



BeyondTrust

Password Safe 22.4 User Guide

Table of Contents

Password Safe User Guide	3
Select a Display Language	3
Log In to the Web Portal	3
Change Your Login Password	4
Reset a Forgotten Password	4
Navigate the Password Safe Web Portal	5
Read the Accounts Grid	5
Use Quick Links	6
Request a Password from Password Safe	7
Request a Password Release	7
Review a Password Request	7
Approve or Deny a Password Request	8
Retrieve a Password	8
Multi-System Checkout	8
Approve a Request for Multi-System Checkout	9
Use the OneClick Feature	9
Request SSH or RDP Sessions in Password Safe	10
Request an RDP Session	10
SSH Direct Connect	10
RDP Direct Connect	11
Enforce Session End Time	12
Request Remote Proxy Session	13
Password Safe Use Cases	15
Request Access to a Linux Account - Password Retrieval	15
Request RDP Access to a Windows Account - Session Management	17
Request Access to a Microsoft SQL Account - Remote Applications	18
Use Secrets Safe	21
Create a Secret in Secrets Safe	21
Manage Folders in Secrets Safe	22
View and Copy a Secret in Secrets Safe	23
Edit and Delete a Secret in Secrets Safe	24

Password Safe User Guide

Password Safe includes a web-based interface for executing password requests and approvals. You can launch the Password Safe web portal by selecting **Password Safe** from the menu in the BeyondInsight management console. The web portal is configured by your Password Safe administrator.

Password Safe's random password generator algorithm does not use any common phrases or dictionary words as inputs or in its generation. It selects each password character randomly from the list of allowable characters, numerals, and symbols to build the password.

A Password Safe user is authorized to log in to the Password Safe U-Series Appliance and perform tasks. The specific tasks a user can perform are determined by the privileges assigned to that user.

Select a Display Language

The Password Safe web portal can be displayed in the following languages:

- Dutch
- English
- French
- Japanese
- Korean
- Portuguese
- Spanish

If your BeyondInsight Administrator has the option enabled, you can select a language from the list on the **Log In** page or by clicking the **Profile and preferences** button, and then selecting it from the **Language** list.



Note: If no languages are available, please contact your BeyondInsight administrator.

Log In to the Web Portal

Your Password Safe administrator configures login credentials for the web portal. Contact your administrator if you are unsure which credentials to use. Potential authentication methods include:

- **Password Safe:** Enter your Password Safe credentials and then click **Login**.
- **Active Directory:** Enter your Active Directory credentials, select a domain from the list, and then click **Login**.
- **LDAP:** Enter your LDAP credentials, select an LDAP server from the list, and then click **Login**.
- **RADIUS:** Enter your Password Safe credentials and then click **Login**. Enter RADIUS code and then click **Submit**.
- **Smart Card:** Select a certificate and then enter the Smart Card PIN.
- **SAML:** Follow the procedure for your third-party authentication type.



Note: A pre-login banner might be configured on your system. You must click **OK** before you can enter your credentials.

Change Your Login Password

In the BeyondInsight Console, click the **Profile and preferences** button, and then click **Change Password**. Your password must be 6-117 characters in length.



Note: You cannot change your password if you are currently logging in with Active Directory or LDAP credentials, or if your account is currently logged out.

Reset a Forgotten Password

If you forget your console password, click **Forgot Password** on the **Login** page. Enter your username and then click **Reset Password**.

You will receive an email from the console administrator. Click the reset link provided in the email.



Note: You cannot reset your password if you are currently logging in with Active Directory or LDAP credentials, or if SMTP is improperly configured.

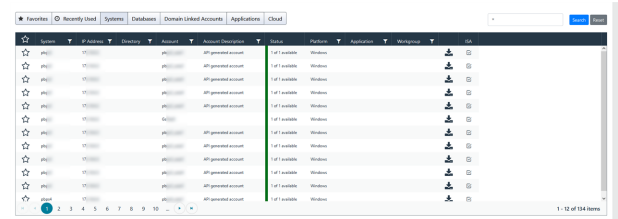


For more information on configuring SMTP, please see [Run the Configuration Wizard](https://www.beyondtrust.com/docs/beyondinsight-password-safe/appliance/install/configure-appliance.htm#run-configuration-wizard) at <https://www.beyondtrust.com/docs/beyondinsight-password-safe/appliance/install/configure-appliance.htm#run-configuration-wizard>.

Navigate the Password Safe Web Portal

In the **Accounts** tab, click a tab to search for the account, system, or application you need to access.

Tip: For optimum efficiency, the web portal screen resolution should be no less than 1280 × 800 pixels.



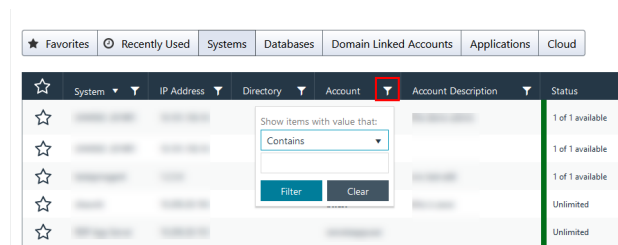
Note: When you first log in to the Password Safe web portal, no accounts are available in the **Favorites** tab.

Read the Accounts Grid

You can rearrange the grid columns by clicking the title and dragging to the desired location. The following information is displayed in the grid:

Favorites	Click the star to add your most used accounts to your list of favorites. You can then select the Favorites tab to display only favorite accounts.
System	The system's name.
OneClick buttons	Click the OneClick buttons to access the OneClick feature. A grayed out button indicates that the account cannot be accessed using OneClick.
Directory	The directory name, if applicable.
Account	The username on the account.
Account Description	The description of the managed account provided when the account was set up.
Status	Indicates if the account is available. Green indicates the account is available. Red indicates it is unavailable.
Platform	The type of operating system.
Application	The application managed by Password Safe, if applicable.
Workgroup	The workgroup the account is tied to, if applicable.
Download RDP Direct Connect File buttons	Click the Download RDP Direct Connect File (down arrow) button to request an RDP Direct Connect session.

Each column title has its own search filter. From the dropdown, select **Contains**, **Starts With**, **Is Equal To**, or **Is Not Equal To**. Enter a search string, and then click **Filter**.



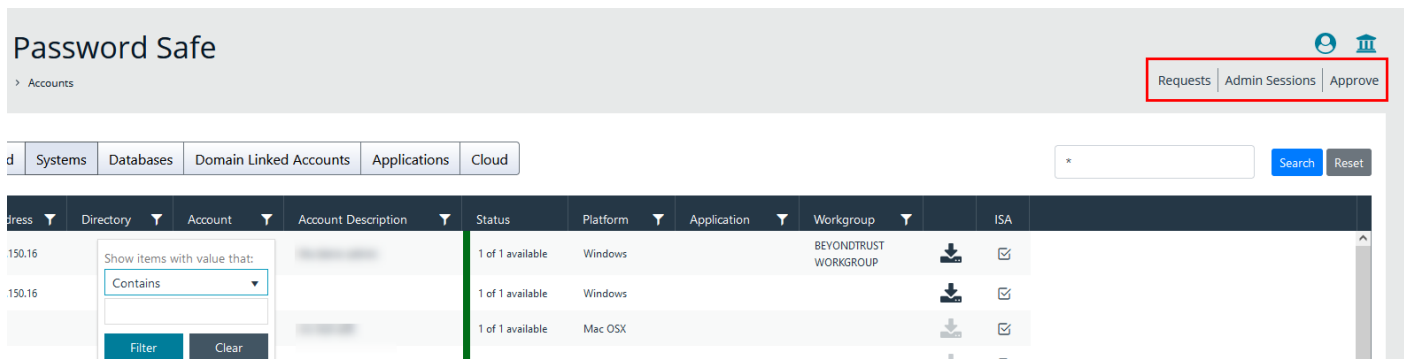
i For more information, please see the following:

- "Use the OneClick Feature" on page 9
- "SSH Direct Connect" on page 10
- "RDP Direct Connect" on page 11







Use Quick Links

The Password Safe web portal uses quick links at the top of the page to navigate to different areas of the application.

The links displayed depend on your assigned Password Safe roles.



The screenshot shows the Password Safe web portal interface. At the top, there is a header with the title "Password Safe" and a navigation menu with links for "Requests", "Admin Sessions", and "Approve". Below the header, there are several tabs: "Systems", "Databases", "Domain Linked Accounts", "Applications", and "Cloud". A search bar is visible with a "Search" button and a "Reset" button. The main content area displays a table with columns: "Address", "Directory", "Account", "Account Description", "Status", "Platform", "Application", "Workgroup", and "ISA". The table contains three rows of data, each representing an account. A filter dropdown menu is open over the "Account" column, showing "Contains" as the selected filter. The table data is as follows:

Address	Directory	Account	Account Description	Status	Platform	Application	Workgroup	ISA
150.16				1 of 1 available	Windows		BEYONDTRUST WORKGROUP	 
150.16				1 of 1 available	Windows			 
				1 of 1 available	Mac OSX			 

Request a Password from Password Safe

If you have a dual control configuration, the password release is a three-step process. Using dual control ensures the security of the system account password, provides accountability, and provides dual control over the managed accounts.

1. **Password request:** An authorized requester requests a password release.
2. **Password approval:** An authorized approver reviews and approves the request for release.
3. **Password retrieval:** The authorized requester retrieves the approved password.

To use a dual control setup, Password Safe users must be assigned one of the following roles: **Requestor**, **Approver**, or **Requestor/Approver**.

Request a Password Release

1. Log in to the Password Safe web portal.
2. On the **Accounts** page, click the tab for the type of system or application you need to access.
3. Select the system from the list.
4. On the **Requests** page, set the following:
 - **Start Date:** Select the start date for the session that corresponds with the access policy.
 - **Start Time:** Select **Immediately** to release the password at the current time, or click the **Scheduling** button for a future release. For example, schedule a release to coincide with scheduled maintenance.
 - **Requested Duration:** Set the length of time that the password should be available.

The default value is two hours. The maximum duration is 365 days. The default and maximum durations are set on the managed account.
 - **Access Request:** For the session type, select **Password**, **RDP Session**, **SSH**, or **Application Session**.
 - **Reason:** Enter a reason for the request. The maximum allowed length is 200 characters.
 - **Ticket System:** Select a ticket system from the list. Ticket systems can be used for cross-reference.
 - **Ticket Number:** Enter a ticket number.



Note: *Reason, Ticket System, and Ticket Number fields may or may not be required, depending upon options configured in the access policy by your Password Safe administrator. Also, if your Password Safe administrator has set a specific ticket system in the access policy, you cannot select a different ticket system with your request.*

5. Click **Submit Request**. An email is sent to the approver if email notification is configured.

Review a Password Request

You can review password requests on the **Requests** page. The list of requests available for review depends on your role. You can review the requests on systems where you are a requester.

1. On the **Requests** page, click the buttons to view all, active, and pending requests.
2. Use the filter setting available on each header to narrow the search. Enter filter criteria in the box.

Approve or Deny a Password Request

When a password request for a system is properly submitted, the associated approvers for that system are notified by email of the pending request. Using the following procedure, an approver can approve or deny the password request:

1. Log in to the Password Safe Web Portal.
2. Select **Approve** and click **Pending**.
3. Click on a pending request.
4. Enter a comment for the approval.
5. Select **Approve** or **Deny**.



Note: An approver will be asked to confirm any denied requests. Once a request is approved, the approver can still deny if the situation warrants.

Retrieve a Password

Passwords approved for release can be displayed at any time (and as often as needed) during the release duration. After the password is approved, an email notification is sent to the requestor's email account. The requestor can then retrieve the password.

1. Click the link to see a window with the date and time the release was approved and any comments made by the approver.
2. Click **Retrieve Password** to display the system account password. The password displays in a separate window. The visibility of the password may be limited, with a timer showing remaining time. The dialog box can be closed before the timeout.
3. To copy the password to the clipboard, click the **Copy** button.
4. Use the password to log in to the system within the password release time period.

Password: *****



Multi-System Checkout

Managed systems can be linked to Active Directory accounts. You can submit a request to these Active Directory accounts and then access the managed systems linked to that account.



Note: Your Password Safe administrator must configure the correct permissions for the managed system to use this feature.

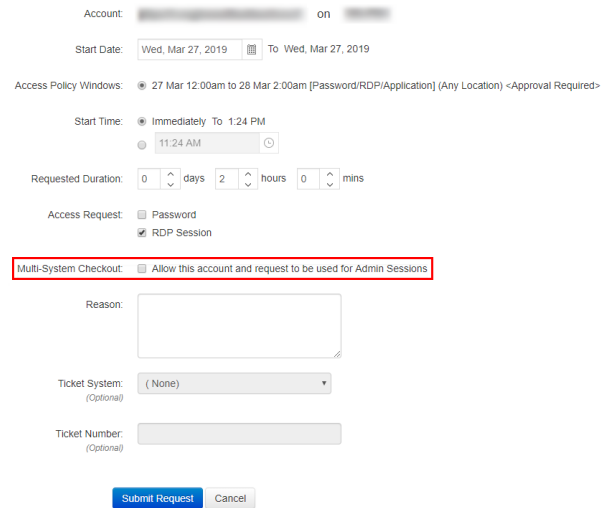
1. Log in to the Password Safe web portal.
2. Click **Menu**, then select **Accounts**.
3. Click the **Domain Linked Accounts** tab for the system type you need to access.
4. Select the account from the list.

5. On the **Requests** page, set the following:

- **Start Date:** Select the start date for the session that corresponds with the access policy.
- **Start Time:** Select **Immediately** to release the password at the current time, , or use the scheduling option to schedule the password release for another time. For example, schedule a release to coincide with scheduled maintenance.
- **Requested Duration:** Set the length of time the password should be available.

The default value is two hours. The maximum duration is 365 days. The default and maximum durations are set on the managed account by your Password Safe administrator.

- **Access Request:** Select the type of access: **Password**, **RDP Session**, **SSH**, or **Application Session**.




Note: The available options will vary depending on the account selected.

- **Multi-System Checkout:** Select this option to use this account and request for **Admin Sessions**. This option is displayed only if the requestor has permissions to use this feature.
- **Reason:** Enter a reason for the request. By default, this field is required, but it can be disabled through BeyondInsight options. The maximum allowed length is 200 characters.
- **Ticket System:** (optional) Select a ticket system from the list. Ticket systems can be used for cross-reference.
- **Ticket Number:** (optional) Enter a ticket number.

6. Click **Submit Request**. An email is sent to the approver if email notification is configured.

Approve a Request for Multi-System Checkout

If the request is approved either automatically or by an approver, the account is available on the **Admin Sessions** page for the duration of the request for which it was approved.

1. On the **Admin Sessions** page, select an account from the **Available Accounts** list.
2. The **Asset/IP** list populates with managed systems that are tied to the account.
3. Select an asset from the **Asset** menu.
4. Once a request is approved, the requestor can then choose to open the session with any computer linked to the approved account regardless of whether or not it was included in the initial request.
5. Click **Connect** to start the RDP or SSH session.

Use the OneClick Feature

A requestor sees the **OneClick (thunderbolt)** button when they log in to Password Safe to make a request. When they open **OneClick**, any access policies that are configured with auto-approve are checked for availability. Clicking the button allows the requestor to choose the duration of the request and connect immediately, as long as they have entered a request which meets the criteria of the access policy. Comprehensive messages are displayed to the requestor if their requests do not meet the requirements configured in the access policy.

Request SSH or RDP Sessions in Password Safe

When configured by your Password Safe administrator, you can request access to a managed system using a remote session. Using the Password Safe request and approval system, you can request remote sessions that use SSH or RDP connection types.

Password Safe acts as a proxy, providing session management to target systems. No passwords are transmitted, allowing inherently secure session management.

Request an RDP Session

1. Log in to the Password Safe web portal.
2. On the **Accounts** page, click the tab for the type of system or application you need to access.
3. Select the account from the list.
4. On the **Requests** page, set the following:
 - **Start Date:** Select the start date for the session that corresponds with the access policy.
 - **Start Time:** Select **Immediately** to start the session at the current time, or click the **Scheduling** button for a future session.
 - **Requested Duration:** Set the length of time that the session should be available. The maximum duration is 365 days. The default and maximum durations are set on the managed account.
 - **Access Request:** Select the session type of **RDP Session**.
 - **RDP Admin Console:** If an administrator has enabled this option in the access policy, you can request a remote session in console mode (`mstsc /admin`). This can be useful if the number of remote sessions is maxed out on the host. An RDP console session allows you to connect without requiring other sessions to disconnect. Running a console session disables certain services and functionality, such as but not limited to:
 - Remote Desktop Services client access licensing
 - Time zone redirection
 - Remote Desktop Connection broker redirection
 - Remote Desktop easy print
 - **Reason:** Enter a reason for the request. By default, this field is required, but it can be disabled through BeyondInsight options. The maximum allowed length is 200 characters.
 - **Ticket System:** (optional) Select a ticket system and enter the ticket number. Ticket systems can be used for cross-reference.



For more information on `mstsc /admin`, please see `mstsc` at <https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/mstsc>.

5. Click **Submit Request**. An email is sent to the approver if email notification is configured.

SSH Direct Connect

Using an SSH client, a user can use the Password Safe Request and Approval system for SSH remote connections. The requester's information, including the **Reason** and the **Request Duration**, are auto-populated with default Password Safe settings.

To access a managed account or application using Direct Connect, the requester has to connect to Password Safe's SSH Proxy using a custom SSH connection string with one of the following formats:

- **For UPN credentials:**

```
<Requester>+<Username@Domain>+<System Name>@<Password Safe>
```

- **For down-level logon names\non-domain credentials:**

```
<Requester>@<Domain\\Username>@<System Name>@<Password Safe>
```

You can override the default SSH port and enter port **4422**. The requester is then prompted to enter their password, which they use to authenticate with Password Safe.

- **For UPN credentials:**

```
ssh -p 4422 <Requester>+<Username@Domain>+<System Name>@<Password Safe>
```

- **For down-level logon names\non-domain credentials:**

```
ssh -p 4422 <Requester>@<Domain\\Username>@<System Name>@<Password Safe>
```

- **For an SSH application:**

```
ssh -p 4422 <Requester>@<Account name>:<Application alias>@<System name>@<Password Safe>
```

Once the requester is authenticated, they are immediately connected to the desired machine.


RDP Direct Connect

You can also use Direct Connect to initiate an RDP session. As the requester, you can access the system without ever viewing the managed account's credentials.

If the requestor is granted approval for RDP sessions, a message displays, stating, *Request requires approval. If the request is not approved within 5 minutes, this connection will close.* After five minutes, the RDP client disconnects, and you can send another connection request. When the request is approved, you are automatically connected.

To use RDP Direct Connect, you must download the RDP file from the Password Safe web portal. This is a one-time download. Each account and system combination requires that you download the unique RDP file associated with it.

1. Log in to the Password Safe web portal.
2. On the **Accounts** page, click the tab for the type of system or application you need to access.
3. Find the account in the list.
4. Click the download arrow.
5. Run the file to establish a connection to the target system.
6. Enter your password that you use to authenticate into Password Safe

Status	Platform	Application	Workgroup	ISA
1 of 1 available	Windows			
1 of 1 available	Windows			Download RDP Direct Connect file



Note: RDP Direct Connect supports only push two-factor authentication. An access-challenge response is not supported.



Note: LDAP users that use the mail account naming attribute cannot use RDP Direct Connect.

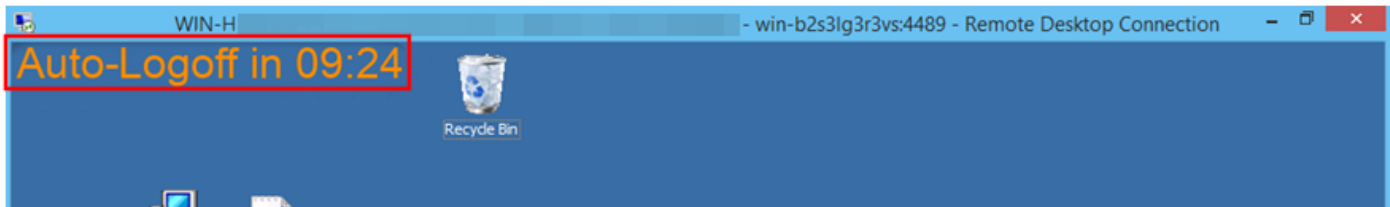
Password Restrictions

- On Windows 2008 and Windows 7, the password cannot exceed 81 characters. If a password is too long, the user cannot log in with the selected account.
- On Windows 2012, the password cannot exceed 127 characters. If a password is too long, the user cannot log in with the selected account.

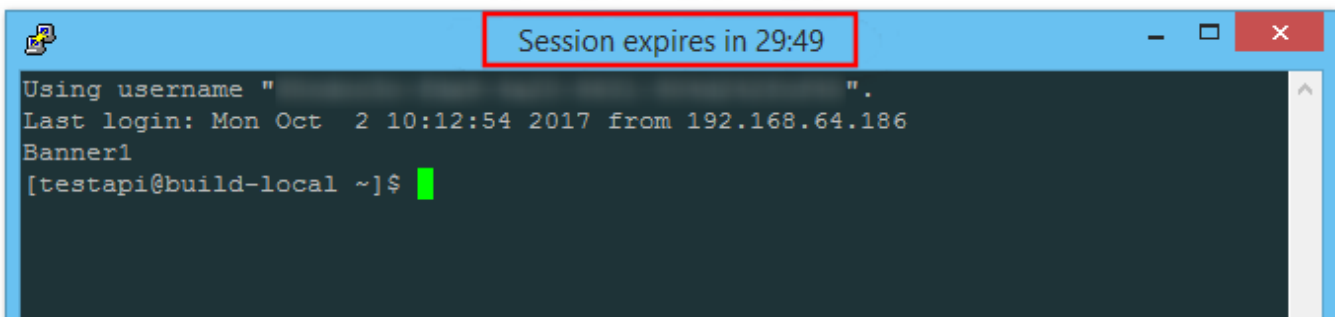
Enforce Session End Time

When a Password Safe administrator creates an access policy, they assign a time frame that permits access to the asset. As part of that policy, the administrator can enforce the end of the session and close the session when the time expires. Sessions display a counter showing when the session will end.

RDP Session



SSH Session



Request Remote Proxy Session

In larger environments, assets you need to access might not be in your region. If configured by your Password Safe administrator, you can select a node associated with another region to proxy these session types:

- Direct Connect sessions
- SSH sessions
- RDP sessions
- Admin sessions

When using OneClick to request a session, click **Open RDP Session**, and then select a node from the list:

Account: **Retina Or** ✕

Requested Duration: Recheck

Access Policy Schedule	Available Until	
AP1	8 Nov 2:26pm	👁️ Retrieve Password 🔌 Open RDP Session

Screen Resolution:

Reason:
(Optional)

Ticket System:
(Optional)
▼
(None)

Ticket Number:
(Optional)

Choose Session Node
✕

na.hostname.com (na.hostname.com)
 ▲▼

Start Session

When requesting a session as a requestor, click **Open SSH Session**, and then select a node from the list:

10/4/2017 4:23 PM	Clark Kent	Approved	Not approved because this account does not require dual-control
-------------------	------------	----------	---

This session may be recorded

Choose Node

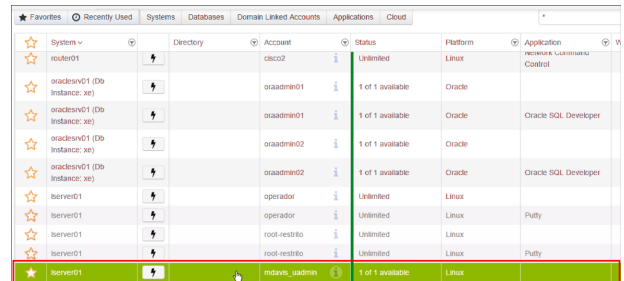
- North America (10.101.23.234)
- United Kingdom (101.239.2.182)

Password Safe Use Cases

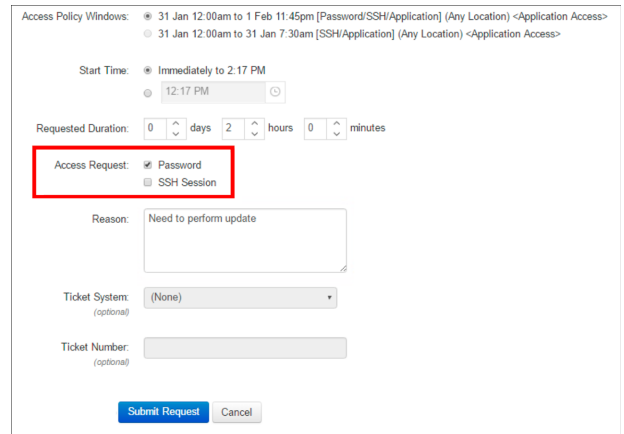
Request Access to a Linux Account - Password Retrieval

In this use case, you log in to the web portal and request access to a privileged account password. The system gives you access to the password after verifying in the policy that you are authorized and do not require approval. If you request the password again, the process repeats. However, you will see that every time, Password Safe gives you a different and unique password to allow proper usage tracking.

1. Log in to the web portal.
2. Scroll to the system **lserver01**, find the **mdavis_uadmin** account, and click to open.
3. Enter a date, time, and duration.
4. Select the **Password** check box and enter a reason for the request.
5. Click **Submit Request**.
6. Depending on your access policy, the request may be auto-approved. If so, you should have an active request immediately available. Otherwise, wait for approval.
7. Select the active request.



System	Directory	Account	Status	Platform	Application
router01		cisco2	Unlimited	Linux	Network Configuration Control
oracledb01 (Db Instance: xe)		oraadmin01	1 of 1 available	Oracle	Oracle SQL Developer
oracledb01 (Db Instance: xe)		oraadmin01	1 of 1 available	Oracle	Oracle SQL Developer
oracledb01 (Db Instance: xe)		oraadmin02	1 of 1 available	Oracle	Oracle SQL Developer
oracledb01 (Db Instance: xe)		oraadmin02	1 of 1 available	Oracle	Oracle SQL Developer
lserver01		operator	Unlimited	Linux	
lserver01		operator	Unlimited	Linux	PuTTY
lserver01		root-resitro	Unlimited	Linux	
lserver01		root-resitro	Unlimited	Linux	PuTTY
lserver01		mdavis_uadmin	1 of 1 available	Linux	



Access Policy Windows: 31 Jan 12:00am to 1 Feb 11:45pm [Password/SSH/Application] (Any Location) <Application Access>
 31 Jan 12:00am to 31 Jan 7:30am [SSH/Application] (Any Location) <Application Access>

Start Time: Immediately to 2:17 PM
 12:17 PM

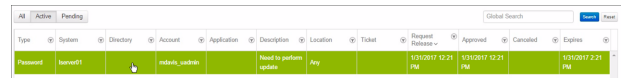
Requested Duration: 0 days 2 hours 0 minutes

Access Request: Password SSH Session

Reason:

Ticket System (optional):

Ticket Number (optional):



Type	System	Directory	Account	Description	Location	Ticket	Request Expires	Approved	Cancelled	Expires
Password	lserver01		mdavis_uadmin	Need to perform update	Any		1/31/2021 12:21 PM	1/31/2021 12:21 PM		1/31/2021 2:21 PM

8. Click **Retrieve Password**.

Request ID: 90

Requested By: **Martha Davis** on 1/31/2017 12:21 PM (2 minutes ago)

Account: **mdavis_admin on lserver01**

Requested Date: 1/31/2017 12:21 PM - 2:21 PM
(Today at 12:21 PM for 2 hours)

Requested Access Type: **Password**

Restricted to Location: **Any**

Reason: **Need to perform update**

Approval History

Approvals Required: 0

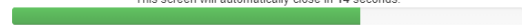
Date	Submitted By	Response	Comment
1/31/2017 12:21 PM	Martha Davis	Approved	Auto-approved because this account does not require dual-control

Check-in Request
Retrieve Password

9. Click the blue reveal password button to view the password, or click the green clipboard button to copy the password.

Password: 👁 📄

This screen will automatically close in 14 seconds.



Close Now

10. Open **PuTTY** on the BeyondInsight host, and open a connection to the **lserver01** host.

PuTTY Configuration

Category:

- [-] Session
 - [-] Logging
 - [-] Terminal
 - [-] Keyboard
 - [-] Bell
 - [-] Features
 - [-] Window
 - [-] Appearance
 - [-] Behaviour
 - [-] Translation
 - [-] Selection
 - [-] Colours
 - [-] Connection
 - [-] Data
 - [-] Proxy
 - [-] Telnet
 - [-] Rlogin
 - [-] SSH
 - [-] Serial

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address) Port

Connection type:
 Raw Telnet Rlogin SSH Serial

Load, save or delete a stored session

Saved Sessions

Default Settings

Direct Connect - admin01

Direct Connect - router01

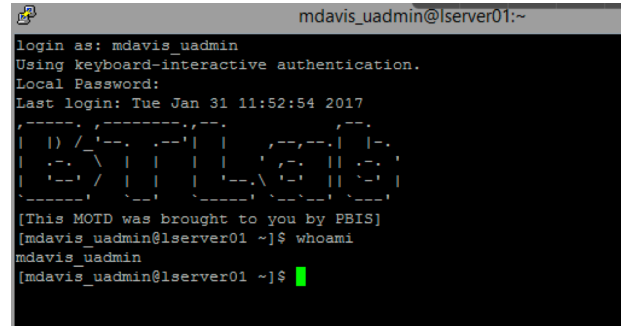
lserver01

Load Save Delete

Close window on exit:
 Always Never Only on clean exit

About Help Open Cancel

11. Log in to **lserver01** as **mdavis_uadmin** and right-click to paste the password from the clipboard. You will be logged in directly.
12. When finished, close the SSH session, and click the **Check-in Request** to release the **mdavis_uadmin** account.



Request RDP Access to a Windows Account - Session Management

In this use case, you log in to the web portal and request access to a privileged account. You choose RDP to provide a proxy session, allowing you to access the account without requiring direct password retrieval.

1. Log in to the web portal.
2. Scroll to the system **dc01** and find the **helpdesk** account that does not have an application configured, then click to open.
3. Enter a date, time, and duration.
4. Check the **RDP Session** box and enter a reason for the request.
5. Click **Submit Request**.
6. Depending on your access policy, the request may be auto-approved. If so, you should have an active request immediately available. Otherwise, wait for approval.
7. Select the active request.

System	Directory	Account	Status	Platform	Application
dc01	btlab-btu-cloud	helpdesk	Unlimited	Windows	
dc01	btlab-btu-cloud	helpdesk	Unlimited	Windows	AD Users and Computers
dc01	btlab-btu-cloud	helpdesk	Unlimited	Windows	DNS Management
dc01	btlab-btu-cloud	helpdesk	Unlimited	Windows	Group Policy Mgmt
dc01	btlab-btu-cloud	helpdesk	Unlimited	Windows	Event Viewer
dc01	btlab-btu-cloud	helpdesk	Unlimited	Windows	IIS MANAGEMENT
bd01 (Db Instance: default)		sa2	1 of 1 available	MS SQL Server	
bd01 (Db Instance: default)		sa2	1 of 1 available	MS SQL Server	SQL Management Studio
app01		administrator	Unlimited	Windows	
app01	btlab-btu-cloud	exchangeadmin	Unlimited	Windows	

Access Policy Windows: 31 Jan 12:00am to 7 Feb 11:45pm [Password/RDP/Application] (Any Location) -Application Access->
 31 Jan 12:00am to 31 Jan 7:30am [RDP/Application] (Any Location) -Application Access->

Start Time: Immediately to 4:47 PM
 2:47 PM

Requested Duration: 0 days 2 hours 0 minutes

Access Request: Password RDP Session

Multi-System Checkout: Allow this account and request to be used for Admin Sessions

Reason:

Ticket System: (None)

Ticket Number: (optional)

8. Select a **Screen Resolution**.
9. Click **Open RDP Session** to download an RDP connection file.

Account: **btlab.btu.cloud\helpdesk on dc01**

Requested Date: 1/31/2017 2:17 PM - 4:17 PM
(Today at 2:17 PM for 2 hours)

Requested Access Type: **RDP**

Restricted to Location: **Any**

Reason: **test**

Screen Resolution: **1024x768**

Smart Sizing:

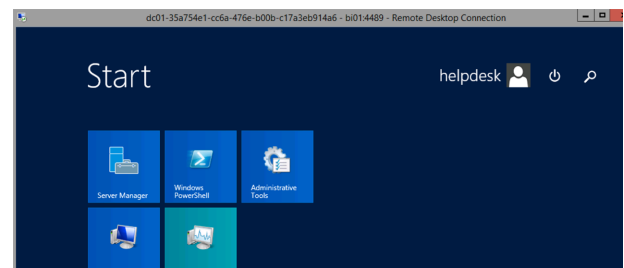
Approval History

Approvals Required: 0

Date	Submitted By	Response	Comment
1/31/2017 2:17 PM	Martha Davis	Approved	Auto-approved because this account does not require dual-control

Check-in Request **Open RDP Session**

10. Run the file to directly access **dc01** as the helpdesk account, using Password Safe as a proxy.



11. When finished, close the RDP window and click **Check-in Request** to release the helpdesk account.


Approval History

Approvals Required: 0

Date	Submitted By	Response	Comment
1/31/2017 2:17 PM	Martha Davis	Approved	Auto-approved because this account does not require dual-control

Check-in Request **Open RDP Session**

This session may be recorded.

 **Note:** The session terminates when you click on **Check-in Request**, even if you leave the RDP session open.

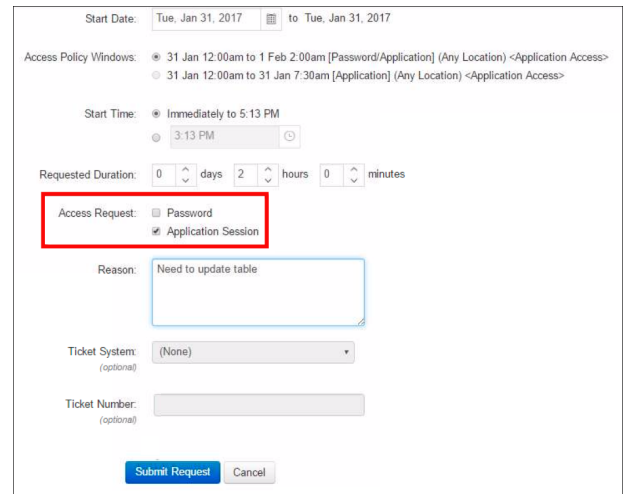
Request Access to a Microsoft SQL Account - Remote Applications

In this use case, you request access to a Microsoft SQL Server. However, you need the SQL Server privileged account just to access Microsoft SQL Server Management Studio. You do not need the password or a full RDP session.

1. Log in to the web portal.
2. Click the **Databases** tab.
3. Scroll to the system **bi01**, find the **sa2** account associated with **SQL Management Studio**, and click to open.

System	Directory	Account	Status	Platform	Application	Workgroup
msd01 (DB Instance - sa1)		msd01	1 of 1 available	Oracle		
msd01 (DB Instance - sa)		msd01	1 of 1 available	Oracle	Oracle SQL Developer	
msd01 (DB Instance - sa)		msd02	1 of 1 available	Oracle		
msd01 (DB Instance - sa)		msd02	1 of 1 available	Oracle	Oracle SQL Developer	
msd1 (DB Instance - default)		sa2	1 of 1 available	MS SQL Server	SQL Management Studio	

4. Enter a date, time, and duration.
5. Select the **Application Session** check box and enter a reason for the request.
6. Click **Submit Request**.



Start Date: Tue, Jan 31, 2017 to Tue, Jan 31, 2017

Access Policy Windows:

- 31 Jan 12:00am to 1 Feb 2:00am [Password/Application] (Any Location) <Application Access>
- 31 Jan 12:00am to 31 Jan 7:30am [Application] (Any Location) <Application Access>

Start Time: Immediately to 5:13 PM
 3:13 PM

Requested Duration: 0 days 2 hours 0 minutes

Access Request: Password
 Application Session

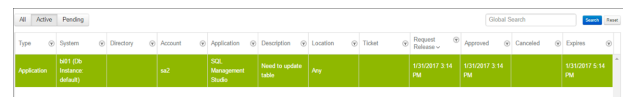
Reason:

Ticket System: (None)

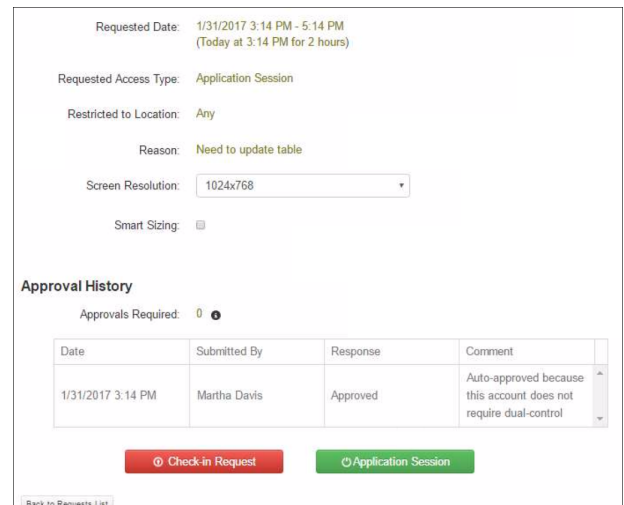
Ticket Number: (optional)

Submit Request Cancel

7. Depending on your access policy, the request may be auto-approved. If so, you should have an active request immediately available. Otherwise, wait for approval.
8. Select the active request.
9. Select a **Screen Resolution**.
10. Click **Application Session** to download an RDP connection file.



Type	System	Directory	Account	Application	Description	Location	Ticket	Request Release	Approved	Cancelled	Expires
Application	sa2	sa2	SQL Management Studio	Need to update table	Any		1/31/2017 3:14 PM	1/31/2017 3:14 PM			1/31/2017 5:14 PM



Requested Date: 1/31/2017 3:14 PM - 5:14 PM (Today at 3:14 PM for 2 hours)

Requested Access Type: Application Session

Restricted to Location: Any

Reason: Need to update table

Screen Resolution: 1024x768

Smart Sizing:

Approval History

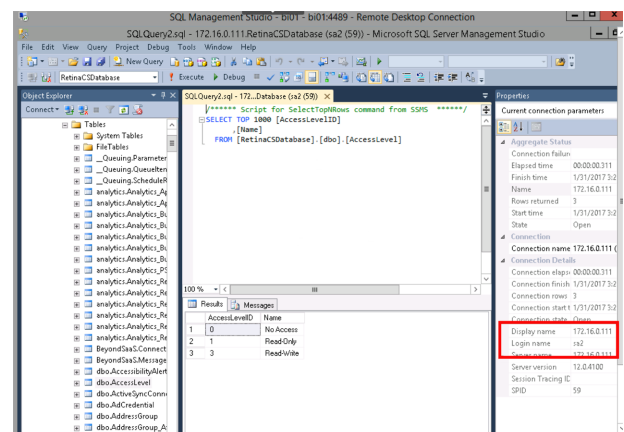
Approvals Required: 0

Date	Submitted By	Response	Comment
1/31/2017 3:14 PM	Martha Davis	Approved	Auto-approved because this account does not require dual-control

Check-in Request **Application Session**

[Back to Requests List](#)

11. Run the file to connect to the **bi01** host, with your connection limited to using SQL Server Management Studio only.
12. When finished, close the application session, and click the **Check-in Request** to release the **sa2** account.



SQL Query2.sql - 172.16.0.111 RetinaCSDatabase (sa2 (59)) - Microsoft SQL Server Management Studio

Script for SelectTopRows command from SSRS *****

```
SELECT TOP 1000 [AccessLevelID]
FROM [RetinaCSDatabase].[dbo].[AccessLevel]
```

Current connection parameters:

- Aggregate Status
- Elapsed time: 00:00:00.311
- Fetch time: 1/31/2017 3:2
- Name: 172.16.0.111
- Rows returned: 3
- Start time: 1/31/2017 3:2
- Date
- Connection
- Connection name: 172.16.0.111
- Connection details
- Connection elapsed: 00:00:00.311
- Connection finish: 1/31/2017 3:2
- Connection rows: 3
- Connection start: 1/31/2017 3:2
- Connection type: Remote Desktop Connection
- Server version: 12.0.4100
- Session Tracking ID: 59
- SPID: 59



Tip: Delegating access based on applications allows you to restrict what certain users can do in your environment. For instance, instead of granting a semi-skilled user a full session to a critical server, you may want to delegate access only to the applications they need to do their job. This helps to avoid incidents caused by someone restarting or deleting something in error.

Use Secrets Safe

The Secrets Safe feature allows you to securely store secrets owned by developers and small groups in a controlled environment that you can audit. Password Safe administrators can assign groups in BeyondInsight to teams, in which each team has its own isolated store where users can secure secrets used within that team. The creator of the secret becomes the owner and can assign ownership of the secret to the entire team or one or more individual members. Password Safe administrators and secret owners can manage secret ownership, edit secrets, and delete secrets, while team members may only view and retrieve secrets. Team members can create a folder structure to organize their secrets. Secrets can be found and accessed easily using search and filtering options.

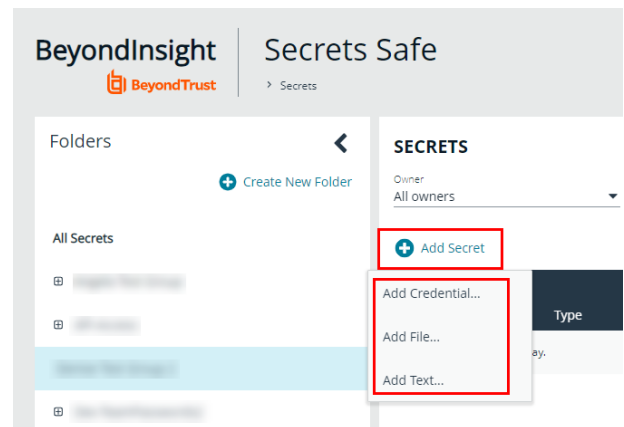
Create a Secret in Secrets Safe

You can create secrets in the parent folder for any of your teams or in any of your team's subfolders. The user who creates the secret is its owner and may change its folder at any time after it has been created.

1. On the left navigation pane in the console, click **Secrets Safe**.
2. From the **Folders** pane, select a folder, and then click **Add Secret**.



Note: Secrets Safe supports 3 different types of secrets: credential, text, and file. There are no restrictions on file type, however files must be 5MB or less.



3. Select secret type:

- If **Add Credential** is selected, in the **Create New Secret** pane:
 - Enter a **Title**, **Description**, and **Username**.
 - Set the password:
 - Select **Manual Input** to manually enter a password.
 - Select **Auto Generate** and select a **Password Policy** from the list to have the password created based on the defined policy.
 - Click **Generate Password**.
 - Add a note if you require additional information to display for this credential other than its description. You can add **Notes** as a column when viewing the list of credentials in the grid, and you can also filter the list by **Notes**.
 - Click **Manage Ownership** if you wish to assign ownership to individual team members or to the entire team.
 - Click **Create Secret**.
- Or if **Add File** is selected, in the **Create New Secret** pane:
 - Enter a **Title** and **Description**.
 - Upload the file by dragging to the pane, or click on the upload file icon and navigate to the file.
 - Click **Manage Ownership** if you wish to assign ownership to individual team members or to the entire team.
 - Click **Create Secret**.
- Or if **Add Text** is selected, in the **Create New Secret** pane:
 - Enter a **Title** and **Description**.
 - Enter the body of the text.
 - Add a note if you require additional information to display for this text other than its description. You can add **Notes** as a column when viewing the list of texts in the grid, and you can also filter the list by **Notes**.
 - Click **Manage Ownership** if you wish to assign ownership to individual team members or to the entire team.
 - Click **Create Secret**.

Create New Secret
➤

This secret will be owned by you. You may change its folder at any time after it has been created.

Folder
New Group Test

Title
Test Credential ✕

Description

Username

Set Password ⓘ

Manual Input Auto Generate

Password Policy
Default Password Policy ▼

GENERATE PASSWORD

Password 🔒

Notes

Owner(s)

[Manage Ownership](#)

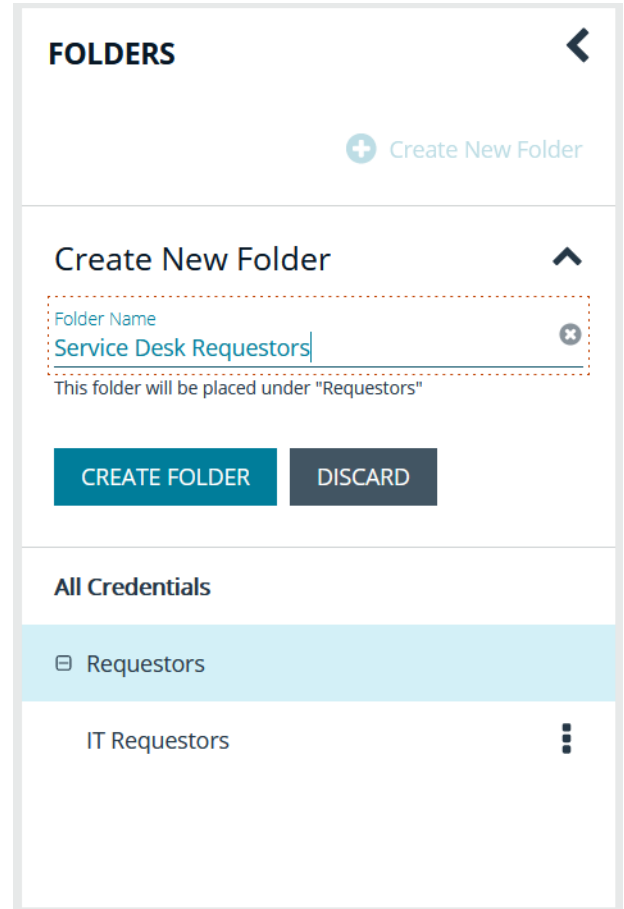
CREATE SECRET
DISCARD

Manage Folders in Secrets Safe


You can organize your team secrets into subfolders under the parent team folder to make locating a secret more efficient.


1. On the left navigation pane in the console, click **Secrets Safe**.

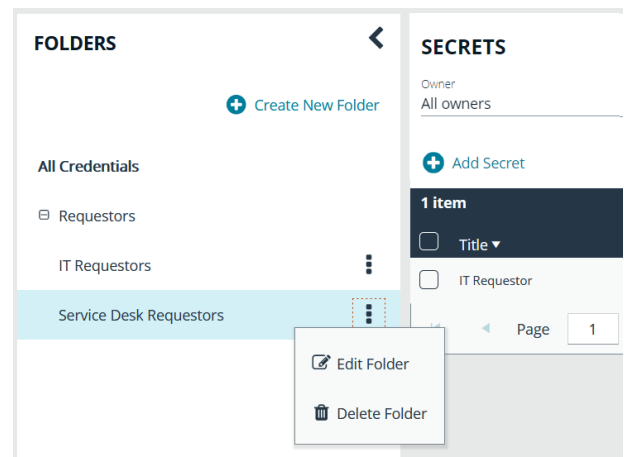
2. To create a new folder, select the parent folder for the team or one of its existing subfolders, and then click **Create New Folder**.
3. Enter a name for the folder, and then click **Create Folder**.



4. The new folder is listed under the folder you selected when creating it. To edit the folder name or to delete the folder, select the folder, click the vertical ellipsis, and then select **Edit Folder** or **Delete Folder**.

 **Note:** You cannot delete parent team folders. Only subfolders may be deleted. Also, if you do not own all of the secrets in a subfolder, you are not able to delete it.

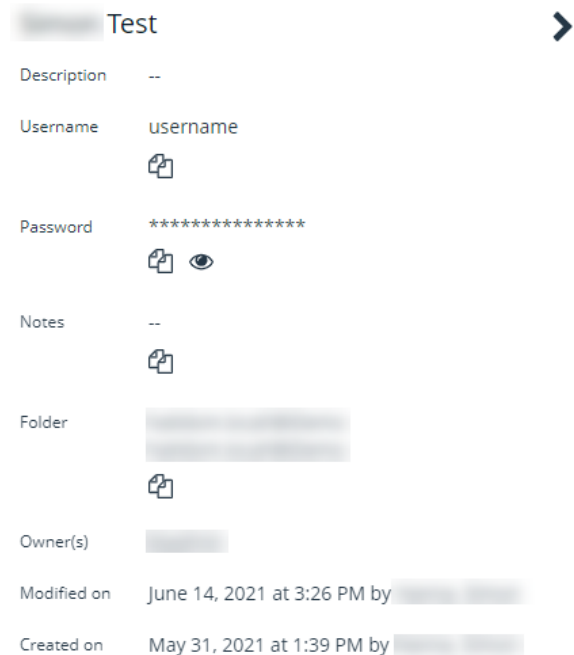
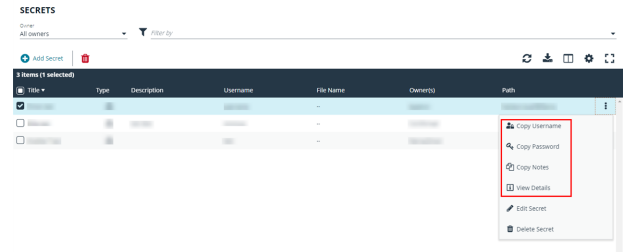
 For more information on how to move a credential to a new subfolder, please see *"Edit and Delete a Secret in Secrets Safe"* on page 24



View and Copy a Secret in Secrets Safe

You can view details for your team's secrets, such as who owns the secret, when the secret was created and modified, and the folder path for the secret. You can also copy the username and password for a team secret so you can use it.

1. On the left navigation pane in the console, click **Secrets Safe**.
2. From the **Folders** pane, select a folder, and then select a secret.
3. Click the vertical ellipsis for the secret.
4. Each secret type has specific options and actions:
 - For credential-type secrets, you can **Copy Username**, **Copy Password**, and **Copy Notes**.
 - For text-type secrets, you can **Copy Text** and **Copy Notes**.
 - For file-type secrets, you can **Download File** and **Copy Notes**.
5. To view the details for any secret, select **View Details** from the dropdown menu.
6. To view the secret password, click the eye icon in the secret details pane.
7. To copy the secret password, click the copy icon in the secret details pane.

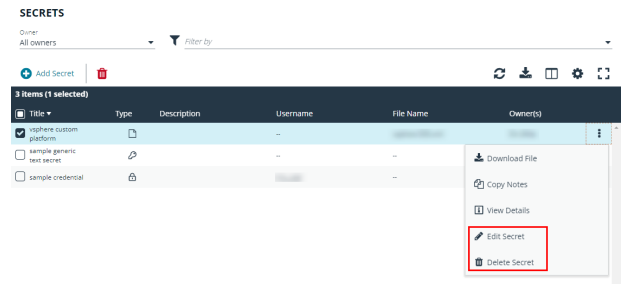


Edit and Delete a Secret in Secrets Safe

Secret owners can edit the properties and manage ownership for secrets they own, as well as delete secrets they own. Password Safe administrators can edit the properties, manage ownership, and delete all secrets in Secrets Safe.

1. On the left navigation pane in the console, click **Secrets Safe**.
2. From the **Folders** pane, select a folder, and then select a secret.
3. Click the vertical ellipsis for the secret.

4. To delete a secret, select **Delete Secret**, and then click **Delete** on the confirmation message.
5. To edit a secret, select **Edit Secret**.
6. Modify the properties for the secret as required.
7. To manage the ownership of the secret, click **Manage Ownership**.



Edit Sample Credential

Title
sample credential

Description

Username

Set Password ?

Manual Input Auto Generate

Password
.....

Notes
ipsum lorem

Folder

Owner(s)

[Manage Ownership](#)

UPDATE SECRET **DISCARD CHANGES**

- Enable the **Assign Ownership to Entire Team** option to assign all members of the team as owners of the secret. When new members are added to the team, they are automatically assigned as owners of the secret.
- Alternatively, select individual team members as owners.
- Click **Apply Ownership Settings**.

Manage Owners Of "[REDACTED]" ✕

Assign ownership of the secret to the team or to one or more individual members.

Assign Ownership to Entire Team ?

Assign Members

SHOW ALL

SHOW SELECTED

5 items (10 selected)

Members ▾

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

1 - 5 of 5 items

APPLY OWNERSHIP SETTINGS **DISCARD CHANGES**

8. Click **Update Secrets** once you have made your edits.