### Remote Support Vault Guide

### **Table of Contents**

BeyondTrust Remote Support Vault Guide 4
Configure User Permissions for Remote Support Vault
Configure User Permissions to Rotate Protected Credentials
Discover and Import Accounts, Services, and Endpoints Using BeyondTrust Vault 7
Initiate a Discovery Job for a New Domain
Import Discovered Endpoints Accounts and Services
Initiate a Discovery Job for an Existing Domain10
Schedule Discovery Jobs11
Add and Manage Vault Accounts
Add Generic Credentials and SSH Keys13
Add a Shared Generic Account
Add a Personal Generic Account
Edit or Delete a Vault Account
View the Status of a Vault Account
Add and Manage Vault Account Groups
Add an Account Group
Add a Vault Account to an Account Group from the Accounts Page
Import a Discovered Account to an Account Group20
Add an Account Group to a Group Policy21
Add and Manage Vault Account Policies
Add an Account Policy
View and Check Out Credentials from the /login Interface
Check Out and Check In a Shared Account
Check Out a Service Account
View and Copy a Personal Account Password
Rotate Privileged Credentials Using BeyondTrust Vault
Rotate Domain and Local Credentials Manually27
Configure Automatic and Scheduled Rotation of Vault Credentials
Use Credential Injection During Support Sessions
View and Track BeyondTrust Vault Activity in Remote Support
Run Vault Reports

SALES: www.beyondtrust.com/contact SUPPORT: www.beyondtrust.com/support DOCUMENTATION: www.beyondtrust.com/docs

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	
Traditional SSH Keys	38
SSH Certificate Authority	38
Use SSH Certificate Authority Accounts	

Λ

### **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 <u>BeyondTrust Vault for Remote Support</u> at <u>https://www.beyondtrust.com/remote-</u> 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.
- 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.

Account Settings 🐱		
General Permissions		
Administration		
Administrator	Allowed to Edit File Store	Allowed to Edit Support Button Profiles
Allowed to Administer Vault	Allowed to Edit Canned Messages	Allowed to Edit Canned Scripts
Allowed to Set Passwords	Allowed to Edit Support Teams	Allowed to Edit Custom Rep Links
Allowed to Edit Jumpoints	Allowed to Edit Jump Groups	Allowed to Edit Access Sponsors
Allowed to Edit Public Site	Allowed to Edit Issues	Allowed to Edit IOS Profiles
Allowed to Edit Customer Notices	Allowed to Edit Skills	
Reporting		
Allowed to View Support Session Reports	Allowed to View Vault Reports	Allowed to View Presentation Session Reports
Not Allowed 🗸	Not Allowed V	Not Allowed 🗸
Allowed to view support session recordings	Not Allowed	
Allowed to View License Usage Reports	View Only His/Her Events	
Representative Permissions 💙	View All Events	
Augustability Cettions		

5

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

SALES: www.beyondtrust.com/contact SUPPORT: www.beyondtrust.com/support DOCUMENTATION: www.beyondtrust.com/docs

### **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:

```
dsacls "dc=cps,dc=com" /G "<yourDomainName>\<yourACcountName>:CA;Reset Password;user" /I:S
dsacls "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 <u>Users: Add User Permissions for a Representative or Admin</u> at https://www.beyondtrust.com/docs/remote-support/getting-started/admin/users.htm.

depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

©2003-2024 Beyond Trust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. Beyond Trust is not a chartered bank or trust company, or

### 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 <u>BeyondTrustRemote Support Jumpoint Guide</u> at <u>https://www.beyondtrust.com/docs/remote-support/how-to/jumpoint/index.htm</u>.

### 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.
- 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.

SACK SAVE AND CONTINUE	
ADD DOMAIN	
Add a domain to the Vault if you do not already have one ava	ailable for discovery.
Required field	
DNS Name of the Domain • 🕕	
myhost.example.com	
Jumpoint • 🕕	
Pollux ~	
Management Account • () New Account	
O Existing Account	
Username •	
exampleuser@beyondtrust.com	
Password •	
•••••	
Confirm Password •	
••••••	

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.

SALES: www.beyondtrust.com/contact SUPPORT: www.beyondtrust.com/support DOCUMENTATION: www.beyondtrust.com/docs

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or TC: 3/4/2024 depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

#### REMOTE SUPPORT VAULT GUIDE

### BeyondTrust

### **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.

DISCOVERY: S	COPE
Discovering endpol	rts enables You't to discover and import your managed domain endpoints, as well as the Windows local accounts for those endpoints. The local credentials will be automatically associated with the relevant endpoint du Itionaly, discovering endpoints enables the Vault administrator to create Remote RDP jumg Dantouts during the import process for those endpoints.
Import process. Add Domain Name	isonaly, discovering endpoints enables the value activities activities wereage know jump shoridules ouring the import process for those enapoints.
lampoint	
Management Access	
and growth states	and the second se
<ul> <li>Required field</li> </ul>	
Scope •	
Domain Accourt	15
Search Path 🚯	
Leave blank to	search all OUs and containers BROWSE
LDAP Query 🚯	
Endpoints Search Path ()	
	search all Ous and containers SECOND
LDAP Query 🕚	
	to discover all endpoints
Local Accou	

- 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 Discorvery.

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 PROG	RESS CANCEL DISCOVERY
You may leave this page a	nd log out at any time without interrupting the ongoing operation.
	eady imported. 3 available for import.
Discovering domain a	ccounts 864 found. 3 already imported. 859 disabled. 2 import candidates.
Waiting for local acco	unt discovery to start
Waiting for sources o	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.

ISCOVERY RESULTS				
lect the items to import. If you select	an endpoint you will be able to configure the settings	on the next page.		
Errors 🛩				
ENDPOINTS (0/4) LOCAL ACCOUNTS	VTS (0/5) DOMAIN ACCOUNTS (0/140) SERVIC	ES (1/6)		
1		× 0		
		~ 0		
n I found. 0 already imported. 9 availabl	e for import. (0 selected)	~ 0		
found. 0 already imported. 9 availabl	e for import. (0 selected) Description	Operating System	Distinguished Name	
found. 0 already imported. 9 availabl			Distinguished Name	
found. 8 already imported. 9 available Norre * JO		Operating System		
i found. 0 already imported. 9 available Norre * JD		Operating System Windows 10 Pro	014	

8

- 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.

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.

АСК Т	TO DISCOVERY JOBS IMPORT SELECTED									
DISC	OVERY RESULTS									
elect	the items to import. If you select an endpoint	you will be able to configure the settings on th	e next page.							
Erro	rs ¥									
END	POINTS (2/5) LOCAL ACCOUNTS (3/8)	DOMAIN ACCOUNTS (0/9) SERVICES (11	/11)							
			× 0							
11 fo	und. 0 already imported. 11 available for in	aport. (0 selected)	Searches "Display Name (Description)", "Short							
11 fo	und. O already imported. 11 available for in Display Name (Description)	nport. (0 selected) Short Name .		sername						
			Searches "Display Name (Description)", "Short	semame 19.local						
•	Display Name (Description)	Short Name	Searches "Display Name (Description)", "Short Name", "Endpoint" and "Username".							
	Display Name (Description) SNMP Trap	Short Name  SNMPTRAP	Searches "Display Name (Description)", "Short Name", "Endpoint" and "Username". 19-DC	19.local						
	Display Name (Description) SNMP Trap App Readiness	Short Name  SNMPTRAP AppReadiness	Searches 'Display Name (Description)', "Short Name", "Endpoint" and "Username". 19-DC WN2016	19.local or19.local						
	Display Name (Description) SNMP Trap App Readiness Microsoft App-V Client	Short Name  SNMPTRAP AppReadiness AppVClient	Searches "Display Name (Description)", "Short Name", "Endpoint" and "Username". 19-DC WIN2016 WIN2016	19.local or19.local						
	Display Name (Description) SNMP Trap App Readiness Microsoft App-V Client Windows Audio Endpoint Builder	Short Name  SNMPTRAP AppReadiness AppVClient AudioEndpointBuilder	Searches "Display Name (Description)", "Shart Name", "Indiplint" and "Username". 19-DC WN2D16 WN2D16 WN2D16	19.local or19.local admin						

BACK TO DISCOVERY RESULTS START

IMPORT DISCOVERED ITEMS

2 endpoints

Account Group Service Accounts

Do not create Jump Item
 Create one Jump Item per End
 Jumpeint
 1 )DC

3 local account
11 services

- 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.

COCKIDENCIONARY RELATE

COCKIDENCIONARY

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.

auto	omatically se overed and i	arching through a provided domain	<ol> <li>This enables you to manage you rators can rotate managed creder</li> </ol>	ar domain and local accounts. Thes	se accounts can be injecte	d or checked out depending o	to add your accounts and credentials on User and Group Policy permission es automatic association of domain c	s. Once
		ISONAL	n one reasons an appoint.					
Q	ch Shared Acco	wrs <b>0</b>	×					
	and the factors	-0						
Ite	ma (O Selecto Type *		Group	Endpoint		Password Age		
Ite			Group Service Accounts	Endpoint	Last Checkout	Password Age	Status V	
te			-		Last Checkout			
)	Туре *	Name	Service Accounts			- No Filter	~	

9

SALES: www.beyondtrust.com/contact SUPPORT: www.beyondtrust.com/support DOCUMENTATION: www.beyondtrust.com/docs

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or TC: 3/4/2024 depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

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.

Search Endpoints	0								
Q,		×						Select visible columns	
16 Items									
					јитр Кета		Distinguished Name		
_			Windows 10 Pro	 0 Accounts	13umg Bem	0 Services	CN+ UDC 16.C	1	Ū
							CN+		Ē
			Windows 10 Pro	0 Accounts	1 June Ben	0 Services	s.DC	/	u

SERVICES						
Search Account Groups 0	×					
17 Items Short Name	Display Name (Description)	Endpoint	Usemane	Last status	Restart	
ADSync	Microsoft Azure AD Sync				•	đ
AudioEndpointBuilder	Windows Audio Endpoint Builder	100000000000000000000000000000000000000				Û
Audiosry	Windows Audio					ā
Audiostv	Windows Audio					Ē.
Audiosry	Windows Audio					a
bthserv	Bluetooth Support Service	-				đ
bthierv	Eluetooth Support Service					Û
SAMPTRAP	SNWP Trap				0	đ

BACK TO JUMP ITEMS			
REMOTE RDP JUMP SHO	RTCUT ASSOCIATION + ASSOCIATE SELECTED		
1 Item (1 Selected)			
🗹 Norre +			
RDP1			

SERVICES						
Search Account Groups 0	×					
17 Items Short Name	Display Name (Description)	Endpoint	Username	Last status	Restart	
ADSync	Microsoft Azure AD Sync		-			0
AudioEndpointBuilder	Windows Audio Endpoint Builder	100000000000000000000000000000000000000				đ
Audiosry	Windows Audio					Ō
Audiostv	Windows Audio					6
Audiosry	Windows Audio				2	6
bthserv	Bluetooth Support Service	-				8
bthserv	Eluetooth Support Service				2	đ
SNMPTRAP	SNMP Trap				0	đ

### 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

SALES: www.beyondtrust.com/contact SUPPORT: www.beyondtrust.com/support DOCUMENTATION: www.beyondtrust.com/docs

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or TC: 3/- depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

- 1. Click the **Discover** button for the domain.
- 2. Define the scope of the discovery, and then click Start Discovery.
- 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. (Sheduled jobs are indicated as being performed by System.)



CONTINUE WITH EXISTING DOMAIN

**DISCOVERY: WINDOWS DOMAIN** 

BACK

# Do you want to discover using a new domain or an existing one? New Domain Existing Domain V

- 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.
- **1** 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
- <u>Discover Domains, Accounts, Endpoints, and Services at https://www.beyondtrust.com/docs/remote-support/getting-</u> started/admin/discovery.htm

depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or

### 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.



### 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.
- 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.

14

### 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 nescessary, 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.

depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

- Modify options as necessary, and then click **Save**.
- To delete:
  - Click **Delete Account** (trash can icon) for the account.
  - Click Yes to confirm.

15

#### 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.

O Password		
SSH Private Key		
O SSH Private Key With Certificate		
SSH Private Key •		
BEGIN OPENSSH PRIVATE KEY		
and the second second		
and the second second	100 C 100	
END OPENSSH PRIVATE KEY		
Only keys in OpenSSH formats are valid.		
SSH Key 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.

Only keys in OpenSSH formats are valid. SSH Key Passphrase	r la OnanSEH formate ara valid
---	--------------------------------

### 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. 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 mouseover a specific status to view more details about it.

5.12
- <b>T</b>
· · ·

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

Q	ch Shared Acco	unts U	×						
									Π
2195	1 Items (0 Se Type	Name			Endpoint	Last Checkout	Password Age	Status	
				– No Filter – 🛛 🗸 🤟			No Filter 🗸 🗸		
0	Local	Reserved in the second	3 cm *	Thgroup-any jump items	W	Never	2 months		
	Local			Default Group	TR Wi	Never	No password configured	Rotation Failed	
				Theroup-any jump		Thu, Nov 18, 2021		Rotation	

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

For more information, see:

i

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

SALES: www.beyondtrust.com/contact SUPPORT: www.beyondtrust.com/support DOCUMENTATION: www.beyondtrust.com/docs

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or TC: 3/4/2024 depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

### 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.

depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

18

### BeyondTrust

- 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**.

- 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.

	DD ACCOUNT GROUP					
	ime • Idmin Group					
	scriptor					
	/ault credentials used by System Ad	Imins				
	ount Poley () Inherit Poley Settings					
	I Specific Policy Scheduled Password Reaston: Allow Maximum Password Age 30 Days Assessed all Password Age 30 Days	Charle for Basery				
		y members assigned to it via group	polities.			
bala dama bala d	CCOUNTS					
and balance of a set	unor Account Group			Destination Account Group (This Group	20	
 A make in a constrained in a co		~			his group.	
<pre>v  we we</pre>	2	×		٩.	×	
	<b>2</b>	Accounts in Group "Default G	resp*		Accounts in Group "Admin Group"	
	✓ testaser Type: Generic (Password)			4. 00A		
<pre>share of the second of th</pre>	4 4 <u>1</u> > >	50 V	Showing Items 1 - 1 of 1	H A I F H	50 V	Showing items 1 - 1 o
	LLOWED USERS					
	ne User Name 🚺	New	Member Rale			
Image: Description: Description:     Image: Description: Description:   Image: Description:   Image: Description: Description:   Image: Description:   Image: Description: Description:   Image: Description:   Image: Description: Description:   Image: Description:   Image: Description: Description:   Image: Description:   Image: Description: Description:   Image: Description:   Image: Description: Description:   Image: Description:   Image: Description: Description:   Image: Description:   Image: Description: Description:   Image: Description: Image: Descriptio	Admin (admin) (Local)	X Inj	ed.	~		
be consistent of the construct of the c	A20					
	user *					
		15.				
Amount equipament equi		account group can be associated w	ith certain jump items so that only the accounts r ed. Associations can be defined using one of the f	elevant to the target machine will be shown to the a	Access Console user during credential inj	ection attempts. Local accounts a
The source source is the source of the s	Any Jump Items Accounts in this group can be injo	ected into any jump item session wi	here the accounts are applicable. <b>O</b>			
To the constraint of the constraint	<ol> <li>Any jump Items         Accounts in this group can be injo         No jump Items         Accounts in this group cannot be         jump Items Matching Criteria         Accounts in this group can be injo             are applicable.         </li> </ol>	ected into any jump item session wi	0	unts		
we is a reducted by provide a provide provide a provide a provide a provide a provide a prov	Any Jorep Items Accounts in this group can be inje No Jorep Items Accounts in this group cannot be group Items Matching Criteria Accounts in this group can be inje are applicable. O	ctted into any jump item session wi injected into any jump item session scied only into jump item sessions i	$\sim$ $0$	urts		
Notice     Notice     Space Mark     Space Mark     Space Mark     Space Mark       1     inclusion	) Any Jamp Items Accounts in this group can be lefe ) to Jamp Items Accounts in this group cannot be ) purp Items Matching or Crientia Accounts in this group can be lefe are applicable. (Jump Items ) Allow applicable accounts in this: Search for a Jamp Item;	ected into any jump item session wi injected into any jump item session ected only into jump item sessions i account group to be injected for the	$\sim$ $0$	ud3		
Image: Control of the second secon	) Any pare terms Accounts in this groups can be right Mo barry terms Accounts in this groups cannob be accounts in this groups can be right accounts accounts in this groups can be right accounts accounts in this groups can be right accounts accounts accounts accounts in this groups can be right accounts accounts accounts accounts in this groups can be right accounts accounts accounts accounts in this groups can be right accounts accounts accounts accounts in this groups can be right accounts accounts	ected into any jump item session wi injected into any jump item session ected only into jump item sessions i account group to be injected for the	$\sim$ $0$	urts		
jung hen Akrikets ● Aka gekannet his kannet gekannet his gehaft is jung tens who a shifuer such his e ches ison.	) any pamp items Accounts in this group can be left ) No pamp items Accounts in this group can be left accounts in this group can be left are applicable. Jump Items () Accounts in this group can be left are applicable. Jump Items () Accounts in this is a left in the all set of the all set of the all set and the applicable accounts in this. South for a left the	cool who any jump item session will injected into any jump item sessions toted only into jump item sessions i account group to be injected for the injected and the injected set of the injected session set.	<ul> <li>D</li> <li>Instruction the orderina you define, where the according to the order of the orde</li></ul>			
Average targets     Interview targets       Interview targets     Interview targets     Interview targets     Interview targets     Interview targets <td>) any pamp items Accounts in this group can be kip (n) pamp items Accounts in this group cannob be any pamp items that accounts in this accounts in this group can be kip are applicable. () jump items () Accounts in this South for a jump item () Accounts in this () Account in this () Accounts in this () Accounts in this () Accounts in this () Accounts in this () Accounts in this () Ac</td> <td>cool who any jump item session will injected into any jump item sessions toted only into jump item sessions i account group to be injected for the injected and the injected set of the injected session set.</td> <td><ul> <li>O</li> <li>but much the orien's you define, where the account much the orien's load below.</li> <li>specific jump there is load</li> </ul></td> <td>ump Group Tag</td> <td></td> <td></td>	) any pamp items Accounts in this group can be kip (n) pamp items Accounts in this group cannob be any pamp items that accounts in this accounts in this group can be kip are applicable. () jump items () Accounts in this South for a jump item () Accounts in this () Account in this () Accounts in this () Accounts in this () Accounts in this () Accounts in this () Accounts in this () Ac	cool who any jump item session will injected into any jump item sessions toted only into jump item sessions i account group to be injected for the injected and the injected set of the injected session set.	<ul> <li>O</li> <li>but much the orien's you define, where the account much the orien's load below.</li> <li>specific jump there is load</li> </ul>	ump Group Tag		
Particular Strategy         Image: Stra	) Any parapeters ) Any parapeters ) De para beam Concerns in the parapeters cannot be parapeters that any concerns the type concerns in this series cannot be type parapeters () Anny paralest accounts in this Second beam () any parapeters () Anny parapeters	cool who any jump item session will injected into any jump item sessions toted only into jump item sessions i account group to be injected for the injected and the injected set of the injected session set.	<ul> <li>O</li> <li>but much the orien's you define, where the account much the orien's load below.</li> <li>specific jump there is load</li> </ul>	ung Group Tag est Group SB		
Image: Second	) Any jump terms Accords in this grange can be here accords any set of the here accords a set of the here a	chchi itsi ang Jump Keni sossion vi ngetadi itsi ang Jump Keni sossion chchi ofny reli jump Keni sossion t account group tri la regional for the account group tri la regional for the Host promotion Li P	A     Hard match the otherus year define, where the access     trapecify jump items totale below.     Jump Matchal     Jump Garet     1	nno Group Itag ent Group G 25 V		
Image: Section of the section of t	) Any jump term Accords in the grange can be here accords in the grange can be here purper bernes @ Accords in the large can be here accords any accord accords and the large accords accords in the based accords and accords and the large forces (accords accords and based can be here accords and based can be accords and ba	contribution provide the relation of the second of the sec	A     Hard match the otherus year define, where the access     trapecify jump items totale below.     Jump Matchal     Jump Garet     1	nno Group Itag ent Group G 25 V		
Second prover     Second	) ary jump term Accords in the grange can be here by ary jump and jump term and accords in the grange controls the party terms of Allow applications of an anti- term of a strange controls in the strange terms of terms	contribution provide the relation of the second of the sec	A     Hard match the otherus year define, where the access     trapecify jump items totale below.     Jump Matchal     Jump Garet     1	nno Group Itag ent Group G 25 V		
Image: Control of the state	) any preparation According that they are good to be trained (According that they are good to be trained (According that they are good to be trained on the trained on t	contribution provide the relation of the second of the sec	A     Hard match the otherus year define, where the access     trapecify jump items totale below.     Jump Matchal     Jump Garet     1	nno Group Itag ent Group G 25 V		
jung men Afrikaise ● Alse optimization in the same group to its specified by pays term where while a check leader. The analysis and the same group to its specified by pays term where while a check leader. The analysis and the same group the specified by pays term where where while a check leader. The analysis and the same group the specified by the same state of th	) any preperties Accords in the grange can be reprint accords any preperties Accords and accord accords in the Accord accords and accord accords any Accord accords accords any Accord accords accords accord accords any Accord accords accords accord accords accord Accord accords accord accords accord accords accord Accord accords accords accord accords accord Accord accords accords accords accords accord Accord accords accord accords accord accords accord Accord accords accord accords accord accords accord Accord accord accords accord accords accord accords accord Accord accord accords accord accord accords accord accord Accord accord accord accord accord accord accords accord Accord accord accord accord accord accord accord accord accord accord Accord accord ac	contribution provide the relation of the second of the sec	A     Hard match the otherus year define, where the access     trapecify jump items totale below.     Jump Matchal     Jump Garet     1	nno Group Itag ent Group G 25 V		Showing Items 1 - 1 o
An expective them And expective them Section 2 with a model and a section that is also a real-base which the starts them Section 2 with a model Section 2 with a model Section 2 with a model and a section 2 with a with	A young and the second se	contribution provide the relation of the second of the sec	A     Hard match the otherus year define, where the access     trapecify jump items totale below.     Jump Matchal     Jump Garet     1	nagtionag tag tert drang 8 <u>a</u> √ m		Showing items 1 - 1 of
Participa dem           Instruction 2 and participation	Je projekti melle se	contribution provide the relation of the second of the sec	A     Hard match the otherus year define, where the access     trapecify jump items totale below.     Jump Matchal     Jump Garet     1	nagtionag tag tert drang 8 <u>a</u> √ m		Showing items 1 - 1 of
() A COLUMN CONTON 1 Cont Marie	) any space of the second seco		A	nang tong tig et ong sig m		Showing items 1 - 1 of
Tane         Image: Second Secon	) and a particular design of the second design of t		A	nang tong tig et ong sig m		Showing items 1 - 1 o
In the function         If	) an a part of the second section of the sec		A	nang tong tig et drag sig m		Showing items 1 - 1 o
B         Monositie         B           (4 ≤ 1) > 1         N         Basegions 1.14           (Basegions 0)         Basegions 1.14         Basegions 1.14			A	nang tong tig et drag sig m		Showing items 1 - 1 o
Karl ( ) ) ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) (	) an a part of the second set		A	nang tong tig et drag sig m		Showing items 1 - 1 o
kan ⊕ Manazat # Mataya @ Manazat # ⊕	) any space of the second seco		A	nang tong tig et drag sig m		Showing terms 1 - 1 or Deceming terms 1 - 1 or Deceming terms 1 - 1 or
La Sable Rendery () Realizer / P			A	να βουχ 1g π ∨ π π		blowing terms 1 - 1 of Decening terms 1 - 1 of
	Jourgeneral and a second secon		A	να βουχ 1g π ∨ π π		blowing terms 1 - 1 of Decening terms 1 - 1 of
Ter O	<ul> <li>Johnson (1999)</li> <li>Johnson (1999)<td></td><td>A</td><td>να βουχ 1g π ∨ π π</td><td></td><td>blowing terms 1 - 1 of Decening terms 1 - 1 of</td></li></ul>		A	να βουχ 1g π ∨ π π		blowing terms 1 - 1 of Decening terms 1 - 1 of
	<ul> <li>Johnson (1999)</li> <li>Johnson (1999)<td></td><td>A</td><td>να βουχ 1g π ∨ π π</td><td></td><td>blowing terms 1 - 1 of Decening terms 1 - 1 of</td></li></ul>		A	να βουχ 1g π ∨ π π		blowing terms 1 - 1 of Decening terms 1 - 1 of

 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.

<sup>©2003-2024</sup> BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or TC: 3/4/2024 depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

20

- 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.

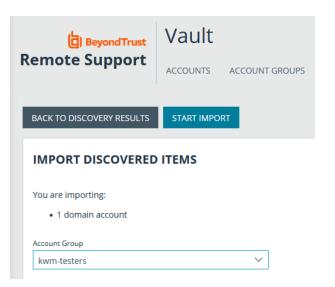
### Import a Discovered Account to an Account Group

- 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.

SALES: www.beyondtrust.com/contact SUPPORT: www.beyondtrust.com/support DOCUMENTATION: www.beyondtrust.com/docs

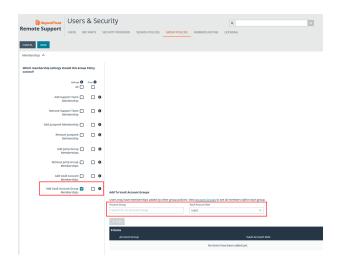


- 7. Select the group from the Account Group list.
- 8. Click Start Import.



### 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.



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.

EDIT ACCOUNT • Required field Name • Admin Group Description Vault credentials used	GROUP			
Name • Admin Group Description				
Name • Admin Group Description				
Admin Group Description				
Description				
Vault credentials used				
	l by System Admi	ins		
			14.	
GROUP POLICIE	5			
The following group po				

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 overidden by the explicitly granted individual access for this this user.

ALLOWED USERS		
New User Name 🚯	New Member Role	
Search for a user	inject ~	
DDA		
Items		
	Vault Account Role	Granted By
Filter by name		
Admin (admin)	Inject And Checkout	
Admin (admin)		Group Policy: <u>Admin</u> Overridden
		Group Policy: General Members
101-11-1000-11-11-1		Group Policy: General Members
		Group Policy: General Members

Admin as Inject And Checkout
 General Members as Inject And Checkout

SALES: www.beyondtrust.com/contact SUPPORT: www.beyondtrust.com/support DOCUMENTATION: www.beyondtrust.com/docs

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

### 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.

SALES: www.beyondtrust.com/contact SUPPORT: www.beyondtrust.com/support DOCUMENTATION: www.beyondtrust.com/docs

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.

Required field Display Name	
Display Name	
	7
Code Name 🚺	7
Description	
h	<i>(</i>
PERMISSIONS	
PERMISSIONS	
Automatic Password Management	Navimum Parcuned Are
	Maximum Password Age
Automatic Password Management Scheduled Password Rotation Rules Not Defined Allow	Maximum Password Age 0 30 Days
Automatic Password Management Scheduled Password Rotation Rules	
Automatic Password Management Scheduled Password Rotation Rules Not Defined Allow	
Automatic Password Management Scheduled Password Rotation Rules Not Defined Allow Deny	
Automatic Password Management Scheduled Password Rotation Rules Not Defined Allow Deny Account Settings Automatically Rotate Credentials after Check In Rules Not Defined	
Automatic Password Management Scheduled Password Rotation Rules Not Defined Allow Deny Account Settings Automatically Rotate Credentials after Check In Rules Not Defined Allow	
Automatic Password Management Scheduled Password Rotation Rules Not Defined Allow Deny Account Settings Automatically Rotate Credentials after Check In Rules Not Defined	
Automatic Password Management Scheduled Password Rotation Rules Not Defined Allow Deny Account Settings Automatically Rotate Credentials after Check In Rules Not Defined Allow	
Automatic Password Management Scheduled Password Rotation Rules Not Defined Allow Deny Account Settings Automatically Rotate Credentials after Check In 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 polices by clicking the **Copy** or **Edit** button for the policy in the grid and modifying the settings as required.

TC: 3/4/2024

### 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.
- 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.

ACCOUNT PASSWORD The password for account "generic" is: Closing in 49 seconds... Copy to ripboard CLOSE 2021

- **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.
- 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.

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

### 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.

ACCOUNT PASSWORD	
The password for account "generic" is:	ut
•••••	①
Closing in 49 seconds	Copy to ipboard
	CLOSE 2021

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or TC: depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

### 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*.

	ch Shared Acco	unts 0						
۹			×					
195	l Items (0 Se	lected)						
		Name 🔷	Username		Endpoint	Last Checkout	Password Age	
				No Filter 🗸 🗸 🗸			No Filter 🗸 🗸	
	Local	Reserved in the second s	Rest"	Thgroup-any jump items	-	Never	2 months	[
	Local			Default Group		Never	No password configured	Rotatie Failed
	Domain	tain		Thgroup-any jump items		Thu, Nov 18, 2021 4:29 PM CST	2 months	Rotati Disabl Delete

### **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 <u>"Configure User Permissions to Rotate Protected Credentials" on page 6</u>.

SALES: www.beyondtrust.com/contact SUPPORT: www.beyondtrust.com/support DOCUMENTATION: www.beyondtrust.com/docs

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or TC: 3/4/2024 depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

### **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.

- 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).

Enter Credentials	:
These credentials will be used to connect to 2.local.	
Credential Store	
Q admin-win	<b>8</b> ~
admin-win	
) s admin-win admin-win	
User Name: User@domain	
Password:	
	OK Cancel

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.
- 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.

BeyondTrust	Reports	
Remote Support	SUPPORT PRESENTATION	LICENSING VAULT COMPLIANCE JUMP ITE
VAULT ACCOUNT ACT	IVITY REPORT	
All events are logged so that rep	orts can be generated. Logs are sa	ved for 90 days.
Date Range		
Find all events within a s	pecific date range.	
Range Start		Range End
07/27/2021	Ö	To Present
		O For 🖬 1 🕒 Day
		O End Date 08/26/2021
Account		
Find all events involving a specific	account:	
Search for an account.		
Performed by		
Find all events involving a specific	User, API account or the System:	
Search for a User, API acco	unt, or the System.	

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.

SALES: www.beyondtrust.com/contact SUPPORT: www.beyondtrust.com/support DOCUMENTATION: www.beyondtrust.com/docs

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or TC: 3/4/2024 depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.



**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 <u>Compliance: Anonymize Data to Meet Compliance Standards</u> at <a href="https://www.beyondtrust.com/docs/remote-support/getting-started/admin/compliance.htm">https://www.beyondtrust.com/docs/remote-support/getting-started/admin/compliance.htm</a>.

i

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

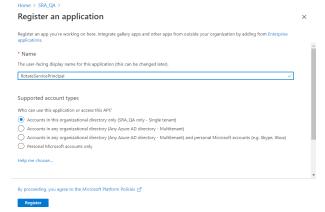
### Create a Service Principal in an Azure Active Directory Domain Services Account

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.

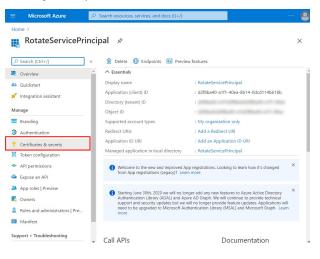
### Create a Registered App

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.
- 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.

	P Search resources, services, and docs (G+/)
Home > RotateServicePrincipal	
RotateServicePri	incipal   Certificates & secrets ⇒ ×
P Search (Ctrl+/)	« 🛇 Got feedback?
B Overview	Add a client secret
4 Quickstart	Description
💉 Integration assistant	AnnualRotateServicePrincipalCert
Manage	Expires
Branding	In 1 year     In 2 years
Authentication	Never
📍 Certificates & secrets	
III Token configuration	Add Cancel
- API permissions	No certificates have been added for this application.
🙆 Expose an API	
App roles   Preview	
👪 Owners	Client secrets
Roles and administrators   Pre	A secret string that the application uses to prove its identity when requesting a token. Also can be
10 Manifest	referred to as application password.
Support + Troubleshooting	+ New client secret
	P Search resources, services, and docs (G+/)     ··· 🧕
Home > RotateServicePrincipal	ncipal   Certificates & secrets 🛷 🛛 🗙 🗙

	ĩ								
<ul> <li>Quickstart <ul> <li>Integration assistant</li> <li>Integration assistant</li> <li>Regretation assistant</li> <li>Quickstart <ul> <li>Upload certificate</li> <li>Branding</li> <li>Quickstart</li> &lt;</ul></li></ul></li></ul>	¢	Search (Ctrl+/)	«	💙 Got feedback?					
Integration assistant <sup>↑</sup> Upload certificate <sup>↑</sup> Certificate <sup>↑</sup> Upload certificate <sup>↑</sup> Upl			^			u won't be able to retrieve	it after you perform anothe	r	
Amage     Thumbprint     Start date     Expires     ID       Branding     No certificates have been added for this application.     No certificates have been added for this application.     ID       Certificates & secrets     In the configuration     No certificates have been added for this application.     In the configuration.       Approver     Approver     Approver     Approver is identify when requesting a token. Also can be referred to as application password.       Boels and administrators   Pre     Description     Expires     Value       Munifest     Configuration     Expires     Value					panana najar				*
Branding     No certificates have been added for this application.       Certificates & secrets     Itoken configuration       Approved Secrets     Client secrets       Approved Secrets     Approved Secrets       Approved Secrets     Approved Secrets       Bespose an API     A secret string that the application password.       Approved Secrets     Approved Secrets       Bespose an API     A secret string that the application password.       Bespose and administrators   Pre     Description       Expires     Value       Munifest     AnnualRotateServic 2/9/2022	Ла	nage		↑ Upload certificate					
Certificates & secrets         If Token configuration         P permissions         Depose an API         A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.         App roles [Preview         Owners         Roles and administrators [Pre         Manifest             Manifest	2	Branding	Ι.	Thumbprint		Start date	Expires	ID	
Token configuration     AP permissions     Client secrets       Expose an API     A secret trining that the application password.       App roles   Preview     • New client secret       Owners     • New client secret       Boles and administrators   Pre     • Description       Manifest     • AnnualRotateServic 2/9/2022	•	Authentication	N	No certificates have been	added for this	application.			÷
API permissions     Client secrets     Spore an API     A secret string that the application uses to prove its identity when requesting a token. Also can be     referred to as application password.     App roles   Preview     Mew client secret     New client secret     Manifest     AnualRotateServic 2/9/2022     Constrained to the secret	ł	Certificates & secrets							1
Arr premissions     Exprose an AP     Apr ordes   Preview     Apr ordes   Preview     Apr ordes   Preview     Owners     Roles and administrators   Pre     Manifest     Annual RotatsServic 2/9/2022     C     SerdBad4-b4f1-d6	l	Token configuration							1
App roles  Preview		API permissions	0	Client secrets					1
App roles   Preview  Owners  Owners  Roles and administrators   Pre.  Manifest  Manifest  ArnualRotateServic 2/9/2022  C  Sef088d4-b4f1-46  C	2	Expose an API				to prove its identity when	requesting a token. Also	can be	:
Owners         Description         Expires         Value         ID           Roles and administrators   Pre         Description         Expires         Value         ID           Manifest         AnnualRotateServic         2/9/2022         .	4	App roles Preview	1.1	elerred to as application	password.				1
Manifest AnnualRotateServic 2/9/2022 Set0884-b4f1-46 C	ė	Owners		+ New client secret					1
(	Ģ	Roles and administrators   Pre		Description	Expires	Value	ID		
upport + Troubleshooting	5	Manifest		AnnualRotateServic	2/9/2022		. 🗋 8ef088d4-b4f1	-46 [	5
	u	oport + Troubleshooting		4				•	Ŧ

### 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.

RotateServicePrin	<b>cipal</b>   API permissio	ons 🖉				×
P Search (Ctrl+/)	: 🕐 Refresh 🕴 🛇 Got fer	edback?				
B Overview	A					
<ul> <li>Quickstart</li> <li>Integration assistant</li> </ul>				an organization. However, use in your organization, or in or		×
Manage						
Branding	Configured permissions					
Authentication	Applications are authorized to list of configured permissions					The
📍 Certificates & secrets	consent					
Token configuration	+ Add a permission 🗸	Grant admin	consent for SRA_QA			
API permissions	API / Permissions n	Туре	Description	Admin consent req S	tatus	
Expose an API	Microsoft Graph (1)					
App roles   Preview	User.Read	Delegated	Sign in and read user	No		
Cowners						
Roles and administrators   Pre	To view and manage permissi	ons and user	consent, try Enterprise ap	plications.		
Manifest						

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or TC: 3/4 depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

- 6. Search for Directory.Read.All and check it in the search results.
- 7. Click Delegated Permissions.

9. Click Add permissions.

8. Search for **Directory.AccessAsUser.All** and check it in the search results.

10. Remove the **User.Read** permission that is granted by default by clicking the ellipses menu and selecting **Remove permission**.

All APIs		
Microsoft Graph		
https://graph.microsoft.com/ Docs		
Vhat 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 withou signed-in user.	ut a
elect permissions	e	expand a
P Application.Read.All		
Permission	Admin consent required	
✓ Application (1)		
Application.Read.All ① Read all applications	Yes	
Add permissions Discard Request API permissions AIAPIs Interpret of permissions upper poor approximation requires.		×
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 withou signed-in user.	it a
elect permissions	expa	and all
Directory.AccessAsUser.All		×
The "Admin consent required" column shows the default value for permission, user, or app. This column may not reflect the value in used. Learn more	r an organization. However, user consent can be customized per your organization, or in organizations where this app will be	×
Permission	Admin consent required	
V Directory (1)		
<ul> <li>Directory (1)</li> </ul>		
Directory.AccessAdUser.All      Access directory as the signed in user  Add permissions Discard	Ves	
Access directory as the signed in user Add permissions Discard  * > RedatGenochhogul	Yes	
Access directory as the signed in user Add permissions Discard  * > Rotacteneouthropal RotateServicePrincipal   API permissions *	Yes	
Access directory as the signed in user  Add permissions Discard  e> Rotacleneithropal RotateServicePrincipal   AP  permissions # anab_Ditrig		
Access directory as the signed in user  Add permissions Discard  re > RotactenetricePrincipal   AP  permissions	Yes ens will have to connect even if they've ainsety done so pericosy.	
Access directory as the signed in user      Add permissions     Discard      Productionscrimequal      RotateServicePrincipal   API permissions     P      Get were detay permission	en ed hans to consert over it flagve analy, dore to precoudy.	. This
Access directory as the signed in user  Add permissions Discard  e) Rotate/Service/Principal   API permissions Rotate/Service/Principal   API permissions Rotate/Service/Principal  () Rotate/		L. This
Access directory as the signed in user  Add permittations Discard  Constructivespal  RotateServicePrincipal   AP  permissions Constructivespal  Constructivespan  Constructive	en ed hans to consert over it flagve analy, dore to precoudy.	L. This

Access directory as the signed in use

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:

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or TC: 3. depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

×

Ťψ

Туре

- BeyondTrust
  - 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.

Microsoft Azure

() Your Bole: Global administrator

Administrative roles

🔎 User Administrator

🗌 🍰 User administrator

Role

All roles

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

Home > All roles > User administrat	or	Add assignments	×
User administrato	<b>r</b>   Assigr		
K Diagnose and solve problems	× + Add	Search ① P Rotate	×
Manage Assignments	1 You	RotateServicePrincipal d2(8ba40-a111-40ea-8b14-0dcd114b618b Selected	
Description	Search Search br		
Activity	Nan		
Bulk operation results Froubleshooting + Support	Test	Selected items	
New support request		RotateServicePrincipal d2f8ba40-a1f1-40ea-8b14-0dcd114b618b	Remove

+ New custom role 📋 Delete custom role 🕐 Refresh 🛛 🚾 Preview features 🛛 💝 Got feedbacks

1 To create custom roles, your organization needs Azure AD Premium P1 or P2. Start a free trial. →

↑↓ Description

nistrative roles can be used to grant access to Azure AD and other Microsoft services. Learn more

× + Add filters

Can manage all aspects of users and groups, including ... Built-in

**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 information about assigning other roles, please see <u>Azure AD built-in roles</u> at <u>https://docs.microsoft.com/en-</u> us/azure/active-directory/roles/permissions-reference.

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or TC: C depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

### 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.

 Image: 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

For more information on creating a service principal in Azure, please see <u>"Create a Service Principal in an Azure Active</u> 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.

35 TC: 3/4/2024

- 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.	<ul><li>Enter the mandatory information:</li><li>Domain Name</li></ul>	CANCEL SAVE
	<ul> <li>Tenant ID</li> <li>Client ID</li> <li>Client Secret</li> </ul>	ADD A SERVICE PRINCIPAL  • Required field
4. 5.	If desired, enter a name to easily identify the service principal. 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 <b>Status</b> is <b>Service Principal Unavailable</b> and <b>Disabled</b> .	Domain Name •
6.		Tenant ID •
	<ul> <li>If adding the service principal is successful, the new service principal displays in the list of domains, with the status OK.</li> <li>If adding the service principal fails, the Status is <b>Disabled</b> and <b>Failed</b>. Click the pencil icon to return to the edit screen, and review the detailed error message.</li> </ul>	Client ID •
7	Due a discourse is he again. In the list of require the account Status is still Asymp AD Menory	a di hartaka Na Osmala a Daimaina ku ata

 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

SALES: www.beyondtrust.com/contact SUPPORT: www.beyondtrust.com/support DOCUMENTATION: www.beyondtrust.com/docs

i

• "Use Credential Injection During Support Sessions" on page 28

SALES: www.beyondtrust.com/contact SUPPORT: www.beyondtrust.com/support DOCUMENTATION: www.beyondtrust.com/docs

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or TC: 3/4/2024 depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

### **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.

depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

38

#### **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 that 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.

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or TC: a depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.