IBM Security Verify Privilege On-Premises Version 10.9

IBM Security Verify Privilege Vault

User Guide

IBM

Contents

Getting Started

Installation

IBM Security Verify Privilege Vault is distributed as an .msi (setup.exe) which installs the web application. A compressed file option is also available if needed but it is not suggested as the setup.exe is much easier. To install IBM Security Verify Privilege Vault, simply run the setup.exe. For more information on setting up prerequisites (IIS, ASP.NET, and connecting to Microsoft SQL Server), see the Installation Guide.

Terminology

Throughout this user guide, certain terms are used to refer to specific features or concepts within IBM Security Verify Privilege Vault:

Administrator
Access to features within IBM Security Verify Privilege Vault is controlled by using user roles. Administrator is a default role that comes pre-configured with IBM Security Verify Privilege Vault. This role can be customized to have different permissions. In this guide, 'administrator' is used when you refer to users who manage the system and have control over global security and configuration settings. Administrators in IBM Security Verify Privilege Vault do not automatically have access to all data stored in the system – access to data is still controlled by explicit permissions on that data.

Secret
A piece of information that is stored and managed within IBM Security Verify 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
IBM Security Verify Privilege Vault uses role-based access control, which can set strict, granular permissions for each user. All features in IBM Security Verify 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, administrators can access all content within the system, regardless of explicit permissions. Access to Unlimited Administration Mode is controlled by using role permissions.

Remote Password Changing
IBM Security Verify Privilege Vault can automatically change passwords on remote devices and various platforms, including the following items: Windows accounts, various database logins, Active Directory accounts, UNIX/Linux/Mac accounts (including root passwords), network appliances, devices, and more.

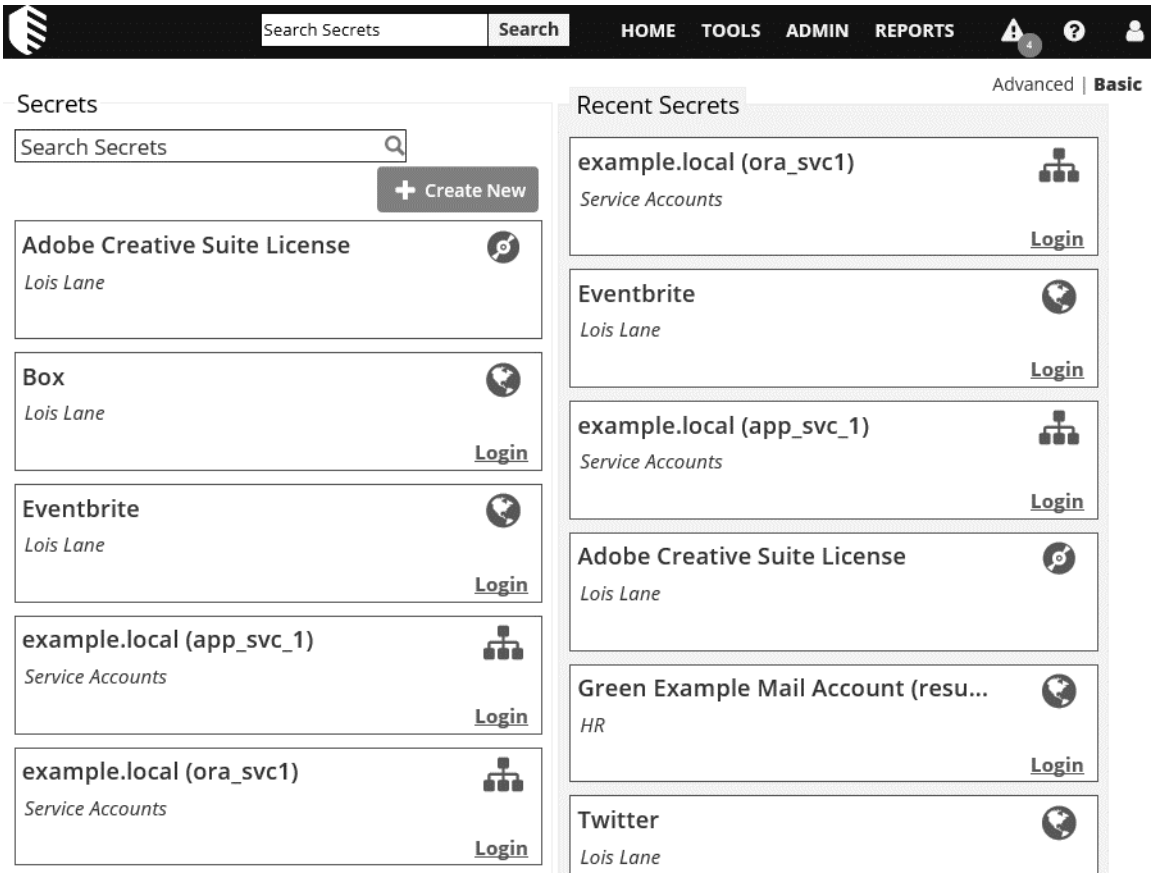
Dashboard

Dashboard is the main screen for searching and viewing Secrets.

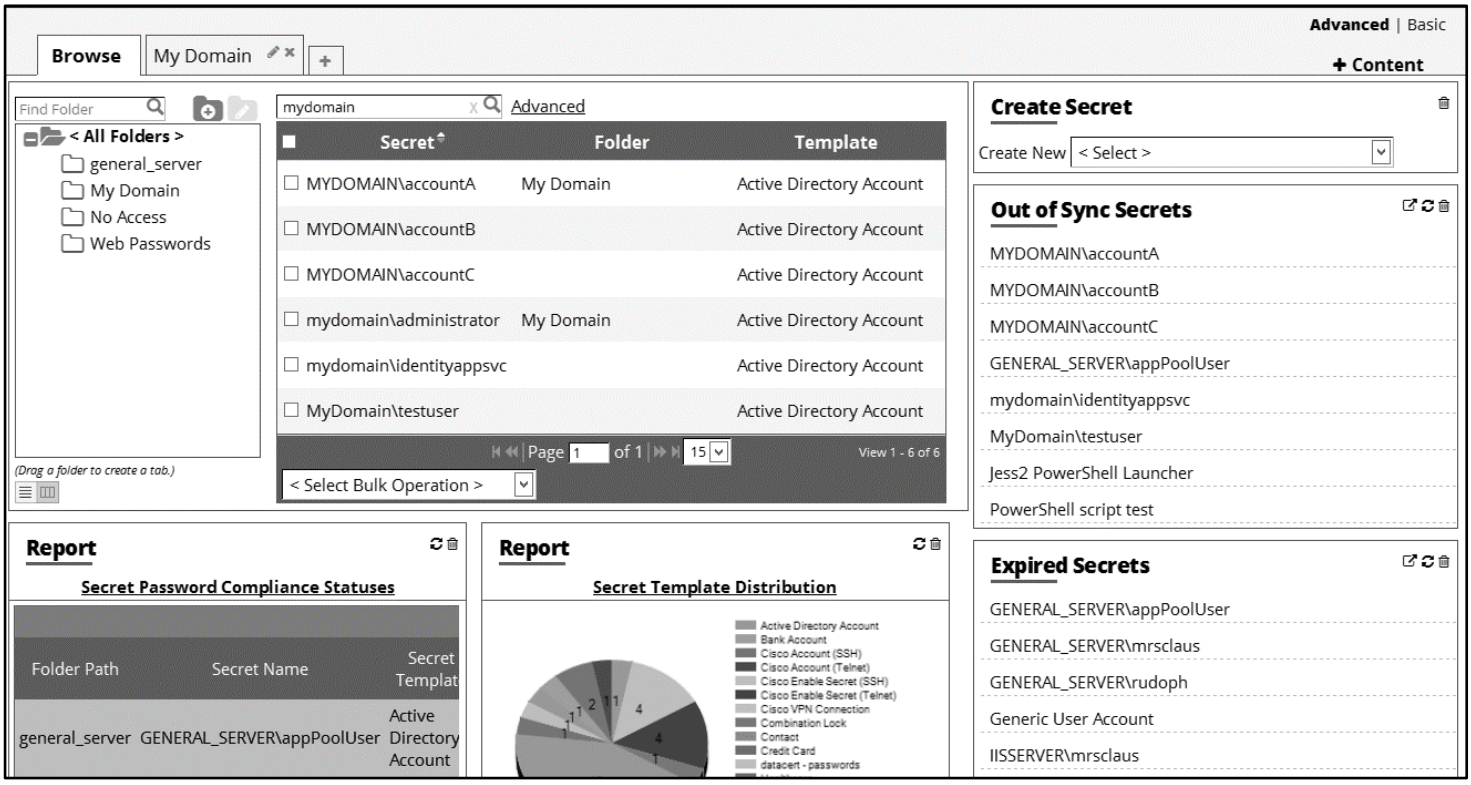
Advanced and Basic Views

An alternate Dashboard view is available called Basic Dashboard. Viewing the Advanced Dashboard requires the role permission View Advanced Dashboard. A role that is called Basic User is included by default and contains the same role permissions as the default User role, except for the View Advanced Dashboard permission. A user that has the View Advanced Dashboard permission can switch between the two views by clicking **Advanced** or **Basic** at the upper-right corner of Dashboard. A user without this permission is restricted to the Basic view, which does not include use of any widgets aside from Recent Secrets.

Basic Dashboard



Advanced Dashboard



Browse Tab

The Browse tab is the only tab that new users see. By default, the Browse tab contains the Search/Browse, Favorite Secrets, Expired Secrets, Create New Secret and Recent Secrets widgets. All widgets except the Search/Browse widget can be added or removed from this tab. The Browse tab cannot be deleted or renamed, but can be moved in the tab order.

Search / Browse Widget

This widget can be used to limit the Secret search results to a particular folder and its subfolders. The Browse tab will always contain a Search/Browse widget based on the < All Folders > root folder.

Create

This widget is created by creating a new custom tab. Only one Search/Browse widget can be present per tab, and they cannot be added to pre-existing tabs.

Delete

Search/Browse widgets can be deleted from custom tabs, but cannot be removed from the Browse tab.

Search

Secret search results can be filtered by selecting a folder on the left, either by clicking it or using the search field above the folder tree. On the right side of the widget, Secrets can be filtered further by specifying search

criteria in the top textbox. The Advanced section allows filtering by Secret template and status and the option to include Secrets that are contained in subfolders. Advanced criteria only remain in effect while those options are expanded (visible).

View and Manage

Secrets that are listed in the results grid can be managed or viewed based on a user's permissions. To view a Secret, click the row and it expands to display. Some of the features available include the copying and unmasking of passwords, by using the launcher, and viewing other pertinent details.

Customize

More columns can be displayed on the grid. This data can be either metadata pertaining to the Secret or Secret template fields that are set to be available for exposure on Dashboard. See Using the Secret template Designer section for further details. To select more columns to display, click the Advanced link and then the Column Selection link. The following metadata fields can be displayed:

- Days until Expiration
- Double Lock
- Hide Password
- Requires Approval
- Requires Comment
- Checkout Enabled
- Is Checked Out
- Expiration Field Changed
- Deleted
- Created
- Inherit Permissions

Search/Browse widgets cannot be rearranged. These widgets always remain in the upper left region of the tab.

Widgets

Widgets are the basis of functionality for Dashboard. All widgets except for the Search/Browse widget share similar UI functions. Widgets can be created, deleted, and rearranged on a per-user basis.

Create Secret

This widget is used to create new Secrets. From the Create New drop-down list, select the Secret template that you want to use. The New Secret page is displayed. See the Creating a Secret section for the details on how to use this screen.

Expired Secrets

Displays Secrets that are expired.

Favorite Secrets

Displays Secrets that are marked as Favorites.

Out-Of-Sync Secrets

Displays Secrets that are out-of-sync, meaning that Heartbeat and/or Remote Password Changing have failed.

Recent Secrets

Displays the Secrets that have been viewed most recently.

Report

Displays a report. Click Create New to select a report from the drop-down menu. One report can be displayed per widget. Click the title of the report to navigate to the Report View page. For further details, see the Reporting in IBM Security Verify Privilege Vault section.

Managing Widgets

The following operations can be performed to manage widgets:

Add Expand the Content area at the upper-left corner of the Dashboard and drag a widget name to the content area below.

Delete click the  icon at the top of the widget.

Refresh click the  icon at the upper right of the widget. This is not available for all widgets.

Custom Tabs

The following operations can be performed to customize tabs:

Create Drag a folder from the Browse/Search widget to the tab region at the top of Dashboard to create a tab that contains a new Browse/Search widget, or click the **+** tab to create a new empty tab.

Edit click the  icon on a tab to enter a new name. Cancel changes by pressing the Esc key.

Delete click the ✖ icon on a tab to permanently delete it. A prompt appears to confirm the change.

Reorder Tabs can be reordered by dragging a tab to the left or right of another existing tab.

Bulk Operations

From the Dashboard, bulk operations can be performed on multiple Secrets. Select the Secrets you want to include by checking the check box next to the Secret's Name. To check them all, check the check box in the column headers row. Then, select the operation from the dropdown list below the list of Secrets.

Currently, Available Bulk Operations:

- Add Share
- Assign To Site
- Assign Secret Policy
- Change Password Remotely
- Change to Inherit Permissions
- Convert Secret template
- Delete
- Disable AutoChange
- Disable Check Out
- Disable Comment on View
- Disable Heartbeat
- Edit Share
- Enable AutoChange
- Enable Check Out
- Enable Comment on View
- Enable Heartbeat
- Hide Launcher Password
- Move to Folder
- Run Heartbeat
- Set Privileged Account
- Undelete

- Unhide Launcher Password

*Bulk Operations differ based on your edition.

Secrets

Secrets are individually named sets of sensitive information that is created from Secret templates. Flexibility in templates allows Secrets to address a broad spectrum of secure data. Secret security can be centrally managed through Sharing settings for each individual Secret. Additionally, folder structure can allow one or more Secrets to inherit permissions from their parent folder. All Secret field information is securely encrypted before being stored in the database, with a detailed audit trail for access and history. For details on using bulk operation to configure Secrets, see the Dashboard section.

Creating a Secret

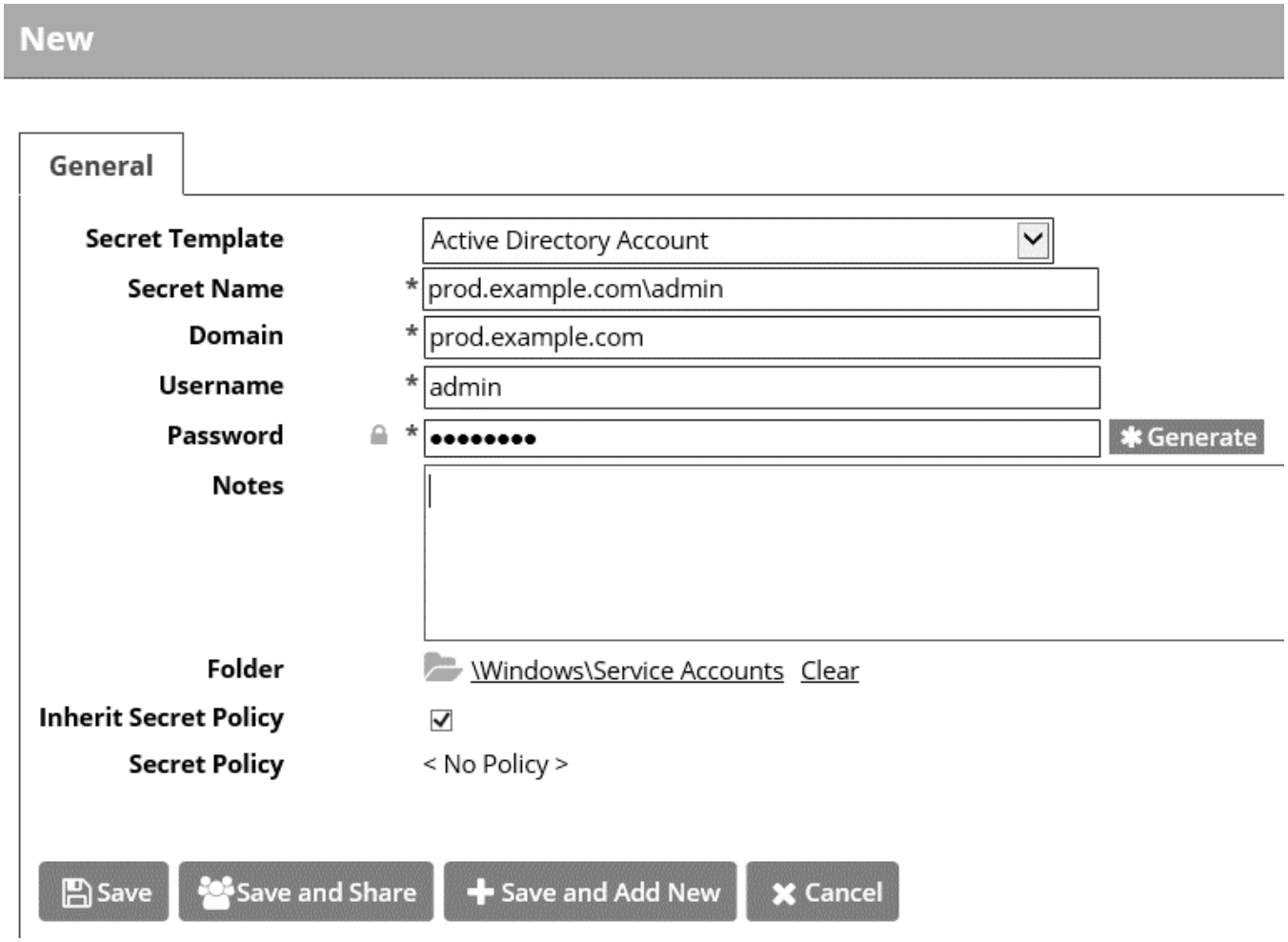
From Advanced Dashboard, find the Create Secret widget and select the Secret template from which to create the Secret. After you select a template, you will be directed to the New Secret page. On Basic Dashboard, click **Create New** and select the desired Secret template type from the **Secret Template** drop-down menu. This template contains all the relevant fields for a Secret. If you do not find a suitable template available, a custom template can be created.

For more information about Dashboard views, see Dashboard.

New Secret Page

For simple Secret templates, Secret creation is intuitive and straightforward. The more complex Secret templates are discussed later in this user guide. On The New Secret page, complete the Secret Name, and the other Secret fields present. Fields with an asterisk * are required (these can be modified at the Secret Template level).

Note The Secret Name field is the text used both for display purposes throughout the application and for search functions (other fields can be used as well; see Searching Secrets for more details).



Click Save and Share after completing the Secret fields to immediately set the Sharing settings on the newly created Secret. Sharing is discussed in more detail in Secret Sharing.

It is possible to import data as Secrets. This topic is discussed in the Secret Import section.

Viewing a Secret

To view the information that is contained in a Secret, you must navigate to the Home page. From there, click the Secret name, then click View. For instructions on browsing your Secrets on the Home page, see the Searching Secrets section.

Only the General tab is discussed in this section. This page is referred to as the Secret View page. For information on the other tabs, see the Secret View Tabs section.

The Secret View page displays the relevant information for a Secret. The password fields of a Secret can be masked, depending on your settings. The icons below will perform the following operations when clicked:

Lock Unmask a field until the cursor is moved away from the icon.

History Display the history of changes to the field.

Copy-to-clipboard Copy the field to the clipboard. You might need an add-on for this to function.

NATO Display the field by using the NATO phonetic alphabet. This 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 depending on the Default Secret Permissions setting in the IBM Security Verify 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 be displayed in the Favorite Secrets widget.

Edit the Secret fields.

Create a duplicate copy of the Secret, which might also be renamed and modified.

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

View the Secret audit log to see which users have accessed the Secret and the actions that have been performed.

Delete the Secret.

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

Advanced Options

Below are the buttons, fields, and icons that are specific to more advanced Secrets:

Run Heartbeat	Initiate Heartbeat, which attempts to verify that the Secret credentials can authenticate.
Expire Now	Expire the Secret manually.
Launcher icon	click to open the Launcher. Further details in the Launcher section.
Site	Edit the Secret to set the Distributed Engine Site. This determines where password changing, heartbeat, and proxied sessions run from.

Secret View Tabs

Personalize Tab

These settings will only be applied to the user who is editing the settings. They will not apply to the other users who have View/Edit/Owner permission to the Secret.

To use the settings in the Email Notifications area, you must have email that is configured correctly in your Configuration settings. You also need a valid email address that is entered for each user account to use these settings. This can be set in the Administration > Users section.

The following Email Notifications settings are available:

Send Email When Viewed
Email the user when the Secret is viewed by any user.

Send Email When Changed
Email the user when the Secret is edited by any user.

Send Email When Heartbeat Fails
Email the user when Heartbeat fails for the Secret. The email contains the Secret name, error code, and details.

The Personalize tab also contains settings that pertain to the type of launcher that is configured for a Secret. If the Launcher type is Remote Desktop, the following settings are available:

Connect to Console Remote Desktop Connection connects to the console session.

Allow Access to Printers Grant Remote Desktop Connection access to local printers.

Allow Access to Drives Grant Remote Desktop Connection access to drives connected to the local machine.

Allow Access to Clipboard Grant Remote Desktop Connection access to the clipboard of the local machine.

Use Custom Window Size Allow user to specify custom window height and width. Use Preferences refer to the user's settings under Profile > Preferences under the Launcher tab.

Users might opt to enable or disable these settings, or to defer to what is configured in their user settings by selecting Use Preferences.

Expiration Tab

Inside the Expiration tab, the expiration period can be modified. The following options are available:

Template Interval Default expiration period that is configured for new Secrets based on the current template.

Custom Interval Specify a custom expiration period in days.

Custom Date Specify a custom expiration date in month/day/year format.

See Secret Expiration for further details.

Security Tab

The Security tab contains settings that can be enabled to increase security for a Secret. The settings that are listed below might or might not be visible, depending on your configuration settings:

Require Check Out
Only one user at a time can have access to a Secret. See Secret Check Out for further details.

Enable DoubleLock
A user must enter their DoubleLock password to decrypt and view a Secret.

Enable Requires Approval for Access
A user must request access to view a Secret. See Requires Approval for Access for further details.

Require Comment
A user must enter a comment before being granted access to view the Secret. The comment is stored in the audit log for that Secret.

Enable Session Recording
Record the Launcher session. This applies to Secrets with a Launcher that is associated with the Secret template. See Session Recording for further details.

Hide Launcher Password
Remove the ability of users with only View permission to copy-to-clipboard or unmask the password field of the Secret. This applies to Secrets with a Launcher that is associated with the Secret template.

Customize Password Requirement
Check this box to specify a password requirement for each field of the Secret that has the type “password.”

Launcher Tab

The Launcher tab appears for Secrets that use either a Custom Launcher or Web Launcher.

If a Custom Launcher is associated with a Secret template, a Secret Owner can configure associated Secrets or a privileged Secret to run the Launcher process. The associated Secret can be tied in to the command line parameters on the Custom Launcher, and the privileged Secret is the identity that starts the launcher process.

If a Web Launcher is associated with a Secret template, the Launcher tab displays how the Web Launcher is configured for that Secret. The following options are available:

Test Launcher	Test the current Web Launcher configuration.
Edit Fields	Modify which Secret fields are mapped to the HTML input controls on the target website.
Reconfigure Web Launcher	Reset the Web Launcher configuration.
Use Web Password Filler	Opt to use the Web Password Filler rather than the Web Launcher.

See the Web Launcher section for further details.

Remote Password Changing Tab

The settings inside the Remote Password Changing tab are used for Secrets that are Remote Password Changing- enabled:

Auto Change	Enable or disable Auto Change for the Secret.
Next Password	Specify the next password

For more information, see the Remote Password Changing section.

Dependencies Tab

The settings inside the Dependencies tab are used for Secrets that have Remote Password Changing enabled. For more information on Dependency checking, see the Dependency Finder section within the Remote Password Changing section.

Editing and Deleting a Secret

If using the Dashboard, see the Dashboard section.

To edit a Secret, navigate to its Secret View page and click Edit. All fields become editable. For passwords, there is an ability to randomly create a password with the **Generate** button. This generates a password according to the rules set at the template level (see Secret templates for more information about password requirements).

To delete a Secret, navigate to the Secret View page and click **Delete**. The Secret is logically deleted from users who do not have a role containing the View Deleted Secrets permission. IBM Security Verify Privilege Vault uses “soft deletes,” to maintain the audit history for all data. However, deleted Secrets are still accessible by administrators (similar to a permanent Recycle Bin) – to ensure that audit history is maintained and to support recovery. A user must have the View Deleted Secrets permission in addition to Owner permission on a Secret

to access the Secret View page for a deleted Secret. For more information about these permissions, see Roles and Sharing a Secret.

To undelete a Secret, navigate to the Secret View page and click **Undelete**.

Secrets can also be deleted in bulk. For details, see Bulk Operations on Secrets.

Sharing a Secret

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

There are three permission levels to choose from when sharing 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 (username, 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.

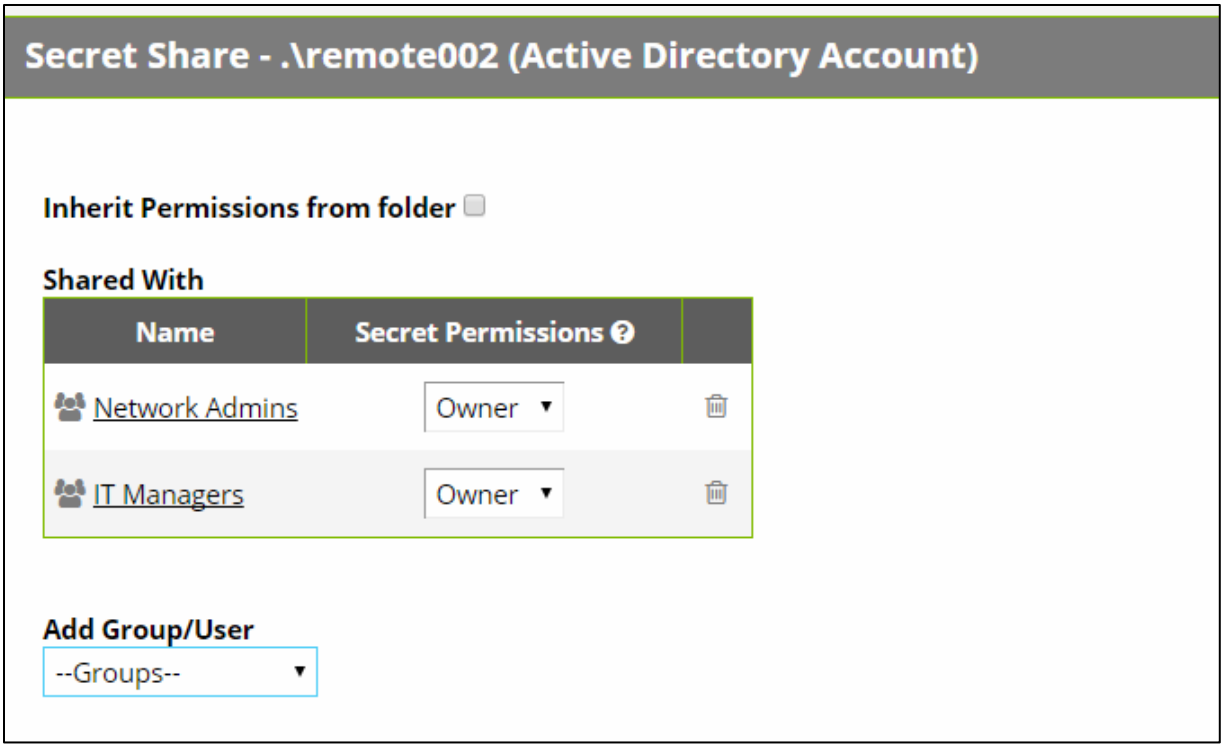
Owner Allows the user to change all the Secret metadata (permissions, security settings, and so on).

Password fields will not be visible if a Secret has a launcher and Hide Launcher Password is turned on or the user does not have the View Launcher Password role permission.

For example, administrators require the Edit permission to the router password, but a contractor doing network upgrades might only need View (read-only) access to that same Secret.

Secrets can be shared with either groups or individual users. Secret Sharing section allows Secrets to be configured for access.

To add and/or remove Sharing from a Secret, navigate to the Secret View page and click **Share**. On the Secret Share page, existing Sharing settings for each user or group are displayed in the grid. To edit these settings, click **Edit**. You can now add or remove users or groups from Sharing on the Secret. You can also modify Sharing settings for users or groups that already have Sharing enabled for the Secret. If a user or group is not displayed, they do not have access to the Secret.



To further simplify the process of Sharing, Secrets can automatically inherit the settings from the folder they are stored in. By enabling the Inherit Permissions from folder option on the Sharing Edit page, a Secret inherits all the parent folder's Sharing settings. For more on folder security, see the Folders section.

Copying a Secret

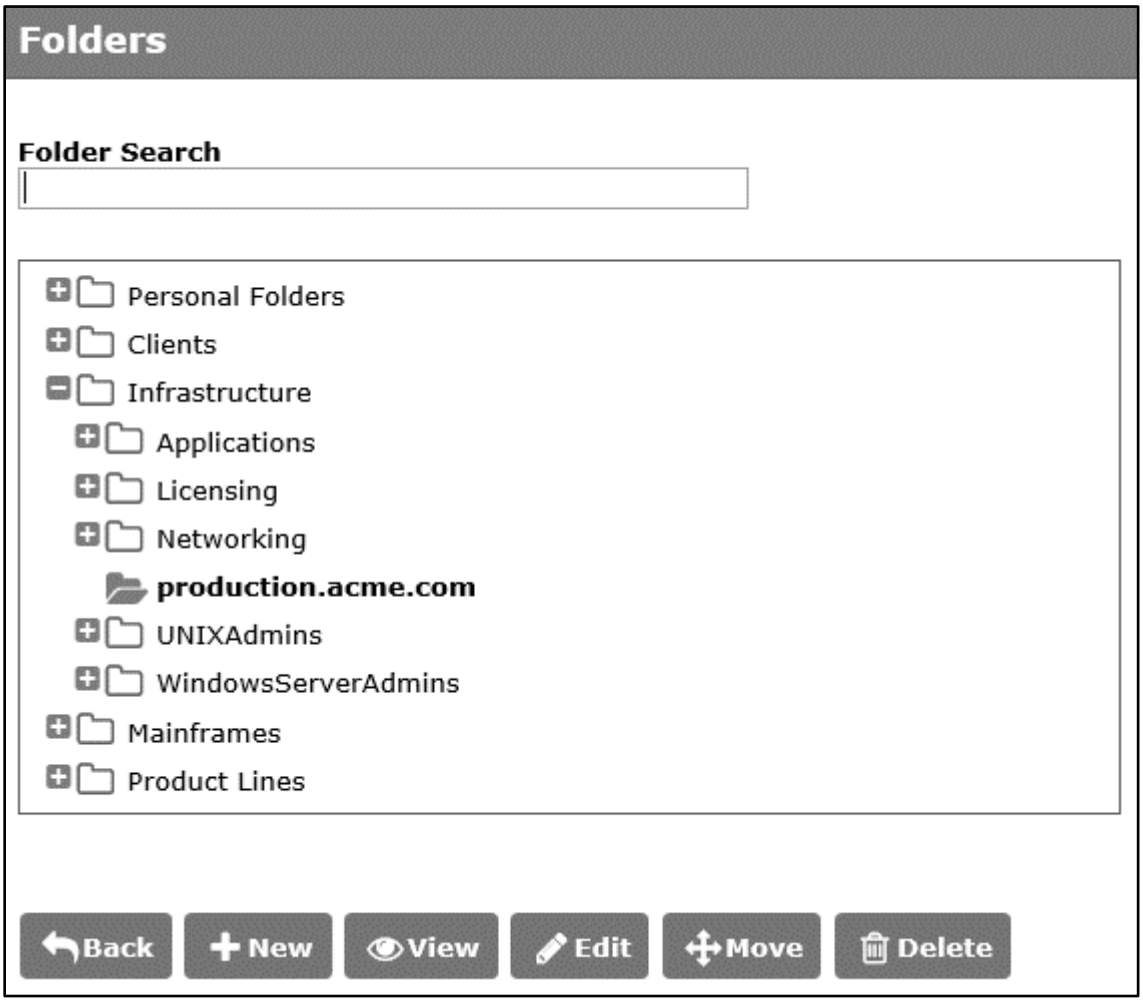
Secret Copy allows for more efficient duplication of secrets. Any user with the Owner secret permission on a secret can click **Copy Secret** at the bottom of the General tab to create a new Secret with information based on the original secret. Secret field information, launcher settings, secret settings, double locks, email settings, and permissions are copied over. Audit records are written to the source Secret and target Secret to indicate that a copy operation took place. Currently, file attachments are not copied.

Folders

Folders allow you to create containers based on your individual needs. These folders help organize your customers, computers, regions, branch offices, and so on, into centralized areas. Folders can be nested within other folders to create further sub-categories for each set of classifications. Secrets can be assigned to these folders and subfolders. A benefit of folders is customizing permissions at the folder level and enabling Inherit Permissions on Secrets within the folders. Setting permissions at the folder level will ensure future Secrets in that folder have the same assigned permissions, and simplify managing access across users and Groups.

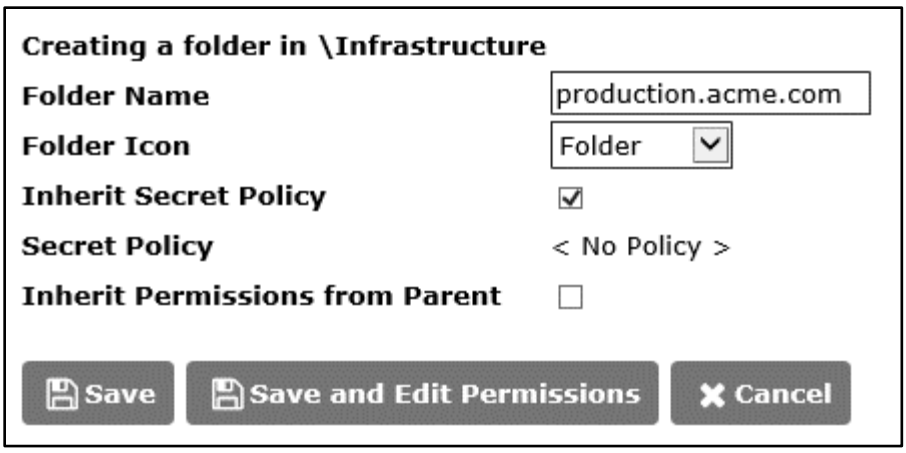
Creating a Folder

To create a folder, select **Folders** from the **Administration** menu.



To view the Folders page and create folders, you must have a Role with the Administer Folder permission.

Click **New** to create a new folder. By default, a new folder is created at the root level. If you want to create a subfolder, select the parent folder from the folder tree before clicking **New**. To return to the root level, click the highlighted folder to clear it. To create a subfolder, you must have Edit or Owner permissions on the parent folder.



By default, the new folder inherits the Secret Policy that is assigned to its parent folder. To disable this, clear the **Inherit Secret Policy** check box. To assign a Secret Policy to this folder, select the policy from the drop-down menu. For more information about configuring these policies, see Secret Policy.

Folder Name will be the text used both for display purposes throughout the application as well as for search functions, and the folder icon setting is used to display the specialized icon in the Folder Tree views and advanced folder searching. The folder icons available are Folder (default), Customer, and Computer.

Folder Tree View

Folder Sharing and Permissions

If the new folder is a subfolder, then you can have it use the Sharing settings of its parent folder by enabling the folder to Inherit Permissions from Parent.

Folders have the following Sharing structure: Edit, View, Add Secret, and Owner.

View Allows the user to see the folder and Secrets in that folder that are inheriting permissions from their folder.

Edit Allows the user to create new folders in that folder (will force “Inherit Permissions from Parent” to on for the new folder), move Secrets into that folder, and add new Secrets into that folder.

Add Secret Allows the user to add a Secret in that folder. Does not grant access to the added Secret.

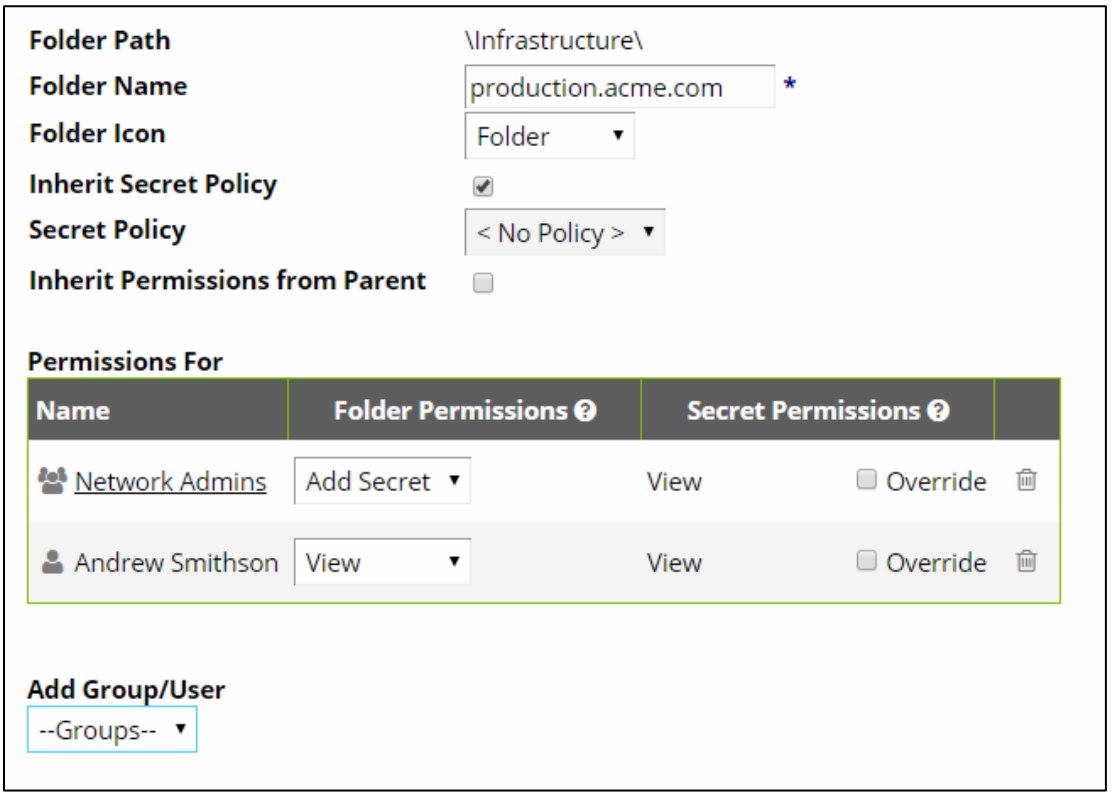
Owner Allows the user to create new folders in that folder without forcing inheritance, move the folder, delete the folder, rename the folder, and change the permissions and inheritance settings on the folder.

Click **Save and Edit Permissions** to configure Sharing settings on the new folder. Depending on your Configuration setup, these settings might affect the permissions of subfolders and Secrets contained in this folder. Folders are not visible to users that do not have View permission (unless the configuration setting

"Require View Permissions on Specific Folder for Visibility" is turned on). This allows users to create and manage their own folders without making them visible to all users.

Editing Folder Permissions

To edit the permissions of a folder, highlight the folder on Dashboard and click the icon. Folder permissions can also be edited from the Administration > Folders page by highlighting the folder and clicking **Edit**.



Below are a few folder-specific settings that you might want to use in your IBM Security Verify Privilege Vault configuration (go to Administration > Configuration): Default Secret Permissions
This setting determines whether new Secrets will by default inherit permissions from their containing folder, copy permissions from their parent folder, or give the creator of the Secret access. The options are as follows:

- **Secrets inherit permissions from folder**
  New Secrets are marked as inheriting from folder, thus will have the same permissions as the folder.
- **New Secrets copy permissions from folder**
  New Secrets will not be marked as inheriting from folder but will start with the same permissions as their folder.

- **Only creator has permissions to new Secrets**
  New Secrets will not be marked as inheriting from folder. Only the creator will initially have permissions on the Secret. Note that when a Secret is copied, the new copy will also have whatever permissions the source Secret had.

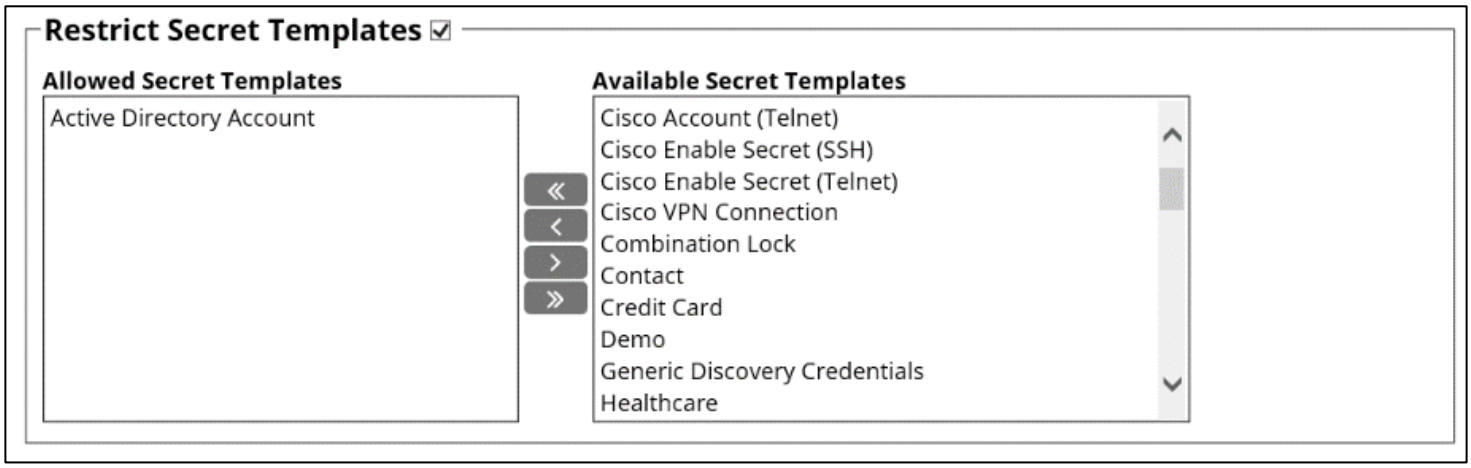
Require View Permission on Specific Folder for Visibility
When enabled, this hides folders that the user does not have explicit View permission on. The folders will not appear in the tree view or allow search and browse. If disabled, the users can see the folders in the folder tree, but they appear empty as the user does not have View permission to the Secrets.

Require Folder for Secrets
This setting is used to force users to always add Secrets to folders.

It is possible to setup an automatically replicated folder structure from an external Database, such as ConnectWise or other CRM systems. This topic is discussed later in Folder Synchronization.

Restrict Secret Templates for a Folder

You might choose to only allow Secrets based on specific Secret Templates to exist within a specific folder or folders by clicking **Edit** on a folder and checking the box for **Restrict Secret Templates**.



Select one or more of the “Available Secret Templates” and use the arrow buttons to place the Secret Templates you want to allow in the folder under the “Allowed Secret Templates” section. Once you are finished, click **Save**.

Adding and Moving Secrets

To add a Secret to a folder, you must have Edit permission on that folder (either direct or through inheritance).

To move a Secret to a folder, you must have Edit permission on that folder (either direct or through inheritance).

To move a Secret from a folder, you must have Edit permission on that Secret. If the Secret has “Inherit Permissions from folder” then you must have Owner permission to move that Secret to a new folder.

When a Secret is moved to a folder, it will automatically get “Inherit Permissions from folder” even if it had specific permissions before the move.

Creating, Deleting, and Moving Folders

The Administer Folders role permission will allow a user to be able to create new folders and manage folders, but specific folder permissions still apply.

Any user with the Administer Folders role permission will be able to create new folders, however to create folders at the root level the user also needs the Create Root Folders permission.

They will also be able to add new folders to any folders where they have Edit or Owner permission on that folder.

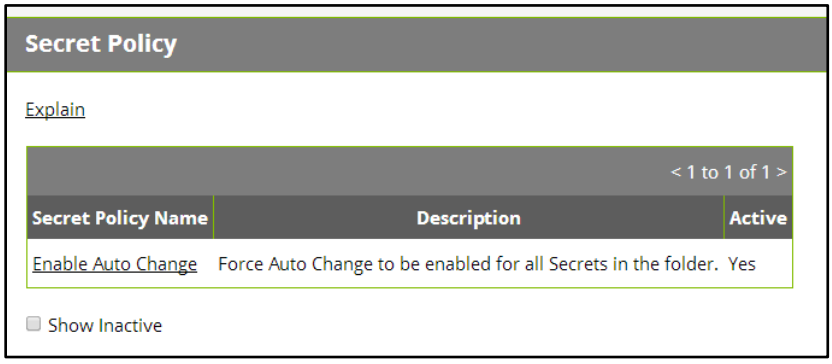
They must have Owner permission to be able to delete a folder.

They can also move folders where they have Owner permission on the source folder and Edit or Owner permission on the target folder (where they are moving it). The folder will automatically “Inherit Permissions from parent” when it is moved (same as when Secrets are moved).

Secret Policy

Secret Policies can be configured to apply Remote Password Changing and Security settings to an entire folder of Secrets. To view existing Secret Policies or create a new policy, select **Secret Policy** from the **Administration** menu.

Click the **Secret Policy Name** of an existing policy to view the policy details and/or edit the policy.

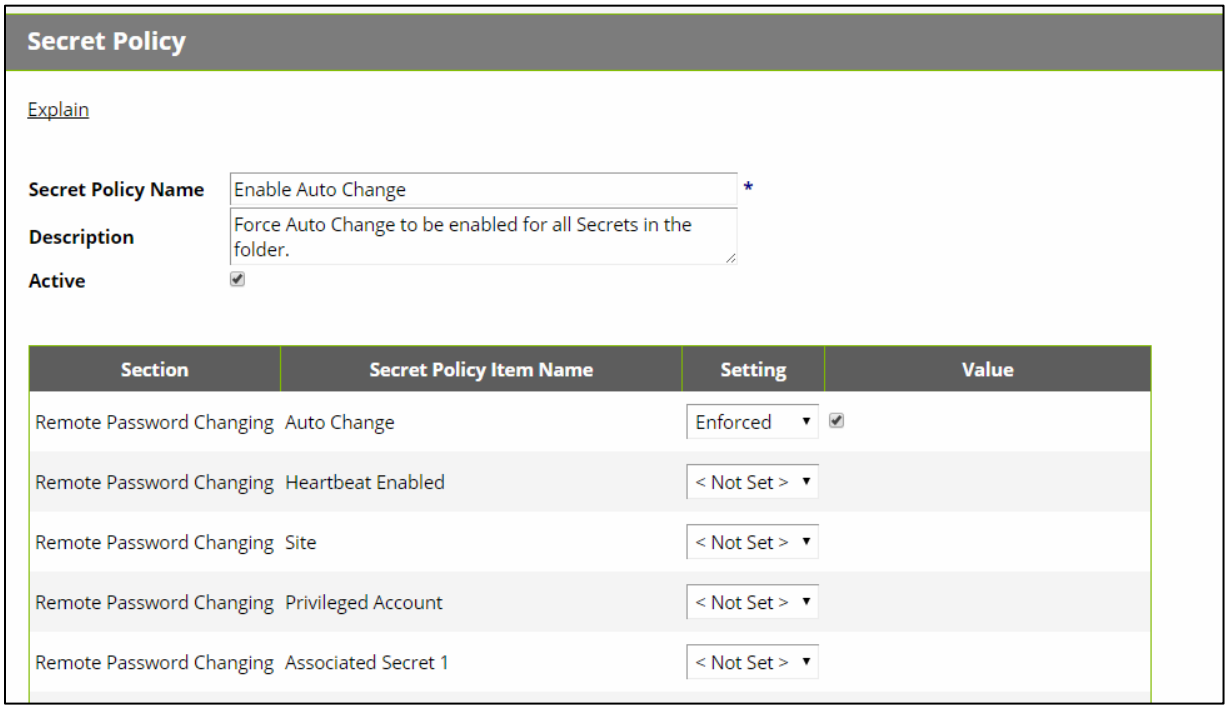


To create a new Secret Policy, click **Create New**. Enter a name for the Secret Policy, and then choose a **Setting** for the setting that you would like to configure. Aside from **< Not Set >**, which means that the setting will not be applied, there are two options:

Default
The policy is applied to all Secrets in the folder initially, but it is possible to manually change the applied Secret settings as well.

Enforced
The policy is applied to all Secrets in the folder initially, and it is not possible to change those applied settings on Secrets in that folder.

Apply the setting by selecting the **Value** check box in that row. Applying the setting might enable configuration of related settings in the grid. For example, enabling Auto Change causes Auto Change Schedule to be available for configuration.



Click **Save** to make the policy available for assignment to folders. To deactivate a policy that you would no longer like to be used, edit the policy and clear the **Active** check box.

For information about applying a Secret Policy to a folder, see Editing Folder Permissions.

Personal Folders

In IBM Security Verify Privilege Vault, we refer to a “personal folder” as a folder that one (and only one) individual has owner access to. No user is able to modify sharing permissions on these folders. A user cannot add subfolders to their personal folder. The purpose of this folder is to allow a user to securely store work-related Secrets that other users do not require access to. Note that when in break the glass mode, an unlimited admin can access a user’s personal folder in order to recover Secrets if needed.

To use personal folders, they will first need to be enabled:

Enable Personal Folders

1. From the **ADMIN** menu, select **Configuration**.
2. Click the **Folders** tab, and then click **Edit**.
3. Select the **Enable Personal Folders** check box.
4. If you would like to customize the root-level folder that will contain all personal folders, you can enter a new **Personal Folder name**.
5. If you would like to display a warning message to users when placing Secrets in their personal folders, select the Show user warning message check box and optionally edit the Warning message text.
6. Click **Save**. A personal folder for each user will now be created in a root-level folder with the **Personal Folder name** specified.

When personal folders are enabled, a user will require the **Personal Folders** role permission in their role to be able to view and use their own personal folder.

Secret Templates

Creating or Editing a Secret Template

Select **Secret Templates** from the **Administration** menu. On this screen, either select a Secret template to edit or create a new one. If creating a new Secret template, a prompt appears to specify the name of the new template. Enter the new name and proceed. The Secret Template Designer page provides all the options for configuring a Secret template as well as which fields appear on any Secret created from that template.

Secret Template Fields

The Secret Template Designer provides several settings to customize Secret template fields. To add a Secret field, complete the values and click the button. To delete a field, click the icon. There will be a confirmation dialog box before deletion takes place. To edit a field, click the icon. Click either the icon to save or the icon to discard the changes.

Secret Template Field Settings

The settings available for fields are listed below:

Field Name	Name of the field. This name will be used for the Create New drop-down list on either the Dashboard's Create Secret Widget or Home page.
Field Description	Description of the field.
Field Type	Type to use in the field. See below for a description of the different fields.

Is Required	Whether or not the field should require a value. These fields will be checked for correct content when the user attempts to create this Secret. A validation error will be displayed if not entered correctly.
History	Number of values to keep in the field's history of values.
Searchable	Whether or not that field should be indexed for searching. By default, passwords are not indexed. File attachments and history fields cannot be indexed for searching.
Edit Requires	Minimum permissions on the Secret needed in order to edit the value on the Secret. Valid options are Edit, Owner and Not Editable. This enables the Secret Field to be locked down at a more granular level than other fields on the template.
Hide On View	If checked, this field will not be displayed to users when viewing the Secret. The field will only be displayed when the Secret is in Edit mode.
Expose For Display	If checked, this field will be available to be displayed as a Custom Column on Dashboard.

All fields that are set to **Expose For Display** will NOT be encrypted in the Database. Only check this value if the Secret field data is not considered privileged information.

The order of appearance of the fields in the Template Designer grid is the order in which they appear when the user views or edits a Secret created from this template. The order can be modified through the up and down arrows on the grid.

Default values can be specified on each field by clicking the Edit Defaults button  . These added values appear as a drop-down list on any Secret created from this template.

Secret Template Field Types

Template fields can be specified as one of several different types to enhance customization.

Text	Single-line text field.
Notes	Multi-line text field.
URL	Clickable hyperlink.
Password	Password type field.
File	File attachment link. File attachments are stored in the Microsoft SQL Server database.

Additional Changes to a Template

For additional changes to a Secret template, click the Change link on the Secret Template Designer page to navigate to the Secret template Edit page.

Expiration Enabled?
Secret templates allow expiration on certain fields. When the Expiration Enabled? option is turned on, an expiration time interval can be specified for a selected field by using the drop-down menu. With this option enabled and a time duration specified, IBM Security Verify Privilege Vault will begin providing alerts if the Secret field is not changed within the specified expiration requirements. See Secret Expiration section.

Keep Secret Name History?
If Keep Secret Name History is enabled, IBM Security Verify Privilege Vault will keep the specified number of entries for viewing. This feature creates a record of every name used when a new Secret is created.

Edit Passwords button
Only visible for templates that contain a field that is of Password type. It is used to alter the minimum password length as well as the character set used for the auto-generation of the Secret's password (see the Editing and Deleting a Secret section for further details on password auto-generation).

Configure Password Changing button
Used to enable Remote Password Changing on these Secrets. For further details, see the Remote Password Changing section.

Configure Launcher button
Used to enable Remote Desktop or PuTTY Launcher or custom launchers on these Secrets. For further details, see the Launcher section.

Configure Extended Mappings button
Extended Mappings allow you to tie a field value to a IBM Security Verify Privilege Vault defined system type for additional functionality. For example, you might have a generic Password Secret Template that has a username and password field. For purposes of looking up credentials, such as a ticket system authentication Secret, IBM Security Verify Privilege Vault needs to know that actual type of the fields since the field name can be custom. Extended mappings available are:

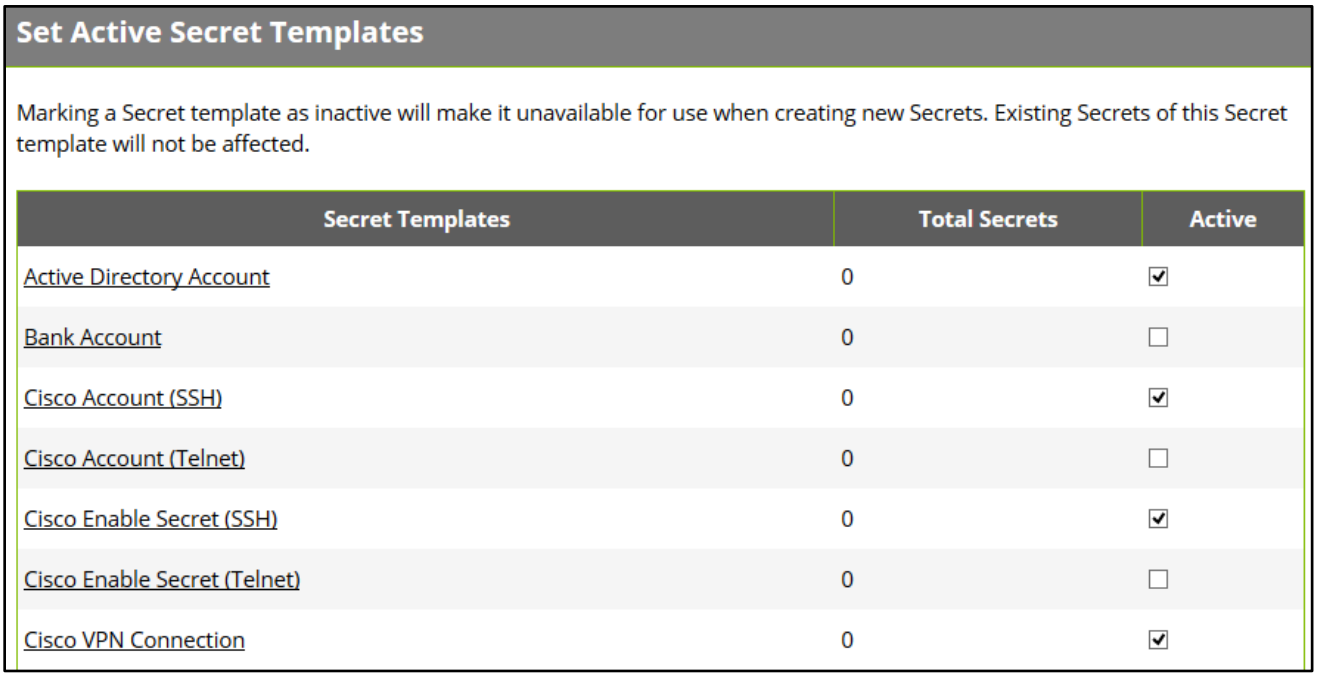
- **SSH Private Key**: Defines which fields make up the SSH Key components of **Private Key, Private Key Passphrase,** and **Public Key.**
- **Username and Password:** Defines which fields contain the username and password.
- **Remote Server SSH Key for Validation:** The machine SHA1 Digest for validating the machine connected to is correct.
- **OATH Secret Key**: For password changing on the Amazon Root Account by using the Web Password Changer. If you enter the OATH secret for two factor, IBM Security Verify Privilege Vault will

generate the OTP automatically for password changing and heartbeat, allowing you to automate that functionality while enforcing two factor on the AWS root credential.

Activating and deactivating Templates

If a template is no longer relevant or outdated, it can be inactivated. This can be done from the specific template's Secret Template Edit page.

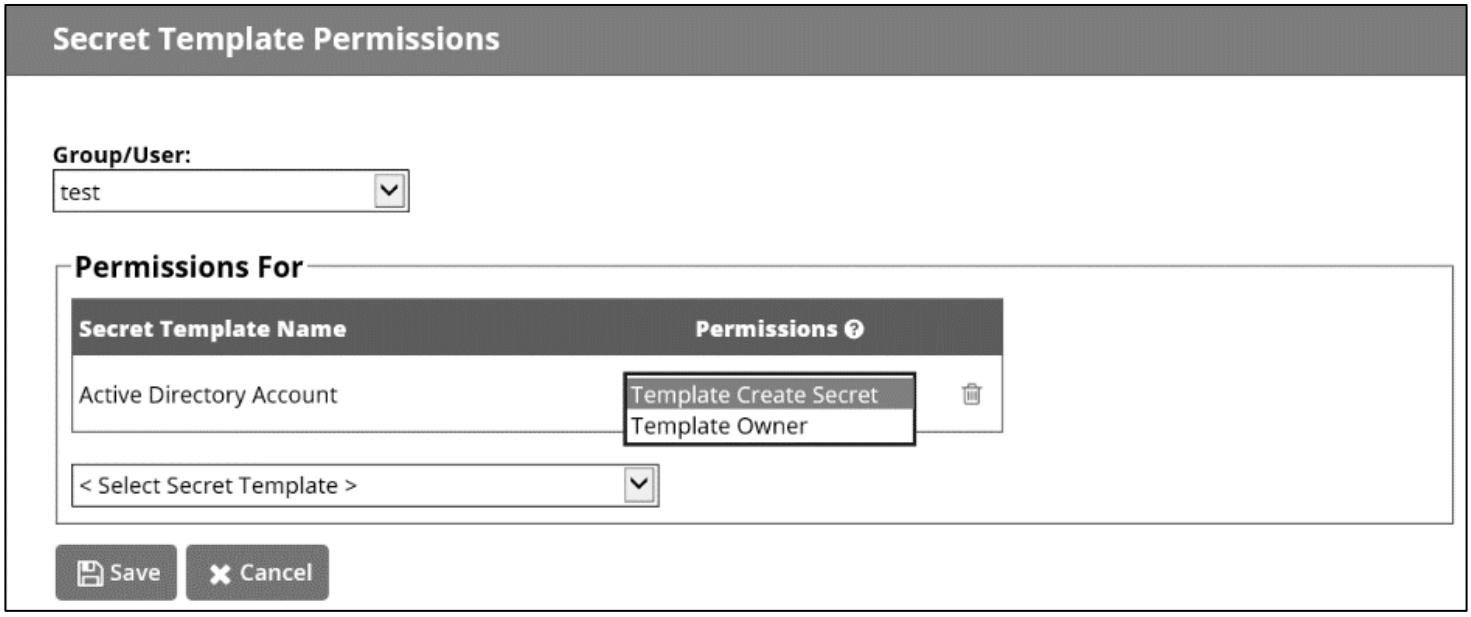
Templates can also be inactivated in bulk from the Manage Secret templates screen. Click the Active Templates button to navigate to the Set Active Secret templates screen. This screen displays all the Secret templates in IBM Security Verify Privilege Vault. Each Secret template can be set as active or inactive. Once the Secret templates are chosen as active or inactive, then saving changes will bring the Secret templates into effect immediately. Note that inactivating a Secret template will not inactivate any Secrets by using that Secret template – those Secrets will still exist but users won't be able to create new Secrets by using an inactivated Secret template.



Configure Secret Template Permissions

As of IBM Security Verify Privilege Vault 10.3 it is possible to assign users/groups to specific Secret Templates, so they can either manage and/or create Secrets based on those templates. This allows you to have more granular control over what Secret Templates are seen by users and groups when they are managing the templates or creating Secrets.

Navigate to **Admin | Secret Templates** and click **Configure Secret Template Permissions**. Select a group or user, click **Edit**, and select a Secret Template you want to assign them to.



You might either assign “Template Create Secret” or “Template Owner” to a user/group. Template Create Secret allows a user/group to create Secrets based on the selected Secret Template. Template Owner allows a user/group to edit a Secret Template and create Secrets based on the selected Secret Template. By default, the Everyone group that targets all users of IBM Security Verify Privilege Vault will have the ability to create Secrets based on any Secret Template. Please note that a user's Secret Template permissions are based on the permissions directly assigned to them as well as the permissions assigned to all of the groups they are a member of. If a user/group does not have Template Create Secret or Template Owner permissions then they are unable to create a Secret based on that Secret Template or see that it exists in IBM Security Verify Privilege Vault.

Character Sets

Character Sets are a collection of distinct characters that are used in Password Requirements and Password Rules. Custom sets can be created and both ASCII and Unicode are supported. For more information on setting up compliance checks and password generation standards see the Password Requirements section. The 5 standard Character Sets are:

- Lower Case (a-z)
- Upper Case (A-Z)
- Numeric (0-9)
- Non-Alphanumeric (!@#$%^&*())
- Default – Includes all the above

To manage Character Sets click the Character Sets button on the Administration > Secret templates page. Only character sets which are not currently used by a Password Requirement can be deleted.

Password Requirements

Requirements can be set on a password field to validate user-entered passwords and/or make auto-generated passwords conform to certain specifications.

A Password Requirement is made up of a minimum and maximum length, a set of characters, and optional rules such as “At least 3 upper-case characters” or “The first character must be lower-case”. The default password requirement is 12 characters from the Default character set, with at least one upper-case, lower-case, numeric, and symbol character.

Password Requirements can be created or edited through the Password Requirements button on the Administration>Secret templates page. Character sets can be created or deleted from the Character Sets button next to the Password Requirements button.

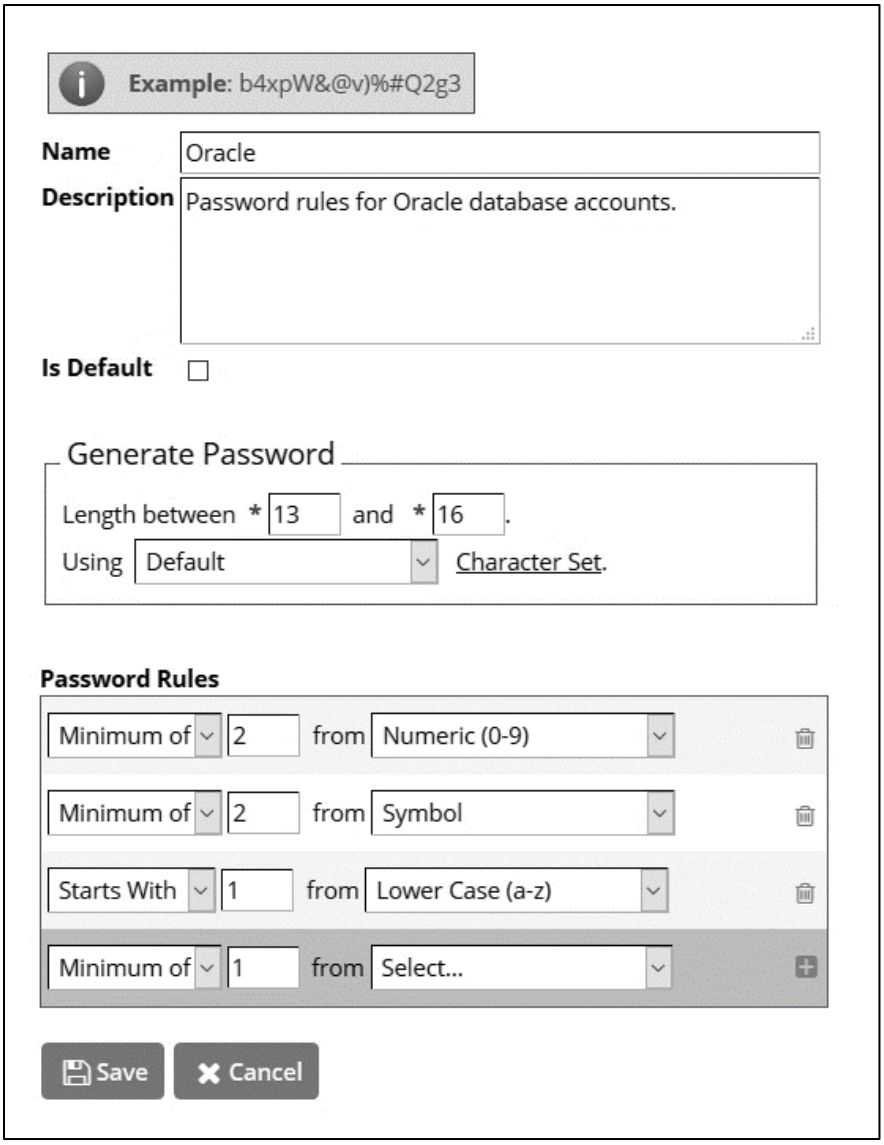
To set the password requirement for a field for a Secret template, click the Edit Passwords button on the Secret Template Edit page. Next, click the Edit icon, select the desired Password Requirement, and click the Save icon to save the changes.

To set a custom password requirement for a specific Secret, use the Customize Password Requirement in the Security tab of a Secret. For further details, see the Security Tab section.

Validation of manually entered passwords can be turned on or off at the Secret template level via the Validate Password Requirements On Create and Validate Password Requirements On Edit settings.

The What Secrets Do Not Meet Password Requirements report shows Secrets containing a password that does not meet the Password Requirements set for its Secret template.

Password requirements cannot include rules with overlapping character sets. For example, if an attempt is made to add both a “Minimum of 1 upper-case” rule and a “Minimum of 3 Default” rule to a new password requirement, an error will be displayed.



Naming Patterns

IBM Security Verify Privilege Vault supports naming patterns for Secret templates. Naming patterns are a way for administrators to maintain consistency for Secret names and can help ease both browsing and grouping Secrets by name. Patterns are created by using regular expressions. Regular expressions are a formal set of symbols commonly used to match text to patterns.

An example regular expression is ^\w+\\w+$, which would allow "NTDOMAIN01\USER3454" but not "USER3454 on NTDOMAIN01". Here the "^" symbolizes the beginning of the text. "\w" specifies alpha-numeric characters, plus the "_" character, while "+" indicates one or more occurrences of the previous symbol. In this case "+" means one or more alpha-numeric characters ("\w"). The "\\" is used to denote a single "\". In regular expressions special characters are escaped with a "\", so to try and match a single backslash requires an extra escape character. Lastly the "$" signals the end of the text.

Convert to New Template

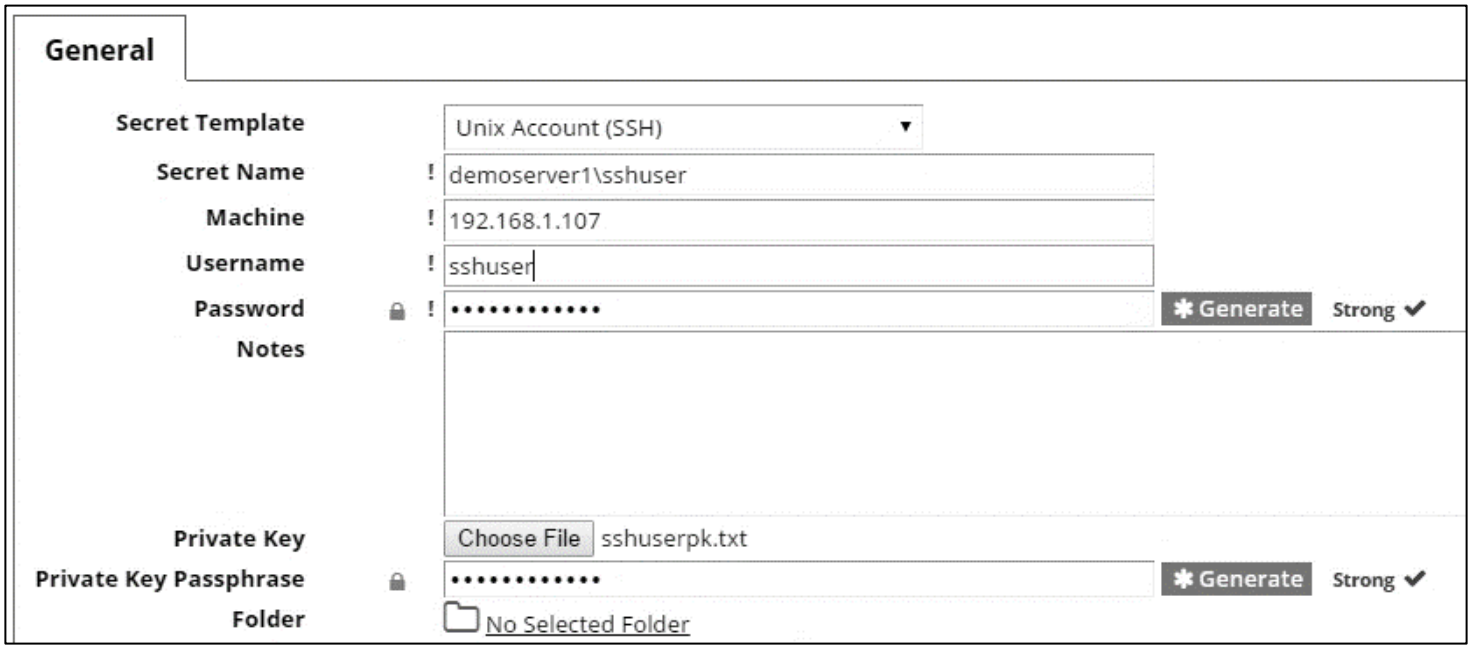
It is possible to convert Secrets from one Secret template to another. To do this, view a Secret and click the Convert Template button. Next, select the target template from the Secret template drop down list. You will then be able to map each field to a new field. To do this, go through each drop-down list and select the target field for each source field on your Secret. If you want to remove the value for a field instead of converting it, then select the <Remove> option on the drop-down list for that field. When you are done selecting, you can choose a folder and click Save.

The Convert Template button is only available to users and groups with the "Owner" permission to the Secret.

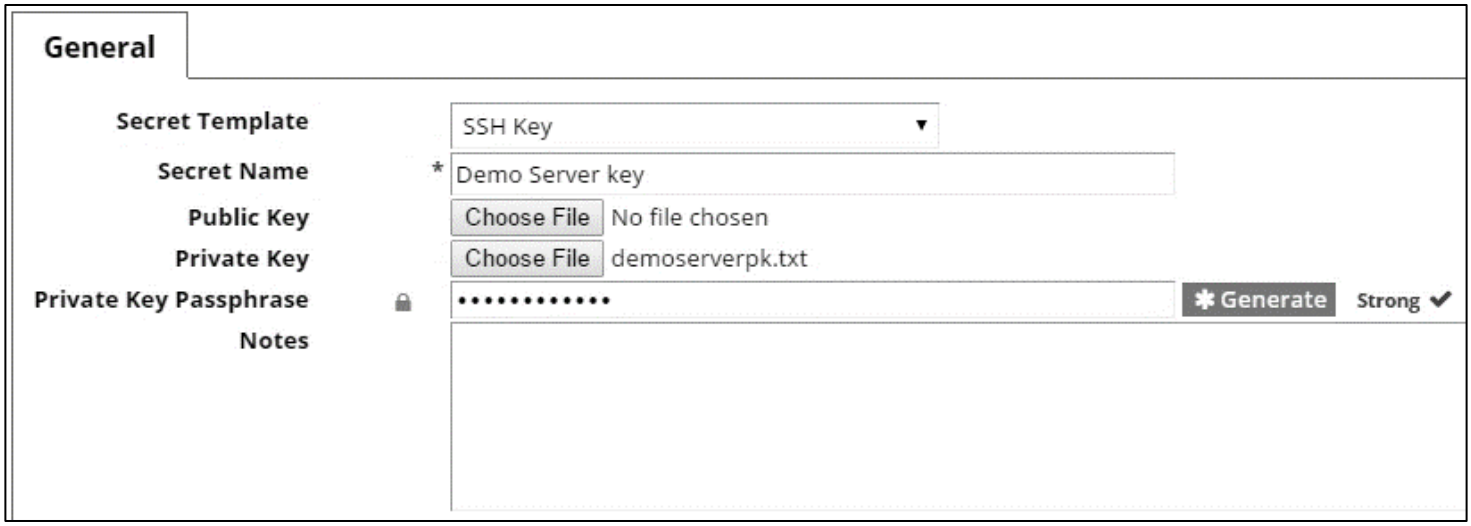
To preserve audit data, when a Secret is converted from one type to another, the old Secret is deleted and a new Secret is created. An admin can view old Secret by searching for deleted Secrets on the dashboard. A user will need "Add Secret," "Edit Secret," "Delete Secret," and "Share Secret" role permissions in order to convert a Secret to a new template.

SSH Key Authentication

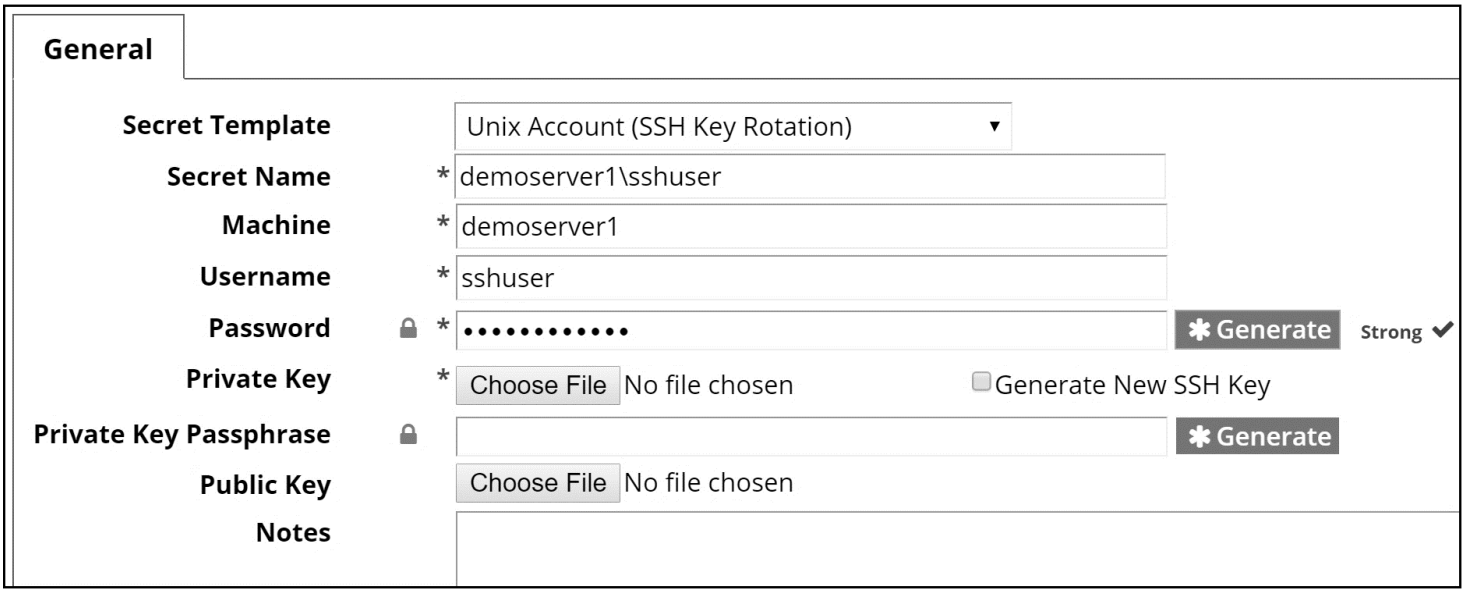
IBM Security Verify Privilege Vault supports SSH Key authentication in version 8.8 and above. With this feature, admins can use private SSH keys for PuTTY Launcher sessions as well as for Remote Password Changing tasks (configurable through password changer settings) and Unix/Linux Discovery. Passphrases can additionally be stored if necessary to decrypt the private keys for additional security. The **Unix Account (SSH)** Secret template includes fields for the Private Key and Passphrase by default:



The **SSH Key** template is included by default and can be used to store SSH keys that can later be selected for use in Remote Password Changing, Discovery or Launcher authentication for other Secrets:



Starting with version 10.1.000000 IBM Security Verify Privilege Vault also supports SSH Key Rotation on secrets.



The **Unix Account (SSH Key Rotation)** and **Unix Privileged Account (SSH Key Rotation)** Secret templates use password changers that change the public key in the account's authorized_keys file as well as change the password on the account. IBM Security Verify Privilege Vault ships with a password changer and custom command sets that allow an account to change its own public key and password, and a password changer and custom command sets that changes a user's public key and password by using a privileged account. These scripts can be customized for different Unix environments.

For more information about SSH Key Rotation, see our SSH Key Rotation and SSH Key Rotation Quick Start KB articles.

Launcher

IBM Security Verify Privilege Vault's Launcher opens a connection to the remote computer or device or logs into a website by using the Secret's credentials directly from the Web page. While this provides a convenient method of opening RDP and PuTTY connections, it also circumvents users being required to know their passwords. A user can still gain access to a needed machine but is not required to view or copy the password out of IBM Security Verify Privilege Vault. The Web Launcher will automatically log into websites by using the client's browser.

Built-In Launcher Types

Remote Desktop
Launches a Windows Remote Desktop session and automatically authenticates the user to the machine.

PuTTY
Opens a PuTTY session and authenticates the user to a Unix system.

Web Password Filler
Uses a bookmarklet or a Chrome extension to automatically log the user into a website with Secret credentials. The Web Password Filler section has more detailed information.

Enabling the Launcher

By default, the Launcher is enabled by the Enable Launcher setting under Administration > Configuration.

The Launcher can be deployed in two ways – either with the ClickOnce application or Protocol Handler application. This can also be configured in the Configuration settings. Protocol Handler allows the Launcher to be used in virtualized environments, or any environment in which the user does not have access to a Windows Temp directory. The Protocol Handler can be downloaded from the Tools > Launcher Tools page. For details on use and deployment of Protocol Handler, see the Protocol Handler Launcher KB article.

Remote Desktop Launcher

Browser Configuration

Firefox Configuration
Firefox requires a Helper Add-on application to run the RDP and PuTTY Launcher. The Microsoft .Net Framework Assistant add-on and .NET framework version 4.5.1 SP1 needs to be installed.

Chrome Configuration
If using ClickOnce Chrome requires a Helper Add-on application to run the RDP and PuTTY Launcher. The ClickOnce add-on for Google Chrome Add-on needs to be installed. The launcher requires .NET framework version 4.5.1 SP1 as well.

SSL Certificates

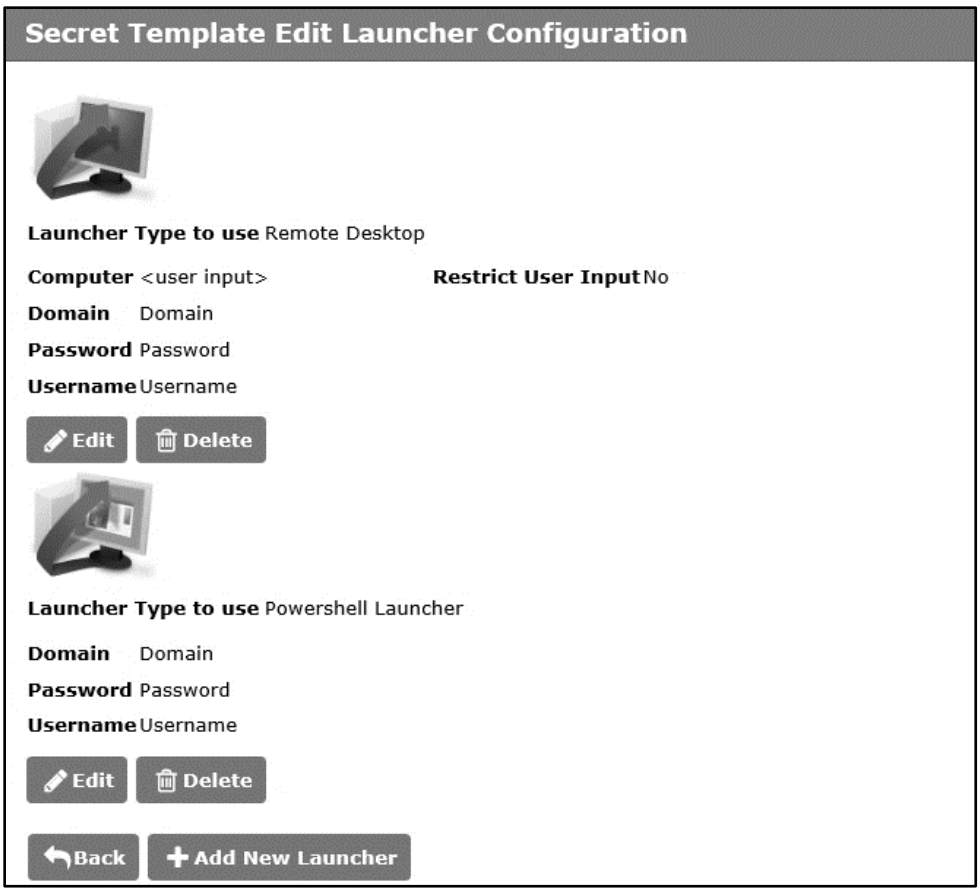
SSL must be set up properly for the RDP launcher to work correctly. If IBM Security Verify Privilege Vault is using SSL certificates, they must be trusted at the user's computer. This will only be an issue with self-created certificates.

Setting Up the Secret Template

Launchers can be accessed from any Secret created from a properly configured template. By default, the templates Windows Account, Active Directory Account, Cisco Account (SSH), HP iLO Account (SSH), Unix Account (SSH), Web Password, and SQL Server Account have the launcher that is configured. Secrets can be configured for the Launcher from within the Secret Template Designer page. Clicking **Configure Launcher** displays the options available.

Add a Launcher

Click Add New Launcher to add a Launcher to the template. On the following page, select a Launcher type from the drop-down menu. The fields below will reflect the fields necessary to map to the Launcher. In the case of a custom Launcher, these fields will be used to run the Launcher process if the Launcher is configured to run as Secret credentials. Choose a Secret field in the drop-down menu on the right to map to each Launcher value on the left. See the following section for further details on editing Launcher configuration. Click Save to add the Launcher to the template.



Edit a Launcher

Click Edit to modify the settings for a Launcher that has already been added to the template. For a Launcher to work properly, IBM Security Verify Privilege Vault requires the appropriate credentials to be taken from Secret fields. Fields must be assigned their corresponding credentials from the drop-down list. In addition to the Secret Fields, the Domain can be mapped to <blank> which passes empty string to be used with Local accounts, and the machine or Host can be mapped to <user input> which prompts the user for a specific machine to be used with Domain accounts.

In cases where there are multiple endpoints to connect to, such as with a domain account, the machines can be restricted to a set list. Under the **Advanced** section of the Secret Template Launcher configuration, enable **Restrict User Input**. When that option is on, the Launcher will show a drop down of machines to connect to, based on a comma-separated list in the specified Secret Field.

Session Recording

Session recording provides an additional level of security by recording a user's actions after a launcher is used. Session Recording will work for any launcher, including PuTTY/SSH, Windows Remote Desktop, Microsoft SQL Management Studio, and custom executables. The resulting movie is viewable from the secret audit. Session recording can be toggled on or off globally on the Configuration page, and set for individual secrets on the

Security tab. Detailed information on supported codecs can be found in the Session Recording KB article. When a user launches a session with session recording enabled, a brief message is displayed to inform the user that their actions will be recorded.

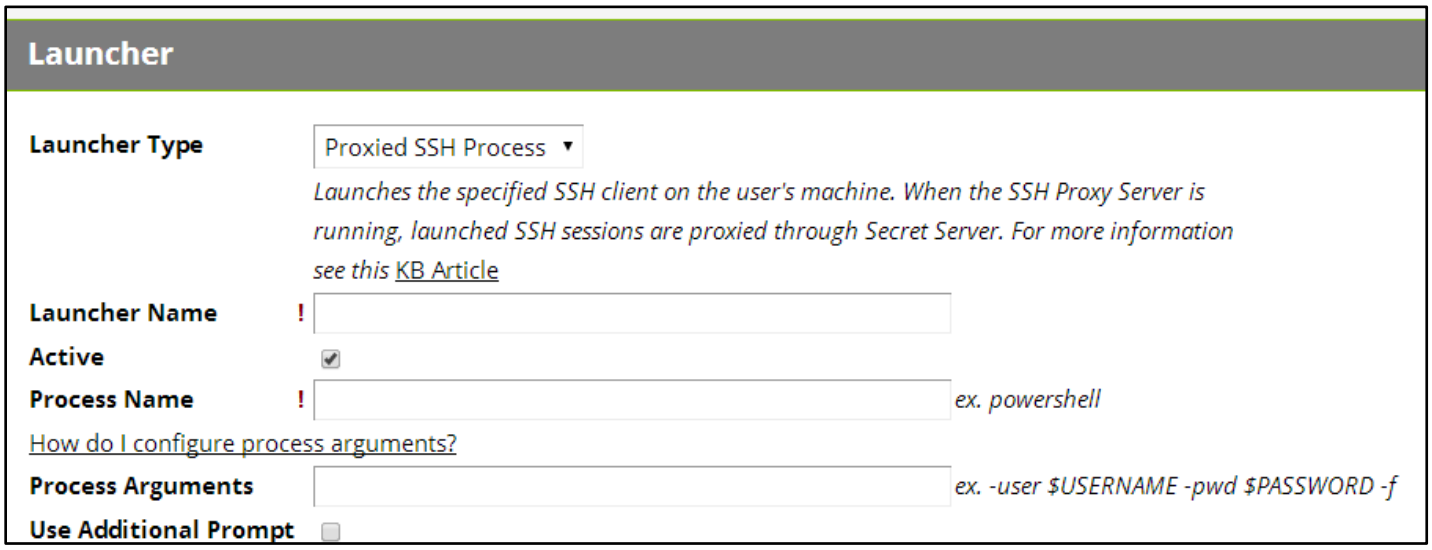
When multiple Launchers are enabled for a Secret template, enabling session recording for a Secret will apply the setting to all Launchers for that Secret.

Custom Launcher

IBM Security Verify Privilege Vault can wire up a program to run when clicking the Launcher on a Secret. Custom process Launchers can be customized to work with any application that can be started by command-line and will pass values to the command-line from the Secret fields. In order for process Launchers to work, the client machine must have the program installed and typically needs the program folder in the PATH environment variable.

There are three types of custom launchers to choose from:

- **Process**
  Launch a process on the client machine that will connect directly to the target system from the client.
- **Proxied SSH Process**
  Launch a process on the client machine that will proxy its connection to the target system through IBM Security Verify Privilege Vault.
  See SSH Proxy for more information about configuring IBM Security Verify Privilege Vault as a proxy.
- **Batch File**
  Launch a batch file from the client machine.



To create a new Custom Launcher, select **Secret Templates** from the **Administration** menu and click the **Configure Launchers** button, then click **New**. The following settings are available:

Launcher Name	Friendly name of the launcher that will be displayed to the user.
Active	Whether or not the Launcher is active for use.
Launcher Type	Select Process, Proxied SSH Process, or Batch File.
Process Name	Name of the process that will be launched.
Batch File	As an alternative to opening a process, upload a .bat file that will be downloaded and executed on the client when the user runs a launcher. The file will be deleted from the client after execution.
Process Arguments	Process arguments depend on the process that is being launched. View the built in SQL Server Launcher for examples on how the fields are substituted. For greater flexibility, other Secrets can be linked on the Launcher tab on the Secret. The field values from those Secrets can also be used in the Process Arguments by using the same prefix $[1][FieldName] syntax as the SSH custom commands. Introduced in 8.1.000035 is a launcher specific token $SESSIONKEY that can be passed to the command line. This passes an identifier to the customer launcher that can be used to anonymously check in the Secret using the CheckInSecretByKey Web Service method.
Run Process As Secret Credentials	If set to true, the process will authenticate as the credentials on the Secret instead of the client user that is using the launcher. This can be overridden at the Secret level to use a privileged account to run the process.
Use Additional Prompt	If enabled, the user will be prompted for additional information when using the launcher.
Additional Prompt Field Name	Name of the field that will be prompted for when the user uses the launcher. This value can be referenced in the Process Arguments with a $ prefix.

Default Launcher Requirements

- **SQL Server Launcher**
  Requires SQL Server Management Studio installed. When installed, the program will be automatically added to the PATH (by default uses 2008).
- **Powershell Launcher**
  Requires Powershell installed. When installed, the program will be automatically added to the PATH.

- **Sybase isql Launcher**
  Requires isql.exe installed.

How to Add a Program Folder to the PATH?

Right click Computer and go to Properties. In the properties window click Advanced system settings. On the Advanced Tab, click the Environment Variables button. In the System Variables section scroll to Path. Click Edit then at the very end of the Textbox, paste the full path to the folder where the program file is located but make sure not to replace any existing entries. The list is semi-colon separated. Click OK to close the dialogs.

Common Errors

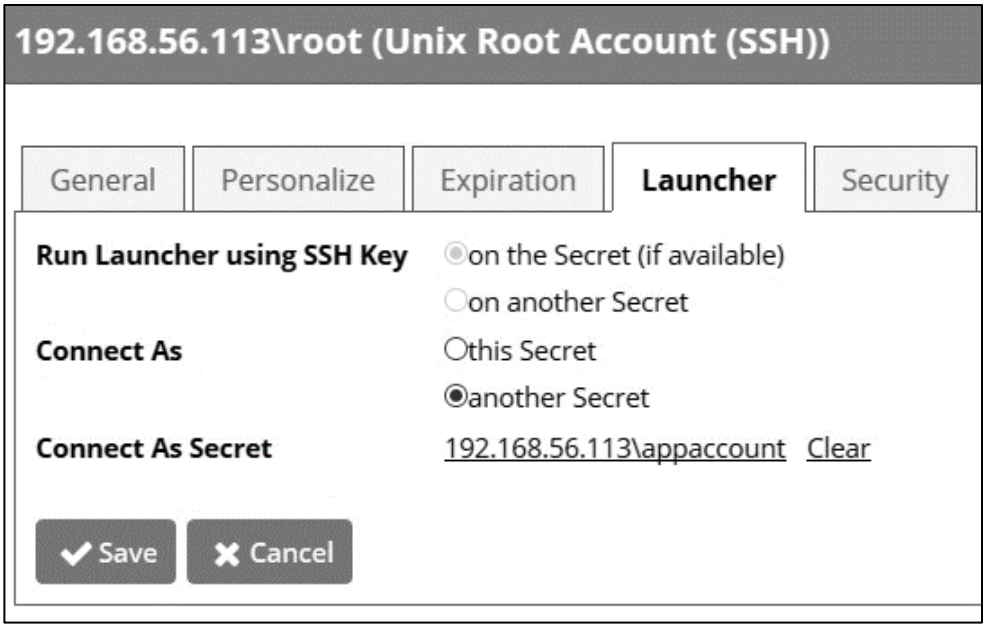
- **The process (process name) was not found**
  The application has not been installed on the machine. If the application was installed, the program folder must be added to the path.
- **The stub received bad data (1783)**
  The process is set to Launch As the Credentials of the Secret but the username or domain is not correct on the Secret or the client machine cannot find the user or domain credentials specified.

Configuring a Launcher on the Secret

Custom and SSH launchers provide additional settings on the Launcher tab of the Secret for customizing authentication to the target.

SSH

- **Run Launcher by using SSH Key:** If there is an SSH key set on the Secret, it will be used by default for authenticating to the target. Alternatively you can specify a key from a different Secret. For more details about SSH keys, see SSH Key Authentication.
- **Connect As**: When an SSH Secret is proxied, you can choose to connect as another user and then do an **su** to the current Secret's user. This is a common practice for connecting with a lower privileged account and then switching to the root user.

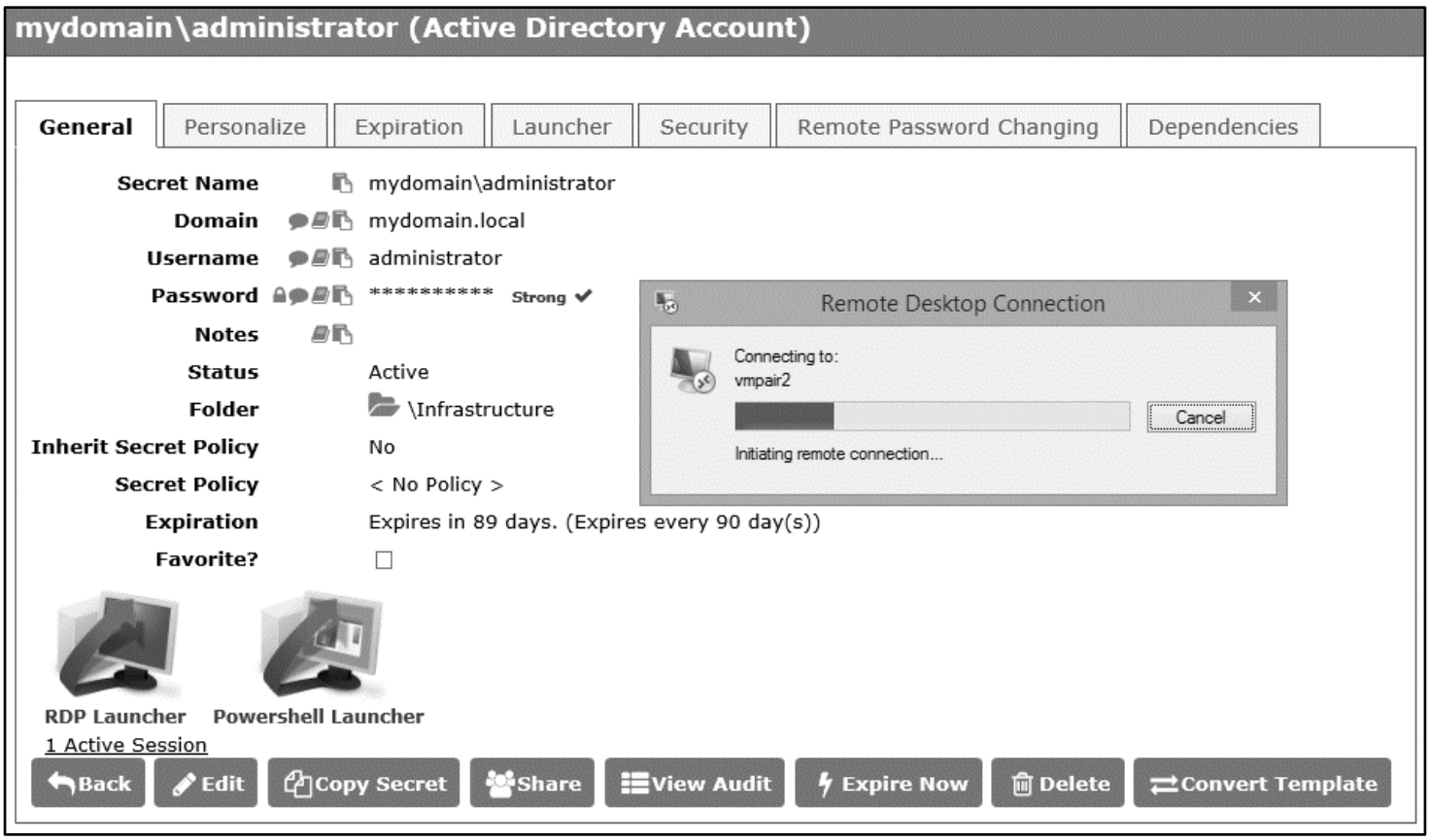


Starting a Session

On the Secret View page, clicking the Launcher icon will launch the Remote Desktop, PuTTY, or custom session directly from the browser or log into the website. The mapped fields will be passed to the Launcher for automatic authentication. If the machine is set to <user input> for Remote Desktop, the console will launch and allow the machine to be specified from the RDP dialog. If the Host is set to <user input>, a prompt will ask for the specific machine before launching the PuTTY session. For certain browser security levels, the user must click Allow for the Launcher application to open.

The View Launcher Password permission can be removed to prevent users from viewing the credentials but will still be able to use the authentication session to access the computer.

The settings under the Launcher Tab are used for Secrets that are enabled for SSH and Custom Launchers.



SSH Proxy

Launchers by using an SSH connection can alternatively use IBM Security Verify Privilege Vault as a proxy rather than the launcher connecting directly to the target system from the machine it is being launched from. Starting with version 8.9, when Proxying is enabled, all RDP sessions will be routed through IBM Security Verify Privilege Vault. In IBM Security Verify Privilege Vault the Distributed Engine service also supports acting as a proxy for session launchers for greater network flexibility and offloading connections from the IBM Security Verify Privilege Vault instance. To configure this, select **SSH Proxy** from the **Administration** menu and click **Edit** to enter your configuration settings:

SSH Bind IP Address

The IP Address of the network adapter that the IBM Security Verify Privilege Vault SSH listener should bind to. This should not be localhost or 127.0.0.1.

If you are not sure which bind IP Address to use, you might use 0.0.0.0, which will bind to all IPv4 interfaces on the machine.

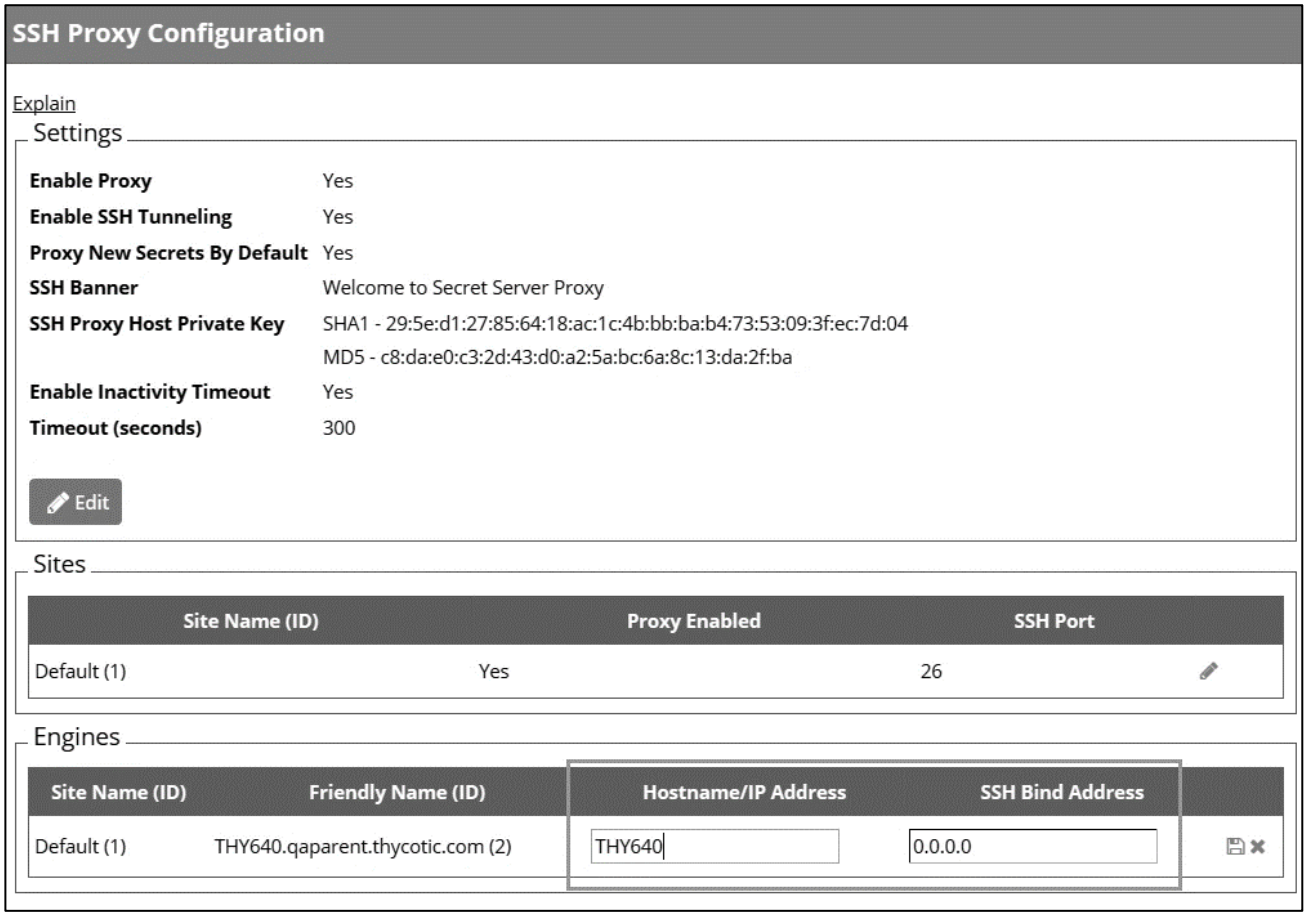
SSH Public Host

The public hostname or IP that the client launcher will connect to. In most cases this can be the same as the SSH Bind IP, however there might be cases where the public IP or host differs than the private IP that IBM

	Security Verify Privilege Vault should bind to (NAT, Amazon EC2 instance, and so on).
Enable SSH Tunneling	SSH Tunneling allows Remote Desktop Sessions to be proxied by using the same proxy configuration settings.
Proxy New Secrets By Default	This setting will determine whether or not newly created Secrets will have proxy enabled; Secret Policy will take precedence over this default.
SSH Proxy Port	The port IBM Security Verify Privilege Vault will listen on. Default is 22.
SSH Banner	Users connecting through IBM Security Verify Privilege Vault will see this as a banner on the SSH client.
SSH Proxy Private Key	The IBM Security Verify Privilege Vault SSH private key, this can be generated by using the corresponding button.
Inactivity Timeout	Closes the session if there is inactivity for a certain number of seconds.

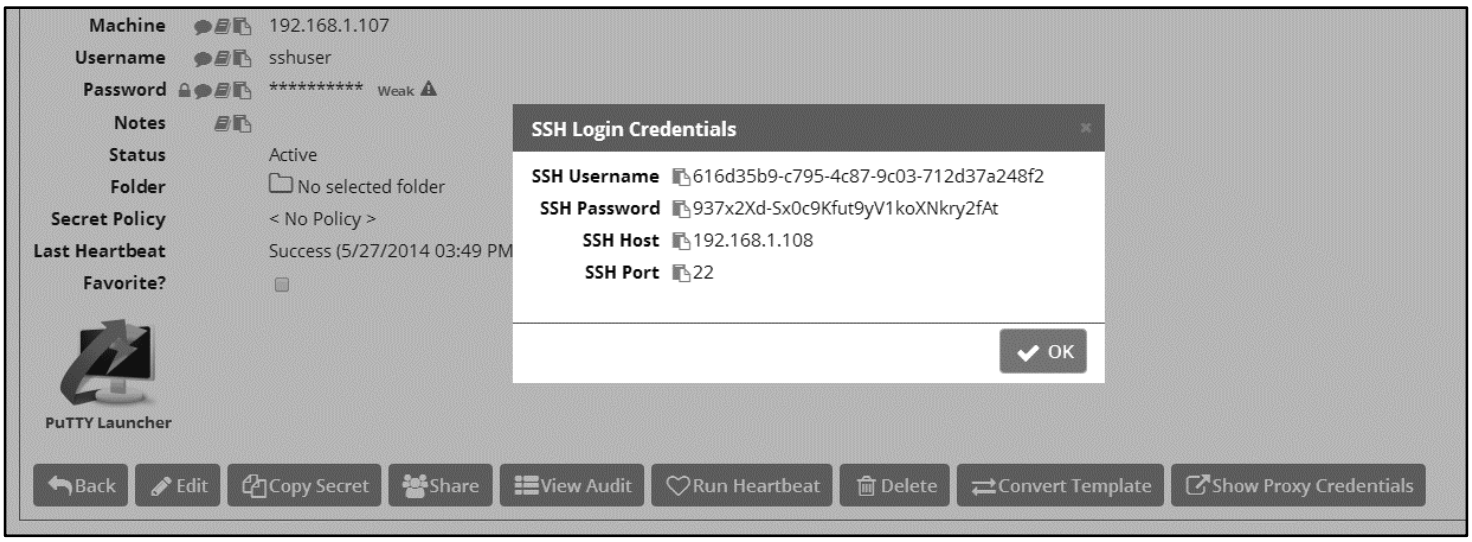
To enable Secrets assigned to a Site edit the corresponding Site and check the box for Proxy Enabled and optionally specify a custom SSH Port.

The engines in that site now show up and you can configure the Public Host and Bind IP on each one. The default values are the FQDN of the machine and 0.0.0.0 which should work for many internal connections but might need to be edited depending on how users are connecting to them.



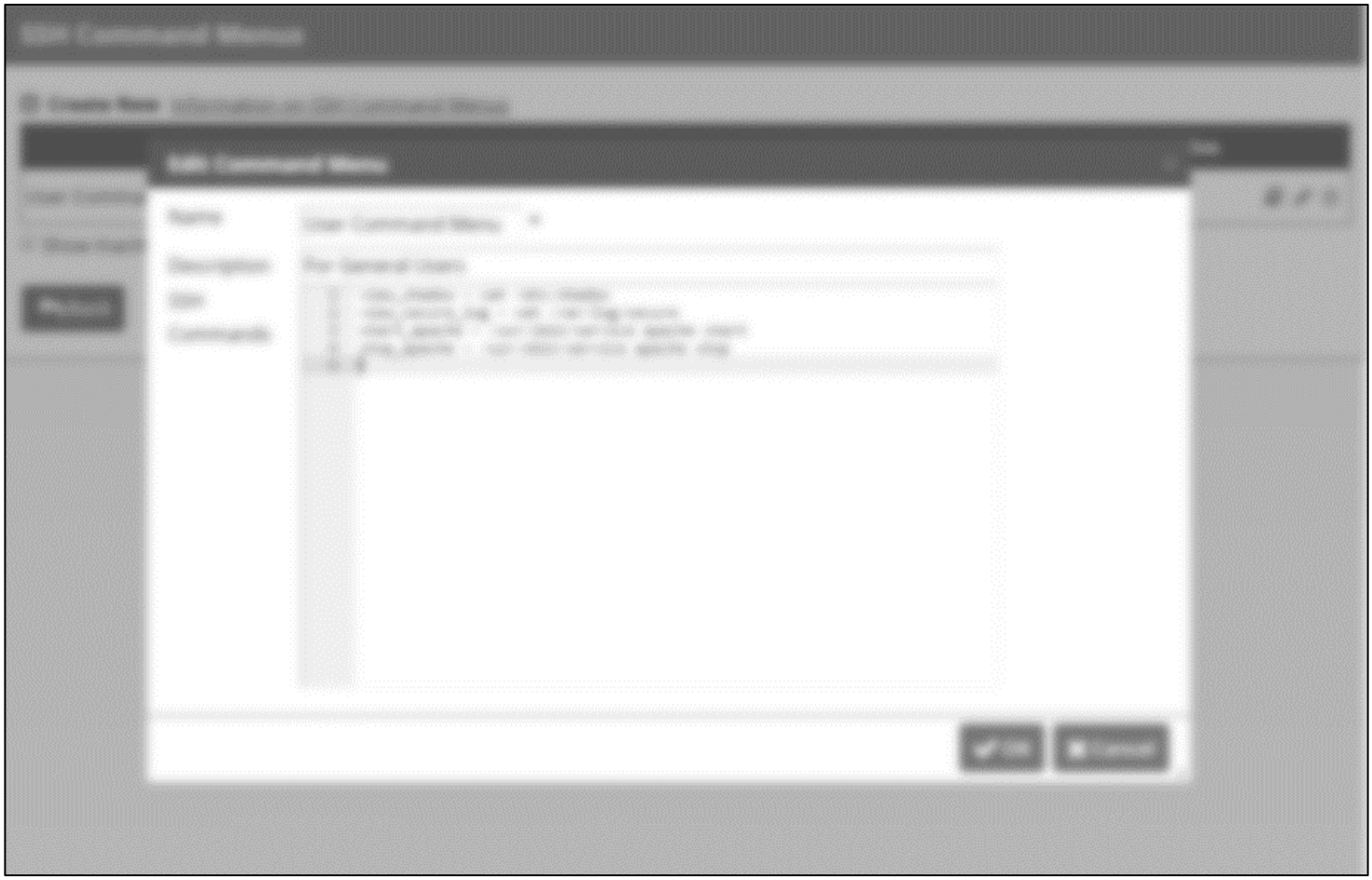
The flow for when a user proxies through an Engine rather than the IBM Security Verify Privilege Vault is the same, except that rather than the user's session launcher connecting to the Public host on the Node, it connects to the Public Host of an engine that is part of a Site the Secret is assigned to.

Once SSH Proxy has been configured, Secrets by using an SSH Launcher will have an additional **Show Proxy Credentials** button available. Clicking this button displays credentials that can be used to connect through IBM Security Verify Privilege Vault to the target system, in case a user would like to start an SSH session manually.



SuperUser Privilege Management

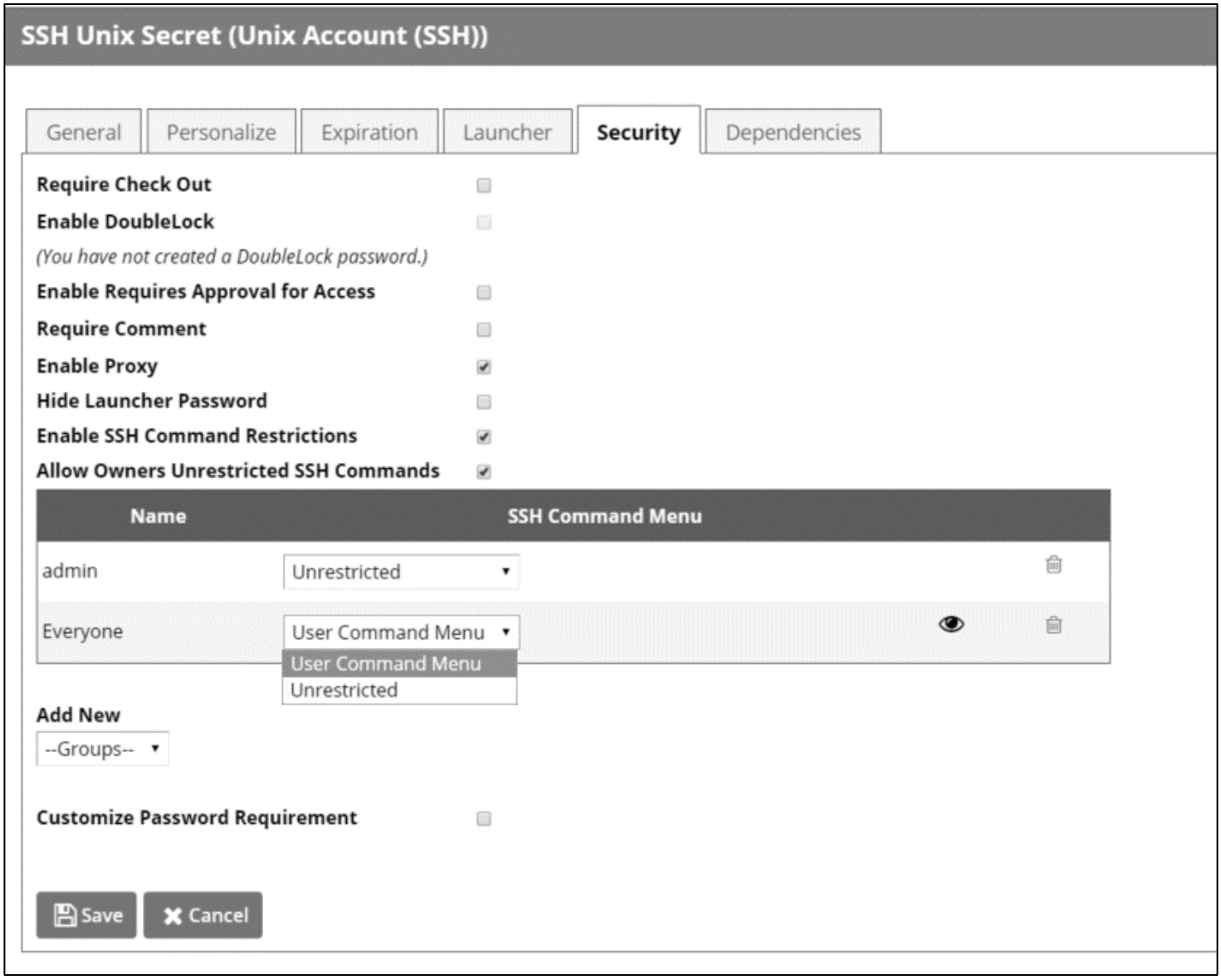
Administrators can create command menus for use with a proxied SSH connection to restrict what commands can be run by users or groups on the connected server. This feature requires an additional license. To add a command menu, navigate to “SSH Command Menus” on the Admin page.



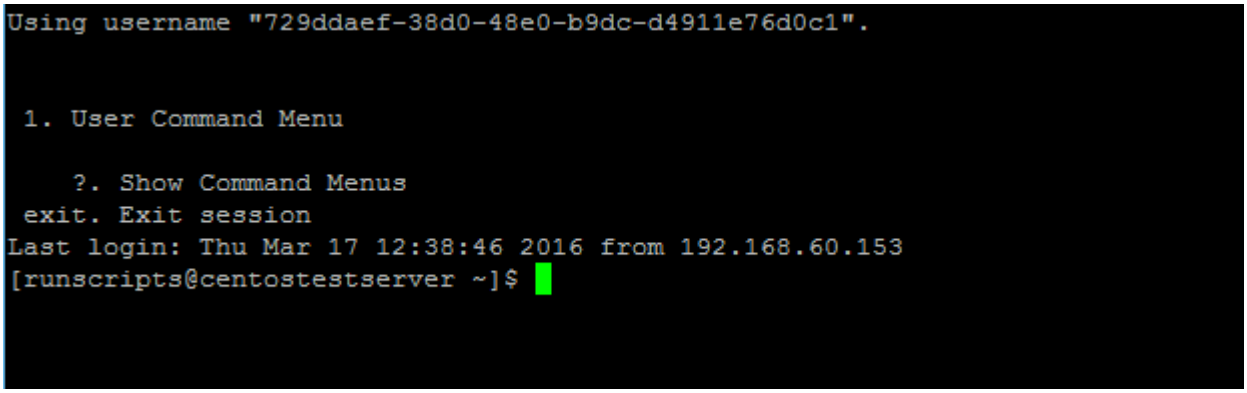
Once one or more Command menus have been created, access can be controlled to individual Unix SSH secrets.

On the “Security” tab of a secret that is able to use a proxied PuTTY session, proxy must be enabled as well as command menu restrictions. If “Allow Owners Unrestricted SSH Commands is enabled, any user who is an owner of the secret will have unrestricted use of the PuTTY session, i.e. that user will be able to type in commands as in a normal session. Additionally, other groups can be assigned the “Unrestricted” role as well.

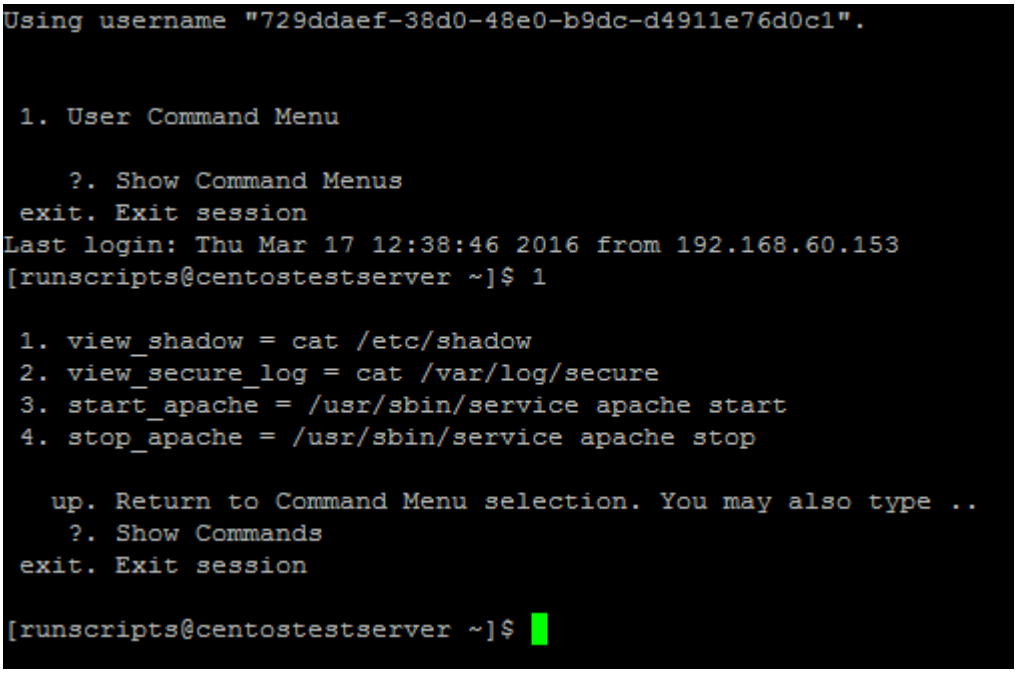
In the following example, the “admin” group will be unrestricted, while everyone who is not in the admin group will be restricted to only being able to run the commands that are enumerated in the “User Command Menu,” created above.



A user who is subject to SSH Command Restrictions will be presented with a screen like the following when connecting to a SSH session:



The user simply enters the number of the command menu to see available commands, or types “?” to display the options again.



Only the commands listed can be run by this user. The user can either enter the number of the command to be run, or the name of the command, which is the word to the left of the equal (=) sign. Other options are available (as shown) to navigate through the available command menus, display help, or exit the session.

Web Password Filler

The Web Password Filler is a login helper that can be used on any web site with a login. To use the Web Password Filler you need install the browser extension for Chrome or Firefox. For Internet Explorer you need to drag a link to the bookmark bar of your browser. The link is available by going to any secret which uses the Web Password Secret template or any other Secret template that has a searchable URL field.

Chrome

Install the extension by clicking on the web launcher icon on a Web Password Secret or install the extension in Chrome from the Chrome store

Firefox

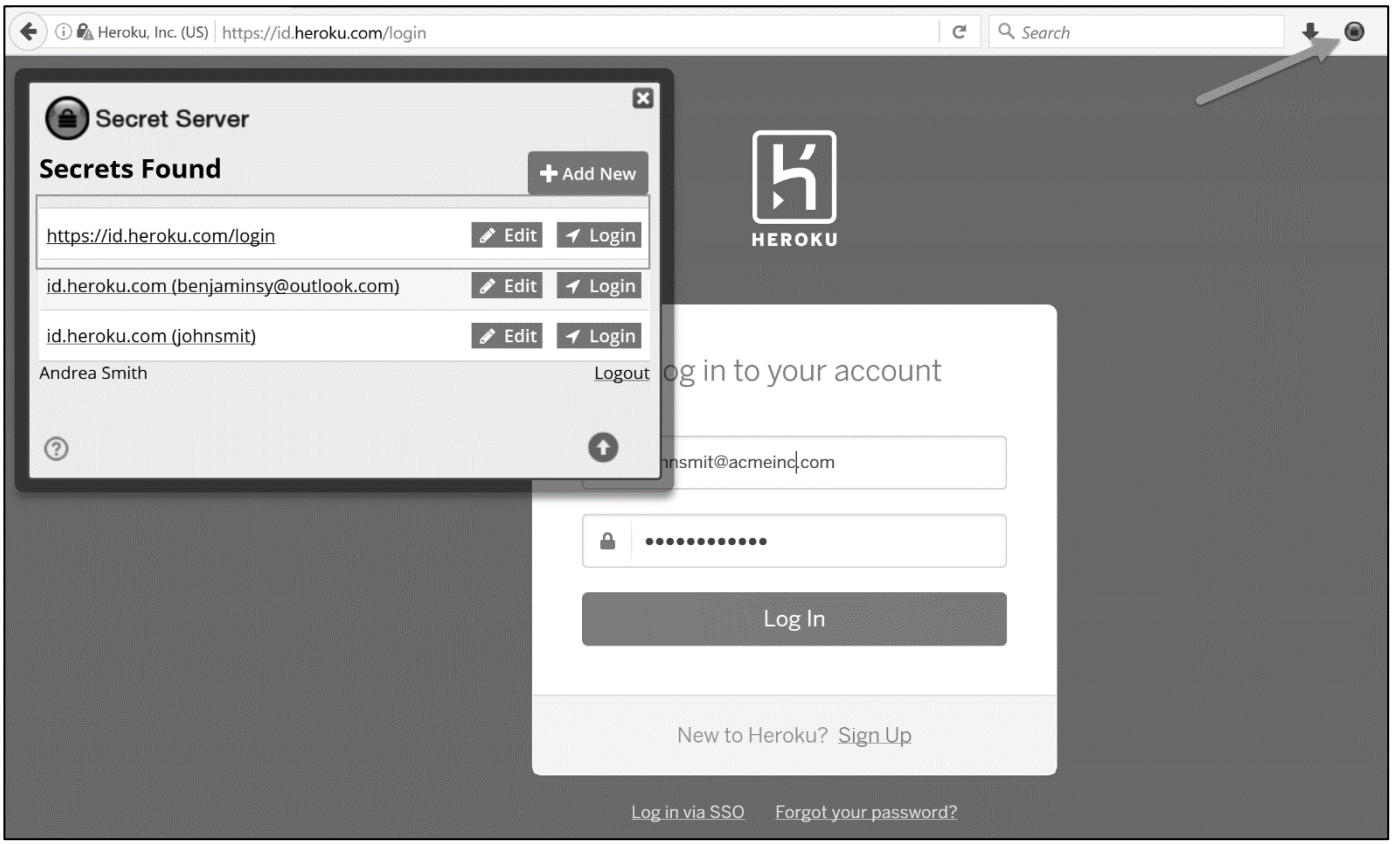
Install the Firefox add on by clicking on the web launcher icon on a Web Password Secret or install the add on from the Firefox listing

Internet Explorer

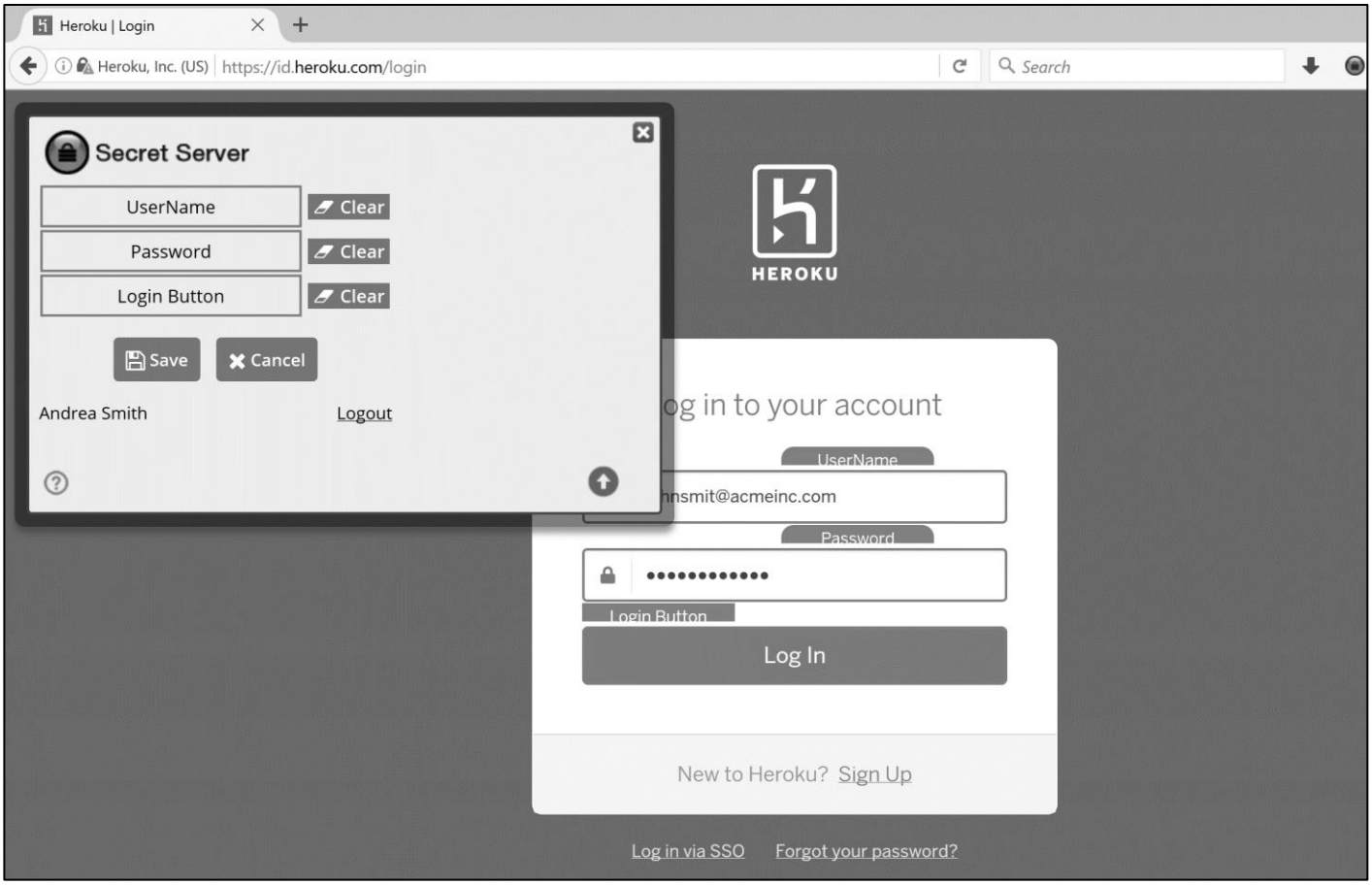
Drag the link from **Tools | Launcher Tools** for the web password filler to the bookmark bar to create a bookmarklet.

Using the Web Password Filler – Firefox & Internet Explorer

Once you have the bookmarklet or extension installed it is ready to use. Navigate to the login page of the website you want to log in to, and then click the extension icon or bookmarklet link. A dialog will open on the login page with the Web Password Filler. The Web Password Filler will show you available Secrets that match the current URL for you to login with. Click the login button or the Secret Name to complete the username and password.



If the Web Password Filler is unable to correctly fill in the username and password fields you can manually set the mappings from the Secret fields to the website fields by clicking the Edit button on a Secret and selecting a Secret field and then clicking on the correct field in the login form.

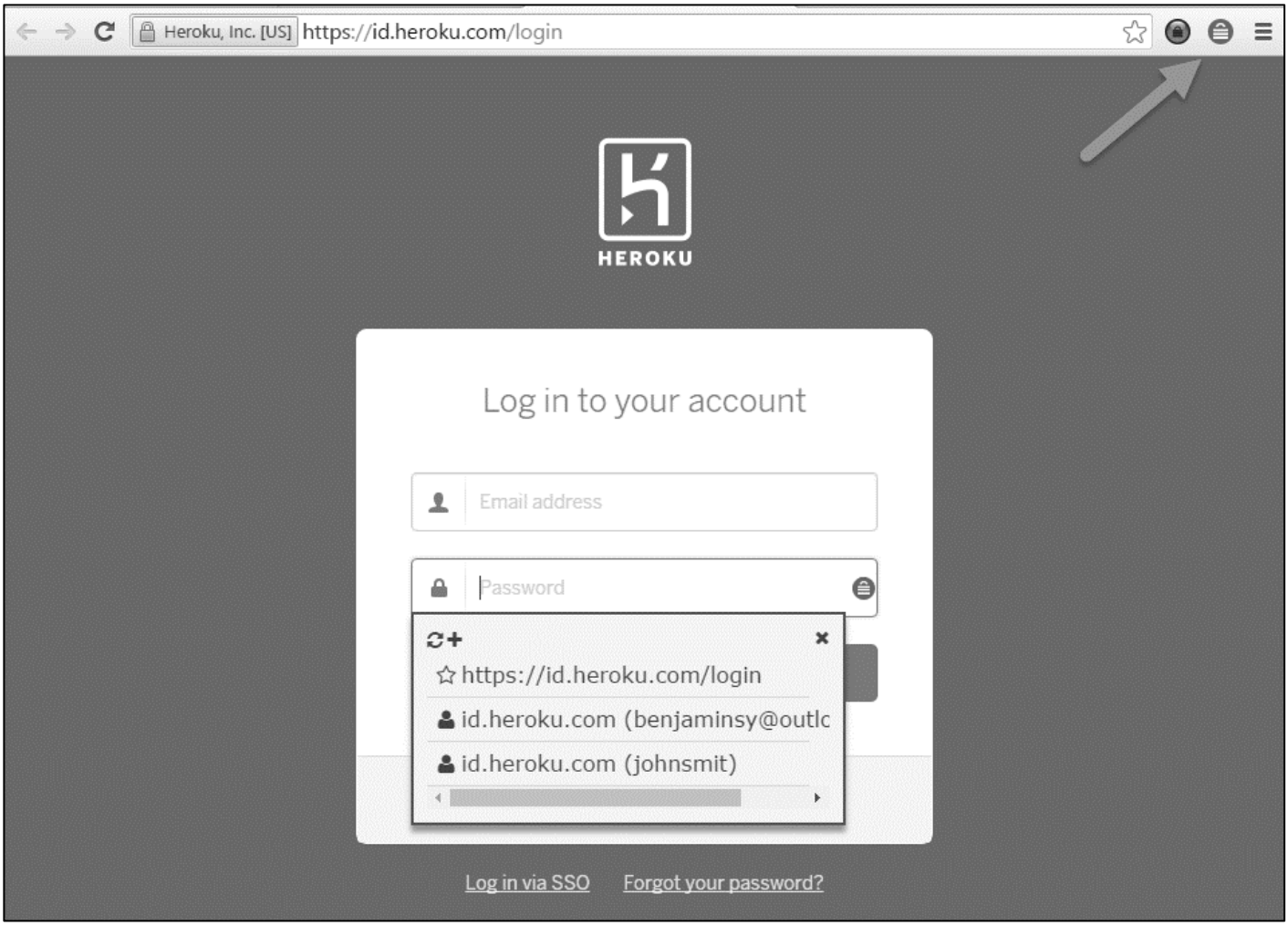


If no Secrets exist, you can click the extension and then click the **Add New** button to create a Secret for that URL.

Using the Web Password Filler – Chrome

As of IBM Security Verify Privilege Vault 9.1 the Chrome extension has new behavior. Rather than having to click the extension to bring up a list of Secrets, login forms are populated with a Secret lock icon that you can click to bring up a list of Secrets.

Secrets are prioritized based on whether they are marked as Favorites, are in your Personal Folder, and then by URL.



To add a Secret if none exist, click the **+** symbol in the Secret List.

Web Launcher

The Web Launcher is a separate method of login from the web password filler and provides a convenient click to automatically log into websites, but will not work on complex login pages that rely on JavaScript. For those login pages use the bookmarklet or browser extension for the Web Password Filler. By default, the web launcher is enabled on the Secret template Web Password, but can be enabled on custom templates as well as described in Enabling the Launcher.

Configuring the Web Launcher for a Secret

Once enabled on the template, the Web Launcher must be configured for the Secret. Each website login is unique and will require the Secret fields to be mapped to the form controls. For a new Secret the Launcher icon appears and clicking on it will take the user to a configuration screen. The user can also view and access the configuration screen from the Launcher Tab. Depending on whether other Secrets with the same website have been configured, the user will have different options.

Configuring the Secret for use with the Web Launcher requires the user to have Owner permission on the Secret.

First, there is the option of downloading the setting. When the Configure Web Launcher page is loaded, IBM Security Verify Privilege Vault will check online for pre-approved matching websites. If any are found, they are downloaded and made available to pick from in the dropdown list.

This functionality can be disabled in IBM Security Verify Privilege Vault in the Configuration Settings. See the Configuration Settings section for further details.

The drop-down list will list all downloaded configurations and other Secrets' configuration for the same domain that the user has permission to view. Select one from the drop-down list and click Next to create a copy of the settings for the Secret.

There is also an option to create a configuration which will allow the Web Launcher to be used on most websites and not rely on published configuration settings. In order to use this, select the last item in the dropdown list and click Next. The next section will discuss the create process.

Creating a Configuration

Entering the Login URL

IBM Security Verify Privilege Vault needs to know the exact URL used to login to be able to figure out the controls and perform the automatic login. Some example login URLS:

- https://login.yahoo.com/config/login
- https://MyServer/Billing/login.aspx
- https://firewall07/login/

The Login URL is typically a secure site with a prefix of https://. If allowed to access the site, IBM Security Verify Privilege Vault will automatically detect if https should be used to ensure the credentials are passed securely.

Providing the Page Source

If IBM Security Verify Privilege Vault is not allowed access to sites, or the login URL is not accessible by an external site, the page source must be provided for the Web Launcher controls to be obtained. Ensure the login URL is correct when the page source is taken. If the site can be accessed by IBM Security Verify Privilege Vault, the page source will be automatically obtained and this step will not be present.

Choosing the Form
The page will be read and the exact login form must be identified. The page forms will be listed in the drop-down list with the most likely selected. If no forms or no likely forms are found, the user must update the URL or page source, as configuration must have at least one textbox and one password box.

Wiring Up the Fields to Controls
In most cases IBM Security Verify Privilege Vault will automatically wire up the Username and Password fields to the correct page controls. If not, the user will complete the control mapping on the Launcher tab.

Starting to a Website

The Web Launcher can be used by clicking the Launcher icon on the Secret View page. The Web Launcher will open a new window in the browser which will attempt to login to the site by using the credentials on the Secret. The Launcher can also be used with the Test Launcher button on the Launcher Tab. Testing the Launcher will create a dialog to offer troubleshooting help and means to upload the configuration. The uploaded configuration will be reviewed and published for all IBM Security Verify Privilege Vault users to use with the Check Online feature. No Secret or identifiable information is uploaded online. Only the website URL and control names are sent.

Setting up Password Masking

Password Masking prevents over the shoulder viewing of your passwords by a casual observer (passwords show as *******). Note the number of asterisk does not relate to the length of the password for added security.

As an administrator, you can force all the Secret Password fields in the system when viewed to be masked. To do this, enable the Force Password Masking setting in the Configuration settings. Only Secret fields marked as a password field on the Secret template will be masked.

There is also a user preference setting which will force password masking on all Secret Password fields viewed by the user. This Mask passwords when viewing Secrets setting is found in the Profile > Preference section for each user. Note that if the Configuration setting discussed above is enabled, this user preference setting will be overridden and cannot be disabled.

See the Viewing a Secret section for instructions on unmasking the password by using the lock icon.

Secret Expiration

A core feature of IBM Security Verify Privilege Vault is Secret expiration. Any template can be set to expire within a fixed time interval. For a Secret to expire, a field must be selected as the target of the expiration. For example, a Secret template for Active Directory accounts might require a change on the password field every

90 days. If the password remains unchanged past the length of time specified, that Secret is considered expired and will appear in the Expired Secrets panel on either the Dashboard's Expired Secrets widget or the Home page.

Secret expiration provides additional security by reminding users when sensitive data requires review. This can assist in meeting compliance requirements that mandate certain passwords be changed on a regular basis. When expiration is combined with Remote Password Changing, IBM Security Verify Privilege Vault can completely automate the process of regularly changing entire sets of passwords to meet security needs.

Setting up Secret Expiration for the Secret template

To set up expiration on a Secret, you must first enable expiration on the template from which the Secret is created.

To enable Secret expiration for a Secret template, navigate to Administration > Secret templates. In the Manage Secret templates page, select the template from the dropdown list and click the Edit button. In the Secret Template Designer page, click the Change link. On this subsequent page, check the Expiration Enabled? box. You can now enter the expiration interval (every x number of days) as well as the field on the Secret you want to expire and require to be changed. The interval setting can be overridden for each individual Secret (see below).

Enabling expiration for a template will enable expiration for all the Secrets that were created by using this template.

Setting up Secret Expiration for the Secret

Now that expiration has been enabled for the template, Secret expiration is enabled for the Secrets that were created by using that template as well as Secrets created in the future. The Expiration tab appears on the Secret View page and requires the user to have Owner permission on the Secret. If you would prefer to set a custom expiration at the Secret level, you can adjust the interval of expiration for the Secret by clicking the Expiration tab in the Secret View page. In the Expiration tab, you can set the Secret to expire by using the template settings (default), a custom interval, or a specific date in the future.

Forcing Expiration

To force expiration, navigate to the Secret View page. From there, click Expire Now. This will force the Secret to expire immediately regardless of the interval setting. The expiration date will read "Expiration Forced".

Resetting an Expired Secret

To reset an expired Secret, you must change the field that has expired and is required to change. For example, if the field set to expire is the Password field and the current Password is "asdf", then a change to "jklh" will reset the expiration interval and thus remove the expiration text on the Secret View page.

If you do not know which field is set to expire, you must go to the Secret template that the Secret was created from. Navigate to Administration > Secret template and select the template. Click the Edit button and then on the next page, click the "Change" link. In the "Change Required On" textbox you will see the field that is set to expire.

DoubleLock

DoubleLock provides an additional layer of security by encrypting Secret data with a custom encryption key that is only accessible with an additional password, regardless of permissions or physical access to the machine running IBM Security Verify Privilege Vault. DoubleLock uses private/public key encryption technology to securely share access to the DoubleLock among users when access is granted.

Creating a DoubleLock Password

Before creating a DoubleLock, you must create a DoubleLock password. This password will be used to generate DoubleLock keys that encrypt sensitive secrets.

Any reference to a password while using DoubleLock will refer to this DoubleLock password, not the user's IBM Security Verify Privilege Vault login password.

Creating a DoubleLock

A DoubleLock is the entity key used to encrypt a given Secret and allow assigned users access to the encrypted Secret.

As an Administrator, to use the DoubleLock functionality on your Secrets, you must first create a DoubleLock. To do that, navigate to Administration > DoubleLock. If you have not created a DoubleLock password yet, you will be prompted to create one.

Before creating a new DoubleLock, you might be prompted to enter your DoubleLock password. After DoubleLock creation, you can assign the DoubleLock to other users who already have DoubleLock passwords. These other users are able to access the Secrets that use this DoubleLock by entering their own DoubleLock password to access each Secret.

Assigning a DoubleLock to a Secret

To assign a DoubleLock, navigate to the Security tab of the Secret View page for the Secret. In there, click the Enable DoubleLock check box. You can now select from a dropdown list the DoubleLock to assign to the Secret.

Changing a DoubleLock Password

A user my change their DoubleLock password by going to Profile > Change DoubleLock Password. The change will update the encryption on the DoubleLock keys for that user and will not affect other users assigned to a common DoubleLock.

Resetting a DoubleLock Password

In the event a user forgets their DoubleLock password, it can be reset by going to Profile > Reset Double Lock Password.

This will result in the loss of access to existing DoubleLocked Secrets.

In the case the DoubleLocked Secret is only accessible by the user, the Secret will be deleted and the data permanently lost, as the password used to encrypt the Secret has been removed. Once the DoubleLock is reset, the other users assigned to a DoubleLock must reassign the user who reset their password.

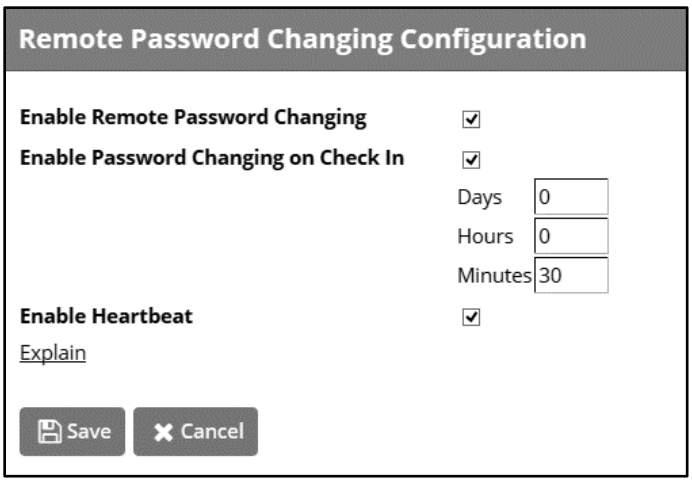
Secret Check Out

The Check Out feature forces accountability on Secrets by granting exclusive access to a single user. If a Secret is configured for Check Out, a user can then access it. If Change Password on Check In is turned on, after "check in," IBM Security Verify Privilege Vault automatically forces a password change on the remote machine. No other user can access a Secret while it is checked out except Unlimited Administrators (see the Unlimited Administration Mode section). This guarantees that if the remote machine is accessed by using the Secret, the user who had it checked out was the only one with proper credentials at that time.

The exception to the exclusive access rule is the assignment of Unlimited Administrator. If Unlimited Administration is enabled, users with Unlimited Administrator Role permission can access checked out Secrets.

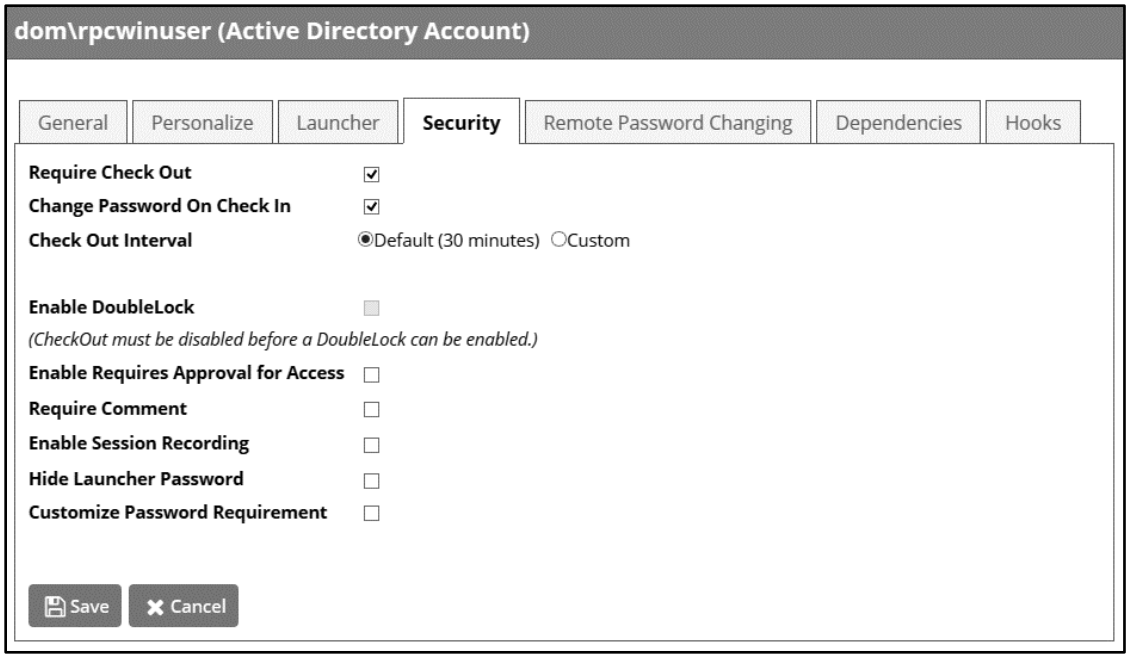
Configuring Password Changing on Check In

To configure Change Password on Check In, navigate to the Remote Password Changing administration page and set Enable Password Changing on Check In. If Remote Password Changing is turned off, it must be enabled before Check Out can be configured. Once Remote Password Changing and Check Out are enabled, Secrets can be configured for Change Password on Check In and Check Out. Optionally, you can also set a Check Out interval that specifies how long a user will have exclusive access to the Secret.



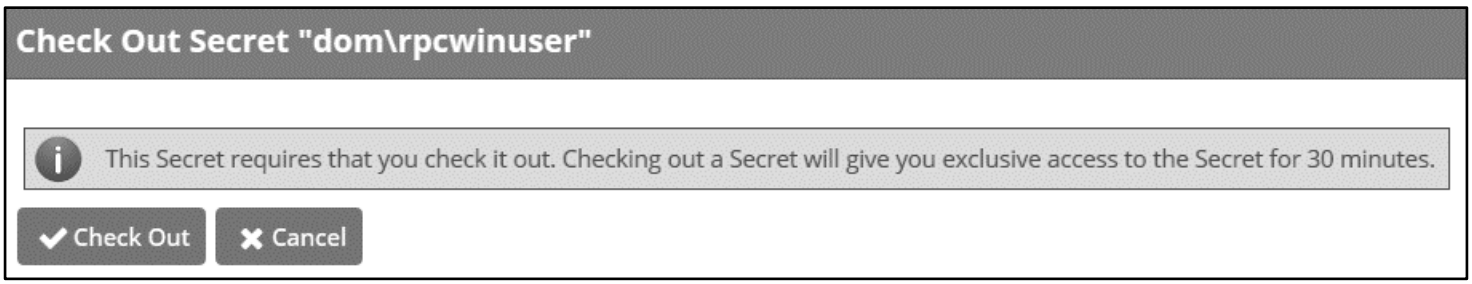
Checking Out Secrets

Each Secret must be individually set to require Check Out. From the Secret View page, open the Security tab to modify a Secret's Check Out setting. The Secret needs to be configured for Remote Password Changing before Change Password on Check In can be set. Enable Require Check Out to force users to check out the Secret before gaining access. And Enable Change Password on Check In to have the password change after the secret is “Checked in.”



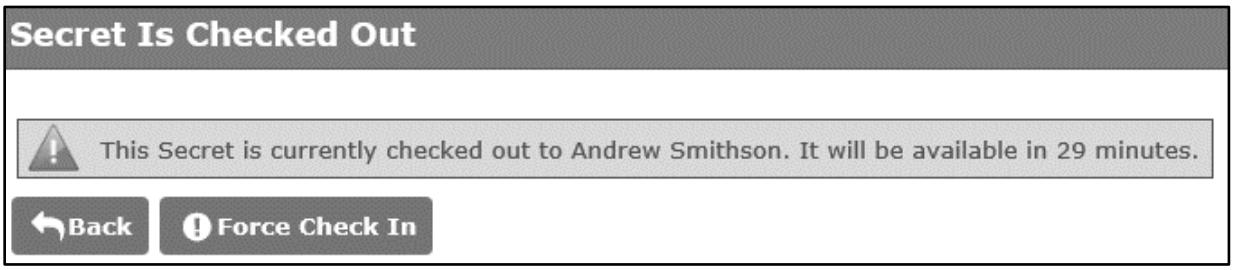
Configuring a Secret for Check Out

After Require Check Out is enabled, users will be prompted for Check Out when attempting to view that Secret.



Exclusive Access

Any user attempting to view a checked out Secret will be directed to a notification dialog informing them when the Secret will be available. IBM Security Verify Privilege Vault automatically checks in Secrets after either 30 minutes or the interval specified on the Secret. Users can check in the Secret earlier from the Secret's page.



Check Out Hooks

In addition to changing the password on Check In, Secret Owners can also specify Administrator created PowerShell scripts to run before or after Check Out and Check In. These are accessed from the Hooks tab of the Secret, which will only show if Check Out is enabled and PowerShell scripts have been created by an Administrator. To specify a Before or After Check Out hook, click Create New Hook and specify the following settings:

Before/After	Whether the PowerShell script should run before or after the Event Action.
Event Action	The Hook will run at either Check In or Check Out.
Name	A descriptive name for the Hook.
Description	An extended description for the purpose of the Hook.
PowerShell Script	Administrator-created PowerShell script to run.
Arguments	Any command line arguments to pass to the PowerShell script.
Stop On Failure	If enabled, IBM Security Verify Privilege Vault will prevent the Event Action if the script returns an error. For example, if Stop On Failure is selected for a Check Out action, then

IBM Security Verify Privilege Vault will prevent the user from Checking Out the Secret if the script fails.

Privileged Account If needed, the script can run as another Secret's identity.

Requires Approval for Access

The Access Request feature allows a Secret to require approval prior to accessing the Secret. Establishing a workflow model, the user will have to request access from the approval group or groups. An email will be sent to everyone in the approval groups, notifying them of the request. The request can be approved or denied by any members of the approval groups. Access will be granted for a set time period. If Owners and Approvers also have Require Approval enabled for their accounts, then even users who are Owners or are in an approval group must request access.

Setting up Access Request for a Secret

To enable Access Request for a Secret, navigate to the Secret View page for the Secret. Go into the Security tab and click the Edit button. You can then check the Enable Requires Approval for Access check box to enable the setting. Once enabled, you must then select users or Groups as Approvers for the Secret. Unless the Owners and Approvers also Require Approval option is turned on, users with Owner share permission for the Secret, or users that are members of the Approvers Group will not need to request access to view the Secret.

Users need at least View access to the Secret to be able to access the Secret even with Access Request enabled. If the users do not have View permission they are unable to find the Secret with Search or Browse.

The email configuration settings must be set up, as well as valid email addresses, for the users in the approval group for the emailing functionality to work.

Requesting Access after Approval is Granted

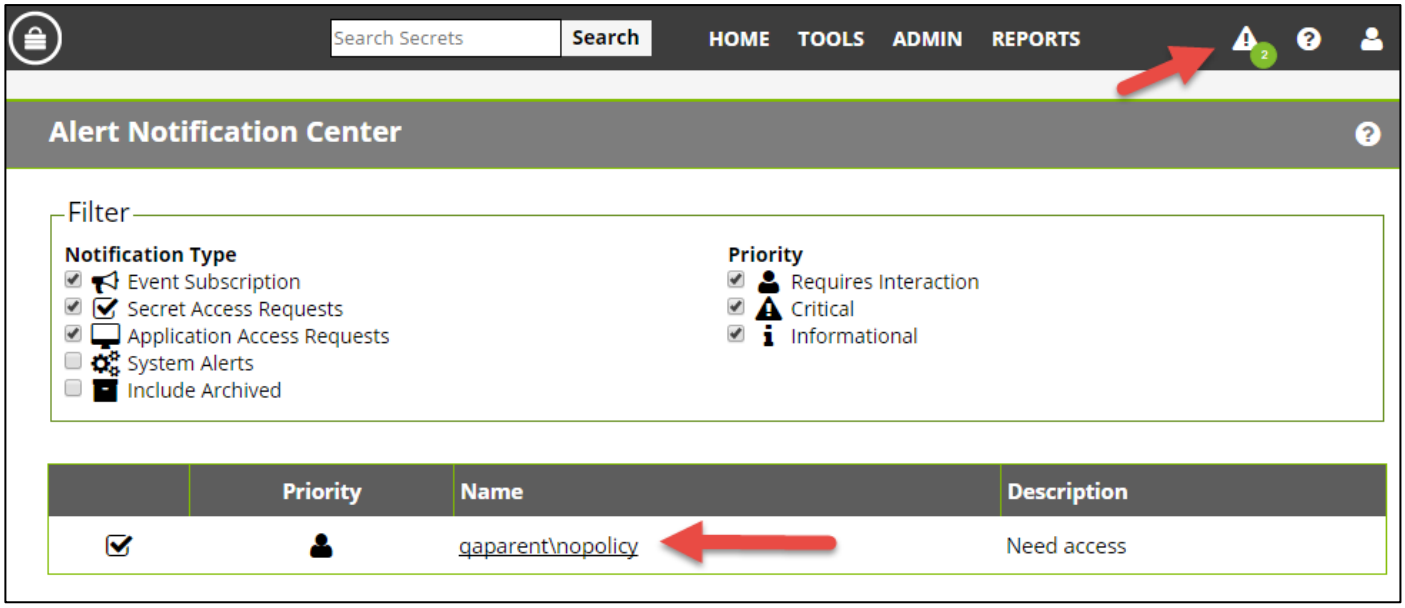
To start the request process for access to a Secret, the user must simply attempt to view the Secret. The user will then be sent to the Request page. In there, the user can explain the reason for the request and then click Request Access to submit the request.

If a member of the Approval Group either approves or denies the request (see below for details), the requestor will be sent an email with the details. If approved, the requestor can access the Secret via the link contained in the email.

Approving a Request

Once a request for access to a Secret has been made, Approvers will receive an email. The email contains one link to the Secret Access Request Approval page for that request in IBM Security Verify Privilege Vault, and five

additional links to approve or deny the request if the **Allow Approval For Access from Email** configuration setting is enabled. The approver can either click one of the links contained in the email or navigate to the Notification Center within IBM Security Verify Privilege Vault. If choosing the latter, in the displayed grid click the access request name. This will take you to the Secret Access Request Approval page.



From here, you can accept or deny the request as well as set an expiration date. The requestor will have access to the Secret until the specified date. Selecting the current date is the smallest window of time allowed and will grant access to the end of the day. With **Allow Approval For Access from Email** enabled, clicking one of the five additional links in the email will allow access for 1, 2, 4, or 8 hours OR deny the request, per the link description in the email.

The expiration date referred to in approval requests is not the same as Secret expiration.

Remote Password Changing

Remote Password Changing (RPC) allows properly configured Secrets to automatically update a corresponding remote account. Secrets can be set for automatic expiry so IBM Security Verify Privilege Vault will automatically generate a new strong password and change the remote password to keep all the account synchronized with IBM Security Verify Privilege Vault.

If IBM Security Verify Privilege Vault fails to change a remote password, an alert appears notifying that there are Secrets out of sync.

Remote Accounts Supported

For the most up-to-date list of account types supported by Remote Password Changing, see List of Built-In Password Changers (KB).

Enabling Remote Password Changing in IBM Security Verify Privilege Vault

RPC is enabled under the Administration, Remote Password Changing page. Click edit to enable Remote Password Changing, Secret Heartbeat, and Secret Checkout. Once enabled, all Secret templates with RPC configured will be available to use RPC.

Configuring a Secret for AutoChange

The Remote Password Changing tab contains the settings for configuring RPC on an individual Secret. Enabling AutoChange on a Secret will allow IBM Security Verify Privilege Vault to Remotely Change the Password when it expires. The user must have Owner permission on the Secret to enable AutoChange. When editing on the RPC tab, the Next Password field can be set or if left blank an auto-generated password will be used.

If the password change fails, IBM Security Verify Privilege Vault will flag the Secret as Out of Sync and continue to retry until it is successful. If the Secret cannot be corrected or brought In Sync, manually disabling AutoChange will stop the Secret from being retried.

Privileged Accounts and Reset Secrets

By default, RPC uses the Credentials on Secret option, by using the credentials stored in the Secret to invoke a password change. For Windows and Active Directory accounts, a privileged account can be used instead by selecting the Privileged Account Credentials option and selecting an Active Directory Secret with permission to change the account's password.

For Secret templates with a Custom Commands Password Type, any number of associated Reset Secrets can assigned for use in the Custom Commands. See section Custom Command Sets (Professional or Premium Edition) for more details on using the Reset Secrets in Custom Commands.

When a Secret is wired up with a Privileged account or Reset Secrets, the ability to Edit the username, Host, Domain, or Machine is restricted if the user does not have access to those associated Secrets. On the RPC tab, the user will see "You do not have access to View this Secret" for the Secret name and on the Edit screen all fields mapped for RPC except the Password will be disabled. This added security prevents the user from changing the username and resetting another account's Password.

If the user does not have access to the privileged account or reset Secrets, the ability to edit all Secret fields mapped for RPC except the password field is restricted to prevent changing the password on another account.

Change Password Remotely

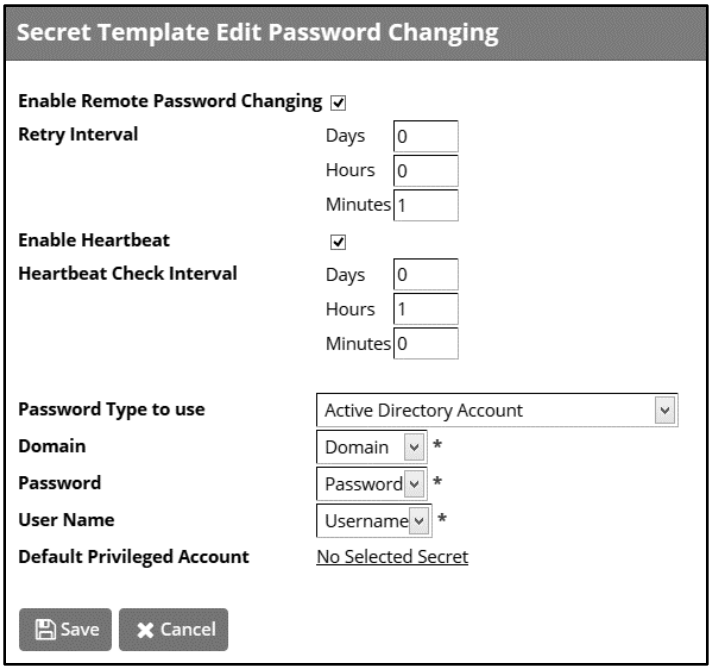
On the RPC tab there is a button called Change Password Remotely that allows the use to change the password immediately instead of waiting for it to expire. When this button is clicked the user is taken to the Change Password Remotely page where they are able to enter in or generate the new password for the account. When the user clicks the Change button the secret will enter the queue for having its password changed. The RPC Log found on the Administration, Remote Password Changing page details the results of the password change attempts and can be used for debugging.

If the secret is a Unix or Linux account and uses a password changer that supports SSH Key Rotation, the user can change the account's password, public/private keypair, and the private key passphrase. The user can enter or generate any of these items.

If the password change fails, IBM Security Verify Privilege Vault will continue to retry until it is successful or the change is canceled by the user. In order to manually cancel the change, click Cancel Password Change on the RPC tab.

Configuring Remote Password Changing – Mapping Account Fields

All the Secret templates with the prefix RPC have RPC configured by default. For creating a custom template that uses RPC it can be configured from the Secret Template Designer. Enable Remote Password Changing must be turned on for Secrets created from the template to make use of this feature. Select the password type for the account and map the fields to be used for authenticating to the remote server. The Secret Fields must be mapped to the corresponding required fields based on the Password change type.



The Retry Interval field is the amount of time that a Secret will wait before once again attempting to change a password after a password change is unable to succeed.

The Default Privileged Account field is the Secret that will be set as the privileged account for all new Secrets that are created with this Secret template. Changing this will not affect any existing Secrets.

Ports Required for Remote Password Changing

Password Changer Type	Port(s)
Unix SSH	22
Unix Telnet	23
Microsoft SQL Server	1433
Windows Kerberos	88 or 441
Windows NTLM	445
Active Directory	389 or 636
Sybase	5000
Oracle	1521 or 1526

AutoChange Schedule

The AutoChange Schedule button will be visible on the Secret View RPC tab when RPC and AutoChange is enabled on a Secret. The AutoChange Schedule page allows you to specify an interval, start date, start time, and time frame for when the password is allowed to be changed. This setting is useful for having the Remote Password Change occur during off-hours in order to prevent disruptions. By default, this setting will be None, which allows the Secret to be changed immediately. Note that regardless of the AutoChange Schedule, the password will still have to expire before being automatically changed.

While the password change is waiting for this next scheduled time, the Remote Password Changing Log (visible by navigating to Configuration > Remote Password Changing) will report the Secret might not be changed because of time schedule. The Secret will also remain expired until this AutoChange Schedule is reached, even if the Secret was forced to expire.

Remote Password Changing Logs

The Remote Password Changing logs for a specific Secret can be accessed by clicking the View Audit button on Secret View page and ticking the check box at the bottom of the page for Display Password Changing Log. The Remote Password Changing logs for all Secrets can be accessed by navigating to Administration > Remote Password Changing.

Remote Password Changing for Service Accounts and SSH Keys

Service Accounts

RPC can be performed on Service accounts where the dependent services will be automatically updated and restarted as the service account password is changed. Administrators will be notified if a dependency fails to restart. The supported dependency types are IIS Application Pools, IIS Application Pool Recycle, Scheduled Tasks, Windows Services, passwords embedded in .ini, .config, and other text files. Custom Dependencies can

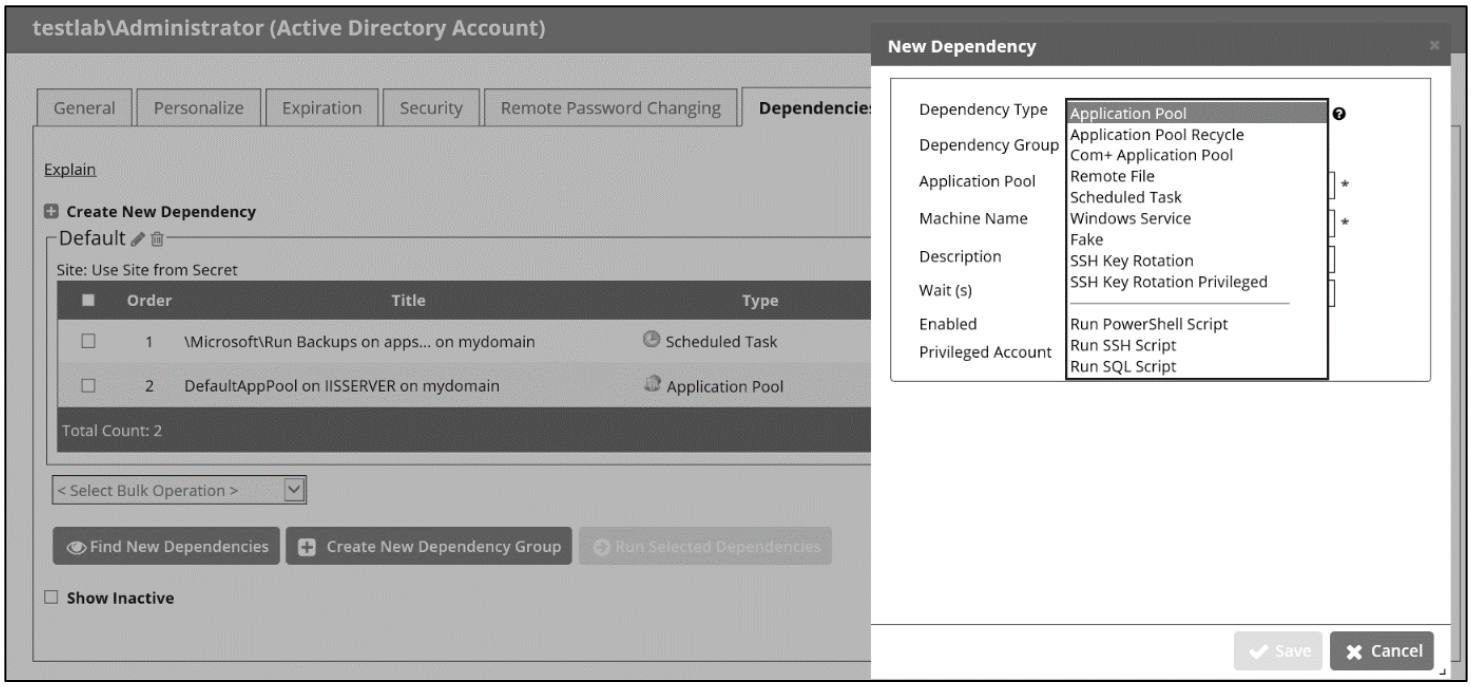
be created by using SSH, PowerShell, or SQL scripts. The Application Pool Recycle will only recycle the specified Application Pool, it does not update the password of the Service Account running the Application Pool. IBM Security Verify Privilege Vault will attempt to unlock the Service Account should the account become locked during the dependency password change as long as there is a Privileged Account assigned to the Secret.

SSH Keys

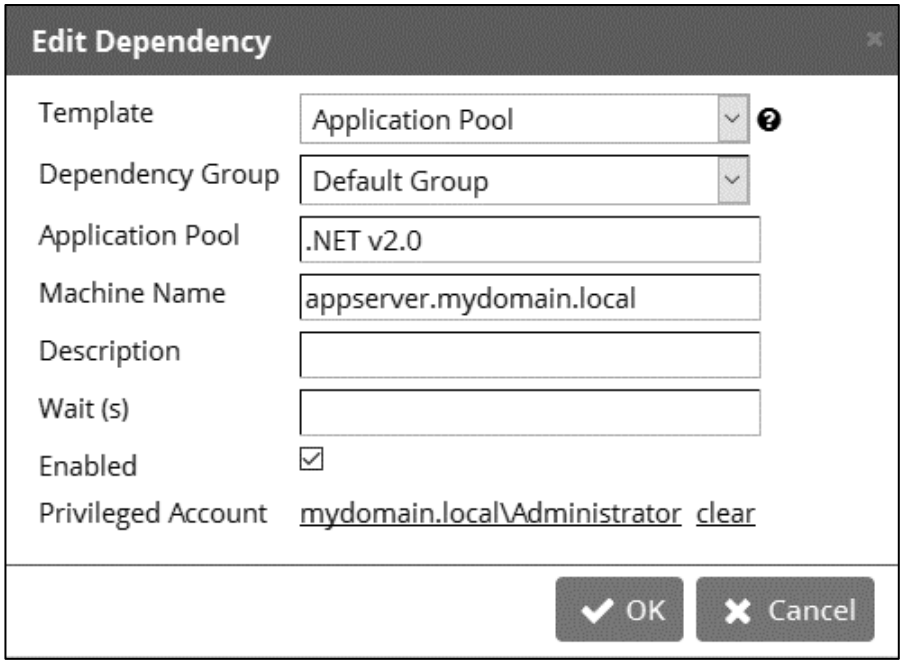
RPC can be performed on multiple Public Keys referencing the same Private Key in IBM Security Verify Privilege Vault. The dependency types for this situation are SSH Key Rotation and SSH Key Rotation Privileged.

Configuring the Dependency Tab

Dependencies are items that rely on the username, password, and/or SSH private key stored in the Secret. By adding them to the dependencies tab, they will automatically be updated when the Secret's password is changed, ensuring they are up to date with the account on which they depend.



Adding a custom Dependency Template might require additional settings (these settings are described in the following section):

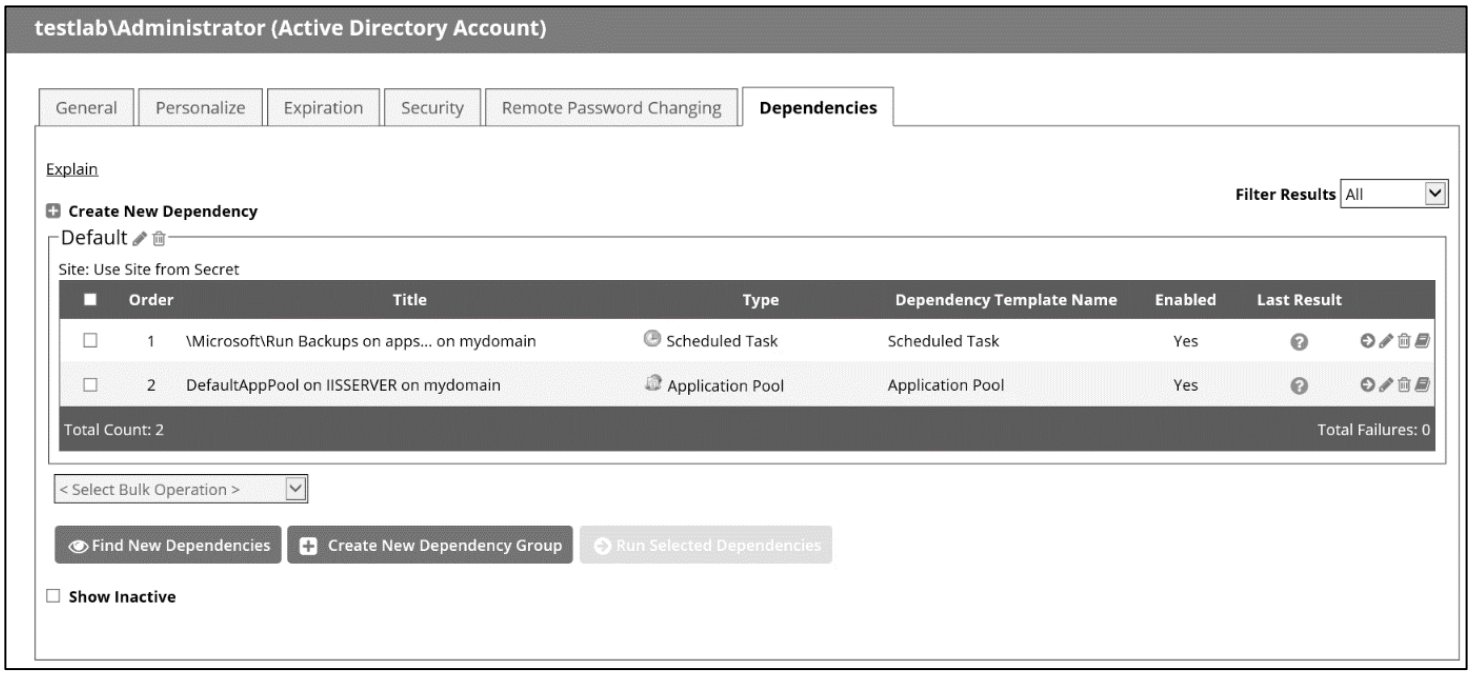


Dependency Settings and Information

Template	Whether the Dependency is an IIS Application Pool, Scheduled Task, Windows Service, Remote File, COM+ Application. Custom Dependencies can also be created by using a SQL, SSH, or PowerShell Script.
Name	Name of the Dependency on the remote machine.
Dependency Group	Name of the Group to run the Dependency update in.
File Path	For Remote File Dependency types, this is the UNC file path on the remote server where the embedded password exists.
Regex	For Remote File Dependency types, the regular expression used to locate the password embedded in the configuration file.
Machine Name	Computer name or IP address on which the dependency is located.
Script	Name of the PowerShell Script, SSH Script, or SQL Script in the Scripts repository configured on the Dependency Template. The actual script selected can be previewed by clicking the eye icon.
Server Name	For SQL Script Dependency types, the server name for the script.
Database	For SQL Script Dependency types, the database name for the script.
Port	For SQL and SSH Script Dependency types, the port name for the script.

Description	Description of the Dependency for documentation purposes.
Wait (s)	Time in seconds which IBM Security Verify Privilege Vault will pause before changing the dependency.
Restart	Determines if the Dependency will be restarted once the account has been updated.
Enabled	Whether IBM Security Verify Privilege Vault will attempt to update the Dependency. A disabled Dependency will be ignored by IBM Security Verify Privilege Vault.
Privileged Account	The account IBM Security Verify Privilege Vault will authenticate as when changing the Dependency's credentials, so it must have privileges on the remote machine to edit the Dependency.
SSH Key Secret	An account with SSH Key that IBM Security Verify Privilege Vault will use to authenticate when executing the SSH Script or SSH Key Rotation Dependency types.
Change Fail Script	For SSH Key Rotation and SSH Key Rotation Privileged Dependency types, this is the built-in script that determines if IBM Security Verify Privilege Vault was unable to update the public key on the dependency.
Change Success Script	For SSH Key Rotation and SSH Key Rotation Privileged Dependency types, this is the built-in script that determines if IBM Security Verify Privilege Vault was able to update the public key on the dependency.
Verification Script	For SSH Key Rotation and SSH Key Rotation Privileged Dependency types, this is the built-in script that verifies that the new public key on the dependency matches the private key on the Secret.
Change Script	For SSH Key Rotation and SSH Key Rotation Privileged Dependency types, this is the built-in script that updates the public key on the dependency.
Public Key	For SSH Key Rotation and SSH Key Rotation Privileged Dependency types, this field holds the value of the public key stored on the dependency.
Server Key Digest	For SSH Key Rotation and SSH Key Rotation Privileged Dependency types, a field that serves as a security control for specifying the SHA1 hash of the SSH host key on the remote server.
Run Condition	Allows the dependency to run conditionally depending on the outcome of the dependencies above it.

Example values for a Windows Service Dependency on a remote computer might be: 192.11.158.99, Windows Service, aspnet_state, DOMAIN\admin.



The following operations can be performed in the Dependency grid:

Test Connection click the return arrow icon to test the Dependency connection, the tests results will be displayed afterward.

Run Dependency click the second arrow icon to run the script on the selected Dependency and set the password on the selected Dependency to the current password for the Secret

Edit click the icon to edit Dependency fields. Cancel changes by pressing the Cancel button.

Delete click the icon to delete the Dependency.

View Dependency History click the icon to view the activity logs for the Dependency.

Due to security constraints, Scheduled Tasks require an Active Directory domain user as the Privileged Account.

Manually Adding a Dependency

To manually add a dependency, click the plus icon next to Create New Dependency on the Dependencies tab. Then, choose your dependency type from the drop-down template list. Next, fill in the Dependency Name, Machine Name, and other information depending on the Dependency type. To choose the account used to change the Dependency password, click the link next to the Privileged Account label. If the Privileged Account is blank, the current Secret's credentials will be used. Click the OK button to finish adding the Dependency.

Custom Dependencies

If there are different dependency types that you want to manage that aren't supported out of the box, new ones can be created based on a script. A custom dependency consists of two components:

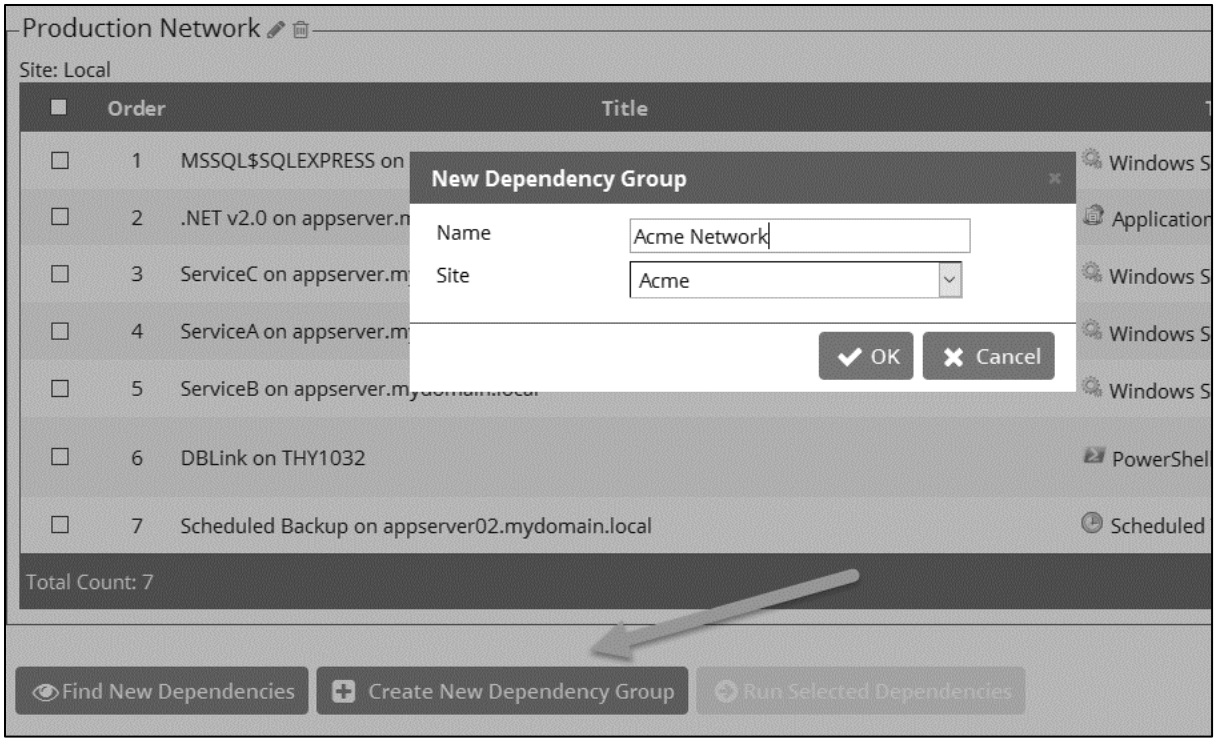
Dependency Template: The Dependency Template defines how a Dependency is matched to discovered accounts and how it updates the target after a password change occurs on the account. To create a new Dependency Template, go to **ADMIN | Secret Templates** and click the Dependency Templates button.

Dependency Changer: A Dependency Changer is a script and the associated parameters to be passed into the script. Dependency Changers can be created and modified by going to **ADMIN > Remote Password Changing > Configure Dependency Changers**.

Please reference the Discovery Guide for a comprehensive guide to configuring and by using Dependency Changers and Dependency Templates.

Dependency Groups

By Default, all Dependencies are updated in the order listed. There are cases where you might want to split out different sets of Dependencies into separate groups. Typically, this is because a single service account might run services across different segregated networks that can communicate with the domain but not each other and have different Distributed Engine Sites assigned. In this case you can create two Dependency Groups and assign them to different Distributed Engine Sites to solve connectivity issues.



Custom Password Changers

The Password Changers Configuration page can be accessed by navigating to **ADMIN > Remote Password Changing > Configure Password Changers**.

There are a few Password changing types that allow the user to enter in specific commands that will be sent to the computer where the password is changing. This enables the system to accommodate for differences in the standard password change procedure. For example: The Unix system that is being changed prompts for the current password twice instead of only once before asking for the new password.

Modifying Password Changers

To modify a password changer, click the password changer name under ADMIN > Remote Password Changing > Configure Password Changers and then use the **Edit** or **Edit Commands** buttons to make changes. For more information about editing the custom PowerShell password changer, see PowerShell Remote Password Changing (KB).

You can find the full, up-to-date list of password changers included with IBM Security Verify Privilege Vault by default in List of Built-In Password Changers (KB).

Deactivating Password Changers

To make a password changer unavailable for use and to hide it from view in your list of password changers, you must mark it as inactive:

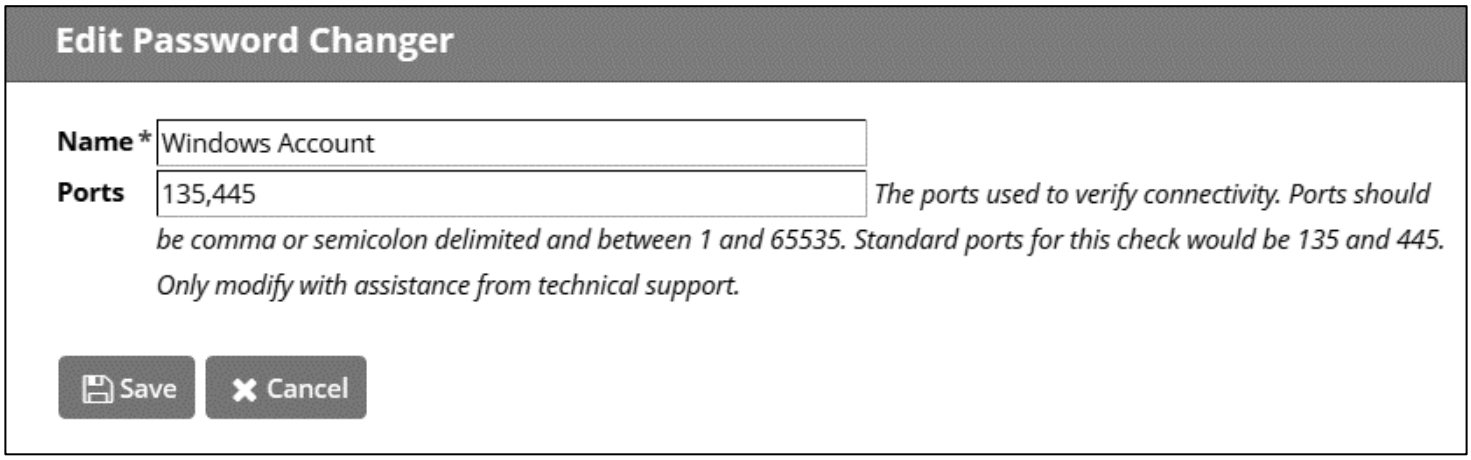
- From the Password Changers Configuration page, click the Password Type Name of the password changer you would like to make inactive.
- Click Edit.
- Uncheck the Active box.
- Click Save.

To view inactive password changers, check the Show Inactive box at the bottom of the list of password changers. The Active column in the table will indicate the status of the password changer.

Changing Ports and Line Endings

To change the port or line ending used on a password changer, click the password changer on the Configure Password Changers page and then click Edit. There, you can choose the line ending and port used by the device. By default, line endings are set to New Line (\n), however some devices and applications (such as HP iLO) use a different line ending system. The port defaults to 22 for SSH connections and 23 for Telnet connections.

For the built in Windows Password Changer there is a Ports field available that can be filled in to help ensure a computer is listening. This can be used if DNS returns multiple IP addresses for a single box and only one is valid. For example, a laptop might get two IP addresses for an Ethernet and wireless connection, but if it is unplugged the Ethernet IP is invalid. In this case, IBM Security Verify Privilege Vault can do a reverse lookup and test each IP until it is able to connect on one of the specified ports. When it gets a response it uses that IP for the password change.



Editing a Custom Command

The SSH type changers use the SSH protocol to access the machine. This type contains custom commands for the password reset functionality and can contain commands for the verify password functionality but most SSH type changers simply verify that a connection can be established with the username and password. The Telnet type changers use the Telnet protocol in order to access the machine and contain custom commands for both the password reset and the verify password functionality. The Verify functionality is used in the Heartbeat, as well as verifying that the password was changed successfully.

SSH Key Rotation type changers also include post-reset success and failure custom commands. These extra command sets are run after both the reset and verify functions are run and are used to either finalize the key rotation and password change (success) or clean up after a failure. If both the reset and verify functions are successful, the post-reset success command set is run. If either the reset or the verify fail, the post-reset failure command set is run.

To edit the custom commands, click the Edit Commands button. This will set the command grids into Edit mode where you can add, update, or delete the commands in order to suit their purpose.

Any Secret Field value can be substituted by prefacing the Field Name with a '$'. For example, in order to echo the Notes value for a Secret, the user would enter: echo '$Notes' as a command. Along with these Secret Field values, the following variables are available in custom commands:

RPC Mapped Fields

- **$USERNAME**
  The username field mapped in RPC on the Secret template.
- $**CURRENTPASSWORD**
  The password field mapped in RPC on the Secret template.
- $**NEWPASSWORD**
  The next password (filled in Next Password textbox or auto-generated).
- **PRIVATEKEY**
  The private key field mapped in RPC on the Secret template.
- $**NEWPRIVATEKEY**
  The next private key (filled in Next Private Key text area or auto-generated).
- $**CURRENTPUBLICKEY**
  The public key field mapped in RPC on the Secret template.
- $**NEWPUBLICKEY**
  The next public key (generated from the next private key).

- $**PASSPHRASE**
  The passphrase field mapped in RPC on the Secret template.

- $**NEWPASSPHRASE**
  The next passphrase (filled in Next Private Key Passphrase text area or auto-generated).

Associated Reset Secrets

- **$[1]**
  Adding this prefix to any field will target the associated Reset Secret with order 1.

- **$[1]$USERNAME**
  The mapped username of the associated secret, identified by order. Can also reference any other property on the associated secret. Common examples include:

  - $[1]$PASSWORD
  - $[1]$CURRENTPASSWORD
  - $[1]$PRIVATE KEY
  - $[1]$PRIVATE KEY PASSPHRASE

- **$[SID:105]**
  Adding this prefix to any field will target the associated Reset Secret with a Secret Id of 105.

- **$[SID:105]$USERNAME**
  The mapped username of the associated secret, identified by Secret Id. Like referencing an associated secret by order, referencing by secret id can also access any field on the secret by name.

Both the mapped fields and Secret Field names can be used.

Check Result Commands

- **$$CHECKFOR <text>**
  Checks that the response from the last command equals <text>

- **$$CHECKCONTAINS <text>**
  Checks that the response from last command contains <text>

- **$$CHECKNOTCONTAINS <text>**
  Checks that the response from last command does not contain <text>

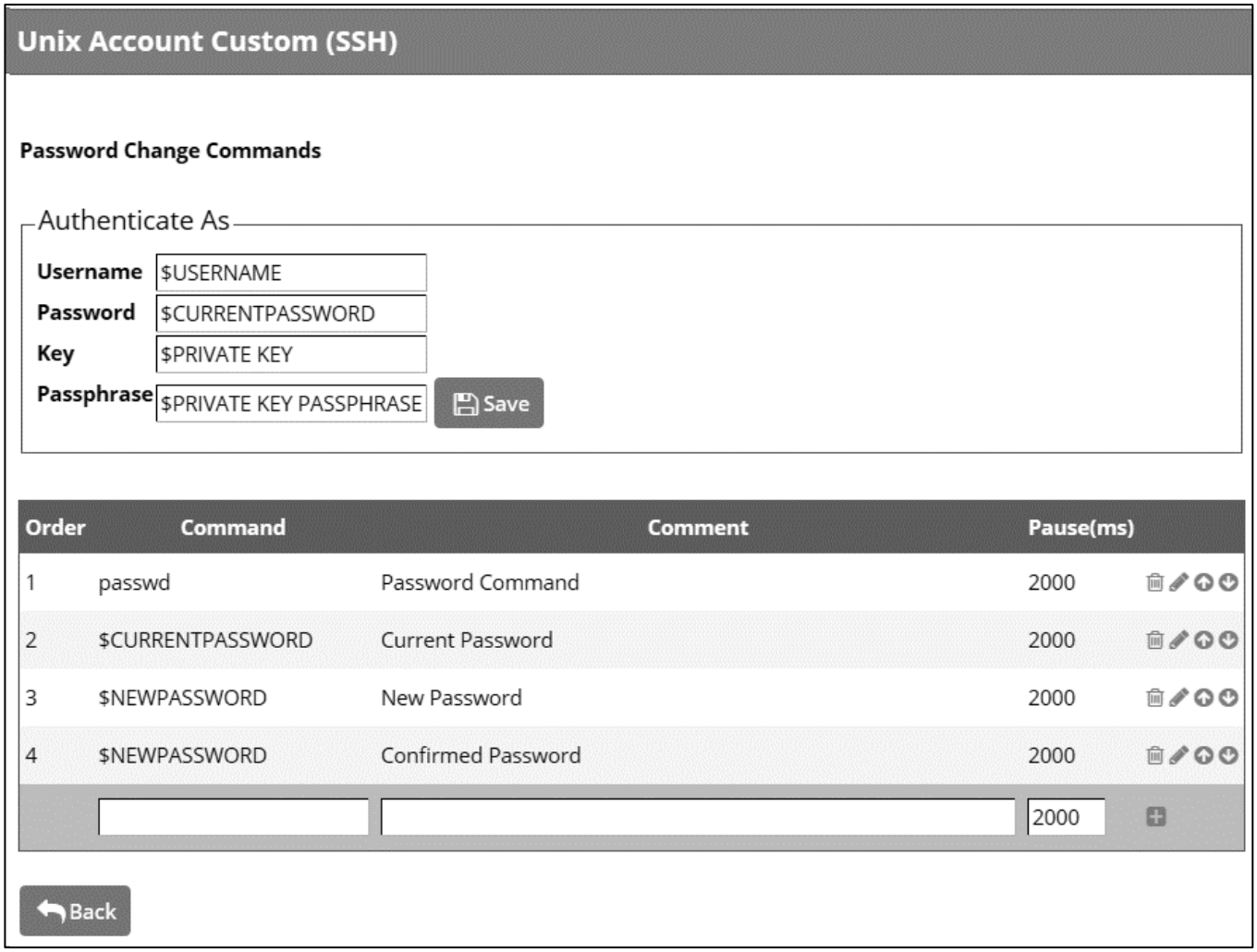
If these conditions are not met the process fails and immediately returns a result.

If you want to exit out of the command set early without triggering a failure, echo an "OK" on the line immediately preceding the "exit 0;" statement. “OK” must be the only text in the response from the server in order for this to work.

You can test out your Password Reset and Verify Password command sets by clicking on the Test Action buttons next to the relevant sections. All communication between IBM Security Verify Privilege Vault and the target machine will be displayed when using these test buttons.

Mapping an SSH Key and/or Private Key Passphrase for authentication

Some password changers might be customized to use SSH Key authentication. IBM Security Verify Privilege Vault needs to know which fields contain the key and the passphrase. These fields can be specified after clicking **Edit** from the password changer page.



The Key and Passphrase must be identified by a **$** sign and the Secret field name, which can be obtained from the Secret template.

To set which fields are your key and passphrase, go to the extended mappings for a Secret Template by clicking **Extended Mappings** from the Secret template edit page. Select the fields that correspond to the SSH Private Key and Passphrase if applicable. So, no matter what you name your key field, IBM Security Verify

Privilege Vault will know what it is. This is set up by default, so you shouldn't need to do this unless you've created custom UNIX templates you want to use keys with.

Once IBM Security Verify Privilege Vault knows which fields contain the private key and private key passphrase, it can automatically use them as a part of launchers.

Creating a New Custom Command Password Changer

- From the Password Changers Configuration page, click New.
- Select a base password changer – it is recommended that you select the option that most closely matches the type of password changer you are creating, as this determines which customizable parameters and test actions are available to you.
- On the next page, make any customizations you would like. To save a new command, click the + icon at the end of the row. The command can be edited once more by clicking the edit button, which is labeled with a small pencil icon at the end of the row.
- To access the test actions for your new password changer, click Back to return to the overview screen.
- To edit additional parameters (if applicable), click Edit from the password changer overview to change settings such as the Name, Line Ending, and Custom Port.

For more information about creating a custom PowerShell password changer, see PowerShell Remote Password Changing (KB).

Heartbeat

Heartbeat allows properly configured Secrets to have the entered credentials automatically tested for accuracy at a given interval. Using Heartbeat on Secrets will ensure the credentials stored in IBM Security Verify Privilege Vault are up-to-date and can alert administrators if the credentials are changed outside of IBM Security Verify Privilege Vault. Heartbeat helps manage Secrets and prevent them from being out of sync.

Remote Accounts Supported

For the most up-to-date list of account types supported by Remote Password Changing, see this KB article.

Enabling Heartbeat

To enable Heartbeat, Enable Heartbeat must first be turned on in the Remote Password Changing Configuration page (navigate to Administration > Remote Password Changing). It must also be set on the Secret template by enabling the Enable Remote Password Changing Heartbeat setting.

Configuring Heartbeat

Heartbeat is configured from the Secret Template Designer. The Heartbeat interval will determine how often the Secret credentials will be tested. See the RPC Section on Configuring Remote Password Changing - Mapping Account Fields.

Using Heartbeat

Heartbeat will run in a background thread to check each Secret where it is enabled. If the credential test fails, the Secret will be flagged as Heartbeat Failed and out of sync. To avoid locking out the account, Heartbeat will no longer run on that Secret until the Secret items are edited by the user. If the machine is determined to be Unavailable the Secret will be flagged as Heartbeat Unable to Connect and the Secret will continue to be checked on the Heartbeat interval.

To manually use Heartbeat to check the credentials the Secret View page has the Heartbeat Now button. The Heartbeat Now button will mark the password as Heartbeat Pending. The background thread will process the Secret in the next 10 Secrets and when the page is refreshed the Heartbeat Status will be updated.

Heartbeat for Windows Accounts is not compatible for accounts on the server that is running IBM Security Verify Privilege Vault. These accounts will be flagged with a status of Incompatible Host.

Heartbeat Logs

The Heartbeat logs for a specific Secret can be accessed by clicking the View Audit button on Secret View page and ticking the check box at the bottom of the page for Display Password Changing Log. The Heartbeat logs for all Secrets can be accessed by navigating to Administration > Remote Password Changing and scrolling down to the second set of logs.

Alerts on Failure

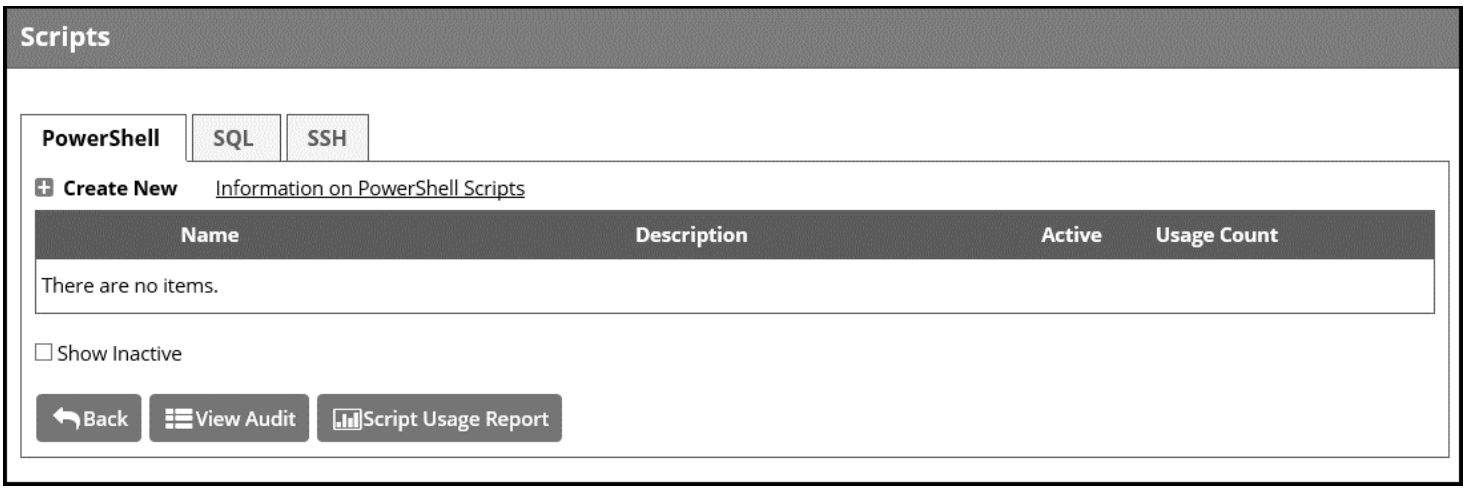
On the Preferences page, the Send email alerts when Heartbeat fails for Secrets setting can be enabled to email the user when Heartbeat fails for any Secret the user has View access to.

Distributed Engine

Distributed Engine allows Remote Password Changing, Heartbeat and Discovery to occur on networks that are not directly connected to the network that IBM Security Verify Privilege Vault is installed on. It was released in version 8.9.000000 and replaced Remote Agents. See the linked KB and its associated white paper for details on configuration and functionality.

Scripts

PowerShell Scripts, SSH Scripts, and SQL Scripts for password changing, dependencies, and discovery custom actions can be created by Administrators with the role permission called Administer Scripts. The scripts can be accessed by going to Administration > Remote Password Changing > Scripts.



IBM Security Verify Privilege Vault requires that WinRM is configured on the web server, for instructions please see the following KB article: Configuring WinRM for PowerShell.

Creating a Script

On the Scripts screen, select desired script tab and click Create New to enter the name of the script, a description, and the commands to run, then click OK. The Script now shows up in the grid. Scripts can be deactivated and reactivated from the grid.

Testing a Script

All scripts will run from the machine that IBM Security Verify Privilege Vault is installed on, or the Site assigned to the Secret. To test a Script, click the Test button on the grid next to the corresponding script.

PowerShell scripts will run as the identity of the Secret, so enter in an Active Directory credential to run the script as or select a Secret to pre-fill the run-as credentials. Then enter in any command line arguments that the script requires. The output of the script will be displayed above the grid for debugging purposes. To test the script over an engine, select a Site from the Site list. This helps in diagnosing server specific issues where engines are installed.

Using a Script

To use a Script as a password changer or Dependency, it must be wired up to the appropriate action under **ADMIN | Remote Password Changing** on the Password Changer or Dependency Changer.

Discovery scripting is done under **ADMIN | Discovery | Extensible Discovery**. For more information on configuring extensible Discovery see the Extensible Discovery overview.

Auditing

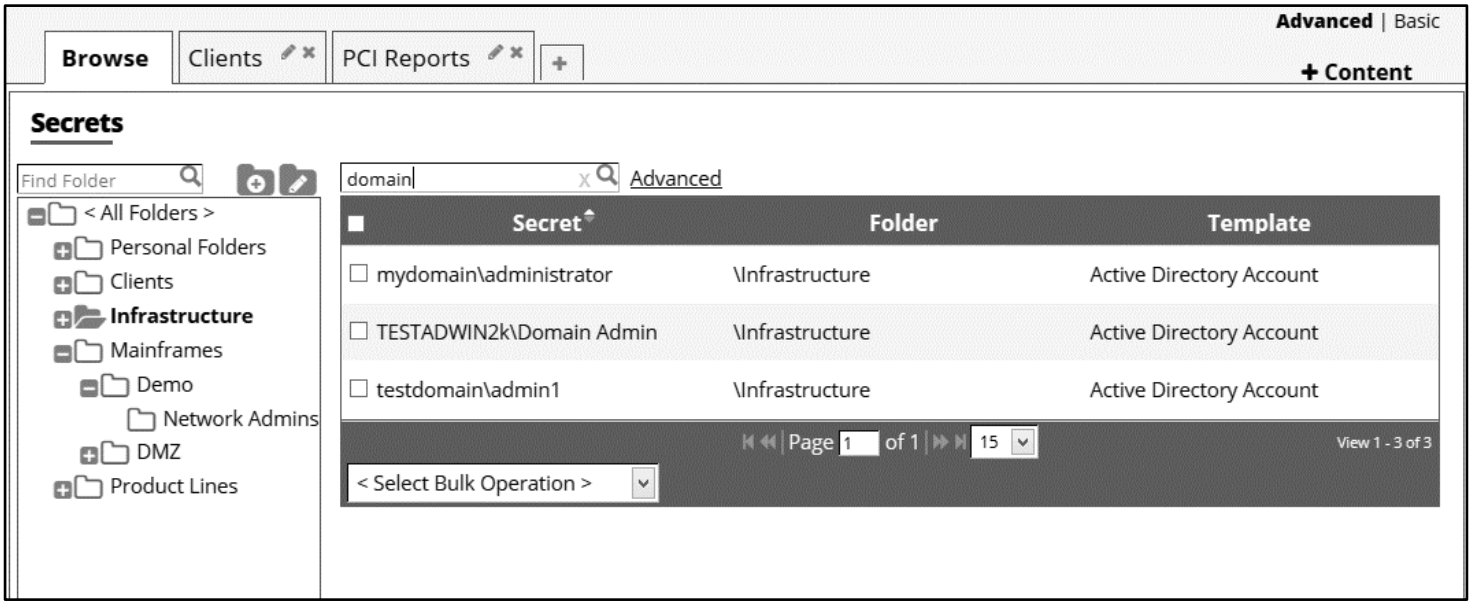
A full history of each PowerShell script is kept and can be downloaded from the audit trail. Click View Audit to view the audit trail for PowerShell. Each time a script is updated, the previous one can be downloaded from the corresponding audit record.

For additional information on setting up PowerShell scripts, please read the following KB article: Creating and Using PowerShell Scripts.

Searching Secrets

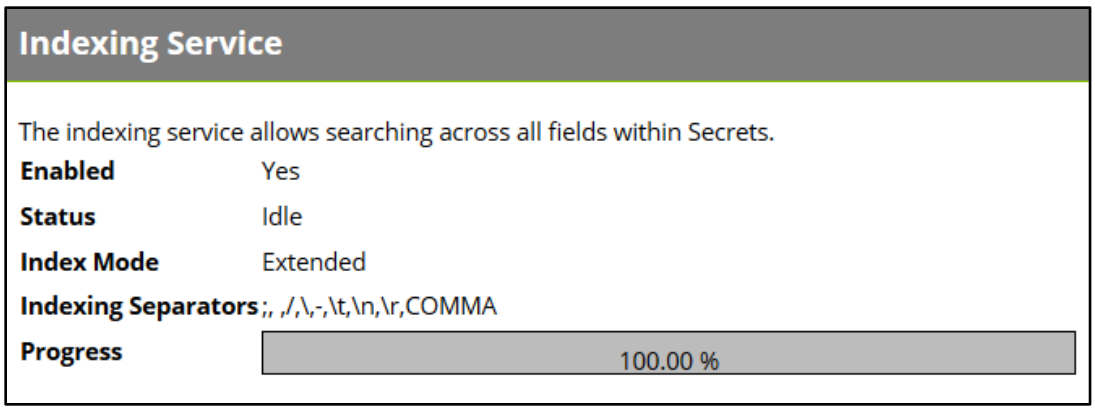
Searching Secrets is performed on the Dashboard from the Search/Browse widget. To make searches more precise, the results can be limited by way of the various parameters available when clicking the Advanced link. Searches will search for all fields that are configured to be "searchable" on the Secret's template if the Extended Search Indexer is enabled. If the Search Indexer is not enabled, searches will only be performed on the Secret Name field.

The Browse tab is a quick way to view all active Secrets available regardless of folders or search parameters.



Search Indexer

The Search Indexer allows searching on all fields set to Searchable on the template. From the Administration > Search Indexer, click the Edit button to configure and enable the indexing service. Save any changes and the Indexer will start indexing all the Secrets. The progress is displayed on the Search Indexer Administration page and indexing might take some time depending on the size of the installation. The indexer runs in the background to avoid the undesirable effect of decreased performance caused by using full server resources.



Search Indexer Edit

Standard Search mode is the default search mode. Standard searching creates indexes on the values of each field set to Searchable (previously Indexable) on the template. However, it will only search on whole words in these fields. For example, a Secret with a field value of “IBM” would only match a search for “IBM.”

Extended Search allows searching on both whole words and sections of words (minimum three letters). For example, the Secret with a field value of "IBM" would be returned on a search for "IBM" or "IB" or "bm". This allows for more fine-grained search results but might impact search performance as well as create a larger index table.

Indexing Separators are used to split the text fields into search terms. By default, the separators are semi-colon, space, forward slash, back slash, tab (\t), new-line (\n), return (\r), and comma. Changes to the Indexing Separators will require a full rebuild of the search index.

Secret Import

IBM Security Verify Privilege Vault's Import feature simplifies integration with legacy systems and allows users to easily add large numbers of Secrets from an Excel or CSV/Tab delimited file. Secrets are batch imported by template, so multiple types of input data must be imported in several batches. The Password Migration Tool supports easy addition of existing Secrets from other third-party password storing applications.

Configuring Data for Import

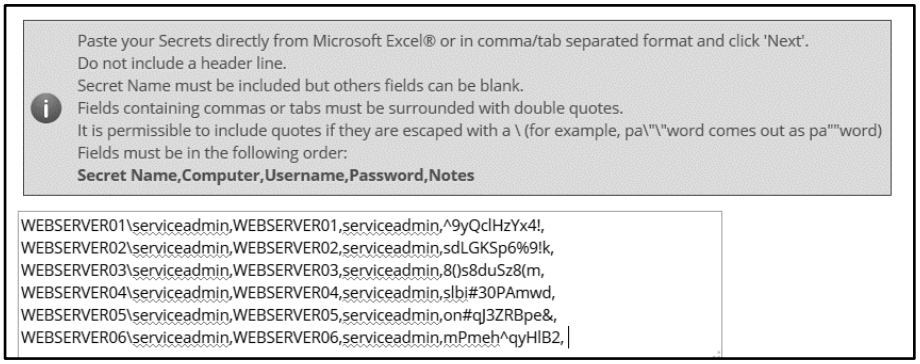
To get started, click Import Secrets from the Tools page. A template corresponding to the type of data in the input file must then be selected; then Continue to add the Secrets.

Paste the Secrets for import directly into the text area in the Import Secrets dialog. The order of the fields being imported will be listed depending on the template selected. A few items to note when importing Secrets:

- Do not include a header line.

- Secret Names must be included but other fields can be blank unless the Secret template indicates that the field is required.
- Fields containing commas or tabs must be surrounded with double quotes.

There are two options for importing Secrets: Ignore Duplicate Secrets and Import With Folder. Ignore Duplicate Secrets will prevent the import of any Secrets with the same name of an already existing Secret. Import With Folder allows an additional field in the import text specifying a fully qualified folder name for the Secret to be created in. IBM Security Verify Privilege Vault displays a preview of the new Secrets prior to being imported.



Importing Secrets

IBM Security Verify Privilege Vault Migration Tool

IBM Security Verify Privilege Vault offers a migration utility for users wishing to import Secrets from other applications. Currently, the Migration Tool supports the following applications:

- Password Corral
- KeePass
- Password Safe

This is done with another Export Tool that creates a single XML file. Please contact support for more details.

Advanced XML Import

The Advanced Import will add folders, Secret templates, and Secrets based on an XML file. Permissions can be specified on the folders and Secrets or the default is to inherit permissions. This import can only be done by administrators with proper role permissions.

For details on the XML file, see the Knowledge Base article Advanced Import with XML.

Discovery

As an alternative to manually creating or importing accounts, IBM Security Verify Privilege Vault has an automatic Discovery option for local Windows accounts, Active Directory Service Accounts, Unix Accounts, VMware ESX/ESXi accounts, and Active Directory Domain Accounts. Account and dependency types not supported out-of-the-box in IBM Security Verify Privilege Vault can still be discovered by writing PowerShell scripts that can be run as custom scanners. This allows administrators to quickly import accounts found by IBM Security Verify Privilege Vault on specified domains or IP addresses.

Please reference the Discovery Guide for a comprehensive guide to configuring and by using Discovery.

To run Discovery on a Domain, IP Address Range, or a custom source, you must first enable the Discovery feature for IBM Security Verify Privilege Vault. Second, you must enable Discovery for each Discovery source you would like to be scanned. For Active Directory sources, this also involves selecting either the entire domain or specific OU's to be scanned.

Enable Discovery for IBM Security Verify Privilege Vault

1. On the **Administration** menu click **Discovery**, and then click **Edit**.
2. Select the **Enable Discovery** check box.
3. Fill in the **Synchronization Interval for Discovery** fields for days, hours, and/or minutes. This determines how often Discovery will run.
4. Click **Save**.

Enable Discovery for your Active Directory Domain

1. On the **Administration** menu click **Active Directory**, and then click **Edit Domains**.
2. Click the **Domain** value for the domain you would like to configure. For more information about adding domains, see Adding a Domain.
3. From the **Enable Discovery** drop-down menu, select **Entire Domain**.
4. Click **Save And Validate**.

Enable Discovery for Specific OU's of a Domain

1. On the **Administration** menu click **Discovery**, and then click **Edit Domains**.
2. Click the **Domain** you would like to configure. For more information about adding domains, see Adding a Domain.
3. From the **Enable Discovery** drop-down menu, select **Specific OUs**.
4. Click **Save And Validate**.
5. If you are not already redirected there, click the **Specific OUs** tab.
6. Type an OU name in the **Include** box to add an OU to the list. If the OU is found, it will auto-populate below the box. Click the name to add it to the list. An included OU appears with a  icon.

7. Type an OU name in the **Exclude** box to exclude it from Discovery. An OU will only be available to be excluded if it is contained within an OU that has already been included. An excluded OU appears with a  icon.
8. To remove an OU from the list, click the ⊗ to the right of the OU.
9. To set a specific Site or Secret to scan the computers in that OU with use the ⍰ icon to the right of the OU.
10. Click **Save**.

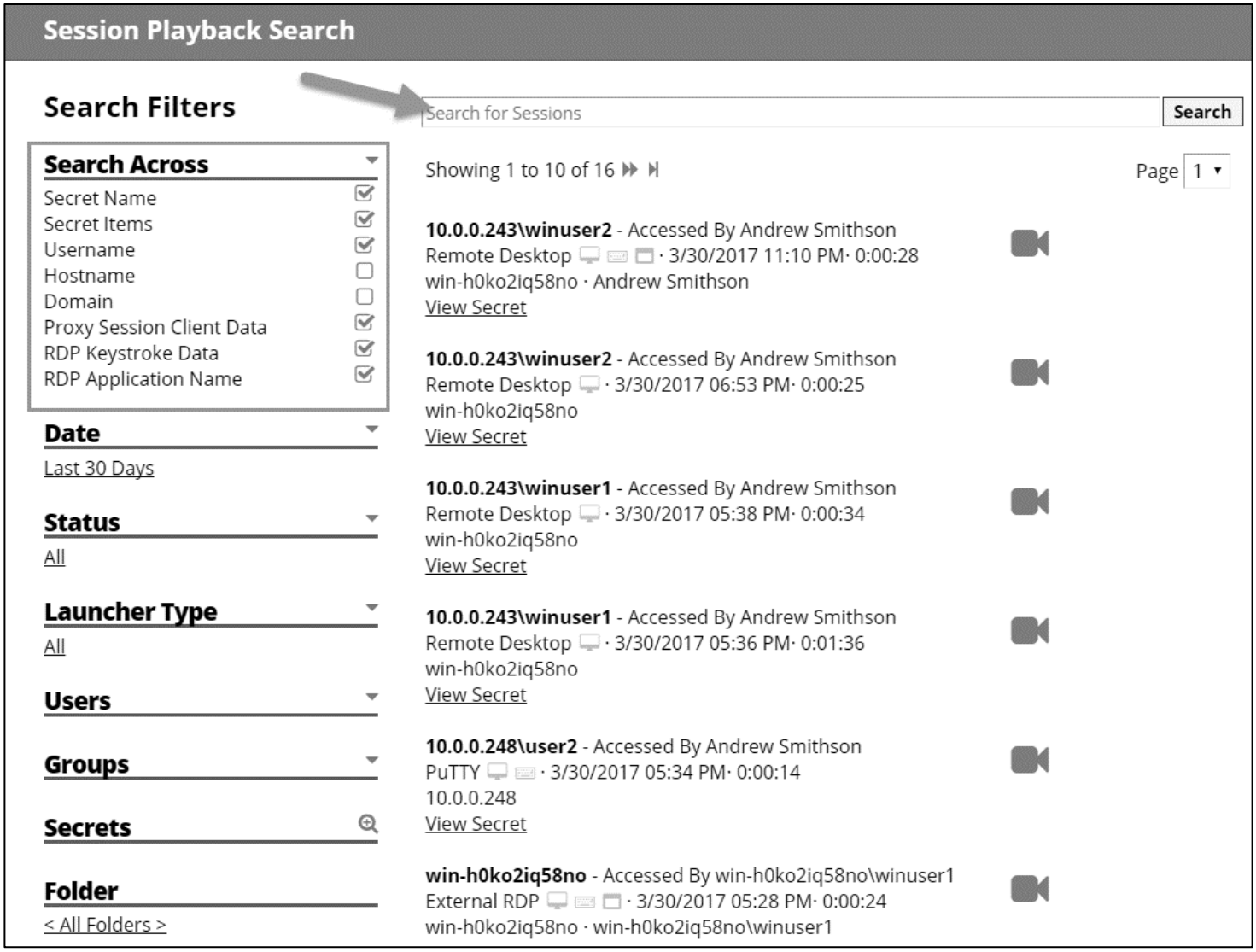
Note The ports required for Discovery are documented in this KB article.

Session Monitoring

Session Monitoring allows Administrators with the Session Monitoring permission to view all active launched Sessions within IBM Security Verify Privilege Vault. If Session Recording is enabled on the Secret, the admin can watch the user's session in real time.

Admins can search through active and ended sessions. To review and search through sessions go to **ADMIN | Session Monitoring**.

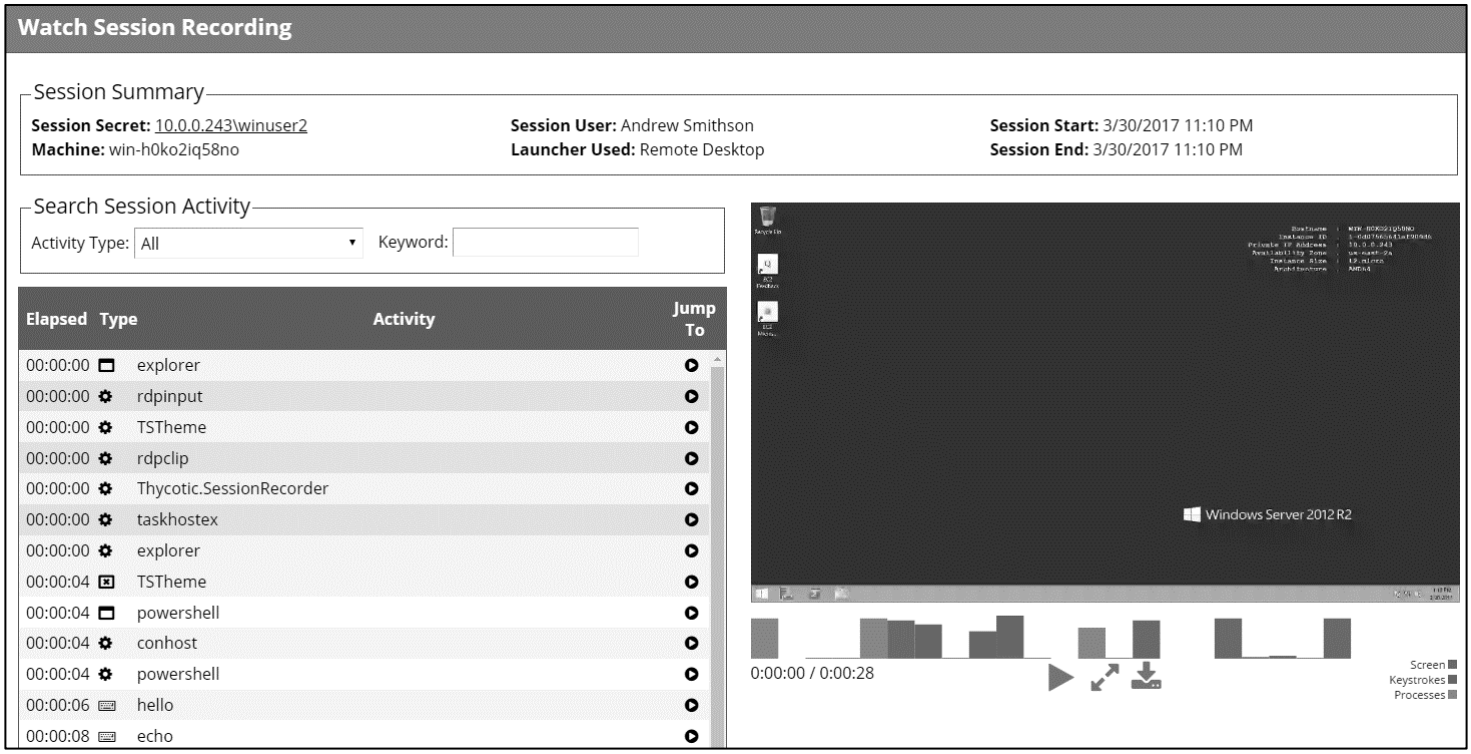
Searching across sessions can search the following data. To select what data is searched across check the options on the Search Filters on the left-hand side.



Some search filters require additional components to be installed or configured.

- **Proxy Session Client Data**: Search within keystroke data of proxied SSH sessions. Requires that the SSH proxy is enabled and SSH sessions are using it.
- **RDP Keystroke Data**: Requires the additional RDP Session Monitoring Agent installed on the target.
- **RDP Application Name**: Requires the additional RDP Session Monitoring Agent installed on the target.

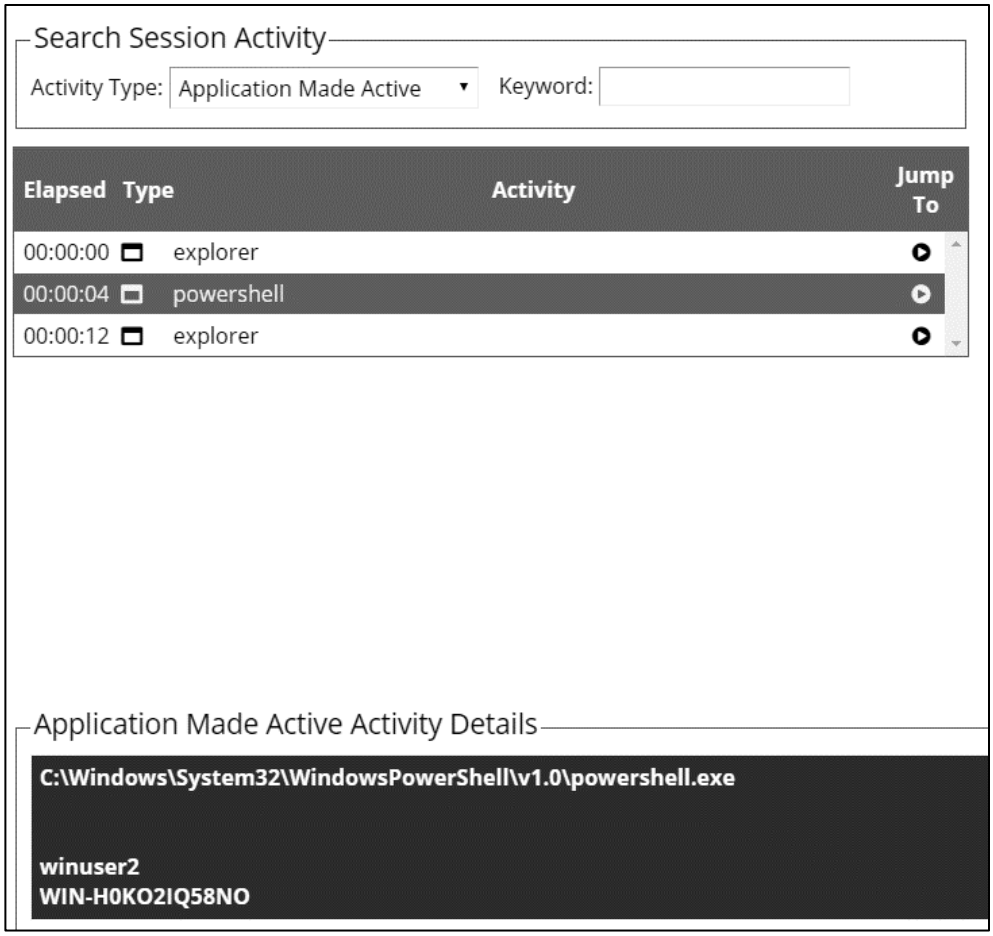
To view a recording, click the camera icon on the session.



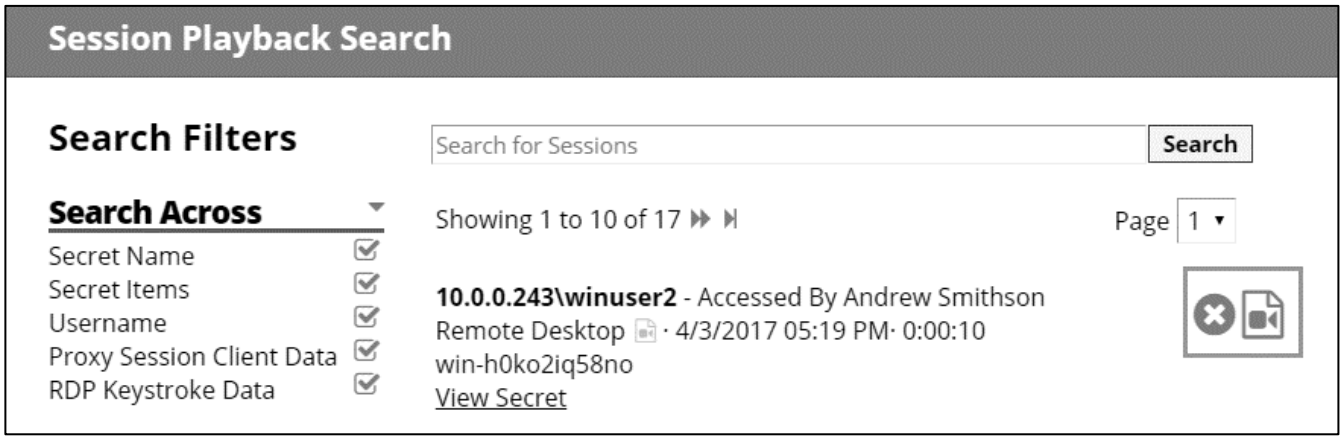
If there is logged session activity, such as keystroke or application data from the RDP agent or SSH proxy then you can search through Session Activity and jump to points within the video playback. The playback also displays an activity map to show points of high activity, such as screen changes, keystrokes, and processes started and stopped.

Selecting an activity in the grid also shows additional details below such as the full folder path where the application started and the user that performed the operation.

Note: SSH Keystroke data is shown in 1-minute segments. So, in a short session of less than minute the Jump To will only go to the beginning of the video.



For active sessions, there are two actions that can be taken:



Watch Live

When session recording is turned on for the Secret and admin can view and replay the user's activity.

Terminate
Send a message to the end user or terminate their session. The end user will see an alert dialog pop up on their machine with the message. Session recording does not need to be enabled for this to work.

For ended Sessions admins can watch the recorded video and view the SSH log if session recording was turned on for the Secret.

Webservices

IBM Security Verify Privilege Vault provides a suite of Webservices which can be used to retrieve and update Secrets, and folders. The Webservices allow IBM Security Verify Privilege Vault to be accessed by using the mobile apps as well as custom built integrations. The Webservices are secure and require authentication in the same manner as regular access to IBM Security Verify Privilege Vault. All actions that involve data are also logged (Secret views, updates, adds, and so on).

Enabling Webservices

Webservices can be enabled at the Administration > Configuration general tab. Enabling Webservices simply makes the ASP.NET Webservices built into IBM Security Verify Privilege Vault available. They are found under /webservices/sswebservice.asmx in your IBM Security Verify Privilege Vault. They run on the same port as the web application. You can view them with a browser to see the functionality that is offered. Specific Webservice functionality is documented in the IBM Security Verify Privilege Vault Webservice API guide.

Windows Integrated Authentication Webservice

IBM Security Verify Privilege Vault also provides a webservice that use Integrated Windows Authentication instead of a user name and password. This webservice can be used in an application or script to access IBM Security Verify Privilege Vault and retrieve Secrets with storing the login credentials in the application or configuration file.

See the Windows Integrated Authentication Webservice KB article for more advanced technical information on using this webservice.

Java Console API for Accessing Secret Values Programmatically

IBM Security Verify Privilege Vault can set up a Java Console API to retrieve values from IBM Security Verify Privilege Vault without embedding a password. This allows scripts to retrieve passwords from IBM Security Verify Privilege Vault while keeping both the password and credentials to IBM Security Verify Privilege Vault secure. The IBM Security Verify Privilege Vault Java Console is setup by using a user in IBM Security Verify Privilege Vault but the password is changed and hardware specific so copying the jar file to other machines will not allow it to access IBM Security Verify Privilege Vault. As a user in IBM Security Verify Privilege Vault, an

admin can choose to share only specific Secrets with the account running the Java Console. As a Java implementation, this can be used on any OS including Windows, Mac, Linux and Unix. For installation instructions and examples see the Application API Guide.

Folder Synchronization

To setup this feature, navigate to Administration > Folder Synchronization.

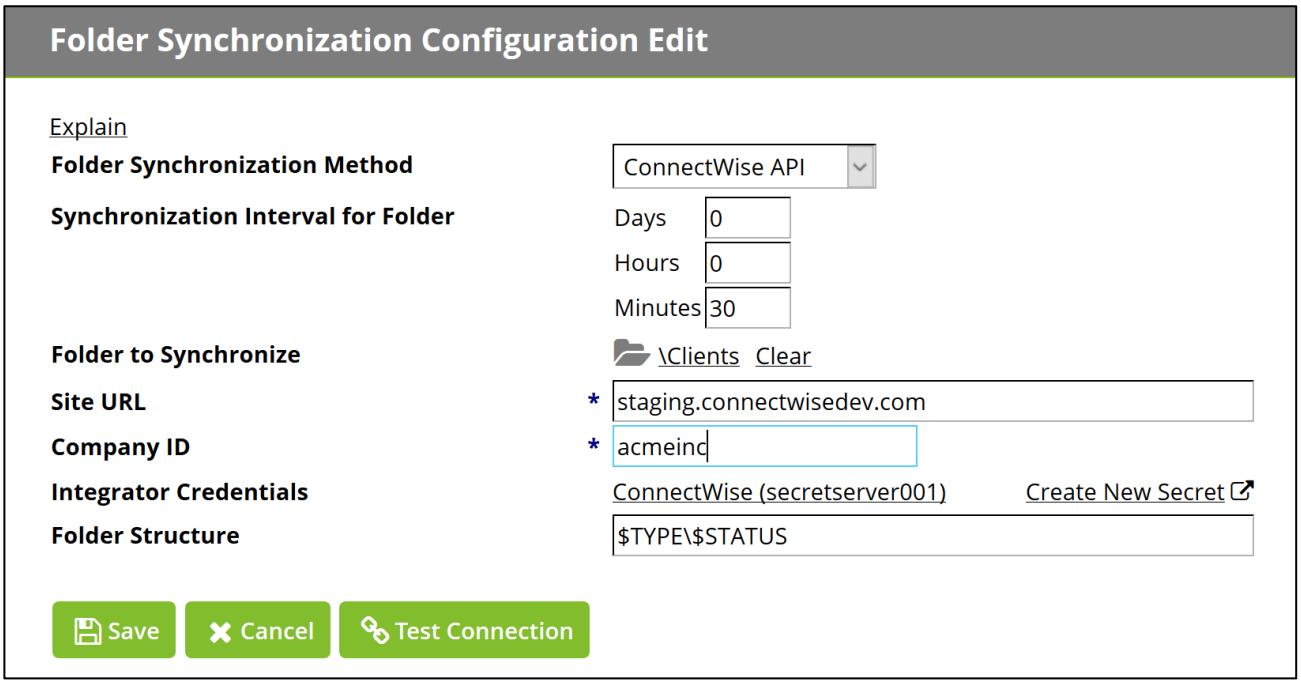
To edit the settings, you must have a Role assignment with Administer ConnectWise Integration permissions.

Enabling folder synchronization will require specifying the synchronization interval in days, hours, and minutes. The Folder to Synchronize is the parent folder where you are creating the folder structure. There are two methods of Folder Synchronization, through the ConnectWise API or through a database view.

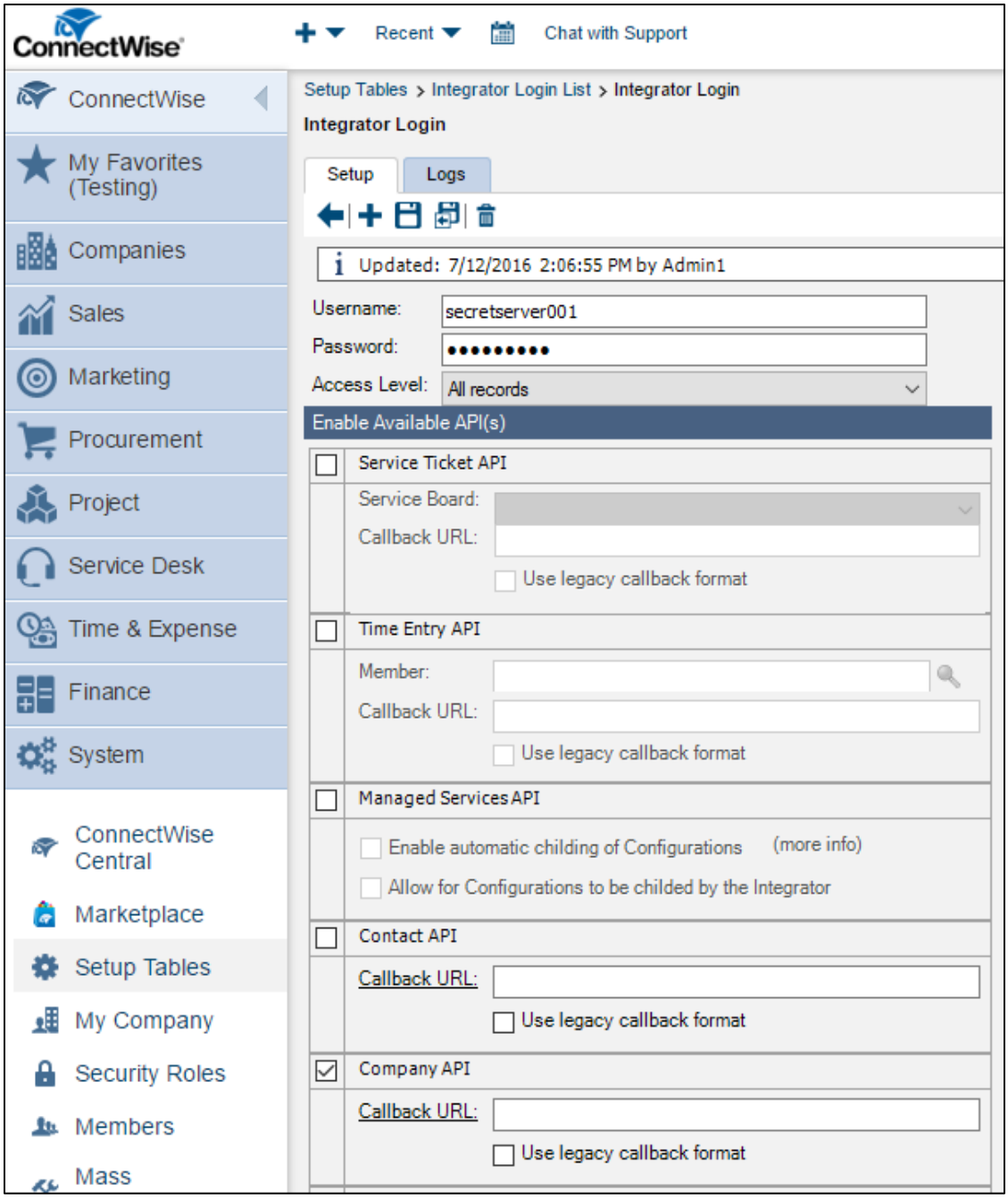
ConnectWise API

The ConnectWise API is the recommended way to synchronize folders from ConnectWise.

- Select **ConnectWise API** from the Folder Synchronization Method drop down.
- Enter your ConnectWise site name and select a ConnectWise integrator Secret for API Access.



- The Integrator account must have access to the Company API in ConnectWise and access to All Records



- Folder Structure defines how Folders will be named under the Clients folder. By default, $TYPE\$STATUS will create subfolders based on the customer type in connectwise, then further sorted by the active status in ConnectWise. For example, the active prospect “Acme Inc” in ConnectWise would get the following Folder created: Clients\Prospects\Active\Acme Inc
- Supported Folder Structure Tokens are:
    - $TYPE – Company Type i.e. Competition, Customer, Partner, Prospect, Suspect, Vendor etc...
    - $STATUS – Company Status i.e. Active, Inactive, not-Approved, etc...

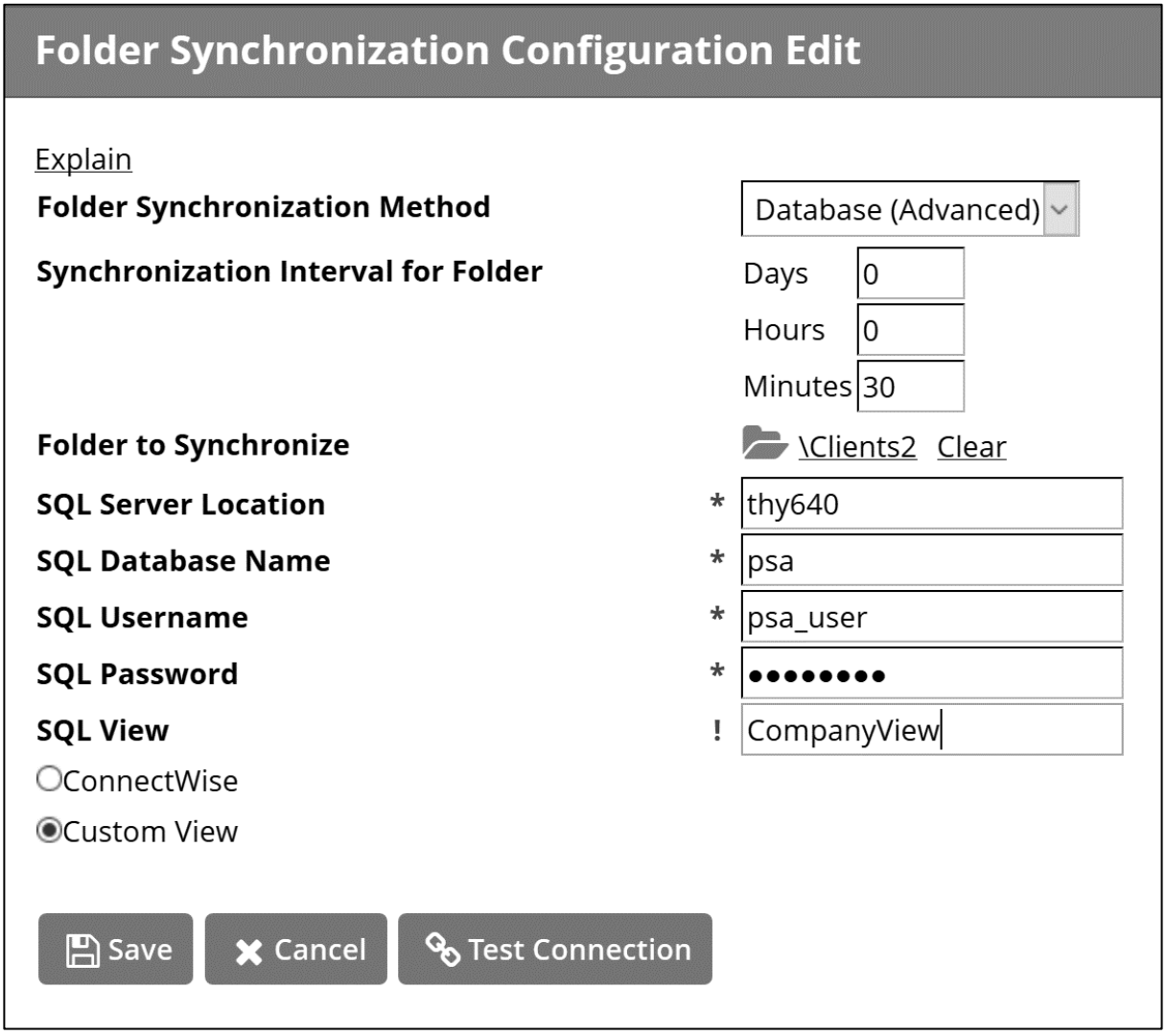
- $COMPANYINITIAL – First letter of company name. Use to organize companies into subfolders of A, B, C, etc....

- When configured, save and scroll down to the bottom and click **Synchronize Now** to run the synchronization

Database (Advanced)

The database synchronization method will query an on premises database for a custom view and parse company information out of it.

Enter the SQL Server Location, SQL Database Name, and the credential information for accessing the reference database, for example to your ConnectWise instance. The SQL View defaults to a standard ConnectWise customer layout but can be customized to meet the desired Folder Layout.



See the How to create a custom view for ConnectWise synchronization KB article for more advanced technical information on setting up the SQL View.

Users

Creating a User

To manually create a single user, navigate to Administration > Users and click the Create New button. On the subsequent page, you can enter the relevant information for a user.

To add many users from your Active Directory setup, you can use Active Directory synchronization (see Active Directory Synchronization).

Below is a brief explanation of each field:

User Name
Login name for the user.

Display Name
Text that is used throughout the user interface, such as in audits.

Email Address
Email address used for Request Access, email two-factor authentication, etc.

Domain
If a drop-down list is visible, selecting a domain from the list is one way to set the expected domain of the user. However, a more dynamic way to have this field (and all the other fields) set is through Active Directory synchronization.

Password
Login password for the user. For the various login settings, see Login Settings section.

Email Two-Factor Authentication
On a login attempt the user will have an email sent to the email address entered above. This email contains a pin code that the user must log into the account. See Email Two-Factor Authentication for more details.

RADIUS Two-Factor Authentication
This field will only appear if RADIUS authentication is enabled in the configuration. On a login attempt the user must enter the RADIUS token sent from the RADIUS server. See RADIUS Authentication section for more details.

RADIUS User Name
This field will only appear if the above RADIUS Two Factor Authentication setting is enabled. This is the username the RADIUS server is expecting. See RADIUS Authentication for more details.

Enabled

Disabling this field will remove this user from the system. Effectively, this is the way to delete a user. IBM Security Verify Privilege Vault does not allow complete deletion of users due to auditing requirements. To re-enable a user, navigate to the Administration > Users page, check the Show Inactive Users check box just under the users grid, and edit the user to mark them enabled (see Configuring Users for details).

Locked Out

If checked, then this user has been locked out of the system due to too many login failures. To remove the lock, uncheck the check box. For more details on locking out users, see Maximum Login Failures setting described in the Login Settings section.

Application Account

If checked, this user can only be used to access IBM Security Verify Privilege Vault through the Java Client/Console API and will not take up a license. See the Application Account KB for more information.

A new user will be assigned the Role called “User” by default. For more information on Roles, see the Roles section.

User Owners

User Administrators can also set another group or user as the User Owners for a IBM Security Verify Privilege Vault local user. User owners are able to manage and edit just that user. For example, a developer might need to unlock or reset the password for an Application Account but shouldn’t have access to all users. Set the Managed By to User Owners on a user and then select Groups or Users. Note that Unlimited Administrator mode can still be used to manage groups with User Owners assigned.

Configuring Users

User settings can be modified by clicking the username in the User Name column on the Users page. Search for users by using the search bar at the top of the grid. To show users that are marked inactive, check the Show Inactive Users box below the grid.

Bulk Operation

Bulk operations on users can also be performed from the Users page. Select one or more users by using the checkboxes beside the User Name column or select all or none by toggling the check box in the header row. Once the appropriate users have been selected, use the Bulk Operation drop-down menu at the bottom of the grid to select an action. Bulk operations on users currently include enabling or disabling user access as well as configuring users for email or RADIUS two-factor authentication.

Login Settings

IBM Security Verify Privilege Vault users can be set up with many different login requirements. For example, you can force strong Login passwords by requiring a minimum length and the use of various character sets.

The following settings are available under the Administration > Configuration page, inside the Login tab:

Allow Remember Me
This option enables the Remember Me check box on the Login screen. When a user chooses to use Remember Me, an encrypted cookie will be set in their browser. This will enable the user to revisit IBM Security Verify Privilege Vault without the need to log in. This cookie will no longer be valid when the Remember Me period has expired. They will then have to enter their login information again. This option allows users to remain logged in for up to a specific period of time (specified in the Remember Me is valid for setting mentioned below). This option can be a security concern as it does not require re-entry of credentials to gain access to IBM Security Verify Privilege Vault.

Remember Me is only visible if Allow Remember Me is enabled. This is the period of time that the Remember Me cookie mentioned above will be valid.

For example: if set to one day, then users taking advantage of Remember Me will have to log in at least once a day. To set a time value (Minutes, Hours, or Days), uncheck the Unlimited check box.

Allow AutoComplete
AutoComplete is a feature provided by most web browsers to automatically remember and pre-fill forms for you. This can be a great security concern since they typically do not save the data in a secure manner. You can enable or disable web browser pre-fill on the login screen by using this option.

Maximum Login Failures
Set the number of login attempts allowed before a user is locked out of their account. Once locked out, they will need a IBM Security Verify Privilege Vault administrator to reset their password and enable their account. For details on how to reset a locked account, see the Creating a User section.

Visual Encrypted Keyboard Enabled
This setting will enable a visual keyboard for logins.

Visual Encrypted Keyboard Required
This setting will require a visual keyboard for logins.

Require Two Factor for these Login Types
This setting specifies which types of login require two factor:

- **Website and Web Service Login**
- **Website Login only**
- **Web Service Login only**

Maximum Concurrent Logins Per User
This setting allows a user to log into IBM Security Verify Privilege Vault from multiple locations at once without logging out their sessions at other locations.

Enable RADIUS Integration
Allow for RADIUS server integration with your user login authentication. Other RADIUS settings appear upon enabling this option. These settings are discussed in the RADIUS Authentication section.

Password Settings

The following settings are found in the Administration > Configuration page, inside the Local User Passwords tab. These settings apply to users that were created manually, not users brought into IBM Security Verify Privilege Vault through Active Directory synchronization:

Allow Users to Reset Forgotten Passwords
If enabled, the Forgot your password? link appears on all users' login screens. Clicking on this link will prompt the user to enter the email address that is associated with the user's IBM Security Verify Privilege Vault account. If the email address is found, then an email containing a link for password reset will be sent. Note that this only works for local user accounts and not for Active Directory accounts.

Symbols Required for Passwords
Force all user IBM Security Verify Privilege Vault login passwords to contain at least one symbol (i.e., !@#$%^&*).

Lowercase Letters Required for Passwords
Force all user IBM Security Verify Privilege Vault login passwords to contain at least one lowercase letter.

Uppercase Letters Required for Passwords
Force all user IBM Security Verify Privilege Vault login passwords to contain at least one uppercase letter.

Numbers Required for Passwords
Force all user IBM Security Verify Privilege Vault login passwords to contain at least one number.

Minimum Password Length
Force all user IBM Security Verify Privilege Vault login passwords to contain at least this many characters.

Enable Local User Password Expiration
When enabled, IBM Security Verify Privilege Vault will force a password change for a user after a set interval elapses. After the interval time has elapsed, the next time the user attempts to log in they will be prompted for the old password, a new password, and a confirmation of the new password. The new password will be validated against all the password requirements (see the earlier settings – Symbols Required for Passwords, and so on). Newly created local users will also be prompted to change their password upon logging into IBM Security Verify Privilege Vault for the first time when this setting is enabled.

Local User Password is valid for
If enabled, this is the interval that a local user password will be valid before it must be changed (see Enable Local User Password Expiration setting for details). If this setting is disabled, the entered value displays as “Unlimited”.

Enable Minimum Local User Password Age
If enabled, the value for this setting reflects the minimum amount of time that needs to elapse before a password can be changed. This will prevent a user from changing their password too frequently, which will allow them to quickly re-use old password.

Enable Local User Password History
If enabled, this will prevent a user from reusing a password. For example, if set to “20 Passwords”, this will prevent the user from using a password they have used the previous 20 times. This in conjunction with Enable Minimum Local Password Age will help ensure that users are using a new and unique password frequently rather than recycling old passwords.

Restriction Settings

The following restriction settings are available:

Force Inactivity Timeout
This setting is the time limit on idle IBM Security Verify Privilege Vault sessions. Once a session expires, the user must login again with their username and password.

IP Restrictions
This setting can be entered by going to Administration > IP Addresses. In there, you can enter the IP ranges you want your users to use. To configure a user to use the ranges, navigate to the User View page and click the Change IP Restrictions button. In the subsequent page, you can add all the ranges you want your user to use.

Login Policy Agreement
The Login Policy Agreement is displayed on the login screen. You can change the contents of the Login Policy Statement by editing the file "policy.txt". By default, this is not enabled. The settings to enable this are accessed by first navigating to Administration > Configuration and going into the Login tab. From here, click the Login Policy Agreement button.

- **Enable Login Policy**
  If enabled, this will simply display the policy. To force the acceptance of the policy, see Force Login Policy below.

- **Force Login Policy**
  This setting will force the checking of the “I accept these terms” check box before allowing the user to login to IBM Security Verify Privilege Vault.

Active Directory Synchronization

IBM Security Verify Privilege Vault can integrate with Active Directory by allowing users to login to IBM Security Verify Privilege Vault by using their Active Directory credentials. Microsoft Active Directory is a component of the Windows Server System that allows a centralized location of user management for a Windows Network. IBM Security Verify Privilege Vault synchronizes Active Directory users from a Security Group in a Domain at a scheduled interval. IBM Security Verify Privilege Vault does not store the Domain user's passwords. Instead, it will pass through the credentials to the Domain for authentication. To synchronize with Active Directory, specify the Domain to Synchronize Groups from, and then select the Groups that IBM Security Verify Privilege Vault will use to replicate users and membership. When a new user is pulled in from Active Directory, IBM Security Verify Privilege Vault will also replicate the email address if one is populated. IBM Security Verify Privilege Vault can synchronize with multiple Domains.

Create a Sync Secret

Before synchronizing or creating users, you'll need to create a secret to be used as the **Sync Secret**. This secret should contain Domain Admin credentials (or an account with appropriate permissions to Search and View the attributes to all your organization's users and groups).

Adding a Domain

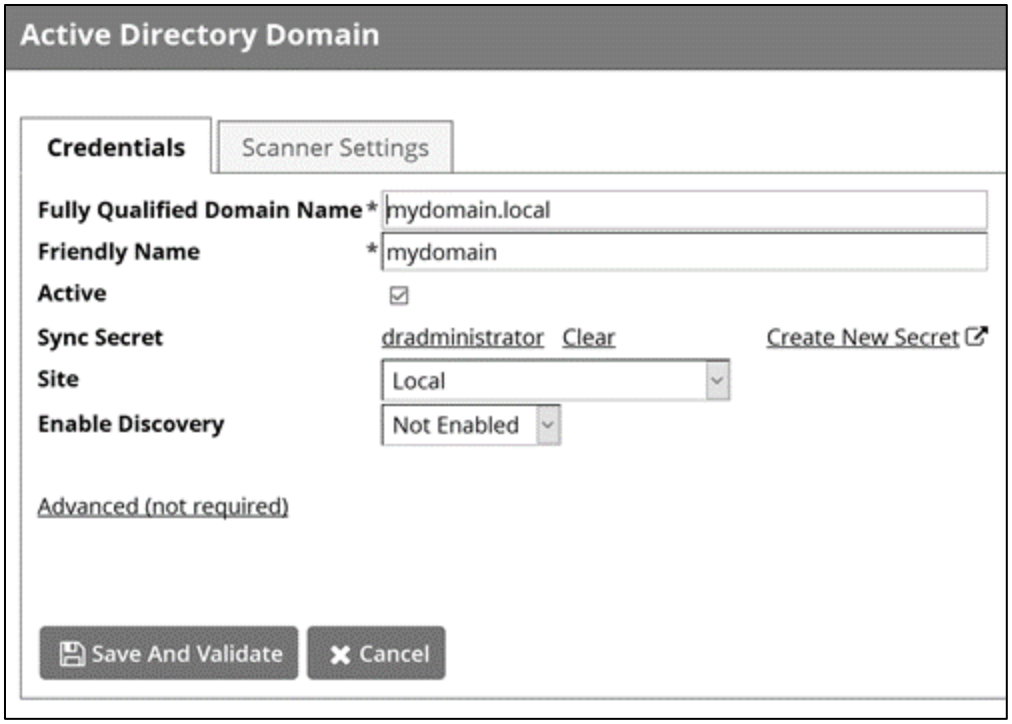
From the **Admin | Active Directory** page, click **Edit Domains** and then **Create New** to add a new Active Directory domain.

If you want to use Secure LDAP, enable the **Use LDAPS** check box under the **Advanced** section. For more information on Secure LDAP, please see the Using Secure LDAP KB Article.

It is possible to **automatically enable Two Factor Authentication** for users synchronized from this domain. This option is also available under the **Advanced** section via dropdown list.

Local Site versus Distributed Engine Site

When synchronizing with Active Directory, you have two choices for how IBM Security Verify Privilege Vault connects to the domain: from the web server *OR* routed through Distributed Engine. If your web server can reach your domain without issue, then by using the Local Site option is recommended. When a user authenticates or AD synchronization is run, the connection to the domain will be from the web server. If your web server can't connect to the target domain, if it's a VM in a cloud environment for example, you can setup an Engine on-premises and assign it to the domain. When a user authenticates, IBM Security Verify Privilege Vault will route the domain calls through the on-premises engine, eliminating the need for site to site connections or persistent VPN's. Review the Distributed Engine guide for steps on setting up Sites and Engines.



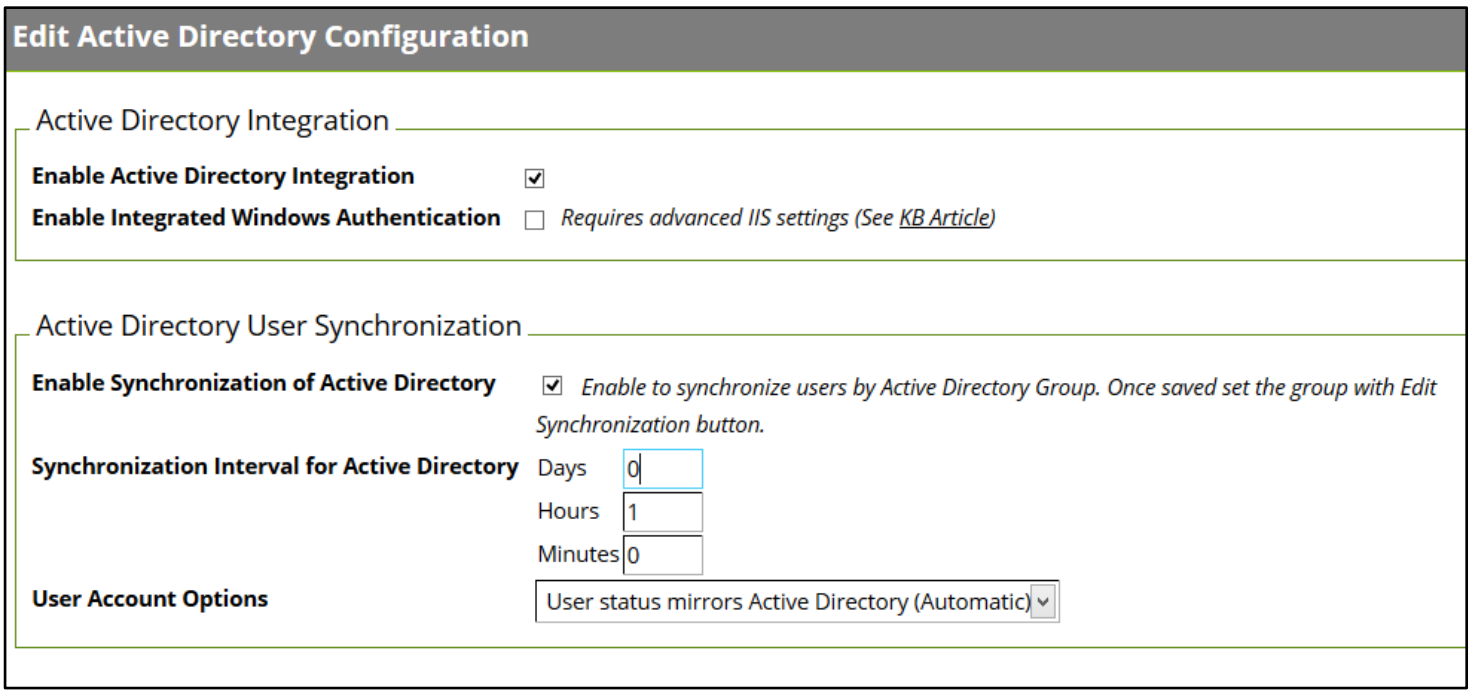
The Active Directory Secret will be used to synchronize users and groups, it will require permission to search and view the attributes of the users and groups. If you plan on using Discovery, the account will also need permissions to scan computers on the network for accounts.

Setting up a Synchronization Group

Once a domain has been added, the Synchronization Groups needs to be set by clicking the Edit Synchronization button on the Active Directory Configuration page. The Available Groups represent all accessible groups on the specified Active Directory domain. The user membership can be previewed with the Group Preview control. Select the desired group from the Available Groups that contains the Active Directory accounts for users you would like to create in IBM Security Verify Privilege Vault. If the specific group does not exist, one can be created by your Active Directory administrator. If you create domain users manually or converting local users to domain users, then see the corresponding sections below before setting the synchronization group.

Configuring Active Directory

Active Directory configuration can be enabled by a user with the "Administer Active Directory" Role. To change these settings, select **Active Directory** from the **Administration** menu and then click **Edit**.



The configuration screen offers several options:

Enable Active Directory Integration
Enable or disable the Active Directory Integration feature.

Enable Synchronization of Active Directory
Enable or disable the automatic synchronization of the selected Synchronization Groups from Active Directory. If you have manually added users and will not be using the Synchronization Group, do not enable this setting or manual users can be locked out.

Enable Integrated Windows Authentication
Enable or disable the Windows Integrated Authentication feature.

Synchronization Interval for Active Directory
Set the interval that IBM Security Verify Privilege Vault will synchronize its users and Groups with the Active Directory.

User Account Options

- **Users are enabled by default (Manual)**
  IBM Security Verify Privilege Vault users will automatically be enabled when they are synced as new users from Active Directory. If they were disabled explicitly in IBM Security Verify Privilege Vault, they will not be automatically re-enabled. If creating a new user will cause the user count to exceed your license limit, the user is created as disabled.

- **Users are disabled by default (Manual)**
  IBM Security Verify Privilege Vault users will automatically be disabled when they are pulled in as new users from Active Directory. If they were enabled explicitly in IBM Security Verify Privilege Vault, they will not be automatically re-disabled.

- **User status mirrors Active Directory (Automatic)**
  When a new user is pulled in from Active Directory, they will be automatically enabled if active on the domain. The exception is when this will cause you to exceed your license count. For existing users, they will automatically be disabled if they are removed from all synchronization groups, deleted in AD, or disabled in AD. They are automatically re-enabled when they are part of a synchronization group and are active in AD.

Creating an Active Directory User

Active Directory users can be created manually by a user that has the Administer Users Role. You can do this by going to Administration > Users, then clicking the Create New button.

Converting Local Users to Domain Users

Local users can be converted to a domain user in a one-way irreversible process. This feature helps existing customers with extensive groups and permissions setup for a local user that they want to convert to an Active Directory user. The page can be accessed on the Administration > Users page by clicking the Migrate To AD button. For the conversion to work the domain user must not exist within IBM Security Verify Privilege Vault. The username will be changed to match the domain user throughout the system.

Unlocking Local Accounts

If a user fails their login too many times (specified in the Local User Passwords section of the configuration page), their account will be locked out and they won't be able to log in. To unlock the account, log in as an administrator, click Administration, then on Users, and then click the user who is locked out. Next, click Edit, uncheck the Locked Out check box, and save.

Advanced Authentication

IBM Security Verify Privilege Vault provides integration options for Windows authentication and SAML to automatically authenticate users to the application when they browse to IBM Security Verify Privilege Vault on their workstations.

Integrated Windows Authentication

Windows Integrated Authentication allows Active Directory users that are synced with IBM Security Verify Privilege Vault to log into workstations and be automatically authenticated to the application. A user's Active Directory credentials are automatically passed through to IIS, logging them into the site.

For further information, Microsoft has a knowledge base article troubleshooting some common client-side issues with integrated authentication.

Enable Integrated Windows Authentication:

Active Directory Integration and Synchronization must be enabled before configuring integrated Windows authentication. For details, see the Active Directory Synchronization section.

- Navigate to Administration > Active Directory, and click Edit.
- Check the enable Integrated Windows Authentication box. Click Save.

Configure IIS

Open IIS and highlight your IBM Security Verify Privilege Vault website or application. In the right pane, double-click Authentication.

Enable Windows Authentication and disable Anonymous Authentication.

For additional information on requirements and troubleshooting, see our KB article on Integrated Windows Authentication.

Logging in as a Local Account

After you have set up Integrated Windows Authentication, you might sometimes want to log in as a local admin account to configure IBM Security Verify Privilege Vault, perform an upgrade, or if AD is down.

First, do one of the following:

- Log in to your computer as an Active Directory account that has Read access to the IBM Security Verify Privilege Vault application directory but is not enabled in IBM Security Verify Privilege Vault.
- Browse to IBM Security Verify Privilege Vault by using Firefox or Chrome.

Next, go to your IBM Security Verify Privilege Vault website. You might be prompted for your AD credentials. If you are, log in as a user with Read access to the IBM Security Verify Privilege Vault application directory that is not enabled in IBM Security Verify Privilege Vault. You should then be redirected to the login page of IBM Security Verify Privilege Vault. Select the “local” domain and enter your local account username and password.

SAML

IBM Security Verify Privilege Vault provides the option to integrate your SAML implementation to automatically authenticate users to the application. See the following sections to configure SAML integration with IBM Security Verify Privilege Vault in your environment.

Enable SAML

Navigate to Administration > Configuration, then click the Login tab. Click Edit and check the Enable SAML Integration box. Enter a SAML Username Attribute, if necessary (this is optional).

Perform the Backend SAML Configuration

There are three parts to the backend configuration for SAML. After performing the following steps, recycle IBM Security Verify Privilege Vault's application pool in IIS to allow the updated settings to take effect.

Step 1: Enable the SAML configuration file (saml.config)
Copy the saml.config.template to saml.config. This, along with setting Enable SAML Integration in the IBM Security Verify Privilege Vault login configuration page, turns on SAML in your IBM Security Verify Privilege Vault installation.

Step 2: Modify the IBM Security Verify Privilege Vault SAML configuration file according your IdP settings
First, complete the ServiceProvider section in the saml.config file:

- Choose an EntityId for your IBM Security Verify Privilege Vault instance. By default, the EntityId in the file is: 'urn:componentspace:SecretServerServiceProvider'. Type this into the [EntityIdForYourSecretServerServiceProvider] section of the saml.config file.
- Verify the AssertionConsumerServiceUrl is: ~/SAML/AssertionConsumerService.aspx.
- Specify the certificate to use (see next section).

Next, complete the PartnerIdentityProvider section in the saml.config file:

- Specify the EntityId of the Identity Provider in the Name attribute..
- Specify the SingleSignOnServiceUrl (the URL on the IdP where users go to sign in).
- Specify the SingleLogoutServiceUrl (the URL on the IDP where users go to sign out).
- Specify the certificate to use (see next section).
- Specify additional options, such as encryption and signing. See this document on SAML for details on these optional settings.

IBM Security Verify Privilege Vault currently supports only one Identity Provider at a time.

Step 3: Specify a certificate for SAML

X.509 certificates are used for XML signatures and XML encryption. A certificate for SAML can be specified in a number of different ways within the saml.config file. A certificate might be stored in a file or the Windows certificate store.

If the certificate is stored on the file system:

- Specify a CertificateFile. This can be an absolute path or a path relative to the application folder.
- Specify a CertificatePassword. This is the password associated with the certificate file. Certificate files (*.pfx) that include the private key should be protected by a password. For a production certificate, the password should be stored encrypted in web.config. Refer to the CertificatePasswordKey attribute directly below for more details.
- Specify a CertificatePasswordKey. This specifies the web.config's appSettings key for the certificate file password. For example, if the CertificatePasswordKey attribute value is localCertificatePassword, then under the web.config's appSettings section an entry with the key name localCertificatePassword is expected and the entry value is used as the password. By encrypting the appSettings section by using the aspnet_regiis utility, the certificate file password is secured.

If the certificate is stored in the Windows certificate store, one of the following methods must be used to reference the certificate:

- Specify a CertificateSerialNumber attribute. Specifies the X.509 certificate by serial number within the certificate store.
- Specify a CertificateThumbprint attribute. Specifies the X.509 certificate by thumbprint within the certificate store.
- Specify a CertificateSubject attribute. Specifies the X.509 certificate by subject within the certificate store.

Step 4: Modify the IdP's metadata for IBM Security Verify Privilege Vault integration

Following the instructions provided by your IdP, add the appropriate entries for IBM Security Verify Privilege Vault as a Service Provider. For an example, see this document on SAML.

- IBM Security Verify Privilege Vault's assertion consumer service is located at: https://<PATH TO YOUR IBM SECURITY VERIFY PRIVILEGE VAULT>/SAML/AssertionConsumerService.aspx
- IBM Security Verify Privilege Vault's SingleLogoutService is located at: https://<PATH TO YOUR IBM SECURITY VERIFY PRIVILEGE VAULT>//SAML/sloservice.aspx
- IBM Security Verify Privilege Vault's EntityId (or URN or other similar reference) is the EntityId chosen in Step 2 above.
- Modify the IBM Security Verify Privilege Vault SAML configuration file to match your IdP settings.

User Preferences

Users can set their preferences by hovering on their profile icon in the top right and selecting preferences.

General Tab

The following configuration settings are available for users under the General tab:

Mask passwords when viewing Secrets
When enabled, this will mask the Password field for a Secret. There is a configuration setting that will force this to be enabled for all users. For details on password masking, see Setting up Password Masking in the Secret section.

Send email alerts when dependencies fail to update
Enables emails to be sent when dependencies fail to update. For further explanation of this, see the Dependency Finder section.

Send email alerts when Secrets are changed
Enables emails to be sent on all changes of any Secret that the user has View permission. There is a limit of one email per five minutes per edit of the same user. For example, if user “User1” edits the Secret twice within this grace period, only one email will be sent.

Send email alerts when Secrets are viewed
Enables emails to be sent on all views of any Secret that the user has View permission. There is a limit of one email per five minutes per view of the same user. For example, if user “User1” views the Secret twice within this grace period, only one email will be sent.

Send email alerts when Heartbeat fails for Secrets
When enabled, the user will be emailed when Heartbeat fails for any Secret the user has View permission to.

Show the full folder path on search results
Enables the full path to be displayed in the folder column on the Home page.

Use the TreeView control for search on the home screen
Enables the TreeView control for the Search tab on the Legacy Home screen. This option does not apply to the Dashboard.

Date Format and Time Format
Date and time format displayed for a user in IBM Security Verify Privilege Vault.

Language and My Theme
Customize the look of IBM Security Verify Privilege Vault on a per user basis. For details, see the Customizing the Look section.

Launcher Tab

The following configuration settings are available to users on the Launcher tab:

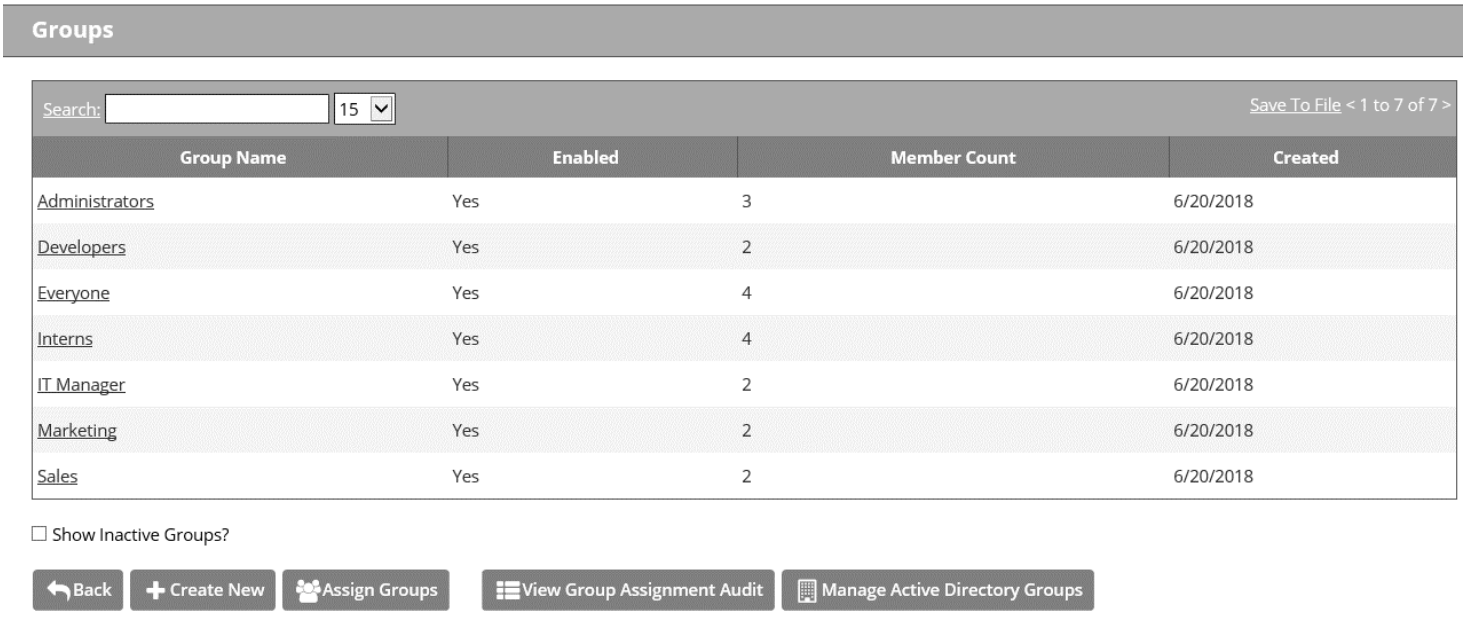
Connect to Console
Allows you to connect to remote machines by using the Remote Desktop Launcher and will connect as an administrator. This is the equivalent of using the /admin or /console switch when launching Remote Desktop.

Allow Access to Printers, Allow Access to Drives, Allow Access to Clipboard
Allow the various items when using the Launcher. See the Launcher section for more details.

Use Custom Window Size
Checking this box displays Width and Height fields for the user to specify a custom window size for the RDP Launcher.

Groups

IBM Security Verify Privilege Vault allows administrators to manage users through groups. Users can belong to different groups and receive the sharing permissions, as well as roles, attributed to those groups. This setup simplifies the management of the various permissions and roles that can be assigned to a user. Additionally, groups can be synchronized with Active Directory to further simplify management.



Creating a Group

You can create and edit groups from the Groups page. You can get to the Groups page by navigating to Administration > Groups. By either selecting an already existing group from the list, or clicking Create New, you can modify or add the group.

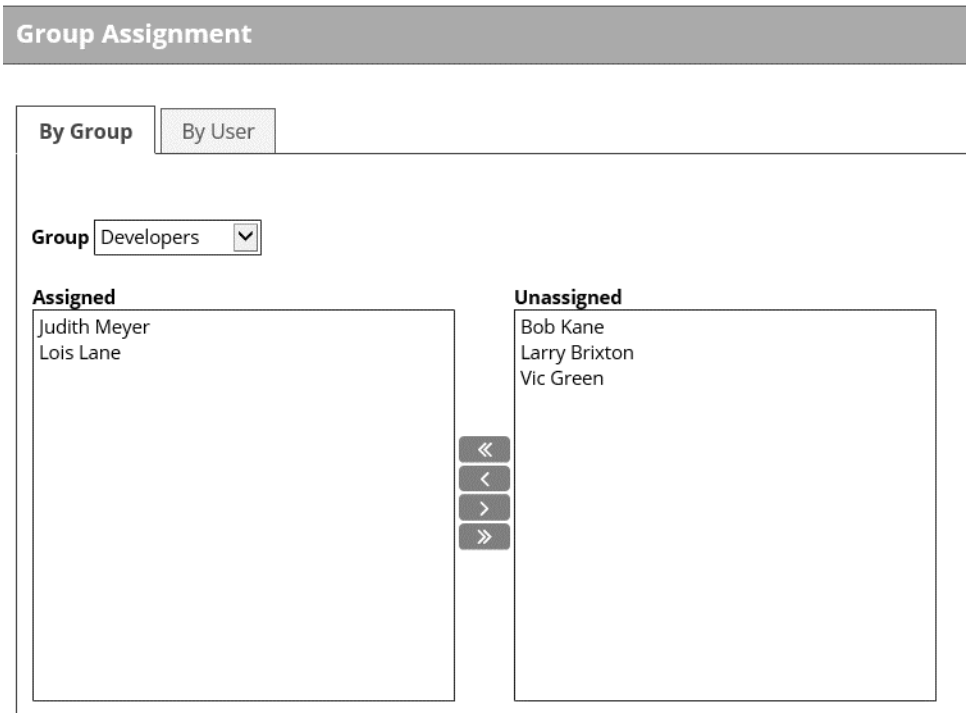
To add groups and the users inside them from your Active Directory setup, you can use Active Directory synchronization (see Active Directory Synchronization section).

Adding Users to a Group

On the Group View page, users can be added and removed from the group. Use the arrow buttons to move users into and out of the current group. If needed, a group can also be enabled or disabled from this page. When you have finished with your changes, click the Save button and your new group members will be added.

Group Assignment

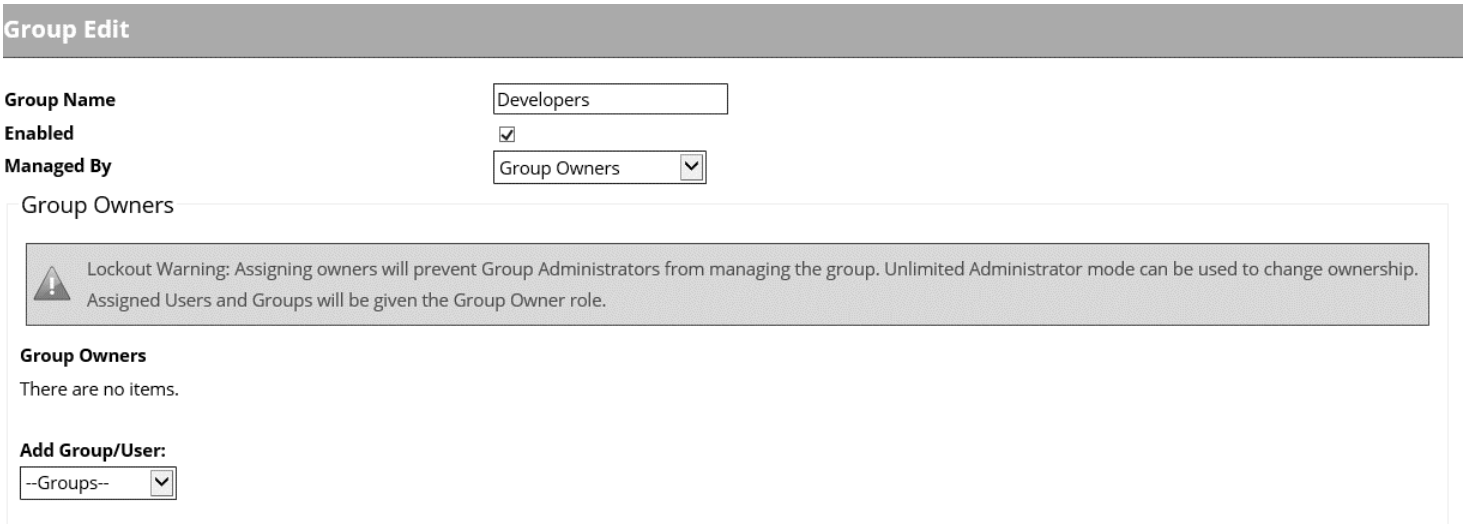
Alternatively, you can click the Assign Groups button on the main Groups page. This will allow you to select a group from a drop-down list and assign or unassign users to the group. In the By User tab, you can select a user from a drop-down list, and assign or unassign the user from the groups in the selectable list boxes.



If the group was created by using Active Directory synchronization, this group will not be editable. See the Active Directory Synchronization section for details on adding and removing users by using Active Directory synchronization.

Group Owners

Group Administrators can also set another group or user as the Group Owners for a IBM Security Verify Privilege Vault local group. Group owners are able to manage membership just for that Group. Set the Managed By to Group Owners on a local group and then select Groups or Users. Note that Unlimited Administrator mode can still be used to manage groups with Group Owners assigned.



Roles

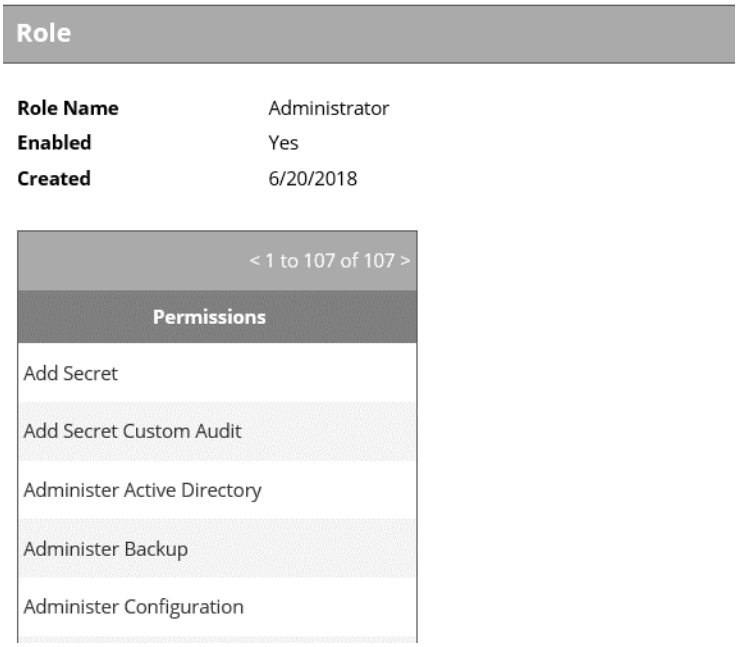
Modeled after the role-based access control mechanism (RBAC), role-based security (RBS) is IBM Security Verify Privilege Vault's method of regulating permission to system access. Each user and group must be assigned to a role. IBM Security Verify Privilege Vault ships with three roles: Administrator, User, and Read-Only User. Each role contains various permissions to match the job function of the user. With RBS, strict granular access to IBM Security Verify Privilege Vault is ensured. A list of role permissions and their descriptions can be found in this KB article.

Multiple permissions can be assigned to a role. For example, you might assign Administer Users, Edit Secret, Share Secret, and View Active Directory permissions to a role. That role can then be assigned to a user or group.

The Unlimited Administrator permission will allow the user to have Unlimited Administrator rights when Unlimited Administrator is enabled in the configuration. By default, it is disabled. See the Unlimited Administrator section for more information.

Creating a Role

You can create roles from the Roles page. To get to the Roles page, navigate to Administration > Roles. Click the Create New button to add the role.



Editing Permissions for a Role

To add or remove permissions to an existing role, click the Role Name of the role you want to edit.

On this Role View page, permissions can be added and removed from the role by clicking the Edit button. Use the arrow buttons to move permissions into and out of the current role. If needed, a role can also be enabled or disabled from this page. If you have finished with your changes, you must click the Save button to have the changes take effect.

Assigning Roles to a User

To assign roles to a user, click the Assign Roles button on the main Roles page. Depending on which tab is selected, this page will allow you either view the roles that are assigned to users or view the users that are assigned to roles. To change these settings, click the Edit button. Now select a role from the drop-down list and assign or unassign users to the role. In the By User or Group tab, you can select a user or group from the drop-down list and assign or unassign roles to them in the selectable list boxes.

IP Address Restrictions

IP Address Restrictions allow you to control which IP Address ranges users can use to log in to IBM Security Verify Privilege Vault.

Creating an IP Address Range

To create an IP Address Range, go to the IP Addresses under Administration. Once there, click the Create New button. In the IP Address/Network Name text box, enter a descriptive name for your range. In the IP Address Range text box, enter an IP Address or IP Address range. IBM Security Verify Privilege Vault supports single IP Addresses (i.e., 10.0.0.4), a range separated by a hyphen (i.e., 10.0.0.1-10.0.0.255), and CIDR notation (i.e., 10.0.0.0/24). Finally, click Save.

Editing and Deleting an IP Address Range

To edit an IP Address Range, go to the IP Addresses page, click a range, and click Edit. To delete a range, click the range and click the Delete button.

Assigning an IP Address Range

To assign a range to a user, go to the Users page under administration, click a user name, and click Change IP Restrictions. Next, check or uncheck the boxes next to the ranges to choose which IP Addresses a user can use to access IBM Security Verify Privilege Vault. If no boxes are checked, the user can access IBM Security Verify Privilege Vault through any IP Address.

Regardless of the restrictions, users can always log in when accessing IBM Security Verify Privilege Vault on the server by using a local IP address (127.0.0.1 or ::1). This is prevents total lockout from IBM Security Verify Privilege Vault.

Administration

IBM Security Verify Privilege Vault is a highly customizable application. Administrators can increase site security through various configuration settings such as force inactivity timeouts and specifying a SMTP server. This level of configuration allows IBM Security Verify Privilege Vault to be altered to meet the needed requirements for the instance. The settings are explained below.

General Tab

The following configuration settings are available in the General tab:

Allow Automatic Checks for Software Updates
Enable this option to be notified of a new IBM Security Verify Privilege Vault release. If a new update is available, displayed at the top of each IBM Security Verify Privilege Vault page will be a link to the latest update. This feature is only available to those with Support licenses.

Enable Webservices
Enable other applications to interact with IBM Security Verify Privilege Vault (still requires them to login as a IBM Security Verify Privilege Vault user).

Maximum Time for Offline Access on Mobile Devices
Amount of time that a mobile device can be disconnected from the server before it removes cached IBM Security Verify Privilege Vault data from the device.

Session Timeout for Webservices
Set a session time limit on use of the web services API. Once the web services session token expires, the user must login again with their username and password.

Prevent Application from Sleeping When Idle
Prevents the application pool that IBM Security Verify Privilege Vault is running under from going to sleep.

Enable Syslog/CEF Logging
Allow IBM Security Verify Privilege Vault to export logs to a SIEM tool server

WinRM Endpoint URL
URL for WinRM, which is used for PowerShell hooks.

Enable CredSSP Authentication for WinRM
Allow credential delegation for PowerShell scripts that might need to access resources outside of the IBM Security Verify Privilege Vault machine.

Force Inactivity Timeout
This setting is used to time out a user's login after inactivity for the specified time interval. See Configuring Users for more details.

Force Password Masking
For more information, see Setting up Password Masking.

Require Folder for Secrets
Enable this setting to force users to select a folder to place a Secret in when creating or moving a Secret. See Folders for more details.

Prevent Application from Sleeping When Idle
Prevents the application pool that IBM Security Verify Privilege Vault is running under from going to sleep.

Allow Approval for Access from Email
Adds links in Request for Approval emails allowing approvers to approve or deny access to a Secret without logging into IBM Security Verify Privilege Vault. See Requires Approval for Access for details.

Secret View Interval Minutes
The number of minutes after which users must enter another comment when Require Comment is enabled.

Default Theme
Select the default IBM Security Verify Privilege Vault theme users will see. See Customizing the Look for more information.

Allow Users to Select Themes
Allows users to customize the theme for IBM Security Verify Privilege Vault. This selected theme would only apply to their login. See the Customizing the Look section for more details.

Enable Launcher
Enables Remote Desktop Launcher capabilities for IBM Security Verify Privilege Vault. See the Launcher section for further details.

Launcher Deployment Type
Select either Protocol Handler (default) or ClickOnce. See the Launcher section for further details.

Allow IBM Security Verify Privilege Vault to Retrieve Website Content
Enables the Web Launcher to retrieve the web site content in order to parse the form and find the login controls.

Allow Web Launcher Mappings to be Downloaded
Enables the Web Launcher Configuration to download pre-approved website launcher settings.

Allow Web Launcher Mappings to be Uploaded Off-site
Enables the user to upload successful Web Launcher Configurations where they will be approved and shared with other IBM Security Verify Privilege Vault users.

There will not be any Secret data uploaded to the product website, only the website URL and control names are sent.

Default Secret Permissions
See the Folders section for more information.

Time Zone
Time zone that all dates will be displayed in.

Default Date, Time Format
Default date/time format used for all users. This setting can be overridden by each user. See User Preferences for more details.

Secret Password History
Enforces whether a recent password can be set on a Secret's password field based on the history. Defaults to 1, which means the same password cannot be immediately re-used on a Secret.

Change Administration Mode
This button will take you to a page where you can enable or disable Unlimited Administration mode. See Unlimited Administration for details.

Login Tab

The Login tab contains the following options:

Allow Remember Me
This option enables the “Remember Me” check box on the login screen. When a user chooses to use “Remember Me”, an encrypted cookie will be set in their browser. This will enable the user to revisit IBM Security Verify Privilege Vault without the need to login. This cookie will no longer be valid when the “Remember Me” period has expired and they will have to log in again.

Allow AutoComplete
AutoComplete is a feature provided by most web browsers to automatically remember and prefill forms for you. This can be a great security concern since they typically do not save the data in a secure manner. You can enable or disable web browser prefill on the Login screen by using this option.

Enable Login Failure CAPTCHA
Enforces a CAPTCHA image if the user fails one or more logins to prevent brute force attacks of user credentials or brute force lockouts.

Maximum Login Failures
Set the number of login attempts allowed before a user is locked out of their account. Once locked out, they will need a IBM Security Verify Privilege Vault administrator to reset their password and enable their account.

Default Login Domain
Allows for the selection of a default domain for user login.

Visual Encrypted Keyboard Enabled
Enables or disables the Visual Encrypted Keyboard for logins.

Visual Encrypted Keyboard Required
Require the Visual Keyboard for logins.

Require Two Factor for these Login Types
Require Two Factor for these Login Types when Two Factor is enabled on the specific user logging into IBM Security Verify Privilege Vault. You can choose from a drop-down list to enable it for Website, Web Service, or both.

Enable RADIUS Integration
Enabling RADIUS integration will allow another form of two factor authentication for users.

Enable Duo Security Integration
Enabling Duo Integration will allow users to use Duo two factor as a form of two factor authentication.

Enable SAML Integration
Enabling SAML Integration will allow users to log-in to IBM Security Verify Privilege Vault by using your SAML Identity Provider.

Folders Tab

The Folders tab contains the following configuration options:

Require View Permission on Specific Folder for Visibility
Users will only see folders they have View permissions on.

Enable Personal Folders
Each user will have a personal folder created and assigned to them.

Personal Folder Name
The name of the root personal folder. Each user's personal folder will be named based on the user.

Show user warning message
Enable warning message for users when creating Secrets.

Warning Message Text
Warning message to display to the users, instructing them to store only work-related data in IBM Security Verify Privilege Vault.

Local User Passwords Tab

This tab contains the following configuration options:

Allow Users to Reset Forgotten Passwords
Allows users to reset their passwords in case they forget it.

Symbols Required for Passwords
Force all local users to include special characters within their login passwords (ie. %#@).

Lowercase Letters Required for Passwords
Force all local users to include lowercase letters within their login passwords.

Uppercase Letters Required for Passwords
Force all local users to include uppercase letters within their login passwords.

Numbers Required for Passwords
Force all local users to include numbers within their login passwords.

Minimum Password Length
Require a minimum length on all local users' login passwords.

Enable Local User Password Expiration
Local User's passwords will expire after a specified interval.

Local User Password is valid for
Specifies the maximum time a Local User can keep a password.

Enable Minimum Local User Password Age
Local Users cannot change their passwords until the password meets a minimum age.

Enable Local User Password History
Local Users cannot change their password if it has been recently used.

Security Tab

The Security tab contains the following configuration options:

Force HTTPS/SSL
Require HTTPS; users will not be able to access IBM Security Verify Privilege Vault by using HTTP.

Enable HSTS
Enable HTTP Strict Transport Security. Not available if Force HTTPS/SSL is turned off.

Allow HTTP Get
Allows the Http Get verb for Web Services. This allows REST-style calls to many Web Service methods but reduces security.

Frame Blocking
Prevents users from accessing the IBM Security Verify Privilege Vault site if it is embedded in an iFrame.

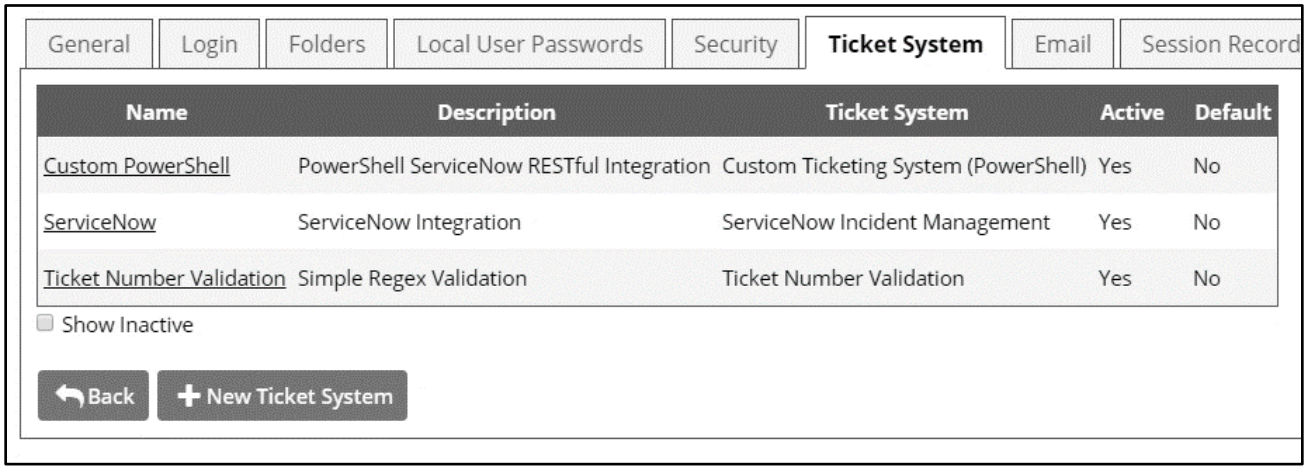
Enable FIPS Compliance
See the FIPS Compliance section.

Encrypt Key by using DPAPI
This will encrypt the IBM Security Verify Privilege Vault AES 256 key by using the machine key. It provides protection from admins copying IBM Security Verify Privilege Vault from the server to their own machine. Note that a backup of the encryption key should be made before using this option. Otherwise, disaster recovery will be impossible if the server dies. After encrypting the key, an administrator of IBM Security Verify Privilege Vault will be able to decrypt it.

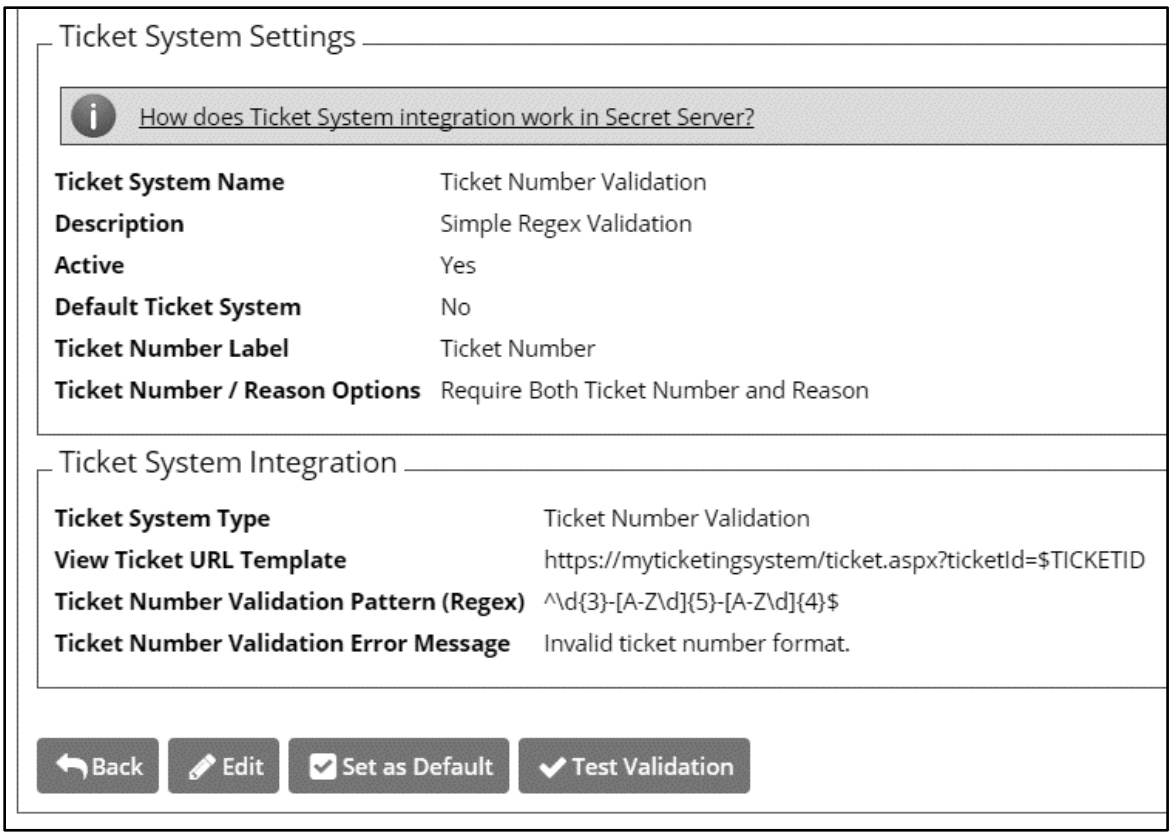
Ticket System Tab

IBM Security Verify Privilege Vault can allow users to enter a ticket number when viewing a Secret. This number can be validated through a regular expression, and can also be marked as required, if needed. IBM Security Verify Privilege Vault can integrate with third party ticket systems. For more information on the ticket system integration, see Ticket System Integration with IBM Security Verify Privilege Vault (KB).

You can add multiple ticket systems from the **Ticket System** tab. To add a new system, click **New Ticket System**.



You can make a select ticket system be IBM Security Verify Privilege Vault's default ticketing system by clicking on the link of the desired system, then clicking **Set as Default**.

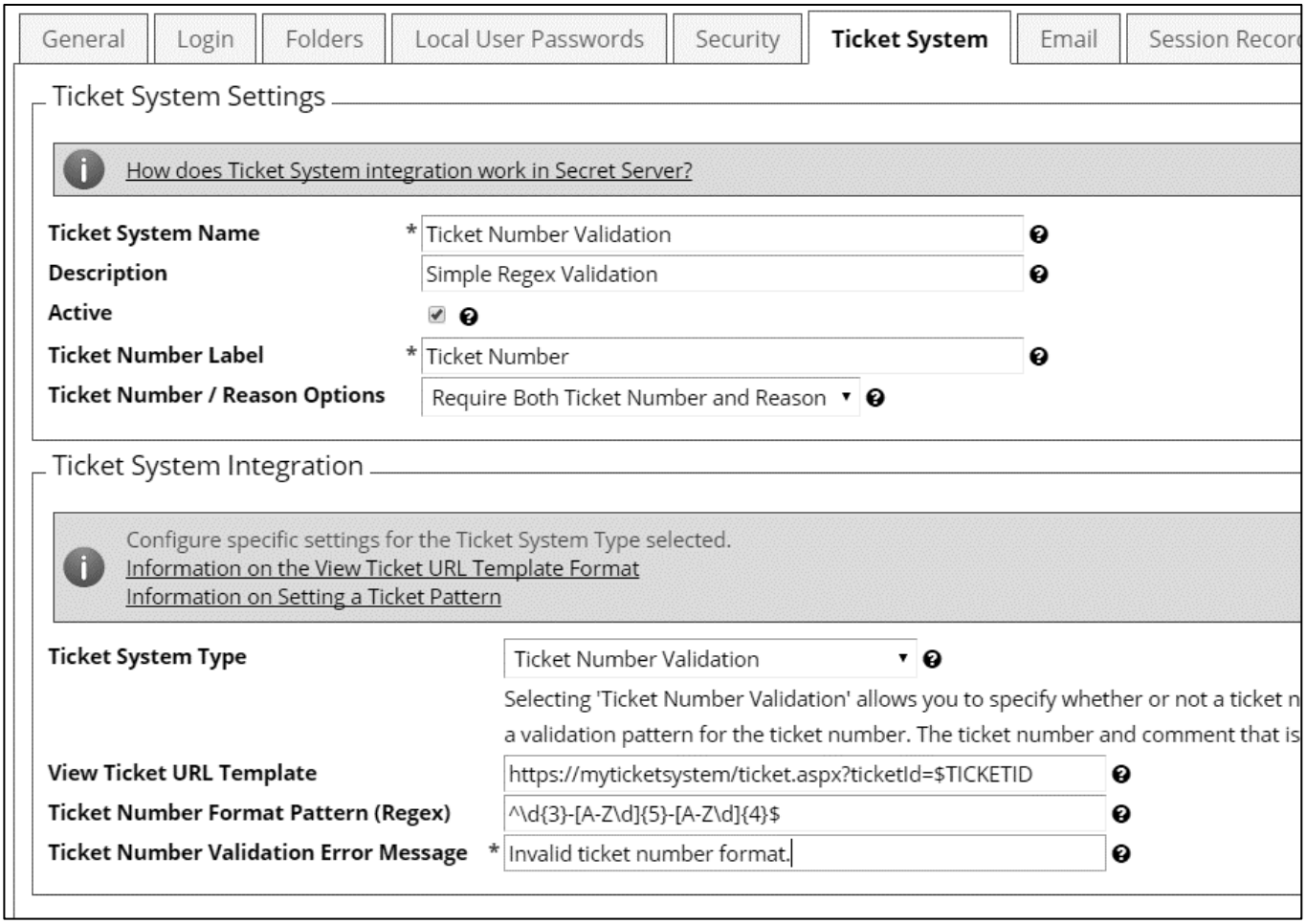


Ticket Number Validation

IBM Security Verify Privilege Vault can require users to enter a ticket number when viewing a Secret. Admins are able to track access to Secrets based on an external ticket system. On the **Ticket System** tab of the **Configuration** page, an administrator can enter the settings to match the ticket system.

After the ticket system is enabled in IBM Security Verify Privilege Vault, a user is able to enter a ticket number on the Comment screen or the Request Access screen.

The Secret must have Require Comment or Requires Approval for Access enabled to allow the user to enter a ticket number. When a ticket number is required, this Secret setting will be displayed as “Require Comment / Ticket Number” on the Security tab.



Configurable Settings

Ticket Number Label

The text that displays next to the ticket number box on the Comment or Request Access screen.

View Ticket URL Template

The format of the URL to be used for viewing the ticket. This will be placed in the audit log so you can easily view the corresponding ticket from IBM Security Verify Privilege Vault. For details on this format, see View Ticket URL Template Format (KB).

Ticket Number Format Pattern (Regex)

A regular expression to use for validating the ticket number entered. This can help prevent typos in the number. For details on creating this expression, see the Setting a Ticket Pattern Regex (KB).

Ticket Number Validation Error Message

The error message to display to the user when their entered ticket number fails the validation pattern regex.

Ticket Number / Reason Options

This option allows fine-grained control of what the user must enter when Require Comment is enabled and ticket system integration is turned on.

- **Reason Only Required** Ticket number is optional, reason is required.
- **Both Required** Ticket number and reason are required.
- **Ticket Number or Reason Required** Either ticket number or reason must be entered.
- **Ticket Number Only Required** Ticket number is required, reason is optional.

Auditing

The ticket number will be appear in the audit log and can be queried in reports. If the **View Ticket URL** has been set, the log will show the ticket number as a hyperlink linking to the external ticket system. Information on setting the URL can be found in View Ticket URL Template Format (KB).

BMC Remedy Integration

IBM Security Verify Privilege Vault can integrate with BMC Remedy's Incident and Change Management. This integration includes validating ticket numbers, their status, and adding Work Detail items to the request.

The integration with BMC Remedy leverages the out of the box SOAP-based web services that are installed with the ITSM product installation. These services must be installed on your mid-tier BMC Remedy server to allow for this integration if they are not already installed and configured.

Requirements

- BMC Remedy SOAP Web Services enabled
- A user name and password that has access to execute the web services. This can be set up in the developer studio by accessing the application in the navigator and viewing Permissions for the CHG_ChangeInterface_WS or HPD_IncidentInterface_WS. This user should also have access to query requests and add work items to requests for the appropriate module.
- IBM Security Verify Privilege Vault environment needs to be able to connect to the BMC Remedy web services via port 80 or 443. SSL is highly recommended because the SOAP messages will contain a user name and password.

Testing your Integration Setup

After configuring the ticket system (see configurable settings below), use the **Test Validation** button to verify that IBM Security Verify Privilege Vault is able to successfully access BMC Remedy. This button will open a dialog in which you can enter a ticket number from BMC Remedy. This validation process will return success or an error code. BMC Remedy might not return much detail in the error message so you must look at the BMC Remedy API log to see a detailed error message, see BMC Remedy Error Messages (KB).

Configurable Settings

Validating Ticket Status

When a BMC Remedy request number is entered into IBM Security Verify Privilege Vault the status of that request will be retrieved to ensure that it is an open state. For example, if an incident number is entered that is in the “Closed” state the user will be informed that the ticket is closed.

Incident Management	Service Incident request cannot be Closed or Canceled.
Change Management	Change Management requests cannot be Complete, Closed, or Canceled.

View Ticket URL Template

The format of the URL to be used for viewing the ticket. This will be placed in the audit log so you can easily view the corresponding ticket from IBM Security Verify Privilege Vault. For details on this format, see View Ticket URL Template Format (KB). Depending on your version of BMC Remedy the URL to link directly to a request might be slightly different.

Incident Management	https://<midtier_server>//arsys/forms/<servername>/SHR%3ALandingConsole/Default+AdmSearchTicketWithQual&F304255610='Incident Number'%3D%22$TICKETID%22
Change Management	https://<midtier_server>//arsys/forms/<servername>/SHR%3ALandingConsole/Default+AdmSearchTicketWithQual&F304255610='Change Number'%3D%22$TICKETID%22

Ticket Number Format Pattern (Regex)

Before even making a call to the BMC Remedy web service, you can have IBM Security Verify Privilege Vault validate that the number matches a pattern. For example, your incident numbers might all be prefixed with “INC” and you want to ensure users enter the prefix.

Some sample expressions to validate the ticket number are listed below:

Incident Management	^INC_CAL_[\d]{7}$
Change Management	^CRQ_CAL_[\d]{7}$

Ticket Number Validation Error Message

The error message to display to the user when their entered ticket number fails the validation pattern regex.

Service Endpoint URL

This is the URL for the SOAP-based web services. Below are some samples for what is expected. You can find the actual endpoint by using BMC Remedy Developer Studio and accessing the correct application from the AR System Navigator and viewing the web services section of the application.

Incident Management	HPD_IncidentInterface_WS	https://<midtier_server>/arsys/services/ARService?server=<servername>&webService=HPD_IncidentInterface_WS
Change Management	CHG_ChangeInterface_WS	https://<midtier_server>/arsys/services/ARService?server=<servername>&webService=CHG_ChangeInterface_WS

System Credentials

Select or create a Secret that contains the user name and password for a user that has access to execute the SOAP web services. The user name and password will be added to the authentication header for the SOAP request.

Authentication

If your installation of BMC Remedy uses an authentication server, enter it in this field. Most installations allow this field to be blank.

Add Comments to Ticket

Check this box if you want the comment that a user enters to be added to the request in BMC Remedy. This will add information such as the Secret for which access is requested, who requested access, and the requester's comments.

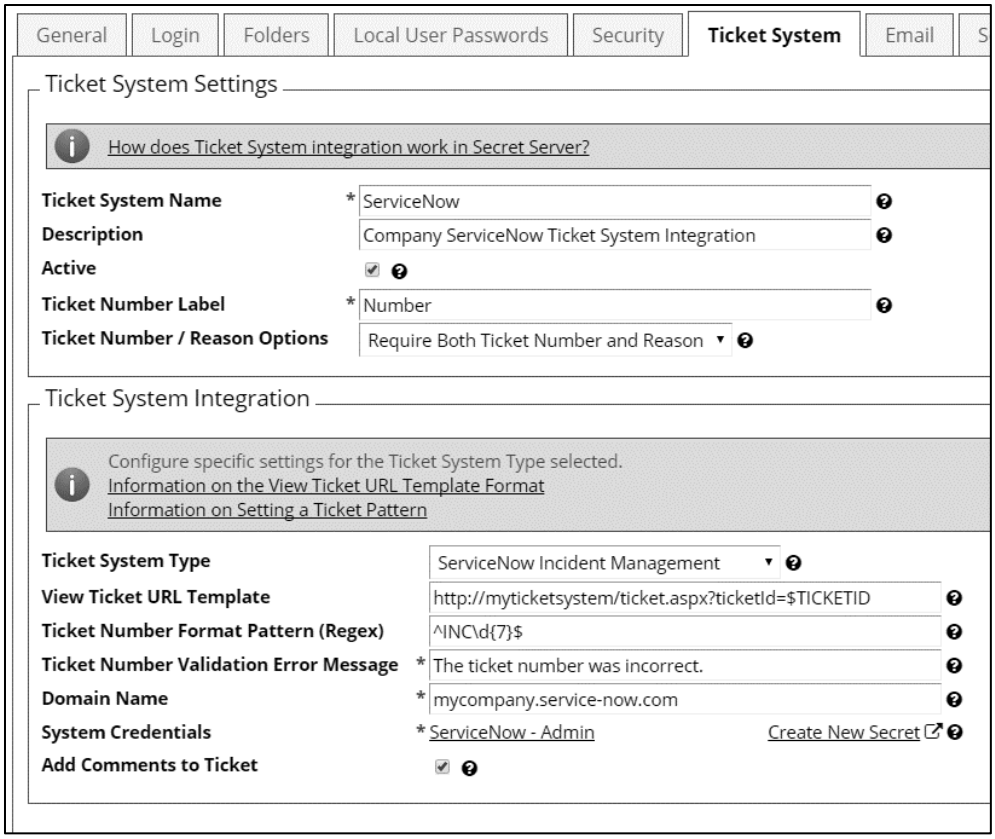
Comment Work Type

When a comment is added to a request as a Work Item, the Work Item Type is required. "General Information" is selected by default, but all default Work Type options are supported.

ServiceNow Integration

IBM Security Verify Privilege Vault can integrate with ServiceNow's Incident and Change Management service. This integration includes validating ticket numbers, their status, and adding Work Detail items to the request.

The integration with ServiceNow leverages the out of the box REST-based web services.



Requirements

- ServiceNow instance running the Eureka version or later with REST services enabled.
- A user name and password that has access to execute the REST services, specifically GET and MODIFY on the following tables: Change Request and Incident.
- The IBM Security Verify Privilege Vault environment needs to be able to connect to the ServiceNow web services via port 80 or 443. SSL is highly recommended since the REST messages will authenticate with a user name and password.

Testing your Integration Setup

After configuring the ticket system (see configurable settings below), use the “Test Validation” button to verify IBM Security Verify Privilege Vault is able to successfully access ServiceNow. This button will open a dialog in which you can enter a ticket number from ServiceNow. This validation process will return success or an error code.

Configurable Settings

View Ticket URL Template

The format of the URL to be used for viewing the ticket. This will be placed in the audit log so you can easily view the corresponding ticket from IBM Security Verify Privilege Vault. For details on this format, see View Ticket URL Template Format (KB).

Incident Management	https://<instance name>.service-now.com/nav_to.do?uri=incident.do?sysparm_query=number=$TICKETID
Change Management	https://<instance name>.service-now.com/nav_to.do?uri=change_request.do?sysparm_query=number=$TICKETID

Ticket Number Format Pattern (Regex)

Before even making a call to the ServiceNow web service you can have IBM Security Verify Privilege Vault validate the number matches a pattern. For example, your incident numbers might all be prefixed with "INC" and you want to ensure they enter this prefix. Some sample expressions to validate the ticket number are listed below:

Incident Management	^INC[\d]{7}$
Change Management	^CHG[\d]{7}$

Ticket Number Validation Error Message

The error message to display to the user when their entered ticket number fails the validation pattern regex.

Instance Name

This is the name of your instance in the format `https://<instance name>.service-now.com`. For example: `https://MyCompany.service-now.com`.

System Credentials

Select or create a Secret that contains the user name and password for a user that has access to execute the REST web services. IBM Security Verify Privilege Vault will use these credentials to authenticate to ServiceNow.

Add Comments to Ticket

Check this box if you want the comment that a user enters to be added to the request in ServiceNow. This will add information such as the Secret to which access is requested, who requested access, and their comments. The comment will be added as a "work note" in the activity section of the request.

PowerShell Integration

IBM Security Verify Privilege Vault can integrate with your ticketing system via PowerShell. This integration includes validating ticket numbers, their status, and adding comments. In our example we are connecting to a ServiceNow instance.

Requirements

- **PowerShell, see** Creating and Using PowerShell Scripts **(KB)**
- Access to your ticket system via some API that can be accessed in PowerShell. This might be a REST API, SOAP API, or native calls

Configurable Settings

View Ticket URL Template

You can configure the view ticket URL if you have a web based ticketing system to allow easy access to link to your ticketing system from IBM Security Verify Privilege Vault.

Ticket Number Format Pattern (Regex)

Before making a call to the PowerShell script you can have IBM Security Verify Privilege Vault validate the number matches a pattern. For example, your incident numbers might all be prefixed with “INC” and you want to ensure they enter this prefix. See Setting a Ticket Pattern Regex (KB).

Ticket Number Validation Error Message

The error message to display to the user when their entered ticket number fails the validation pattern regex.

Run As Credentials

In IBM Security Verify Privilege Vault a domain credential is required to execute the PowerShell script. This is a required field.

System Credentials

The system credentials are specific to your ticketing system. Any secret by using the Username and Password extended mapping can be used as your system credential. More arguments can be populated from field on this secret and referenced in your script.

Validating Ticket Status

To validate tickets you must create a PowerShell script to retrieve and validate the ticket. The integration will use arguments to pass custom values to your script. By default we will map certain fields to the first set of arguments.

Adding Comments to Tickets

To add a comment to tickets create a script that will do just that. The arguments are passed in the following order:

- $ticket = $args[0]
- $comment = $args[1]
- $user = $args[2]
- $password = $args[3]
- $url = $args[4]

Adding Comments to a General Audit Log

In addition to adding comments to specific ticket you might want general audit entries made in your ticket system. The arguments are passed in the following order:

- $comment = $args[1]
- $user = $args[2]
- $password = $args[3]

Email Tab

The Email tab contains the following configuration options:

Email Server
Specify the domain name or IP address of your SMTP server. For example: “smtp.example.com”

From Email Address
This is the email address that emails sent by IBM Security Verify Privilege Vault will be from.

Use Credentials
Whether or not to use credentials when sending emails. Requires username/password to be entered when enabled.

Domain
The domain of the credentials to use (optional).

Use SSL
Whether or not to use SSL when sending emails.

Use Custom Port
Whether or not to use a custom port when sending emails. Requires a custom port to be specified when enabled.

Session Recording Tab

The Session Recording tab contains the following configuration options:

Enable Session Recording
Enable Session Recording for launched sessions.

Video Code
Specify the codec to use to create the videos from the launcher screenshots. This codec will have to be installed on the web server (or servers if clustering is enabled) that IBM Security Verify Privilege Vault is installed on. Note that the Microsoft Video 1 codec is for testing only and does not support in browser playback. Sessions encoded with Microsoft Video 1 can still be downloaded for review.

Save Videos To
By default, videos are stored in the database, IBM Security Verify Privilege Vault can also store them directly to a network share. This network share must be accessible from all web servers that IBM Security Verify Privilege Vault is installed on.

Enable Moving To Disk
After the **Days Until Moved To Disk** value, IBM Security Verify Privilege Vault can move videos from the database to an archive path on disk.

Enable Deleting
After the **Days Until Deleting** value, IBM Security Verify Privilege Vault will delete the videos from disk.

For details on the settings in the Login and Local User Passwords tab, see Configuring the Users in the Users section.

HSM Tab

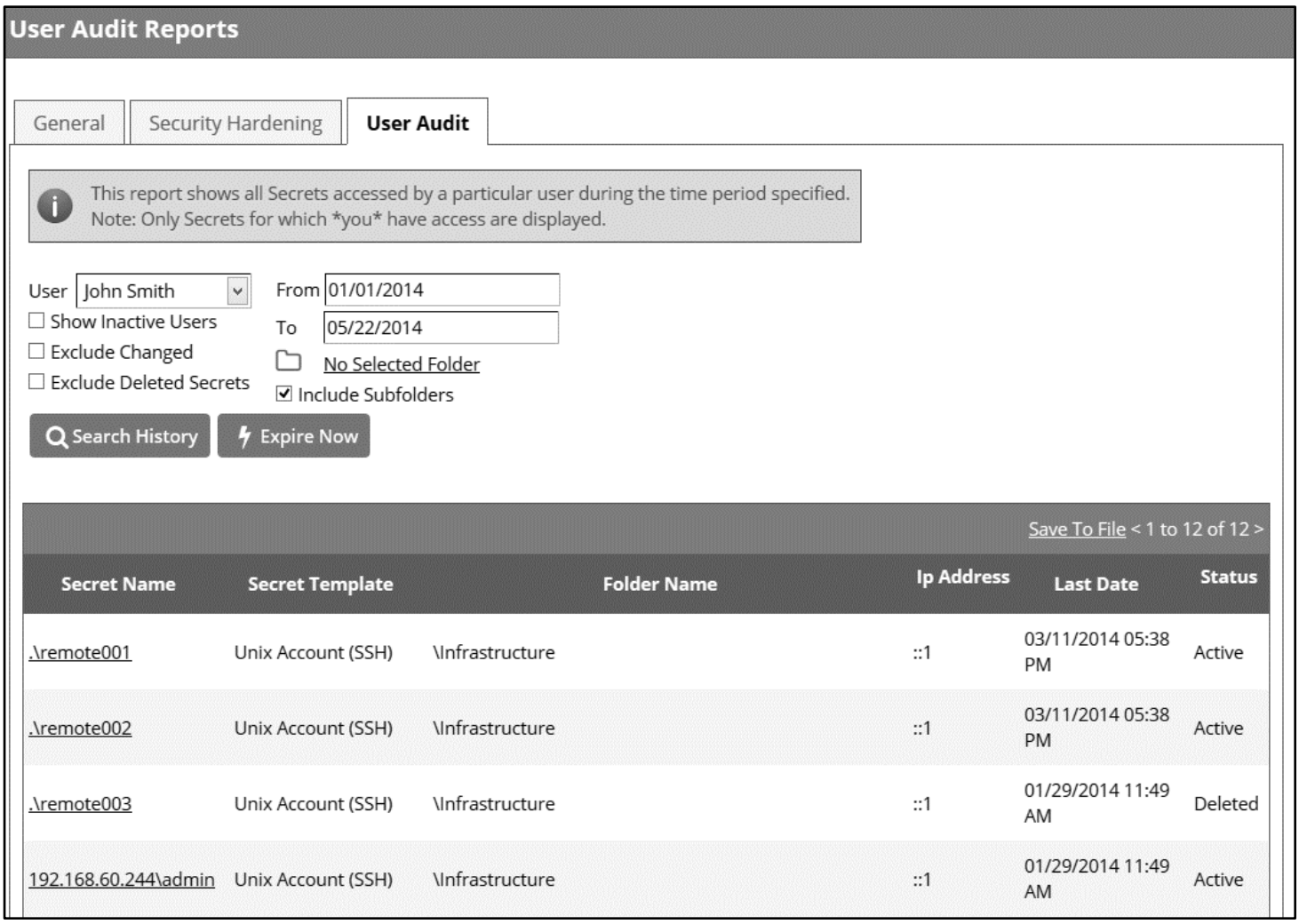
From the HSM tab, you can enable or disable HSM for encryption. For more details about HSM configuration, see our HSM Integration Guide (PDF).

Administrator Auditing

IBM Security Verify Privilege Vault keeps a detailed audit history for users and Secrets. IBM Security Verify Privilege Vault implements a detailed tracking system for actions made on Secrets. Auditing users is an indispensable component of any password management system. The audit trail allows administrators to know which Secrets were accessed and ensures that Secrets are being properly used. Additionally, the User Audit report helps SEC regulated companies comply with the Sarbanes Oxley Act of 2002 as well as other regulatory compliance mandates.

User Audit Report

From the Reports page, click the User Audit tab. From the dialog on the tab select a user and a date range to view, then click Search History to view the user's audit trail.



The Audit Search displays results for all the Secrets the selected user has viewed or edited during the selected time period. The administrator has the option of expiring all the viewed Secrets, to notify users to change sensitive information, or to force password changing (if the Remote Password Changing is configured).

To get a full view of the actions taken on a Secret, select that Secret from the results list. The Secret Audit displays the specific user actions for a Secret.

Secret Audit

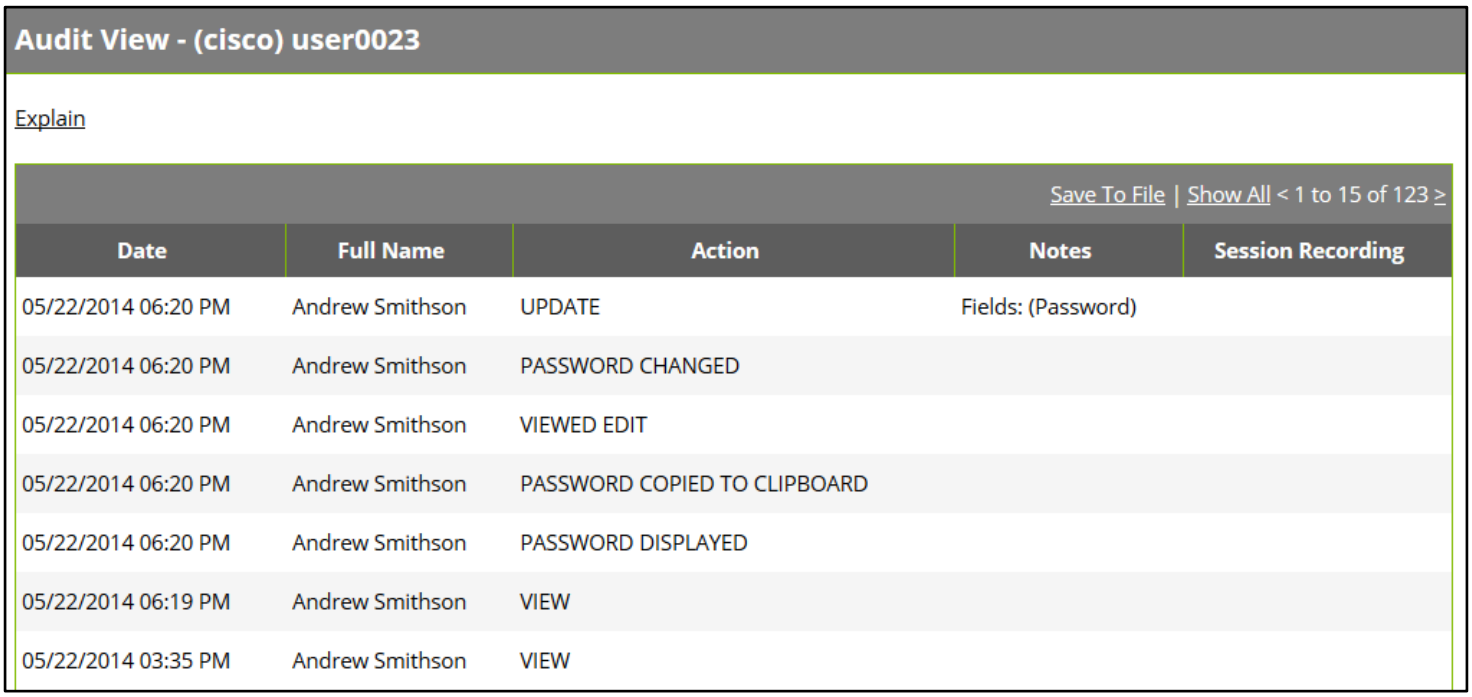
The audit log for a Secret can be accessed by clicking the View Audit button on Secret View page or navigating from the User Audit Report. The log will show the date, the user name, the action, and any other details about the event.

Secret auditing provides a detailed view of each change or view on a Secret. Secret Audits are taken for the following user actions:

- View

- Update
- Editing Permissions
- Forced expiration
- Check Out
- Set for Check-In
- Hide launcher password changes
- Adding, Updating and Removing Secret Dependencies

For certain audit items, action notes are added providing additional details. For example, if permissions are edited, an audit record is generated detailing which users or groups gained or lost permissions. Detailed audit records add accountability to sensitive Secrets where auditors or administrators need to know exactly what was modified.



Date	Full Name	Action	Notes	Session Recording
05/22/2014 06:20 PM	Andrew Smithson	UPDATE	Fields: (Password)	
05/22/2014 06:20 PM	Andrew Smithson	PASSWORD CHANGED		
05/22/2014 06:20 PM	Andrew Smithson	VIEWED EDIT		
05/22/2014 06:20 PM	Andrew Smithson	PASSWORD COPIED TO CLIPBOARD		
05/22/2014 06:20 PM	Andrew Smithson	PASSWORD DISPLAYED		
05/22/2014 06:19 PM	Andrew Smithson	VIEW		
05/22/2014 03:35 PM	Andrew Smithson	VIEW		

Below the audit records is a check box for Display Password Change Log. Ticking this check box displays logs for Heartbeat and Remote Password Changing amongst the audit items.

Report Auditing

In addition to the User Audit and individual Secret Audit, the Reporting feature provides a series of activity, user, and Secret reports.

Users can also create their own, custom reports. See Creating and Editing a Report for more information.

Backup / Disaster Recovery

IBM Security Verify Privilege Vault supports manual and scheduled database and IIS directory backups. The database access settings support SQL Mirror and automatic failover. As an additional disaster recovery measure, administrators can export Secrets to a CSV spreadsheet.

Backup Settings

The following configuration options are available on the **Tools | Backup** page of IBM Security Verify Privilege Vault:

Backup File Path
This directory must exist on the web server and will store the zip file of the application directory.

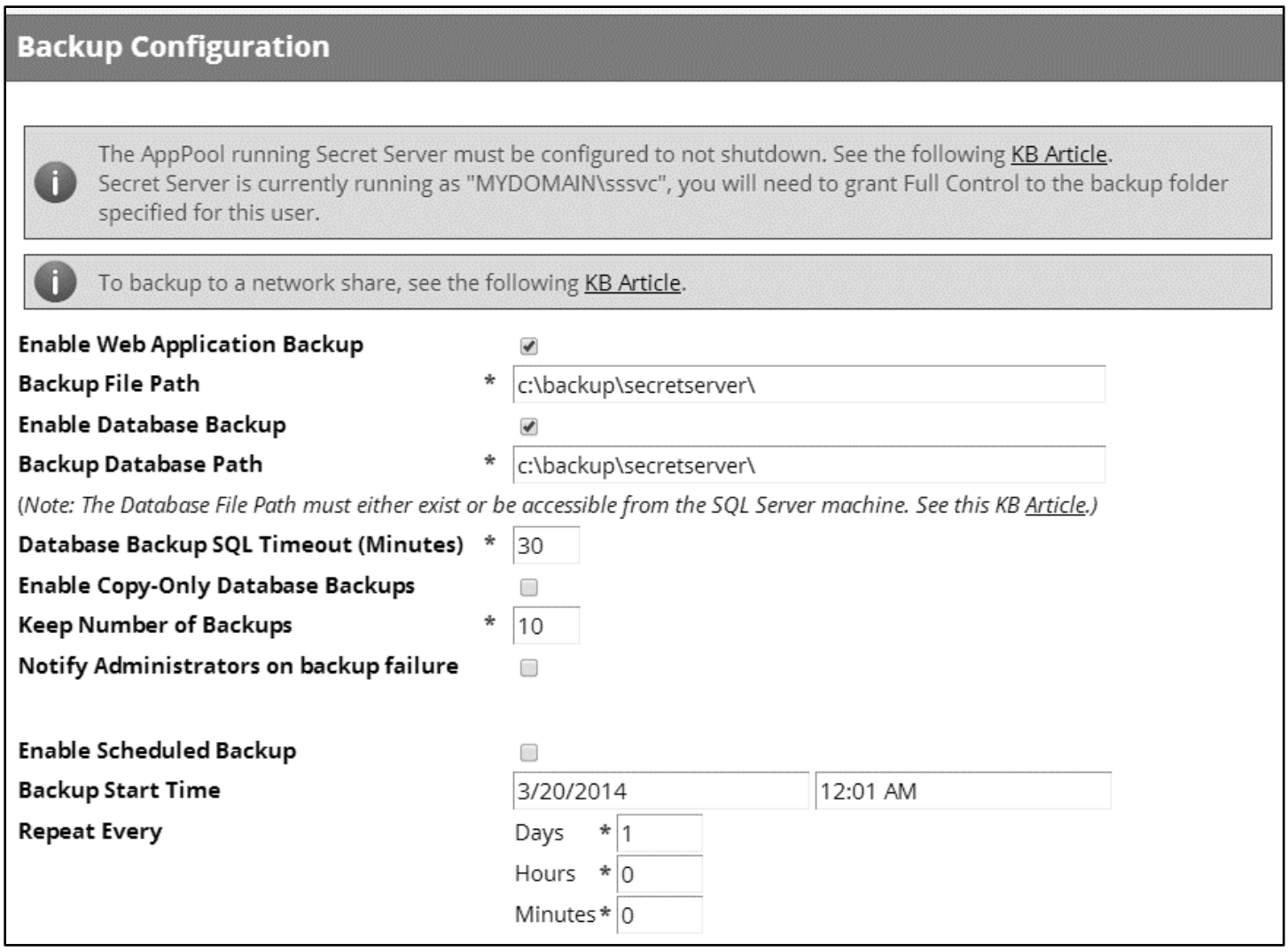
Backup Database File Path
This folder must be accessible by the SQL server and will store the database.bak file.

Database Backup SQL Timeout (Minutes)
Number of minutes that IBM Security Verify Privilege Vault will wait for the database backup to complete successfully before timing out.

Keep Number of Backups
Number of previous backups to keep.

Notify Administrators on Backup Failure
Users with the Administer Backup role permission will be notified if the backup fails.

Enable Scheduled Backup
Enables automatic backups on a set schedule.



Folder Permissions

From the Backup Administration page, specify the correct directory paths for the IIS IBM Security Verify Privilege Vault file directory and the database backups to be stored. The backup path must be local to the server where the IBM Security Verify Privilege Vault database or file directory exists. The directories must also have the proper permissions to allow IBM Security Verify Privilege Vault to automatically store backups at those locations. The account that requires permission will be displayed as an alert on the Backup page.

Manual Backups

On the Backup Administration page, click Backup Now to force an immediate backup. This is useful for testing the backup settings and is recommended to be done before upgrading.

Scheduled Backups

There are numerous options to consider when backing up IBM Security Verify Privilege Vault. Backups can be scheduled to run on a specific time interval. To prevent the directory from growing too large, the number of backups to keep can be defined as well. Depending on size constraints or preferences of the DBA who would be administrating a disaster recovery scenario, the database backup can either truncate the transaction log or keep it intact. The additional schedule settings are available when the Enable Schedule Backup is enabled and the view page will indicate the time and date of the next scheduled backup.

File Attachment Backups

Files uploaded to Secrets can be backed up using the standard IBM Security Verify Privilege Vault backup function. Upon backup completion, they retain their encrypted status and will be inside the application backup file (the .zip file).

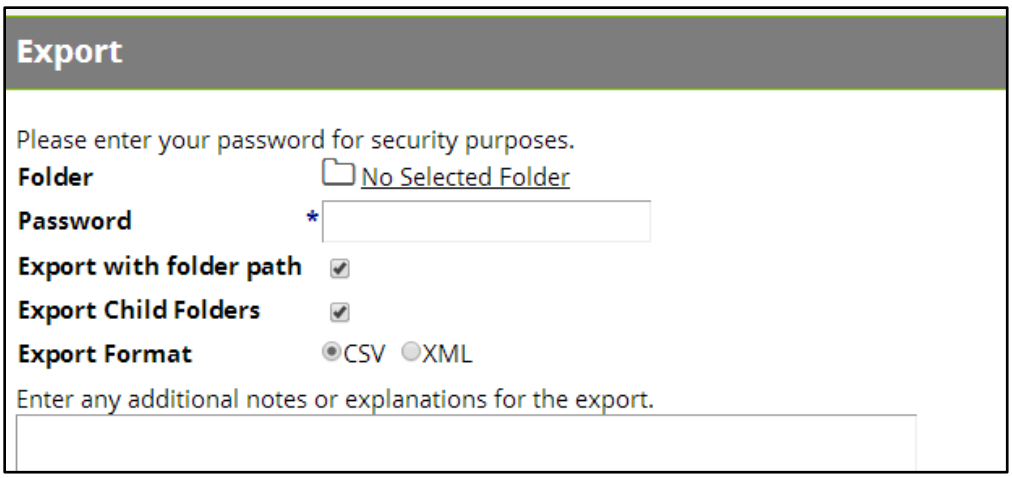
Exporting Secrets

From within the Administration > Export page, select the folder that needs to be exported. By default, all Secrets will be exported if a folder is not selected. In the event that no particular folder is selected, all Secrets will be exported by default. The administrative password must be entered, as it is a security measure to verify the permission of the user performing the export.

Only the Secrets the user has View access to will be exported.

Exports can be configured further with options to Export With Folder Path and Export Child Folders. Export With Folder Path adds the full folder path to the export. Folder paths in the export file provide organizational structure if Secrets need to be imported at a later date.

By default, the option to Export Child Folders is active. While this option is enabled, any export of a specified folder will also export content located in folders beneath the initial selection.



Exported File Format

Secrets are exported as a comma-separated file (.csv) or as XML. The .csv file can be easily handled in Excel or other spreadsheet applications. The file is grouped by Secret template and each cluster of Secrets has a header row that contains the template field names followed by all exported Secrets based on that template.

The XML file follows the exact structure of the Advanced XML Import. As such, this can be useful with migrating data from one IBM Security Verify Privilege Vault installation to another.

Secrets are exported in the exact structure as a Secret Import. As long as exports are maintained, an installation of IBM Security Verify Privilege Vault can be completely reproduced on a separate instance by applying the exported file.

Recovery

Recovery requires by using the application and database backups. To restore web application directory, extract the root directory to the web server. The encryption.config file is most important for being able to read the contents of the database. The SQL database can be restored by using the standard process in SQL Server Management Studio from the .bak file.

For detailed instructions see the Restoring IBM Security Verify Privilege Vault from a backup KB article.

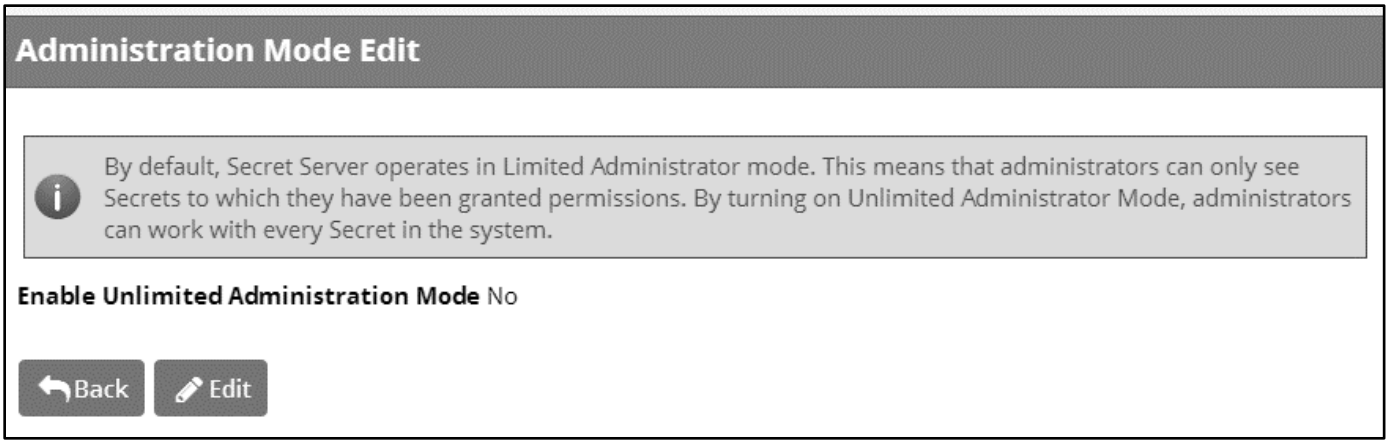
Unlimited Administration Mode

Unlimited Administration Mode is a feature designed to allow an administrator access to all Secrets and folders in their IBM Security Verify Privilege Vault instance without explicit permission. This can be used in the instance a company has an emergency situation where access to a particular Secret is needed when no users who have permission are available. Alternately, it can be used when company policies require administrators to have access to all information in the system.

An alert visible to all users will be displayed at the top of the Secret View page when Unlimited Administration Mode is enabled.

For a user to be an Unlimited Administrator they must be assigned a role with the Unlimited Administrator permission and Unlimited Administration Mode must be enabled in Configuration settings.

To navigate to the Unlimited Administration section, select **Configuration** from the **Administration** menu, and then click **Change Administration Mode**. It is recommended that administrators have specific permissions to folders and Secrets and this mode is only used temporarily to assign the correct permissions.



Changes to the administration mode are logged in an audit grid. The grid shows the user, time of the change, and any notes made by the user.

System Log

The System Log is used to communicate the different events that are occurring while IBM Security Verify Privilege Vault is executing. It can be helpful in troubleshooting unexpected behavior. The system log can be enabled by clicking Edit and checking the Enable System Log box on the Administration > System Log page.

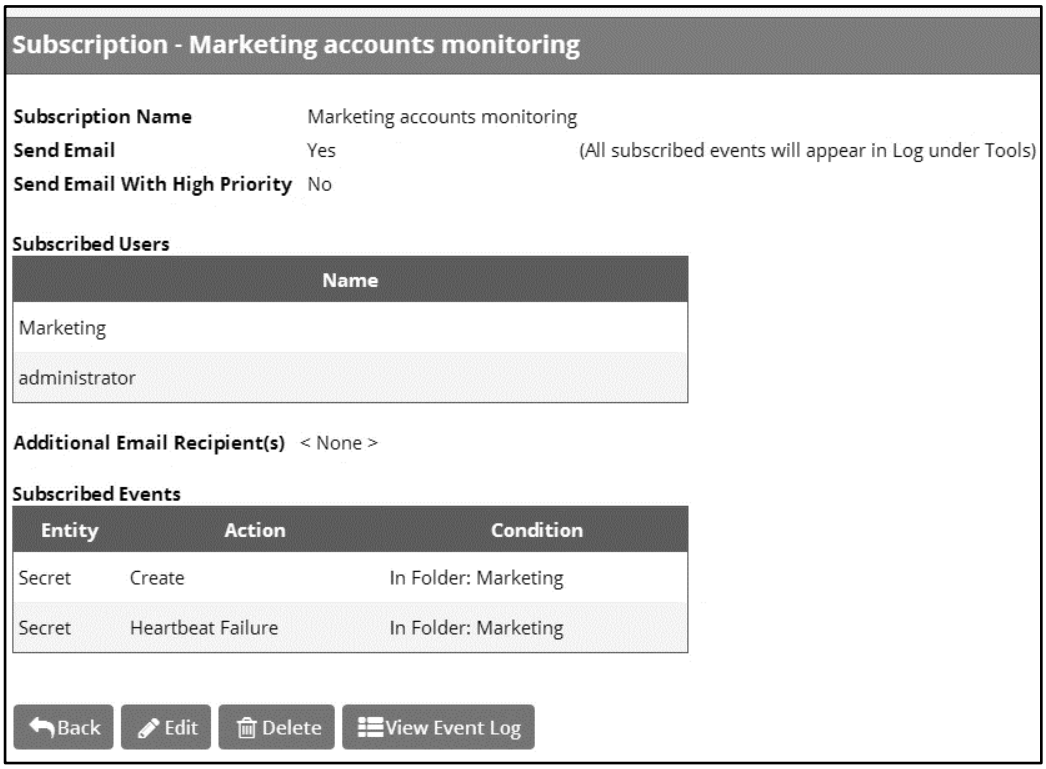
Maximum Log Length
This is the maximum number of rows to keep in the System Log table in the SQL database. When it reaches that amount, it will be reduced by 25%.

Notify Administrators when System Log is Shrunk
This setting is used to send an email to all System Log administrators when the System Log has been truncated. A System Log administrator is any user in a role with the Administer System Log permission included.

To clear the system log of all its records, click **Clear**.

Events and Alerts

Event Subscription Page



Subscription Name Name for the subscription.

Send Email Alerts Sends an email to both users and all the users contained in the groups for this subscription. It also sends an email to all email addresses in the Additional Email Recipients list (see below).

Send Email with High Priority Sends the email for this subscription with High Priority set.

Subscribed Users List of the IBM Security Verify Privilege Vault users and groups subscribed to this event.

More Email Recipients List of additional email addresses to send the email to.

These entries are meant to be outside of the users' email addresses as known to IBM Security Verify Privilege Vault. One of these might be, for example, User1's home email address.

Subscribed Events List of the events that are contained in this subscription.

Creating an Event Subscription

To add an event subscription, navigate to Administration > Event Subscriptions. On this page, click New.

In the Subscription Name field, enter a name for this new event subscription.

Add users and groups to this subscription by selecting them from the Add New drop-down selector. They will be added to the Subscribed Users list above the Add New drop-down selector.

Add events to this subscription by adding rows to the Subscribed Events data grid. To do this, select an entity type from the drop-down selector in the Entity column of the first row (Secret, User, Folder, and so on). After an entity is chosen, you can now select an action (Create, Delete, Edit Permissions, and so on). After an action is selected, a condition might be available. Select the condition you want to implement. Finally, to add this event to the subscription, click the  button. This must be done before the Save button at the bottom of the page is clicked in order to add this event to the subscription.

Editing a Subscription

To edit an event subscription, navigate to Administration > Event Subscriptions, click the subscription name, and then Edit. To remove a subscribed user, group, or event, click the  button next to the entry in the appropriate list. To add entries to either list, see the Creating an Event Subscription section above. Click Save to save all changes.

Deleting a Subscription

To delete an event subscription, navigate to Administration > Event Subscriptions, click the subscription name. Click Delete on the following page.

Viewing the Event Subscription Log

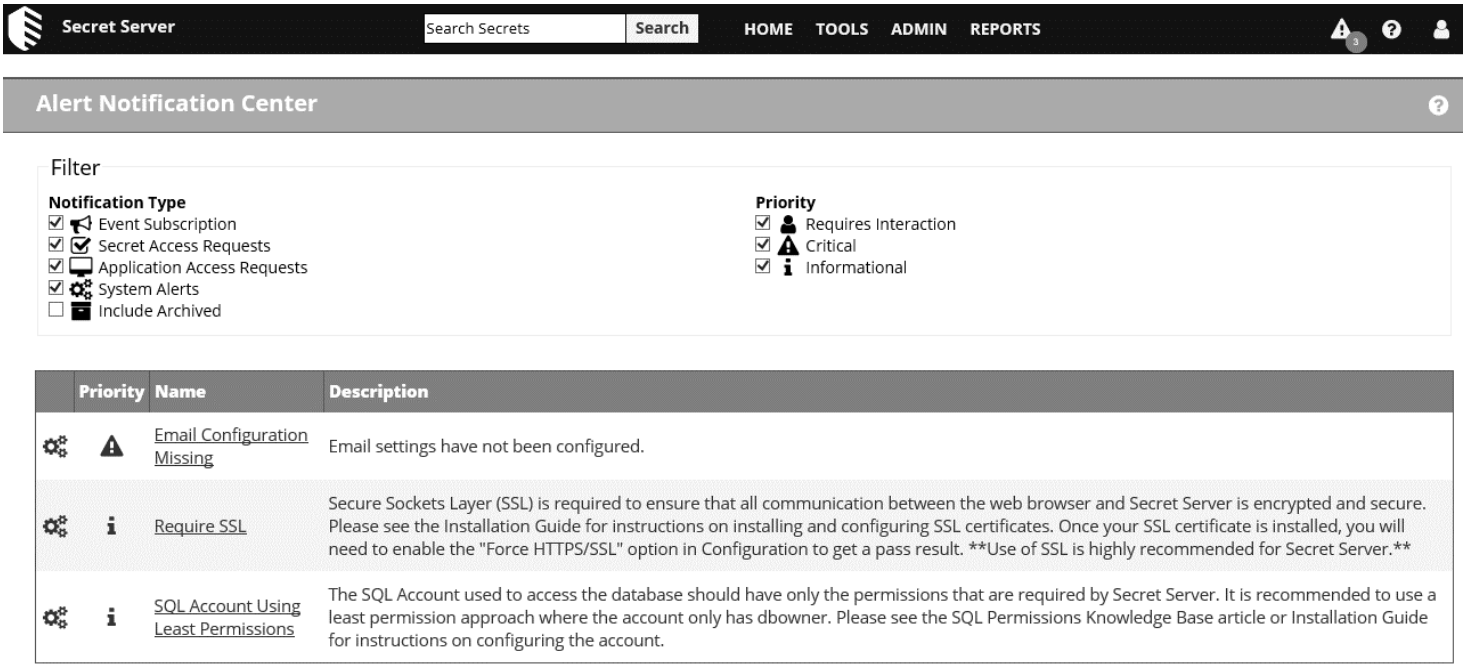
To view the events that have been triggered in a subscription, navigate to Administration > Event Subscriptions and click View Audit. In the Event Subscription Activity list, the most recent events to have been triggered will be on top of the list. To select a specific time frame, click the ... buttons and select start and end dates at the top of the page. Click Update Report to return the corresponding log entries.

It might take a few seconds for the events to make it into the Log.

Alert Notification Center

The Alert Notification Center shows event subscriptions, access requests, and other configuration alerts in a single interface. You can access the Alert Notification Center by clicking the alert badge on the top right of your screen.

Event subscriptions will disappear from the notification center after you view them. System alerts and access requests will stay active until resolved.



CEF / SIEM Integration

IBM Security Verify Privilege Vault can log to a CEF or Syslog listener. When this is configured, all event engine events and important system log entries are sent to the CEF or Syslog server that is entered in the configuration. The written events contain data such as user information, time, IP Address, and any other important details about the event.

Configuring CEF

When in Administration > Configuration, click the Edit button and check the Enable Syslog/CEF Logging check box. When you do this, three additional settings appear:

Syslog/CEF Server IP address or name of the server.

Syslog/CEF Port Port that the events will be sent to the server on.

Syslog/CEF Protocol Either UDP or TCP, the protocol used by your server.

Once you have entered these values, click Save.

Testing CEF

After enabling CEF, your server should start to receive messages right away if you entered the data correctly. In order to force an event to happen, perform a log out and then log back in. If the event does not appear on your CEF server soon after, there is something wrong with your configuration.

Customizing the Look

By default, IBM Security Verify Privilege Vault is set to a default theme unless specified within the Configuration settings. IBM Security Verify Privilege Vault comes with three other bundled themes: Blue, Dark, and Green. The default theme can be set at Administration > Configuration on the general tab. Theming differences can be allowed by individual users with the Allow User to Select Themes setting.

Creating Themes

Themes are controlled from the Theme Roller. To create a custom theme go to ADMIN | More | Themes. For detailed instructions on using the Theme Roller please see this KB guide.

Embedded Mode

Embedded Mode will remove the header and footer to allow IBM Security Verify Privilege Vault to be more easily placed within a frame. To activate Embedded Mode for the session, add an "embedded=true" query string parameter to the URL when accessing IBM Security Verify Privilege Vault. For example, if you normally access IBM Security Verify Privilege Vault by going to "https://myserver/Secretserver/login.aspx", then you can enable embedded mode by going to "https://myserver/Secretserver/login.aspx?embedded=true". This parameter can be added to the URL on any page in IBM Security Verify Privilege Vault. To disable embedded mode simply change the query string to "embedded=false."

Reporting in IBM Security Verify Privilege Vault

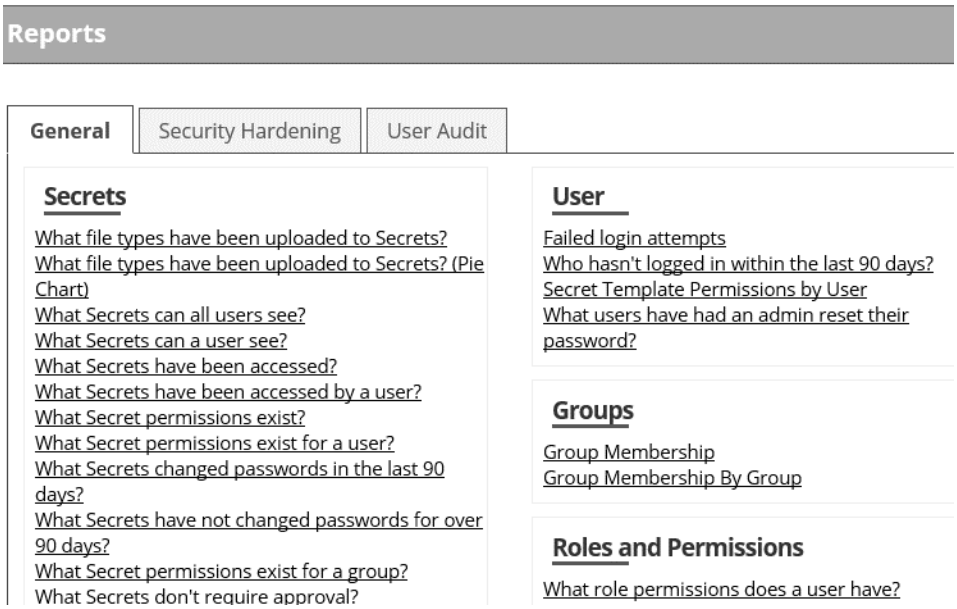
The reporting interface comes with a set of standard reports. These reports include a variety of 2D and 3D charting/graphing components and a full grid of data. Some of the reports are purely data detailed and have no charts. You can also create your own reports based on any IBM Security Verify Privilege Vault data (user, audit, permissions, folders, and so on). You can create report categories to aid in the organization of your reports. Reports can be arranged to provide access to auditors and meet compliance requirements. These reports can be accessed in the General tab.

The Security Hardening Report checks aspects of IBM Security Verify Privilege Vault to ensure security best practices are being implemented. While IBM Security Verify Privilege Vault will run with all the items failing,

administrators should be aware of possible security issues within an installation. For more details on this, see the Security Hardening Tab section below.

The User Audit Report shows all Secrets accessed by a user during a specified period of time. For a more detailed explanation of this, see the User Audit section below.

General Tab



Reports View Page

The reports are listed under the report categories. To view a report, click the name. This will take you to the Report View page.

You can view a record of all the actions performed on reports by clicking on the View Audit button. For more information on this, see the Auditing section.

For details on the Edit button, see the Reports Edit Page section below.

The “Create it” link is a shortcut for creating a new report. For further explanation, see the Creating and Editing a Report section.

Viewing a Report

On this page you will see the graph, chart, grid, etc. for the report. To see a grid representation of the report, click the Show Data link to expand that area. If there is no data, then no graph will be visible and the text “There are no items” will be displayed in the Show Data section.

Some reports use dynamic values like User, Start Date, End Date, etc. Adjust these values to generate the report you need. Click the Update Report button to generate the new report.

The Edit button allows you to alter the report to fit your requirements. See the Creating and Editing a Report section below for details.

Deleting or Undeleting a Report

To delete a report, click the Delete button.

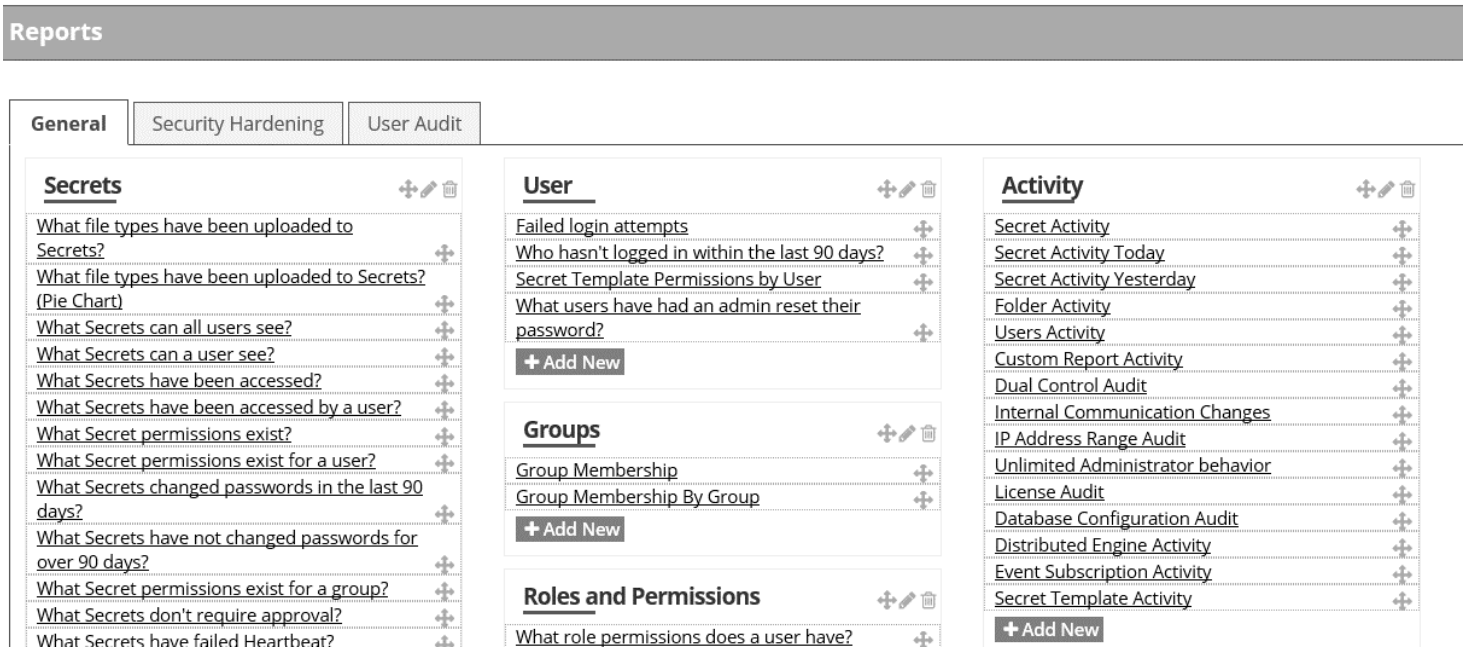
To undelete a report, you must navigate to the Reports Edit page (see the Reports Edit Page section) as deleted reports are not visible on the Reports View page. On the Reports Edit page, click the Show Deleted button. This displays a Deleted Report category which contains all the deleted reports. Either drag the report to a report category that is not deleted or click the report name to go into its Report View page. In there, click the Undelete button.

Auditing for a Report

You can view a record of all the actions performed on a report by clicking on the View Audit button. For more information on this, see the Administrator Auditing section.

Reports Edit Page

You can adjust the look of the Reports View page. The report categories as well as the reports can be rearranged on the page. To do this, click Edit on the Reports page.



Modifying Report Categories

For details on the Show Deleted button, see Undelete a Report earlier in the section.

Rearrange

Any item with the  icon can be dragged and dropped to a new location. Report categories can be moved anywhere within the page. Reports can be moved from one report category to another.

Create New

Click Create Report Category and specify a category name and description on the following page. Note that the Report Category Description is used as the tooltip for the report category on the Reports View page.

Delete

Click the  icon next to the report category name. This will delete all the reports in the category. To undelete the reports, see Undelete a Report section.

Edit

Click the  icon next to the report category name to change the name or description of the category.

Creating and Editing a Report

There are two ways to create a Report. From the Reports Edit page, click the Add New link at the bottom of a Report Category. Or alternatively, from the Reports View page, click the Create it link at the bottom of that page.

To edit a Report, navigate to the Report View page and click **Edit**.

The SQL script text cannot be edited for standard reports.

Below is an explanation of the different fields for the Report Edit page:

Report Name	Name that is displayed on the Reports page as a link underneath its containing category.
Report Description	Description for the Report. This is displayed in the Report View page. It is also used as the Tooltip for the Report name on the Reports page.
Report Category	Selection for which Report Category to place the Report into.
Chart Type	Type of chart to use for displaying the results. If set to None, then a grid will be displayed.
3D Report	Specify a 3D style to render the chart in.
Page Size	Page size limit setting for the data displayed in the grid.

Report SQL SQL script that is used to generate the report.

Reports support the embedding of certain parameters into the SQL to give the user the ability to dynamically change the resulting data set. Another option available for custom reports is to apply a different color to returned rows dependent on certain conditions. For more information as well as examples, see the Using Dynamic Parameters in Reports KB article.

Also available to aid the creation of custom reports is the means to show IBM Security Verify Privilege Vault's SQL database information. By selecting the SQL Table from the drop-down list, the details of the table's columns will be displayed in a grid. Click the Show IBM Security Verify Privilege Vault SQL database information link to see the SQL Table drop down list and SQL Table Columns grid.

Click Preview at the bottom of the page to see a preview of the chart. The resulting chart displays in the Report Preview section at the bottom of the page.

Scheduled Reports

Creating a New Schedule for a Report

To create a schedule for a report, click Schedule on the Report View screen. Once on the Custom Report Schedules page, click Create New.

Viewing Existing Report Schedules

To view existing schedules for a report, click Schedule on the Report View screen. A list of existing schedules for the report are visible in the grid. To view the details of a schedule, click the schedule name in the grid. Deleted schedules can be made visible by checking the Show Deleted box at the bottom of the grid. Click the View link in the History column of the grid to view the history of all generated reports for that schedule.

Editing Schedule Settings

When viewing a report, click Schedule and then the name of the report schedule to modify it. The following configuration options are available:

Schedule Name
Name of the schedule for the report. This name must be unique to the IBM Security Verify Privilege Vault installation.

Health Check
When enabled, an email notification will only be sent when the report contains data.

Recurrence Schedule
Specify that the schedule will run every X number of days, weeks, or months, with the option to specify particular days of the week or month as well. The date and time that the report schedule will be effective can be specified in this section as well.

Save Generated Reports
When enabled, IBM Security Verify Privilege Vault will save the history of generated reports in the database for later viewing. Enabling this setting will also allow you to specify the number of generated reports to save.

Send Email
When enabled, IBM Security Verify Privilege Vault will send an email containing the generated report every time the schedule runs. Enabling this setting will also allow you to specify if the email will be sent with the high priority flag and a list of IBM Security Verify Privilege Vault users or Groups that will receive the generated report email. Add additional email recipients in the text box below the subscribers, separating recipients by a semi-colon.

The following configuration options appear if the report being scheduled contains at least one dynamic parameter in the SQL of the report:

User Parameter Value Value of the #USER parameter to set in the report when it is generated.

Group Parameter Value Value of the #GROUP parameter to set in the report when it is generated.

Start Date Parameter Value Value of the #STARTDATE parameter to set in the report when it is generated.

End Date Parameter Value Value of the #ENDDATE parameter to set in the report when it is generated.

Security Hardening Tab

The Security Hardening Report checks aspects of IBM Security Verify Privilege Vault to ensure security best practices are being implemented. While IBM Security Verify Privilege Vault will run with all of the items failing, administrators should be aware of possible security issues within an installation. Below is an explanation of the different values:

Browser AutoComplete
Browser AutoComplete allows web browsers to save the login credentials for the IBM Security Verify Privilege Vault login screen. These credentials are often kept by the web browser in an insecure manner on the user's workstation. Allowing AutoComplete also interferes with the security policy of your IBM Security Verify Privilege Vault by not requiring the user to re-enter their login credentials on your desired schedule. To prevent the AutoComplete feature, disable the Allow AutoComplete option on the Configuration page.

Force Password Masking
Password masking prevents over-the-shoulder viewing of your passwords by a casual observer (when masked, passwords show as *******). To activate this option, turn on the Force Password Masking option on the Configuration page.

Frame Blocking
Frame blocking prevents the IBM Security Verify Privilege Vault site from being placed in an iFrame. This is to prevent clickjacking attacks. There might be legitimate reasons for placing IBM Security Verify Privilege Vault in a frame, such as embedding the UI in another site. To turn frame blocking on, enable the setting under the Security tab in Configuration.

Login Password Requirements
Login passwords can be strengthened by requiring a minimum length and the use of various character sets. A minimum password length of 8 characters or longer is recommended. In addition, all character sets (lowercase, uppercase, numbers and symbols) are required to get a pass result. Turn on these login password settings on the Configuration page.

Maximum Login Failures
The maximum number of login failures is the number of attempts that can be made to login to IBM Security Verify Privilege Vault as a user before that user's account is locked. A user with user administration permissions will then be required to unlock the user's account. The maximum failures allowed should be set to 5 or less to get a pass result. Change the "Maximum Login Failures" settings on the Configuration page.

Remember Me
Remember Me is a convenience option that allows users to remain logged in for up to a specific period of time. This setting can be a security concern as it does not require re-entry of credentials to gain access to IBM Security Verify Privilege Vault. Turn Remember Me off on the Configuration page to get a pass result. It must be set to be valid for 1 day or less to not get a fail result.

SQL Server Authentication Password Strength
SQL Server authentication requires a username and password. The password must be a strong password to get a pass result. Strong passwords are 8 characters or longer and contain lowercase and uppercase letters, numbers and symbols. The SQL Server authentication credentials in use can be changed by going to the installer (installer.aspx) and changing them on Step 3. A pass result is also given if Windows authentication is used to authenticate to SQL Server.

SQL Server Authentication Username
The SQL Server authentication username should not be obvious. The use of "sa", "ss" or "secretserver" will give a fail result. The SQL Server authentication credentials in use can be changed by going to the installer (installer.aspx) and changing them on Step 3. A pass result is also given if Windows authentication is used to authenticate to SQL Server.

Windows Authentication
Windows authentication takes advantage of Windows security to provide secure authentication to SQL Server. The SQL Server authentication options can be changed by going to the installer (installer.aspx) and changing them on Step 3. Please see the Installation Guide for instructions on configuring Windows authentication to SQL Server.

Require SSL
Secure Sockets Layer (SSL) is required to ensure that all communication between the web browser and IBM Security Verify Privilege Vault is encrypted and secure. Once the SSL certificate is installed, Force HTTPS/SSL in Configuration to get a pass result. Please see the Installing a Self-Signed SSL/HTTPS Certificate Knowledge Base article for instructions.

Using SSL
SSL needs to be running with at least a 128-bit key size to get a pass result. A warning result indicates your key size is less than 128 bits. A fail result indicates you are not using SSL.

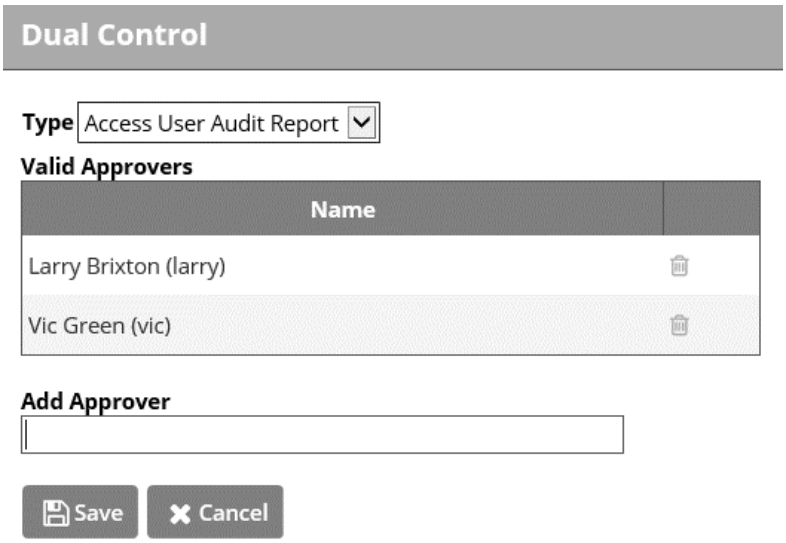
Use of SSL is highly recommended for IBM Security Verify Privilege Vault.

User Audit Tab

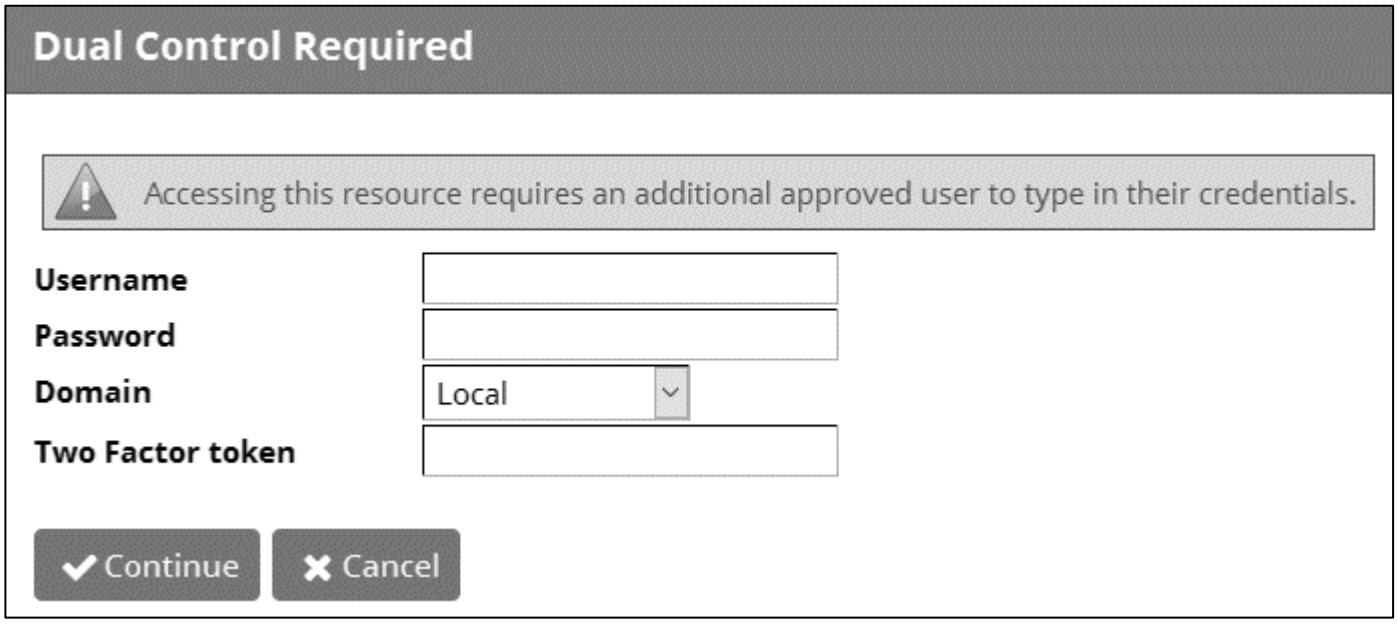
User Audit Reports show all Secrets accessed by a user during a specified period of time. For a more detailed explanation of this, see User Audit Report in the Audit section.

Dual Controls

If there are requirements around protecting potentially personally identifying information when running reports or viewing recorded sessions, you can enforce that another user has authorized you by enabling dual control for a Secret or Report. You can configure Dual Controls by clicking **ADMIN** and then **Dual Controls**. Dual Controls is not in the **ADMIN** drop-down and must be accessed from the full administration menu.



When enabled a user in the approver group must enter in their credentials before a report or session can be viewed.



Once the approver has entered their credentials, the resource can be accessed. The following resources can have Dual Control applied.

- **Access Report:** Protect any report from the General tab of the Reports view.
- **Access User Audit Report:** Protects the user audit report for any user.
- **Secret Session Access:** Requires dual control for any recorded or live sessions for a Secret
- **Create Report**: Require dual control for anytime a user creates a custom report.

Server Clustering

IBM Security Verify Privilege Vault can run with multiple front-end web servers. For a critical instance, clustering offers a redundant system to limit potential down time from a single point of failure. Clustering will also allow users to load balance for better performance.

For instructions on enabling Clustering in IBM Security Verify Privilege Vault, see the Setting up Clustering KB article.

Encryption and Security

Advanced Encryption Standard

IBM Security Verify Privilege Vault uses different types of encryption to ensure data security. Every field, except name, on a Secret is encrypted at the database level with the Advanced Encryption Standard (AES) 256-bit algorithm. Database encryption prevents unauthorized access of sensitive data on the server.

The AES encryption algorithm provides a high level of security for sensitive data. The creation of AES was instigated by the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) to find a replacement for the Data Encryption Standard (DES), which had numerous issues, namely small key size and efficiency.

Encryption algorithms use keys to obfuscate the data. While DES only had a key size of 56 bits, AES can have a key size of 128, 192 or 256 bits. Larger keys provide more security as their size makes brute force attacks infeasible.

To address concerns from the cryptographic community, the NIST embarked on a transparent selection process. During the selection process the NIST solicited designs from the global cryptographic community and voted for a winner from within fifteen finalists. The eventual winner was a team of Belgian cryptographers with their submission of the Rigndael encryption method.

For more information about the technical specifications of AES, please see the official standard.

SSL

IBM Security Verify Privilege Vault can be configured to run by using Secure Sockets Layer (SSL) certificates. It is strongly recommended that IBM Security Verify Privilege Vault installations run by using SSL. Not using SSL will significantly reduce the security of the contents of IBM Security Verify Privilege Vault since browsers viewing the site will not be using an encrypted connection.

Two-Factor Authentication at Login

Users who access IBM Security Verify Privilege Vault from laptops or other mobile devices are more vulnerable to having a device stolen. Requiring multiple forms of authentication provides additional security against theft or attempts to crack a user's password.

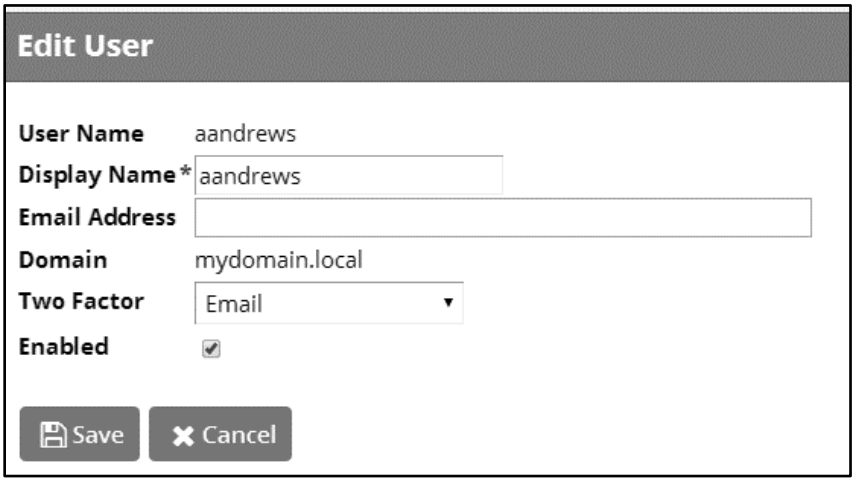
Two-factor authentication is a method of strong authentication that requires two different forms of identification instead of the traditional single password. The types of two-factor authentication supported by IBM Security Verify Privilege Vault include the following:

- **Email**
  A one-time pincode is emailed to the user. For further information, see Email Two-Factor Authentication, below.
- **RADIUS**
  Users will be prompted for their RADIUS password or token as second factor of authentication.
- **Mobile App / Soft Token**
  Users will be prompted to configure their mobile app or soft token by using either Duo Security or TOTP RFC6238, such as Google Authenticator or Microsoft Authenticator.

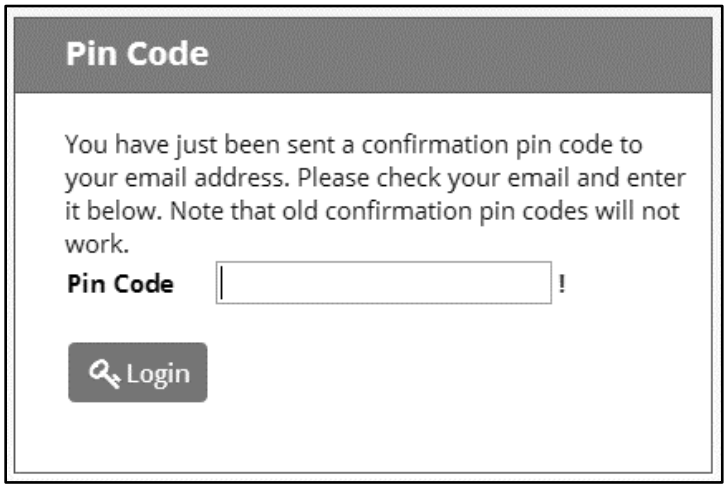
Email Two-Factor Authentication

IBM Security Verify Privilege Vault uses this design by allowing administrators to require two-factor authentication through a confirmation email for designated users. For additional information on two-factor authentication, please see this Wikipedia article.

To configure email two-factor authentication, from the Users administration page select a user to configure. Click Edit, check the Email Two Factor Authentication box, and click save. Verify that the correct email address information is set, as that address is where the confirmation email will be sent.



The next time that user attempts to login to the system, a unique confirmation code will be emailed to them. The user will then be required to enter a new confirmation code at each login.



RADIUS Authentication

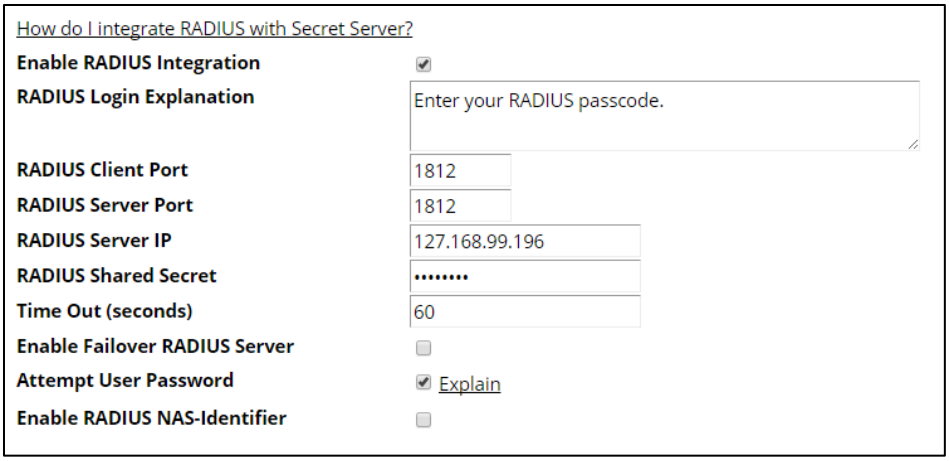
IBM Security Verify Privilege Vault allows the use of RADIUS two-factor authentication on top of the normal authentication process for additional security needs. IBM Security Verify Privilege Vault acts as a RADIUS client that can communicate with any server implementing the RADIUS protocol.

Configuring RADIUS

RADIUS can be set up on the Login tab of the Configuration page. This requires enabling RADIUS Integration, specifying the server address, the ports, and the RADIUS Shared Secret. The shared secret is a specific term for RADIUS clients and is not a reference to Secrets in IBM Security Verify Privilege Vault.

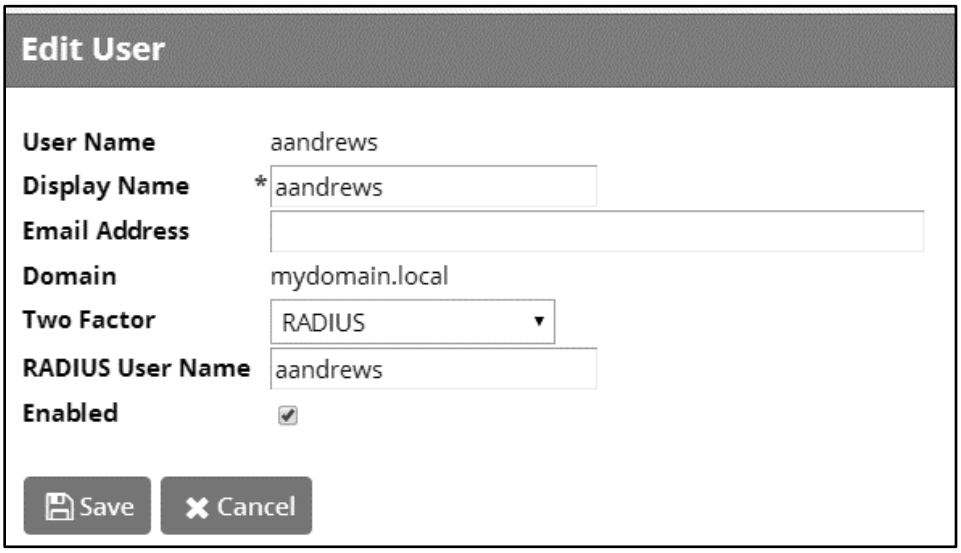
The RADIUS Login Explanation can be customized to give users detailed instructions for entering their RADIUS information.

Once enabled, the Test RADIUS Login button appears on the Login tab for testing the communication with the RADIUS Server. If you have a failover RADIUS Server, you can specify it by clicking the Enable RADIUS Failover check box and entering the required information. If the primary RADIUS server can’t be accessed, the failover server will be used.



Enabling RADIUS for a User

After enabling RADIUS on your IBM Security Verify Privilege Vault, you must enable RADIUS two-factor authentication for each user on a per-user basis. On the User Edit page, enter the RADIUS User Name for this user to match the RADIUS server. RADIUS can be set to Enabled for new users by domain, see the Adding a Domain section for details.



TOTP Authentication

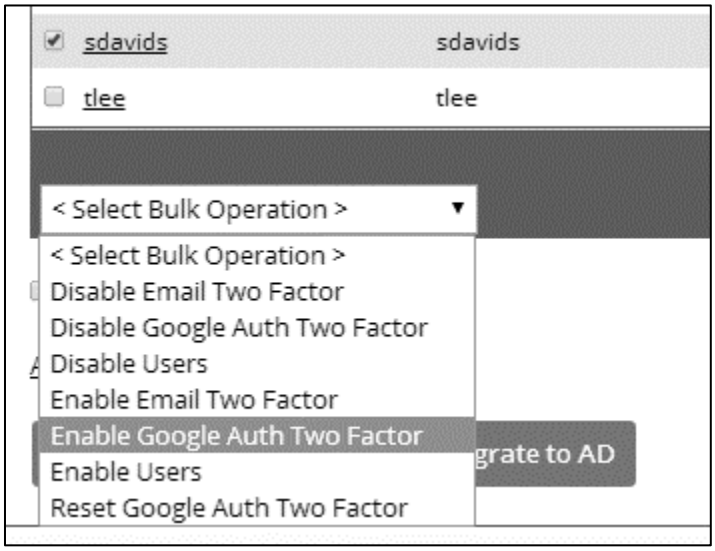
IBM Security Verify Privilege Vault support by using any type of soft token/mobile app authentication by using the TOTP RFC6238 algorithm. This includes Google Authenticator and Microsoft Authenticator. See instructions for setup below:

Enable TOTP Two-Factor Authentication

1. From the **ADMIN** menu, select **Users**.

2. Select the check box beside each user to enable two-factor authentication for.
3. From the **< Select Bulk Operation >** drop-down menu, select **Enable Google Auth Two Factor**.
4. Click **OK** in the dialog that appears, confirming the operation.
5. The user(s) will now be required to complete the soft token setup with a mobile device the next time they log into IBM Security Verify Privilege Vault. See **User Setup of Soft Token Two-Factor Authentication** for further details on the account and mobile app setup that will follow.

To disable soft token two-factor authentication, follow the same process as enabling soft token two-factor authentication for a user, selecting **Disable Google Auth Two Factor** from the bulk operation drop-down menu instead.



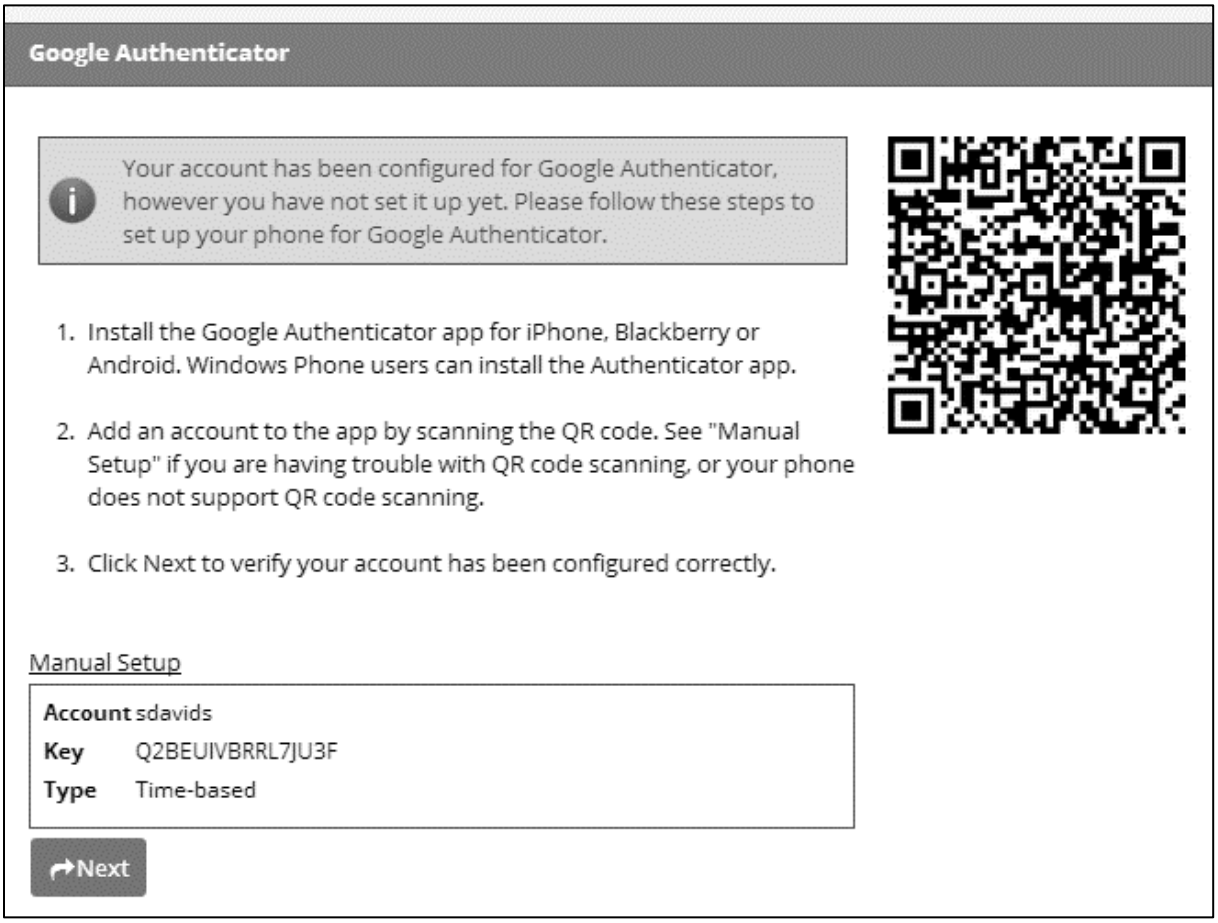
Reset TOTP Two-Factor Authentication

1. From the **ADMIN** menu, select **Users**.
2. Select the check box beside the user to reset two-factor authentication for.
3. From the **< Select Bulk Operation >** drop-down menu, select **Reset Google Auth Two Factor**.
4. Click **OK** in the dialog that appears, confirming the operation.
5. The user will now be required to complete the soft token setup with a mobile device the next time they log into IBM Security Verify Privilege Vault. See **User Setup of Soft Token Two-Factor Authentication** for further details on the account and mobile app setup that will follow.

User Setup of TOTP Two-Factor Authentication

1. Log into the main IBM Security Verify Privilege Vault login screen.
2. After successful authentication, a new screen will appear with instructions.
3. Follow the instructions to configure the mobile device for soft token authentication. To enter the key manually rather than scanning the QR code, click the **Manual Setup** link (see image below).
4. Click **Next** to continue, and enter the token in your mobile app to complete the setup.

Note If you experience errors while setting up soft token authentication with a mobile device, see Troubleshooting Google Authenticator for more information.



Duo Security Authentication

Note Using this method of two-factor authentication requires that you have an active account for Duo Security.

IBM Security Verify Privilege Vault support by using Duo Security as a second factor of authentication. See below for setup instructions:

Enable Duo Security Two-Factor Authentication

1. From the **ADMIN** menu, select **Configuration**.
2. Click the **Login** tab, and then click **Edit**.
3. Select the **Enable Duo Integration** check box.
4. Enter the **API Hostname**, **Integration Key**, and **Secret Key** values (obtain these by logging into your account at duosecurity.com).
5. Click **Save**.

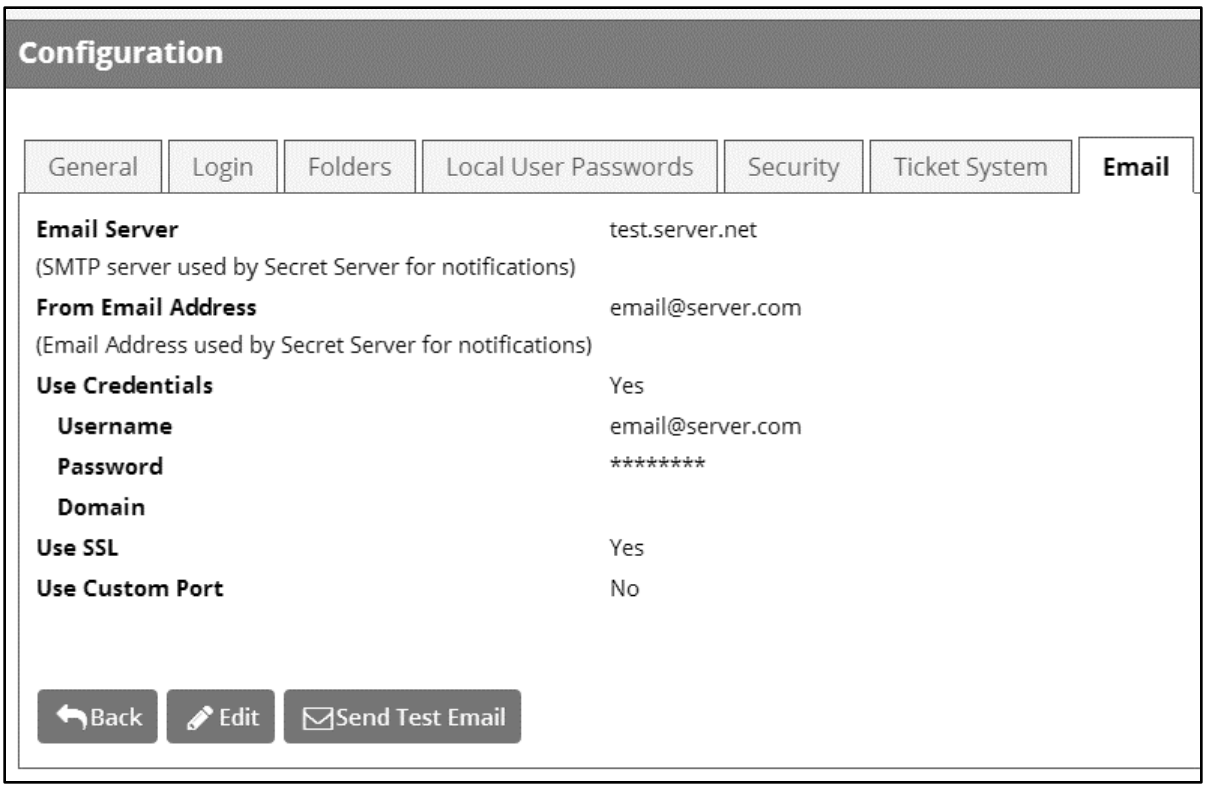
6. See **User Setup of Duo Two-Factor Authentication** for further details on the procedure that the user will follow.

User Setup of Duo Two-Factor Authentication

1. Log into the main IBM Security Verify Privilege Vault login screen.
2. After successful authentication, a new screen will appear with the option to select a method to authenticate with.
3. Select one of the options (they might be **Duo Push**, **Send SMS**, and/or **Phone**, depending on your setup with Duo) and complete the selected authentication process to log in.

SMTP Configuration

IBM Security Verify Privilege Vault requires that a connection to a SMTP server be properly configured to send out confirmation code emails. Enter the SMTP server information and an email address that will be used to send notifications.



When configuring IBM Security Verify Privilege Vault to an SMTP server, the server's availability can be verified through Telnet:

In the command prompt run the following:

"telnet servername 25"

In this command, servername can be replaced by the SMTP server, and 25 is the port that IBM Security Verify Privilege Vault is configured to attempt to connect through. An example command would look like:

"telnet smtp.somesite.com 25"

If virus protection is running, a rule to allow aspnet_wp.exe to send e-mails might be necessary.

FIPS Compliance

The Federal Information Processing Standard 140-1 (FIPS 140-1) and its successor (FIPS 140-2) are United States Government standards that provide a benchmark for implementing cryptographic software. IBM Security Verify Privilege Vault has been tested within environments that are FIPS compliant.

For instructions to enabling FIPS in IBM Security Verify Privilege Vault, see the Enabling FIPS Compliance in IBM Security Verify Privilege Vault KB article.

PCI Datacenter Compliance

IBM Security Verify Privilege Vault can make it easier to comply with various PCI-DSS requirements:

Requirement 8 Assign a unique ID to each person with computer access|

Requirement 10 Track and monitor all access to network resources and cardholder data

Requirement 11 Regularly test security systems and processes

Requirement 12 Maintain a policy that addresses information security

Our solution will help you comply with Requirement 8 by providing a secure repository for you to maintain an automated password changing schedule; forcing each user to have a unique, secured password. IBM Security Verify Privilege Vault's web-based access makes it easy to access these passwords.

As for Requirement 10, IBM Security Verify Privilege Vault can monitor all access to network resources. By employing Remote Password Changing to force password changes, administrators can monitor and update network resources on a customized scheduled. You can create a password changing schedule that best suits your environment.

IBM Security Verify Privilege Vault can help regularly test security systems and processes for Requirement 11 through features like Heartbeat and Reports that create visibility about who is accessing what resources while ensuring that security functionality is working and effective.

Lastly, to help you comply with Requirement 12, our software's global configuration and template-driven data structure can be optimized to fit the requirements of your current information security policy or assist in creating a policy based around IBM Security Verify Privilege Vault.

The following configuration options are available:

- Two-factor authentication
- Local User Password requirements
- Force HTTPS/SSL
- Require Folder For Secrets
- Enable Launcher
- Enable Webservices
- Heartbeat

HSM Integration

IBM Security Verify Privilege Vault can be configured to use an HSM. The HSM is a hardware device which will handle the encryption/decryption in hardware. As the encryption keys are stored within the hardware device itself (and never leave the device), use of an HSM increases the security of the encrypted data. Supported HSMs include SafeNet or Thales PCI or Network HSMs (paired PCI HSMs, for failover can be used as well).

SafeNet and Thales HSM's are FIPS 140-2 certified and are the type of HSM most typically used by government and military customers.

IBM Security Verify Privilege Vault does not require an HSM to function, but it is available as an option for environments that require the highest levels of security. For information about configuring an HSM with IBM Security Verify Privilege Vault see the HSM Integration Guide.

Network HSMs are supported by IBM Security Verify Privilege Vault version 8.8 and higher. Prior to that version only PCI HSMs are supported.

Key rotation

Secret key rotation is the process by which the encryption key used for securing Secret data is changed and Secret data is re-encrypted. Each Secret receives a new, unique AES-256 key. Secret key rotation can be used to meet compliance requirements that mandate encryption keys be changed on a regular basis. Secret Key Rotation requires the **Rotate Encryption Keys** role permission.

To perform Secret key rotation, go to the **ADMIN** menu and select **Configuration**, then click the **Security** tab. Under the **Key Rotation** section, click **Rotate Secret Keys**.

Secret key rotation will begin as soon as IBM Security Verify Privilege Vault enters Maintenance Mode. Because Maintenance Mode disables various functionality (e.g. Secrets cannot be updated), the timing of Secret key rotation merits consideration of IBM Security Verify Privilege Vault usage with regard to processing time. We recommend running Secret key rotation during off-peak or non-business hours. To learn more about Maintenance Mode, see (KB) Maintenance Mode.

For further details about the processing time for key rotation, see (KB) Secret Key Rotation.

Licensing

Installing New Licenses

Once a license is obtained, it can be installed by copying the license name and code into the corresponding fields to a new license page. To access this page, select **Licenses** from the **Administration** menu, and then click **Install New License**.

Converting from Trial Licenses

If you previously had evaluation licenses and recently purchased, you must remove all evaluation licenses and install your purchased licenses. Normal trial licenses expire one month after issue. If the new licenses are not installed, users will start getting "License has expired" error messages.

Activating Licenses

All non-evaluation licenses require activation after install. Activation is per license/web server combination. Therefore, if you bring up a new web server, it must be activated even if your previous web server was already activated. After installing each license, you will be prompted to activate. Follow the on-screen prompts for online or offline activation. The activation process gathers the name, email, and phone number of the individual activating for internal purposes only. No other personal information will be sent to IBM.

Limited Mode

If you fail to activate, your system will be placed in limited mode, which will prevent the following actions:

- Creating and editing Secrets
- Importing Secrets
- Active Directory sync
- Web services (mobile applications)
- Manual Remote Password Changing