

IBM Security Verify Privilege On-Premises
Version 10.9

End User Guide

Contents

Glossary	1
Logging In.....	2
Logging in with an Active Directory account	2
Logging in with a local account.....	2
Dashboard	3
Advanced View.....	3
Basic View	3
Creating a Secret.....	5
Advanced View.....	5
Basic View	6
Viewing a Secret	7
Icon definitions	7
Common Configuration Options	7
Editing a Secret.....	9
Deleting a Secret.....	10
Sharing a Secret.....	11

Last updated : 22 September 2020

Glossary

Throughout this user guide, certain terms are used to refer to specific features within Privilege Vault:

Secret

A piece of information that is stored and managed within Privilege Vault is referred to as a Secret. Secrets are derived from Secret templates. Typical Secrets include, but are not limited to, privileged passwords on routers, servers, applications, and devices. Files can also be stored in Secrets, allowing for storage of private key files, SSL certificates, license keys, network documentation, Microsoft Word, or Excel documents and more.

Secret Template

Secret templates are used to create Secrets and allow customization of the format and content of Secrets to meet company needs and standards. Examples include: Local Administrator Account, SQL Server Account, Oracle Account, Credit Card, and Web Password. Templates can contain passwords, usernames, notes, uploaded files, and drop-down list values. New Secret templates can be created, and all existing templates can be modified.

Role-based Security

Privilege Vault uses role-based access control, which sets strict, granular permissions for each user. All features in Privilege Vault are made available to users based on permissions, which collectively make up roles.

Unlimited Administration Mode

The emergency, "break-the-glass" feature. When this mode is enabled, your Privilege Vault administrators can access all content within the system, regardless of explicit permissions. Access to Unlimited Administration Mode is controlled by using role permissions.

Logging In

Depending on how your administrators configured Privilege Vault, you will log in with either your Active Directory account OR a local account.

Logging in with an Active Directory account

On the login screen, enter your:

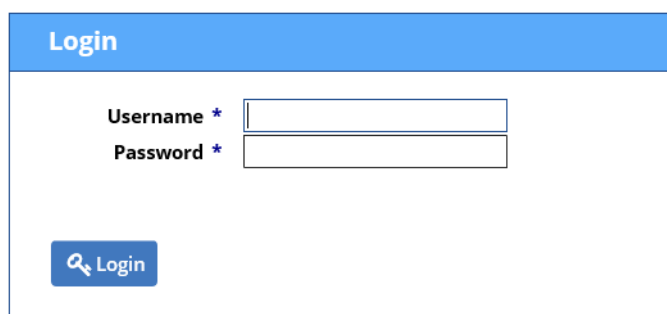
1. Active Directory username
2. Active Directory password
3. Select the appropriate domain from the list.

Logging in with a local account

If your administrators configured local account logins for Privilege Vault, they provide you with a username and a temporary password for your first login. On the login screen, enter:

1. Username
2. Temporary password, and
3. From the Domain dropdown, select “**Local**”.

After you log in with your local account for the first time, you will be prompted to change your password immediately.



The screenshot shows a login interface with a blue header bar containing the word "Login". Below the header, there are two input fields: "Username *" and "Password *". The "Username *" field is a simple text box, while the "Password *" field is a text box with a small eye icon on the right side, indicating a password field. Below these fields is a blue button with a magnifying glass icon and the text "Login".

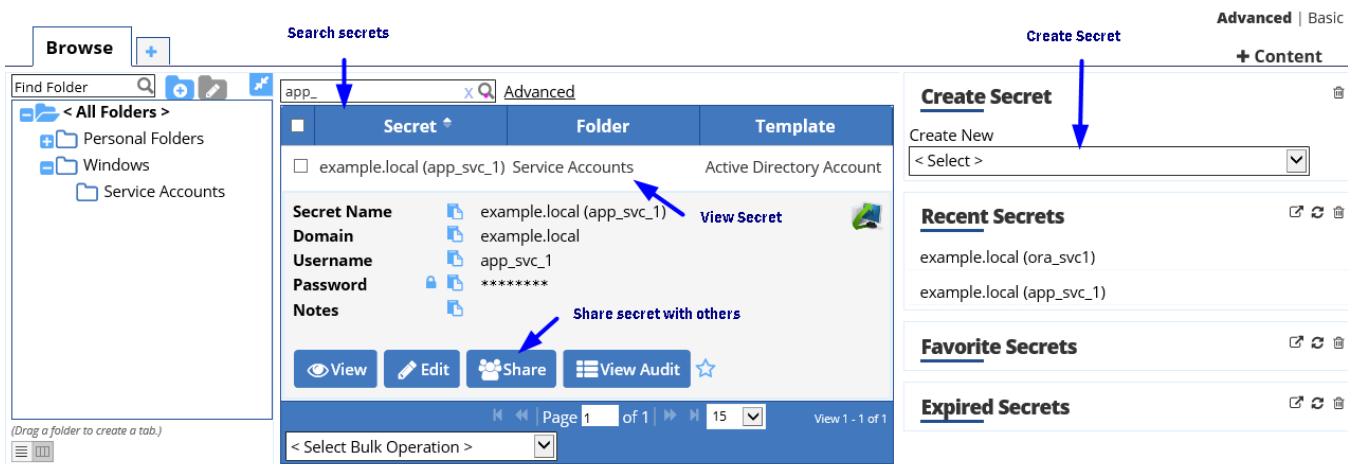
Dashboard

Dashboard is the main screen for searching and viewing Secrets. Two Dashboard views are available, Advanced and Basic.

Widgets or Options	Basic View	Advanced View
Create New Secret	✓	✓
Recent Secrets	✓	✓
Search Bar	✓	✓
Expired Secrets		✓
Favorite Secrets		✓
Out of Sync Secrets		✓
Reports		✓

Advanced View

Viewing the Advanced Dashboard requires the **View Advanced Dashboard** role permission. If you have this permission, you can view the Basic dashboard.



See a visual demonstration of the [Advanced Dashboard here](#).

Basic View

A user without the “View Advanced Dashboard” permission is limited to the Basic view, which does not include use of any widgets aside from Recent Secrets.

Secrets

Advanced | **Basic**

Secrets		+ Create New	
Adobe Creative Suite License <i>Lois Lane</i>		Box <i>Lois Lane</i>	 Login
Eventbrite <i>Lois Lane</i>	 Login	example.local (app_svc_1) <i>Service Accounts</i>	 Login
example.local (ora_svc1) <i>Service Accounts</i>	 Login	Gmail <i>Lois Lane</i>	 Login
Happy Bank pin code		Twitter <i>Lois Lane</i>	

Recent Secrets

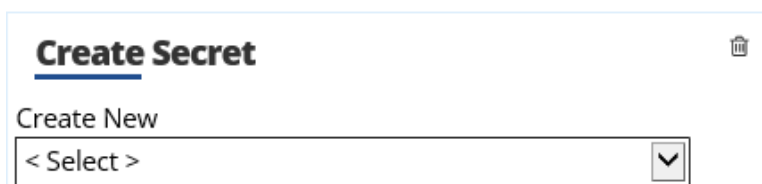
Twitter <i>Lois Lane</i>	 Login
Box <i>Lois Lane</i>	 Login
Gmail <i>Lois Lane</i>	 Login
Adobe Creative Suite License <i>Lois Lane</i>	

Creating a Secret

Advanced View

Viewing the Advanced Dashboard requires the **View Advanced Dashboard** role permission.

1. From Dashboard, find the **Create Secret** widget.



2. Select a template from the drop-down menu. For this example, use a **Web Password**.
3. Enter the information for your Secret in the fields (fields with an asterisk * are required).
4. If you want to organize the Secret into a specific folder, click the folder name that is listed, and select the desired folder. Otherwise, click **Clear** to store the Secret at the root level.
5. Click **Save** to save your settings.

(Other save options)

6. Click **Save and Share** to share the Secret with another user or group.
7. Click **Save and Add New** to save this Secret and create another Secret with the same template.

New

General

Secret Template	Web Password
Secret Name	* Green Example Mail Account (resumes) ×
URL	* www.gmail.com
UserName	* jkecompanyjobs@gmail.com
Password	* •••••••• Generate Strong ✓
Notes	This inbox is for resume submissions.
Folder	📁 \HR Clear
Inherit Secret Policy	<input checked="" type="checkbox"/>
Secret Policy	< No Policy >

Save Save and Share + Save and Add New × Cancel

Basic View

1. From Dashboard, find the **Create New** button.
2. Select a template from the drop-down menu. For this example, use a **Web Password**.
3. Enter the information for your Secret in the fields (fields with an asterisk * are required).
4. If you want to organize the Secret into a specific folder, click the folder name that is listed, and select the desired folder. Otherwise, click **Clear** to store the Secret at the root level.
5. Click **Save** to save your settings.

(Other save options)


6. Click **Save and Share** to share the Secret with another user or group.
7. Click **Save and Add New** to save this Secret and create another Secret with the same template.



Viewing a Secret



To view the information that is contained in a Secret (such as password or special notes), navigate to the Home page (your dashboard). From there, click the Secret name, then click “View”.




Green Example Mail Account (resumes) (Web Password)


General | Personalize | Expiration | Launcher | Security

Secret Name  Green Example Mail Account (resumes)


URL   www.gmail.com

UserName   jkecompanyjobs@gmail.com

Password    *****

Notes  This inbox is for resume submissions.


Status Active








Folder  \HR

Inherit Secret Policy Yes

Secret Policy < No Policy >





Favorite?


Web Password Filler
[How do I use the Web Password Filler?](#)

Icon definitions

The icons perform the following operations:

- Lock**  Unmask a field until the cursor is moved away from the icon.
- History**  Display the history of changes to the field.
- Copy**  Copy the field to the clipboard. You might need an add-on for this feature to function.
- NATO**  Display the field by using the NATO phonetic alphabet. This phonetic alphabet is helpful when you communicate a password over the phone.

Common Configuration Options

The following configuration options are common to every Secret:

- Folder** Folder location of the Secret. The Secret inherits permissions of this folder that depends on the Default Secret Permissions setting in the Privilege Vault Configuration options.

Favorite

Click the star from the Dashboard or check this box on the Secret View page to mark the Secret as a favorite. It will then display in the Favorite Secrets widget.



Edit the Secret fields.



Create a duplicate copy of the Secret that can be renamed and modified.



Configure the sharing settings, or permissions, for the Secret.



View the Secret audit log to see which users that have accessed the Secret.



Delete the Secret.



Change which template is being used to store and display information in this Secret.

Editing a Secret

To edit a Secret, navigate to its Secret View page and click **Edit**. All fields become editable. For passwords, you can create a random, unique, password by clicking **Generate**.

Note: Editing passwords in a secret template does not update the password within accounts that are managed outside of Privilege Vault.

Green Example Mail Account (resumes) (Web Password)

General	Personalize	Expiration	Launcher	Security
Secret Name	* Green Example Mail Account (resumes) ✕			
URL	* www.gmail.com			
UserName	* jkecompanyjobs@gmail.com			
Password	* ●●●●●●●●			* Generate
Notes	This inbox is for resume submissions.			
Folder	📁 \HR Clear			
Inherit Secret Policy	<input checked="" type="checkbox"/>			
Secret Policy	< No Policy >			
📁 Save ✕ Cancel				

Deleting a Secret

To delete a Secret, navigate to the Secret View page and click **Delete**.

Sharing a Secret

Sharing passwords is crucial for collaborative teams. Due to the sensitive nature of sharing secure information, Privilege Vault takes all necessary security measures to ensure that shared passwords are tracked and protected.

You can choose from four permission levels when you share Secrets with another user or group:

- View** Allows the user to see all Secret data (fields – user name, password, and so on) and metadata (permissions, auditing, history, security settings, and so on).
- Edit** Allows the user to edit the Secret data (user name, password, and so on). Also allows users to move the Secret to another folder unless Inherit Permissions from Folder is turned on, in which case the user needs Owner permissions to move the Secret.
- List** Allows the user to see the secret in a list (such as a list returned by running a search) but not to view any more details about a Secret or edit it.
- Owner** Allows the user to change all the Secret metadata (permissions, security settings, and so on).