# Table of Contents

- BeyondTrust Remote Support Vault Technical Whitepaper ........................................... 3
- Configure User Permissions for BeyondTrust Remote Support Vault .......................... 4
- Discover and Import Domain Endpoints and Accounts Using BeyondTrust Vault ........ 6
- Add and Manage Vault Accounts ................................................................................. 9
- Add and Manage Vault Account Groups ...................................................................... 12
- View and Check Out Credentials from the /login Interface ........................................ 15
- Rotate Privileged Credentials Using BeyondTrust Vault ............................................. 17
- Use Credential Injection During Support Sessions ....................................................... 19
- View and Track BeyondTrust Vault Activity in Remote Support ................................ 20
- Create a Service Principal in an Azure Active Directory Domain Services Account ...... 22
- Use BeyondTrust Vault with Microsoft Azure Active Directory Domain Services Account .................................................................................................................. 26
BeyondTrust Remote Support 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 cover the following topics:

- **Vault Configuration**: Enable the user permissions needed to start using BeyondTrust Vault.
- **Credentials Discovery & Import**: Find and track privileged accounts commonly used by your privileged users and import them into the BeyondTrust Vault.
- **Adding Credentials Manually**: Manually add shared and personal generic accounts into the BeyondTrust Vault.
- **Credential Grouping**: Use account groups to logically group Vault accounts and grant users access to multiple accounts at one time.
- **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.
- **Using Vault with Azure AD Azure AD Domain Services accounts**: Create a Microsoft Azure AD service principal and use Vault to discover and manage Azure AD Domain Services accounts.

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

  **Note:** If a user has not been granted this permission, they cannot view or add shared generic vault accounts. However, they can add and manage their own personal generic vault accounts.

- **Allowed to View Vault Reports:** This permission indicates what level of rights a user has for viewing Vault reports.
  - **Not Allowed:** The user does not have permission to view any Vault reporting events.
  - **View Only His/Her Events:** The user has permission to view only their Vault reporting events and cannot view any other user account activity.
  - **View All Events:** The user has permission to view all Vault reporting events for all users.

  **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 the **Allowed to View Vault Reports - 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 Account.
3. Under the General Permissions > Administration section, check Allowed to Administer Vault.
4. Under General Permissions > Reporting, select the permission from the Allowed to View Vault Reports dropdown.
5. Click Save.

**Note:** Vault administration and report privileges 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 and Import Domain 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 Domain Discovery Job

1. From the /login interface, go to Vault > Discovery.
2. Click New Discovery Job.
3. Leave the default Windows Domain option selected, and then click Continue.
4. Enter a valid fully qualified DNS name for the domain you are performing the discovery action on.
5. Choose an existing Jumpoint located within the environment you wish to discover accounts.

   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. Discovery is currently supported on Windows Jumpoints only.

6. 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.

   Note: This account is used to connect and perform the discovery of accounts and endpoints in the specified domain. It should be a functional account that has permissions to change and reset passwords.

7. Click Save and Continue.
8. Select the account types you wish Vault to discover: **Domain Accounts**, **Endpoints**, and **Local Accounts**.

9. Enter a **Search Path**, or leave it blank to search all OUs and containers.

10. Click **Browse** if you want to refine your search by specifying which OUs to target.

11. Use the **LDAP Query** field if you want to narrow the scope of user accounts and endpoints searched.

12. 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 appears, listing the number of endpoints and accounts selected for import. If importing endpoints, select a **Jump Group** from the list or select the **Do not create Jump Item** option. If importing accounts, select an **Account Group** from the list.
5. 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](https://www.beyondtrust.com/docs/remote-support/getting-started/admin/vault.htm).
Add and Manage Vault Accounts

You can add and manage credential accounts manually from the Accounts page.

Add Generic Credentials and SSH Keys

Outside of the discovery process, you can manually add individual credential accounts to BeyondTrust Vault. You can add shared generic accounts and personal generic accounts. Shared generic accounts may be used by all users who have been assigned to the account with the Inject or the Inject and Check Out Vault account role. Personal generic accounts may be used only by the account owner (the user who created the account). To add generic accounts, follow the steps below.

Add a Shared Generic Account

1. From the /login interface, go to Vault > Accounts.
2. Click Add.
4. Complete the information on the Add Shared Account page. The required fields are:
   - Name
   - Username
   - Authentication
   - Password
5. Check Allow Simultaneous Checkout if you want to allow this credential to be checked out by multiple users at the same time.
6. Select an Account Group from the list to add this account to a group.

**Tip:** Adding a credential account to an account group allows all users who have been assigned to that group to use this credential. If an account group is not selected, you must add account users individually to this new credential and assign their role.

7. If you are not adding this new credential account to an account group, add users and their Vault role individually in the Account Users section.
8. Click Save at the top of the page to save the new shared credential account.

Add a Personal Generic Account

1. From the /login interface, go to Vault > Accounts.
2. Click Add.
4. Complete the information on the Add Personal Account page. The required fields are:
   - Name
   - Username
   - Authentication
   - Password
5. Click Save at the top of the page to save the new personal credential account.
Edit a Vault Account

1. From the /login interface, go to Vault > Accounts.
2. For shared accounts:
   - From the Shared tab, locate the account you wish to edit.
   - Click the Actions menu (ellipsis) for the account.
   - Select Edit.
3. For personal accounts:
   - From the Personal tab, locate the account you wish to edit.
   - Click Edit Account (pencil icon) for the account.
4. Modify options as necessary, and then click Save.

Delete a Vault Account

1. From the /login interface, go to Vault > Accounts.
2. For shared accounts:
   - From the Shared tab, locate the account you wish to delete.
   - Click the Actions menu (ellipsis) for the account.
   - Select Delete.
3. For personal accounts:
   - From the Personal tab, locate the account you wish to delete.
   - Click Delete Account (trash can) for the account.
4. Click Yes to confirm.

View the Status of a Vault Account

On the Vault > Accounts page, a Status column displays when at least one the accounts has a warning, error, or checked out status to indicate. Accounts managed by Azure Active Directory Domain Services accounts are identified in the status column, along with an alert if there is no service principal for the account. Multiple statuses for an account are stacked and displayed in different colors. You can mouse-over a specific status to view more details about it.
Note: The Status column is auto-hidden when none of the accounts have a status set.

For information about working with Azure Active Directory Domain Services accounts, please see "Use BeyondTrust Vault with Microsoft Azure Active Directory Domain Services Account" on page 26.
Add and Manage Vault Account Groups

Vault admins can use account groups to logically group credentials together, providing a quick and easy way to grant users access to multiple shared Vault accounts at one time. Account groups can also be associated to a group policy, granting policy members access to that group of shared Vault accounts.

**Note:** A shared Vault account can belong to only one group at a time and personal Vault accounts cannot be added to an account group.

**Add an Account Group**

1. From the /login interface, go to Vault > Account Groups.
2. Click Add.
3. Provide a Name and Description for the group.
4. Under Accounts, select the accounts you wish to add to the group from the Accounts Not in a Group list.
5. Click Add to move the accounts over to the Accounts in This Group list.

**Tip:** The None group is a system generated group that contains all user accounts that do not belong to an account group. The None group is selected by default. You can filter the list of available accounts to add to the group by selecting a group from the Source Account Group list or by using the Search Selected Account Group box to search by Name, Endpoint, and Description.

6. In the Allowed Users section, add a user and select their Vault role from the New Member Role dropdown, and then click Add.
7. Click Save at the top of the page.

**Add a Vault Account to an Account Group from the Accounts Page**

1. From the /login interface, go to Vault > Accounts.
2. From the Shared tab, select the account, click the ellipsis to access the Actions menu, and then select Edit.
3. Select the group from the **Account Group** list, and then click **Save** at the top of the page.

### Import a Discovered Account to an Account Group

1. From the `/login` interface, go to **Vault > Discovery**.
2. Scroll down to the **Discovery Jobs** section.
3. Click **View Results** for the job.
4. Select the **Local Accounts** or **Domain Accounts** tab as applicable.
5. Select the account you wish to import.
6. Click **Import Selected**.
7. Select the group from the **Account Group** list.
8. Click **Start Import**.

### Add an Account Group to a Group Policy

1. From the `/login` interface, go to **Users & Security > Group Policies**.
2. Click **Edit** for the desired group policy.
3. Scroll down to the Memberships section.
4. Check the Add Vault Account Group Memberships setting.
5. Select the Account Group from the list.
6. Select the Vault Account Role from the list.
7. Click Add.
8. Click Save at the top of the page.

9. The group policy and its Vault account role are now displayed under the Group Policies section for the account group that was added to the policy.

10. The members of the group policy are now added under Allowed Users for the account group.

**Note:** If a user was granted access individually from the account group edit page and also through a group policy, the group policy access is overridden by the explicitly granted individual access for this user.
View and 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 for a shared account, or view and copy a password for a personal account, from the /login interface.

Check Out and Check In a Shared Account

1. Go to Vault > Accounts.
2. From the Shared tab, locate the account you wish to use, and then click Check Out.
3. 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.

Tip: When an account is checked out, the Status column is visible, and Checked Out appears in the Status column. You can the mouse hover over the Checked Out status to view who has it checked out.

4. 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.
View and Copy a Personal Account Password

1. Go to Vault > Accounts.
2. From the Personal tab, locate the account you wish to use, and then click View Password.

3. 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.

Note: Only the owner of a personal account is able to view its password. A Credential Used event is logged when the owner views the password. Vault administrators can view this activity in a Vault report.

For more information, please see Discover Domains, Accounts, and Endpoints at https://www.beyondtrust.com/docs/remote-support/getting-started/admin/vault.htm.
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. Three 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.
- Scheduled password rotation is enabled and the password has reached its maximum age.

Rotate Domain and Local Credentials Manually

1. From the /login interface, go to Vault > Accounts.
2. Click the Actions menu (ellipsis) for the account you wish to rotate.
3. Select Rotate Password.

Once rotation is complete, the Password Age information updates with a time stamp of a few seconds.

Configure Automatic Rotation of Vault Credentials

1. From the /login interface, go to Vault > Accounts.
2. Click the Actions menu (ellipsis) for the account password you wish to configure.
3. Select Edit.
4. Check **Automatically Rotate Credentials after Check In.**
5. Click **Save.**

After each use, the account automatically rotates.

---

**Schedule Password Rotation for Vault Accounts**

You can configure passwords to automatically rotate for all Vault accounts when the password reaches a specified maximum age as follows:

1. From the `/login` interface, go to **Vault > Options.**
2. Check **Enable Scheduled Password Rotation.**
3. Set the **Maximum Password Age** value in days.
4. Click **Save.**

*Note: Accounts that are checked out are rotated after they are checked in, based on their configuration.*
Use Credential Injection During Support Sessions

After BeyondTrust Vault has been configured and accounts imported or manually added, the rep console can begin using credentials stored in BeyondTrust Vault to log in to 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.

**Note:** Credential injection is not available for Mac or Linux Jump Clients.

1. While in a support session in the rep console, you can inject credentials by clicking the key icon. A dialog appears where you can click on the dropdown icon to select a credential from the list, or type in part of the account name to filter credentials to select from. If multiple accounts have the same name, you can select credential by account (user name).

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 in to 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 B Series 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 B Series Appliance simply displays all the possible credentials.

The credential list recommends no more than five credentials.
View and Track BeyondTrust Vault Activity in Remote Support

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

- Account creations and deletions
- Credential check ins and check outs
- Personal credential used
- Password rotations and changes

To run Vault reports:

1. From the /login interface, go to Reports > Vault. The following report parameters are available for selection:
   - **Date Range**: View all events within a specific date range.
   - **Account**: View all events associated with a specific domain or local account.
   - **Performed By**: View all events involving a specific user, API account, or the system.

2. Make your selections, and then click Show Report, or click Download Report if you want to download it to a CSV, XML, or XLSX file. The report provides 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 credentials checked in or checked out, or password rotated.
   - **Performed By**: The user who triggered the event.
   - **Data**: Relevant system information message, for example if a password rotation failed, the error message is indicated.

**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.
Create a Service Principal in an Azure Active Directory Domain Services Account

The BeyondTrust Vault can manage Azure AD Domain Services accounts. This requires a service principal. The service principal is required to discover and rotate Azure ADDS accounts.

Create a Registered App

Sign into Azure and connect to Azure AD tenant where you wish to manage passwords. Then follow these steps:

1. On the left menu, select App registrations.
2. Click + New Registration.
3. Under Name, enter a unique application name.
4. Under Supported account types, select Accounts in this organizational directory only.
5. Click Register.

6. Select the new registered app from the list of Apps Registrations (if not already visible).
7. Select Certificates & secrets from the left menu.
8. Click + New Client Secret.
9. Provide a Description and appropriate Expiry. If you select 1 or 2 years, the service principal must be refreshed in PRA/RS with a new client secret on the anniversary of its creation.
10. Click Add.

11. Create a copy of the client secret and store it in a safe place. This is the only time it is displayed. This is needed to add the account to the Vault.

Assign API Permissions to the Registered App

Browse to the application using App registrations in Azure Active Directory, and follow these steps:

1. Select API Permissions from the left menu.
2. Click + Add a permission.
3. Click Microsoft Graph.
4. Click Application Permissions.
5. Search for User.ReadWrite.All and check it in the search results.
6. Search for `Directory.Read.All` and check it in the search results.
7. Click `Delegated Permissions`.
8. Search for `Directory.AccessAsUser.All` and check it in the search results.

9. Click `Add permissions`.
10. Remove the `User.Read` permission that is granted by default by clicking the ellipses menu and selecting `Remove permission`.

11. Click `Grant Admin Consent for <directory name>` to give consent to the app to have those permissions.

Assign Roles to the Registered App

Search Azure for `Azure AD roles and administrators`, and follow these steps:
1. Search for the role **Privileged authentication administrator** or **User Administrator**.  
   - **Privileged authentication administrator** gives the application sufficient permissions to change most user and administrator passwords, including Global Admin.  
   - **User Administrator** gives the application sufficient permissions to change most passwords, with the exception of Authentication Admin, Global Admin, Privileged Authentication Admin, and Privileged Role Admin.

2. Click the **Role** or the ellipsis button for role and then click **Description**.

3. On the left menu, click **Assignments** (if not already selected).

4. Click **+ Add assignments**.

5. In the **Search** box, type the name of the registered app that was created earlier. Registered apps are not listed with users and can only be found this way.

6. The previously created registered app is visible in the search results. Select it and click **Add**.

---

**Note:** Using BeyondTrust Vault with Microsoft Azure Active Directory Domain Services Account requires both an Azure AD license and an Azure AD Domain Services license.

---

Use BeyondTrust Vault with Microsoft Azure Active Directory Domain Services Account

Administrators can use Vault to discover and manage Azure AD Domain Services accounts. Managing Azure AD Domain Services accounts requires a service principal, which is defined under the relevant domain in the Vault section of the /login interface.

Note: A service principal must be created in Azure before you can add it to the BeyondTrust Vault. Information such as the Client Secret is obtained from Azure when you create the service principal. For more information on creating a service principal in Azure, please see "Create a Service Principal in an Azure Active Directory Domain Services Account" on page 22.

Note: Vault cannot be used with Azure domain controllers other than Azure Active Directory Domain Services.

Discovery job results identify Azure AD Managed accounts in the Status column, as well as whether or not the service principal has been added. When the Status displays No Service Principal, the account cannot be selected for import.

Add or Edit a Service Principal

Adding or editing a service principal can be done before a Discovery job, or after a Discovery job has identified accounts that require a service principal.

1. From the /login interface, go to Vault > Domains.
2. Scroll down to **Microsoft Azure AD Service Principals** and click +Add.
   - Service principals already added can be edited by clicking the pencil icon at the right end of the row.
   - To delete a service principal, click the trash can icon at the right end of the row. The deletion request must be confirmed. Deleting a service principal deletes all associated accounts.

3. Enter the mandatory information:
   - Domain name
   - Tenant ID
   - Client ID
   - Client Secret

4. If desired, enter a name to easily identify the service principal.

5. The service principal can be disabled. This does not remove it, but no actions, such as rotation, can be taken with the account. In the list of Discovery results, the account **Status** is Service Principal Unavailable and Disabled.

6. Click Save. Service principal details are validated against the details in your Azure tenant.
   - If adding the service principal is successful, the new service principal displays in the list of domains, with the status OK.
   - If adding the service principal fails, the Status is Disabled and Failed. Click the pencil icon to return to the edit screen, and review the detailed error message.

7. Run Discovery again. In the list of results, the account **Status** is still Azure AD Managed, but the No Service Principal note does not display. The account can now be selected for import.

**Note:** If the account is a shadow account, the **Status** displays "Externally Sourced," and the account is not available for import.
8. If you have multiple domains for the Azure AD Domain Services instance, repeat the process of adding a service principal for each domain.

On the edit screen for an imported Azure AD account, Azure Active Directory Managed displays at the bottom of the screen. Rotation, credential injection, and other actions are managed as for other accounts.

**Note:** Using BeyondTrust Vault with Microsoft Azure Active Directory Domain Services Account requires both an Azure AD license and an Azure AD Domain Services license.

For more information, please see the following:

- "Discover and Import Domain Endpoints and Accounts Using BeyondTrust Vault" on page 6
- "Rotate Privileged Credentials Using BeyondTrust Vault" on page 17
- "Use Credential Injection During Support Sessions" on page 19