Remote Support
Vault Whitepaper
# Table of Contents

BeyondTrust Vault Technical Whitepaper .......................................................... 3
Configure User Permissions for BeyondTrust Vault ............................................. 4
Discover Domains, Endpoints, and Accounts Using BeyondTrust Vault ............... 6
Rotate Privileged Credentials Using BeyondTrust Vault ................................ 10
Check Out Credentials from the /login Interface ........................................ 12
Use Credential Injection During Support Sessions ....................................... 13
View and Track BeyondTrust Vault Activity ................................................... 14
BeyondTrust Vault Technical Whitepaper

Service desk technicians are often required to use administrative credentials with elevated privileges to resolve support issues. Although compromised privileged account credentials are a common target for hackers, credential management best practices are often secondary to the need to resolve issues quickly. With the pressure to provide support as quickly and efficiently as possible, many service desk teams share and store credentials in plain text for convenience. BeyondTrust Vault for Remote Support mitigates that risk in your service desk by enabling secure credential management without sacrificing convenience and business productivity.

BeyondTrust Vault fits seamlessly with service desk workflow because it is integrated directly with the Remote Support solution. Technicians do not have to learn to use another tool or even exit BeyondTrust to retrieve passwords. With just one click in the BeyondTrust representative console, users can simply select the correct credential from the dropdown and log directly into a remote system - 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.
- **Credentials Discovery**: Find and track privileged accounts commonly used by your service desk.
- **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 representative console.
- **Reporting**: View and track credential activity, including the use of shared credentials.

For more information, please see BeyondTrust Vault for Remote Support at https://www.beyondtrust.com/remote-support/features/vault.
Configure User Permissions for BeyondTrust Vault

The Vault features and configuration options are available in the /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 Secure Remote Access 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 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, representatives are not given access to credentials. However, if an administrator grants a representative access to a credential, the representative can begin using the credential in BeyondTrust sessions and can check out the credential in /login (if enabled). Once the representative uses the credential, they are able to view reporting about their credential use.

By default, when BeyondTrust Vault is enabled, users with administrator privileges in BeyondTrust Remote Support 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 General Permissions 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 Representative or Admin at https://www.beyondtrust.com/docs/remote-support/getting-started/admin/user-accounts.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.


The first step to implementing BeyondTrust Vault into your environment is to use the built-in discovery tool to find these 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 within the environment you wish to discover accounts.

   ![Domain Discovery Form]

   - **DNS Name**: `example.beyondtrust.com`
   - **Jumpoint**: `Building1`
   - **Management Account**
     - New Account
     - Existing Account
   - **Username**: `example@beyondtrust.com`
   - **Password**: `********`
   - **Confirm Password**: `********`

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

3. Select the management account needed to initiate 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.

4. Click **Continue**.
5. Select what account types you wish Vault to discover: Domain Accounts or Endpoints.

6. Once the scope is defined, click Start Discovery.

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 complete, a Discovery Results page appears and lists all discovered endpoints, local accounts, and domain accounts.

From the results page, 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 BeyondTrust Vault for continued management, use, and maintenance.

1. Choose any of the tabs: Endpoints, Local Accounts, or Domain Accounts.
2. Check the box located beside the endpoint or account you wish to import.
3. Click Import Selected.
4. The Import Discovered Items section will appear, listing the number of endpoints and accounts selected to be 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/remote-support/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.
3. Complete the information on the Add Account page. The required fields are:
   - Name
   - Username
   - Authentication
   - Password

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

4. When finished, click Save.

At any point, you can edit the account's information by clicking ... > Edit.
Rotate Privileged Credentials Using BeyondTrust Vault

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 support 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 the ellipse and then select 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 the ellipse and then select Edit.
4. From the edit screen, check **Automatically Rotate Credentials**.

5. Click **Save**.

After each use, the account will automatically rotate.

For more information, please see Discover Domains, Accounts, and Endpoints at https://www.beyondtrust.com/docs/remote-support/getting-started/admin/vault.htm.
Check Out Credentials from the /login Interface

If you need to retrieve passwords for use outside of a BeyondTrust support 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 are able to see the password in plain text for one minute. In 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 are checking in a domain credential with automatic rotation configured, the password automatically rotates.

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

For more information, please see Discover Domains, Accounts, and Endpoints at https://www.beyondtrust.com/docs/remote-support/getting-started/admin/vault.htm.
Use Credential Injection During Support Sessions

After BeyondTrust Vault has been configured and accounts imported, the rep console can begin using credentials stored in BeyondTrust Vault to log into remote systems during support sessions. Credential injection is available for elevating sessions, logging into remote systems, and any other events requiring privileged account information during a support session.

1. While in a support session in the rep console, 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 rep console retrieves the selected credentials from BeyondTrust Vault and injects them into the session.

Choose from Favorite Credentials for Injection

After a representative has used a set of credentials to log into an endpoint, the system stores the user's preferred credentials for the endpoint and the context in which they were used (to login, to perform a special action, to elevate, or to push) in the appliance database. The next time the user wants to use credentials 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 the possible credentials.

No more than 5 credentials are recommended to the representative in the credentials list.
View and Track BeyondTrust Vault Activity

Reporting is available to track account and representative 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.
- **Representative**: View all events involving a specific representative.

Make your selections and then 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 or representative 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 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/remote-support/getting-started/admin/compliance.htm.