



BeyondTrust

Remote Support Vault Guide

Table of Contents

BeyondTrust Remote Support Vault Guide	4
Configure User Permissions for Remote Support Vault	5
Configure User Permissions to Rotate Protected Credentials	6
Discover and Import Accounts, Services, and Endpoints Using BeyondTrust Vault	7
Initiate a Discovery Job for a New Domain	7
Import Discovered Endpoints Accounts and Services	8
Initiate a Discovery Job for an Existing Domain	10
Schedule Discovery Jobs	11
Add and Manage Vault Accounts	13
Add Generic Credentials and SSH Keys	13
Add a Shared Generic Account	13
Add a Personal Generic Account	15
Edit or Delete a Vault Account	15
View the Status of a Vault Account	16
Add and Manage Vault Account Groups	18
Add an Account Group	18
Add a Vault Account to an Account Group from the Accounts Page	20
Import a Discovered Account to an Account Group	20
Add an Account Group to a Group Policy	21
Add and Manage Vault Account Policies	23
Add an Account Policy	23
View and Check Out Credentials from the /login Interface	25
Check Out and Check In a Shared Account	25
Check Out a Service Account	25
View and Copy a Personal Account Password	26
Rotate Privileged Credentials Using BeyondTrust Vault	27
Rotate Domain and Local Credentials Manually	27
Configure Automatic and Scheduled Rotation of Vault Credentials	27
Use Credential Injection During Support Sessions	28
View and Track BeyondTrust Vault Activity in Remote Support	29
Run Vault Reports	29

Create a Service Principal in an Azure Active Directory Domain Services Account	31
Create a Registered App	31
Assign API Permissions to the Registered App	32
Assign Roles to the Registered App	33
Use BeyondTrust Vault with Microsoft Azure Active Directory Domain Services Account	35
Add or Edit a Service Principal	35
Use SSH Certificate Authority in Vault	38
Traditional SSH Keys	38
SSH Certificate Authority	38
Use SSH Certificate Authority Accounts	38

BeyondTrust Remote Support Vault Guide

BeyondTrust Vault for Remote Support mitigates the risk of shared privileged account credentials by enabling secure credential management, including credential discovery, masking, injection, and rotation.

BeyondTrust Vault fits seamlessly into your service desk workflow by integrating directly with the Remote Support solution, allowing administrator accounts to access systems without exiting BeyondTrust. With just one click in the Remote Support representative console, users can select the correct credential and log directly in to a remote system, keeping your privileged accounts more secure.

This document covers the following topics:

- **Vault Configuration:** Enable the user permissions needed to start using BeyondTrust Vault.
- **Discovery & Import:** Find privileged accounts commonly used by your privileged users, along with their associated endpoints, as well as Windows service accounts, and import them into the BeyondTrust Vault.
- **Add Credentials Manually:** Manually add shared and personal generic accounts into the BeyondTrust Vault.
- **Use SSH keys with a Certificate Authority:** Vault can provide unique private keys for each usage request, ensuring the user never receives the private key that is trusted by the endpoint. Each key can be time-limited and valid only until its expiry time. After that, it becomes useless. Short-lived keys reduce the risk of attacks, as the keys hold less value to an attacker.
- **Credential Grouping:** Use account groups to logically group Vault accounts and grant users access to multiple accounts at one time.
- **Vault Account Policies:** Use account policies to define account settings related to password rotation and credential checkout and apply those settings to multiple accounts at once.
- **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.
- **Use Vault with 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](https://www.beyondtrust.com/remote-support/features/vault) at <https://www.beyondtrust.com/remote-support/features/vault>.

Configure User Permissions for Remote Support Vault

BeyondTrust Vault provides two different permissions you can assign to Remote Support users. Assigning permissions grants users access to capabilities like modifying accounts or viewing Vault reports.

- **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.
 - 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. 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.

When BeyondTrust Vault is enabled, users with administrator privileges in BeyondTrust Remote Support 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.

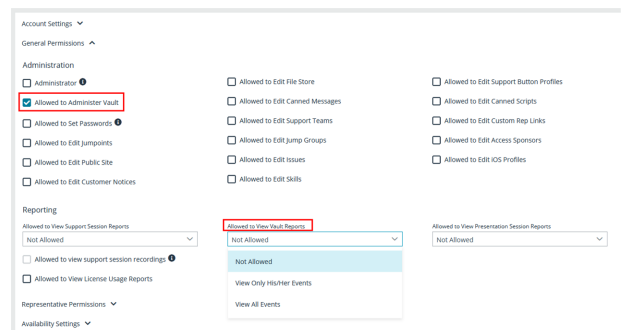
If a user wishes to rotate passwords on protected users such as domain admins, enterprise admins, etc., additional permission configuration is required.



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.

Follow the steps below to set Vault permissions for a user:

1. From the `/login` interface, navigate to **Users & Security > Users**.
2. Locate the user you wish to assign the permission to. Click **Edit Account** (pencil icon).
3. Click **General Permissions** to expand that section.
4. Under **Administration**, check **Allowed to Administer Vault**.
5. Under **Reporting**, select a permission from the **Allowed to View Vault Reports** dropdown.
6. Click **Save**.




Note: Vault administration and report privileges can also be configured via group policy at **Users & Security > Group Policies**.

Configure User Permissions to Rotate Protected Credentials

Follow the process below to configure additional permissions for rotating passwords on protected users such as domain admins, and enterprise admins.

First, go to the Command Prompt as an admin on the domain controller.

Run the following commands, where *dc=cps*, *dc=com* is the information for your domain:

```
dsacl "dc=cps,dc=com" /G "<yourDomainName>\<yourAccountName>:CA;Reset Password;user" /I:S
dsacl "CN=AdminSDHolder, CN=System, DC=cps, DC=com" /G
"<yourDomainName>\<yourAccountName>:CA;Reset Password"
```

Next, manually run the sdprop process, following these steps:

1. Run `ldp.exe` as admin.
2. Select **Connection > Connect...** from the Ldp window.
3. In the Connect window, make sure 389 is listed in the Port field.
4. Click **OK**.
5. Select **Connection > Bind...** from the Ldp window.
6. Select **Bind as currently logged on user**.
7. Click **OK**.
8. Select **Browse > Modify** from the Ldp window.
9. Configure the following fields in the Modify window:
 - **DN field:** empty
 - **Attribute field:** type `RunProtectAdminGroupsTask`
 - **Values field:** 1
 - **Operation:** click Add and then click Enter.
10. Click **Run**.



For more information, please see [Users: Add User Permissions for a Representative or Admin](https://www.beyondtrust.com/docs/remote-support/getting-started/admin/users.htm) at <https://www.beyondtrust.com/docs/remote-support/getting-started/admin/users.htm>.

Discover and Import Accounts, Services, and Endpoints Using BeyondTrust Vault

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

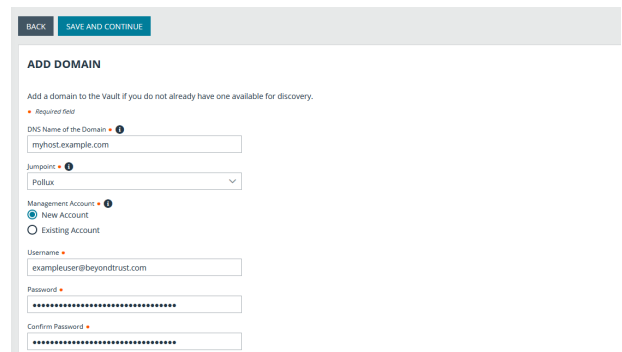
BeyondTrust Vault provides a built-in discovery tool to automatically find these accounts, endpoints, and services. Once discovered, results can be imported into your Vault for use.



For more information on Jumpoints, please see [BeyondTrust Remote Support Jumpoint Guide](https://www.beyondtrust.com/docs/remote-support/how-to/jumpoint/index.htm) at <https://www.beyondtrust.com/docs/remote-support/how-to/jumpoint/index.htm>.

Initiate a Discovery Job for a New Domain

1. From the `/login` interface, navigate to **Vault > Discovery**.
2. Click **New Discovery Job**.
3. Leave the default **Windows Domain** option selected, and then click **Continue**.
4. If a domain doesn't exist in Vault, you are presented with the **Add Domain** form to add one. If a domain does exist in Vault, you are presented with the option to select a new or existing domain to discover. Select the **New Domain** option.
5. Enter a valid fully qualified DNS address for the domain you are performing the discovery action on.
6. Choose an existing Jumpoint located within the environment you wish to discover accounts.




Note: The **Jumpoint** field is required for discovery. Enter the DNS name of domain controller within the environment you wish to scan. Discovery is currently supported on Windows Jumpoints only.

7. Select the **Management Account** needed to initiate the discovery job. Using a new account requires a **Username**, **Password**, and **Password Confirmation**. You may also use an existing account.




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

8. Click **Save and Continue**.

Define the Discovery Scope

9. Select the types of objects you wish Vault to discover:

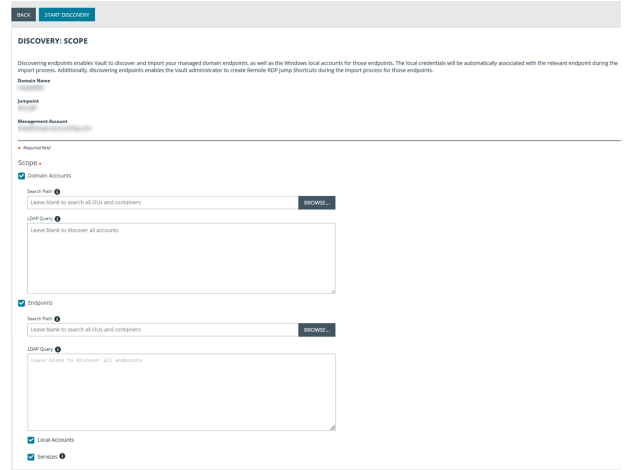
- Domain Accounts
- Endpoints
- Local Accounts
- Services



Note: Discovery of **Services** is available only if **Domain Accounts**, **Endpoints**, and **Local Accounts** are selected, only Windows service accounts are discovered.

10. Enter a **Search Path**, or leave it blank to search all OUs and containers.
11. Click **Browse** to refine your search by specifying which OUs to target.
12. Use the **LDAP Query** field to narrow the scope of user accounts and endpoints searched.
13. 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.



DISCOVERY PROGRESS CANCEL DISCOVERY

You may leave this page and log out at any time without interrupting the ongoing operation.

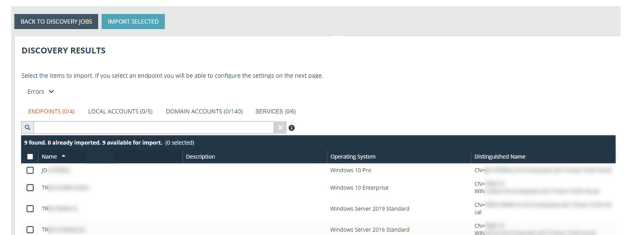
Endpoints: 5 found. 2 already imported. 3 available for import.

- Discovering domain accounts... 864 found. 3 already imported. 859 disabled. 2 import candidates.
- Waiting for local account discovery to start...
- Waiting for sources of authority discovery to start...

Import Discovered Endpoints Accounts and Services

Once the discovery job is complete, a **Discovery Results** page appears. You can switch between the **Endpoints**, **Local Accounts**, **Domain Accounts**, and **Services** tabs to view the discovered items and import them. Importing items saves them for later use in your Vault.

- **Endpoints:** Shows the **Name** and **Description** of the endpoints discovered, as well as their **Operating System** and **Distinguished Name**.
- **Local Accounts:** Shows the **Username**, **Endpoint** (system associated with account), **Description**, **Last Login Date**, **Password Age**, and **Status** for all discovered local accounts.
- **Domain Accounts:** Shows the **Username**, **Distinguished Name**, **Description**, **Last Login Date**, and **Password Age**, and **Status** for all discovered domain accounts.
- **Services:** Shows the **Display Name (Description)** (name displayed in Services snap-in), **Short Name** (name used by Service Controller command line tool), **Endpoint** (system where service is used), and **Username** (account used to run the service) for all discovered service accounts.

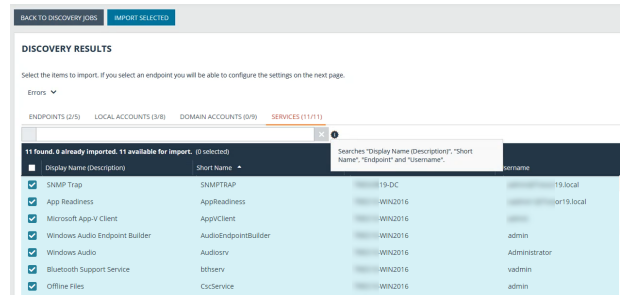


Name	Description	Operating System	Distinguished Name
JD		Windows 10 Pro	CN=...
TE		Windows 10 Enterprise	CN=...
TE		Windows Server 2019 Standard	CN=...
TE		Windows Server 2019 Standard	CN=...

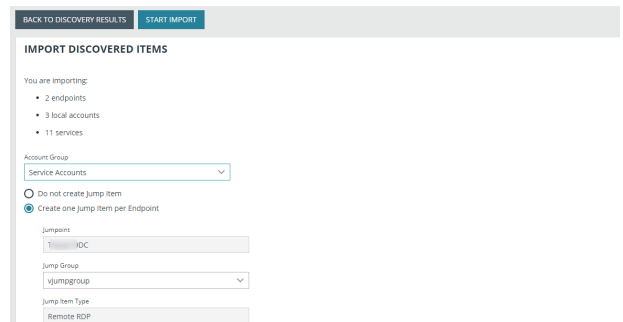
Note: Only services that use an account other than a built-in account to run are returned in the discovery results.

1. Choose any of the tabs: **Endpoints**, **Local Accounts**, **Domain Accounts**, or **Services**.
2. Select the items you wish to import, and then click **Import Selected**.

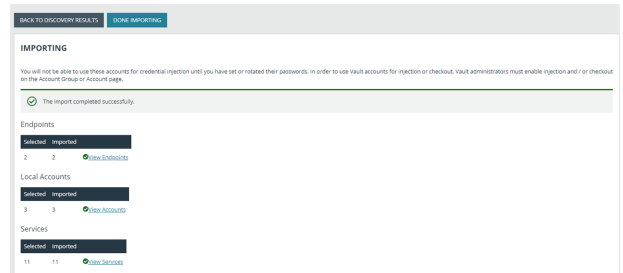
Tip: You can filter the list of items based on their attributes using the filter box above the grid. For each tab, click the *i* next to the filter box to see which attributes can be searched.



3. The **Import Discovered Items** page appears, listing the number of endpoints, accounts, and services 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.
4. Click **Start Import**.

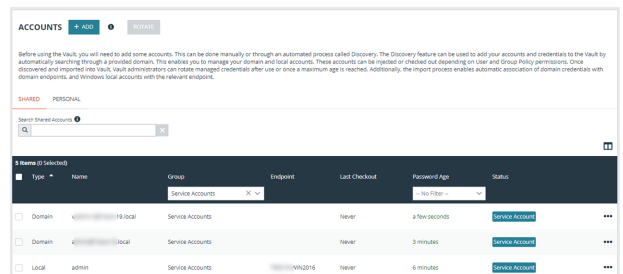


5. A status page appears, indicating the import completed successfully, and lists the number of endpoints, accounts, and services imported. You can click the links to view the specific items that were imported. Click **Done Importing** to close the status page.



Upon successful import, the accounts, endpoints, and services are listed in the grids on the **Accounts**, **Endpoints**, and **Services** pages in **/login > Vault**.

On the **Accounts** page, the endpoints associated with the shared accounts are indicated for each account, and if the account is used to run a Windows service, this is indicated in the **Status** column.



On the **Endpoints** page, the number of accounts, Jump Items, and services associated with each endpoint is indicated. You can view the specific associated accounts, Jump Items, and services by clicking the links.

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

Tip: Click the **Select visible columns** button above the grid to customize the columns displayed in the grid.

Non-domain linked endpoints can be associated with RDP items for improved security and user experience. To create the association, click **Jump Items** on the **Endpoints** screen. Then click **Add** and select **Add Remote RDP Jump Shortcut** or **Associate Existing RDP Jump Shortcuts**.

If associating an existing shortcut, click the shortcut(s) to add, and then click **Associate Selected**.

On the **Services** page, the endpoints and accounts associated with each service are indicated, as well as the last status of the service. Also, from the **Services** page, you have the option to restart the service upon rotation of the service account by checking the **Restart** box for the service.

Name	Hostname	Description	Operating System	Domain	Accounts	Jump Items	Services	Disassociated Name
Endpoint 1	Windows 10 Pro	...	0 Accounts	1 Jump Item	0 Services	...
Endpoint 2	Windows 10 Pro	...	0 Accounts	1 Jump Item	0 Services	...
Endpoint 3	Windows 10 Pro	...	2 Accounts	1 Jump Item	0 Services	...

Short Name	Display Name	Description	Endpoint	Username	Last Status	Restart
ADSync	Microsoft Azure AD Sync	<input checked="" type="checkbox"/>
AudioEndpointBuilder	Windows Audio Endpoint Builder	<input checked="" type="checkbox"/>
AudioSvc	Windows Audio	<input checked="" type="checkbox"/>
AudioSvc	Windows Audio	<input type="checkbox"/>
AudioSvc	Windows Audio	<input checked="" type="checkbox"/>
Bluetooth	Bluetooth Support Service	<input checked="" type="checkbox"/>
Bluetooth	Bluetooth Support Service	<input checked="" type="checkbox"/>
SmartMail	SMTP Trap	<input type="checkbox"/>

REMOTE RDP JUMP SHORTCUT ASSOCIATION

1 item(s) Selected

Hostnames: ...

25

Showing items 1 - 1 of 1

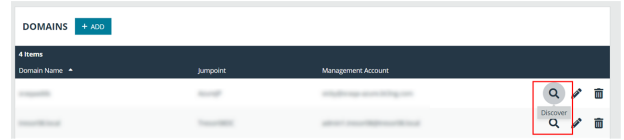
Short Name	Display Name	Description	Endpoint	Username	Last Status	Restart
ADSync	Microsoft Azure AD Sync	<input checked="" type="checkbox"/>
AudioEndpointBuilder	Windows Audio Endpoint Builder	<input checked="" type="checkbox"/>
AudioSvc	Windows Audio	<input checked="" type="checkbox"/>
AudioSvc	Windows Audio	<input type="checkbox"/>
AudioSvc	Windows Audio	<input checked="" type="checkbox"/>
Bluetooth	Bluetooth Support Service	<input checked="" type="checkbox"/>
Bluetooth	Bluetooth Support Service	<input checked="" type="checkbox"/>
SmartMail	SMTP Trap	<input type="checkbox"/>

Initiate a Discovery Job for an Existing Domain

Discovery jobs can be initiated on domains that have already been added or imported to BeyondTrust Vault. From **/login**, you can initiate a discovery job from the **Vault > Domains** page and from the **Vault > Discovery** page. Both methods are documented below.

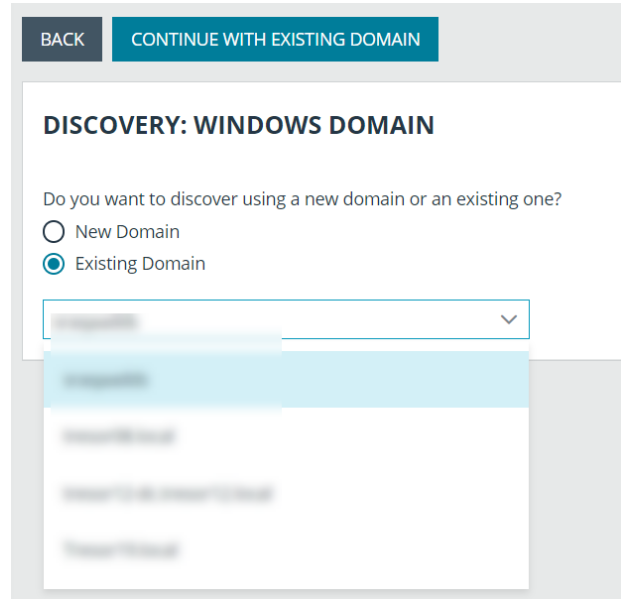
From Vault > Domains Page

1. Click the **Discover** button for the domain.
2. Define the scope of the discovery, and then click **Start Discovery**.
3. Select the items to import from the discovery results and start the import.



From Vault > Discovery Page

1. Click **New Discovery Job**.
2. Leave the default **Windows Domain** option selected, and then click **Continue**.
3. Select **Existing Domain**.
4. Select the domain from the dropdown list.
5. Click **Continue with Existing Domain**.
6. Define the scope of the discovery, and then click **Start Discovery**.
7. Select the items to import from the discovery results and start the import.



Discovery and Rotation of Vault Accounts - Port Requirements

Active Directory:

- Port 389
- Port 636

Local Account Management:

- Port 445

Schedule Discovery Jobs

Discovery jobs can be scheduled to run on defined days and times, avoiding the need for manually initiating new jobs on regularly updated workspaces.

Schedule Discovery Job for a New Domain

1. From the **/login** interface, navigate to **Vault > Domains**.
2. Click **Add**.
3. Follow the same steps as detailed above for initiating a discovery job for a new domain, but also set the **Scheduled Domain Discovery** settings.
4. Click **Save**. The discovery job runs on the days and time you specify.
5. To import items discovered from scheduled jobs:
 - Navigate to **Vault > Discovery**.
 - Locate the completed scheduled job. (Scheduled jobs are indicated as being performed by System.)

- Click **View Results** for the completed job.
- Import selected items.

Schedule a Discovery Job for an Existing Domain

1. From the **/login** interface, navigate to **Vault > Domains**.
2. Click the **Edit** button (pencil icon) for a listed domain.
3. Scroll down to the **Scheduled Domain Discovery** section and check **Enable Schedule Delivery**.
4. Select the days and time for the schedule.
5. Define the **Discovery Scope**, and then click **Save**.



The process for defining the discovery scope, viewing the results, and importing the discovered items is the same for all methods of discovery described in the above sections.

For more information, please see the following:

- ["Define the Discovery Scope" on page 8](#)
- ["Import Discovered Endpoints Accounts and Services" on page 8](#)
- [Discover Domains, Accounts, Endpoints, and Services at https://www.beyondtrust.com/docs/remote-support/getting-started/admin/discovery.htm](https://www.beyondtrust.com/docs/remote-support/getting-started/admin/discovery.htm)

Add and Manage Vault Accounts

Credential accounts can be added and managed in the **Accounts** page. Adding accounts enables users with the correct roles to access the account credentials for injections and rotations.



Note: Vault can import, rotate, and manage up to 60,000 accounts.

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**.
3. Select **Shared Generic Account**.
4. Provide a **Name**, **Description**, and **Username** for the account.
5. Select the type of authentication the account uses:
 - **Password**
 - Enter and confirm the password.
 - Select a specific policy for the account or leave **Account Policy** set to the default value of **Inherit Policy Settings**, in which case the account inherits the policy settings of the account group. If no account group is selected for the account, the account inherits the policy settings set for the global default account policy on the **Vault > Options** page.
 - **SSH Private Key**
 - If using an SSH private key, provide the key and passphrase.
 - **SSH Private Key with Certificate**
 - If using an SSH private key with certificate, provide the key, passphrase, and certificate.
 - A public key is generated after the account is saved, and can be viewed and copied by editing the account.
 - **SSH Certificate Authority**
 - Select if the private key is generated by BeyondTrust Remote Support or you will upload your own key.
 - If uploading your own key, provide the key and passphrase. The private key cannot be modified or retrieved.



Note: After creating and saving the account, select the **Edit** action and copy the public key. It starts with **cert-authority**. Add this public key to the endpoint's SSH configuration as a trusted CA or in an account's `known_hosts` file, so that the endpoint trusts certificates signed by the CA.

6. Select an **Account Group** from the list to add this account to a group. If no account group is selected, the account is automatically added to the **Default 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. Select the type of **Jump Item Associations** for the account. The **Jump Item Associations** setting determines which Jump Items the account is associated with, so the account is available only for relevant target machines in the representative console during credential injection attempts. Select one of the following associations methods:
 - **Inherited from the Account Group:** Associations for this account are determined by the associations defined in this account's **Account Group**.
 - **Any Jump Items:** This account can be injected within any session started from a Jump Item in which the account is applicable.
 - **No Jump Items:** This account cannot be injected into any session started from a Jump Item.
 - **Jump Items Matching Criteria:** This account can be injected only within sessions started from Jump Items that match the criteria you define, in which the account is applicable.
 - You can define a direct association between Vault accounts and specific Jump Items by selecting the Jump Items from the list, and then clicking **Add Jump Item**.
 - You can further define the association between Vault accounts and Jump Items by specifying matching criteria based on the following Jump Item attributes. If configured, the account is available for injection for any Jump Items that match the specified attribute criteria in addition to any specific Jump Items you added as matching criteria.
 - **Shared Jump Groups:** Select a Jump Group from the list.
 - **Name:** This filter is matched against the value that appears in the **Name** column of the jump item in the representative console.
 - **Hostname / IP:** This filter is matched against the value that appears in the **Hostname / IP** column of the Jump Item in the representative console.
 - **Tag:** This filter is matched against the value that appears in the **Tag** column of the Jump Item in the representative console.
 - **Comments:** This filter is matched against the value that appears in the **Comments** column of the Jump Item in the representative console.



Tip: Click the *i* icon for each option and attribute to view more specific information about it.



Note: Local accounts are available for injection within the endpoints on which they were discovered.

9. Click **Save** at the top of the page to save the new shared credential account.

Add a Personal Generic Account

Personal generic accounts may be used only by the account owner (the user who created the account).

1. From the **/login** interface, go to **Vault > Accounts**.
2. Click **Add**.
3. Select **Personal Generic Account**.
4. Provide a **Name**, **Description**, and **Username** for the account.
5. Select the type of authentication the account uses: **Password**, **SSH Private Key**, or **SSH Private Key with Certificate**.
 - If using an SSH private key, provide the key and passphrase.
 - If using an SSH private Key with certificate, provide the key, passphrase, and certificate.
 - A public key is generated after the account is saved, and can be viewed and copied by editing the account.
6. Click **Save** at the top of the page to save the new personal credential account.



Note: Vault administrators can view personal accounts but cannot edit them, inject them, or view their passwords. Only the user who created the personal account can modify, inject, or view the account's password.



Note: Users can create up to 50 Cloud Vault personal accounts.

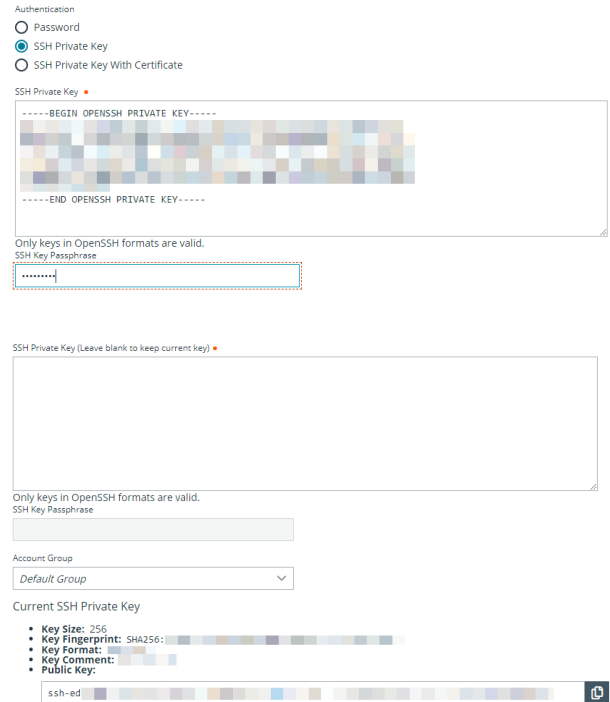
Edit or Delete a Vault Account

1. From the **/login** interface, go to **Vault > Accounts**.
2. For shared accounts:
 - From the **Shared** tab, locate the account you wish to edit or delete.
 - Click the ellipsis button for the account.
 - To edit:
 - Select **Edit**, modify options as necessary, and then click **Save**.
 - To delete:
 - Select **Delete** and click **Yes** to confirm.
3. For personal accounts:
 - From the **Personal** tab, locate the account you wish to edit or delete.
 - To edit:
 - Click **Edit Account** (pencil icon) for the account.
 - Modify options as necessary, and then click **Save**.
 - To delete:
 - Click **Delete Account** (trash can icon) for the account.
 - Click **Yes** to confirm.

View or Copy an SSH Public Key

When creating the account, enter the SSH private key and passphrase. It is validated when the account is saved. The account cannot save if the key is invalid, not in an accepted format, or cannot be decrypted with the provided passphrase.

After saving the account, edit the account to view details for the public key, and copy the public key. The public key details can also be queried with an API.



View the Status of a Vault Account

On the **Vault > Accounts** page, a **Status** column displays when at least one of 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. Accounts used to run a Windows service are indicated as **Service Account** in the **Status** column. 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.

Type	Name	Username	Group	Endpoint	Last Checkout	Password Age	Status
Local			Thgroup-any jump items	Willis	Never	2 months	Reason Failed
Local			Default Group	TELL Willis	Never	No password configured	Rotation Disabled
Domain			Thgroup-any jump items		Thu Nov 18, 2021 4:23 PM CST	2 months	Checked Out



Tip: Click the **Select visible columns** button above the grid to customize the columns displayed in the grid.



Note: The **Status** column is auto-hidden when none of the accounts have a status set.



For more information, see:

- ["Use BeyondTrust Vault with Microsoft Azure Active Directory Domain Services Account" on page 35](#)
- ["Use SSH Certificate Authority in Vault" on page 38](#)

Add and Manage Vault Account Groups

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



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

Add an Account Group

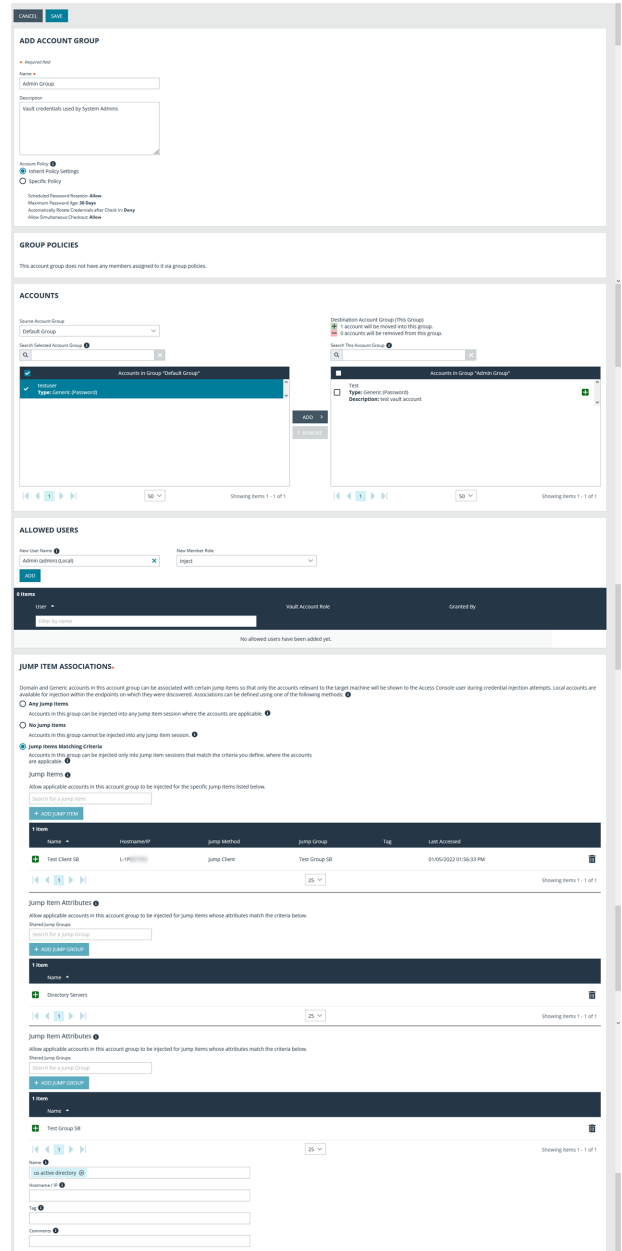
1. From the `/login` interface, go to **Vault > Account Groups**.
2. Click **Add**.

3. Provide a **Name** and **Description** for the group.
4. Select a specific policy for the account group or leave **Account Policy** set to the default value of **Inherit Policy Settings**, in which case the accounts in this account group inherit the policy settings set for the global default account policy on the **Vault > Options** page.
5. Under **Accounts**, select the group from the **Source Account Group** list, and then select the accounts to add to this group.



Tip: The **Default Group** group is a system generated group that contains all user accounts that do not belong to an account group. The **Default Group** 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. Click **Add** to move the accounts over to the **Accounts in This Group** list.
7. In the **Allowed Users** section, add a user and select their Vault role from the **New Member Role** dropdown, and then click **Add**.
8. Select the type of **Jump Item Associations** for the account group. The **Jump Item Associations** setting determines which Jump Items the accounts in this account group are associated with, so that only the accounts relevant to the target machine are available in the representative console during credential injection attempts. Select one of the following associations methods:
 - **Any Jump Items:** Accounts in this group can be injected into any Jump Item session in which the accounts are applicable.
 - **No Jump Items:** Accounts in this group cannot be injected into any Jump Item session.
 - **Jump Items Matching Criteria:** Accounts in this group can be injected only into Jump Item sessions that match the criteria you define, in which the accounts are applicable.
 - You can define a direct association between applicable accounts in this account group and specific Jump Items by selecting the Jump Items from the list, and then clicking **Add Jump Item**.
 - You can further define the association between applicable accounts in this account group and Jump Items by specifying matching criteria based on the following Jump Item attributes. If configured, accounts in this account group are available for injection for any Jump Items that match the specified attribute criteria in addition to any specific Jump Items you added as matching criteria.



- **Shared Jump Groups:** Select a Jump Group from the list.
- **Name:** This filter is matched against the value that appears in the **Name** column of the Jump Item in the representative console.
- **Hostname / IP:** This filter is matched against the value that appears in the **Hostname / IP** column of the Jump Item in the representative console.
- **Tag:** This filter is matched against the value that appears in the **Tag** column of the Jump Item in the representative console.
- **Comments:** This filter is matched against the value that appears in the **Comments** column of the Jump Item in the representative console.



*Tip: Click the **i** icon for each option and attribute to view more specific information about it.*



Note: Local accounts are available for injection within the endpoints on which they were discovered.

9. Click **Save** at the top of the page.

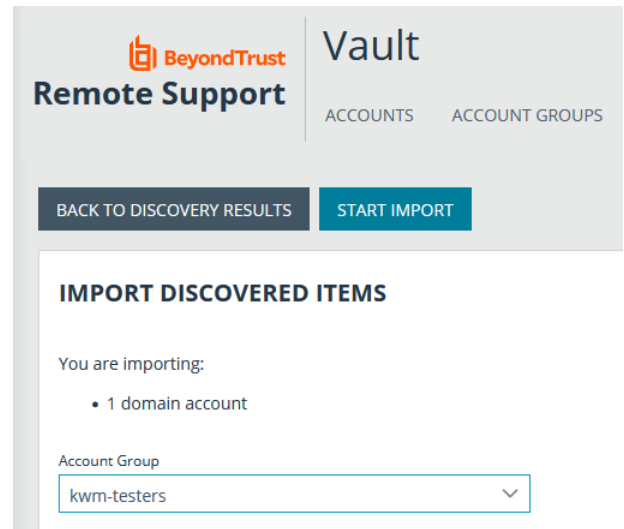
Add a Vault Account to an Account Group from the Accounts Page

1. From the **/login** interface, navigate to **Vault > Accounts**.
2. From the **Shared** tab, click the ellipsis button for the account, 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

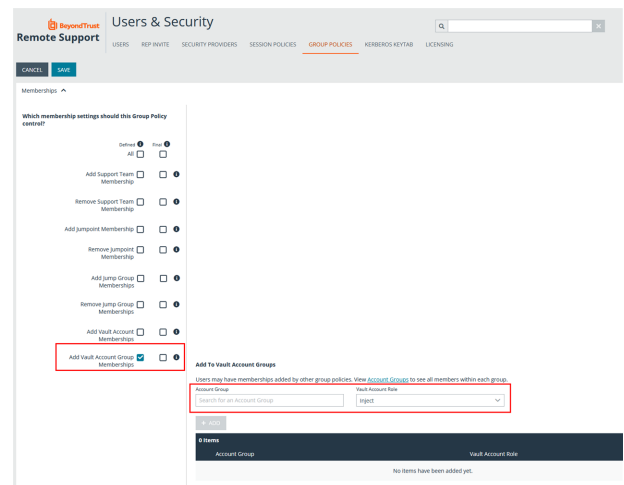
1. From the **/login** interface, go to **Vault > Discovery**.
2. Scroll down to the **Discovery Jobs** section.
3. Click **View Results** for the job.
4. Select the **Local Accounts** or **Domain Accounts** tab as applicable.
5. Select the account you wish to import.
6. Click **Import Selected**.

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** (pencil icon) 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.



- 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.

CANCEL
SAVE

EDIT ACCOUNT GROUP

• Required field

Name •

Description


Vault credentials used by System Admins

GROUP POLICIES

The following group policies assign members to this account group:

- [Admin](#) as Inject And Checkout
- [General Members](#) as Inject And Checkout

- 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 this user.

ALLOWED USERS

New User Name •
 Search for a user

New Member Role
 Inject

ADD

9 Items	User	Vault Account Role	Granted By
	Filter by name		
	Admin (admin)	Inject And Checkout	
	Admin (admin)	Inject And Checkout	Group Policy: Admin Overridden
	General Members	Inject And Checkout	Group Policy: General Members
	General Members	Inject And Checkout	Group Policy: General Members
	General Members	Inject And Checkout	Group Policy: General Members
	General Members	Inject And Checkout	Group Policy: General Members

Add and Manage Vault Account Policies

Vault account policies provide a method to define account settings related to password rotation and credential checkout and apply those settings to multiple accounts at once.

Vault account policies give admins the ability to specify the following account settings:

- Enable scheduled password rotation and set the maximum password age or deny scheduled password rotation.
- Allow or deny the automatic rotation of credentials after the credential is checked in.
- Allow or deny credentials to be checked out simultaneously.

If a setting in an account policy is not defined, it inherits the settings from the global default account policy, configured from the **Vault > Options** page in /login.

The global default account policy must define an option for each setting. If an account does not have a setting defined using a specific policy, it inherits the policy from the account group. If the account group does not have a setting defined using a specific policy, it inherits the policy from the global default account policy.

Multiple account policies that apply to a single Vault account are applied in the following order, from top to bottom:


- The account policy associated with the Vault account
- The account policy associated with the Vault's account group
- The global default account policy settings

If multiple account policies define a setting, then the value from the first applied policy is used.

Add an Account Policy

1. From the /login interface, go to **Vault > Account Policies**.
2. Click **Add**.

3. Provide a **Display Name**, **Code Name**, and **Description** for the policy.

 **Note:** *Code Name and Description are optional. Code Name is for integration purposes. If you do not set a code name, Remote Support creates one automatically.*

4. Under **Permissions**:
 - Allow or deny the ability to automatically rotate account passwords when the specified maximum password age is reached.
 - If automatic password rotation is allowed, set the **Maximum Password Age**.
 - Allow or deny the ability to automatically rotate credentials after check in.
 - Allow or deny simultaneous checkouts for accounts.
5. In the **Allowed Users** section, add a user and select their Vault role from the **New Member Role** dropdown, and then click **Add**.
6. Click **Save** at the top of the page.

CANCEL
SAVE

ADD ACCOUNT POLICY

• Required field

Display Name •

Code Name ?

Description

PERMISSIONS

Automatic Password Management

Scheduled Password Rotation Rules

Not Defined
 Maximum Password Age ?

 Days

Allow

 Deny

Account Settings

Automatically Rotate Credentials after Check In Rules

Not Defined

 Allow

 Deny

Allow Simultaneous Checkout Rules

Not Defined

 Allow

 Deny

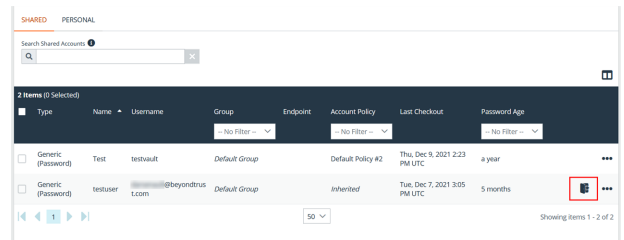
After an account policy is created, it is listed in the grid on the **Account Policies** page. You can copy or edit any of the listed policies by clicking the **Copy** or **Edit** button for the policy in the grid and modifying the settings as required.

View and Check Out Credentials from the /login Interface

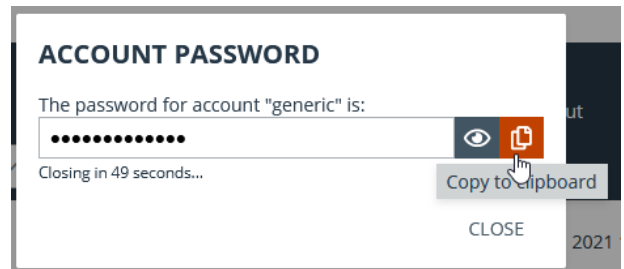
Stored passwords can be retrieved for use outside of a BeyondTrust support session. The `/login` interface allows you to manually check out a password for a shared account, or view and copy a password for a personal account.

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.
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.
5. For SSH Certificate Authority accounts, the signed public key and the private key display. Users must authenticate within 5 minutes. The credentials can also be accessed via API using the `bt vault` subcommand of the Command Line Interface.



Tip: When an account is checked out, it's indicated in the **Status** column. You can hover over the **Checked Out** status to see who has it checked out.

6. When you are finished using a credential, return to the **Accounts** page and click **Check In** to check the password back into BeyondTrust Vault.
7. For SSH Certificate Authority accounts, there is no need for check in, as the credentials are unique for each check out or injection.



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



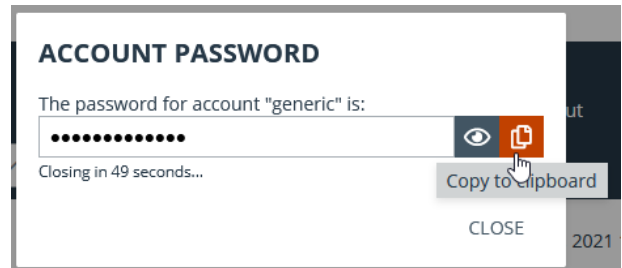
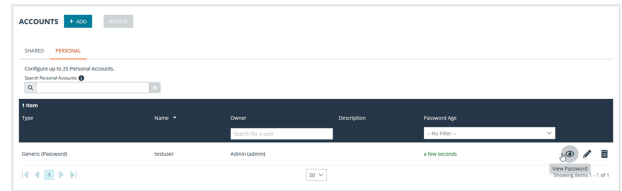
Note: Non-administrative users can only view and modify credentials for which they have access.

Check Out a Service Account

The process for checking out service accounts is the same as other accounts; however, the password must be manually set by the administrator before checking out the account.

View and Copy a Personal Account Password

1. Go to **Vault > Accounts**.
2. From the **Personal** tab, locate the account you wish to use.
3. Click **View Password**.
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.



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.

Rotate Privileged Credentials Using BeyondTrust Vault

Frequently rotating or changing privileged credentials is considered a security best practice. Credentials stored in BeyondTrust Vault can be set to automatically rotate after each use, and can be manually rotated at any time.

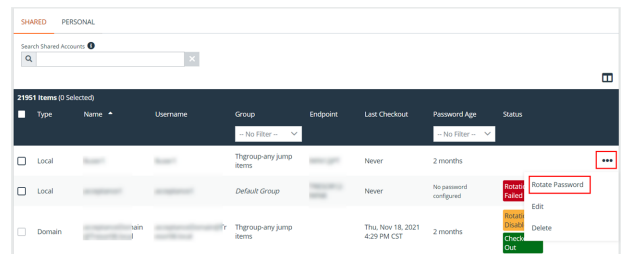
Three actions trigger the automatic rotation of domain credentials:

- Manually checking in a credential from the **/login** interface
- Leaving a support session in which credential injection has been used
- The password reaching its maximum age when scheduled password rotation is enabled

Rotate Domain and Local Credentials Manually

1. From the **/login** interface, go to **Vault > Accounts**.
2. Click the ellipsis button for the account password 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*.



Type	Name	Username	Group	Endpoint	Last Checkout	Password Age	Status
Local			Tgroup-any jump items		Never	2 months	Rotate Password
Local			Default Group		Never	No password configured	Rotate Password
Domain			Tgroup-any jump items		Thu Nov 18, 2021 4:29 PM CST	2 months	Rotate Password

Configure Automatic and Scheduled Rotation of Vault Credentials

To configure passwords for Vault accounts to automatically rotate after each use, enable the **Automatically Rotate Credentials after Check In Rules** option in the account policy being used for the account.

You can schedule password changes for Vault accounts by enabling the **Scheduled Password Rotation Rules** option in the account policy being used for the account.



Note:

- *Service accounts running in a failover cluster environment cannot be rotated. The error "Failover Cluster detected. Unable to change the run-as password for the service <service_name>" appears when a rotation attempt is made and **Rotation Failed** is indicated in the **Status** column for the service.*
- *Services using a Microsoft Graph account as the Run As account cannot be rotated.*
- *Services that have dependent services cannot be rotated, due to the risk of services within the service chain not restarting successfully.*



For more information, please see the following:


- *Account policies, please see ["Add and Manage Vault Account Policies"](#) on page 23.*
- *Rotating credentials for protected users, please see ["Configure User Permissions to Rotate Protected Credentials"](#) on page 6.*


Use Credential Injection During Support Sessions

Credentials stored in BeyondTrust Vault can be used to log in to remote systems during support sessions. Ensure the BeyondTrust Vault has been configured and accounts are imported or manually added for the representative console to use credential injection.

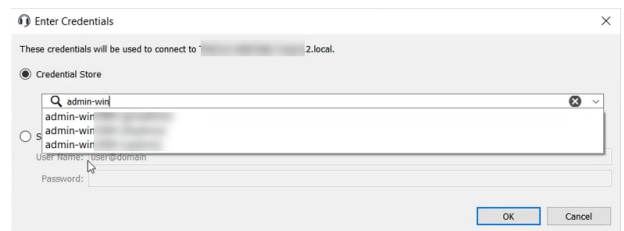
Credential injection is available for:

- Elevating sessions
- Logging into remote Windows systems
- Answering a UAC prompt
- Running a special action

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

 **Note:** This feature is not supported for ARM-based Windows systems.

1. While in a support session in the rep console, you can inject credentials by clicking the **key** icon.
 - a. A dialog appears, allowing you to 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.
 - b. 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.

For SSH Certificate Authority accounts, the TTL is 5 hours. If you are in a shell jump session that exceeds 5 hours and need to perform an action that requires re-authentication, such as stopping all shells and starting again, the action will fail.

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 B Series 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, under **Recommended Accounts**, followed by any remaining credentials. If no credential history exists for an endpoint, the B Series Appliance displays all possible credentials, grouped by accounts that are associated with the Jump Item and not associated with the Jump Item. Jump Item associations for accounts and account groups are configured in /login.

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. Report administrators and users can view and track information about the following:

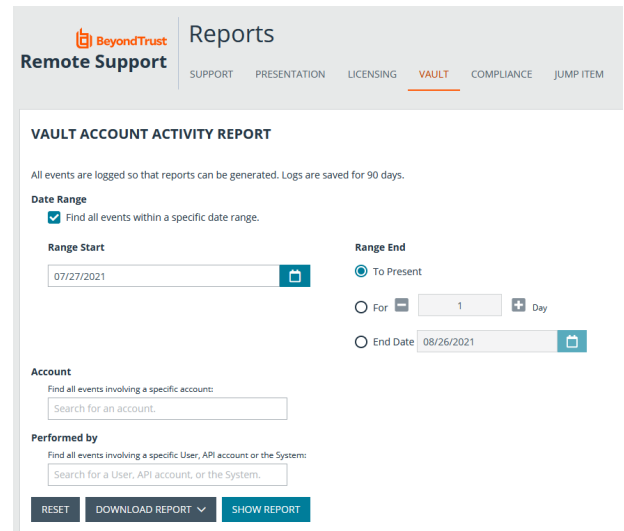
- Account creations and deletions
- Credential check ins and check outs
- Personal credential used
- Password rotations and changes

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.



The screenshot shows the 'Reports' section of the BeyondTrust Remote Support interface. The 'VAULT' tab is selected. The 'VAULT ACCOUNT ACTIVITY REPORT' section is active, displaying the following configuration options:

- Date Range:** A checkbox labeled 'Find all events within a specific date range.' is checked. Below it, 'Range Start' is set to '07/27/2021' and 'Range End' is set to 'To Present'. There are also options for 'For' (set to '1' Day) and 'End Date' (set to '08/26/2021').
- Account:** A search box labeled 'Find all events involving a specific account:' with the placeholder text 'Search for an account.'
- Performed by:** A search box labeled 'Find all events involving a specific User, API account or the System:' with the placeholder text 'Search for a User, API account, or the System.'

At the bottom of the form are three buttons: 'RESET', 'DOWNLOAD REPORT' (with a dropdown arrow), and 'SHOW REPORT'.



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](https://www.beyondtrust.com/docs/remote-support/getting-started/admin/compliance.htm) at <https://www.beyondtrust.com/docs/remote-support/getting-started/admin/compliance.htm>.



For more information, please see [Vault: Report on Vault Account and Rep Activity](https://www.beyondtrust.com/docs/remote-support/getting-started/admin/reports-vault.htm) at <https://www.beyondtrust.com/docs/remote-support/getting-started/admin/reports-vault.htm>.

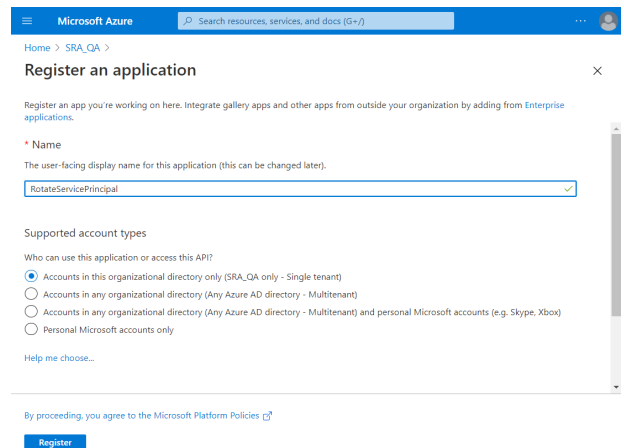
Create a Service Principal in an Azure Active Directory Domain Services Account

Managing Azure Active Directory Domain Services accounts requires a service principal, which is used to give BeyondTrust Vault permission to access Azure AD resources. The following guide describes how to create a new service principal in Azure for BeyondTrust Vault.

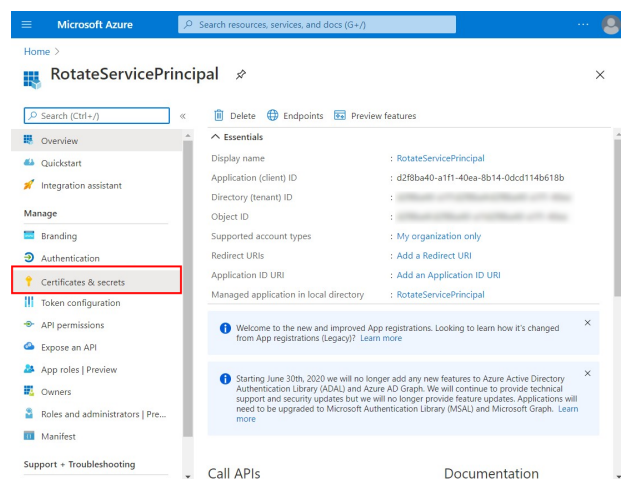
Create a Registered App

Sign into Azure and connect to the Azure AD tenant where you wish to manage passwords, then follow the steps below.

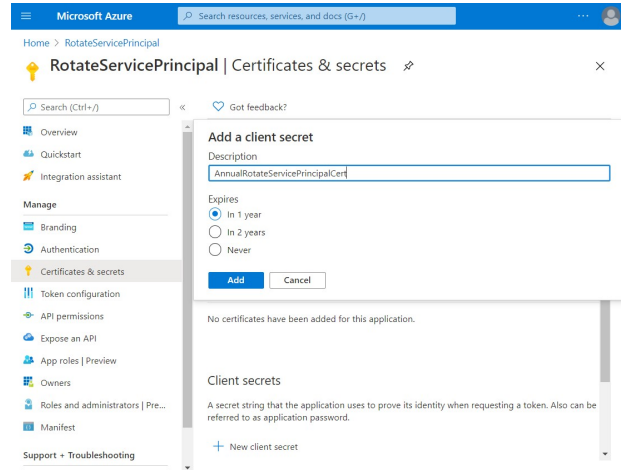
1. On the left menu, select **App registrations**.
2. Click **+ New Registration**.
3. Under **Name**, enter a unique application name.
4. Under **Supported account types**, select **Accounts in this organizational directory only**.
5. Click **Register**.



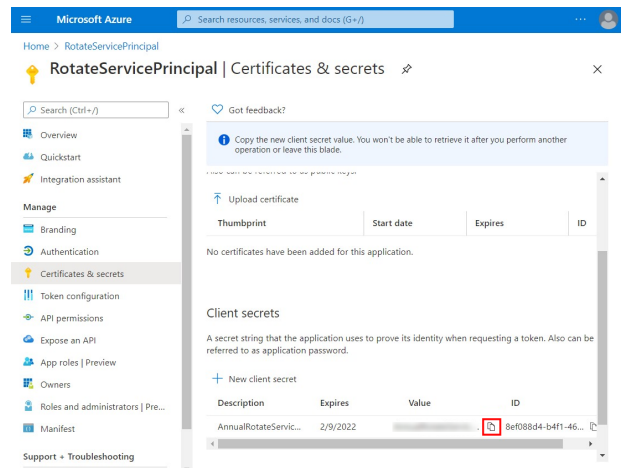
6. Select the new registered app from the list of **Apps Registrations** (if not already visible).
7. Select **Certificates & secrets** from the left menu.
8. Click **+New Client Secret**.
9. Provide a **Description** and appropriate **Expiry**. If you select 1 or 2 years, the service principal must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



10. Click **Add**.



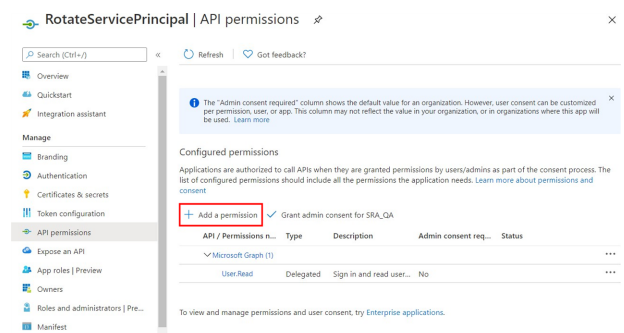
11. Create a copy of the client secret and store it in a safe place. This is the only time it is displayed. This is needed to add the account to the Vault.



Assign API Permissions to the Registered App

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

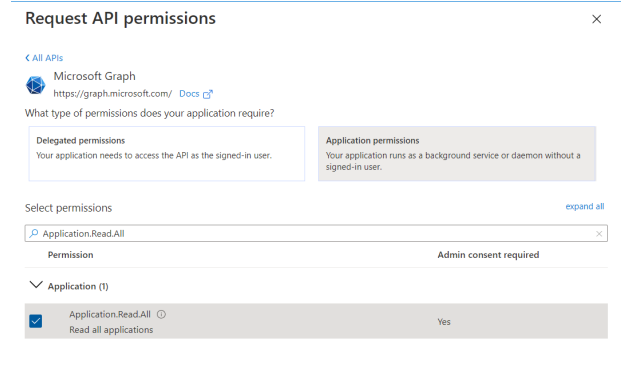
1. Select **API Permissions** from the left menu.
2. Click **+ Add a permission**.
3. Click **Microsoft Graph**.
4. Click **Application Permissions**.
5. Search for **User.ReadWrite.All** and check it in the search results.



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.



Request API permissions

Microsoft Graph
https://graph.microsoft.com/ Docs

What type of permissions does your application require?

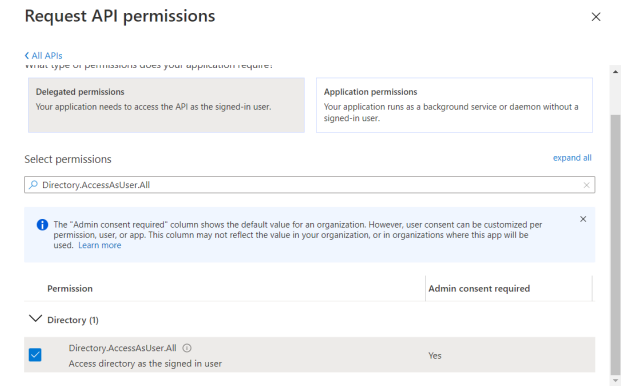
Delegated permissions: Your application needs to access the API as the signed-in user.

Application permissions: Your application runs as a background service or daemon without a signed-in user.

Select permissions

Application.Read.All

Permission	Admin consent required
Application (1)	
Application.Read.All Read all applications	Yes



Request API permissions

Microsoft Graph

What type of permissions does your application require?

Delegated permissions: Your application needs to access the API as the signed-in user.

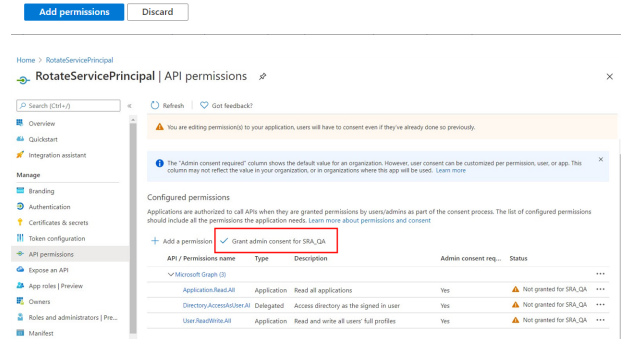
Application permissions: Your application runs as a background service or daemon without a signed-in user.

Select permissions

Directory.AccessAsUser.All

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. Learn more

Permission	Admin consent required
Directory (1)	
Directory.AccessAsUser.All Access directory as the signed in user	Yes



Home > RotateServicePrincipal | API permissions

RotateServicePrincipal | API permissions

Overview

Integration assistant

Manage

- Branding
- Authentication
- Certificates & secrets
- Token configuration
- API permissions
- Expose an API
- App roles | Preview
- Owners
- Roles and administrators | Pre...
- Manifest

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

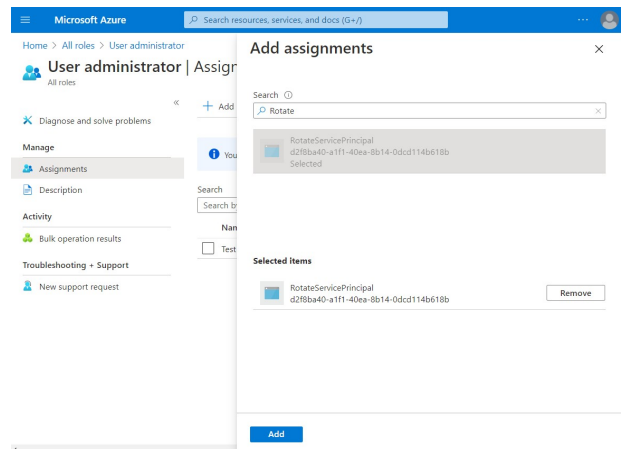
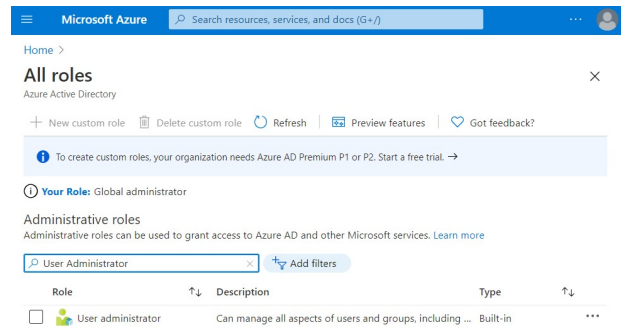
+ Add a permission

API / Permission name	Type	Description	Admin consent req...	Status
Application.Read.All	Application	Read all applications	Yes	Not granted for SRA_GA
Directory.AccessAsUser.All	Delegated	Access directory as the signed in user	Yes	Not granted for SRA_GA
User.ReadWrite.All	Application	Read and write all users' full profiles	Yes	Not granted for SRA_GA

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.

i For information about assigning other roles, please see [Azure AD built-in roles](https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference) at <https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference>.

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.



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.

Status
Azure AD Managed
No Service Principal
Azure AD Managed
No Service Principal
Azure AD Managed
No 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 31](#).

Add or Edit a Service Principal

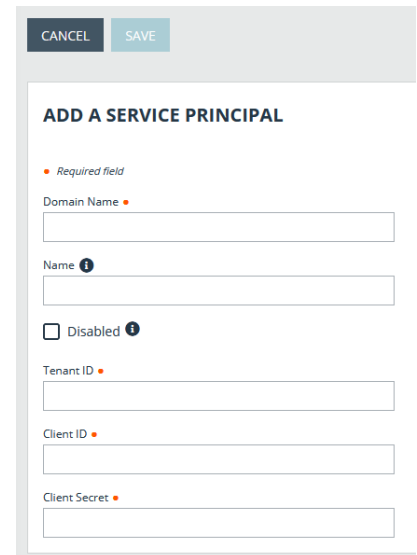
Adding or editing a service principal can be done before a discovery job, or after a discovery job has identified accounts that require a service principal.

1. From the **/login** interface, navigate 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.



Note: *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 a discovery job 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 Accounts, Services, and Endpoints Using BeyondTrust Vault" on page 7](#)
- ["Rotate Privileged Credentials Using BeyondTrust Vault" on page 27](#)



- ["Use Credential Injection During Support Sessions" on page 28](#)

Use SSH Certificate Authority in Vault

This topic explains how SSH certificate authority in Vault provides an alternative to traditional SSH key discovery, management, and rotation for Vault accounts.

Traditional SSH Keys

With basic SSH keys, users have a public/private key pair. The endpoint system is configured to trust the public key, and then anyone with the private key is granted access.

In this scenario, Vault is storing the private key, and it gives the same private key to any user who uses the stored vault account, or requires creating, storing, and assigning a different private key for every user in the Vault and configuring the endpoint to trust a separate public key created by each of the private keys. Since the public and private keys are tied together, if any changes are made, the endpoints would have to be reconfigured to trust each new public key.

SSH Certificate Authority

An alternative to the single public/private key pair, and the sharing of the private key, is to configure the endpoints to trust a public key as a certificate authority. This means the endpoints will trust any certificate signed by the private key of the trusted certificate authority. New certificates are generated, but no changes on the endpoint have to be made as long as the certificates are signed by the private key of the certificate authority.

Benefits

Vault sends new certificates for each user and access request, and these certificates are all short-lived. Short-lived certificates are important because the TTL (time to live) means they are only valid through the expiry time. They cannot be used after, even if shared.

Using short-lived certificates greatly reduces the attack surface, as the certificates can essentially only be used once.

When using a certificate authority for SSH, you no longer have to manage a sprawling inventory of key pairs across all of your endpoints. Just add the public key of the certificate authority to each endpoint once and you're done.

Use SSH Certificate Authority Accounts

Create SSH Certificate Authority Accounts

SSH Certificate Authority accounts are stored in Vault as a type of generic account. SSH Certificate Authority accounts can be added only as shared accounts.

When adding an SSH Certificate Authority account, the admin can choose to have Vault generate the private key, or upload an existing private key.

If they choose to upload a key, they must provide the passphrase for the key, if there is one. The private key cannot be changed or retrieved once the account is created.

The account group, permissions, and Jump Item associations can be edited like any other generic account. SSH Certificate Authority accounts can get both the **Inject** and **Inject and Checkout** roles.

Inject SSH Certificate Authority Accounts

Using SSH Certificate Authority accounts in the Console works like regular SSH keys. For shell jump sessions, the credential shows up as an option in the credential dialog if the user has permission to inject the account and the account can be used for the Jump Item.

When the credential is used in this way, the TTL on the certificate is five hours. If the shell jump session is longer than five hours and requires an action that needs re-authentication (e.g. stop all shells and start again), then the action will fail.

Check out SSH Certificate Authority Accounts

SSH Certificate Authority accounts can be checked out with the same rules as generic username/password accounts. Users can be given permission to checkout the account, and API accounts with Vault permissions can check the account out.

When checking out, the user gets two pieces of information they need: the certificate and the private key. They need both pieces to use the credential. After check-out, the user has five minutes to use it for authentication.

Checking out the credential in the web and the desktop console result in the same style of dialog. A dialog shows the certificate and private key in single line text fields. Both fields allow the user to copy each value with a single click and paste them into files for use with their SSH tool. Users of the desktop client can also retrieve the credentials using the **bt vault** subcommand of the rep cli.

Since the credentials are uniquely generated for each check-out/injection, there is no need to check the credential back in.