed to start using BeyondTrust Vault.
- **Credential Discovery:** Find and track privileged accounts commonly used by your privileged users.
- **Credential Rotation:** Rotate passwords, manually or automatically, after each use.
- **Check In and Check Out:** Retrieve credentials for use outside of a BeyondTrust session.
- **Credential Injection:** Inject credentials into a remote system directly from the BeyondTrust access console.
- **Reporting:** View and track credential activity.

Configure User Permissions for BeyondTrust Vault in the BeyondTrust PRA /login Interface

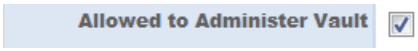
There are two permissions you can assign to users to help manage your BeyondTrust Vault instance.

- **Allowed to Administer Vault:** This permission grants the user full rights to discover, add, modify, and manage privileged accounts stored on the BeyondTrust Appliance.
- **Vault Reporting Permissions:** This permission indicates what level of rights a user has for viewing Vault reports.
  - **View All Events:** The user has permission to view all Vault reporting events for all users.
  - **View His/Her Events:** The user has permission to view only their own Vault reporting events and cannot view any other user account activity.
  - **Not Allowed:** The user does not have permission to view any Vault reporting events.

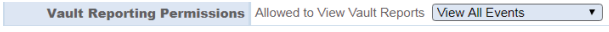
> ***Note:*** *By default, users are not given access to credentials. However, if a BeyondTrust administrator grants a user access to a credential, the user can begin using the credential in BeyondTrust access sessions and can check out the credential in* ***/login*** *(if enabled). Once the user uses the credential, they can view reports about their credential use.*

By default, when BeyondTrust Vault is enabled, users with admin rights in BeyondTrust Privileged Remote Access will automatically possess the **Allowed to Administer Vault** and **Vault Reporting Permissions - View All Events** permissions. For other users, these permissions need to be explicitly configured. Follow the steps below to set these permissions.

1. From the **/login** interface, go to **Users & Security > Users**.
2. Locate the user you wish to assign the permission. Click **Edit**.
3. Under the **Permission** section, check **Allowed to Administer Vault**.



4. Locate **Vault Reporting Permissions** and make a selection from the dropdown.



5. Click **Save Changes**.

> ***Note: Allowed to Administer Vault*** *and* ***Vault Reporting Permissions*** *can also be configured via group policy at* ***Users & Security > Group Policies****.*

For more information, please see Users: Add User Permissions for a User or Admin at https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/users.htm.

Discover Domains, Endpoints, and Accounts Using BeyondTrust Vault

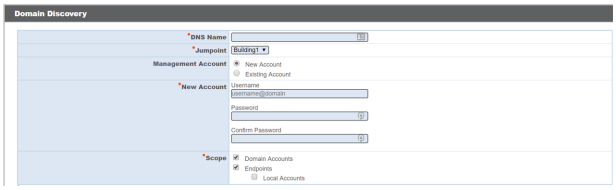
With the BeyondTrust Vault add-on, you can discover Active Directory accounts, local accounts, and endpoints. Jumpoints are used to scan endpoints and discover the accounts associated with those endpoints.

To learn more about Jumpoints, please see BeyondTrust Privileged Remote Access Jumpoint Guide at https://www.beyondtrust.com/docs/privileged-remote-access/how-to/jumpoint/index.htm.

The first step to implement BeyondTrust Vault in your environment is to use the built-in discovery tool to find accounts. To initiate a discovery job, follow the steps below.

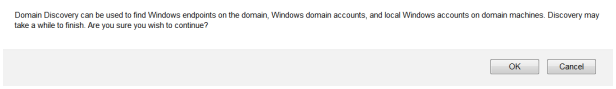
Initiate a Discovery Job

1. From the **/login** interface, go to **Vault > Discovery**.
2. Choose an existing Jumpoint located in the environment where you wish to discover accounts.



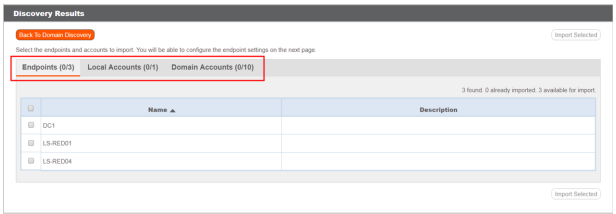
***Note:** The Jumpoint field is required for discovery. The Jumpoint should be the DNS name of a domain controller within the environment you wish to scan.*

3. Select the management account needed to start the discovery job. Choose to use a new account, which requires a **Username**, **Password**, and **Password Confirmation**. Or choose to use an existing account discovered from a previous job or added manually in the **Accounts** section. Then, select what account types you wish Vault to discover. Once the scope is defined, click **Discover**.
4. When the confirmation prompt appears asking if you wish to continue, click **OK**.



The discovery process can take some time. While discovery is underway, the **Discovery Progress** screen appears and tracks the number of accounts and endpoints discovered.

Once the discovery job is done, a **Discovery Results** page appears. You can switch between the **Endpoints**, **Local Accounts**, and **Domain Accounts** tabs to view the discovered items.



- **Endpoints:** Shows the names of the endpoints discovered, as well as a description, if available.
- **Local Accounts:** Shows the **Username**, **Endpoint** (association), **Description**, **Last Login Date**, and **Password Age** for all discovered local accounts.
- **Domain Accounts:** Shows the **Username**, **Distinguished Name**, **Description**, **Last Login Date**, and **Password Age** for all discovered domain accounts.

Import Discovered Endpoints and Accounts

You can import endpoints, local accounts, or domain accounts into Vault for continued management, use, and maintenance.

1. Choose any of the tabs: **Endpoints**, **Local Accounts**, or **Domain Accounts**.
2. Check the box located by the endpoint or account you wish to import.
3. Click **Import Selected**.
4. The **Import Discovered Items** sectionl appears, listing the number of endpoints and accounts selected for imported. Click **Start Import**.

Once the import is complete, the endpoint or account becomes available in the **Endpoints** and **Accounts** sections.

> ***Note:*** *For imported endpoints, RDP Jump Shortcuts are created with an automatic association to local accounts.*

> For more information, please see Discover Domains, Accounts, and Endpoints at https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/vault.htm.

Add Generic Credentials and SSH Keys

Outside of the discovery process, you can manually add individual credential accounts to BeyondTrust Vault. To add generic accounts, follow the steps below.

1. Go to **Vault > Accounts**.
2. Click **Add New Account**.
3. Complete the information on the **Generic Account :: Add** page. The required fields are:
   - **Name**
   - **Username**
   - **Authentication**
   - **Password**

> For more information about adding generic accounts, please see Generic Account :: Add at https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/vault.htm.

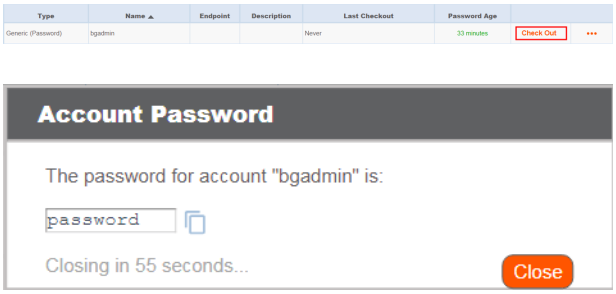
4. When finished, click **Add Account**.

At any point, you can edit the account's information by clicking **... > Edit**.

Check Out Credentials from the BeyondTrust PRA /login Interface

If you need to retrieve passwords for use outside of a BeyondTrust access session, you can manually check out a password from the **/login** interface.

1. Go to **Vault > Accounts**.
2. Locate the account you wish to check out.
3. Click **Check Out**.
4. The **Account Password** dialog appears, and you can see the password in plain text for one minute. During that time, you can copy the password by clicking the **Copy** icon.



Check In

When you are finished using a credential, return to the **Accounts** page and click **Check In** to check the password back into BeyondTrust Vault.

Note: *If you check in a domain credential with automatic rotation configured, the password automatically rotates.*

Note: *Non-administrative users can view and modify only credentials for which they have access.*

For more information, please see Discover Domains, Accounts, and Endpoints at https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/vault.htm.

Rotate Privileged Credentials Using BeyondTrust Vault for Privileged Remote Access

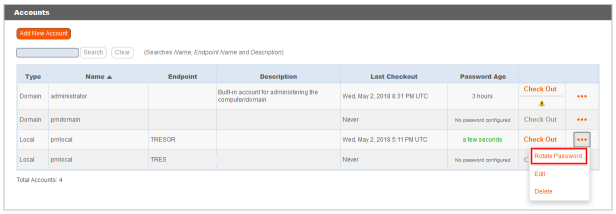
It is a security best practice to rotate or change privileged credentials frequently. With BeyondTrust Vault, you can choose to set imported domain credentials to automatically rotate after each use, or you can manually rotate credentials at any time. Two actions trigger the automatic rotation of domain credentials:

- Manually checking in a credential from the **/login** interface.
- Leaving a access session where credential injection has been used.

Local accounts cannot be automatically rotated and require manual rotation from **/login**.

Rotate Domain and Local Credentials Manually

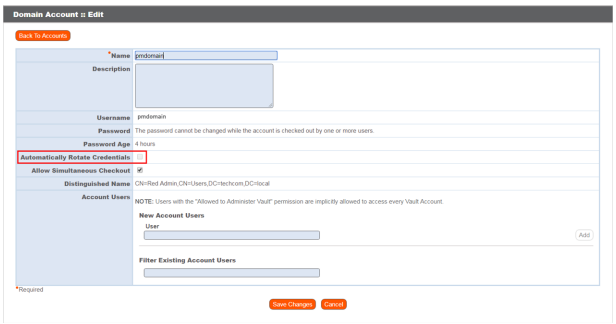
1. From the **/login** interface, go to **Vault > Accounts**.
2. Locate the account you wish to rotate.
3. Click **...**.
4. Click **Rotate Password**.



Once rotation is complete, the **Password Age** information updates with a timestamp of "*a few seconds*".

Configure Automatic Rotation of Domain Credentials

1. From the **/login** interface, go to **Vault > Accounts**.
2. Locate the domain account you wish to automatically rotate.
3. Click **...**.
4. Click **Edit**.
5. From the edit screen, check **Automatically Rotate Credentials**.
6. Click **Save Changes**.



After each use, the account will automatically rotate.

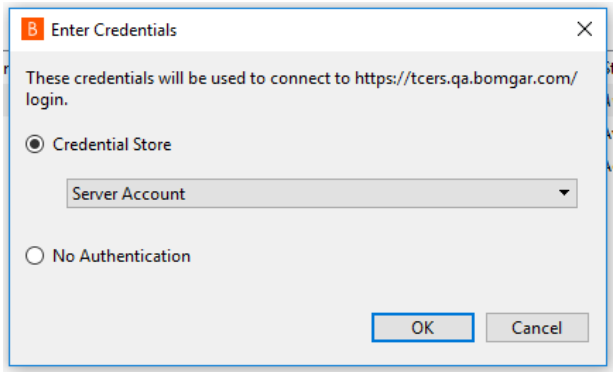
> ***Note:*** *The **Automatically Rotate Credentials** setting is not available for local accounts.*

For more information, please see Discover Domains, Accounts, and Endpoints at https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/vault.htm.

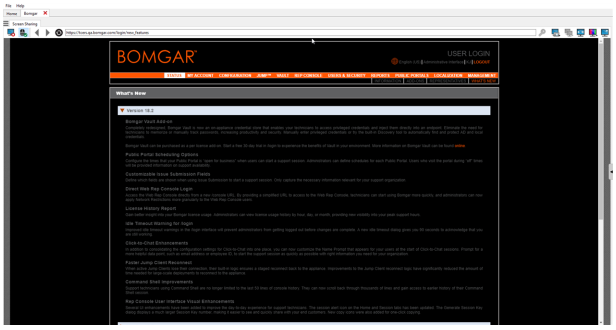
Use Credential Injection During Access Sessions

After BeyondTrust Vault has been configured and accounts imported, the access console can begin to use credentials stored in BeyondTrust Vault to log into remote systems. Credential injection is available to log into remote systems and any other events requiring privileged account information during an access session.

1. While in an access console session, you can inject credentials by clicking the key icon. A dropdown credential dialog appears, listing the credentials available for selection from BeyondTrust Vault.
2. Select the appropriate credentials.



The access console retrieves the selected credentials from BeyondTrust Vault and injects them into the session.



Choose from Favorite Credentials for Injection

After you have used a set of credentials to log into an endpoint, the system stores your preferred credentials for the endpoint and the context in which they were used (to log in, to perform a special action, to elevate, or to push) in the appliance database. The next time you use a credential to access the same endpoint, the credential injection menu makes a recommendation for which credentials to use. The credentials are displayed at the top of the credentials list, followed by any remaining credentials. If no credential history exists for an endpoint, the appliance simply displays all possible credentials.

The credential list recommends no more than five credentials.

View and Track BeyondTrust Vault Activity in BeyondTrust Privileged Remote Access

Reporting is available to track account and user activity. Specifically, report administrators and users can view and track information about the following:

- Check in and check out
- Password rotations and changes

To run reports, go to **Reports > Vault** in the **/login** interface. The following report parameters are available for selection:

- **Date Range:** View all events occurring within a specific date range.
- **Account:** View all events associated with a specific domain or local account.
- **User:** View all events involving a specific user.

Make your selections and click **Show Report**. The report will provide the following information:

- **Timestamp:** The date and time the event occurred.
- **Account:** The account name used with the event.
- **Event Type:** The type of event which occurred, such as a check in, check out, or password change.
- **User:** The user who triggered the event.

Note: *Events are logged in order to generate reports, and these logs are saved for 90 days.*

Note: *Non-administrative users may experience a more limited* ***/login*** *user experience, depending on the access granted to them by their administrator. For example, a Vault user with limited permissions may potentially see only the* ***Accounts****,* ***Vault****, and* ***Reports > Vault*** *tabs.*

Note: *If a user has been anonymized in an effort to follow compliance standards, the* ***Vault Account Activity*** *report may display pseudonyms for user data or may indicate that information has been deleted. To learn more about data anonymization and deletion for compliance efforts, please see Compliance: Anonymize Data to Meet Compliance Standards at https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/compliance.htm.*

For more information, please see Vault: Report on Vault Account and User Activity at https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/reports-vault.htm