Passwordstate

Enterprise Password Management

Passwordstate User Manual

Table of Contents

1 Passwordstate User Manual

Welcome to the Passwordstate User Manual.

This Manual will provide instructions for the basic usage of Passwordstate, as well as more detailed instructions for settings and permissions as they relate to Password Lists.

Getting Started - Glossary

Before getting into the detail of this manual, it is recommended you first read the brief glossary so you are aware of some of the terms used throughout this manual - Glossary.

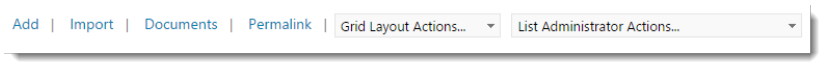
Getting Started - New Users

If you are new to Passwordstate, please study the Quick Start Tutorials to familiarize yourself with the basics.

1.1 Glossary

Please become familiar with the following Passwordstate glossary, as a knowledge of each of the definitions will be useful in understanding the rest of the content in this manual.

Definition	Description
List Administrator Actions	A drop-down list of actions (functions) applicable to each Password List, and accessible by Password List Administrators
Password	A secret word of phrase that must be used to gain access to something i.e. IT infrastructure, business system, secure web site, etc
Password List	A collection of related passwords
Password List Administrator	A registered user of the system who has been granted 'administrator' permissions to a Password List - allowing them to control settings, permissions, run various reports, etc.
Password List Template	A template for a collection of related passwords, whose settings can be used as a basis for creating new Password Lists, or linked to existing Password Lists.
Shared Password List	A collection of related passwords which can be shared amongst multiple users

Private Password List	A collection or related passwords which are only visible to the user who created the Private Password List
Password Folder	A collection of related Password Lists
Navigation Menu	The horizontal menu system visible at the bottom of the screen i.e. Passwords, Generator, Auditing, Preferences, Administration and Help
Navigation Tree	The tree-structure visible on the left-hand side of Passwordstate interface which shows all the Password Lists and Folders you have access to
Security Administrator	A registered user of the system who has elevated privileges, allowing them to administer various system wide settings
Actions Toolbar	A number of buttons/controls visible at the bottom of each of the Passwords grids. 

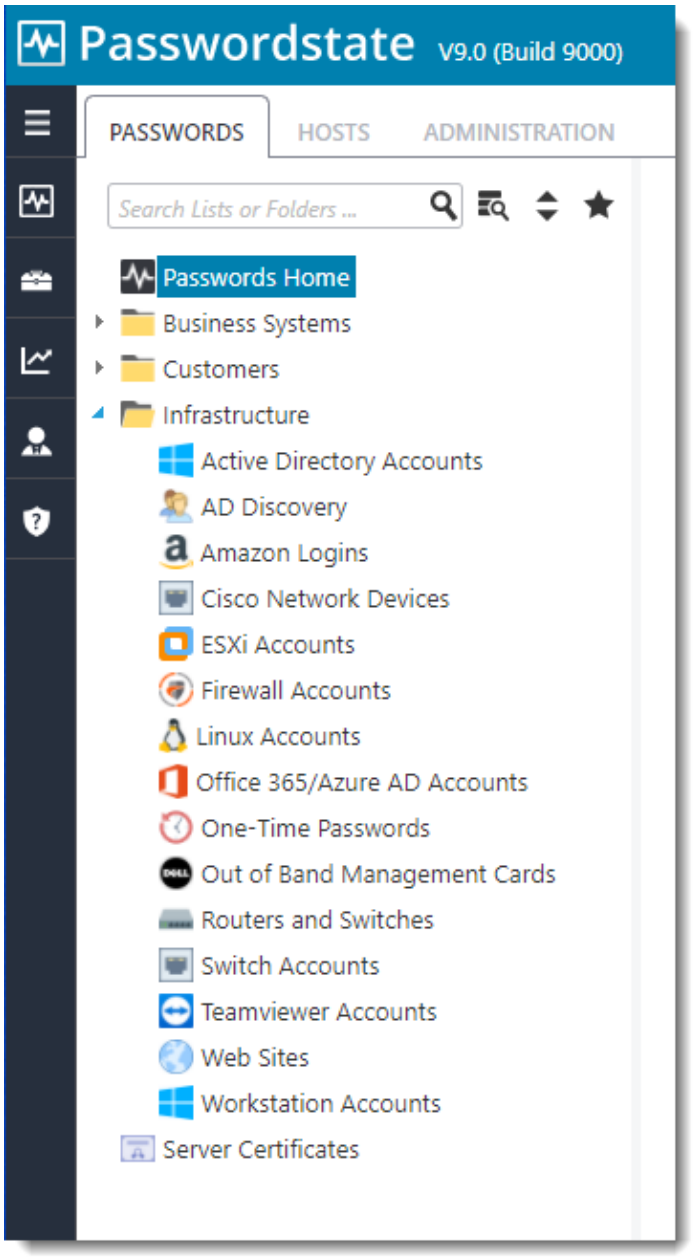
1.2 Quick Start Tutorials

The following is a few quick tips to get you familiar with the Passwordstate interface, and some of the features it offers.

Organizing Password Lists Navigation Tree

You can organize the Password Lists Navigation Tree, displayed on the left hand side of Passwordstate, by simply dragging and dropping the tree nodes. Any changes you make to how the tree structure appears, will automatically be saved and displayed the same next time you use Passwordstate.

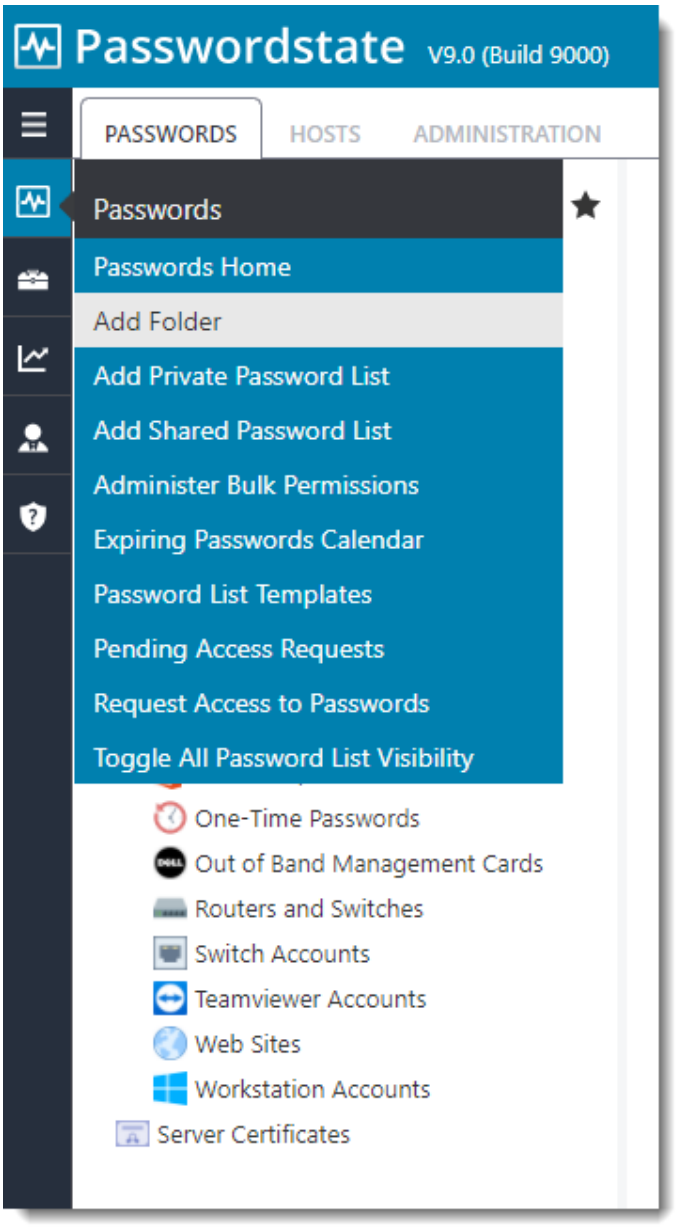
If you want a tree node to be displayed at the root of the navigation tree, simple drag and drop onto the highlighted 'Passwords Home' node you see in this picture.



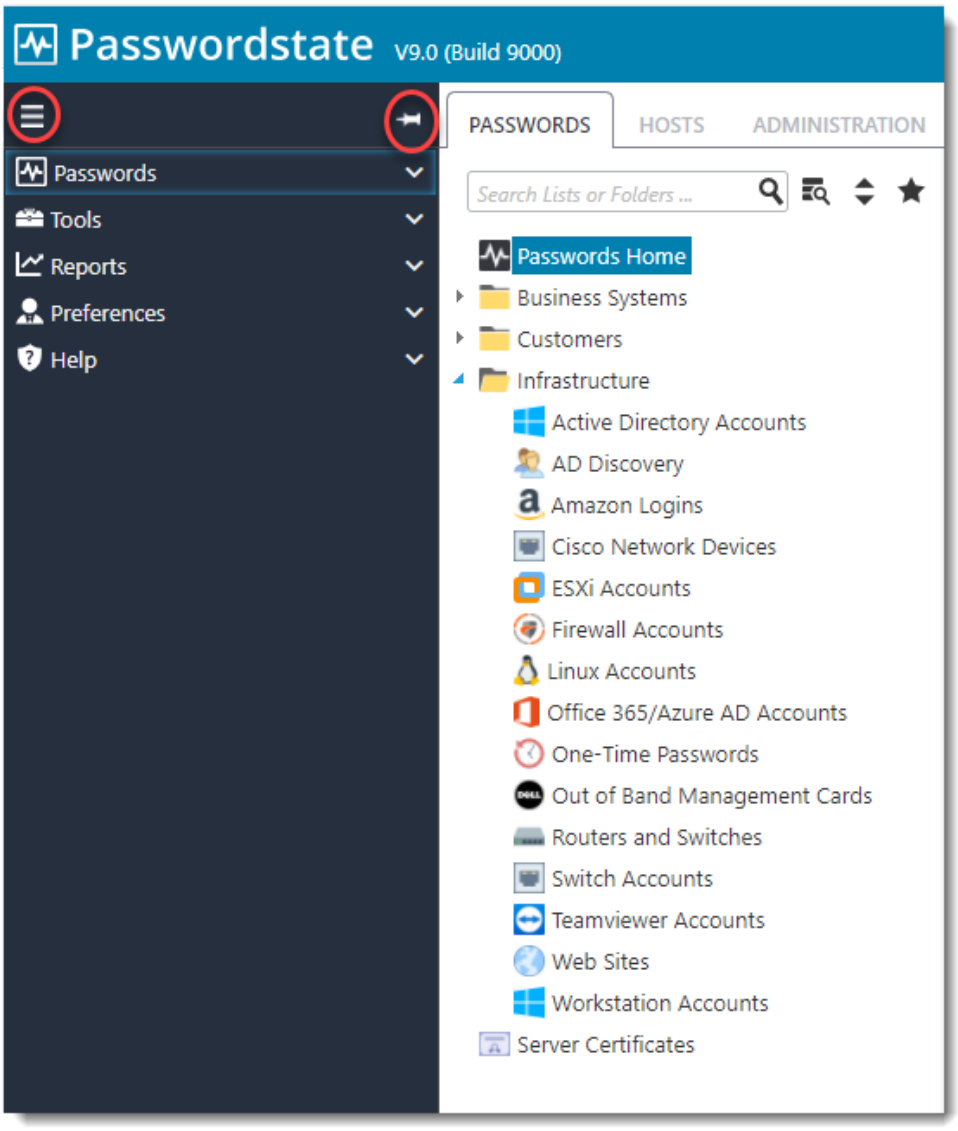
Navigation Menu

The Main Navigation Menu can be found on the left hand side of the screen. Each of these Menus have sub-menus providing access to the core functionality within Passwordstate.

Note: Some of these actions may be disabled, or hidden, by your Security Administrators of Passwordstate.



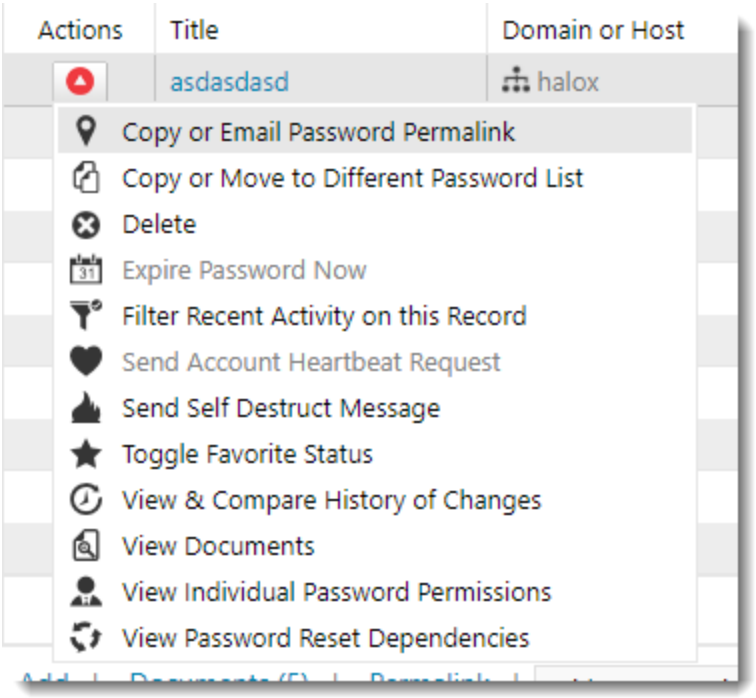
You can also expand and pin the Vertical Menu.



Grid Actions Drop-down Menus

On the majority of the grids which you will see, there is a little Green graphic which you can click on to provide various actions. With the image to the left, this is the available actions for individual passwords.

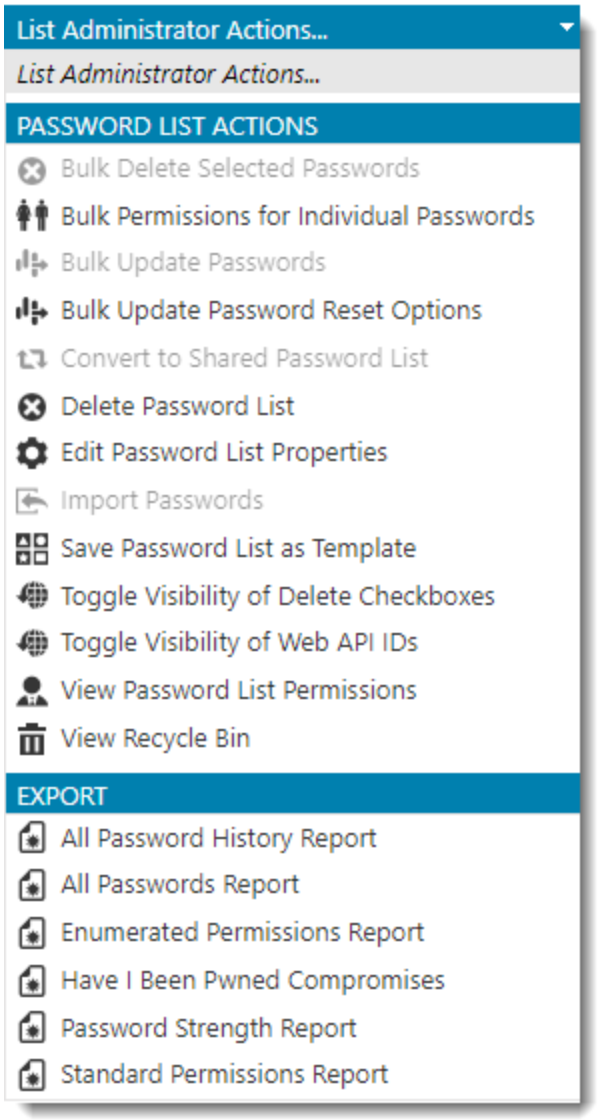
Note: Some of the actions may be disabled depending on some site wide settings, or on your own access rights.



Password List Administrator Actions

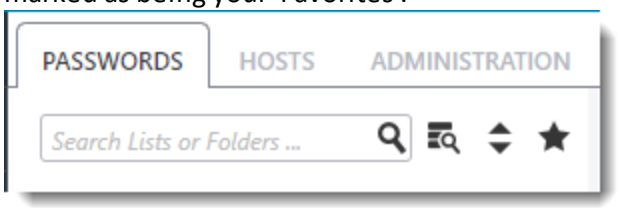
At the bottom of each of the Passwords grids, you may see a 'List Administrator Actions' drop-down list as per the image to the left. From this drop-down you are able to administer permissions and edit details for the Password List, as well as various types of reporting.

Note: This drop down list will not be available to you if you only have Read or Modify access to the Password List.



Searching for Password Lists and Folders in the Navigation Tree

If you have a many Password Lists you need to manage, the Quick Navigation search box makes it easy to search and automatically select the correct Password List - it will even search nodes which are collapsed and not visible. The Star symbol also allows you to filter any Password Lists you have marked as being your 'Favorites'.



Resizing the Navigation Tree Pane

> You can re-size the Navigation Tree pane by simply dragging the following re-size divider.
>
> Resizing the Navigation Pane is also automatically saved for the next time you use Passwordstate.

View or Copy Password to Clipboard

Within each of the Password Grids, you can quickly view a Password by clicking on the masked password (******), or you can copy to the clipboard by clicking on the icon.

Both of these actions will add an audit event record.

Password and Password List Permissions

Permissions can be applied for individual User Accounts, or Security Groups (either a Local Security Group, or an Active Directory Security Group). The following types of permissions are possible:

- Password Lists:
  - View: Can only view the passwords
  - Modify: View access, plus edit and delete passwords
  - Administrator: Modify access, plus administer permissions and make changes to the Password List
- Individual Passwords:
  - View: Can only view the password
  - Modify: View access, plus edit and delete password

Searching for Passwords

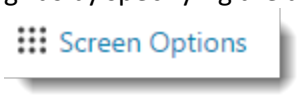
You can search for one or more Passwords by using the Search box at the top of each page - see image below. This search box will search all text based fields within the Password List i.e. it won't search numeric, Boolean or date fields.

If you have clicked on the 'Password Home' tree node, or any Folders, then this will search through all passwords nested beneath this node.

Resetting Number of Rows in Grids

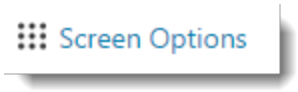
You can reset the number of rows displayed in grids by selecting the appropriate option in the drop-down combo-box.

On the main 'Passwords' or 'Passwords Home' pages, any number of rows can be specified for the grids by specifying the appropriate value in the area.



Screen Options

For the main 'Passwords' or 'Passwords Home' pages, ensure you click on the button, as this will provide you multiple options for configuring how the screen looks and behaves.



Note: Some of these options may be disabled as your Security Administrators of Passwordstate can specify some of these settings for you.

Reordering and Resizing Grid Columns

All the grids displayed in Passwordstate can have their columns reordered by dragging them left and right, and the columns can be re-sized.

Once you have the grids displaying just how you like, ensure you select 'Save Grid Layout' from the drop-down combo-box, so your settings are retained for future use.

Generate a Random Password

Anywhere you see the following icon  , clicking on this icon will generate a random password based on the settings you have specified either in the 'Password Generator' area, or for the settings specific to the Password List you are viewing.

Preferences

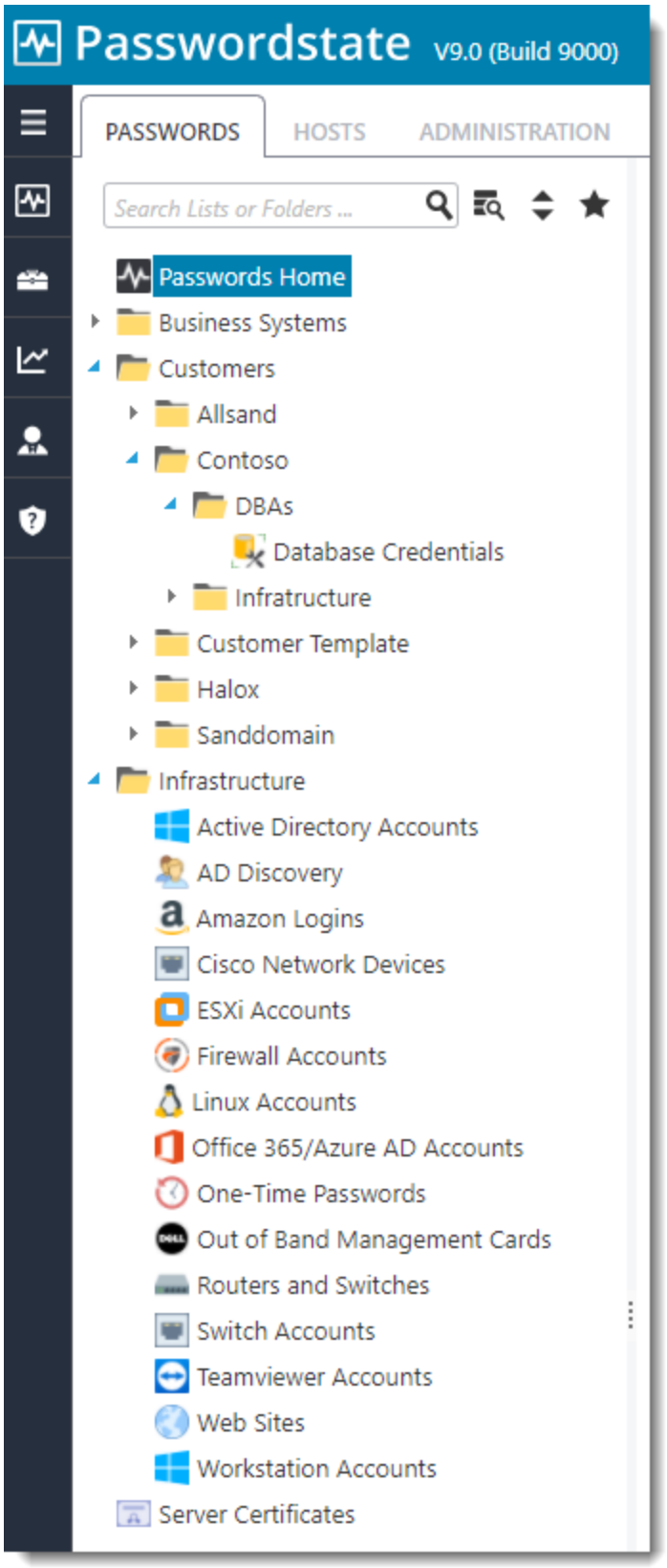
By clicking on the main 'Preferences' Menu Item, you can specify multiple settings which are specific to your account. In particular:

1. Settings under the Passwords tab
2. Settings under the Hosts tab
3. Various miscellaneous settings
4. Color Themes
5. Authentication options
6. Mobile access options
7. Browser extension settings

2 Passwords

The Passwords Tab will show all of the Password Lists and Folders your account has been given access to, and is there area within the product were all standard user password management tasks will be managed from.

By using one of the menus in Passwords Menu, you can add new Folders and Password Lists, navigate back to Passwords Home, we well as various other features relating to this tabbed area of Passwordstate.



2.1 Passwords Menu

The "Passwords Menu" is where you will spend the majority of your time in Passwordstate, as this is where you access all the Shared and Private Password Lists.

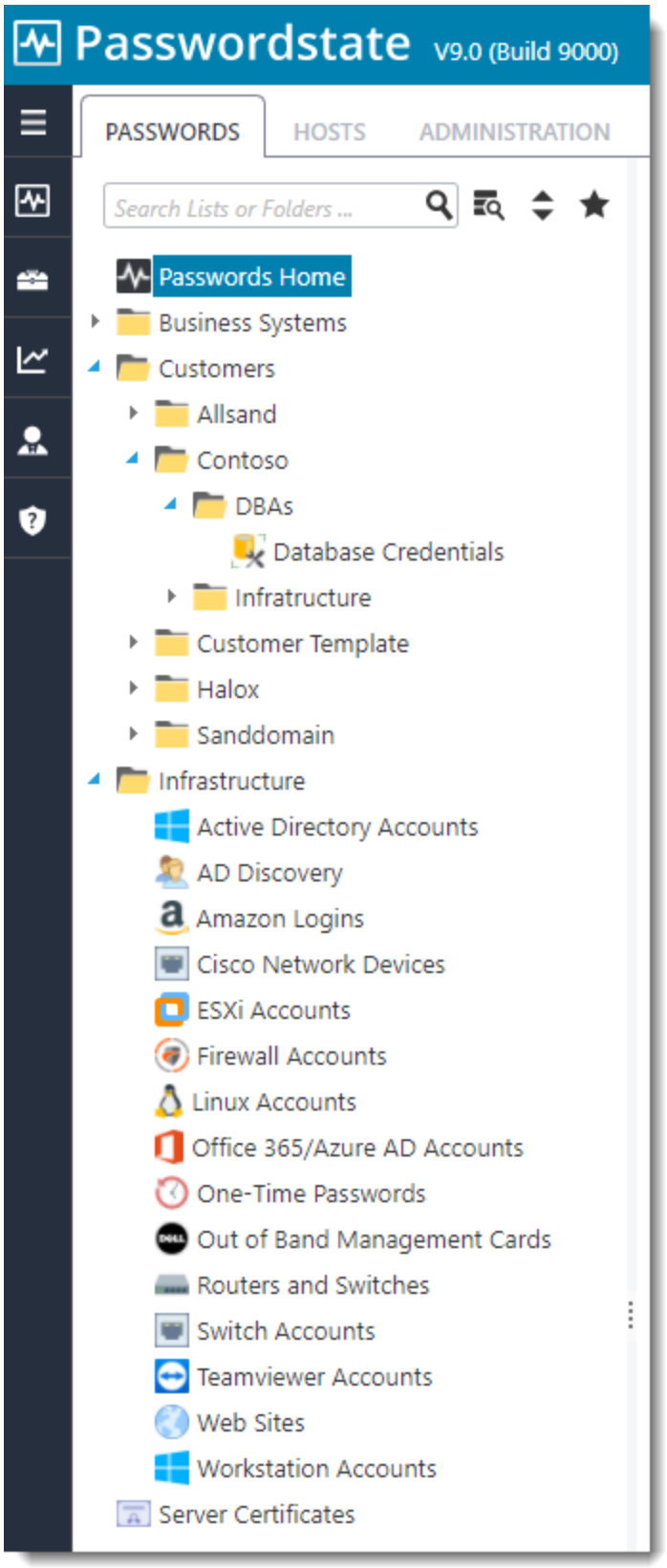
The following is a list of menu options available, of which some may be disabled/hidden by your Passwordstate Security Administrators:

Menu Item	Description
Passwords Home	Clicking on Passwords Home will display whatever Password List, or Folder, you have selected as being your default Home Page in the Preferences area
Add Folder	Allows you to add a new Folder, for organizing a group of related Password Lists
Add Private Password List	Allows you to create a new Private Password List, which is only visible to you - even Security Administrators of Password List are not aware of the existence of any Private Password Lists
Add Shared Password List	Allows you to create a new Shared Password List, which can be shared with other users in Passwordstate
Administer Bulk Permissions	Allows you to assign permissions to multiple Password Lists at once, for either user accounts in Passwordstate, or security groups
Expiring Passwords Calendar	The Expiring Passwords Calendar shows you a calendar style view of passwords who have their 'Expiry Date' field set. You can navigate back and forth either by day, week or month
Password List Templates	Password List Templates allow you to create a 'template' of settings and permissions, which can be used when either creating/editing a Password List settings, or you can link Password Lists to a Template, and then manage all the settings for multiple Password Lists from the one Template
Pending Access Requests	Allows you view/process any access requests you are responsible for, or view our own status of access requests
Request Access to Passwords	Allows you to search for Password Lists or Password Records, and request access to them
Toggle All Password List Visibility	This feature will show all Password Lists and Folders in the navigation tree, regardless of whether you have access or not. Items will be highlighted in Red if you do not have access, and clicking on them will allow you to request access

2.1.1 Passwords Home

Clicking on Passwords Home will display whatever Password List, or Folder, you have selected as being your default Home Page in the Preferences area.

It is this menu option where you will spend most of your time in Passwordstate, and is the default menu option when you first browse to the site.

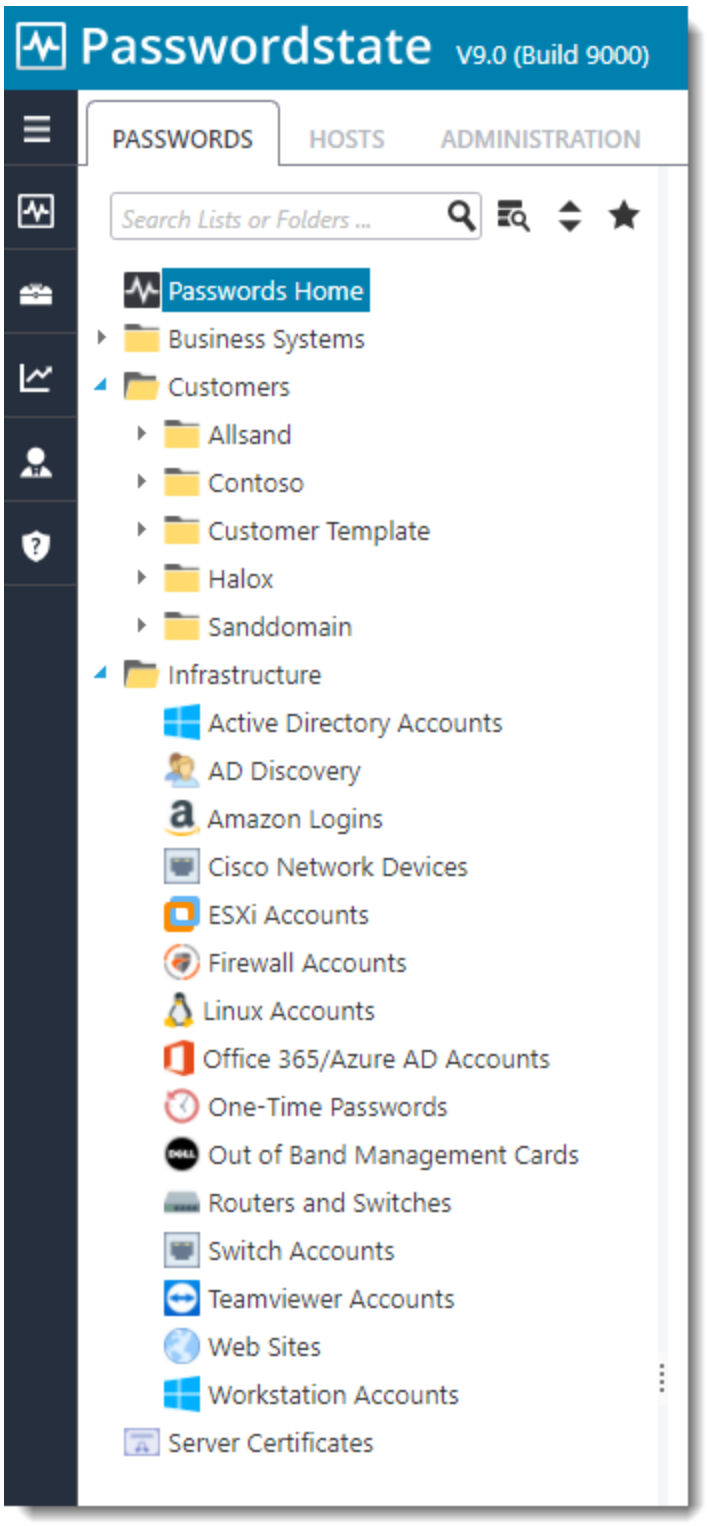


2.1.1.1 Navigation Tree

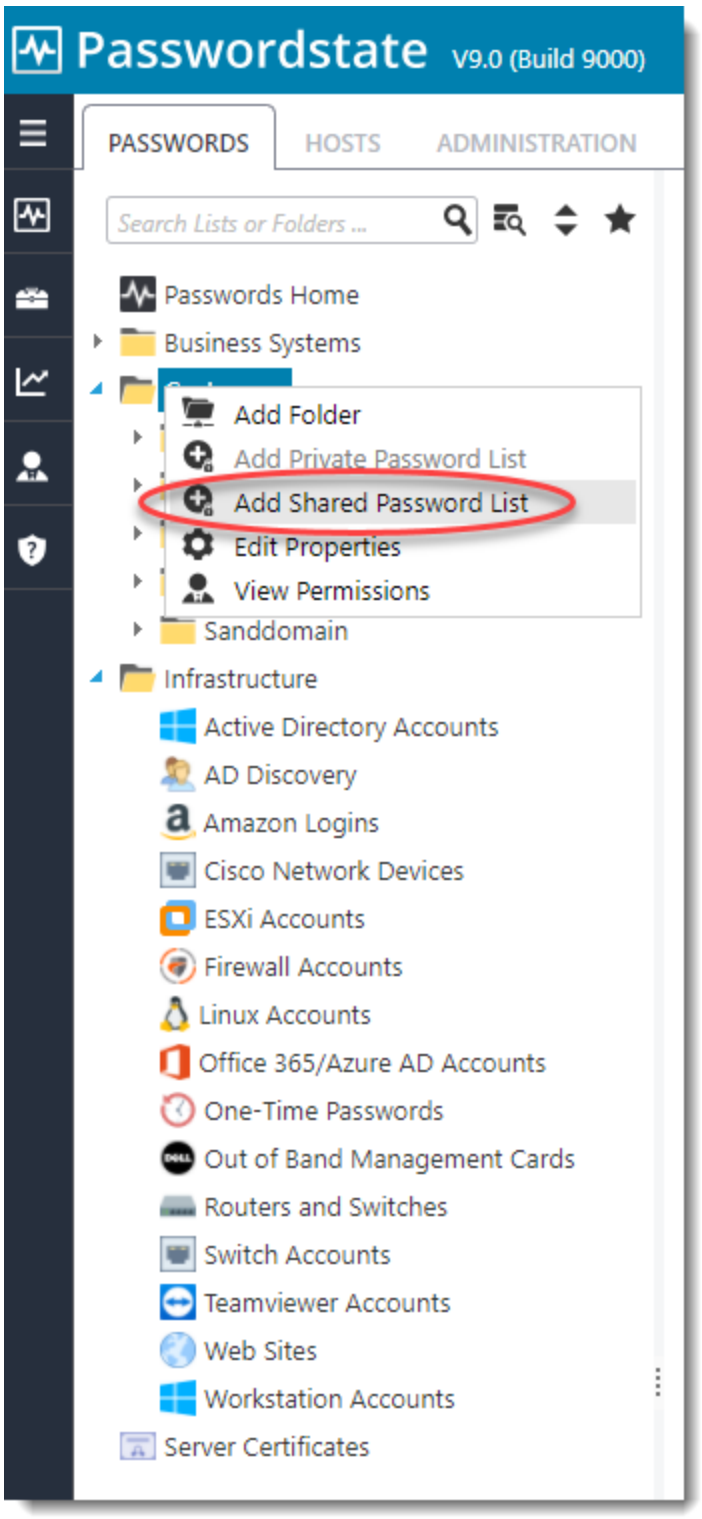
The Passwords **Navigation Tree** is used to access all of the Password List you have been given access to, and it is used to logically group related Password Lists and Folders. The only Folders and Password Lists visible in this panel are the ones you have been given access to.

Some of the features of the Navigation Tree are:

- The **Search Password Lists or Folder** textbox allows you to quickly search for the desired Password List or folder, and can be useful if you have many Password Lists and Folders displayed
- Clicking on a Folder will display a screen to the right which allows you to:
  - View/Edit Settings for the Folder if your account has access to it
  - View a Guide for the Folder
  - View/Manage Documents and External Links for the Folder
- Clicking on a Password List will display a screen on the right which shows all the passwords in the selected Password List. Note: not all passwords for the selected Password List may be displayed, as it's possible you may have been given access to individual passwords within the Password Lists, instead of the entire Password List
- It is possible to drag-n-drop the Folders and Password Lists around in the Navigation Tree, although the default settings only allows users who are Administrators of the Folders and Password Lists to do this
- The view/structure you see in the Navigation Tree is the view all users who have been give access will see - it's a shared view. The only time it will look different is if they haven't been given access to all of the Folders Password List in the tree structure you see
- Re-organizing items in the Navigation Tree will generate email alerts to other users who have the same access
- When expanding/collapsing tree nodes, if you hold down the Control Key while doing so, it will expand/collapse all nested Password Lists/Folders beneath the one you are clicking on
- The Star symbol also allows you to filter any Password Lists you have marked as being your 'Favorites'.



You can also right-click on the Navigation Tree, and create Folders or Password List beneath the item you right-click in.



2.1.1.1.1 Passwords Home

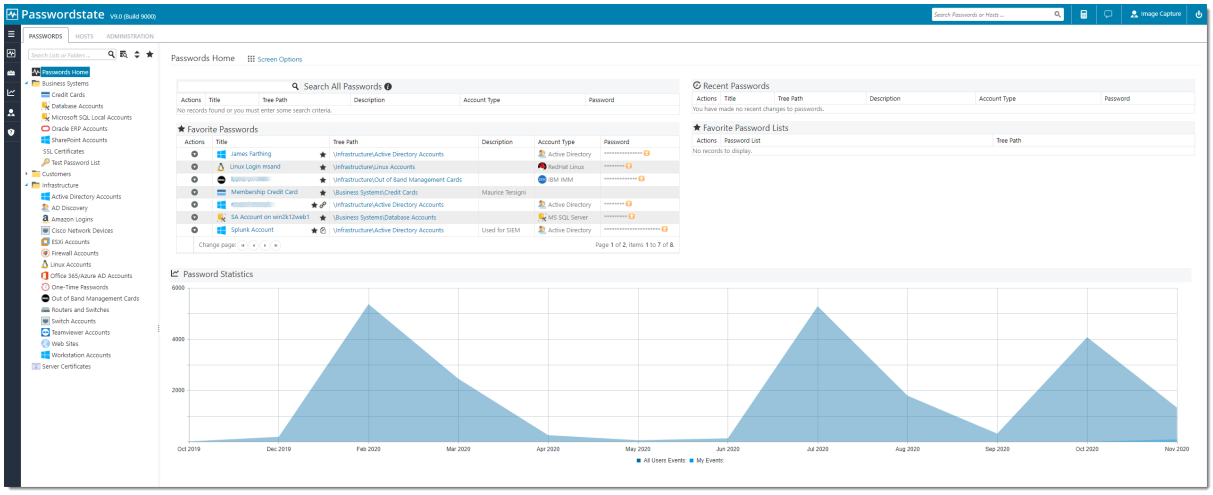
Clicking on the **Passwords Home** icon will display the screen below. This screen will be a **filtered view** of all Password Lists you have access to (.

Note: Some of these features detailed below may be hidden or disabled for you, depending on your access rights, and what settings have been applied to the various Password Lists you have access to.

On this screen you can:

- Search for Passwords across all the Password Lists you have access to (from Passwords Home), or all passwords within the selected Folder. Note: To perform an exact match search, enclose your search term in double quotes i.e. "root_admin"
- View and access Passwords you've recently used i.e. viewed/editing/copied to clipboard, etc
- View your tagged Favorite Passwords
- View your tagged Favorite Password Lists
- View some basic auditing statistics statistics
- Customize the screen by clicking on the Screen Options button
- You can edit/view a password by clicking on the hyperlink in the **Title** column
- You can view a password on the screen by clicking the masked ******* (the speed at which the password is again hidden can be control by your Security Administrators)
- You can copy a password to the clipboard by clicking on the icon (if using Internet Explorer, the clipboard can be cleared after a set time, which is set by your Security Administrators)
- You can perform various Password Actions by selecting the appropriate menu option from the Actions drop-down menu

Please Note: For the Recent Passwords Grid, none of the icons next to the Title field will be visible, due to performance reasons. When there are thousands of recent auditing records for a user, having these icons could cause performance issues due to the volume of data



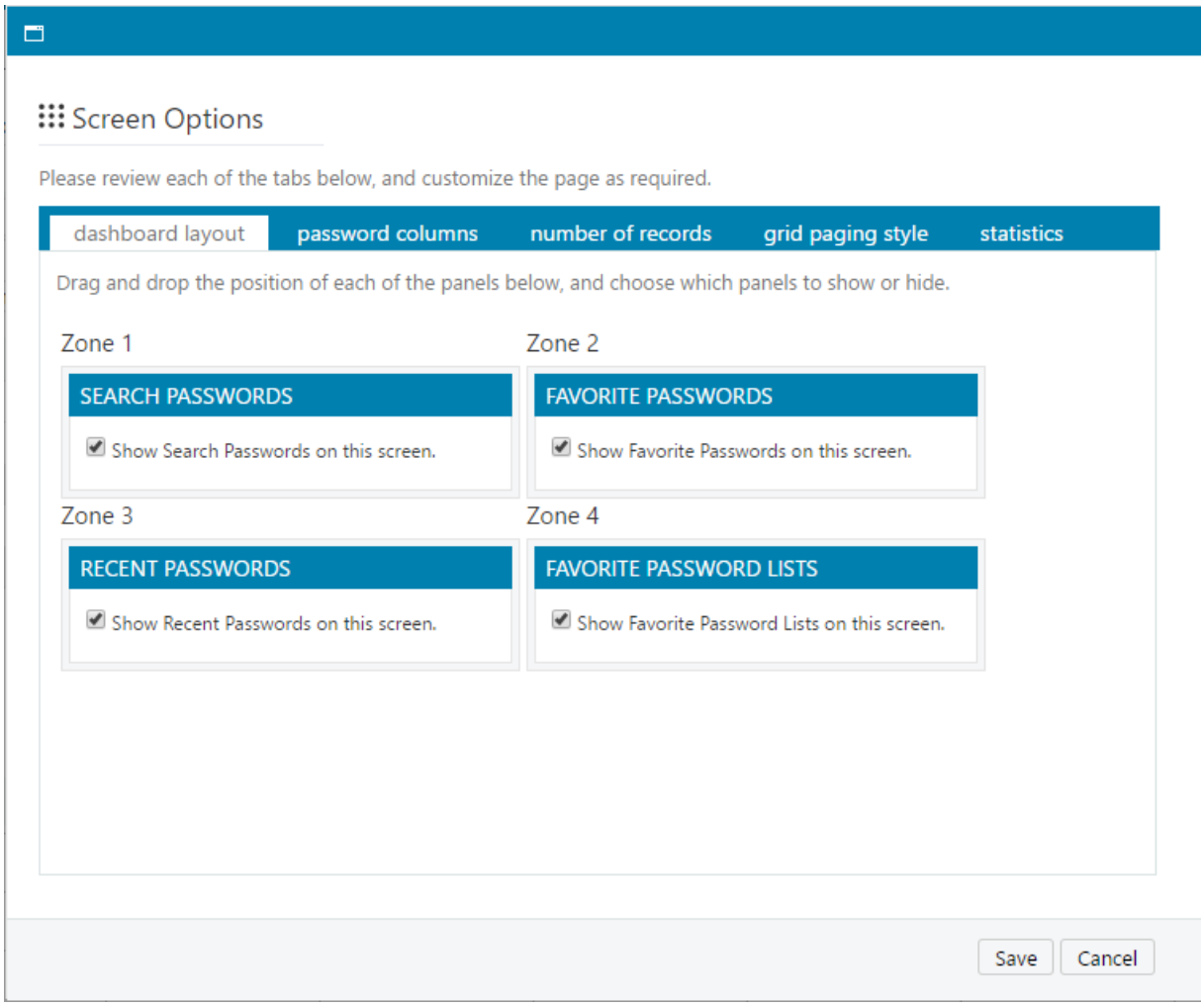
2.1.1.1.1.1 Screen Options

Screen Options allows you to specify various settings for how you would like to see the grids and charts displayed on the screen.

Please note that some of these settings may be set by your Security Administrator(s) of Passwordstate, and if so the controls will be disabled. You will see an icon like , and message telling you if this is the case.

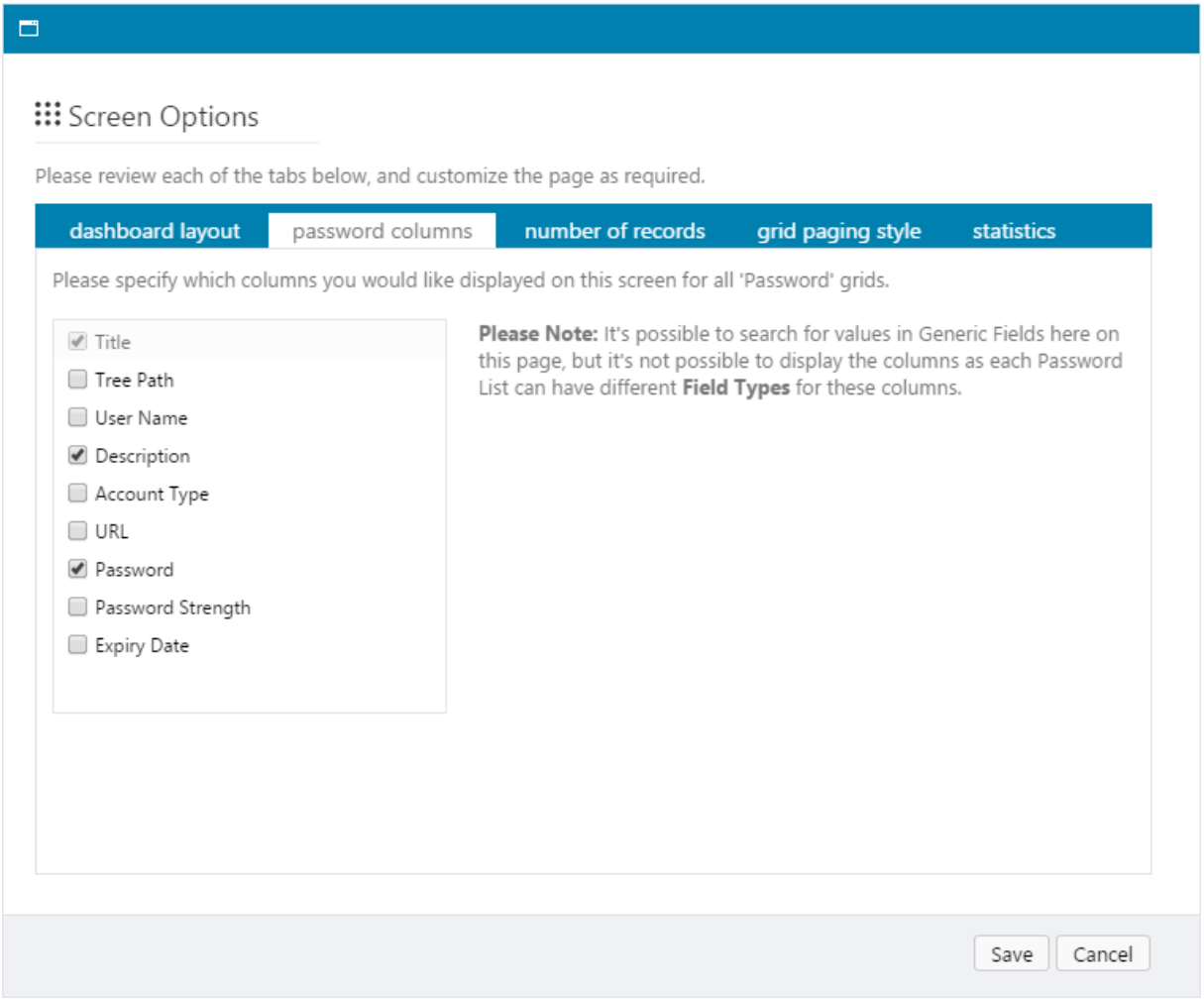
Dashboard Layout Tab

The Dashboard Layout tab allows you to select which Panels you would like to display, and in which Zone position. You can drag-n-drop the Panels around within the different Zones, so they appear in the position you like.



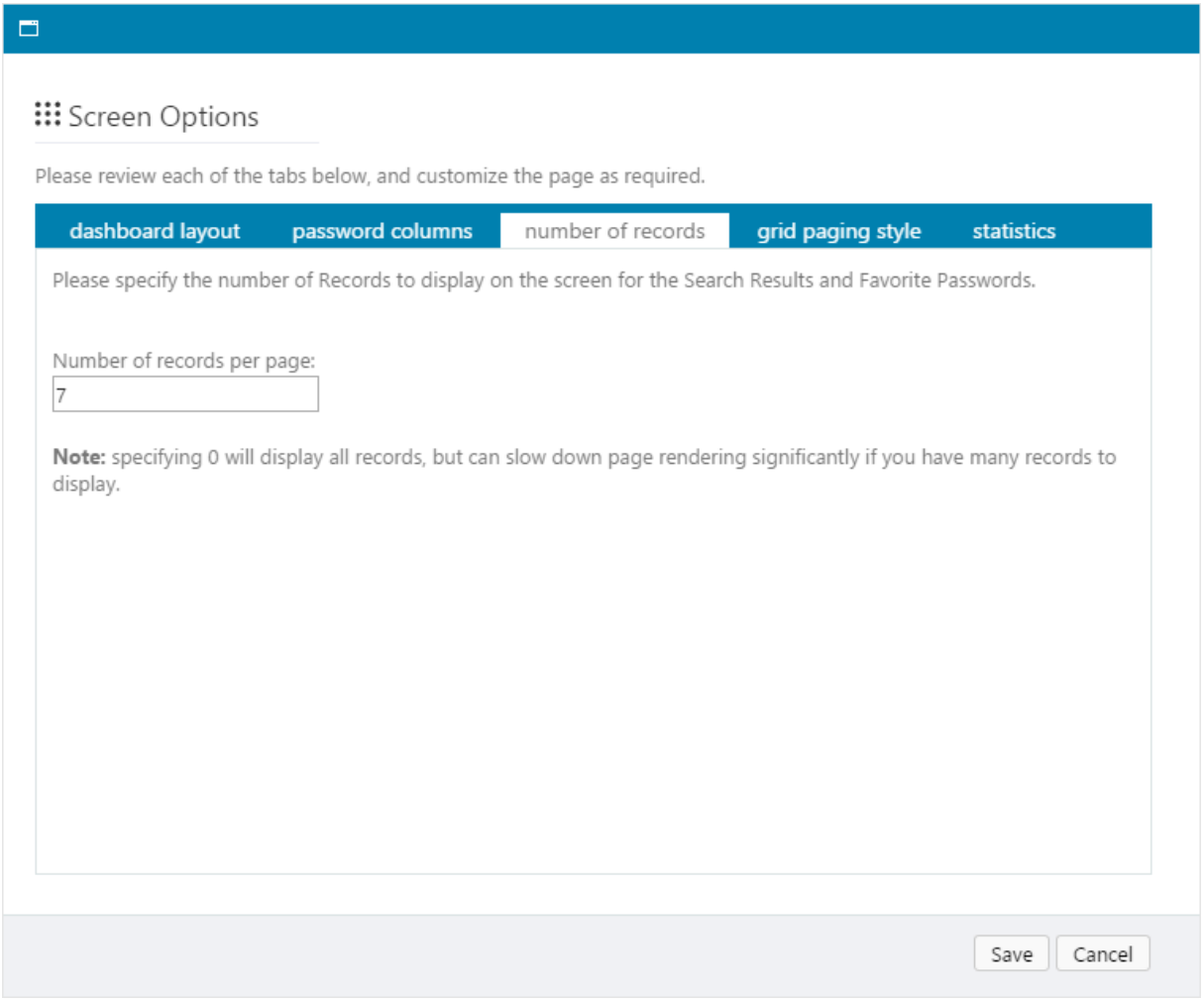
Password Columns Tab

The Password Columns tab allows you to select which columns you want displayed for each of the Passwords Grids.



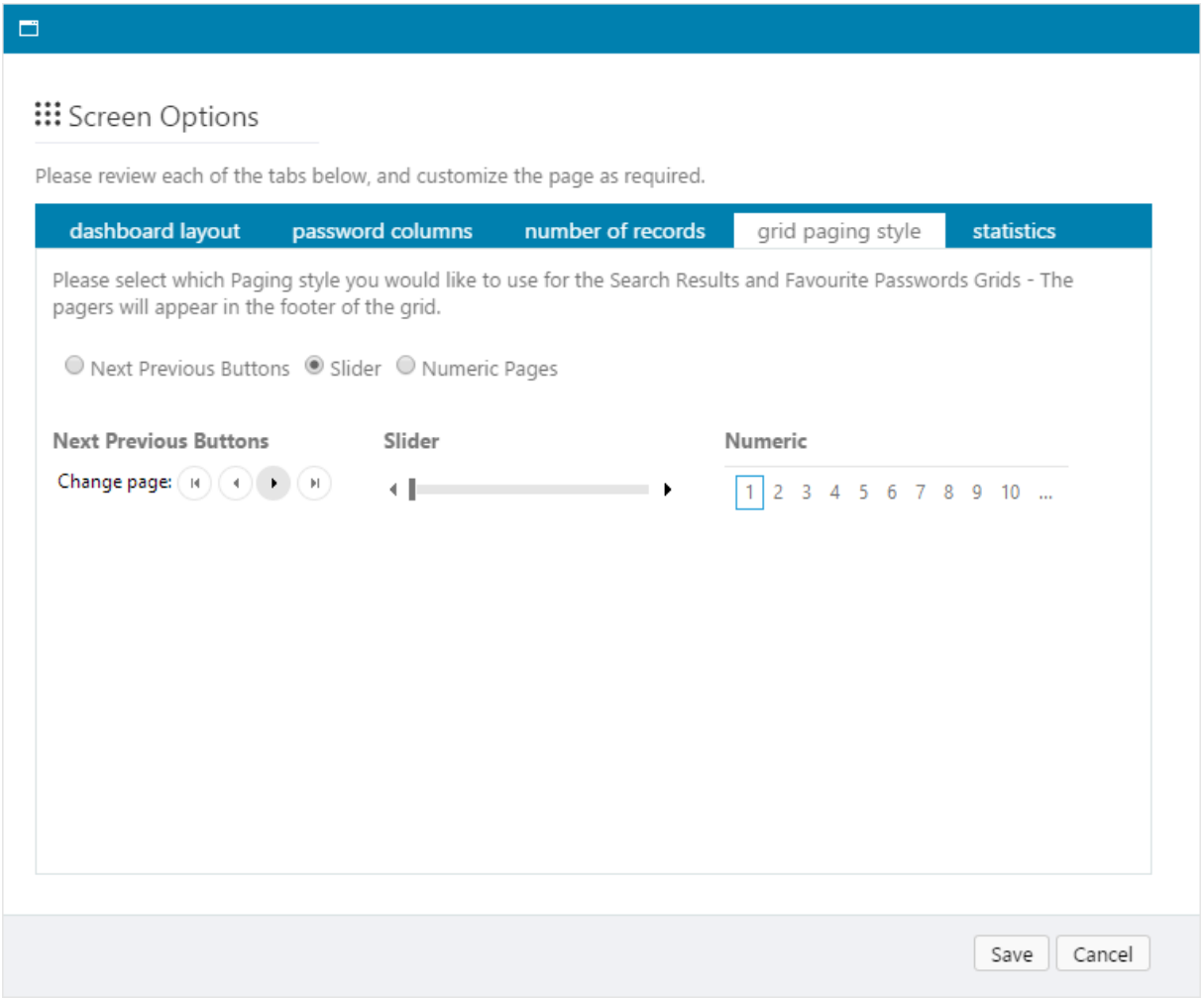
Number of Records Tab

The Number of Records tab simply allows you to specify how many records you would like displayed within any of the Grids, before the 'paging' controls will be displayed.



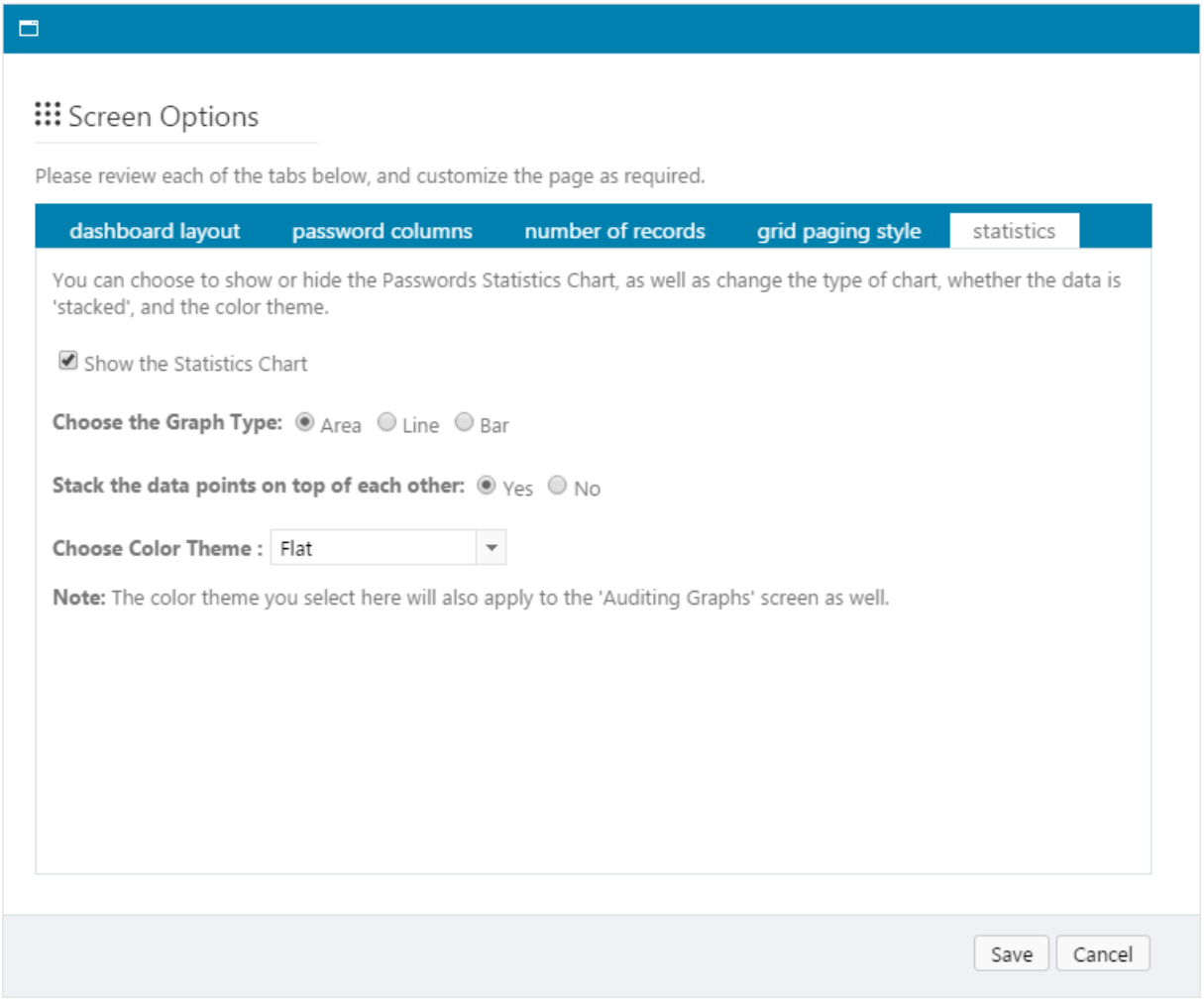
Grid Paging Style Tab

The Grid Paging Style tab allows you to choose one of three different types of 'Paging' styles, which will be used when there are more records returned than the grids are set to display.



Statistics Tab

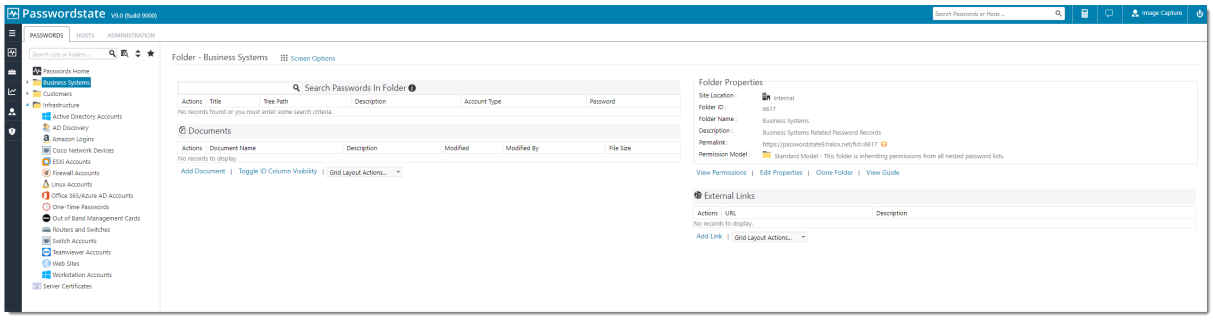
The Statistics tab allows you to either hide or show the statistics graph on the page, and which style and color of graph you would like to be displayed.



2.1.1.1.2 Folders

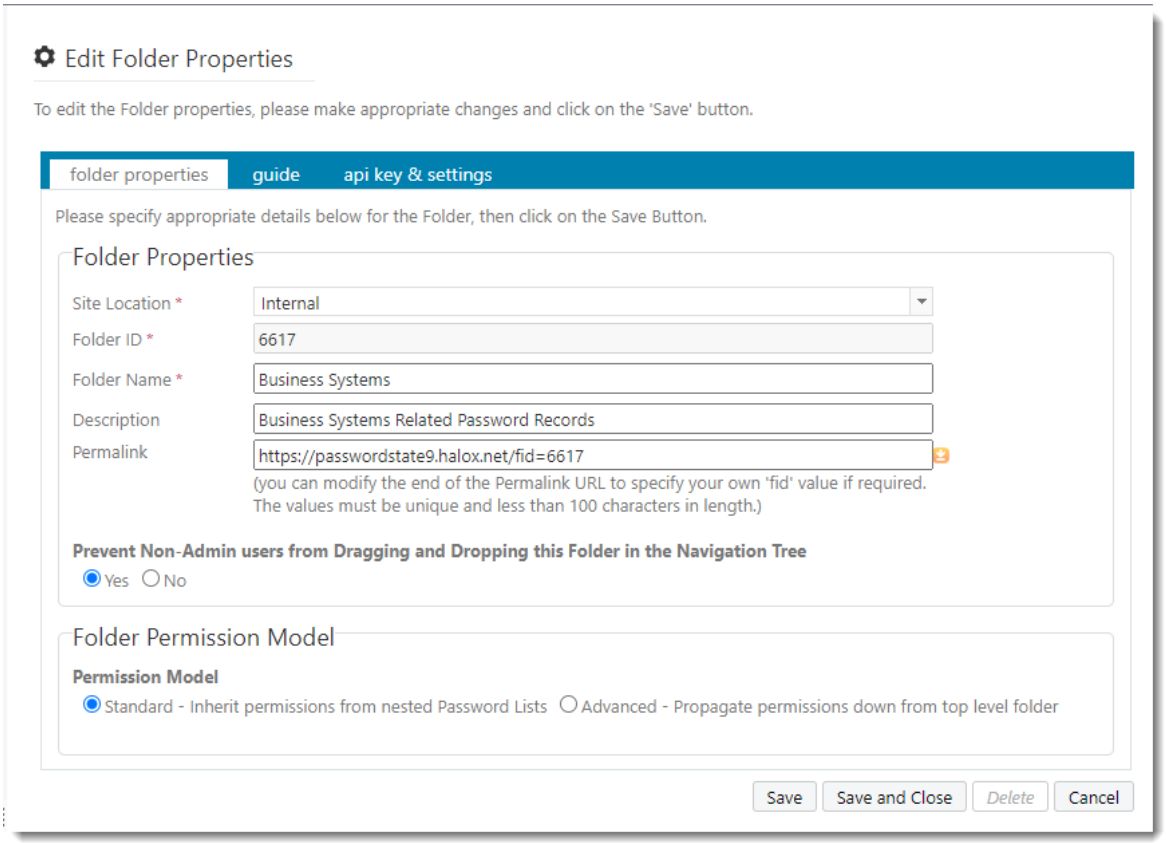
Clicking on a **Folder** will display a screen similar to below. This screen will show the following details for the Folder:

- Properties of the Folder - depending on your access level, you can edit these properties
- Permissions for the Folder
- The Guide for the Folder
- Any Documents which have been uploaded and associated with the Folder
- And any external web site links which have been associated with the Folder



2.1.1.1.2.1 Folder Properties

Folder Properties screen allows you to edit various settings related to the selected Folder, as well as various options for how permissions work for the Folder.



Folder Properties Tab

On the Folder Properties tab you can:

- Select the Site Location - By default, the "Internal" site location will be the most common, unless you have purchased a subscription for the Remote Site Locations module
- Specify the Name and Description for the folder

- Choose to prevent users with non-admin rights from dragging-and-dropping the folder in the Navigation Tree
- The Permalink allows someone to click on the URL specified, and navigate directly to the Folder

Folder Permissions Model

There are two types of permission models available in Passwordstate:

- Standard - the folder will inherit permissions from any nested Password Lists beneath it
- Advanced - the folder will propagate permissions down to all nested Folders and Password Lists

When using the Advanced Permission Model, it's also possible to select the option to "Disable Inheritance of any permissions from upper-level folders" for any nested Folders or Password Lists. By doing this, you can have different permissions set, in this propagating structure.

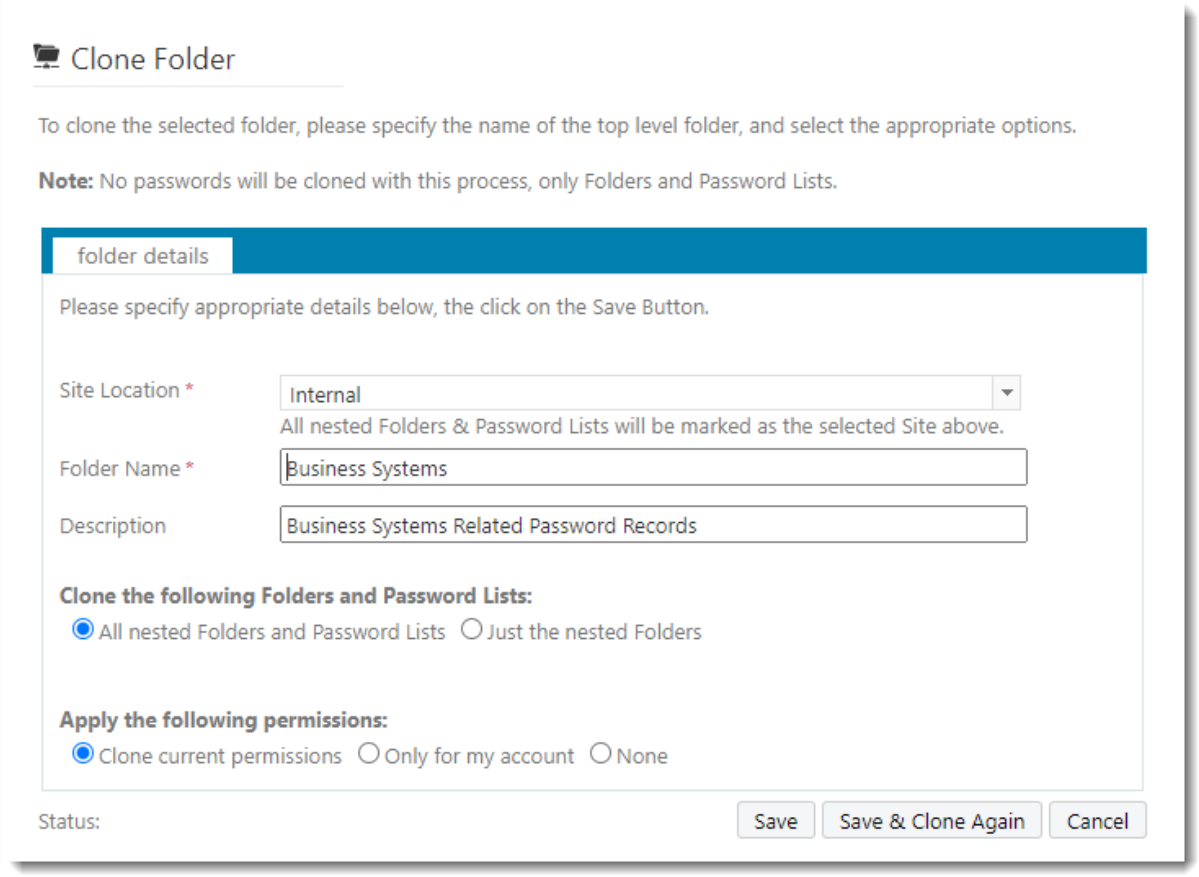
2.1.1.1.2.2 Clone a Folder

By clicking on the 'Clone Folder' button, there are various options available for you to clone the selected folder. The Options are:

- Clone all nested Folders and Password Lists, or just the nested Folders
- You can also choose to clone the current permissions applied to all the nested Folders/Password Lists, or apply just permissions for your own account, or you can choose not to clone any permissions

When cloning a folder, it will be positioned in the root of the Navigation Tree, and you can then drag-n-drop to wherever needed.

Note: No passwords are actually cloned using this method - it is only the Folders and Password Lists, plus there settings and permissions, which are cloned.



2.1.1.2 Password Lists

The Password List screen shows you the Passwords stored within the selected Password List. Not all Passwords may be visible to you here, as permissions can be applied to individual records within the Password Lists, as opposed to the whole Password List.

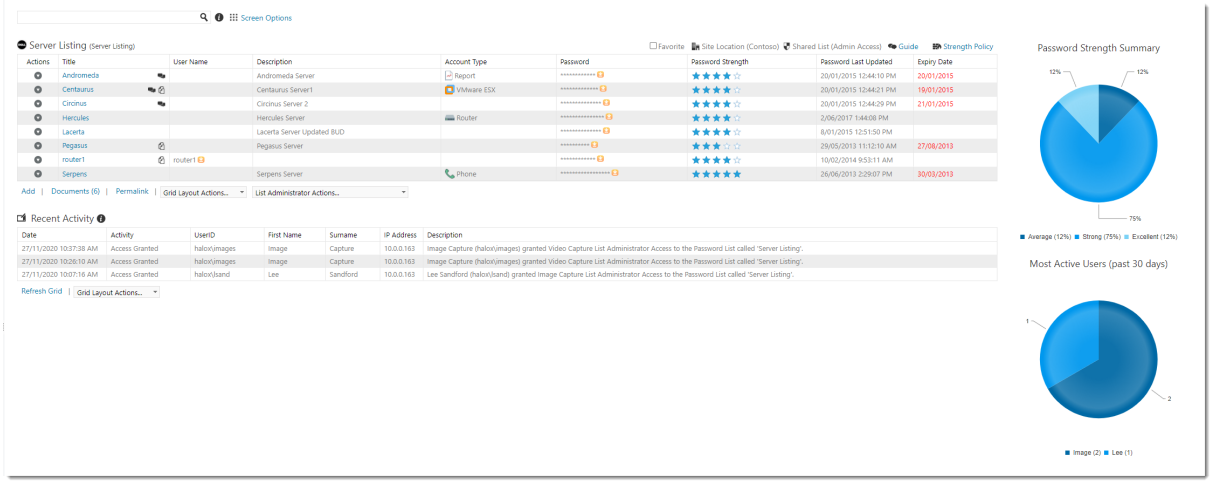
Note: Some of these features detailed below may be hidden or disabled for you, depending on your access rights, and what settings have been applied to the selected Password List.

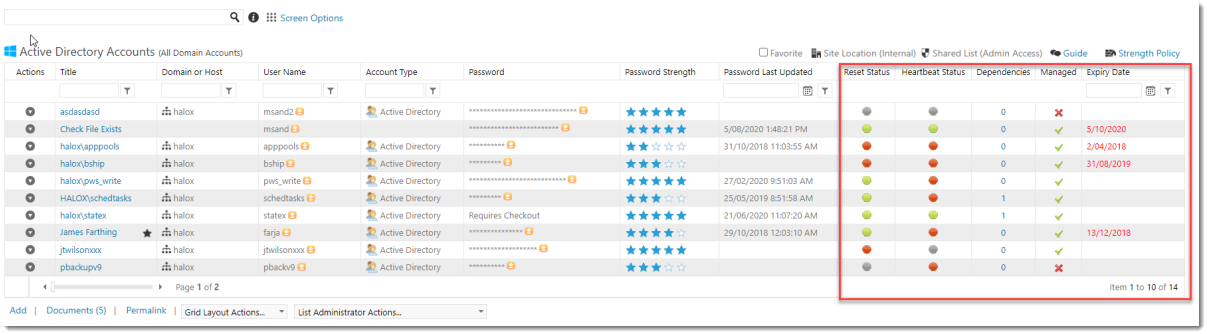
On this screen you can:

- Search for Passwords contained within the selected Password. Note: To perform an exact match search, enclose your search term in double quotes i.e. "root_admin"
- View various statistics about the selected Password List
- Customize the screen by clicking on the Screen Options button
- View what access you have to the Password List, and 'Guide' which has been added for the Password List, and also the specific Password Strength Policy settings which have been applied
- View Auditing data related to the Password List (Recent Activity)
- You can edit/view a password by clicking on the hyperlink in the **Title** column
- You can view a password on the screen by clicking the masked ******* (the speed at which the password is again hidden can be control by your Security Administrators)

- You can copy a password to the clipboard by clicking on the icon (if using Internet Explorer, the clipboard can be cleared after a set time, which is set by your Security Administrators)
- You can perform various Password Actions by selecting the appropriate menu option from the Actions drop-down menu
- Add Passwords, view Uploaded Documents, or Email Permalinks
- If you have Admin privileges to the Password List, there will also be multiple options available to you via the List Administrator Actions Actions drop-down list
- By clicking on one of the segments in the 'Password Strength Summary' pie chart, you can filter the results in the Passwords grid
- By clicking on one of the segments in the 'Most Active Users' pie chart, you can filter the results in the Recent Activity grid

The first screenshot below shows a standard Password List which is not configured to perform Password Resets on remote systems. The second screenshot below shows a Password List configured for this, and shows the additional columns you would expect to see.





2.1.1.2.1 Screen Options

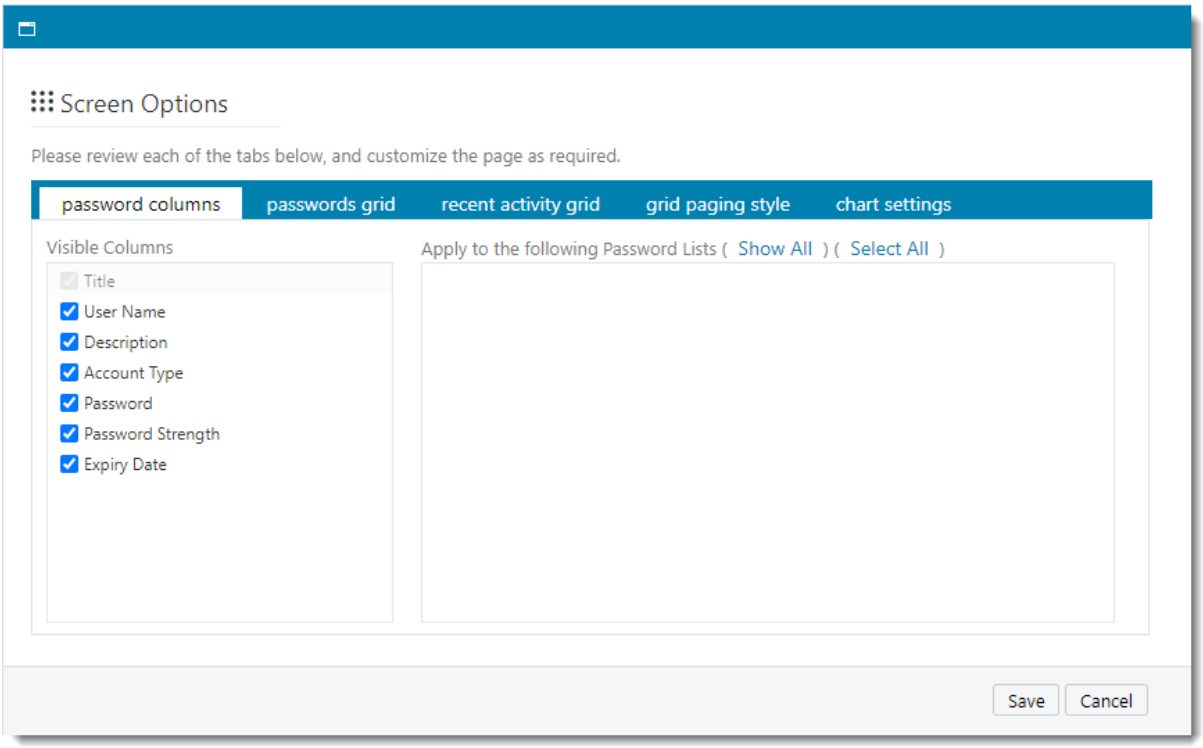
Screen Options allows you to specify various settings for how you would like to see the grids and charts displayed on the screen.

Please note that some of these settings may be set by your Security Administrator(s) of Passwordstate, and if so the controls will be disabled. You will see an icon like , and message telling you if this is the case.

Password Columns Tab

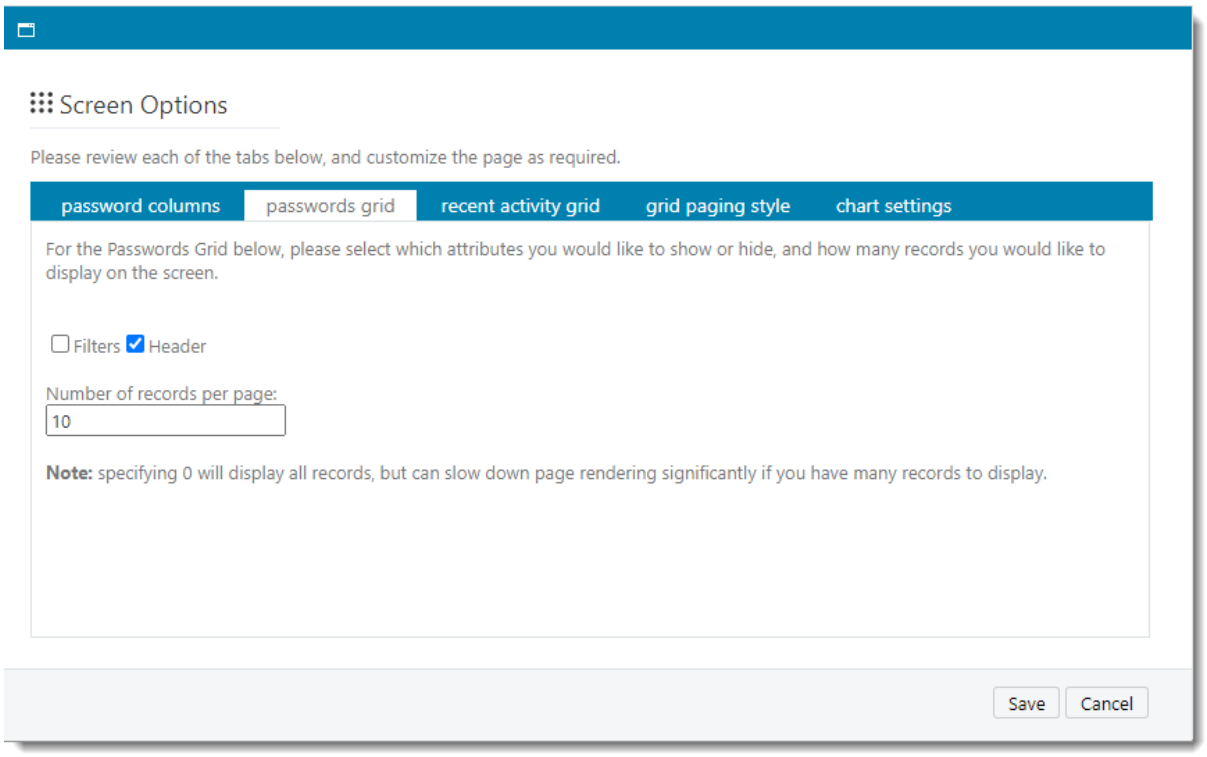
The Password Columns tab allows you to choose which columns are visible in the Passwords grid.

Once you've chosen the columns you want visible, simply click the 'Save' button. If you also want to apply the same 'view' to other Password Lists, click on the 'Show All Button', select the Lists you want to apply the view to, then click on the Save button. **Note**: Each Password List can be configured to use different columns, so some columns may or may not show for other selected Password Lists.



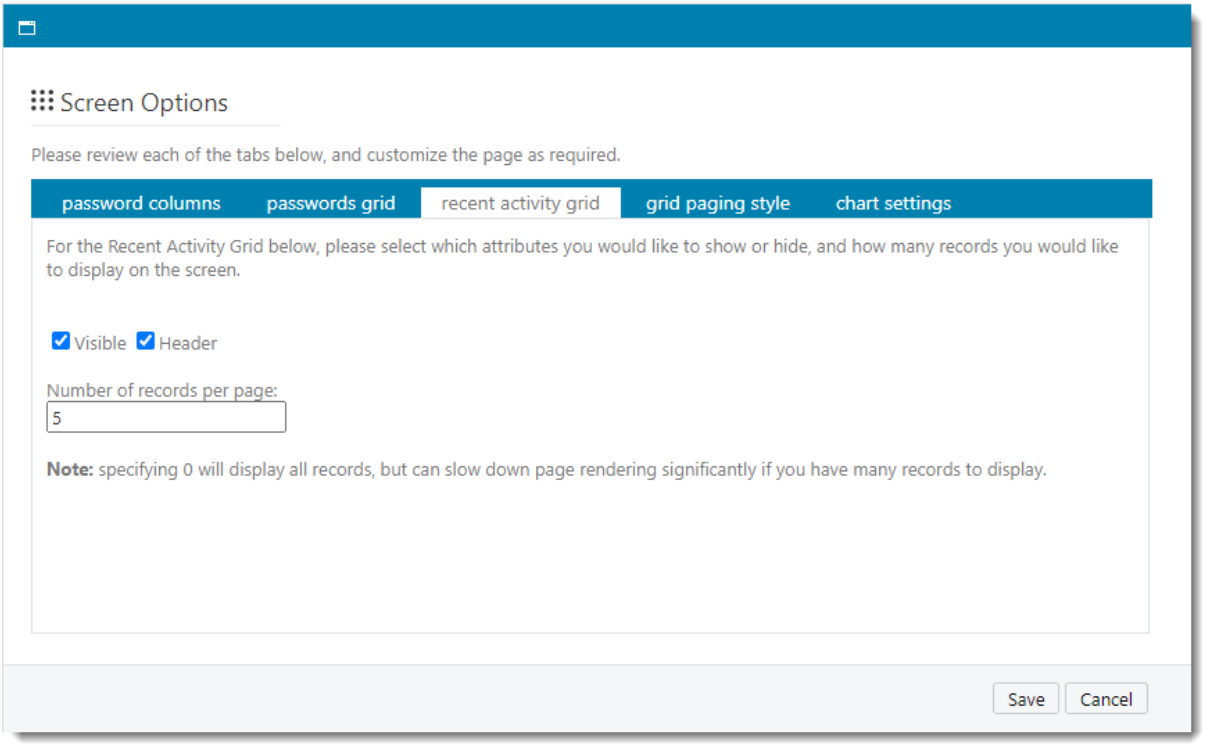
Passwords Grid Tab

The Passwords Grid tab allows you to show or hide the Header and Filters feature for the Passwords grid, as well as specify the number or records to display in the grid.



Recent Activity Tab

The Recent Activity tab allows you to show or hide the Recent Activity grid (auditing data), as well as the grids header, and how many records you would like to be displayed in the grid.



Grid Paging Style Tab

The Grid Paging Style tab allows you to choose one of three different types of 'Paging' styles, which will be used when there are more records returned than the Password grid is set to display.

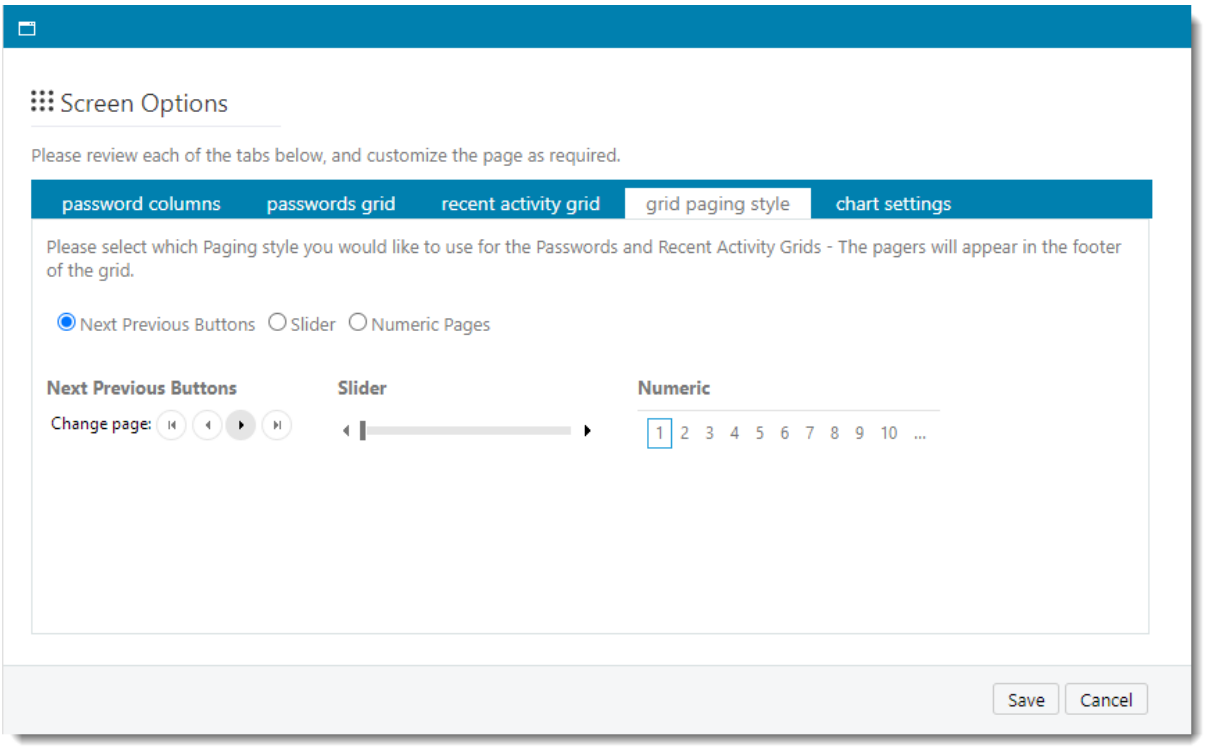
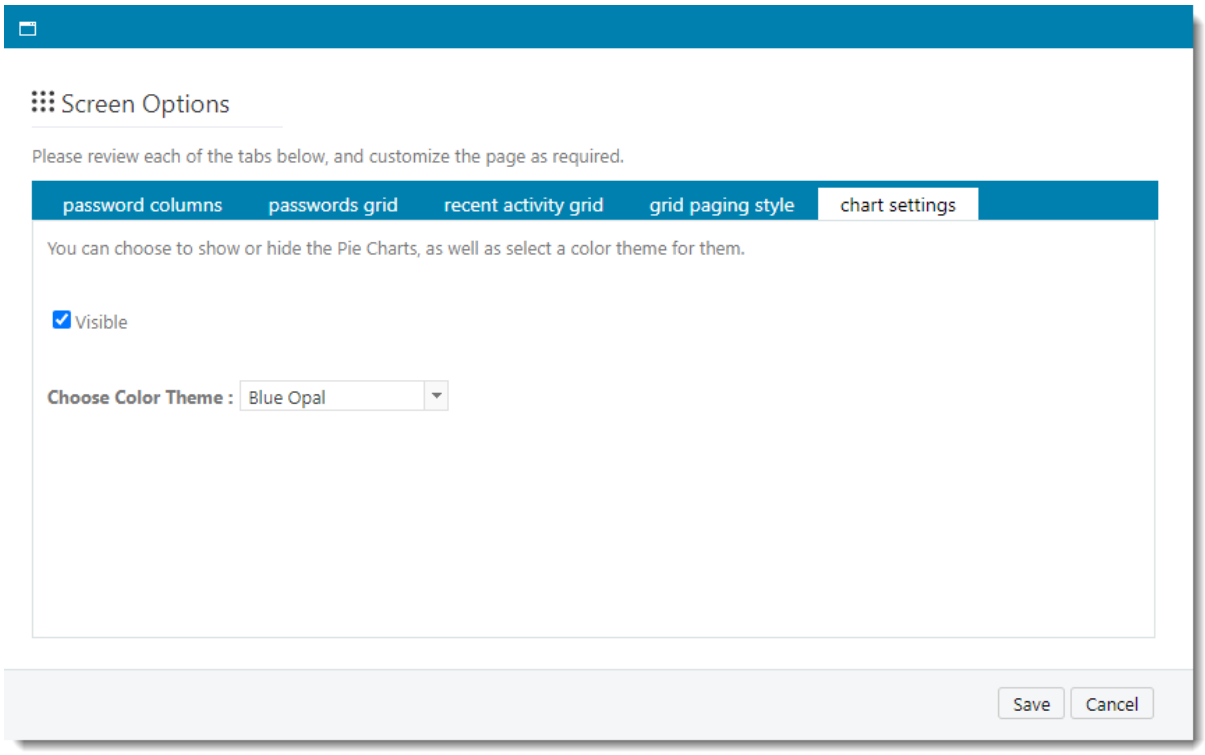


Chart Settings Tab

The Chart Settings tab allows you to either hide or show the Password Strength Summary and Most Active Users pie charts on the right-hand side of the screen. You can also choose the color scheme for the pie charts.



2.1.1.2.2 Add Password

The Add Password screen allows you to add a new Password record to the selected Password List.

When adding a new password record, the fields visible on the screen can be different for each Password List, as each Password List can be configured to use different fields. There are a total of 9 fixed fields which can be used, and 10 Generic Fields which can take on different field types.

Password Details Tab

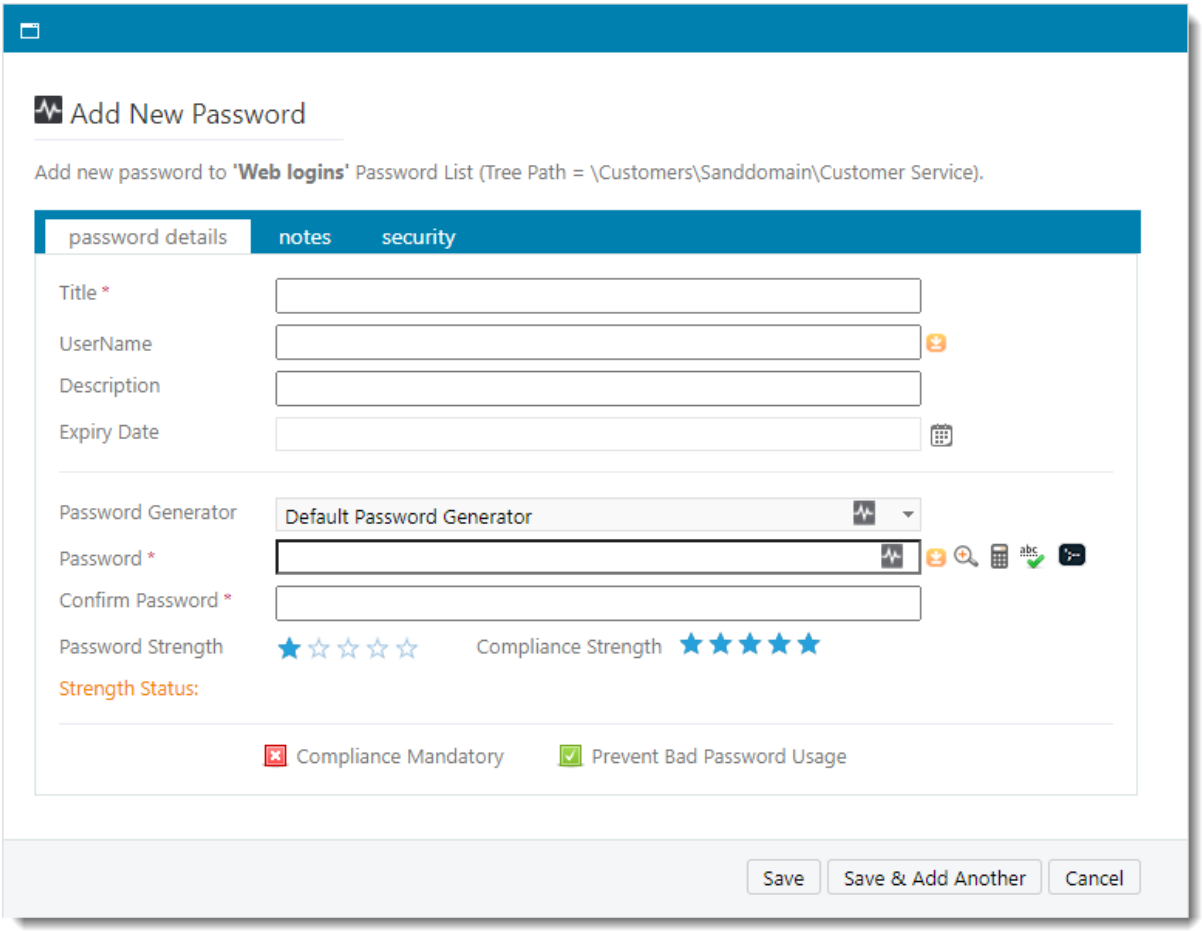
The Password Details tab is where you specify the values for the majority of fields associated with the selected Password List, and each field can be configured of different types i.e. URL, Text, Date, Radio Buttons, etc.

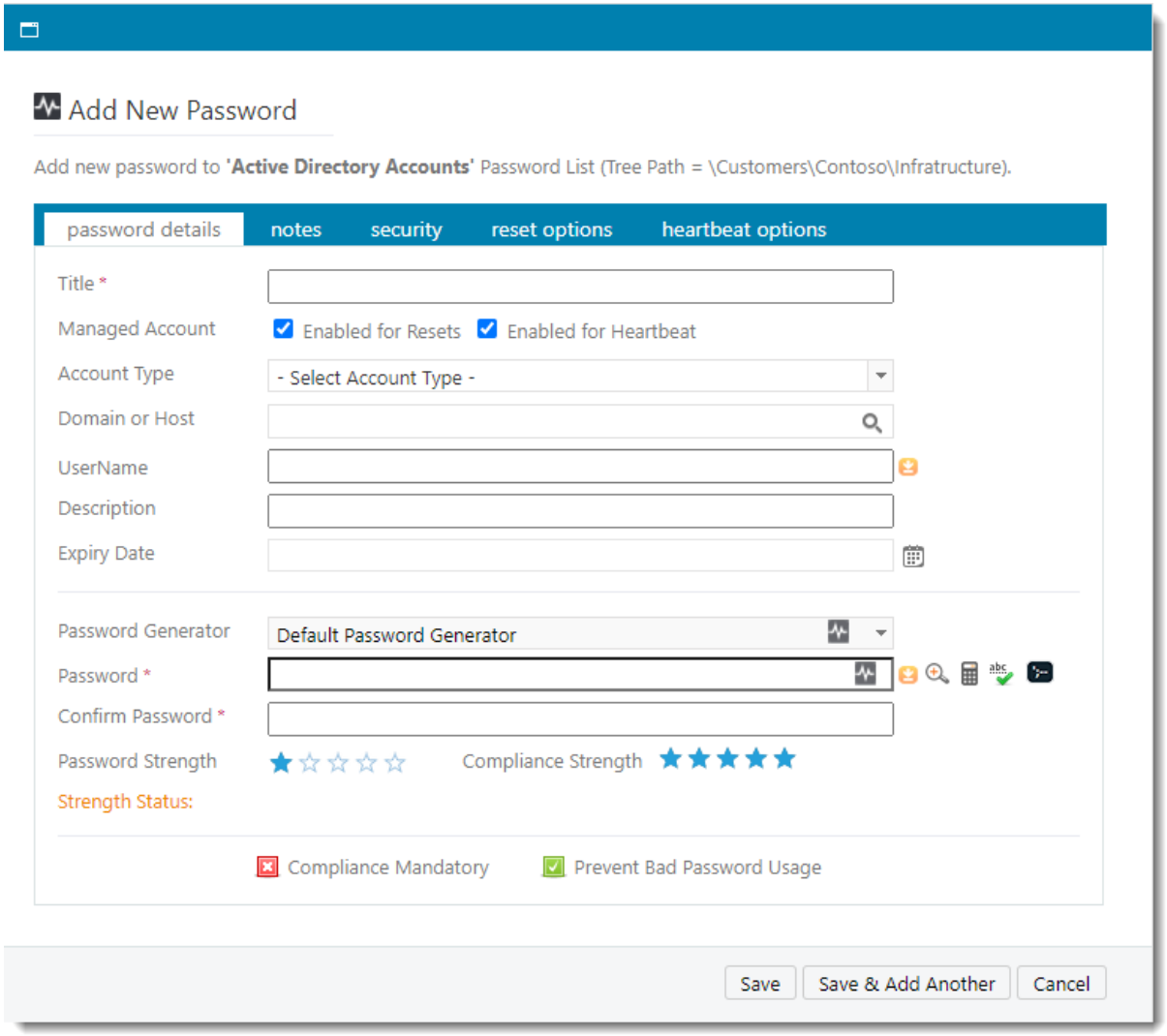
A few things to note on this tab is:

- Any fields which are denoted with * are mandatory fields, and you must specify a value for them
- The Password Strength indicators and text at the bottom of the screen only apply to the 'password' field - they do not apply to any Generic Fields which may be configure of type Password
- You can choose to prevent exporting of this Password record if required
- You can choose to generate a new random password by clicking on the icon, copy the password to the clipboard by clicking on the , or show the password on the screen by clicking on the icon

- The policy set for the selected Password List may also place certain restrictions to the Password record, like a certain Password Strength must bet met before the record can be saved, or that passwords deemed as 'Bad' cannot be used. You will need to refer to one of the Administrators of the Password List to understand what settings and restrictions have been applied
- The Spell Check type icon shows a popup window which spells out the password in the format of 'PAPA alpha sierra sierra whiskey oscar romeo delta'

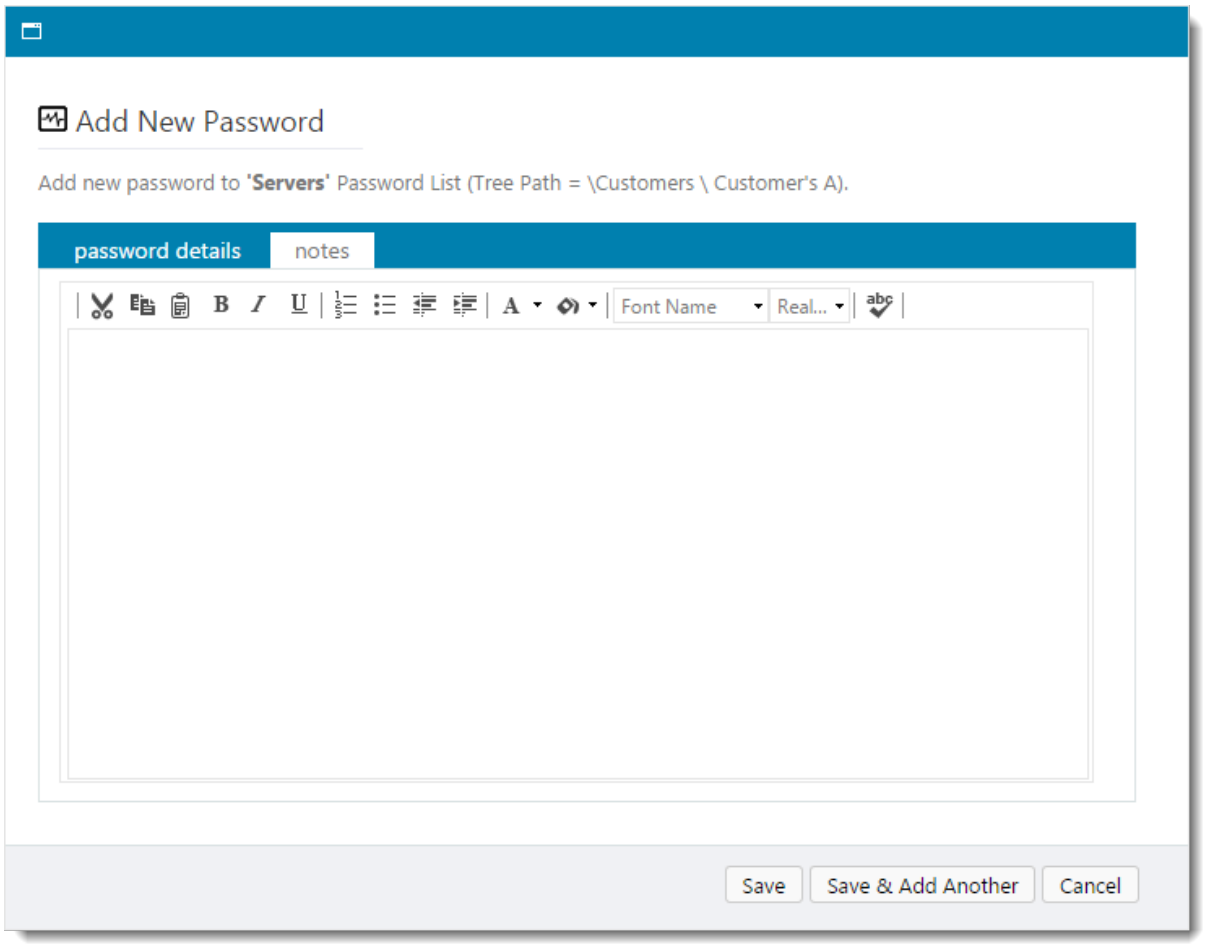
The Add Password screen will also look different, depending on whether it's Password List is configured for Password Resets or not. In the two screenshots below, the first is from a Password List which is not configured to allow Password Resets on remote systems, and the second screenshot is from a Password List configured to allow this.





Notes Tab

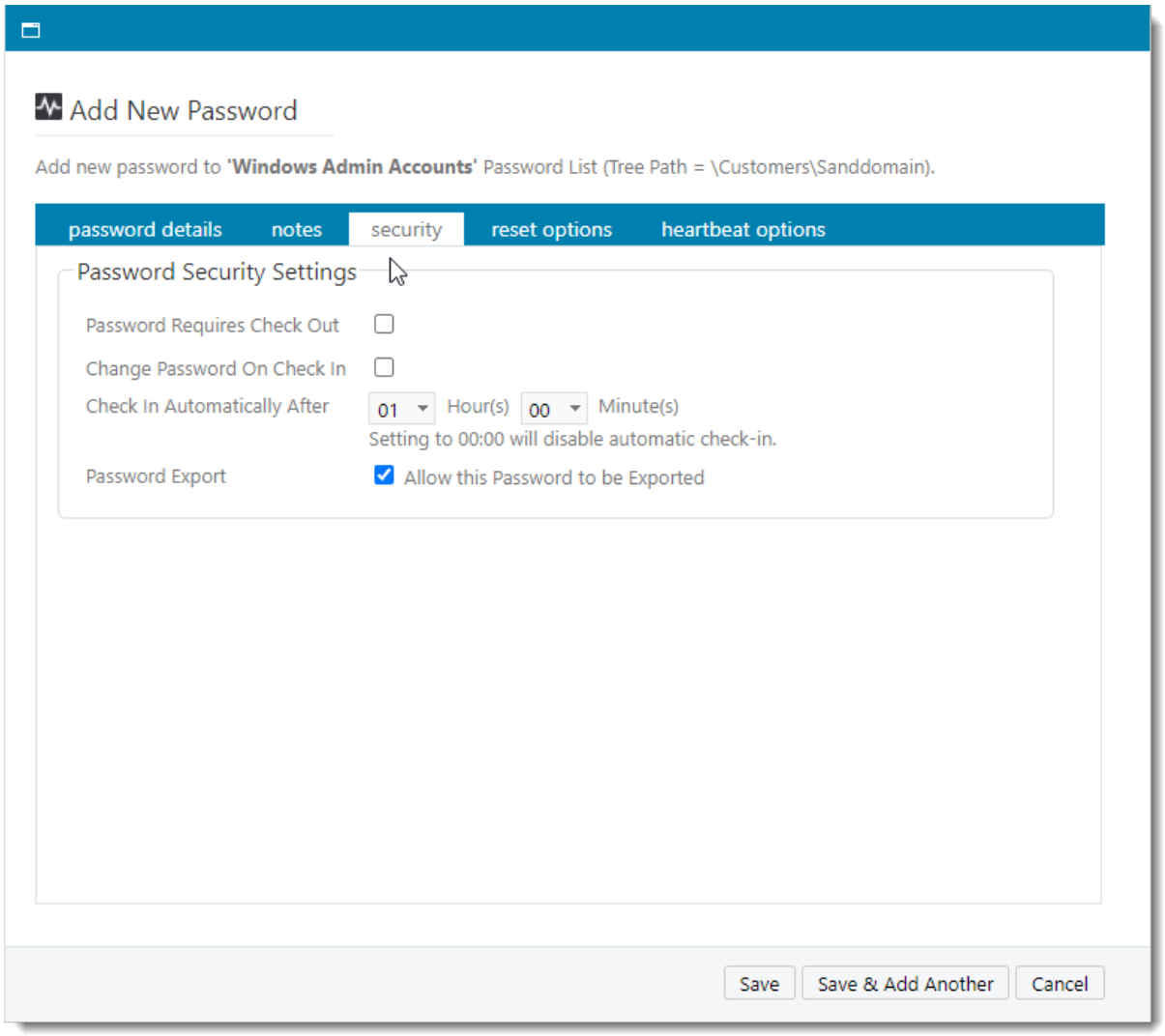
The Notes tab allows you to specify longer verbose text to explain what the record is for, and also allows basic HTML formatting.



Security Tab

Using the Security Tab, you can also require the password record be exclusively check-out to a user so they can access it - when check-out, no other users can access the record. There are options to perform a password reset on check-in as well, and also a timer for when the password should be automatically checked in if the user forgets to manually check the record in.

If needed, Security Administrators can also check the password back in manually. Manual check ins can be done from the 'Actions' menu for the password record.



Reset Options and Heartbeat Options Tabs

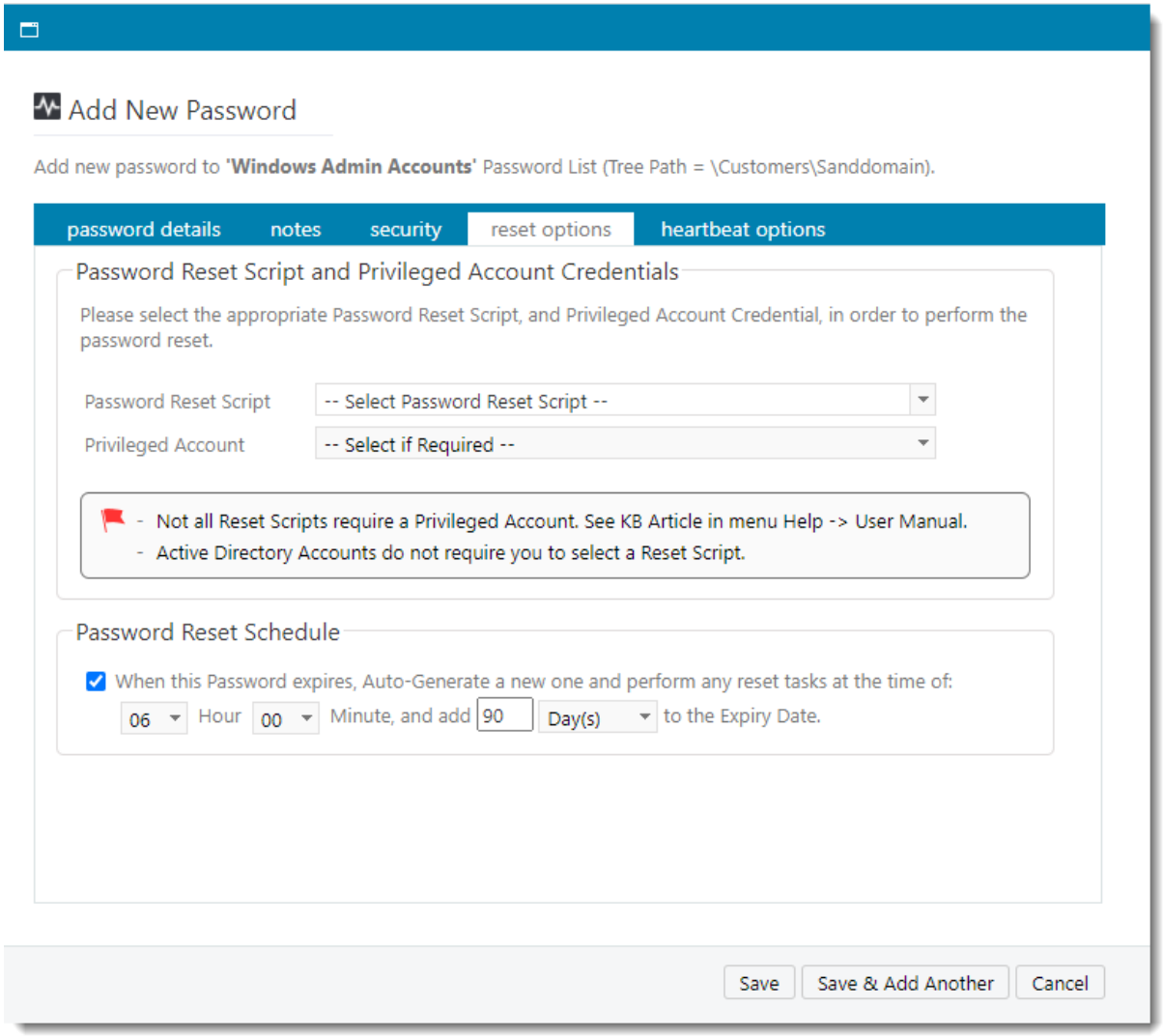
The Reset Options and Heartbeat options tabs **will only be visible** if the password record has been configured to perform password resets. For a complete example of how to configure a password for resets, please reference the Privileged Account Management manual under the Help menu in Passwordstate.

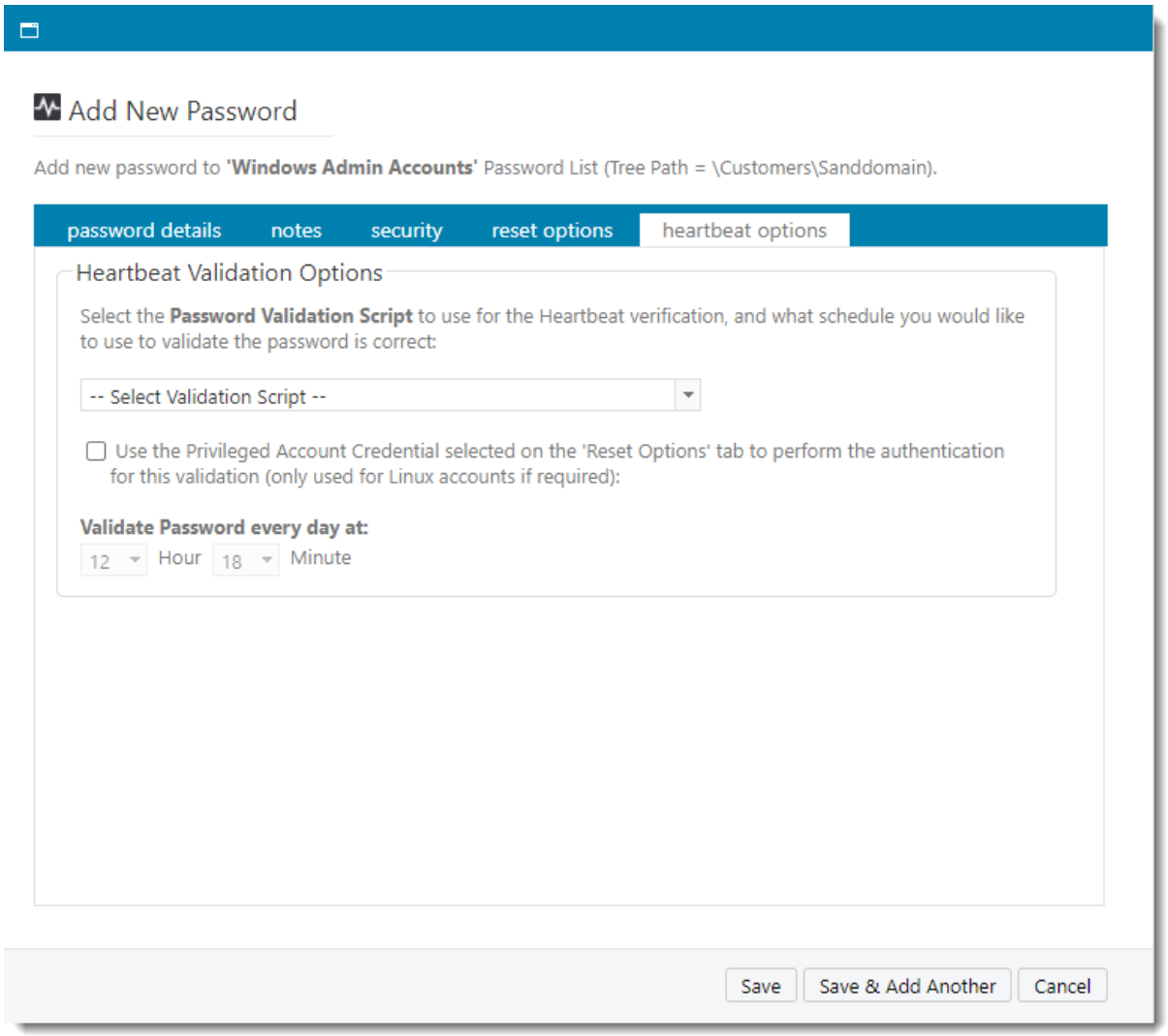
Options available are:

- The Password Reset Script to be used for this account
- The Privileged Account Credential to associate with the record so a Password Reset can occur - not all Reset Scripts require this, so please reference the Privileged Account Management manual under the Help menu in Passwordstate
- Whether or not to auto-generate a new password for the record
- At what time of the day should the password be reset, once the Expiry Date has been reached

- How many days should be added to the Expiry Date field, once the password has been automatically reset
- And what Validation Script and schedule to use for the Heartbeat process

The Administrators of the Password List can also set the default options for all password records at the Password List level. Once set, new password records will inherit the settings, but can be changed in individual records at any time, or by bulk using the Bulk Update Password Reset Options feature





Validating Linux Root Account Passwords

By default, most Linux Operating Systems do not allow you to SSH in using the root account – for security reasons.

Because of this restriction, on the 'Heartbeat Options' tab for password record, we have an option you can select to SSH in with the Privileged Account Credential that is selected for the record, and then validate the password for the root account.

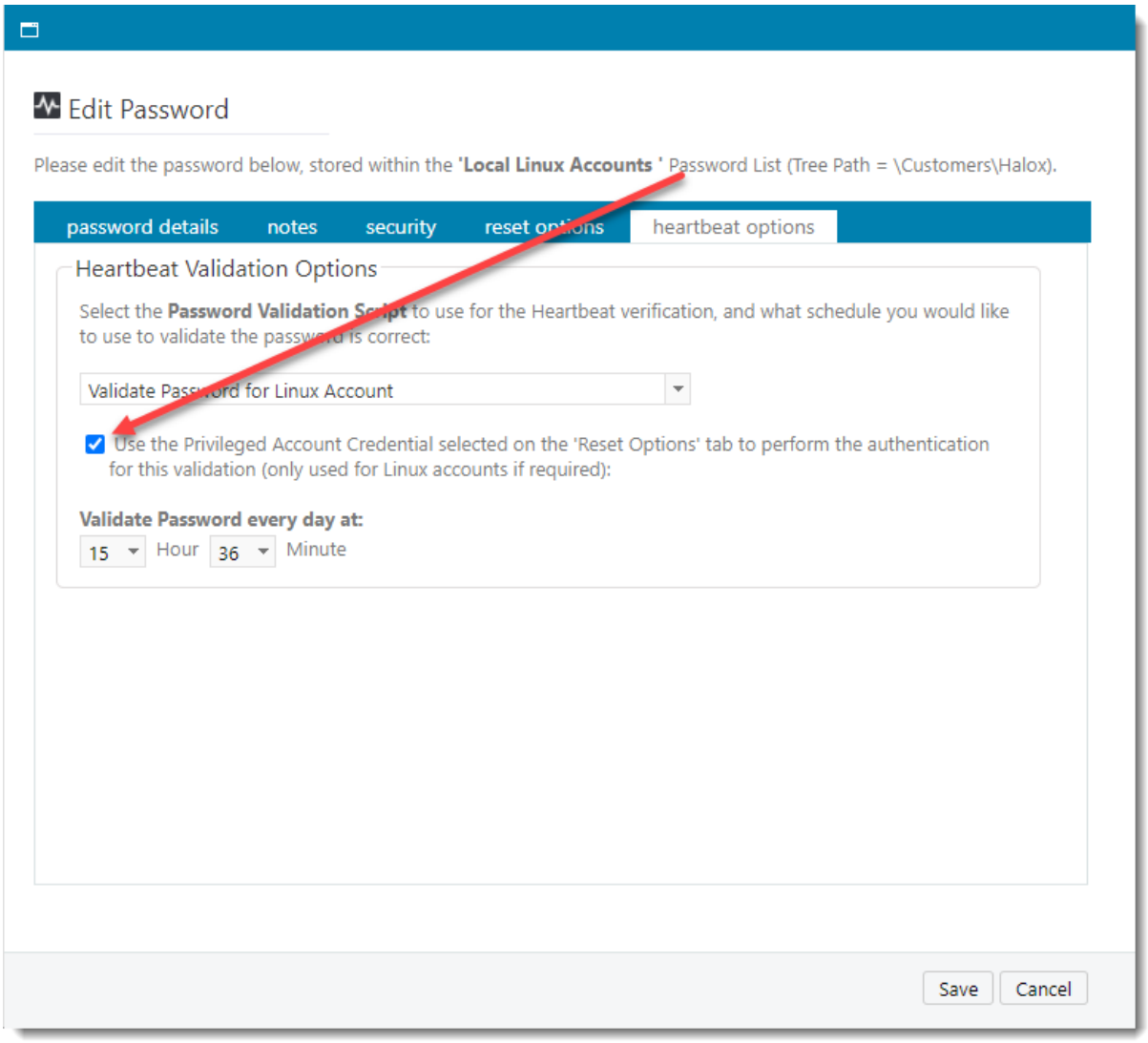
In order for this functionality to work, changes are required to each of the Sudoers file on your Linux desktops/servers. Below are the changes required:

- Open the Sudoers file with visudo using the following command:

  Sudo visudo -f /etc/sudoers

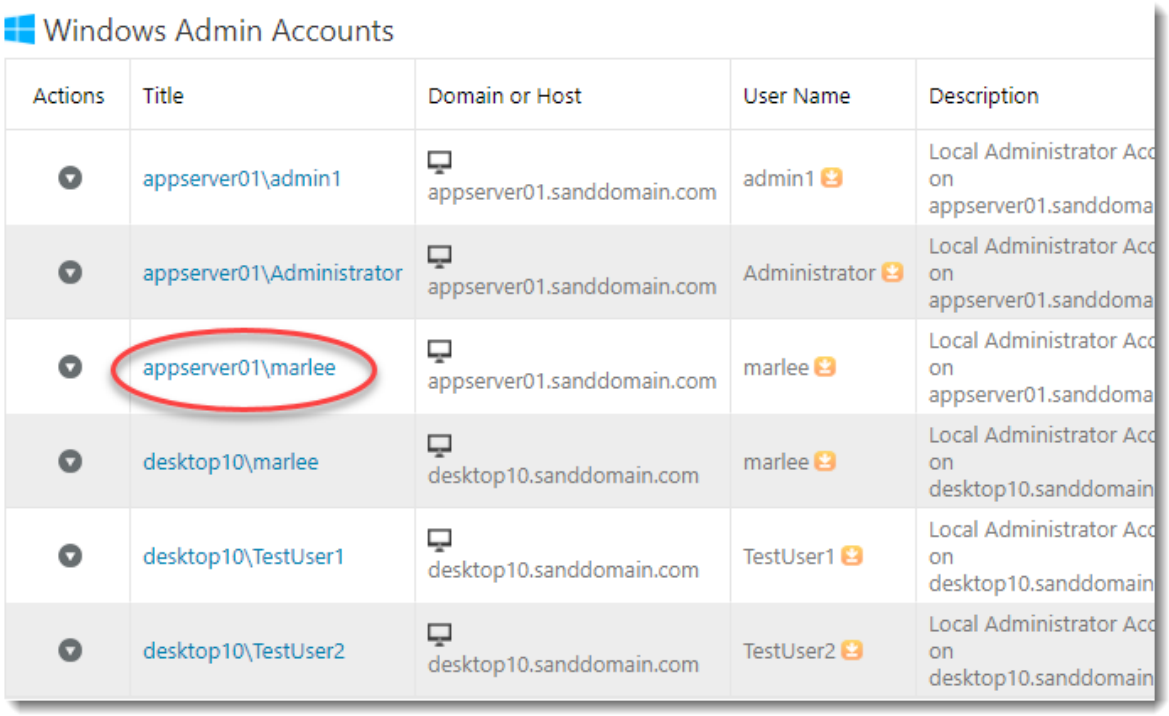
- When editing the Sudoers file, scroll to the bottom and add the following two lines, entering in the appropriate username you use in Passwordstate as your Privileged Account:

  ## Enable sudo rootpw for Passwordstate Privileged Account
  Defaults:<username> rootpw



2.1.1.2.3 Edit Password

Editing a Password is possible by clicking on the Title field hyperlink you see in the grids as per the below screenshot.

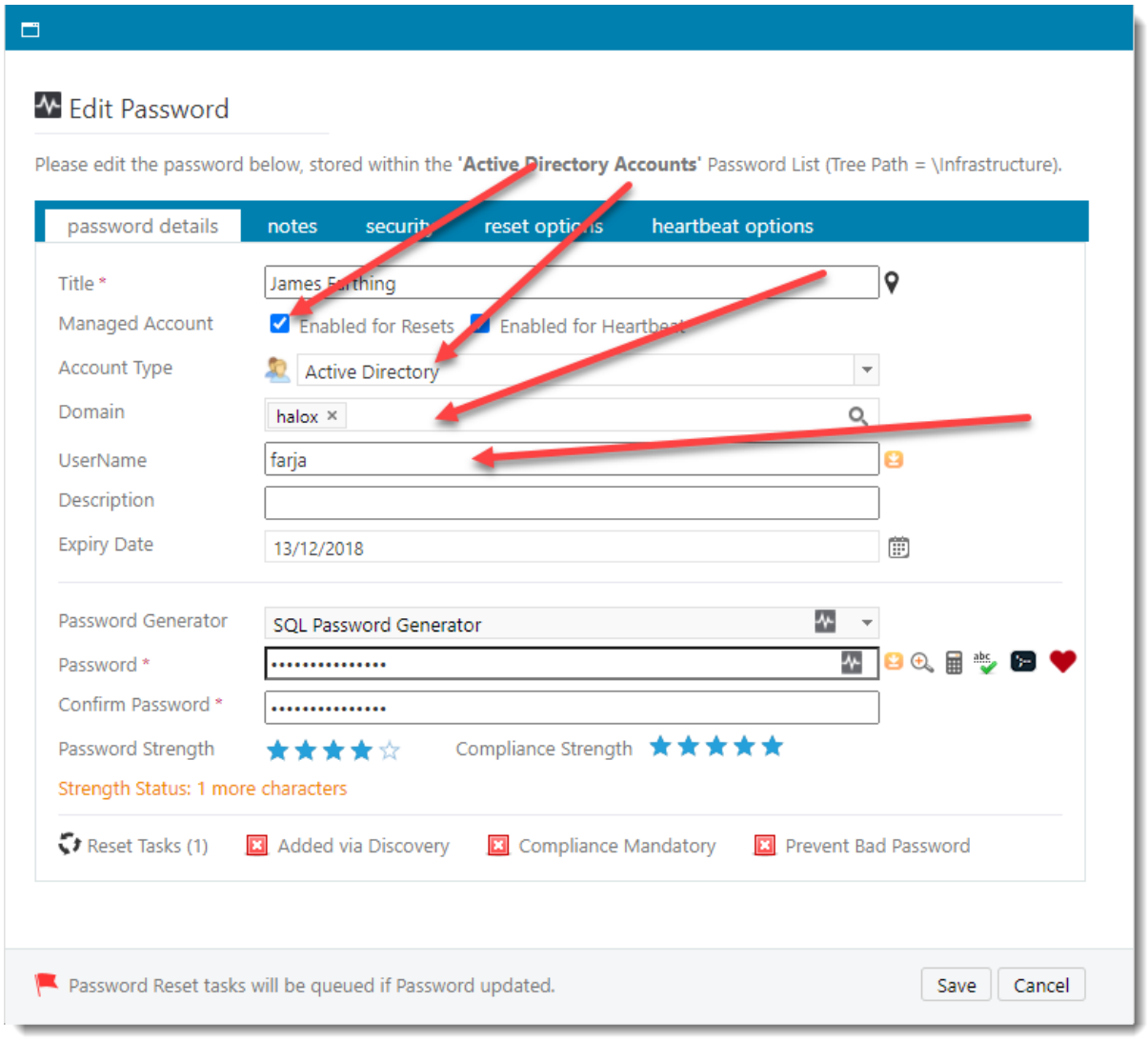


Once the Edit Password screen is open, each of the fields and options on the Tabs is similar to the Add Password screen.

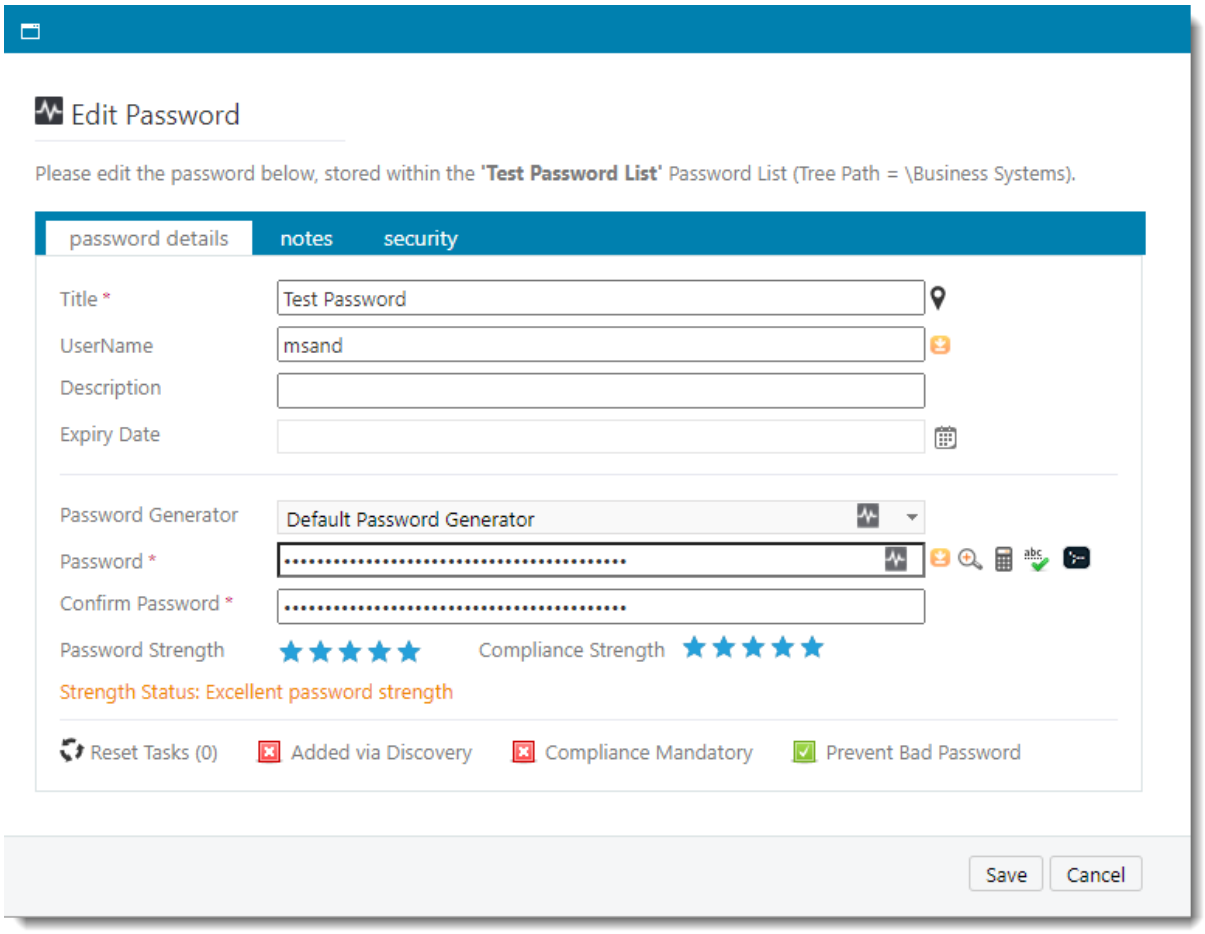
Password Details tab

The fields available on the Password Details tab will look different, depending on what fields you have selected for a Password List, and also if the Password List is configured to allow Password Resets to occur. Below is a screenshot of an Active Directory account, which is configured to perform password resets.

Note: Please refer to the Privileged Account Management manual under the Help menu in Passwordstate

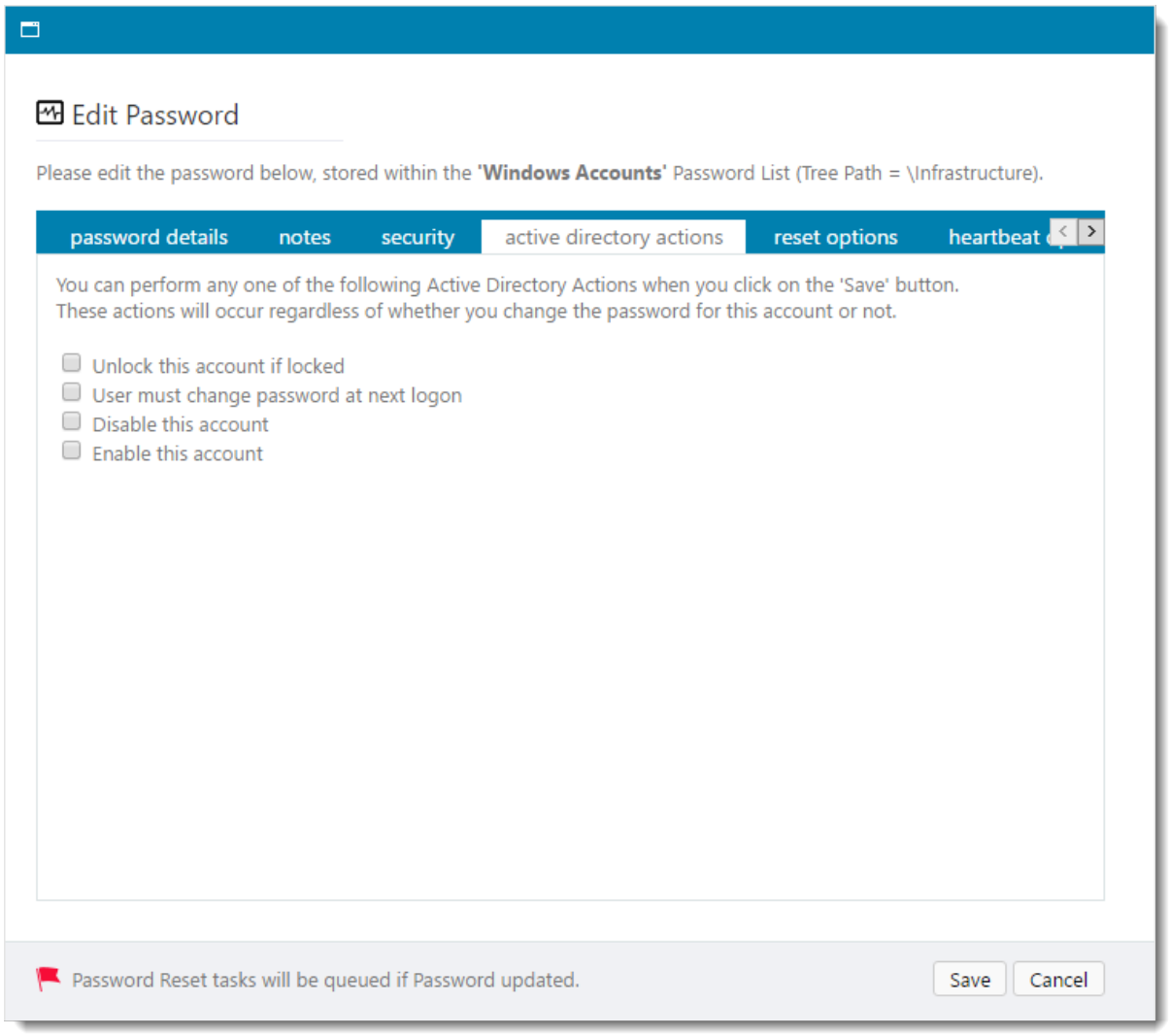


If the Password List is not configured for Password Resets, then the Password Details tab would look similar to the screenshot below.



Active Directory Actions tab

If the Password List has the option to show Active Directory Actions, then you can perform various AD functionality as well, as per the options in the screenshot below.



Reset Options and Heartbeat Options Tabs

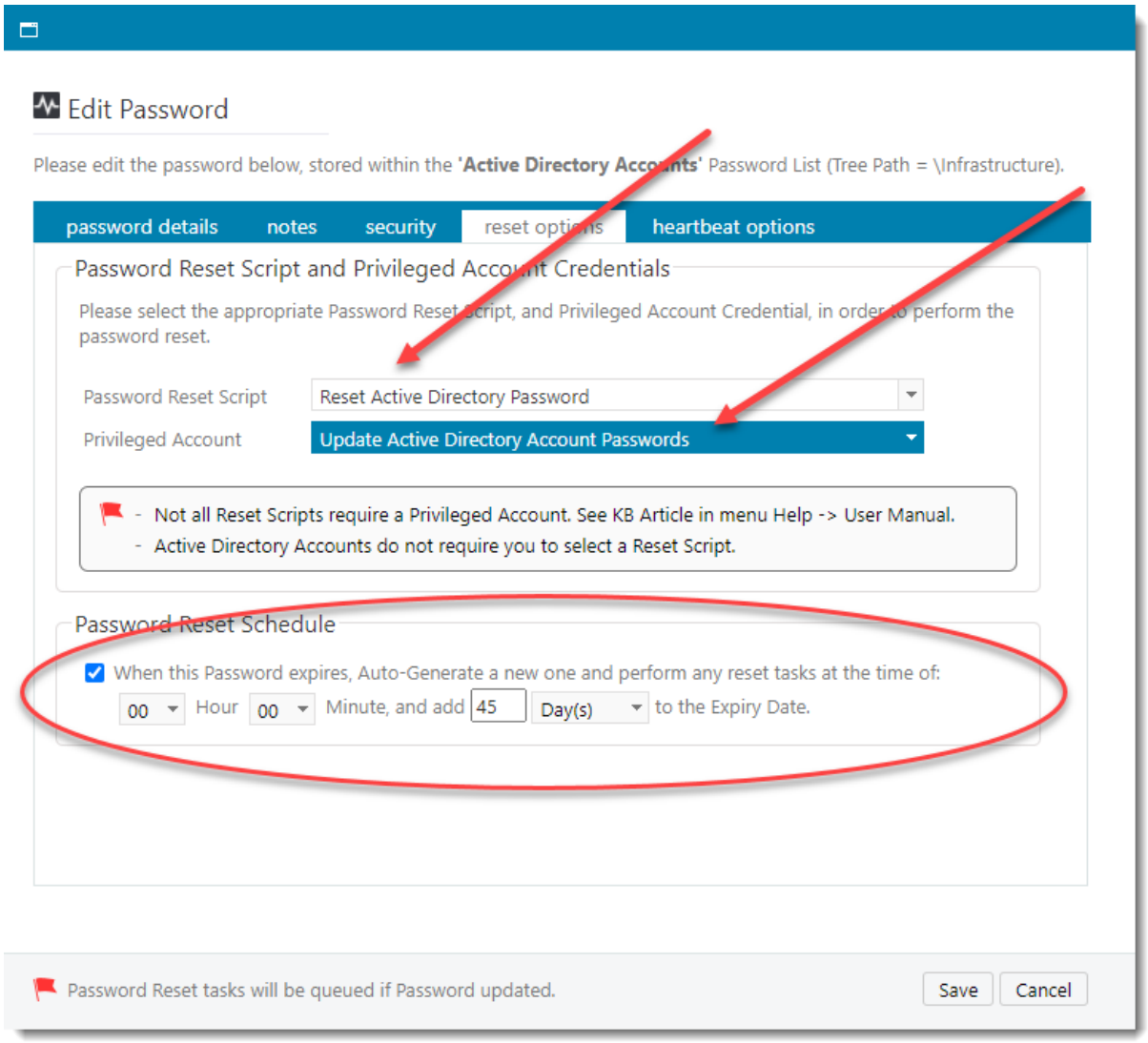
The Reset Options and Heartbeat options tabs **will only be visible** if the password record has been configured to perform password resets. For a complete example of how to configure a password for resets, please reference the Privileged Account Management manual under the Help menu in Passwordstate

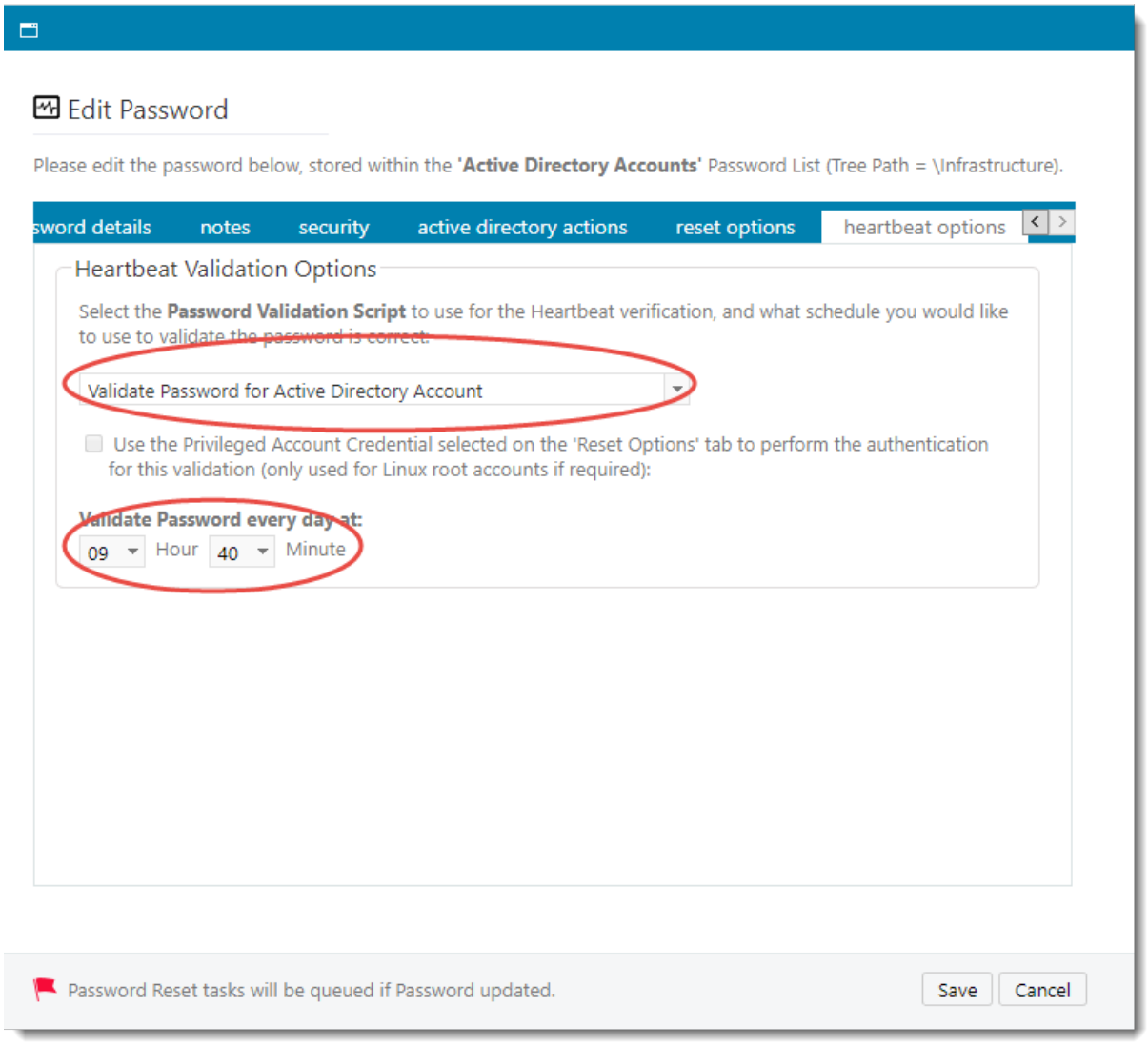
Options available are:

- The Privileged Account Credential to associate with the record so a Password Reset can occur - not all Reset Scripts require this, so please reference the Privileged Account Management manual under the Help menu in Passwordstate
- Whether or not to auto-generate a new password for the record
- At what time of the day should the password be reset, once the Expiry Date has been reached
- How many days should be added to the Expiry Date field, once the password has been automatically reset

- And what Validation Script and schedule to use for the Heartbeat process

The Administrators of the Password List can also set the default options for all password records at the Password List level. Once set, new password records will inherit the settings, but can be changed in individual records at any time, or by bulk using the Bulk Update Password Reset Options feature



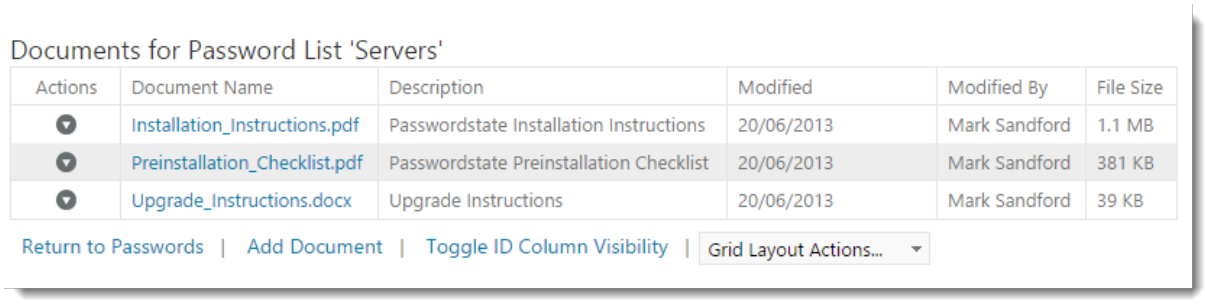


2.1.1.2.4 Upload Documents

It is possible to upload one or more document/attachments to Passwordstate, and associate them with either the Password List itself, or individual Password records. Uploaded documents are also encrypted within the database, using the same type of 256bit AES encryption as other encrypted data.

On the 'Documents' screen for Password List, the following is possible:

- Adding a new document
- Retrieving a document from the database by clicking on the 'Document Name' hyperlink
- You can edit some basic properties for the document
- Add also delete the document if required. Note, deleting a document does not place it in any recycle bin.

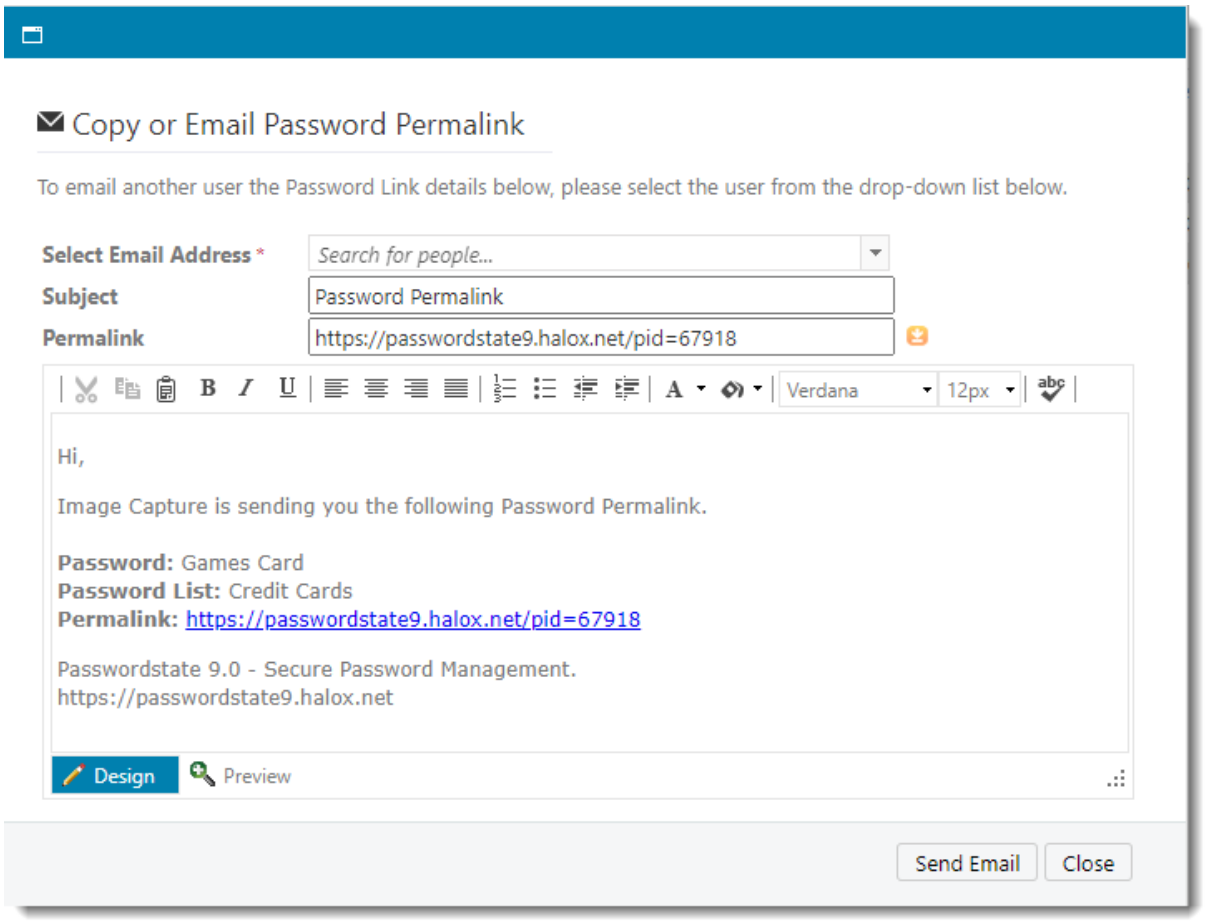


2.1.1.2.5 Email Permalinks

Passwordstate supports the concept of 'Permalinks' for Password Lists, or individual Password records.

A Permalink is a shortened URL which can be copied to the clipboard, or email to other users, and allows easy access to a resource by simply clicking on the provided URL.

Note: If you provide a Permalink to another user who does not have access to the Password List, they will be redirected to another screen where they can request access. All requests for access will be sent to the Administrators of the Password List.



2.1.1.2.6 Password Actions

Every Password added to a Password List has certain functions, or 'Actions', which can be performed for the record. Below is a table summarizing each of the Actions, and more detail can be found by clicking on each of the hyperlinks.

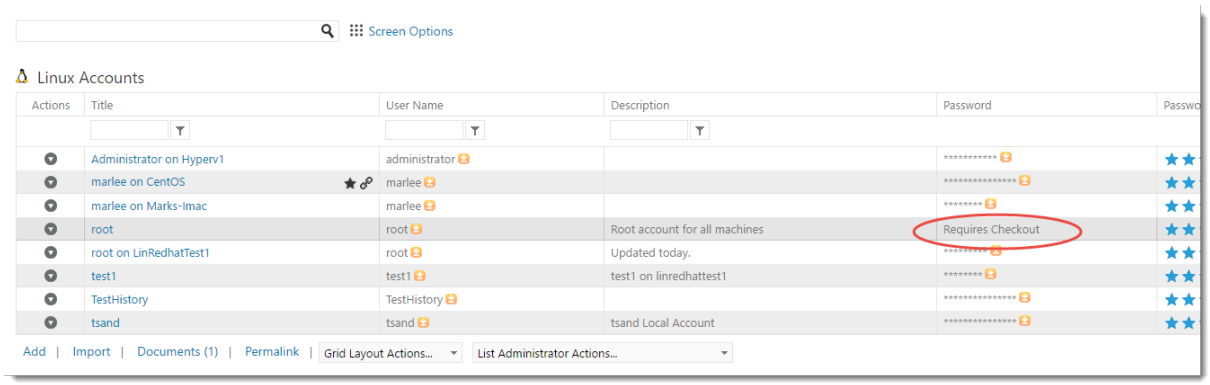
Check-In Password	Allows a user to check a record back in, after they have checked it out for exclusive use
Copy or Email Password Permalink	Similar to Permalinks for Password Lists, you can also copy or email Permalinks for individual Password records
Copy or Move to Different Password List	It's also possible to copy or move individual Password records between Password Lists, and it's even possible to link them - so all changes are synchronized between Password Lists
Delete	When you delete an individual Password record, it is moved to the Recycle Bin for the Password List. Administrators of the Password List can restore back from the Recycle Bin if required
Expire Password Now	Selecting 'Expire Password Now' for an individual Password record, will set it's Expiry Date field to the current date, and trigger any associated Password Reset tasks as well
Filter Recent Activity on this Record	If you need a quick method of filtering the audit data (Recent Activity) for an individual Password record, you can use the 'Filter Recent Activity on this Record' menu option
Link Account to Multiple Web Site URLs	If using our Chrome or Browser extensions, and you use the same account to login to multiple different web sites (normally internal sites), then you can use this feature to achieve that.
Remote Session Launcher with these Credentials	This menu will be available if the record is a local account for a Host record, and you have been give access to use the Remote Session Launcher feature
Send Account Heartbeat Request	If the password record has the option enabled to perform account Heartbeats, to validate the password is correct against the remote Host or Active Directory, then you can use this menu option to perform the validation real-time.
Send Self Destruct Message	This menu option allows you to send a Self Destruct Message, with the contents being details for the selected Password record.
Toggle Favorite Status	If you have Password records which you use frequently, you can tag them as your favorites and they will show up

	in the 'Favorite Passwords' grids on the Password Home page, or any of the Password Folder pages. A Favorite password is also denoted by the ★ icon on the Passwords grid
View & Compare History of Changes	Every change made to a Password record retains a history of the change. By clicking on 'View & Compare History of Changes' you can visually compare what has changed, at what time, and by who.
View Documents	You can upload one or more documents/attachments and associate them with individual Password records
View Individual Password Permissions	Instead of applying permissions to an entire Password List for users, you can choose to apply permissions just to individual Password records if required. When the user browsers to the Password List, they won't see all the records, just the individual ones they've been given access to
View Linked Passwords	If the password record is linked to another password in a different Password List, then this menu option will show. It allows you to view what other Password Lists this record is linked to
View Password Reset Dependencies	Shows any password reset dependencies which are linked to the selected Password record. Typically these would be Windows Services, IIS Application Pools and Scheduled Tasks.
Unlink & Delete Password	Allows you to unlink and delete a linked password record - it will be moved to the recycle bin
Unlink Password	Allows you to unlink a linked password record

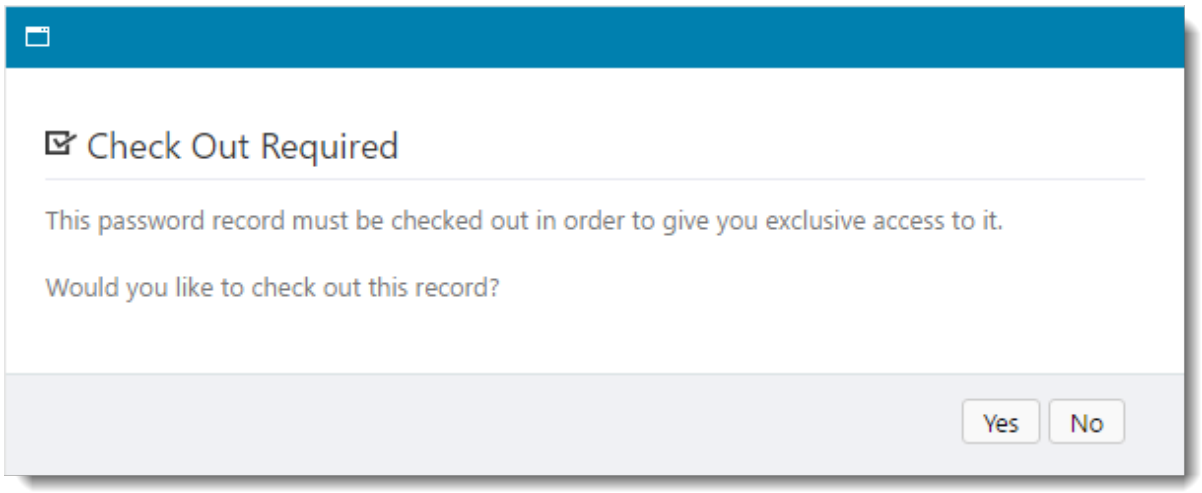
2.1.1.2.6.1 Check-In Password

When a password is configure to require exclusive access via the Check-In/Check-Out process, and menu item called 'Check-In Password' will be visible when the password is checked out. This menu item will only be available to the user who checked the record out.

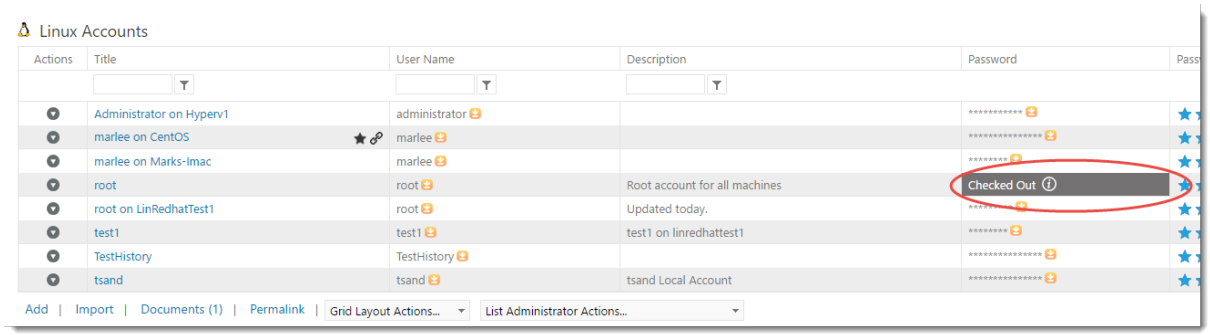
When a password is required to be checked out, it hides the value of the password, and instead indicates a check out is required.



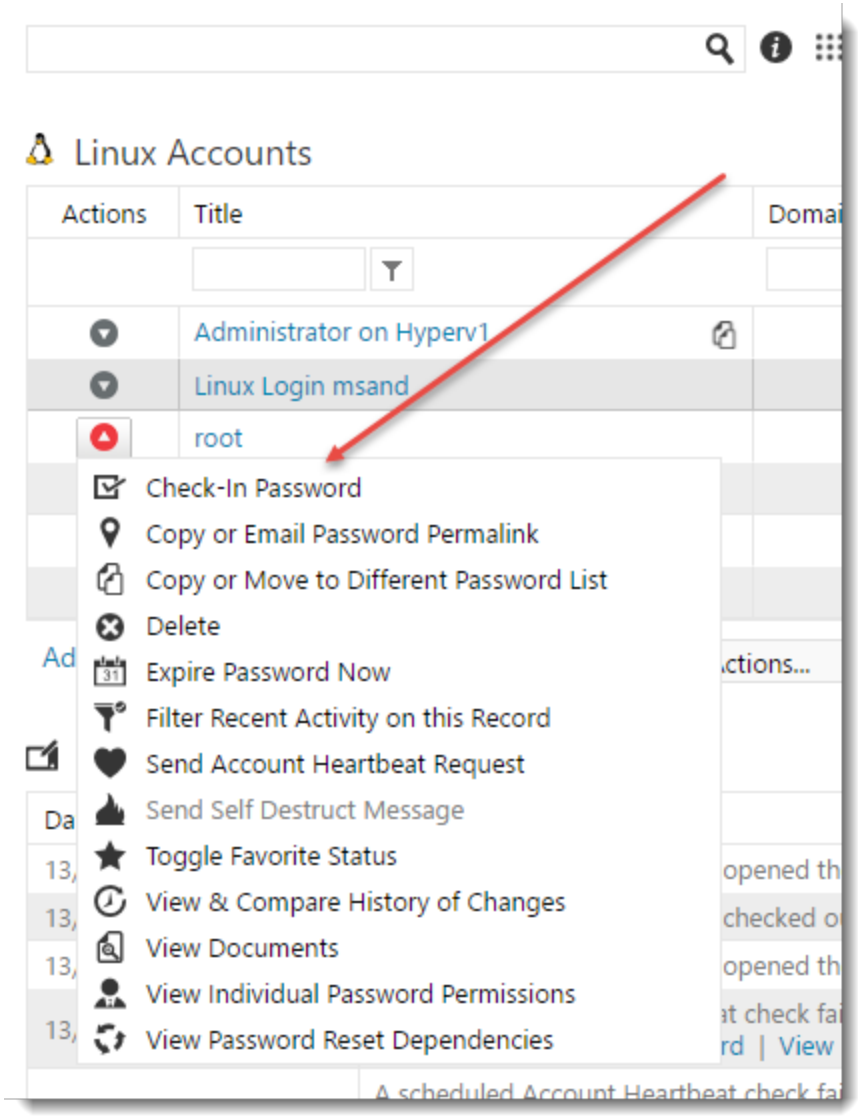
When you click on the Title for the record to access it, you will be asked to check the record out.



When checked out, it also indicates this in the password grid, and no other users can access the password until it is checked back in.



And the user who checked the record out, can check it back in via the Action menu.



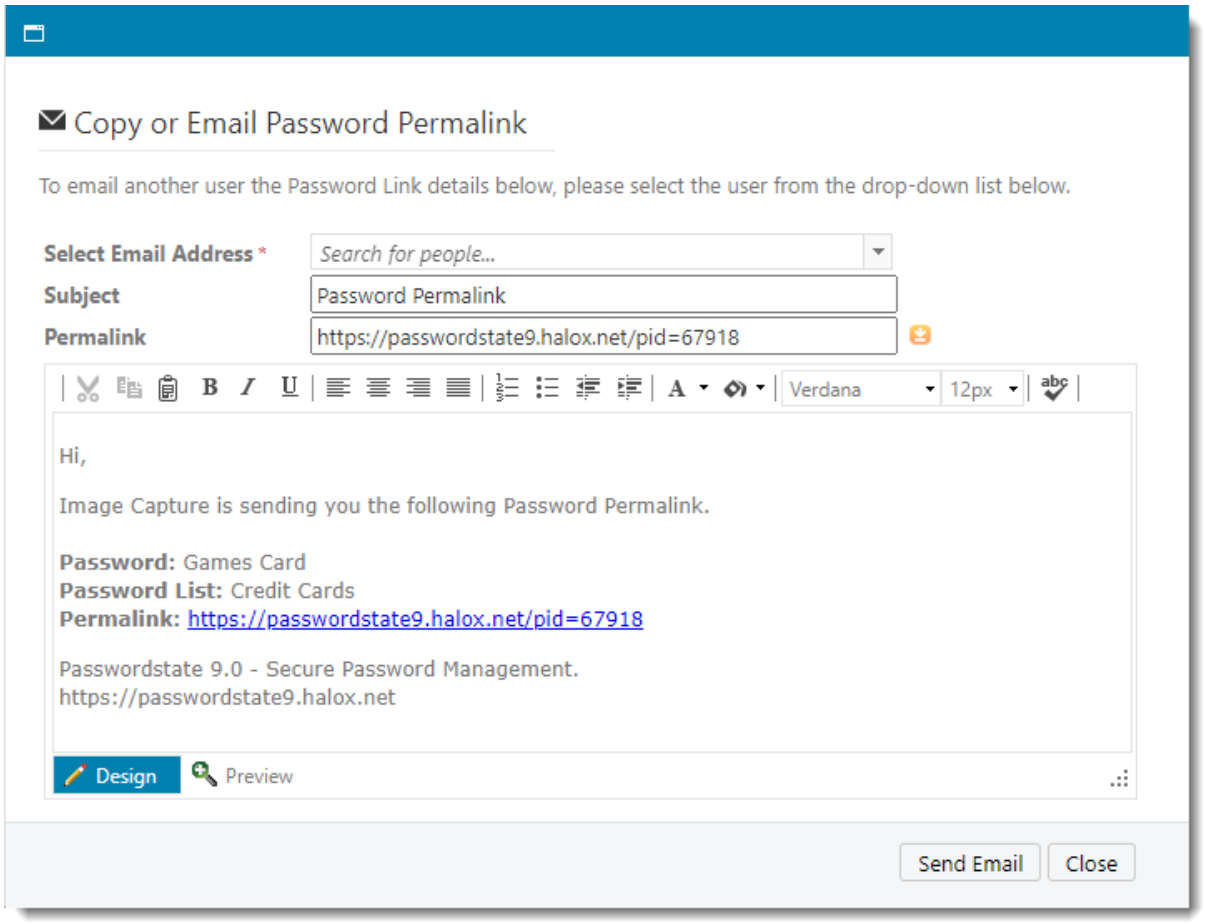
Security Administrator Checking Back in Password record
If the user who checked a record out is unavailable to check a record back in, Security Administrators can also check the record back in for the user.

The Security Administrator needs to go to the screen Administration -> User Accounts, and "Impersonate" the user who has the record checked out - they can access the 'Impersonate User Account' from the Actions drop down menu, for the appropriate user.

2.1.1.2.6.2 Copy or Email Password Permalink

Similar to a Permalink for Password List, you can also copy a Password record's Permalink to the clipboard, or email it to another user.

As with Permalinks for Password Lists, if a user navigates to a Password record via the use of a Permalink, and the user doesn't have access to the Password, then they can request access on the screen.

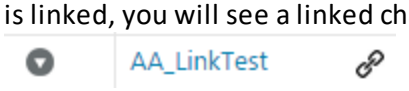


2.1.1.2.6.3 Copy or Move to Different Password List

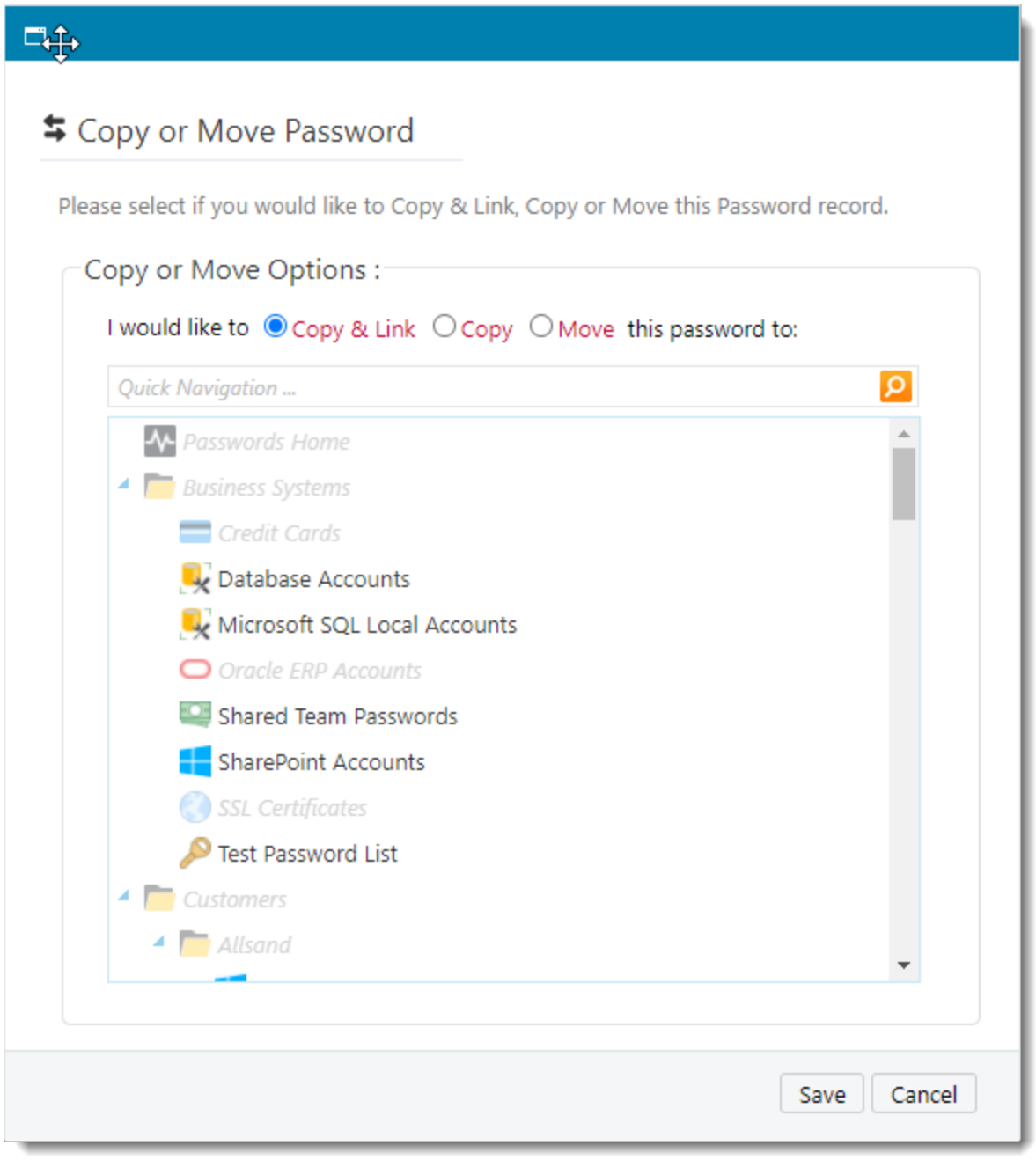
It is possible to copy or move a Password record to a different Password List, but there are a couple of exceptions which may prevent you from doing this:

- You need at least Modify rights to the Destination Password List
- The Destination Password List must have the same selected fields as the Source Password List
- For security reasons, you also cannot move a password in a Shared Password List, into a Private Password List
- And you cannot copy records into Private Password Lists

If a Password List is grayed out and disabled on the pop-up windows below, then one of the three restrictions above would be the cause. Hovering over the disabled item, should provide you a Tooltip with the specific reason why
Copy & Link will create a duplicate record in the Destination Password List, and all linked records will be kept in sync when any changes are made to either of the records. When a Password record is linked, you will see a linked chain icon next to the Title, similar to this image



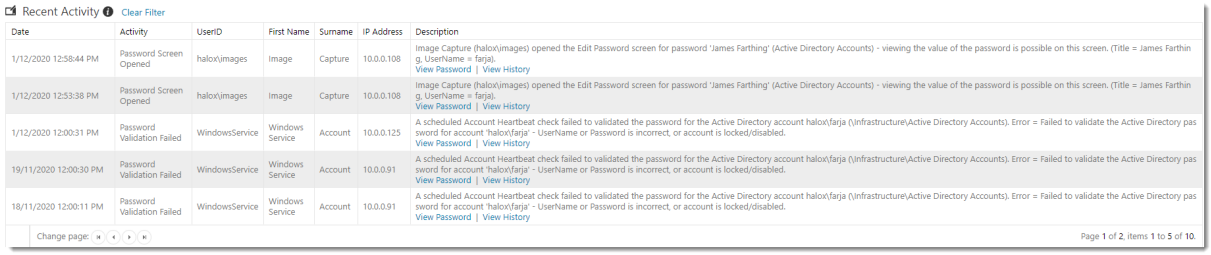
Note: There is a System Setting called "Synchronize the 'Deleted' status of Linked Password records across all affected Password Lists" which can be configured to delete records in other linked Password Lists, or not, when you delete from a Password List.



2.1.1.2.6.4 Filter Recent Activity on this Record

Sometimes it might be useful to quickly filter all the auditing data on information relevant to a single Password. When selecting 'Filter Recent Activity on this Record', all contents of the Recent

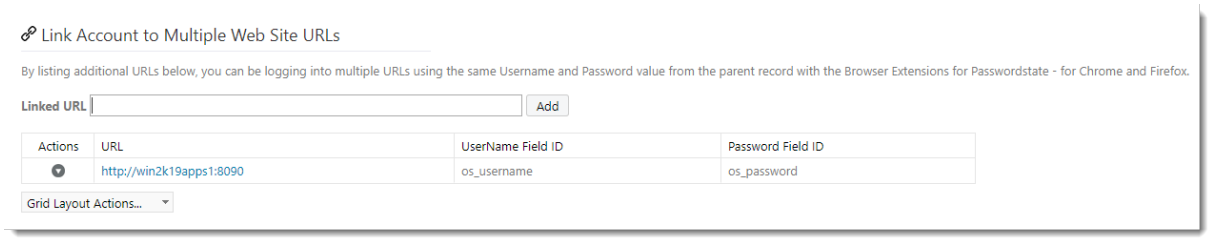
Activity grid will be filtered, and the 'Clear Filter' button will be displayed, allowing you to remove the filter.



2.1.1.2.6.5 Link Account to Multiple Web Site URLs

If using our Chrome or Browser extensions, and you use the same account to login to multiple different web sites (normally internal sites), then you can add those additional URLs to the screen you see below.

After you make changes here, you can restart your browser so the extension picks up the changes immediately, or after 1 minute the extension will pick up the changes automatically.



2.1.1.2.6.6 Send Self Destruct Message

This menu option allows you to send a Self Destruct Message, with the contents being details for the selected Password record.

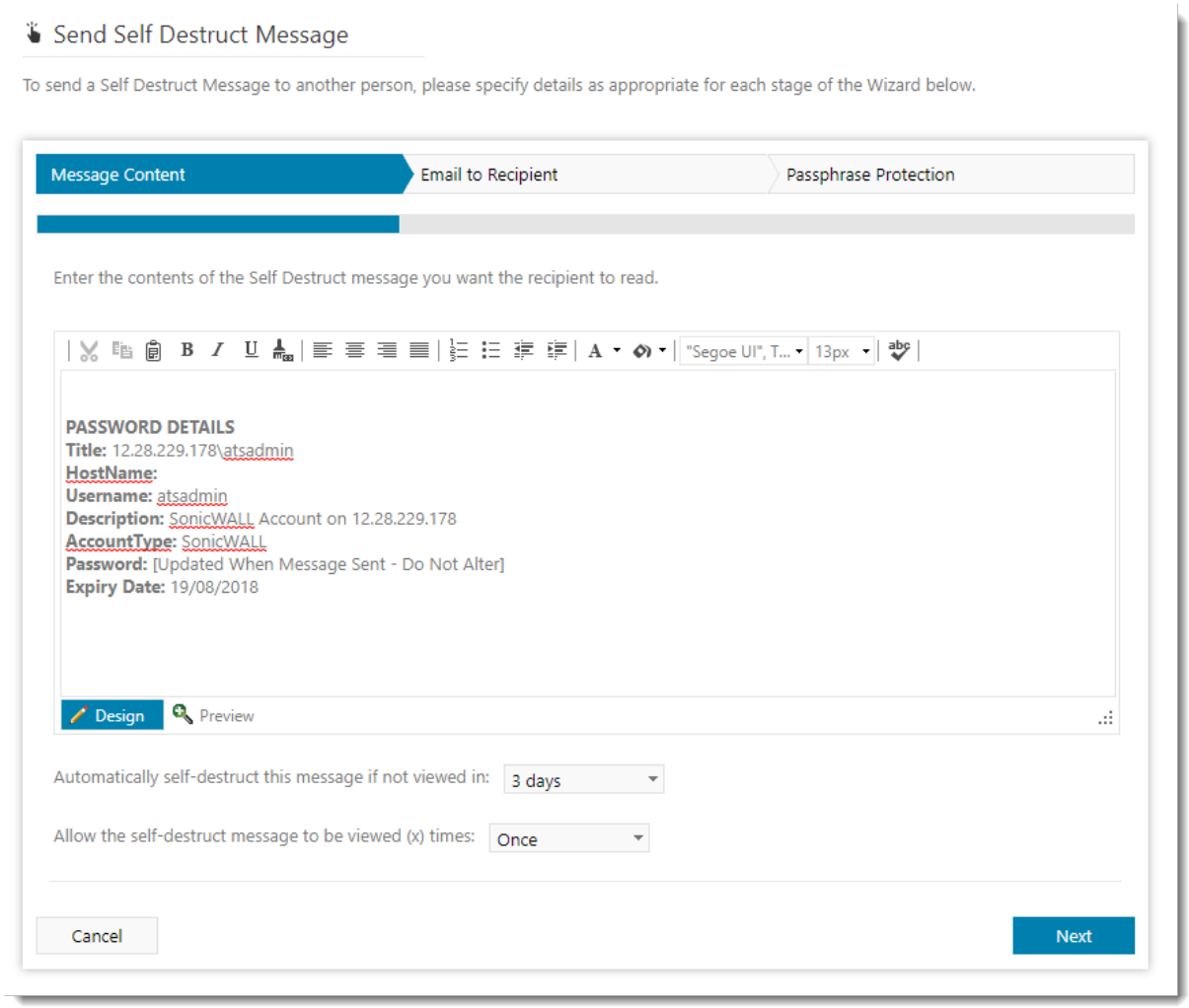
Creating a Self Destruct message is a three step process:

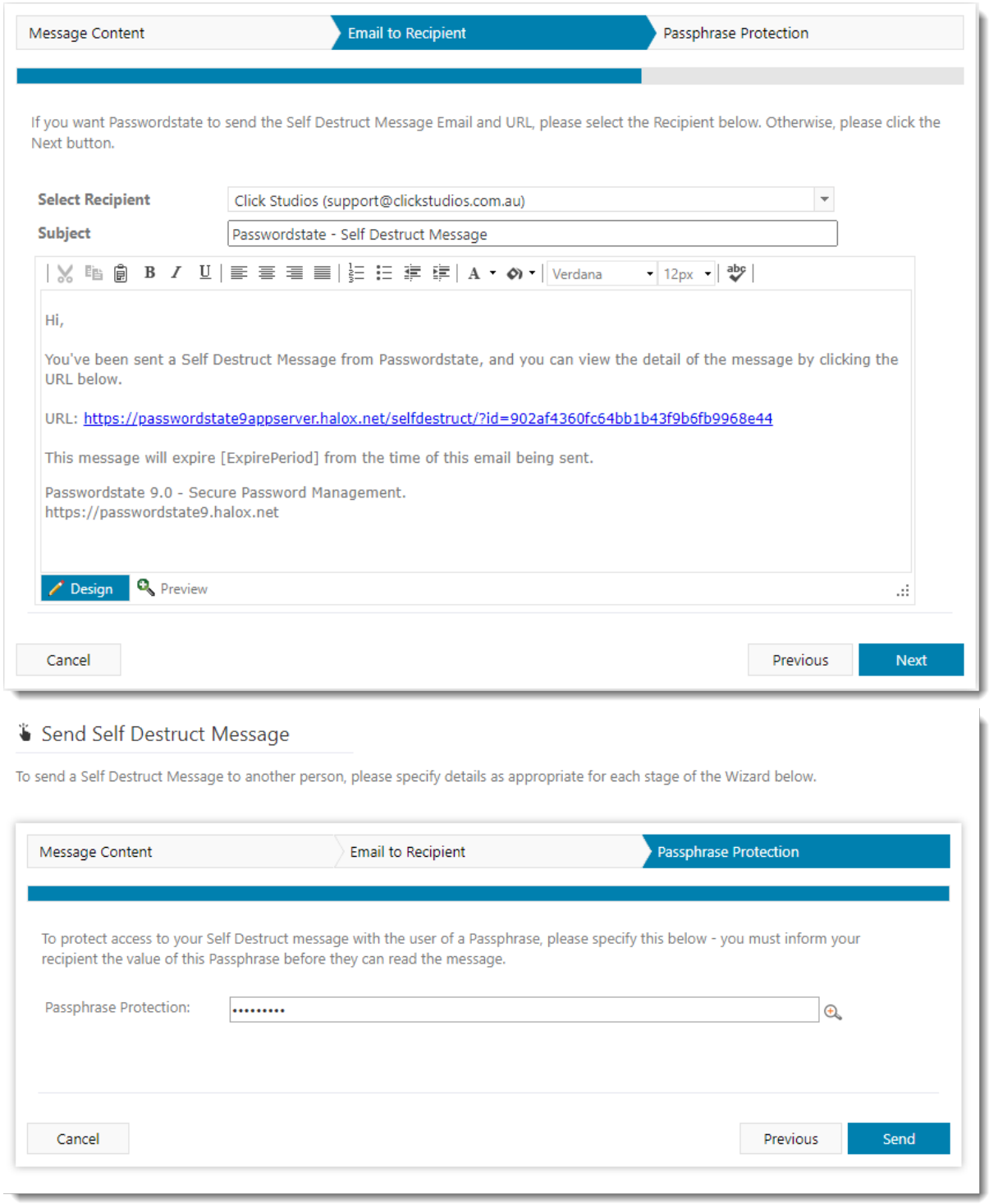
1. Specify the message, how long the message will be active for, and how many times the message can be viewed
2. Choose the user you want to send the message to - this can either be another user of Passwordstate, or a recipient from the Address Book, or someone else simply by typing their email address
3. And specify any Passphrase protection you might want - there is a default Passphrase value which can be configured by your Security Administrators on the screen Administration -> System Settings -> Self Destruct Messages, or contacts in the Address Book Book can also have their own Passphrase. The intended recipient need to know what this Passphrase is prior sending them messages

The message will no longer be available for viewing either when the user has viewed it the specified number of times, or the message has expired.

Note 1: Auditing records are added when a message is sent and read, and can be viewed on the screen Administration -> Auditing

Note 2: This menu option can be hidden on the screen Administration -> System Settings -> Password Options tab





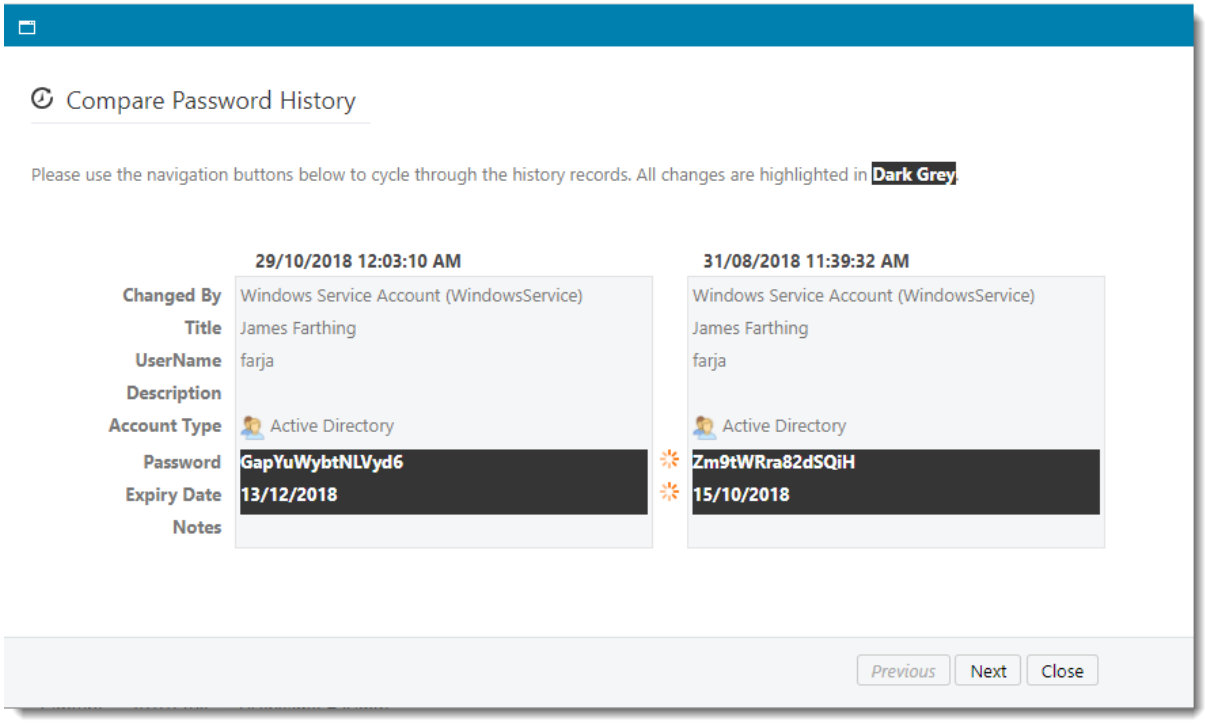
2.1.1.2.6.7 View & Compare History of Changes

Any changes made to a Password record will not only generate an audit log record, but also the history of changes will be maintained so you can easily compare what has change, when, and by whom

When you open the Compare Password History screen, you can:

- See what has changed as the adjacent fields will be highlighted in Dark Blue
- You can navigate back and forth between records by using the appropriate Previous and Next buttons

Note: An audit log record will be added when you open this screen, as it's possible to see Password values here.

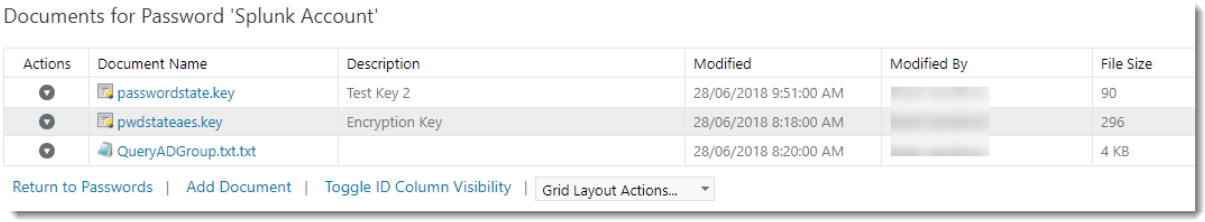


2.1.1.2.6.8 View Documents

As with Password Lists, it's also possible to upload one or more document/attachments and associated them with an individual Password record. Uploaded documents are also encrypted within the database, using the same type of 256bit AES encryption as other encrypted data.

On the 'Documents' screen for a Password record, the following is possible:

- Adding a new document
- Retrieving a document from the database by clicking on the 'Document Name' hyperlink
- You can edit some basic properties for the document
- Add also delete the document if required. Note, deleting a document does not place it in any recycle bin.



2.1.1.2.6.9 View Individual Password Permissions

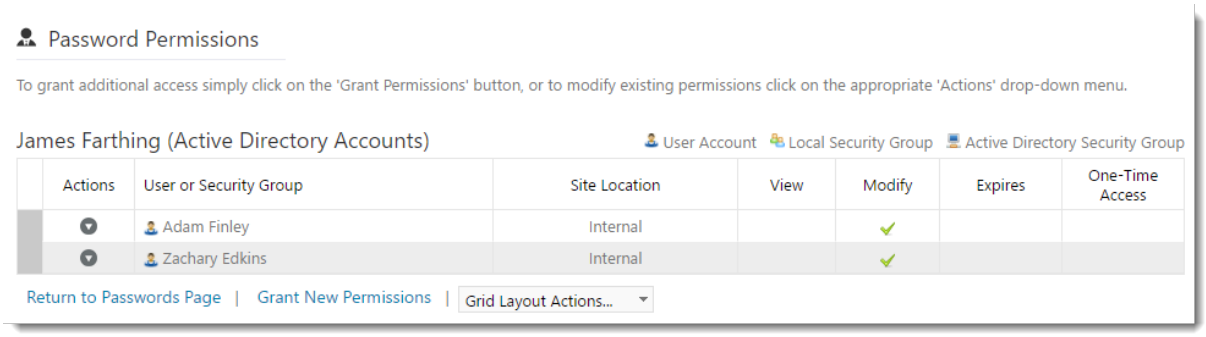
In addition to applying permissions to an entire Password List for users, you can choose to apply permissions just to individual Password records if required. When the user browsers to the Password List, they won't see all the records, just the individual ones they've been given access to

When you click on the 'View Individual Password Permissions' menu item, you will be directed to a screen which shows what permissions have been applied to the individual Password record.

Note: If a user doesn't already have access to the Password List, and you grant access to an individual Password record, then they will be given 'Guest' access to the Password List. Guest access is required so the Password List will show for the user in the Navigation Tree.

You can grant access to either user accounts or security groups, and the types of permissions you can apply are:

- View - only allows read access to the record
- Modify - allows the user to update and delete the Password record



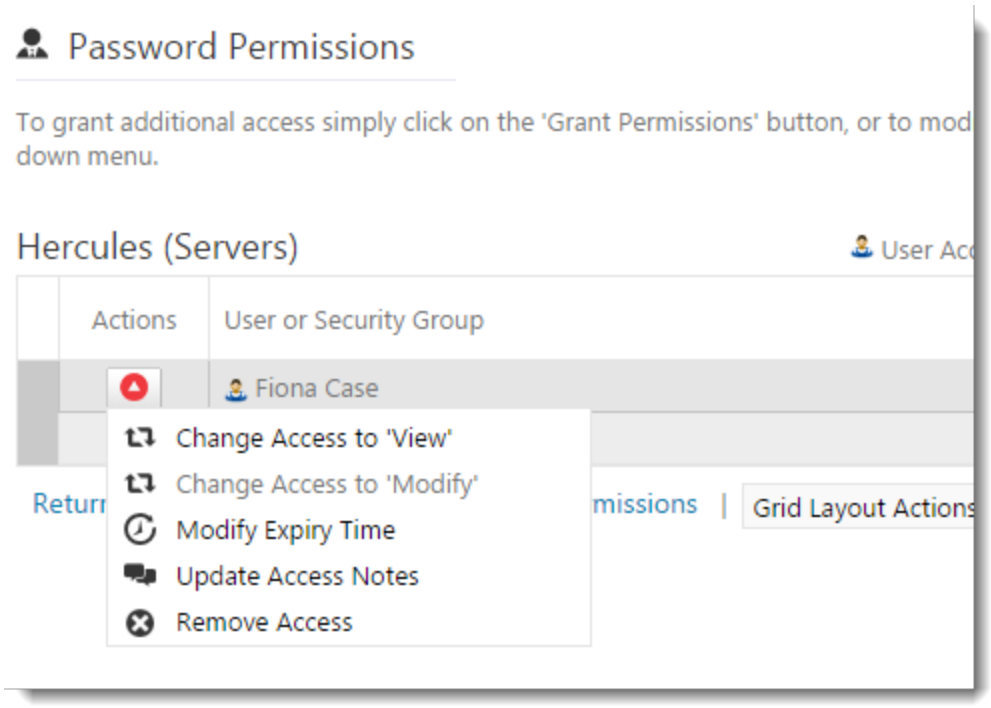
From the 'View Individual Password Permissions' screen, you have the following features available:

Password Permission Actions

When you click on the 'Actions' menu item for access which has been granted to a user or security group, you can:

- Change the permissions to View or Modify
- Set or modify the time in which their access will be removed - if required
- Allow you to update a notes field as to why the access was given

- Or remove the access altogether



Grant New Permissions

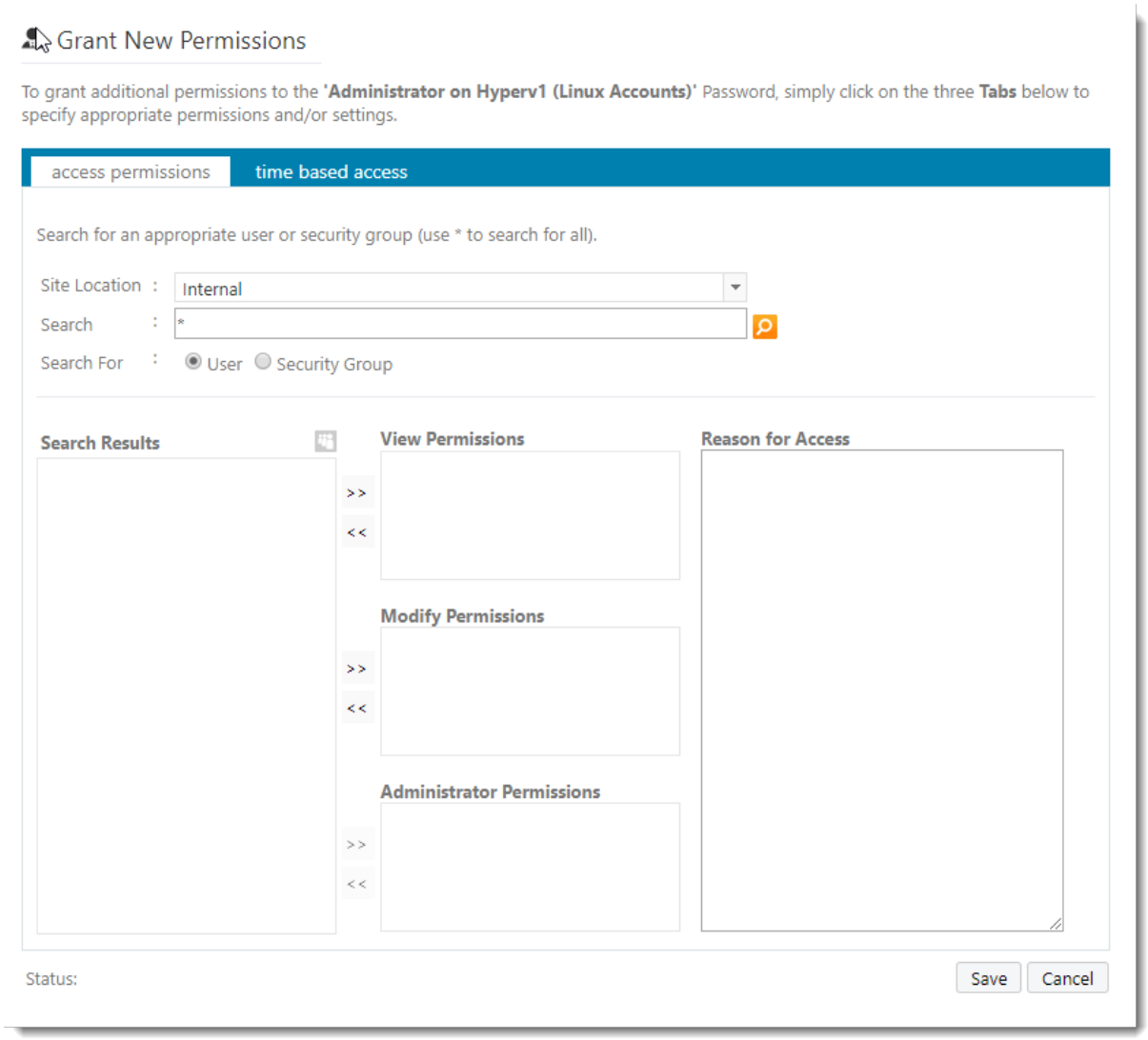
To grant new permissions to a user's account, or to the members in a security group, you can click on the Grant New Permissions button.

When granting new permissions (access) to a Password record, there are three tabs of features available to you:

Access Permissions

The 'Access Permissions' tab allows you to search for users and/or security groups, and either grant View Access, or Modify Access

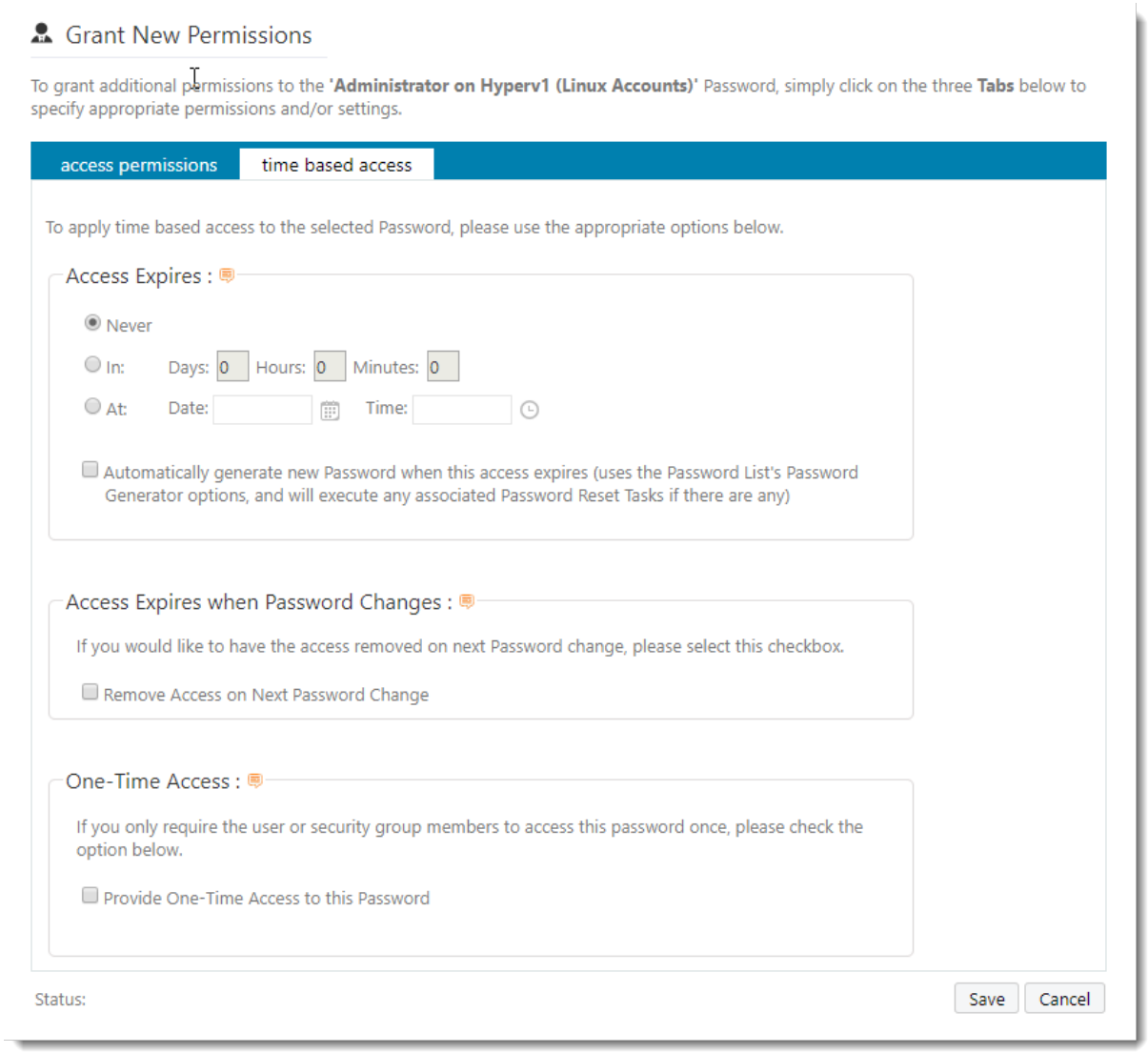
Note: You cannot apply Administrator permissions to an individual Password record - this is reserved for Password Lists only



Time Based Access

There are multiple 'Time Based Access' features available for individual Password records, and they are:

- Access Expires - specify a future date and time in which the users/security groups access will be automatically removed
- Access Expires when Password Changes - any event which changes the actual value of the password field for the record, will cause this access to be removed
- One-Time Access - you have the option to only allow access to the Password record once. Once the user has viewed the password, their access will be removed. You also have the option of generating a new random password when this event occurs as well.



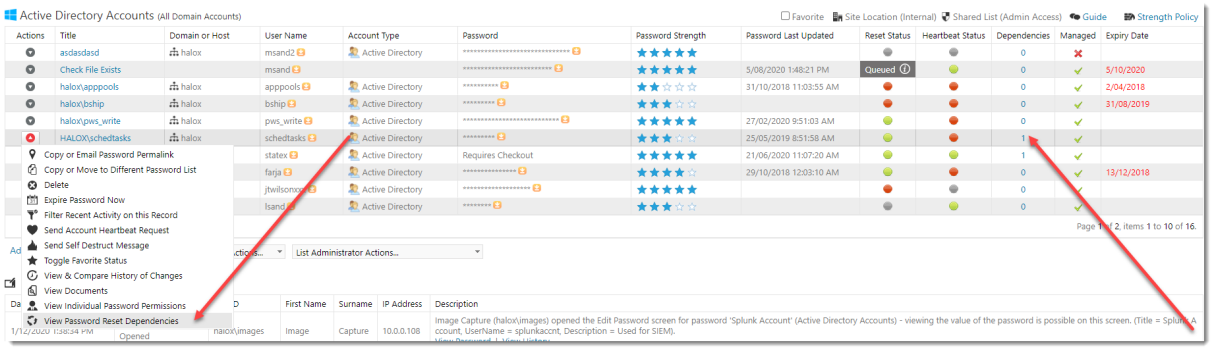
2.1.1.2.6.10 View Password Reset Dependencies

In addition to performing Password Resets for accounts, you can also add various 'dependencies' to a password record, which can also trigger a Password Reset script after the password for the account has been reset.

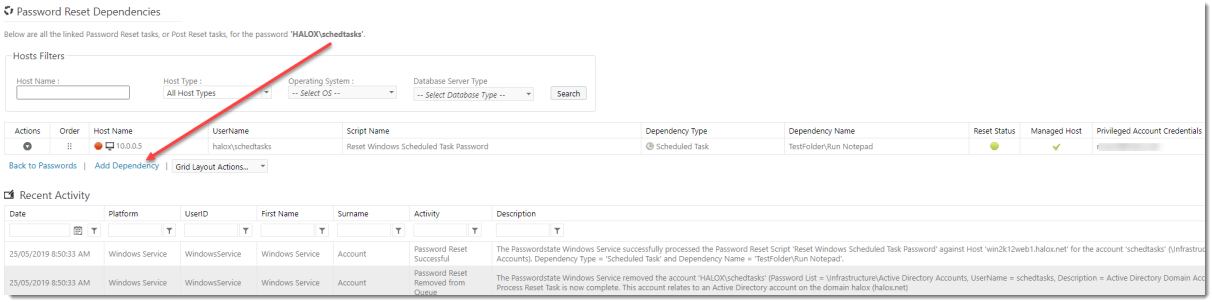
A typical example of this would be where the account is an Active Directory account, and it's being used as the "identity" for operations of Windows Services, Scheduled Tasks, IIS Application Pools or COM+ Components. It is also possible to automate account discovery, and these dependencies as well - Account Discovery

It is also possible to execute any custom type of PowerShell script you want as well, and the script does not necessarily have to be associated with a Host record.

To add a "dependency" to a password record, you can either select the 'View Password Reset Dependencies' menu item, or click in the count in the Dependencies column in the grid.



Then you click on the 'Add Dependency' button.

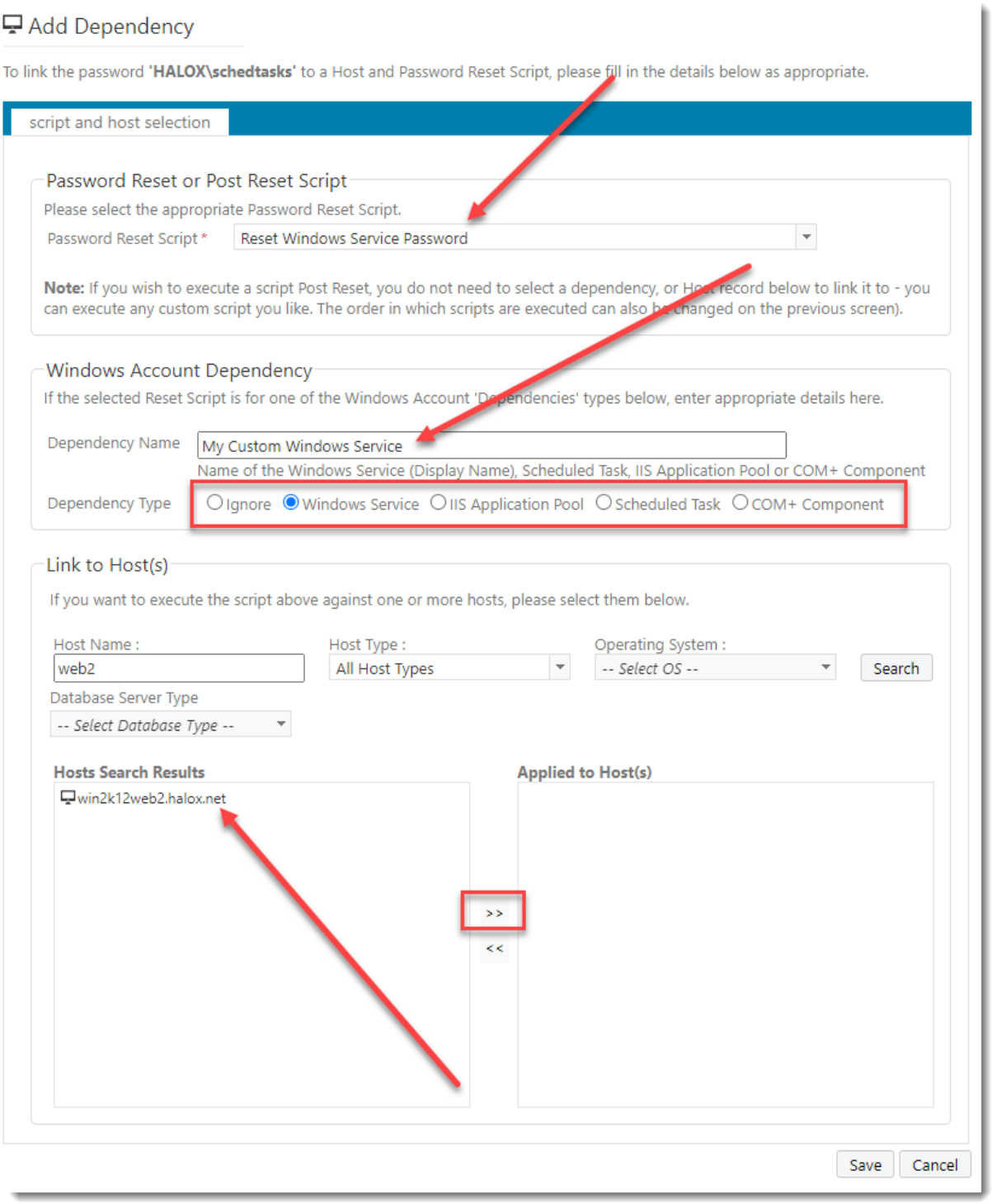


And then select the following options as appropriate:

1. The Password Reset Script
2. If this dependency relates to a 'Windows' type resource, specify the name of the dependency and select the appropriate Dependency Type as well
3. And to specify which Host the dependency is currently is installed on, search for the appropriate host and select it

Note 1: Any custom PowerShell script can be selected here, and it does not need to be associated with a Host either

Note 2: This dependency will use the selected Privileged Account Credential to execute, of which is selected for the password record itself.



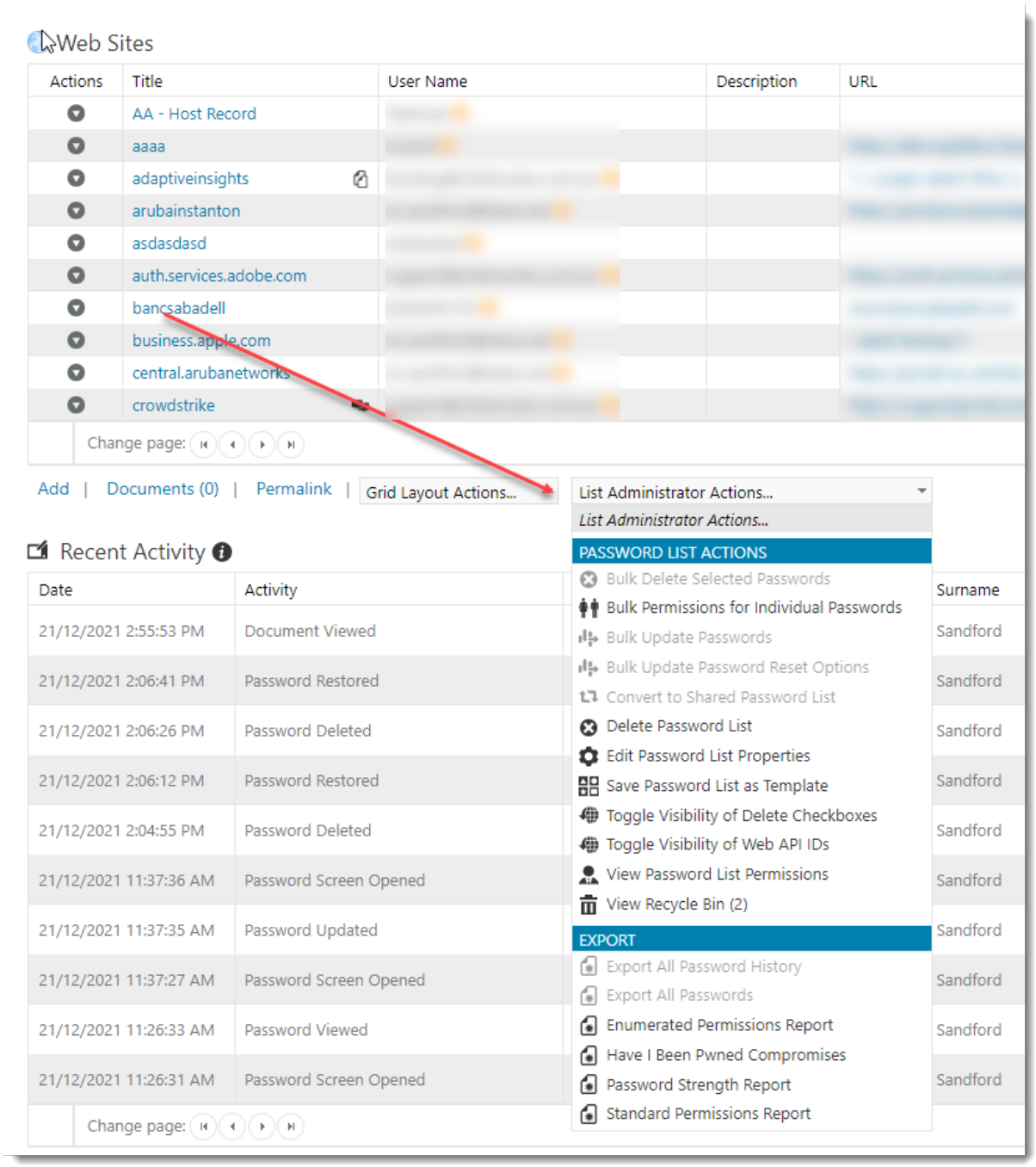
2.1.1.2.7 List Administrator Actions

If you have 'Administrative' privileges to a Password List, all of the features in the 'List Administrator Actions' drop-down list will be available to you.

A summary of the features are:

Bulk Delete Selected Passwords	Use in conjunction with the 'Toggle Visibility of 'Delete Checkboxes', it is possible to delete more than one password record at a time
Bulk Permissions for Individual Passwords	Allows you to apply permissions for a User's Account, or a Security Group, to multiple individual passwords records at once
Bulk Update Passwords	Instead of editing data/fields for a single Password record, 'Bulk Update Passwords' allows you to use a CSV file to update many records at once
Bulk Update Password Reset Options	When you have a Password List enabled to perform Password Resets, you can use this feature to change multiple "reset" options for one or more password records i.e. schedules, Privileged Account Credentials, etc
Change Owner of Private Password List	If the Password List is Private, you can change the owner of the List in the event the UserID for a user needs to change i.e. new domain, change in name, etc
Convert to Shared Password List	If the Password List is a Private one, and you wish to convert it to a Shared one, then you can use this menu option.
Delete Password List	Deleting a Password List will delete the List itself and all related data. Note: There is no Recycle Bin for a Password List, so please use this feature with caution
Edit Password List Details	Allows you to modify existing settings for the Password List, change which fields you would like to use, and create an API key so records in the Password List can be queried or manipulated via the Passwordstate API
Save Password List as Template	Allows you to save all the settings and chosen fields as a Template, which can then be used for the creation or management of other Password Lists
Toggle Visibility of 'Delete Checkboxes	When you select this menu item, checkboxes will appear next to the 'Title' field in the grid. You can then select any number of records, and then use the 'Bulk Delete Selected Passwords' menu item to delete more than one record at a time
Toggle Visibility of Web API IDs	Allows you to see various ID fields required for the Passwordstate API
View Password List Permissions	Allows you to view existing permissions applied to this Password List, modify existing permissions and add new ones
View Recycle Bin	Allows you to see what Password records have been deleted, and gives you the option to restore from the Recycle Bin or permanently delete
Export All Password History	The report will export all history relating to each Password record, including the date data was changed, and who it was

	changed by. Note: The password field values will be exported in clear text with this report
Export All Passwords	The report will export all the fields and their values for each of the Password records. Note: The password field value will be exported in clear text with this report
Enumerated Permissions Report	This report will show an enumerated permissions list on individual Password records, just for User Accounts - Security Group will be enumerated as well to shown as User Accounts
Password Strength Report	This report will show the password strength for each of the Password records, based on the Password Strength Policy set for the Password List
Standard Permissions Report	Will export to csv file a list of permissions applied to the Password List, or any individual Password records



2.1.1.2.7.1 Bulk Update Passw ords

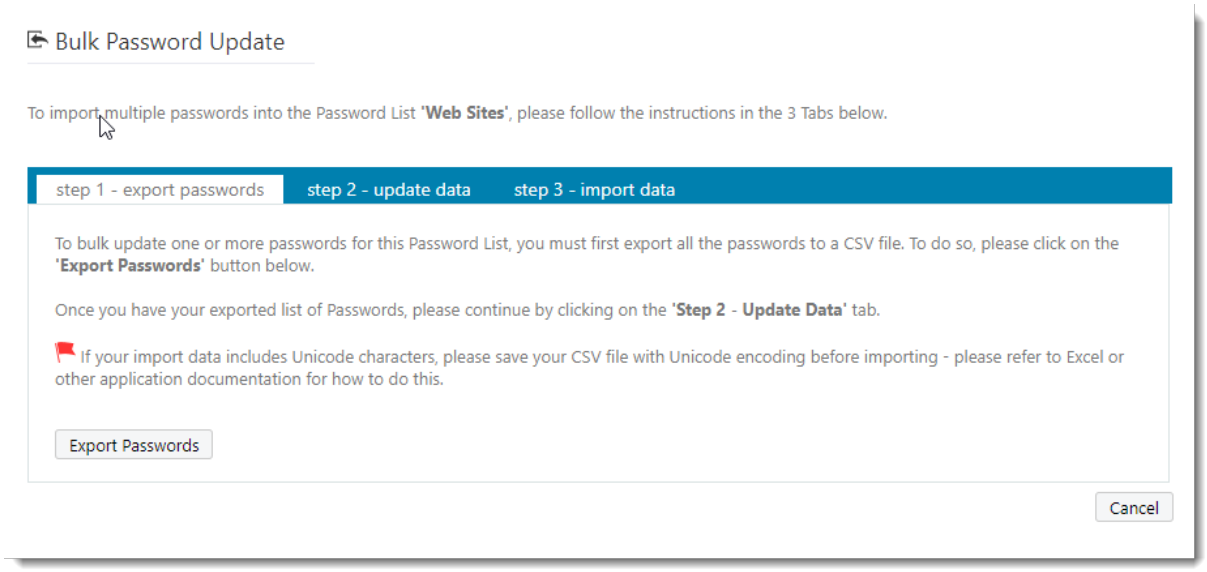
If you have a requirement to update more than one Password record at a time, then you can use the 'Bulk Update Passwords' feature.

This feature will allow you to export all the passwords to a csv file, which you can then update as appropriate, and then re-import back into the Password List.

Note: This feature will not update passwords in Active Directory for any records configured as Active Directory accounts, and it will not execute any related Password Reset Tasks
Note: The 'Export Passwords' button on the Step 1 tab will export all Passwords to the csv file. It's okay to delete any records from the CSV file which you don't intend on updating
Note: Please do not delete or modify the contents of the PasswordID column in the csv file - this is what is used to know which records to update in the database

Step 1 - Export Passwords

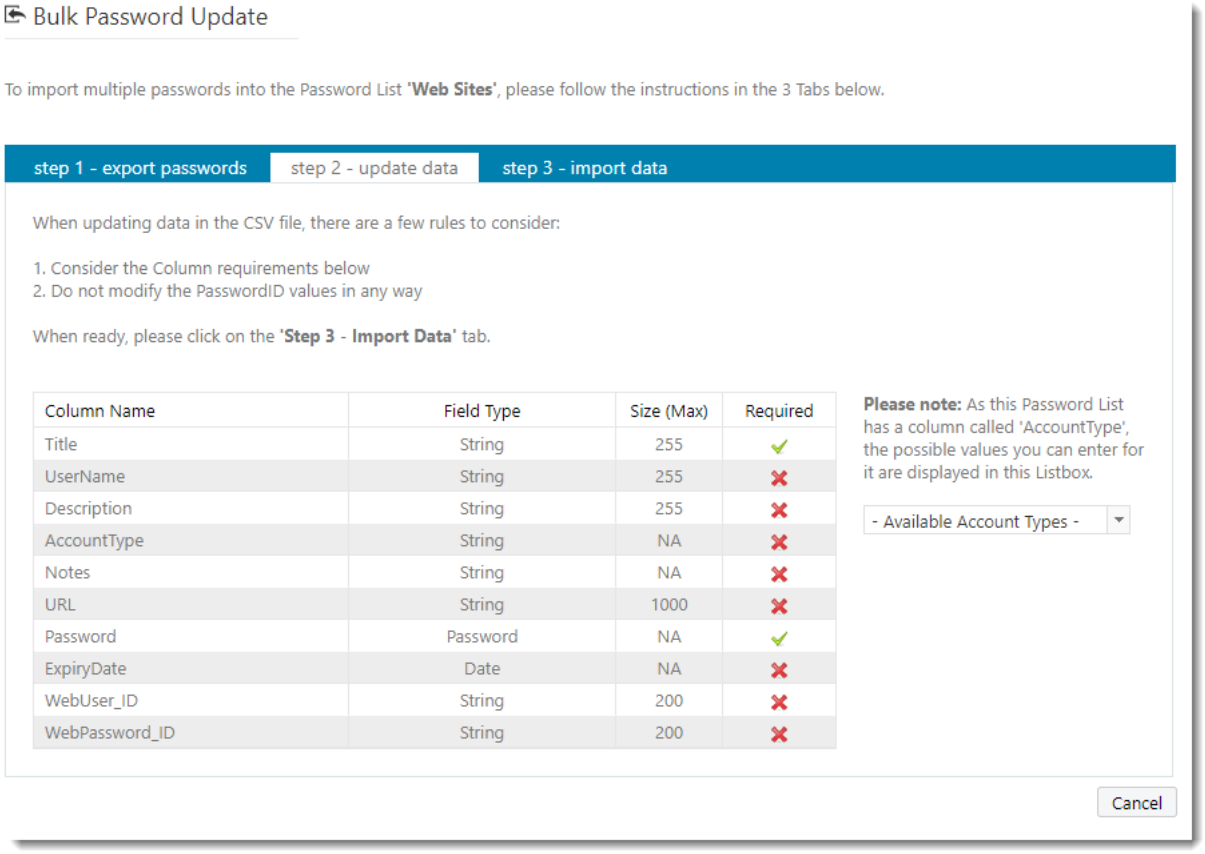
Clicking on the 'Export Passwords' button will export all Password records to a csv file. Once you have your csv file, you can move onto the next tab 'Step 2 - Update Data'.



Step 2 - Update Data

The Step 2 tab shows you what fields can be updated as part of this process, and if any of the fields are mandatory. As mentioned previously, you can delete any rows in the csv file you do not wish to update. Once you have the csv file updated as required, you can move onto the next tab 'Step 3 - Import Data'.

Note: If a field already has data associated with it, but you don't wish to update the data for this field, you simply leave the value as it is - if you remove the data for this field, it will also remove it in the database when the import process occurs

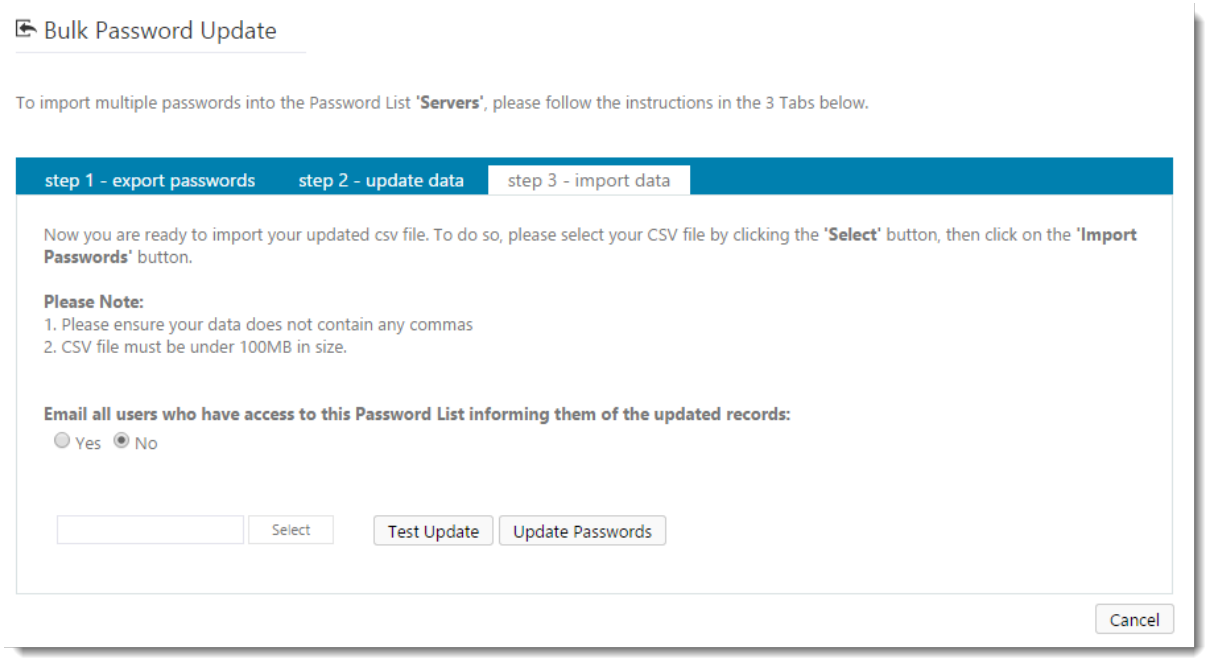


Step 3 - Import Data

The final tab allows you to upload your csv file to the Passwordstate web site, and then either test the import first, or perform the actual import. Both the test and actual import will report back to you if there are any errors experienced with the import process, and they will also tell you what row in the csv file the error occurred.

Note: This is not an import in the traditional sense, as it won't add new records, simply update records as appropriate

Note: While the option is available, it's not recommended you select the option to email all users who have access to the Password List, unless it is a small number of records you are importing - otherwise, each user who has access to the Password List will receive one email per record, indicating a new record has been added to the Password List.

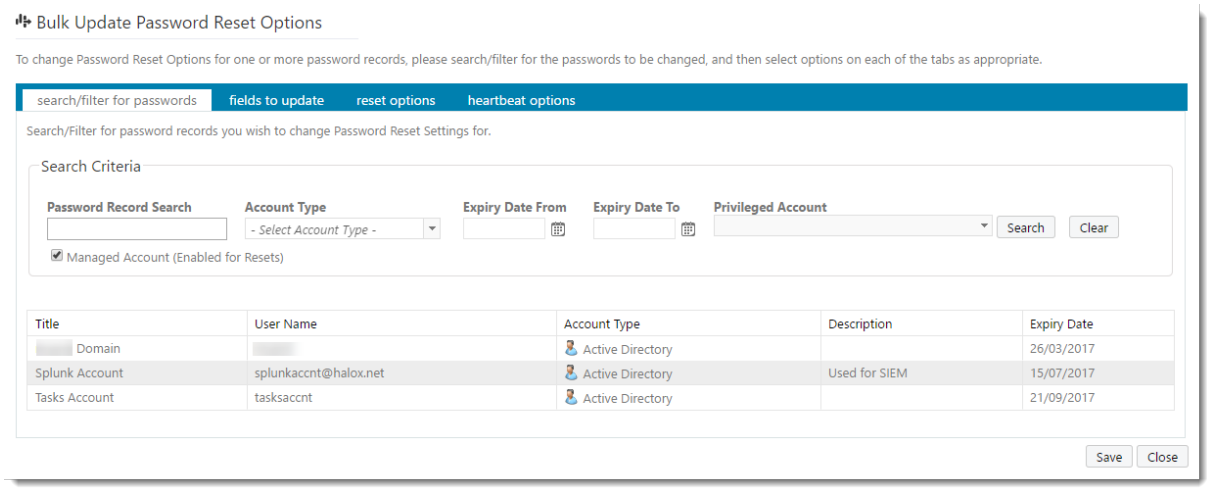


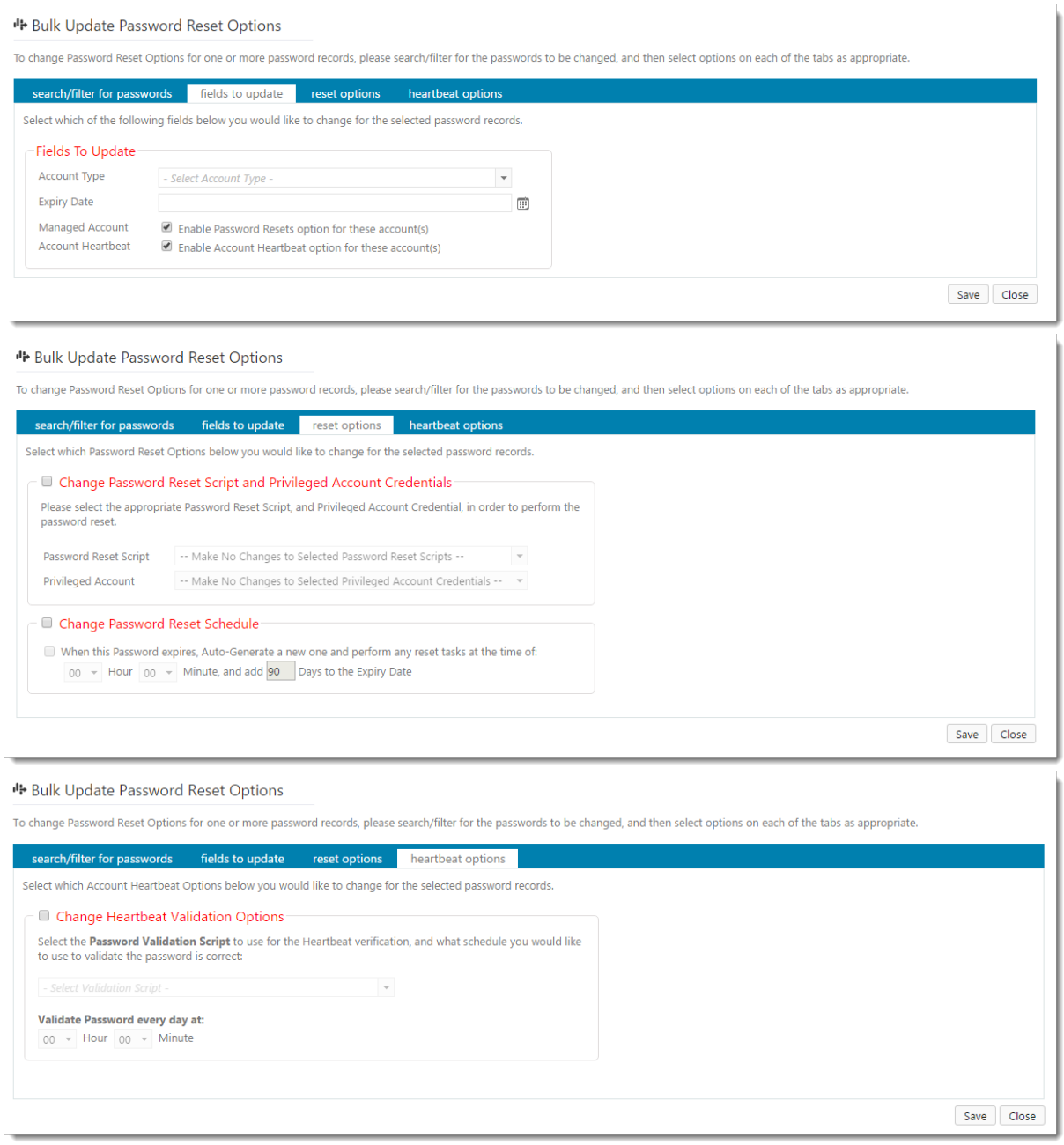
2.1.1.2.7.2 Bulk Update Passw ord Reset Options

If you need to update Password Reset settings for more than one password record at a time, then you can use the 'Bulk Update Password Reset Options' available from the 'List Administrators Actions' dropdown list on each Password List.

With this feature you can:

- Search for the password records you wish to update - based on certain criteria
- You can then update various fields, scheduled reset options, and the Heartbeat validation options as well





2.1.1.2.7.3 Edit Password List Properties

The Edit Password List Properties feature allows you to change any number of settings associated with the Password List, and choose which fields (columns) you would like to use.

Note: If the Password List is 'Linked' to a Template, then the majority of options on this page will be disabled, as the settings are meant to be controlled centrally from the Template.

The following four tabs allows you to configure the Password List with the options are fields required.

Password List Details Tab	This tab is where the majority of settings are configured for the Password List
Customize Fields Tab	This tab allows you to choose which fields you would like to use with the Password List
Guide Tab	The Guide Tab allows you to provide some instructions to your users as to the intended use of the Password List
API Key Tab	If you need to take advantage of the API (Application Programming Interface) for the Password List, you will first need to create and API Key - each Password List has it's own separate API Key

The Password List Details tab is where the majority of settings are specified for the Password List, and it also allows you to copy settings from another Password List or Template, and copy permissions form another Password List or Template.

Note: The various Password related options below do not apply to any Generic Fields (Customize Fields Tab) you configure of type 'Password' i.e. prevent password reuse, prevent saving bad password, reset expiry date field, etc.

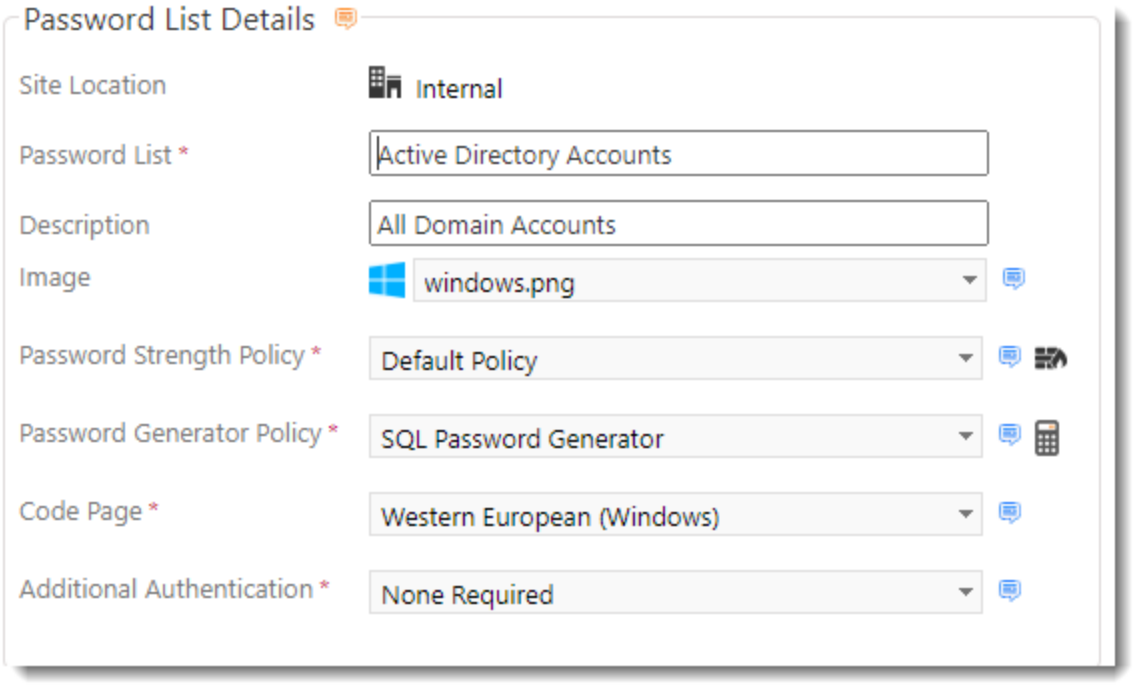
Below is some detail for each of the sections in the Password List Details tab.

Password List Details Section

The following table describes each of the fields/options for the Password List Details section:

Site Location	A Site Location of "Internal" will be used if the Password List is being created in the root of Passwords Home, or it will inherit the location of its parent Folder. Adding different Site Locations requires an active subscription for the Remote Site Locations module
Password List	The Title for your Password List, as it would be displayed on the Navigation Tree
Description	A brief description outlining the purpose of the Password List
Image	An image you would like displayed for the Password List in the Navigation Tree
Password Strength Policy	The Password Strength Policy you would like applied to the Password List. Clicking on the icon will provide detail for the selected policy
Password Generator Policy	The Password Generator Policy you would like applied to the Password List. Clicking on the icon will provide detail for the selected policy
Code Page	The Code Page (character encoding) you would like to use when importing or exporting data from the Password List

Additional Authentication	If you want a second level of authentication for your users before they can access the Password List, you can choose any one of the authentication methods in this drop-down list



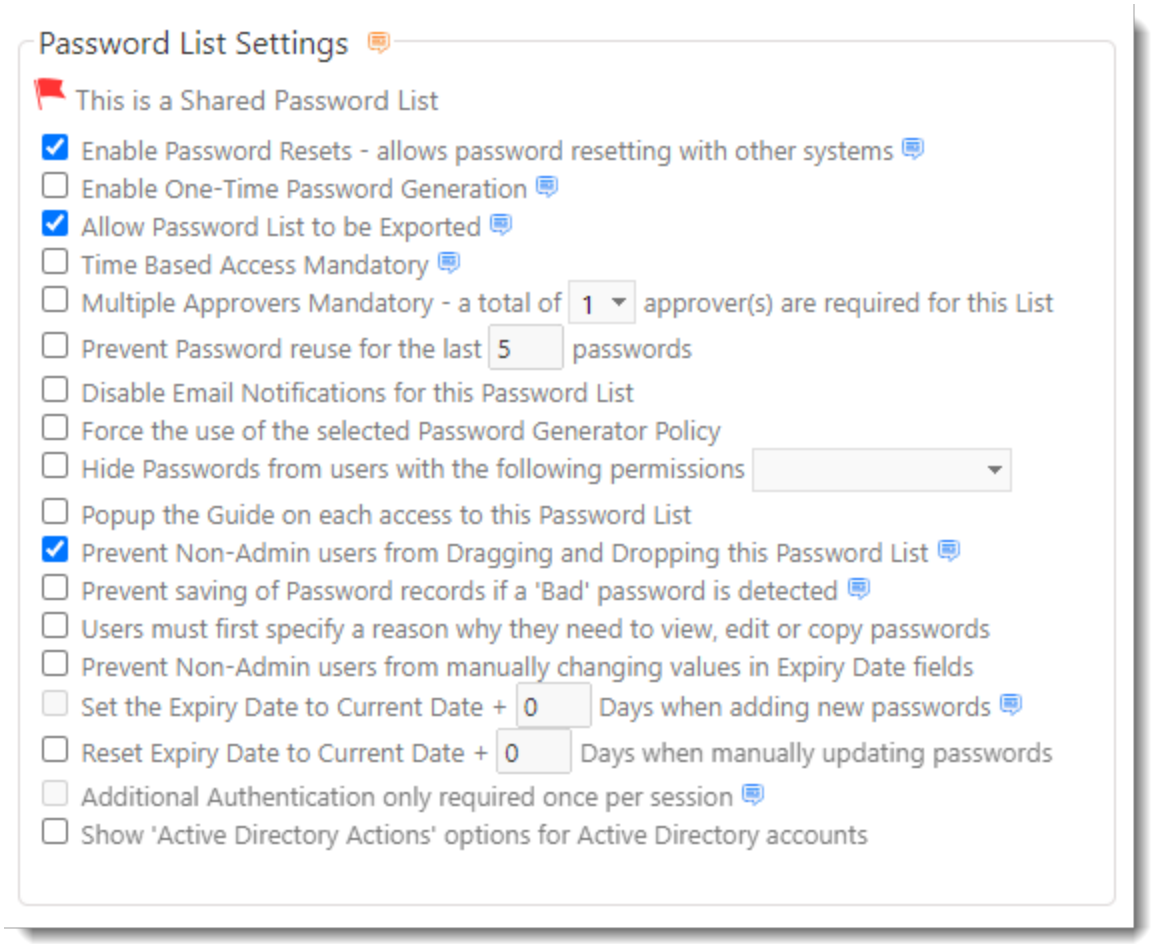
Password List Settings Section

The following table describes each of the options for the Password List Settings section:

Enable Password Resets	Allows passwords stored within the Password List to perform Password Resets on other remote systems/hosts
Enable One-Time Password Generation	Store One-Time Passwords for logging into web sites by scanning a QR Code for your login
Allow Password List to be Exported	Allows or prevents the passwords and their history from being exported
Time Based Access Mandatory	If this option is set, any time new permissions are applied to the Password List for user accounts or security groups, you must specify a future date/time when the permission will be automatically removed
Multiple Approvers Mandatory	If required, you can specify that more than one administrator must approve access to the Password List, or to records contained within it
Prevent Password reuse for the last [x] passwords	You can choose to prevent reusing of Passwords (the password value) by selecting this option, and specifying how many password changes are required before a password can be reused

Disable Email Notifications for this Password List	Disable email notifications for this specific Password List i.e. Password Added, Updated, Deleted, Copied to Clipboard, etc
Force the use of the selected Password Generator Policy	With this option set, users cannot enter their own passwords manually - they must use the Password Generator button to generate new passwords
Hide Passwords from users with the following permissions	You can hide passwords, and disable copy to clipboard, based on permissions the user has to the Password List i.e. View, Modify or Admin
Popup the Guide on each access to this Password List	If you would like the 'Guide' to be displayed every time a user accesses this Password List, you can select this option
Prevent Non-Admin users from Dragging and Dropping	You can select this option to minimize who can drag and drop the Password List around in the Navigation Tree
Prevent saving of Password records if a 'Bad' password is detected	Your Security Administrators maintain a list of passwords in Passwordstate which are deemed to be 'bad' i.e. common, or easy to guess/brute force. By selecting this option, user's won't be able to save any changes to the record if a Bad Password is used - the user is also shown what the Bad Password is, to educate them on not what to use
Users must first specify a reason why they need to view, edit or copy passwords	If you would like your users to specify why they need to view a Password prior to being able to view it, then select this option. Your users will be presented with a dialog window asking them for the reason they wish to use the Password, and this reason is then added to auditing data, which can be reviewed at a later date if needed
Prevent Non-Admin users from manually changing values in Expiry Date fields	You can choose to prevent users with View or Modify rights from changing the Expiry Date field value for password records. This is useful for ensuring the Expiry Date isn't reset, without the actual Password being reset
Set the Expiry Date to Current Date + [x] Days when adding new passwords	When adding new Passwords to the Password List, you can automatically generate the Expiry Date field value based on a certain number of days in the future, by selecting this option
Reset Expiry Date to Current Date + [0] Days when manually updating passwords	When updating Passwords in the Password List, you can automatically generate the Expiry Date field value based on a certain number of days in the future, by selecting this option
Additional Authentication only required once per session	If you choose one of the 'Additional Authentication' options for the Password List, you can choose to make your users authenticate ever single time they wish to view the contents of the Password List, or only once per session - once per session means once they have authenticated to the Password List, they won't need to authenticate again while their session on the web site is active i.e. if they log out of Passwordstate, they will need to re-authenticate again to the Password List

Show 'Active Directory Actions' options for Active Directory Accounts	Provides you with another Tab on the Edit Password screen which allows: • Unlock this account if locked • User must change password at next logon • Disable this account • Enable this account

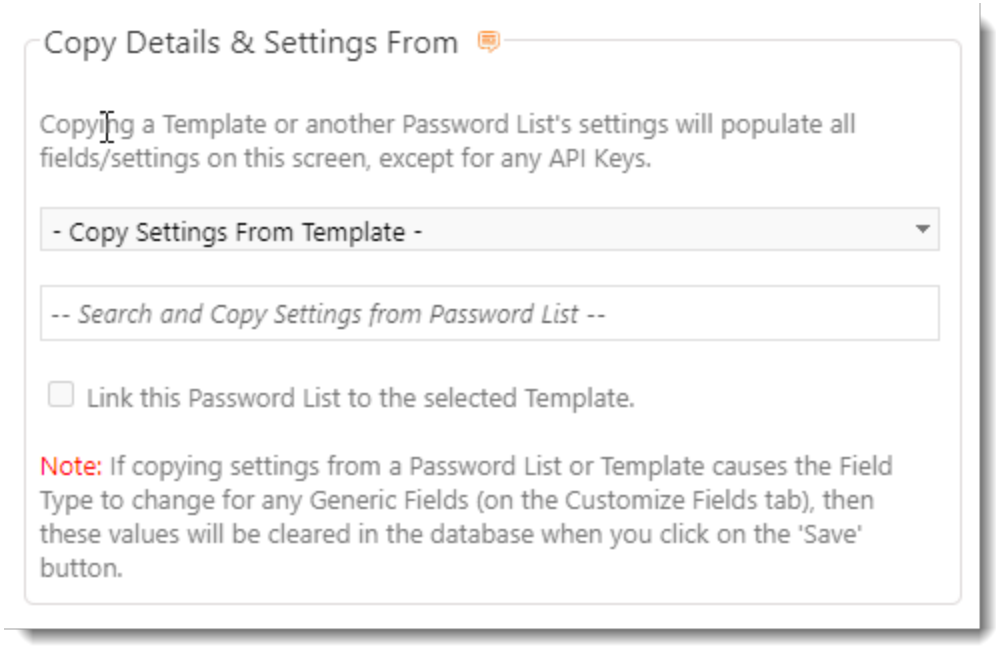


Copy Details & Settings from Section

This section allows you to copy Password List settings, and fields to use, from another Password List or Template.

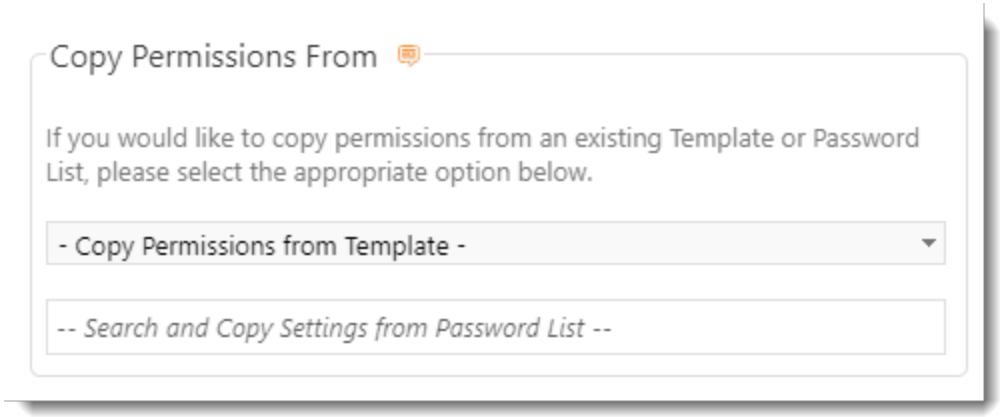
Note 1: When copying settings from another Password List or Template, you need to be aware of incompatible field types for Generic Fields. If a selected Generic Field in one Password List/Template is of type 'Text Field', and of type 'Password' in the Password List you are editing, then the values in the Password List you are editing will be erased/blanked in the database - this is because you cannot mix different Generic Field data types. There are multiple warning messages within the Passwordstate as well for this, so please be aware.

Note 2: If you select to copy settings from a Template, you can also link the Password List to the Template at the same time. By doing this, all subsequent changes to settings and fields needs to be done on the Template itself, and not on the Password List



Copy Permissions From Section

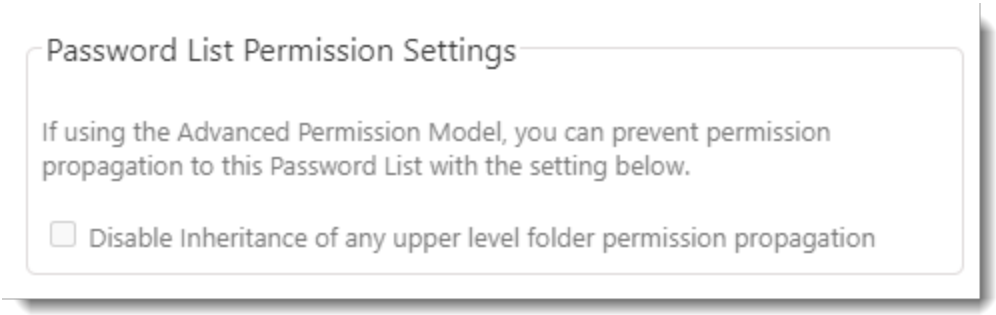
This section allows you to apply permissions based on what's set for another Password List, or Template. This will override any permissions you already have applied to the Password List.



Password List Permission Settings

When using the Advanced Permission Model, you can prevent permissions propagating down to a Password List, by using the 'Disable Inheritance' setting you see below. You can then manage permissions on the Password List, independently of any upper level folders.

Note: If you are unticking this option when it was previously ticked, it is first recommended you review the permissions on the Password List and set the as required, prior to unticking this setting.



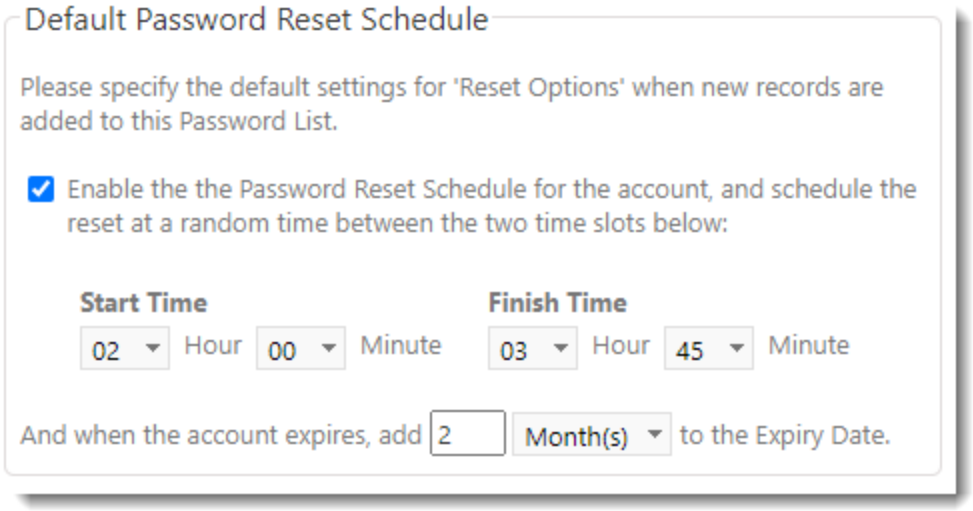
Default Password Reset Schedule

If a Password List is configure to perform Password Resets with other systems/hosts, you can then set various Automatic Password Reset settings - used for resetting a Password once the Expiry Date field value is reached.

You can set what the 'default' values are for each of the individual Password records for these settings, by setting them here at the Password List level.

Note: Once these default options have been applied to a Password record, and the record saved, making changes for these default values at the Password List level will have no effect on Password records. There is a feature where you can update these settings in bulk though, and you can find the detail here - Bulk Update Password Reset Options

Note: Making changes to these default values at the Password List level will have no effect on Password records where their settings have already been saved. This allows you to have different Password Reset schedules for each of the Passwords stored in a Password List - if required.



The Customize Fields tab is where you specify which fields you would like to use with the Password List, which of the fields are mandatory, and specify certain 'Field Types' for any one of the 10 Generic Fields.

The fields can be categorized in one of two ways - Standard Fields which are fixed and cannot be modified in any way, and Generic Fields which can be renamed and their Field Type changed. A summary of the different fields available are:

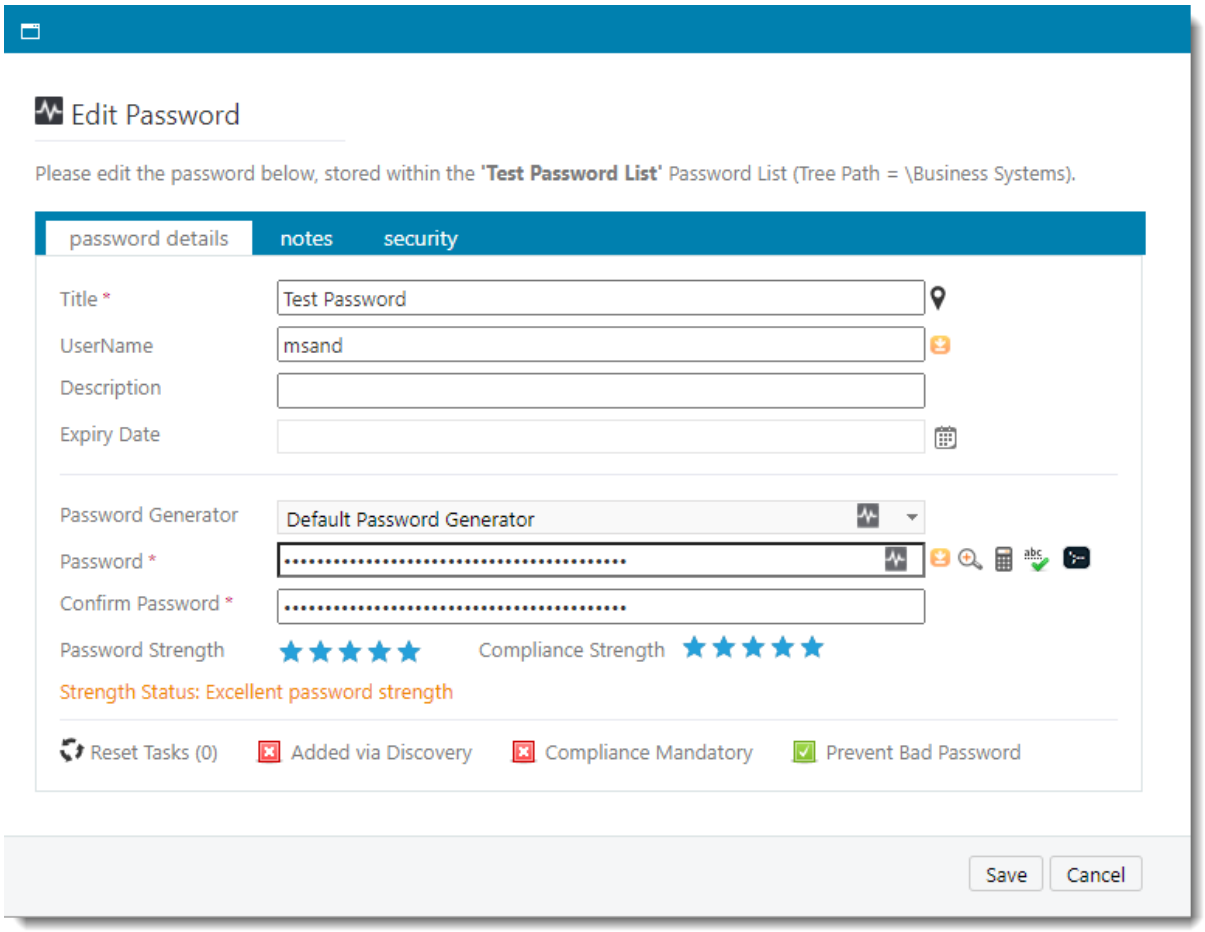
Title	This is the one mandatory field you must specify, and it's intended as a brief description as to what the Password record relates to
Username	If you must specify a username to authenticate against the end resource, this is the field you would use i.e. Username and Password to authentication to a web site, or network switch, etc
Description	A longer description as to what the Password record relates to
Account Type	Account Type can be used to visually show the type of account the record belongs to i.e. a switch, a firewall, and web login, etc.
URL	If you would like to associate as web sites URL with the Password record, then you can use this field. You can launch the URL by clicking on it when shown in the Passwords grid
Password	The actual password itself
Password Strength	You cannot enter any data for the Password Strength field - it's a graphical representation of how strong the password is, based on the selected Password Strength Poilcy
Expiry Date	All passwords should be reset after a certain period of time. The Expiry Date field can be used to indicate when this time is, and can be used for reporting purposes, or for Automatic Password resetting
Notes	Allows you to specify longer HTML formatted text for any general notes you need to maintain for the record
Generic Fields (1 to 10)	Generic Fields can be configured for any purpose you like, and also named any way you like. The following Field Types are available for Generic Fields: • Text Field — A single line text field • Free Text Field — Multiple line text field • Password — An encrypted password field • Select List — A vertical drop-down list of predefined values • Radio Buttons — A horizontal checklist of predefined values • Date Picker — A popup calendar style control for picking date values • URL Field — Allows you to click on the URL in the Grid view and launch the web site

Note 1: If you change a Generic Field's Field Type after the fields have been populated with data, then the values for the changed field will be erased/blanked in the database when you click

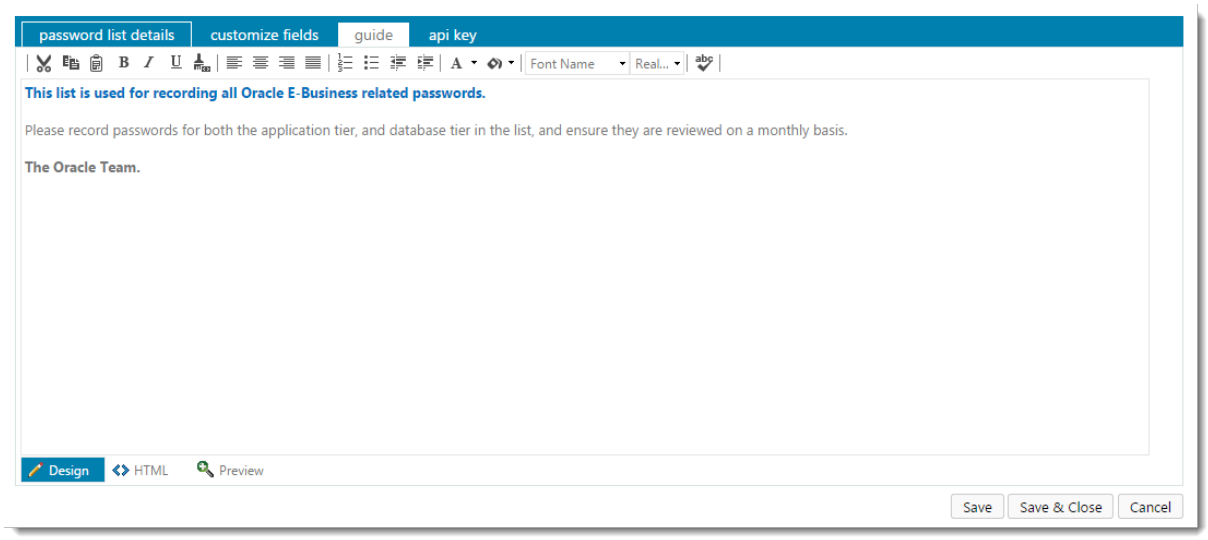
on the 'Save' button - this is because the different Generic Field Field Types need to have their data treated differently. There are multiple warning messages within the Passwordstate as well for this, so please be aware.

Note 2: Selecting/deselecting the 'Encrypt' option for any of the Generic Fields will perform the encryption/decryption in the database for all existing records in the Password List when you click on the Save button

Note 3: By checking one of the 'Hide Column' checkboxes, this will hide the column in the Passwords Grid from all users - so they do not need to do this under their own 'Screen Options' area. This only applies to the standard Password List page, not when searching for passwords on Passwords Home, or from within a Folder.

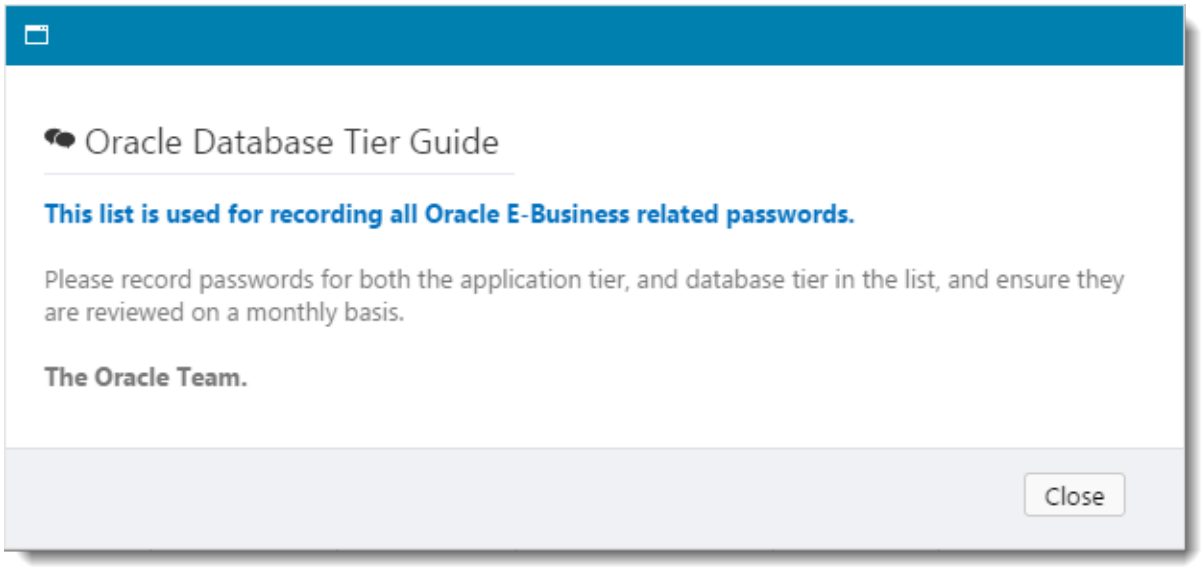


The Guide tab allows you to provide detail as to the intended use of the Password List, and can include some basic HTML style formatting.



Once you have specified the required detail in the Guide tab, your users can view the guide by clicking on the 'View Guide' button at the top right-hand side of the Password Grid.

When the click on the 'View Guide' button, they will be presenting with a popup window with the Guide.



Passwordstate has two types of APIs available (Application Programmable Interface):

- Standard API - One in which requires the use of API Keys, and is not 'user account' aware

- Windows Integrated API - One which is integrated with Active Directory and is 'user account' aware

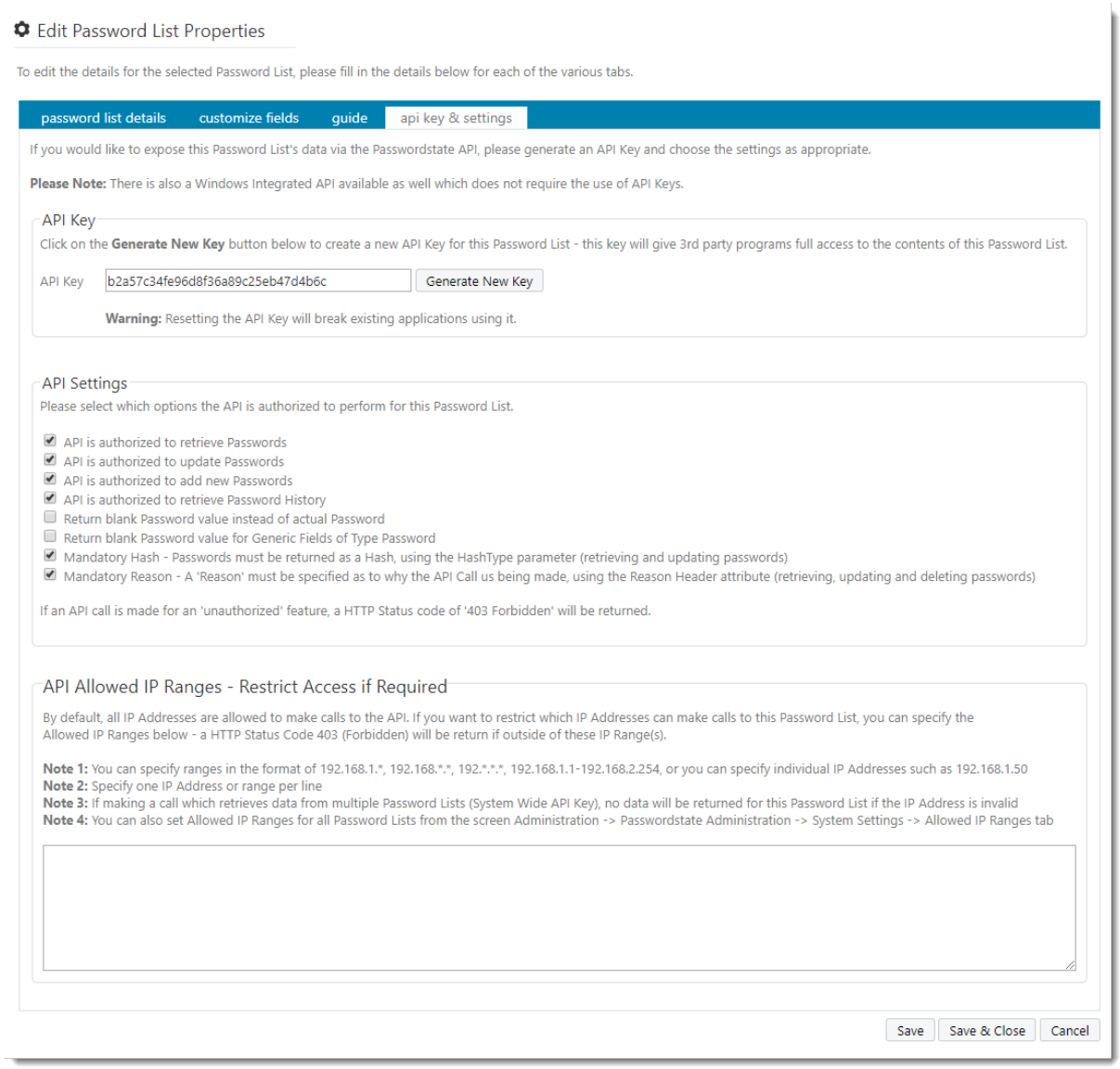
If using the Standard API, either a System Wide API Key can be used, or per Password List API Keys. If you are using the Windows Integrated version, there is no need to generate any API Keys, as the API Integrates with the logged on user account - with access being the same as the user logging into the Passwordstate UI.

In addition to specifying the API Key if required, you can set certain options to authorize various API Calls:

- To retrieve Passwords or Password History from the API
- To update Passwords via the API
- To add new Password records via the API
- To return blank values for Password fields, instead of returning plain-text Passwords - some customers may find this useful for additional security, where they can write their own code to to compare hashed strings stored in other fields to validate the password
- Whether you want to make the HashType and Reason parameters mandatory when making calls to this Password List
- Allowed IP Ranges - in addition to the System Wide Setting for restricting access to the API via trusted network ranges, you can also specify IP restrictions for individual Password Lists as well

Caution: It is imperative that you take great precautions in ensuring the API Key is not exposed to any users who should not have access. Doing so means they have unrestricted access to all the API function calls relevant to the Password List.
Note: If an API Key is set to restrict retrieving of passwords, then any API Calls which retrieve passwords from more than one Password List at a time will simply ignore Password Lists which have this setting - as opposed to returning a HTTP Status code of '403 Forbidden'

For more information about the functions the Passwordstate API can perform, please reference the 'Web API Documentation' from the Help navigation menu within Passwordstate.



2.1.1.2.7.4 Save Password List as Template

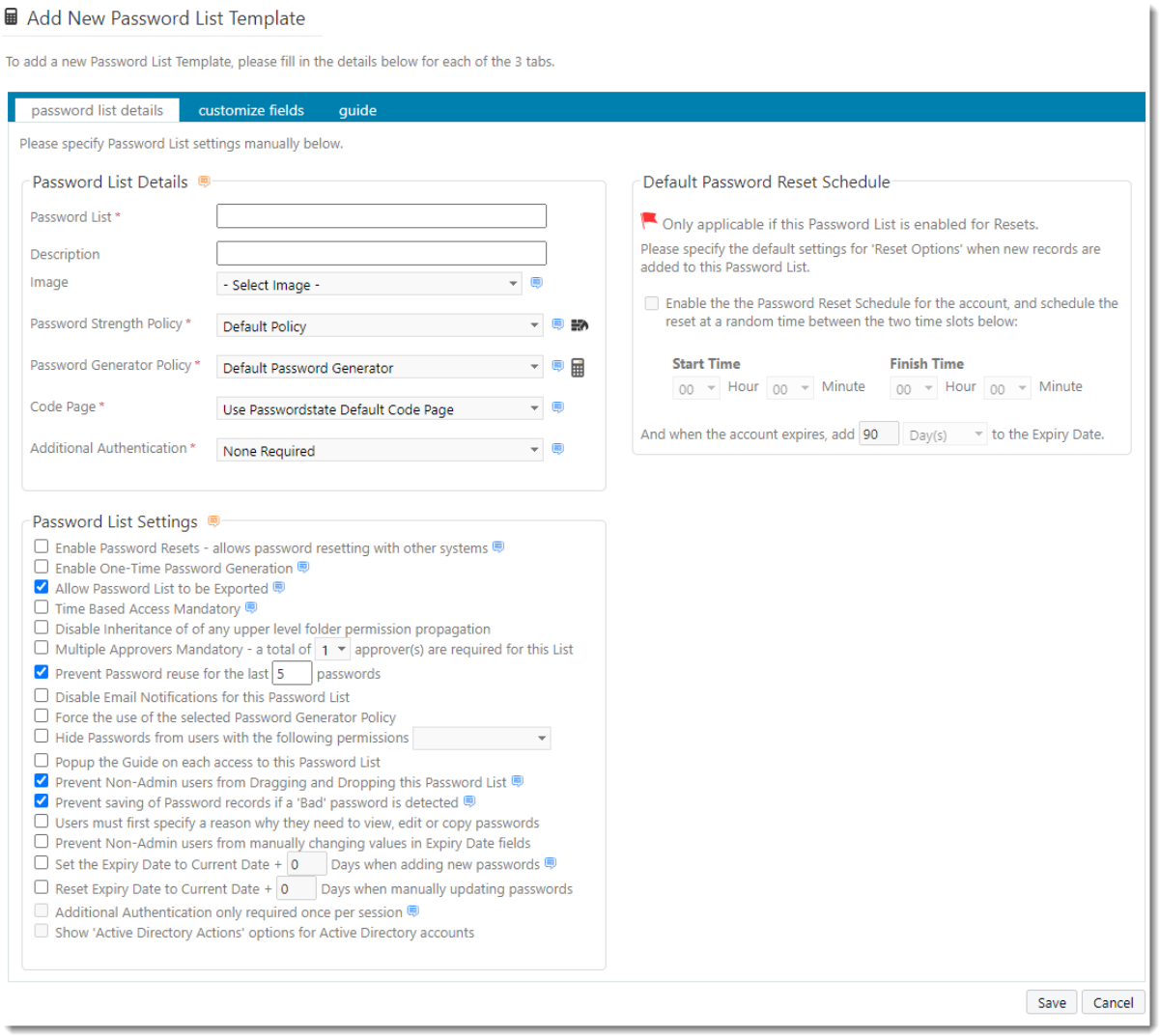
Password List Templates can be used for applying consistency to the settings for your Password Lists, either as a once of when you are creating or editing Password Lists, or on an ongoing basis when you link Password Lists to Templates (Linked Password Lists).

When you click on the menu item 'Save Password List as Template', you will see a screen very similar to the Add/Edit Password List screen, with a few small exceptions:

- The options under 'Copy Details and Settings From' is not visible or relevant
- The options under 'Copy Permissions From' is not visible or relevant
- The API Key tab is missing, as each Password List must have it's own unique API Key

Excluding the exceptions above, each of the settings on the various tabs is the same as the Add/Edit Password List screen, and you can view each of the documentation for them here - Password List Details Tab, Customize Fields Tab & Guide Tab.

Once you have saved the Password List's setting as a template, you can access them from here - Password List Templates.

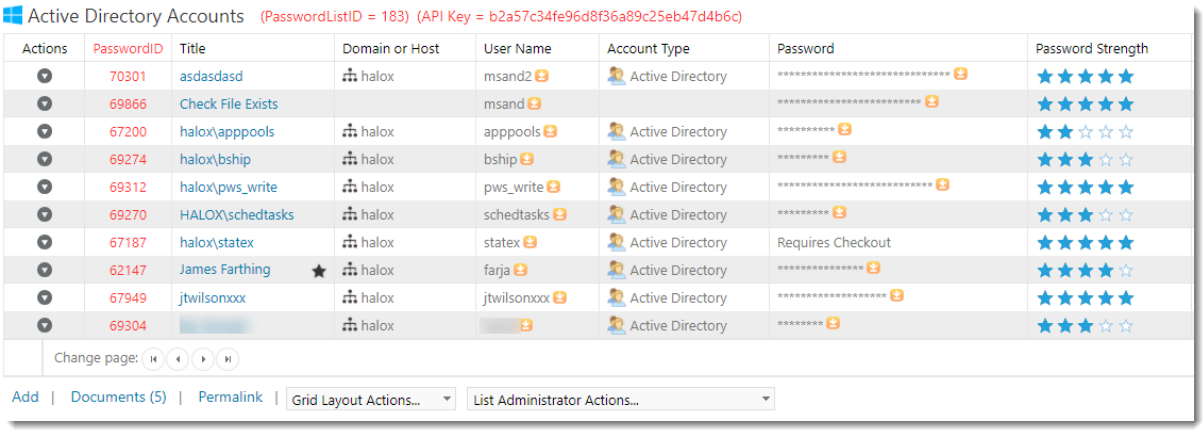


2.1.1.2.7.5 Toggle Visibility of Web API IDs

When working with the Passwordstate API, you will often need to know various ID values for Password Lists (PasswordListID) and Password records (PasswordID), to perform one or more of the API Calls. By default, these ID values are not exposed within the web interface of Passwordstate, but they can be accessed using the 'Toggle Visibility of WEB API IDs' menu item.

When you select this menu option, the ID values will be shown on the screen, and can be again hidden by clicking on the same menu item.

For more information about the functions the Passwordstate API can perform, please reference the 'Web API Documentation' from the Help navigation menu within Passwordstate.

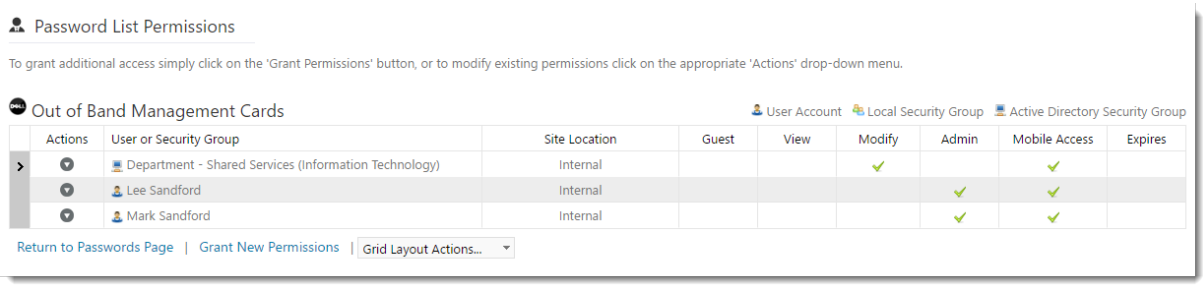


2.1.1.2.7.6 View Password List Permissions

When you click on the 'View Password List Permissions' menu item, you will be directed to a screen which shows what permissions have been applied at the Password List Level.

You can grant access to either user accounts or security groups, and the types of permissions you can apply are:

- Guest - is granted to a user when they don't have access to the Password List, but are granted permissions to an individual Password record within the Password List
- View - only allows read access to Passwords within the Password List
- Modify - by default, allows the user to view, add, update and delete Password records Note: The Security Administrators can change the behavior of 'Modify' permissions on the page Administration -> System Settings -> Password List Options
- Admin - Provides modify access, plus all the features under the List Administrator Actions drop-down menu
- Mobile Access - In addition to access Password Lists through the web interface, you can also grant Mobile App Access for each of the different permissions as well

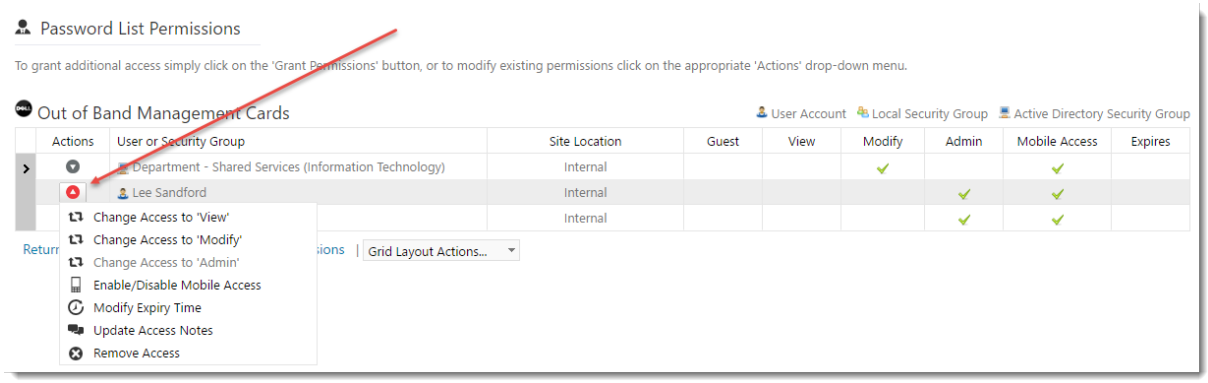


From the 'View Password List Permissions' screen, you have the following features available:

Password List Permission Actions

When you click on the 'Actions' menu item for access which has been granted to a user or security group, you can:

- Change the permissions to View, Modify or Admin
- Enable or disable Mobile App access for the permission
- Set or modify the time in which their access will be removed - if required
- Allow you to update a notes field as to why the access was given
- Or remove the access altogether



Grant New Permissions

To grant new permissions to a user's account, or to the members in a security group, you can click on the Grant New Permissions button.

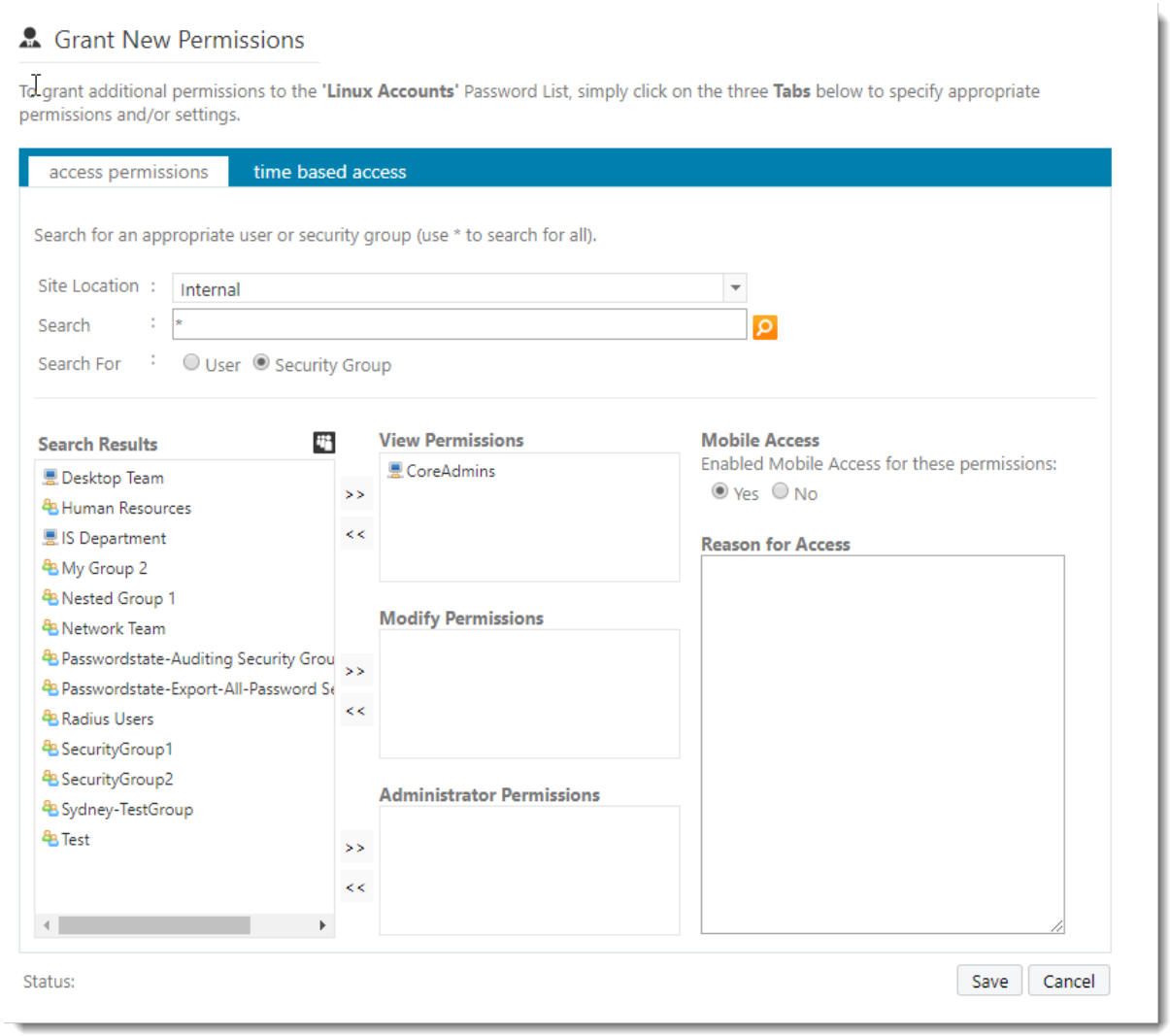
You can grant new permissions to either User Accounts, or members of a Security Group - either local Security Groups within Passwordstate, or Active Directory based Security Groups.

As you apply new permissions for users, they will also be granted permissions to any upper-level Password Folders the Password List may be nested beneath - there may be an exception to this if a Folder is configured to manager permissions manually, but this is the default setting.

When granting new permissions (access) to a Password List, there are three tabs of features available to you:

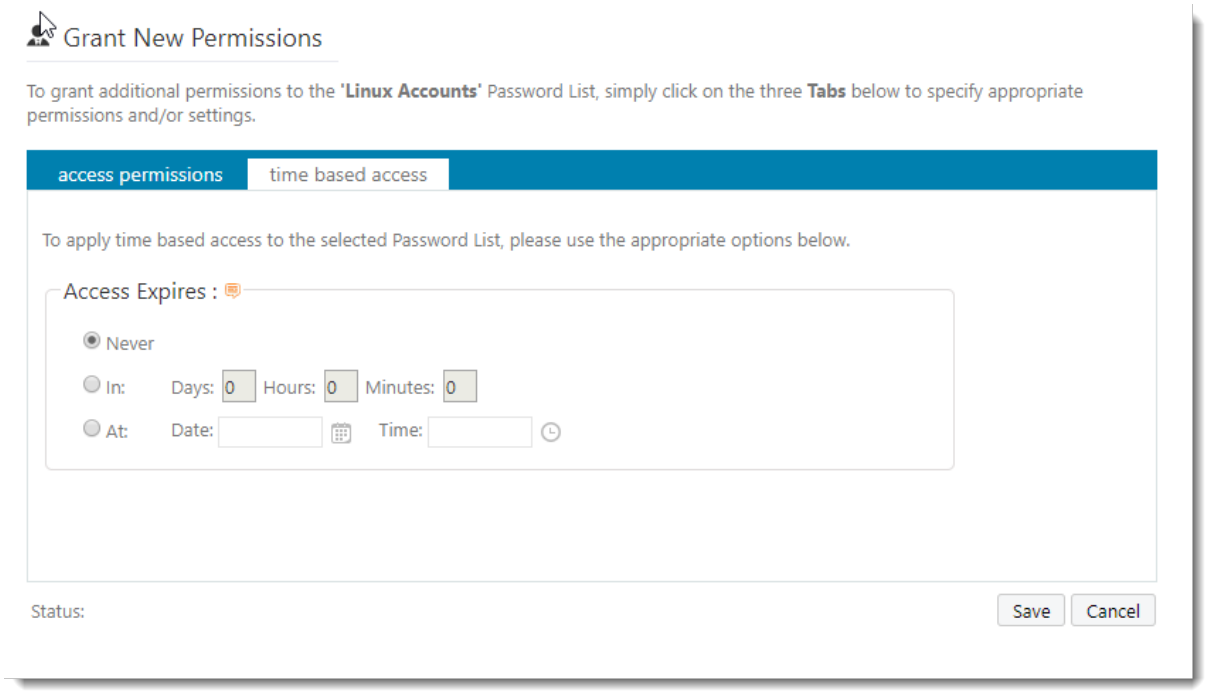
Access Permissions

The 'Access Permissions' tab allows you to search for users and/or security groups, and either grant View, Modify or Admin Access. You can also enable or disable Mobile App Access for any permissions added here.



Time Based Access

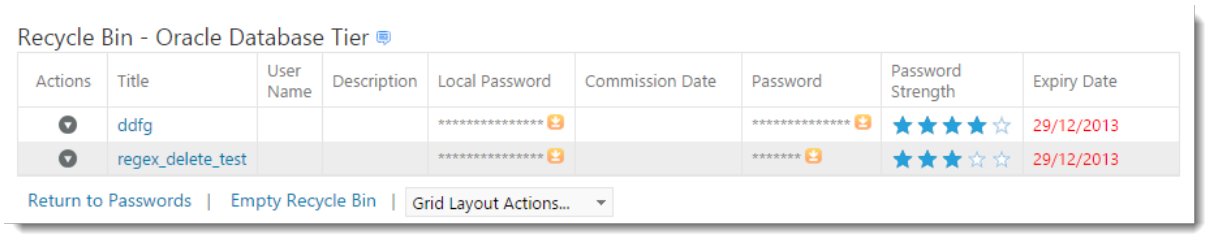
If you require the permissions to be removed after a certain period of time, or at a set time, you can specify the appropriate time period on the 'Time Based Access' tab.

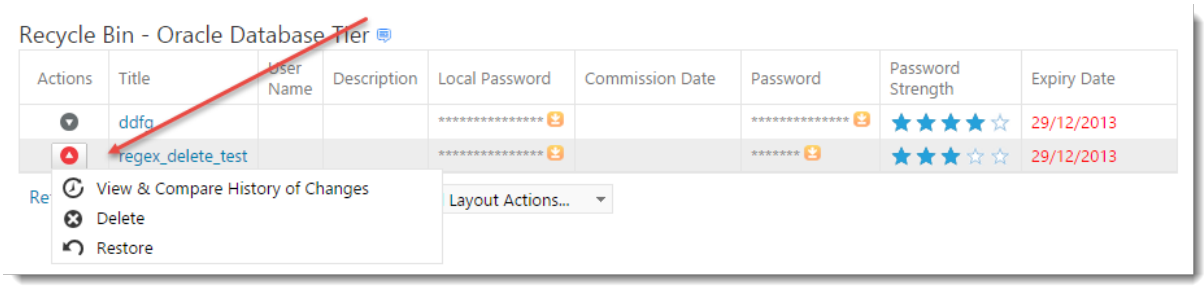


2.1.1.2.7.7 View Recycle Bin

When a Password record is deleted by the user, it is moved to the Recycle Bin, where it can be later restored or permanently deleted.

Note: Clicking on 'Empty Recycle Bin, or 'Delete' from the Actions drop-down menu will permanently deleted the record(s), along with other related data.
Note: There is an option Security Administrators can set on the page Administration -> System Settings -> Password Options Tab which can also permanently delete linked Password records as well if required - by default, this is disabled





2.1.2 Add Folder

Folders are used to simply logically group other Folders or Password Lists - similar to a directory structure on a file system.

When adding a new folder, there are only a few options you must specify, and they are:

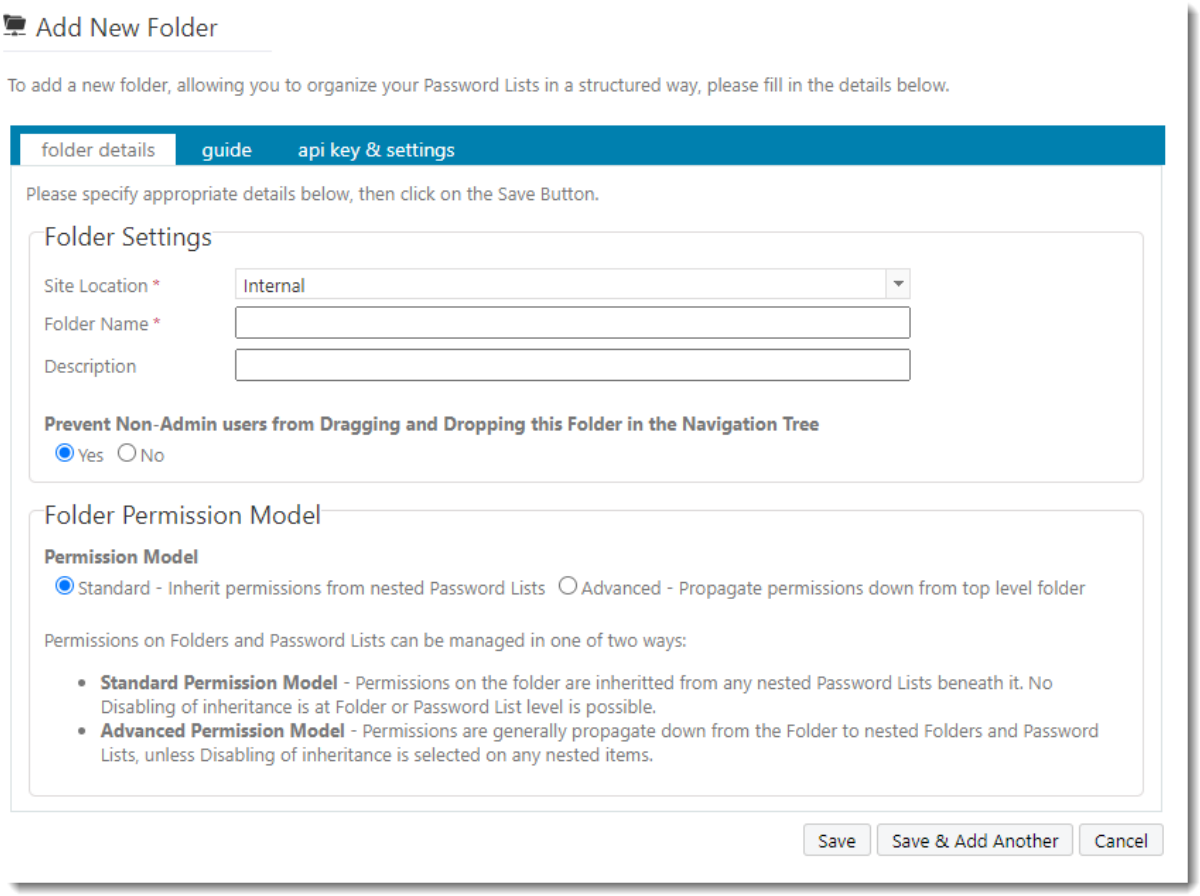
Site Location	By default, the "Internal" site location will be the most common, unless you have purchased a subscription for the Remote Site Locations module
Folder Name	The name of the Folder as it will be displayed in the Navigation Tree
Description	A description of the folder describing it's purpose
Prevent Non-Admin users from Dragging and Dropping this Password Folder in the Navigation Tree	You can prevent users with Non-Admin rights to the Folder from dragging-and-dropping the position of the folder in the Navigation Tree
Folder Permission Model	Select from one of the two permission models available

Folder Permissions Model

There are two types of permission models available in Passwordstate:

- Standard - the folder will inherit permissions from any nested Password Lists beneath it
- Advanced - the folder will propagate permissions down to all nested Folders and Password Lists

When using the Advanced Permission Model, it's also possible to select the option to "Disable Inheritance of any permissions from upper-level folders" for any nested Folders or Password Lists. By doing this, you can have different permissions set, in this propagating structure.

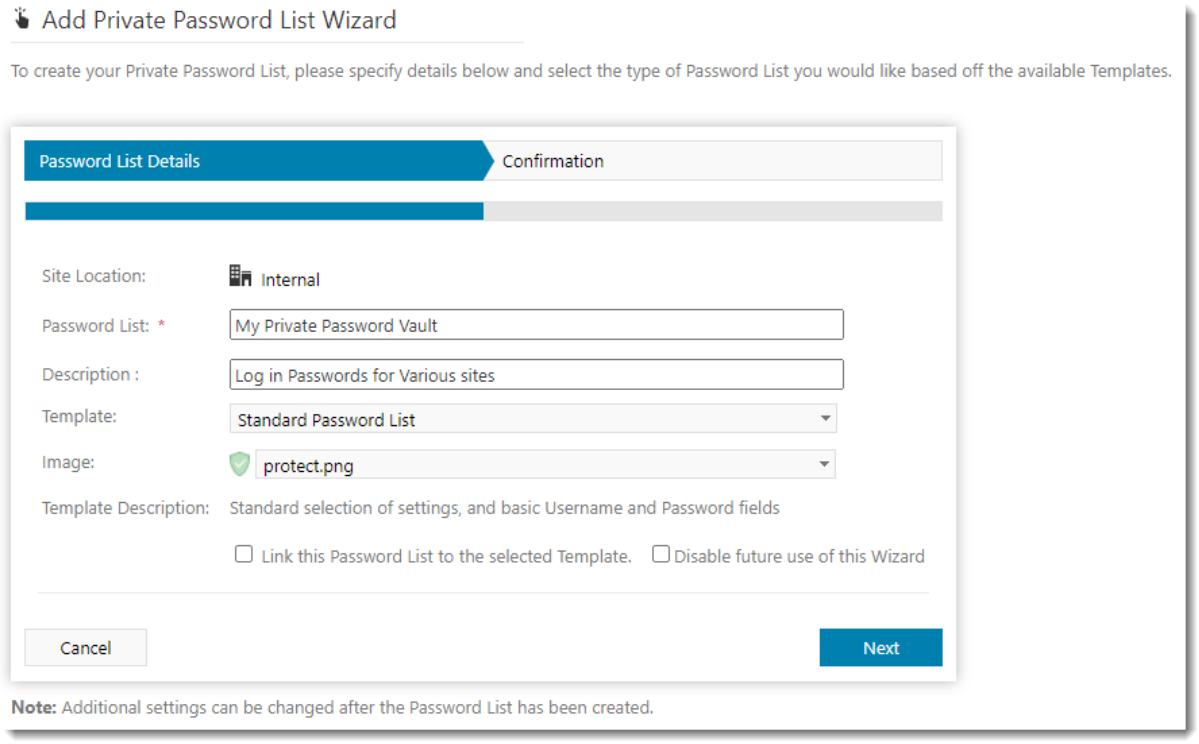


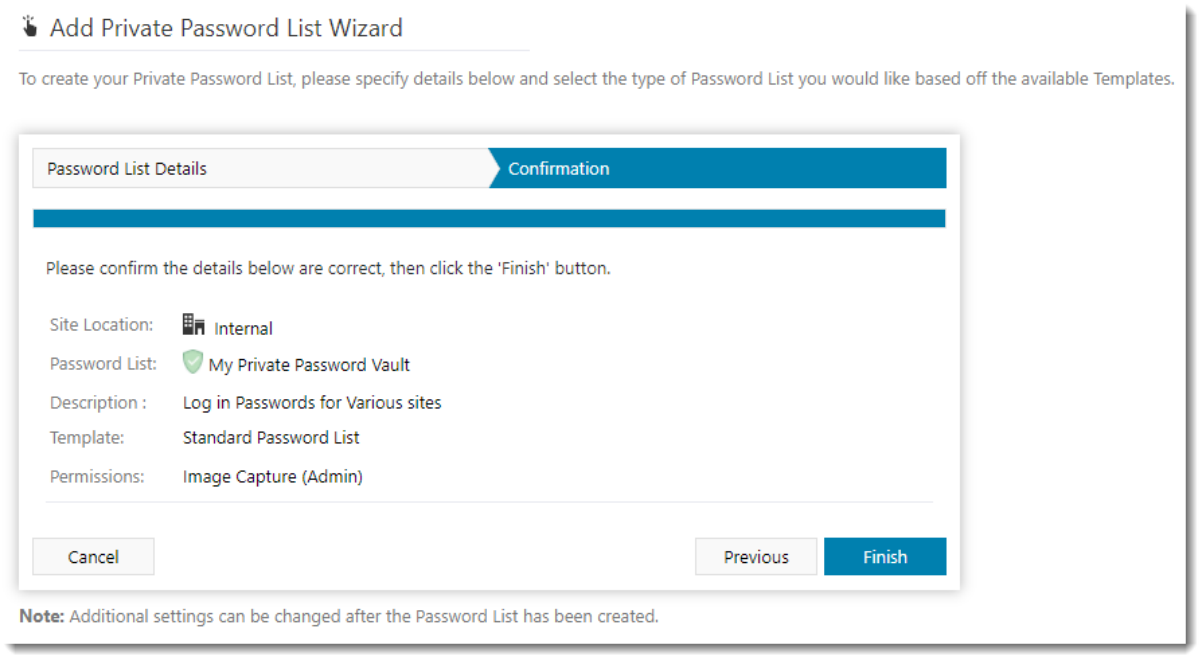
2.1.3 Add Private Password List

Private Password Lists are almost identical to Shared Password Lists, except the only person who can see a Private Password List and its contents, is the person who created it .

One other difference to Shared Password Lists is 'permission' related options - any options which relates to permissions will be disabled, as you cannot grant permissions to other users to a Private Password List.

When creating the Private List, you will by default be presented with the following Add Password List Wizard, where you can specify basic details about your Password List, based on settings from one of the available Password List Templates.



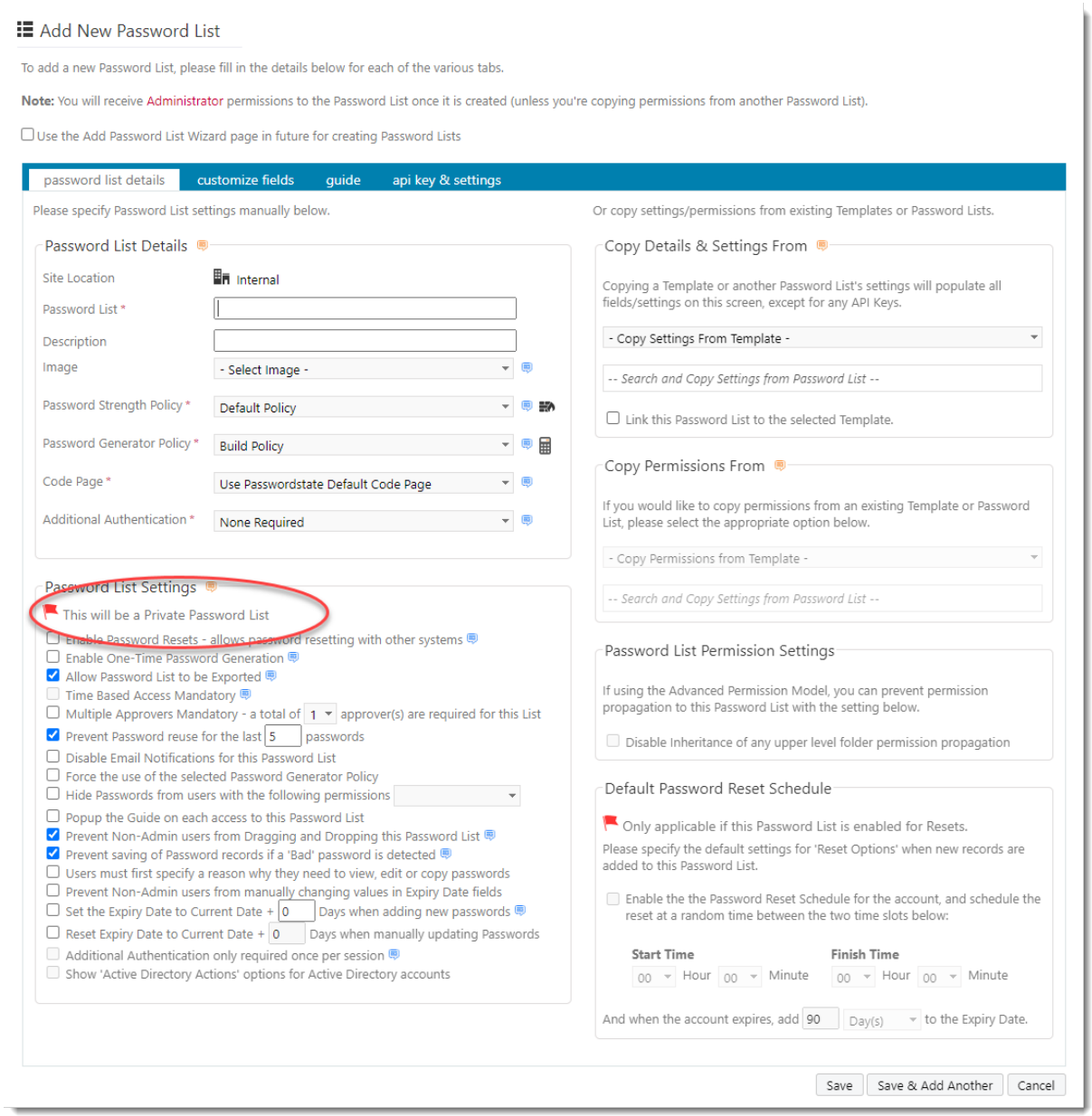


If you would like more granular settings when creating your Password List, then you can tick the option to disable future use of the Wizard, or your Passwordstate Security Administrators can also control this on the screen Administration -> Feature Access -> Password List Options tab.

When the Wizard is disable, then all the settings will be available to you, as per the screenshot and detail below.

As the majority of settings and features available when creating a Private Password List are the same as Adding/Editing a Shared Password List, you can view the documentation for each of the tabs here - Password List Details Tab, Customize Fields Tab, Guide Tab & API Key & Settings Tab.

Note 1: Be careful if you choose the 'Use Separate Password' Additional Authentication option for your Private Password Lists. If you forget this Password, Security Administrators of Passwordstate are not able to reset it, meaning you will have lost access to the Password List.
Note 2: When you add a new Private Password List, your account will be granted Admin rights to the Password List, and it will be positioned in the Navigation Tree just below the selected node (Password List or Folder). You can then drag-and-drop the Password List to any position in the Navigation Tree that you like.
Note 3: The Site Location for Password Lists will always be 'Internal' if created in the root of Passwords Home, otherwise if nested beneath a Folder, it will use the same Site Location the Folder is set at.

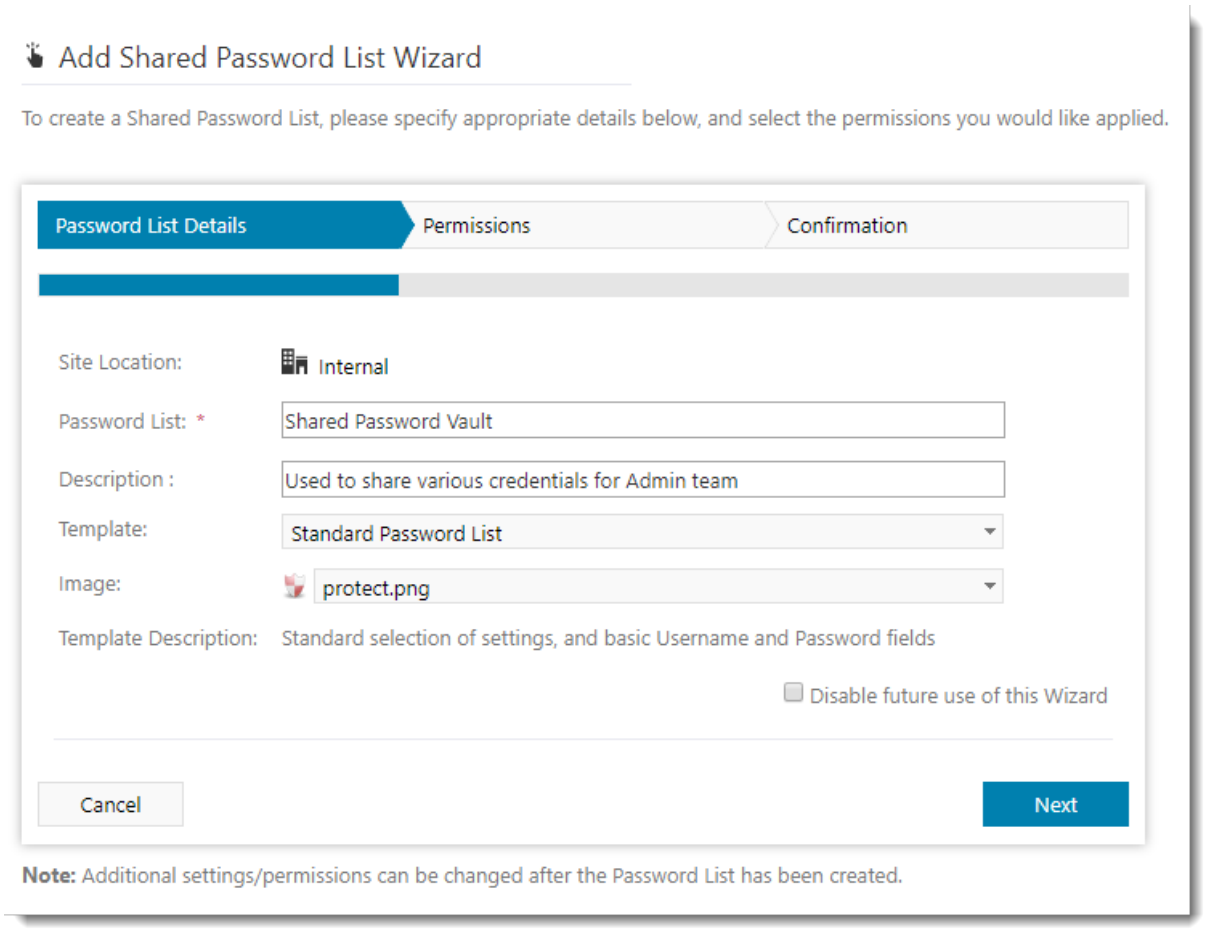


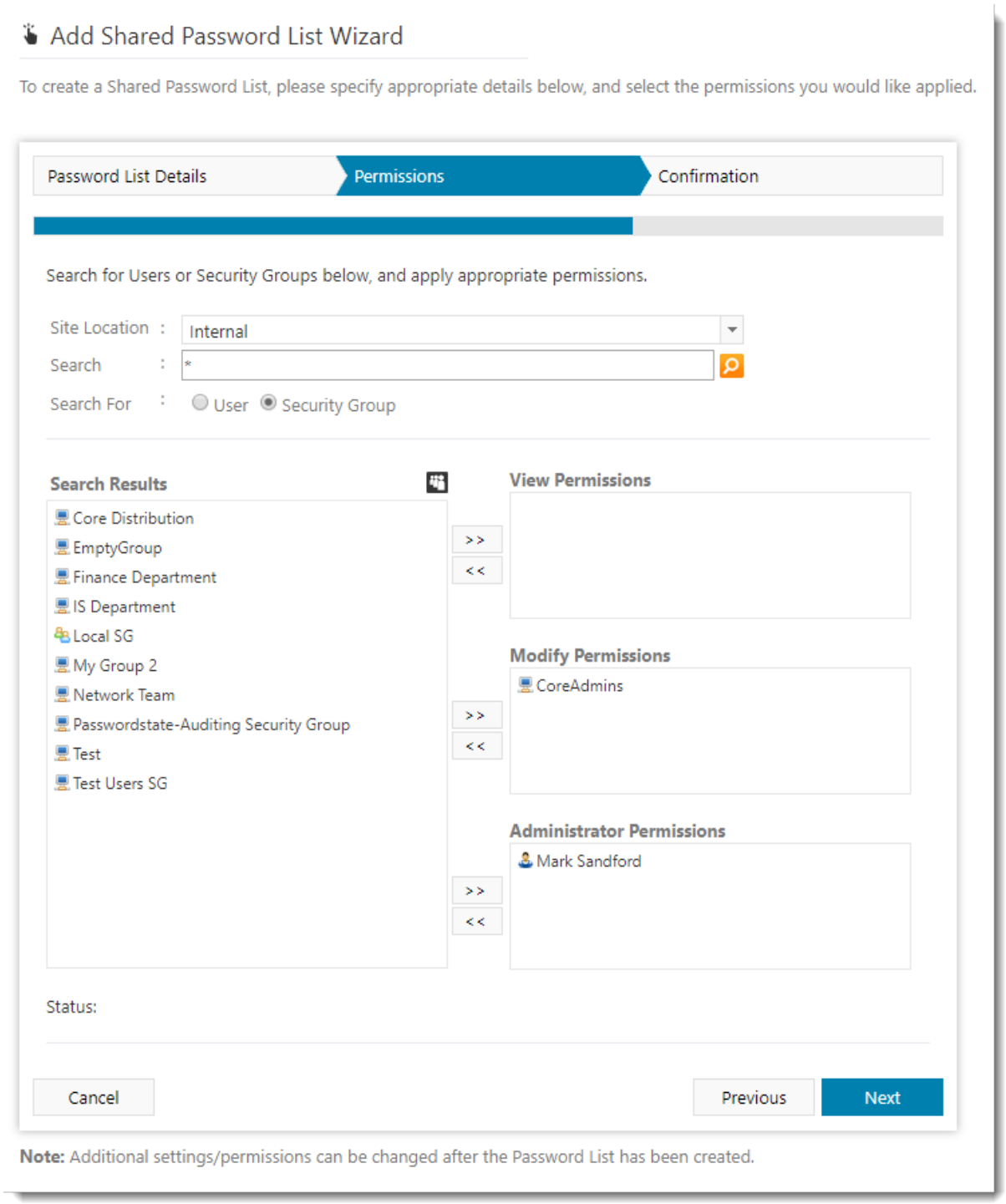
2.1.4 Add Shared Password List

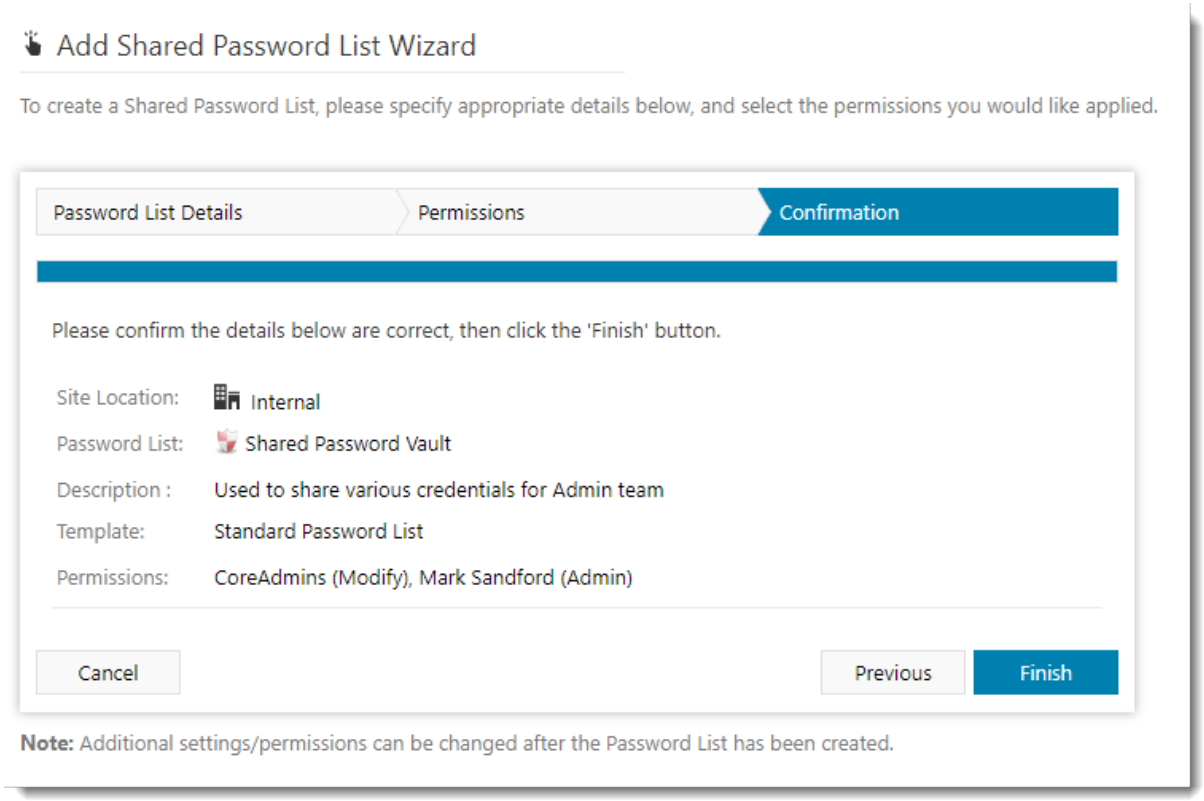
Shared Password Lists are used to share Passwords with teams of people, and allows various types of permissions to be applied - View, Modify or Administrator.

Once a Shared Password List is created, you can then start adding passwords to it, and then sharing those passwords with other team members.

When creating the Private List, you will by default be presented with the following Add Password List Wizard, where you can specify basic details about your Password List, based on settings from one of the available Password List Templates.





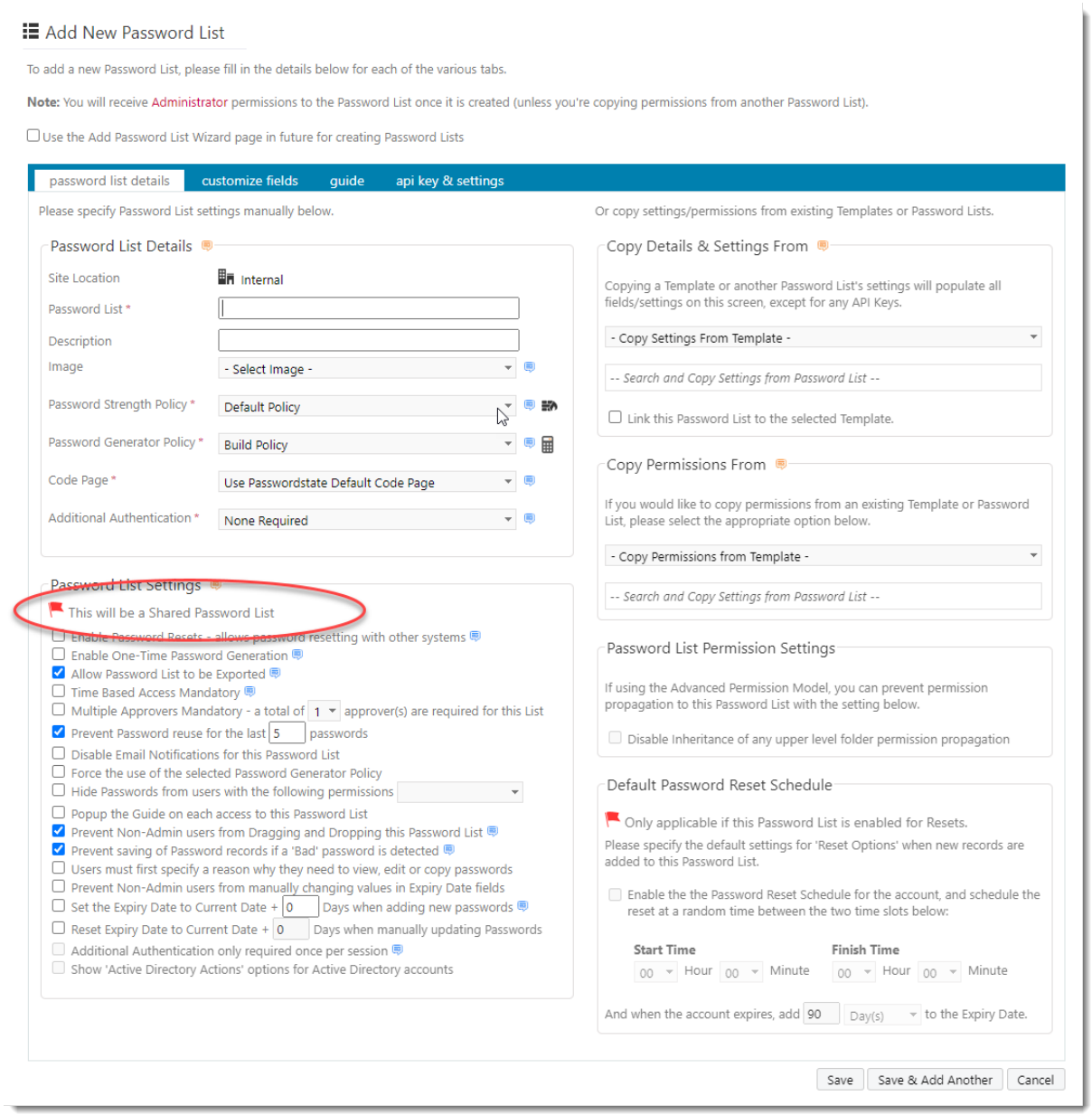


If you would like more granular settings when creating your Password List, then you can tick the option to disable future use of the Wizard, or your Passwordstate Security Administrators can also control this on the screen Administration -> Feature Access -> Password List Options tab.

When the Wizard is disable, then all the settings will be available to you, as per the screenshot and detail below.

As the settings and features available when creating a Shared Password List are the same as Editing a Shared Password List, you can view the documentation for each of the tabs here - Password List Details Tab, Customize Fields Tab, Guide Tab & API Key & Settings Tab.

Note 1: When you add a new Shared Password List, by default your account will be granted Admin rights to the Password List (Security Administrators of Passwordstate can change this setting though), and it will be positioned in the Navigation Tree just below the selected node (Password List or Folder). You can then drag-and-drop the Password List to any position in the Navigation Tree that you like.
Note 2: The Site Location for Password Lists will always be 'Internal' if created in the root of Passwords Home, otherwise if nested beneath a Folder, it will use the same Site Location the Folder is set at.

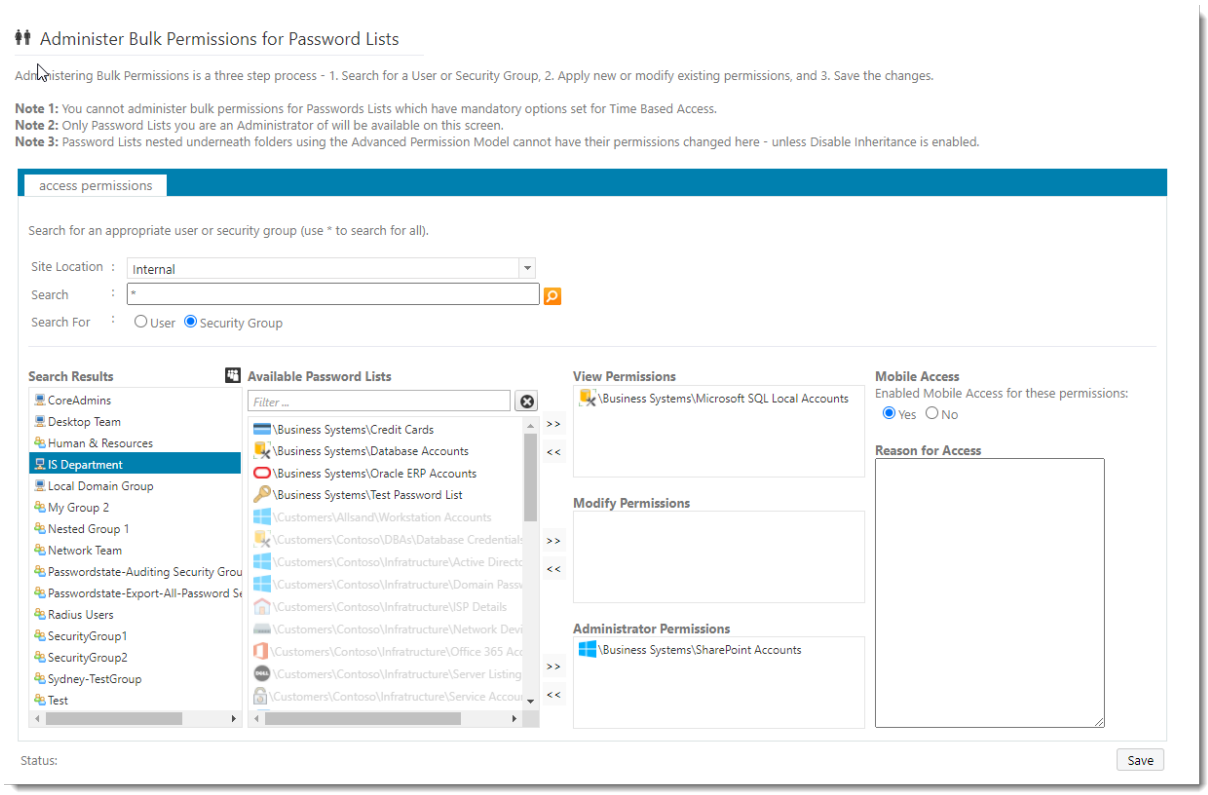


2.1.5 Administer Bulk Permissions

The standard method of apply permissions to a Password List is via the Grant New Permissions button for each individual Password List.

The Administer Bulk Permissions feature allows you to search for either a User Account or Security Group, and then apply permissions to multiple Password List at once. When you search for a User Account or Security Group, it will show the Password Lists they don't have access to (Available Password Lists), and the Password Lists they already have access to (either in the View, Modify or Administrator Permissions text boxes).

Note: A couple things to note about this feature - 1. Only Password Lists will show which you have Administrator rights to, and 2. Any Password Lists which have Time-Based Access set as mandatory, will be disabled in the search results.

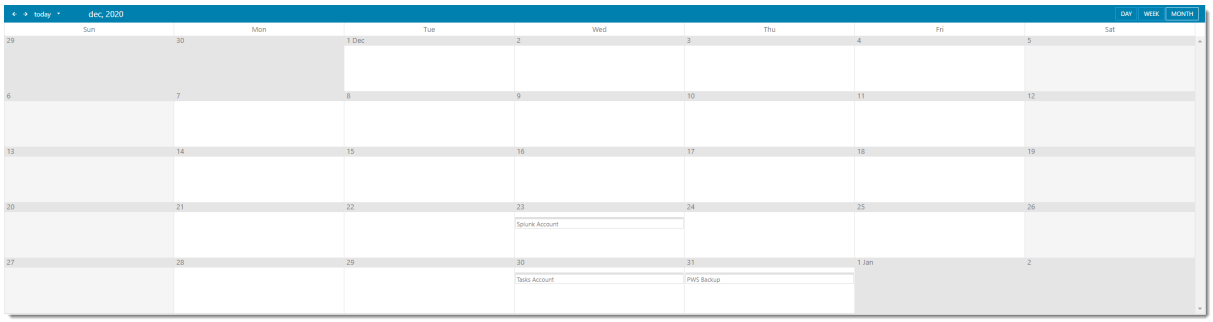


2.1.6 Expiring Passwords Calendar

The Expiring Passwords Calendar feature provides you wish a graphical calendar view of when Passwords are set to expire - based on the Expiry Date field.

On this calendar you can:

- Navigate back and forth by Day, Week or Month
- Click on the Password record allowing you to edit it's details i.e. reset the password and the Expiry Date field if you want.



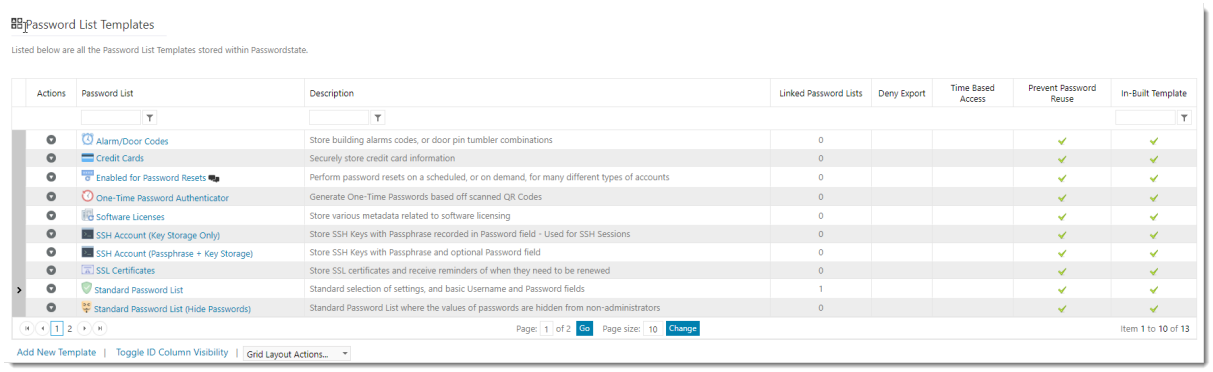
2.1.7 Password List Templates

Password List Templates can be used to apply consistency to settings for your Password Lists. They can be used in the following way:

- You can apply a Template's settings as needed (once off) when you add a new Password List, or edit an existing Password Lists' settings (Password List Details Tab)
- You can link Password Lists to a Template, and then manage all settings from the Template. When you do this, the majority of options for the Password List will be disabled when you chose to Edit Password List Details
- You can also apply permissions to a Template, and these permissions can be used for:
  - Allow other users to see the Templates via the 'Password List Templates' menu option
  - Allow other users to also modify the settings for the Template via the 'Password List Templates' menu option
  - Applying permissions to a Password List as needed (once off) when you add a new Password List, or edit an existing Password Lists' settings (Password List Details Tab)

Note: Permissions on a Template are not used when Linking Password Lists to a template - this can only be done when adding a new Password List, or editing the settings for an existing one.

You can either create Templates by clicking on the Add New Template button on this screen, or via the Save Password List as Template option for an existing Password List.



Editing a Template Settings

Editing the settings for a Template is almost identical to that of a Password List, and can be accessed via clicking on the appropriate 'Password List' hyperlink you see in the Grid above. Please reference the documentation for each of the tabs here - Password List Details Tab, Customize Fields Tab & Guide.

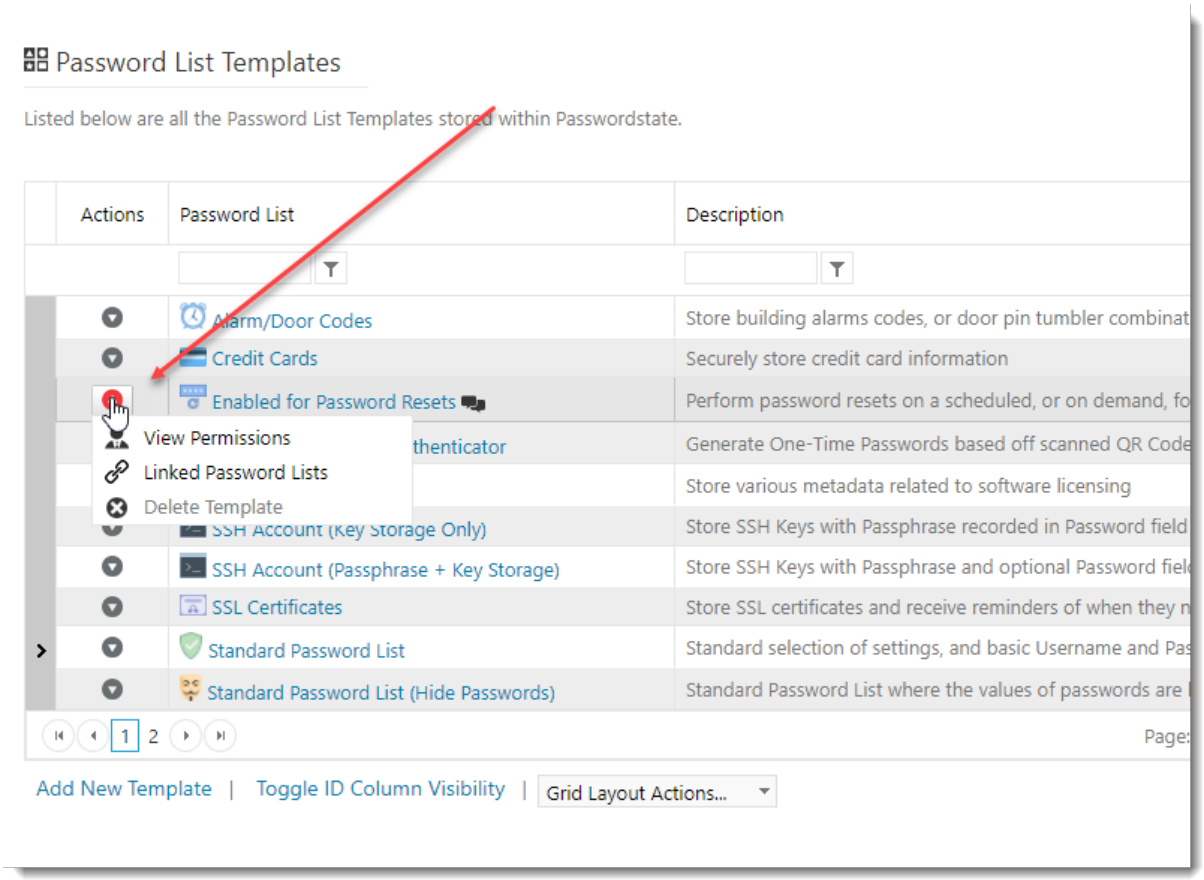
Caution: When editing a Template's settings when it is linked to other Password Lists, if you change any of the Field Types for any Generic Fields, these fields will have their data cleared/blanked in the database when you click on the 'Save' button. This is because the different Generic Field Field Types need to have their data treated differently. There are multiple warning messages within the Passwordstate as well for this, so please be aware.

Password List Template Actions

From the 'Actions' drop-down menu, you have various features available:

- View Permissions applied to the Template - this also allows you to add/update/delete permissions as required
- You can Link Password Lists to the Template
- You can delete the template

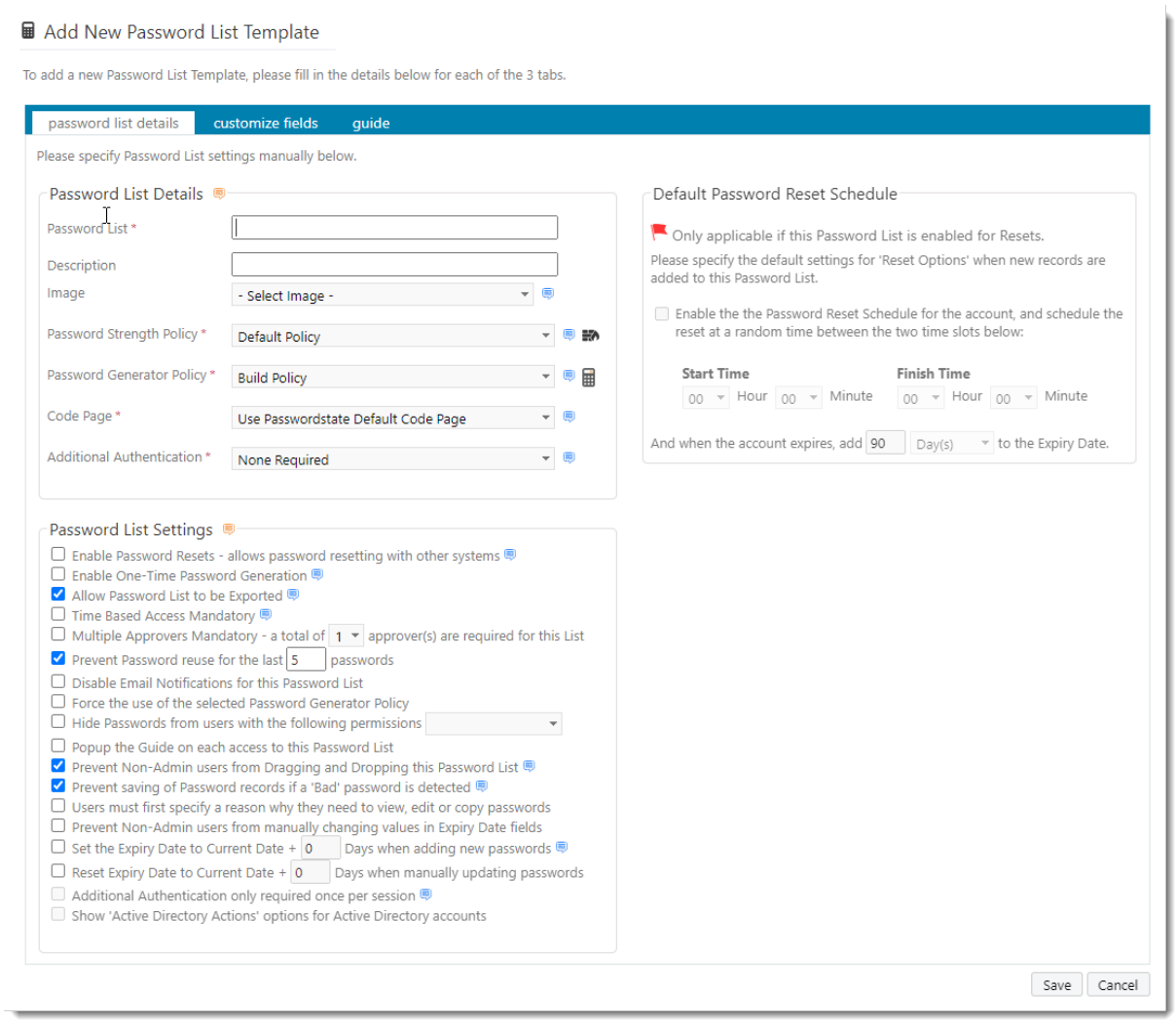
Note: If you delete a Template which is linked to one or more Password Lists, these Password Lists will bet set to use the Templates' settings as there were prior to you deleting the Template. You can then go ahead and modify the settings of the Password Lists as required.



2.1.7.1 Add New Template

You will notice from the screenshot below the settings for a Template are almost identical to a Password List, so please reference the documentation for each of the tabs here - Password List Details Tab, Customize Fields Tab & Guide Tab. One exception to this is the API Key tab, as each Password List's API Key details must be unique.

Note: When you add a new Template, you will be giving Administrator rights to it.

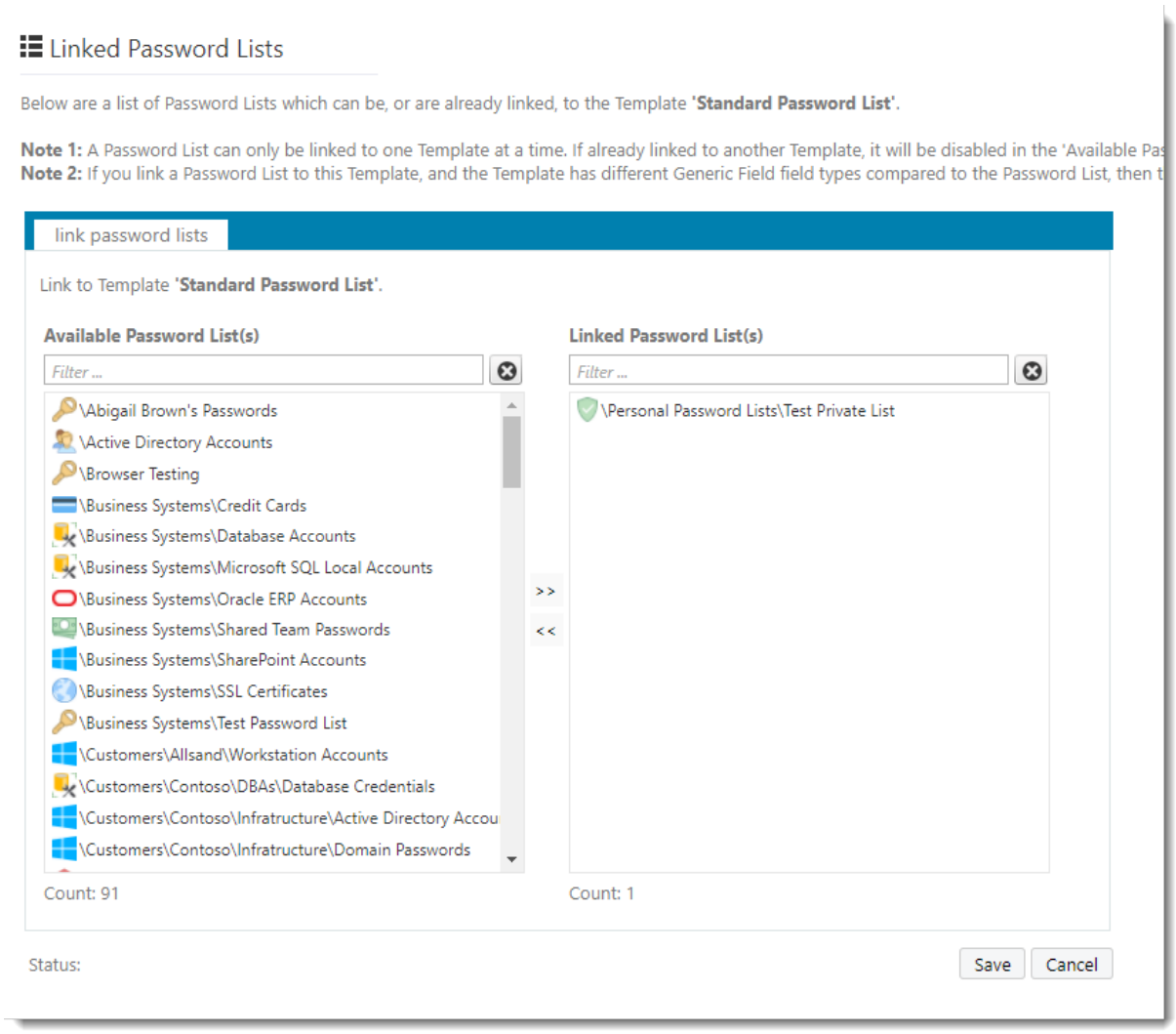


2.1.7.2 Linked Password Lists

When you link one or more Password Lists to a Template, the majority of settings for the linked Password Lists are then managed via the Template - which the exception of the details on the API Key Tab.

Linking Password Lists to a Template is very simply process - move the Password List you want to link into the 'Linked Password List(s)' text box, and click on the 'Save' button.

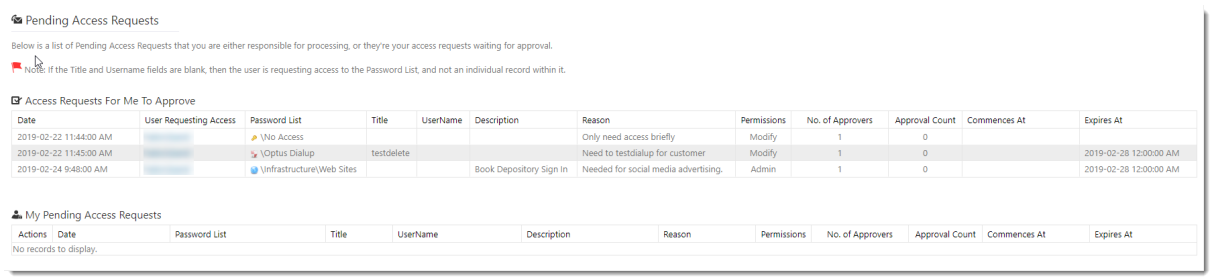
Caution: When linking Password Lists to a Template for the first time, if the Password List has some Generic Fields specified which are different to any Generic Fields specified for the Template, these fields will have their data cleared/blanked in the database when you click on the 'Save' button. This is because the different Generic Field Field Types need to have their data treated differently. There are multiple warning messages within the Passwordstate as well for this, so please be aware.



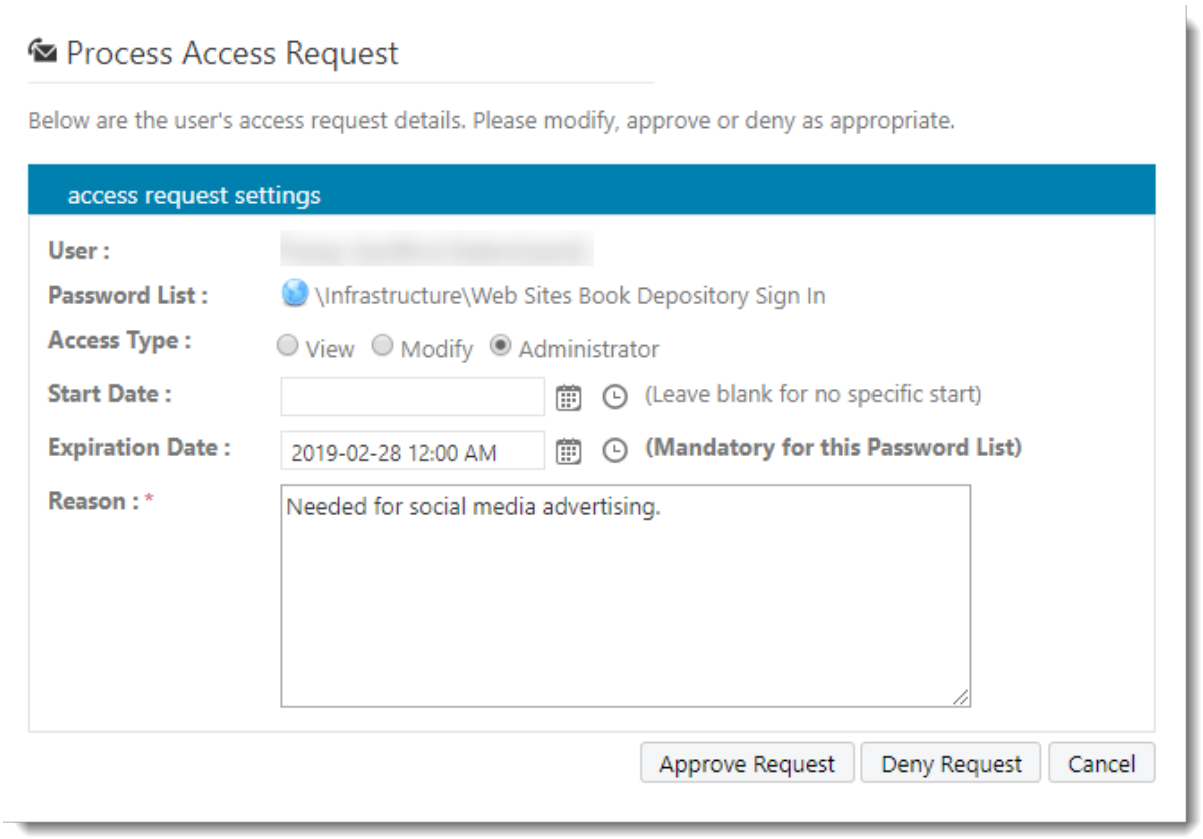
2.1.8 Pending Access Requests

The Pending Access Requests screens can be used for two purposes:

- View and process any pending access requests that have been sent to you
- View any of your own pending access requests that are waiting for approval



When an 'Approver' processes and Access Request, they can also modify various settings as per the screenshot below.

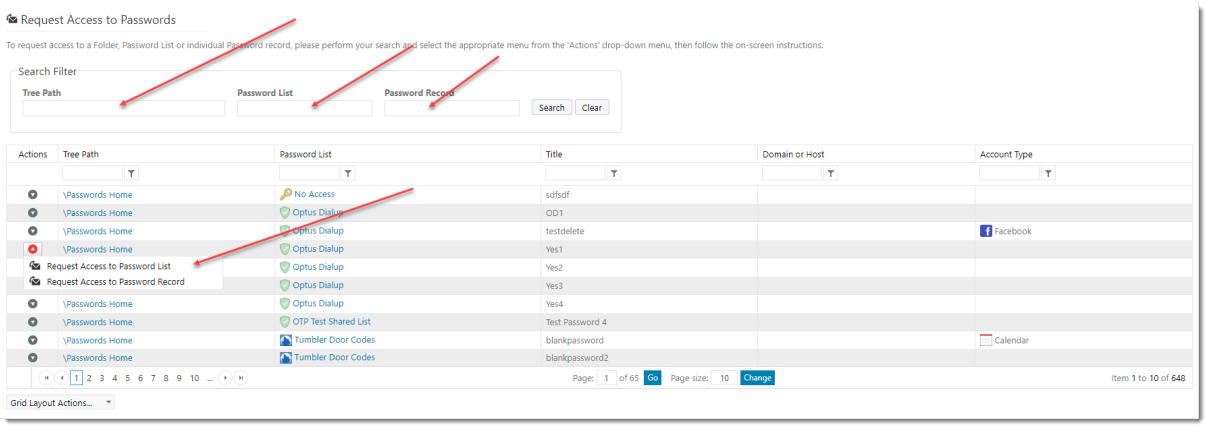


2.1.9 Request Access to Passwords

The Request Access to Passwords screen allows you to search for either a Password List, or individual password record, and request access to it.

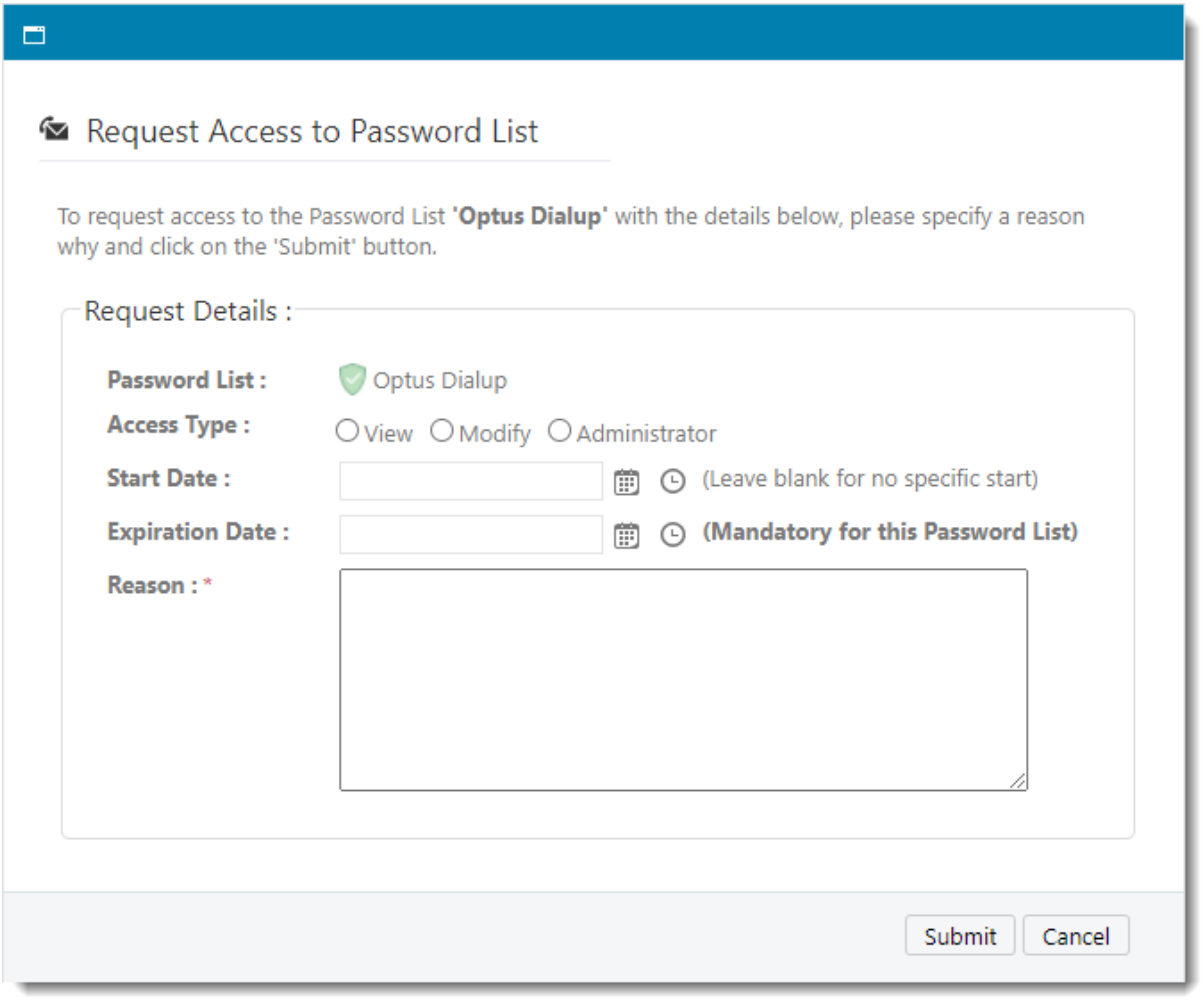
There are various filtering options based for the TreePath the Password List exists in, or on the Password List or password record as well. Once you have found the record you need, you can request access to either the Password List or Password record from the Actions menu.

Note: On the screen Administration -> Passwordstate Administration -> System Settings -> Passwords Options tab, there are settings to hide the Username, Description and Notes fields on this screen.



When you request access, you will be given various options for what level of access you require, and the start and expiration date for access (if applicable). You must also supply a reason as to why you are requesting this level of access, so the approver(s) can determine if they should approve or deny the request.

Once you request has been processed, you will be notified via email - or you can monitor the approval process on the Pending Access Requests screen.

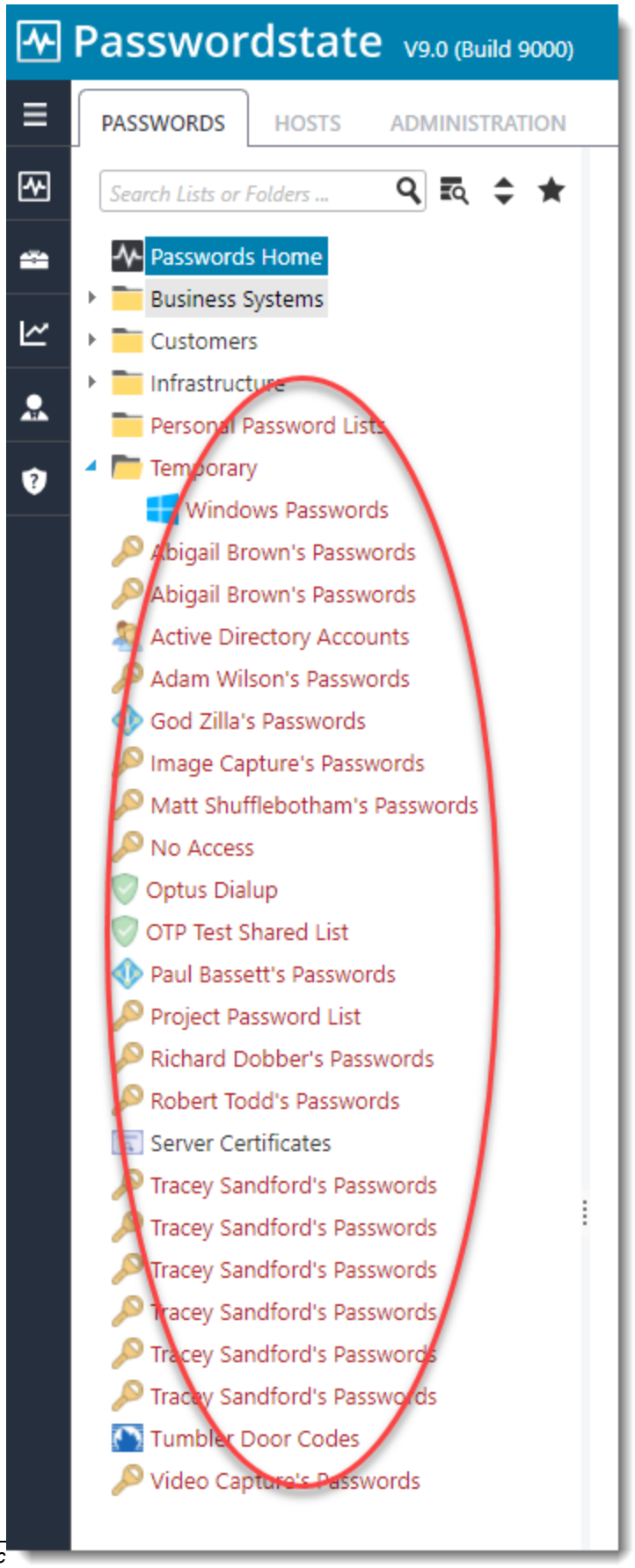


2.1.10 Toggle All Password List Visibility

By clicking on the 'Toggle All Password List Visibility' menu option, all Shared Password Lists will be displayed in the Navigation Tree.

The Password Lists you do not have access to will be colored in Red, and by clicking on the Password List in the Navigation Tree, you will be given the opportunity to request access to the Password List.

Caution: Depending on how many Password Lists and Folders are recorded in your database, making them all visible on the screen may cause delays in rendering the Navigation Tree - it depends on entirely how much HTML needs to be rendered. If this is of a concern, your Security Administrators can disable this feature from the Administration -> Passwordstate Administration -> Menu Access screen.


Passwordstate V9.0 (Build 9000)
PASSWORDS
HOSTS
ADMINISTRATION
Search Lists or Folders ...
Passwords Home
Business Systems
Customers
Infrastructure
Personal Password Lists
Temporary
Windows Passwords
Abigail Brown's Passwords
Abigail Brown's Passwords
Active Directory Accounts
Adam Wilson's Passwords
God Zilla's Passwords
Image Capture's Passwords
Matt Shufflebotham's Passwords
No Access
Optus Dialup
OTP Test Shared List
Paul Bassett's Passwords
Project Password List
Richard Dobber's Passwords
Robert Todd's Passwords
Server Certificates
Tracey Sandford's Passwords
Tracey Sandford's Passwords
Tracey Sandford's Passwords
Tracey Sandford's Passwords
Tracey Sandford's Passwords
Tracey Sandford's Passwords
Tumbler Door Codes
Video Capture's Passwords

2.2 Tools Menu

There are three options available under the Tools menu.

Account Discovery	Allows you to add/view/edit various Account Discovery Jobs, for finding accounts in use on your network
Have I Been Pwned Password Check	Allows you to perform adhoc password checks against the Have I Been Pwned API to determine if the password has been used in a known compromised data breach in the past
Import Passwords	Import password from different sources into Passwordstate
Password Generator	Allows you to generate one or more randomly generated passwords
Password Resets in Progress	This screen shows any Password Resets which are sitting in the queue, pending any processing.
Self Destruct Message	Allows you to generate and send a Self Destruct email message to another user

2.2.1 Account Discovery

The Account Discovery Menu allows you to perform various account discoveries on your network, based on Host records which have been added under the Hosts tab area.

The following Account Discovery jobs are available:

1. Active Directory Accounts
2. Cisco IOS Accounts
3. Fortigate Accounts
4. HP H3C Accounts
5. Juniper Junos Accounts
6. Linux and Mac Accounts
7. MS SQL Database Accounts
8. MySQL Database Accounts
9. Oracle Database Accounts
10. PostgreSQL Database Accounts
11. SonicWALL accounts
12. Windows Dependency Accounts - Windows Services, IIS Application Pools and Scheduled Tasks which are configure to use a domain account as their identity
13. Windows Local Admin Accounts

Note 1: Please refer to the document 'Password Discovery Reset & Validation Requirements.pdf' for system requirements for the Discovery Process to work - it relies on PowerShell in your environment to function

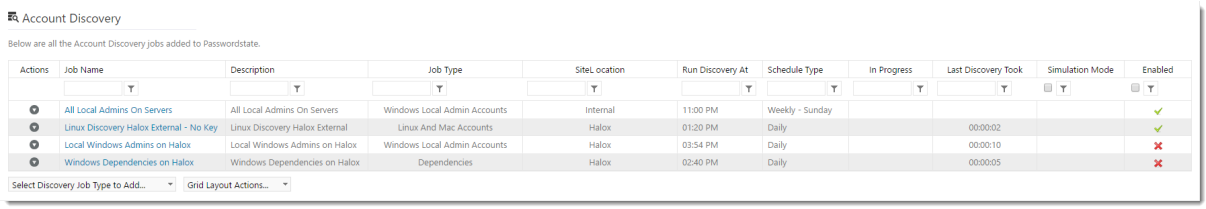
Note 2: If you only want a Discovery Job to execute once, you can disable it in the 'Actions' dropdown menu

Note 3: By ticking the 'Simulation Mode' checkbox, it will perform the discovery and email you the results, without making any changes to the Passwordstate database.

Note 4: If discovering accounts on a Mac, the option to reset the password on discovery will be ignored, as another account (the Privileged Account Credential) cannot update the keychain for a different account - this is by design by Apple

Note 5: For the 'Active Directory Accounts' discovery job, this job should not be used for Privileged AD Accounts which are used on Windows Services, IIS App Pools and Scheduled Tasks - you should use the Windows Dependency Discovery Job for that purpose

Note 6: For the 'MS SQL Database Accounts' discovery job, the Privileged Account to be used to can be either a SQL Account, or an Active Directory account



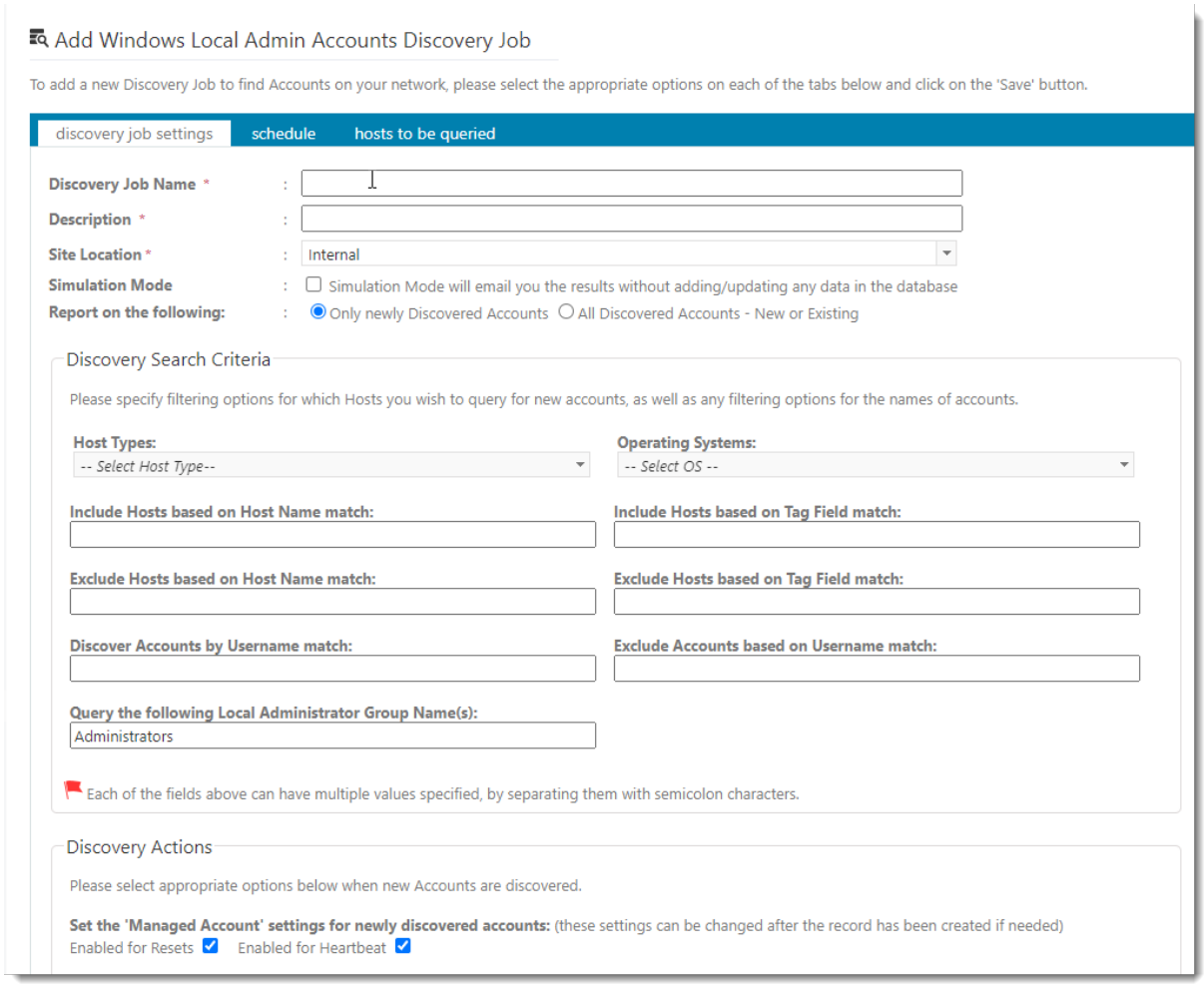
Discover Accounts

When discovering Accounts on various Hosts, there are many options available to you. In particular:

- You can filter on the type of Hosts you want to query, based on the Operating System type, or any sort of Host Name wildcard match
- If a new account is found, you can specify which Password List to store the password record into. If the account is found in another Password List when the discovery executes, it will not add in a duplicate record
- As it's not possible to decrypt most passwords for discovered accounts, you will need to specify what password will be recorded in Passwordstate initially for the account, or you can generate a random one. You also have the option to perform a password reset for any newly discovered accounts, and the password value for these accounts will be set to what's selected here - either a static password, or a randomly generated one
- When new records are added to the selected Password List, you have the option to also specify some detail for the Title and Description fields.
- You also need to specify the Privileged Account Credentials to use when interrogating your Hosts on the network - this account will need sufficient privileges to interrogate the Host for local accounts - generally an account with Admin (elevated privileges) is required here
- If you do not wish to automatically configure the discovered accounts to perform scheduled resets, you can set the 'Managed Account' option to No. Then later within the Password List, you can enable this option for one or more records at a time - either by editing individual records, or using the Bulk Update Password Reset Options feature
- There are also various options where you can set the Check In/Out feature as well
- When applying permissions to the Job after it is created, whoever is given access can then administer the job, as well receive an emails with the results of the job execution

Note : It is strongly recommended that you set the **'Default Password Reset Scheduled'** for the Password List (Password List Details Tab) prior to any new records being discovered and added to

the Password List, that way each record will have it's Password Reset schedule set accordingly. There is a Bulk Update Password Reset Options feature for each Password List which allows you to change these values for more than one password record at a time.



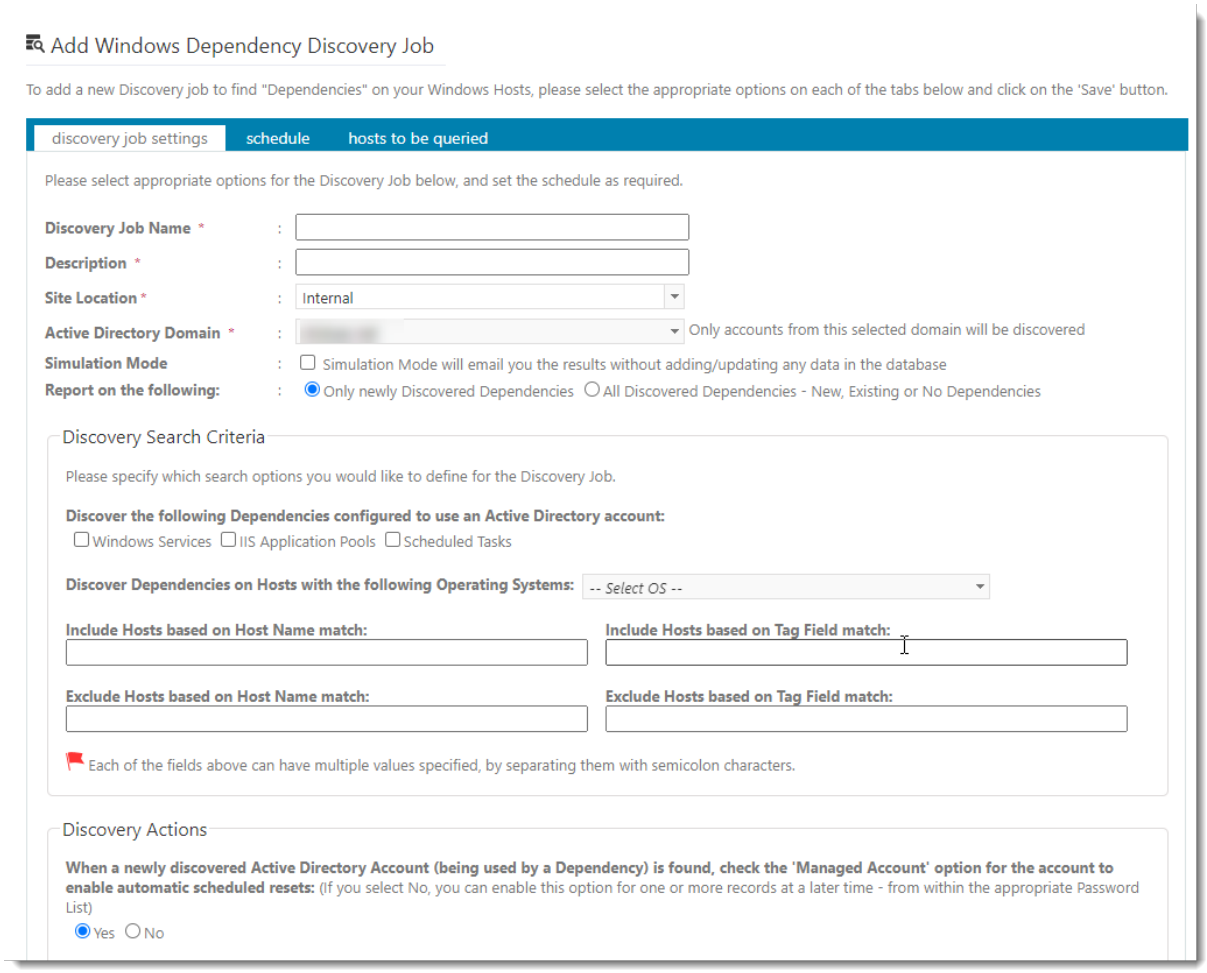
Discover Windows Dependencies

It's possible to also discovery various 'Windows Dependencies on your network that are using domain accounts as their identity to run under i.e. Windows Services, IIS Application Pools & Scheduled Tasks. When setting up such a Discovery Job, the following options are available:

- You need to select which 'Dependencies' you want to try and discover - Windows Services, IIS Application Pools or Scheduled Tasks - can you select all of them as part of the same Discovery Job if you want
- The rest of the options are very similar to discovery of other types of Accounts, as specified above

- If you do not wish to automatically configure the discovered accounts to perform scheduled resets, you can set the 'Managed Account' option to No. The later within the Password List, you can enable this option for one or more records at a time
- And don't forget to set the Schedule

Note : It is strongly recommended that you set the **'Default Password Reset Scheduled'** for the Password List (Password List Details Tab) prior to any new records being discovered and added to the Password List, that way each record will have it's Password Reset schedule set accordingly. There is a Bulk Update Password Reset Options feature for each Password List which allows you to change these values for more than one password record at a time.

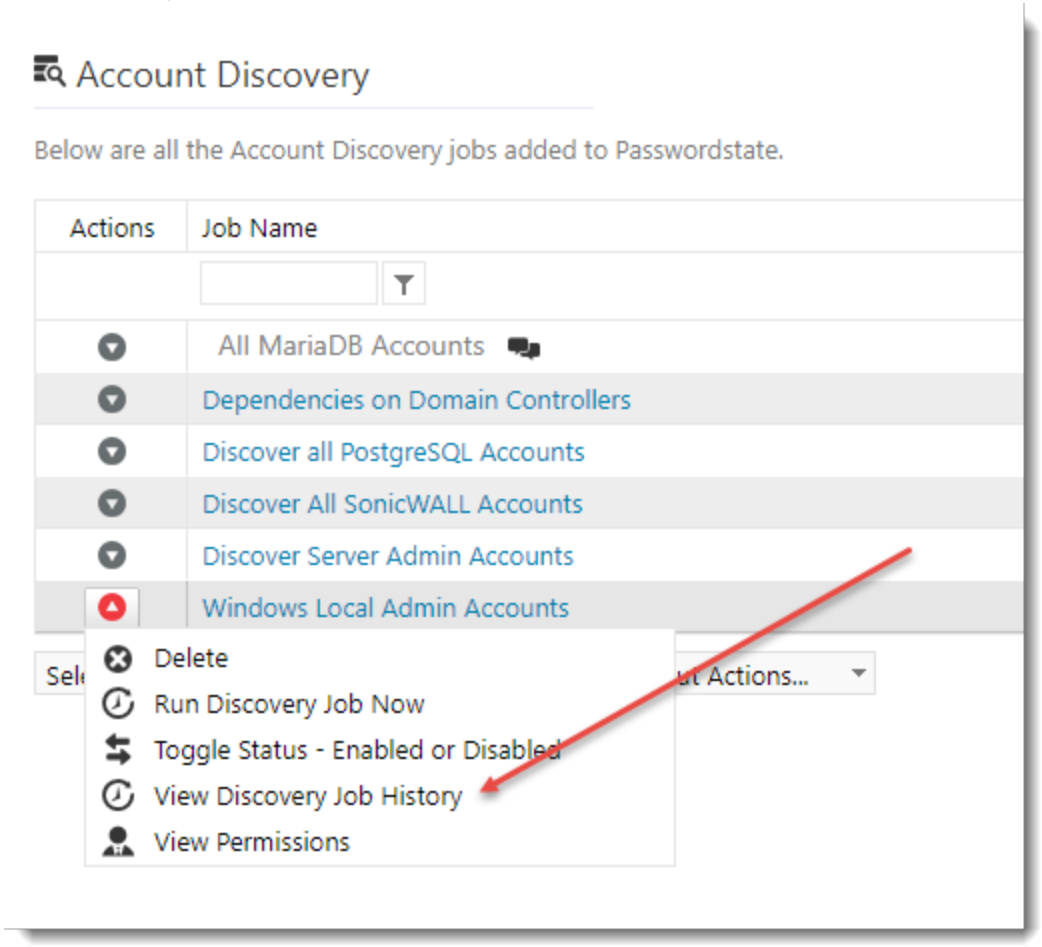


Discovery Job History

In addition to the emails you will received for results of Discovery Jobs, a History of all changes to the database are also recorded and can be viewed anytime - as per the screenshot below.

If your Discovery Job does not actually query any Hosts though, then it will not record any data i.e. You may have a Host filter set on the Discovery Job that does not return any Host records, or

possibly you have not added any Host records into Passwordstate (under the Hosts tab at the top of the screen).

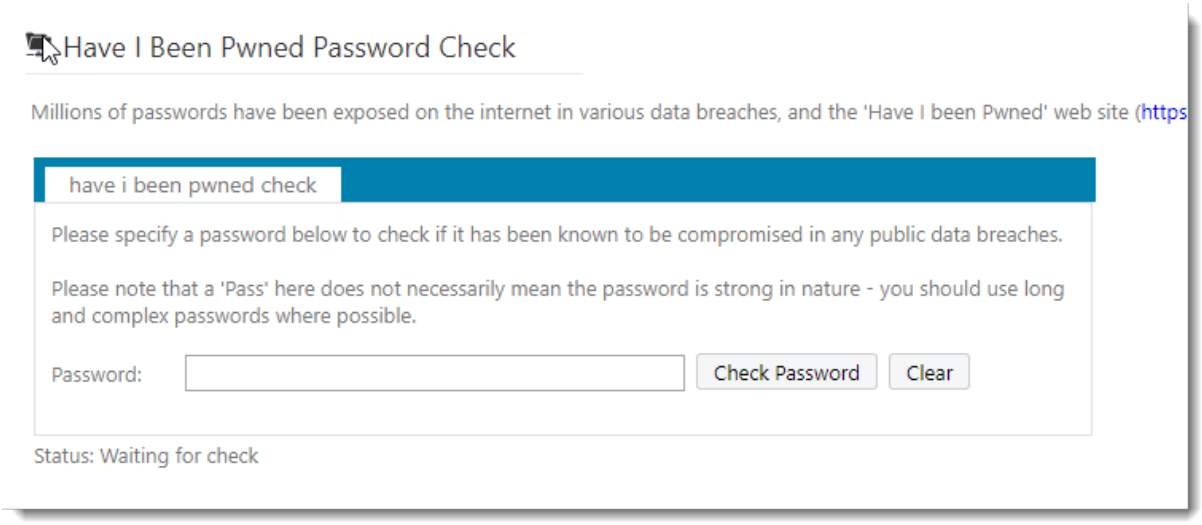


2.2.2 Have I Been Pwned Password Check

Millions of passwords have been exposed on the internet in various data breaches, and the 'Have I been Pwned' web site (https://haveibeenpwned.com) tracks and provides an API to check if passwords have been exposed in prior breaches.

On this screen, you can perform ad hoc checks of password values to see if they have be known as previously compromised.

Your Passwordstate Security Administrators can also enable this option for the Add/Edit Passwords screen, and this can be enabled via the screen Administration -> Bad Passwords.



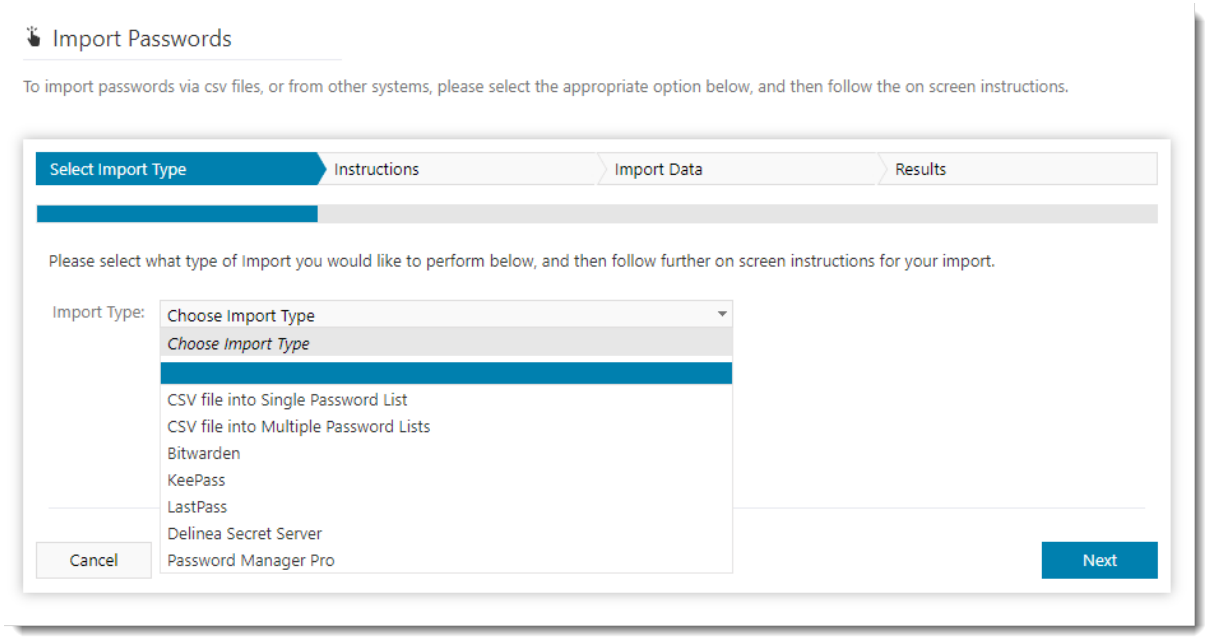
2.2.3 Import Passwords

The Import Passwords screen, allows you to import data from different sources into Passwordstate. The options are:

1. CSV file into Single Password List
2. CSV file into Multiple Password Lists
3. Bitwarden
4. KeePass
5. LastPass
6. Delinea Secret Server
7. Password Manager Pro

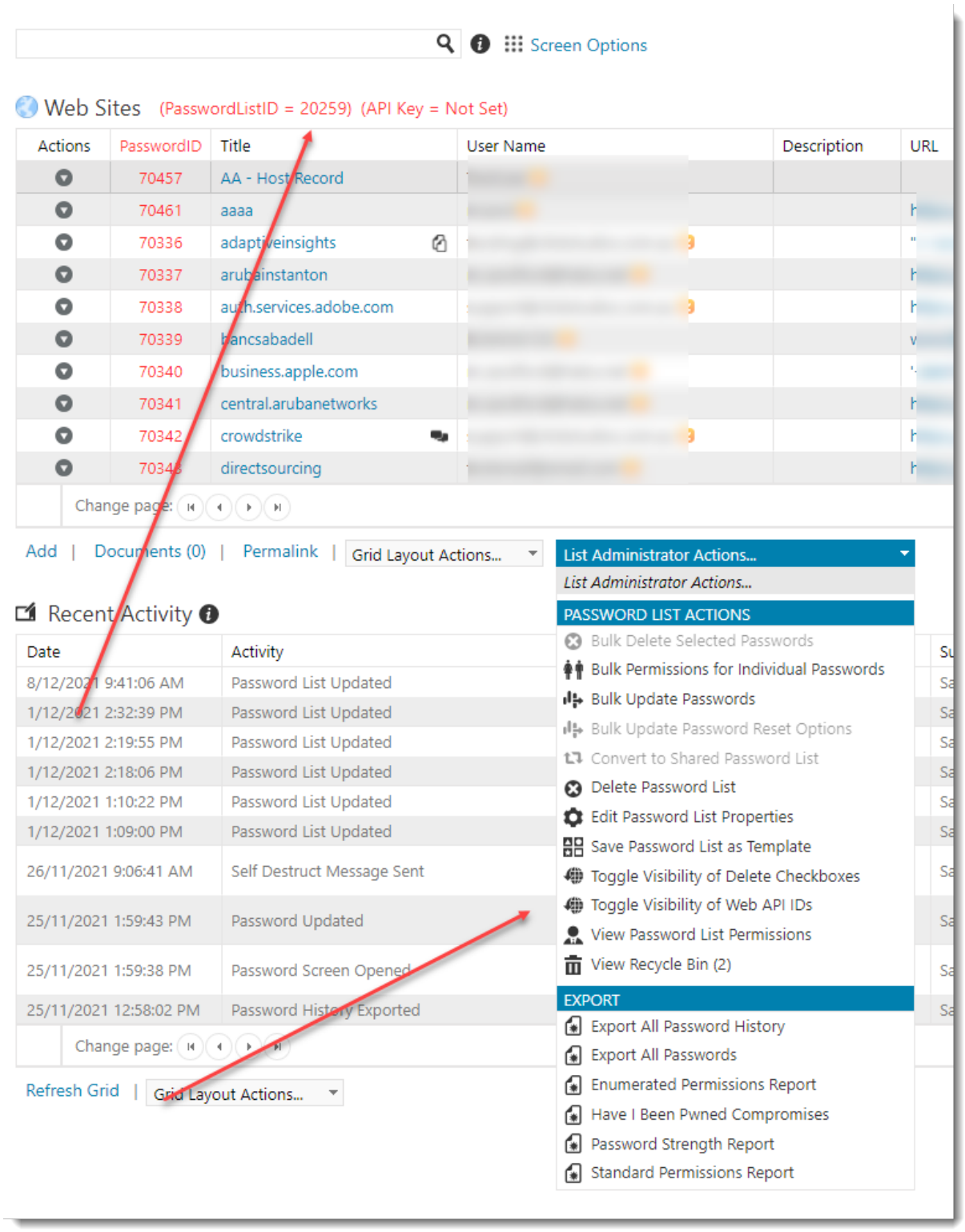
This screen provides you Wizard based functionality, where it guides you through the process of exporting your data, and then importing into Passwordstate.

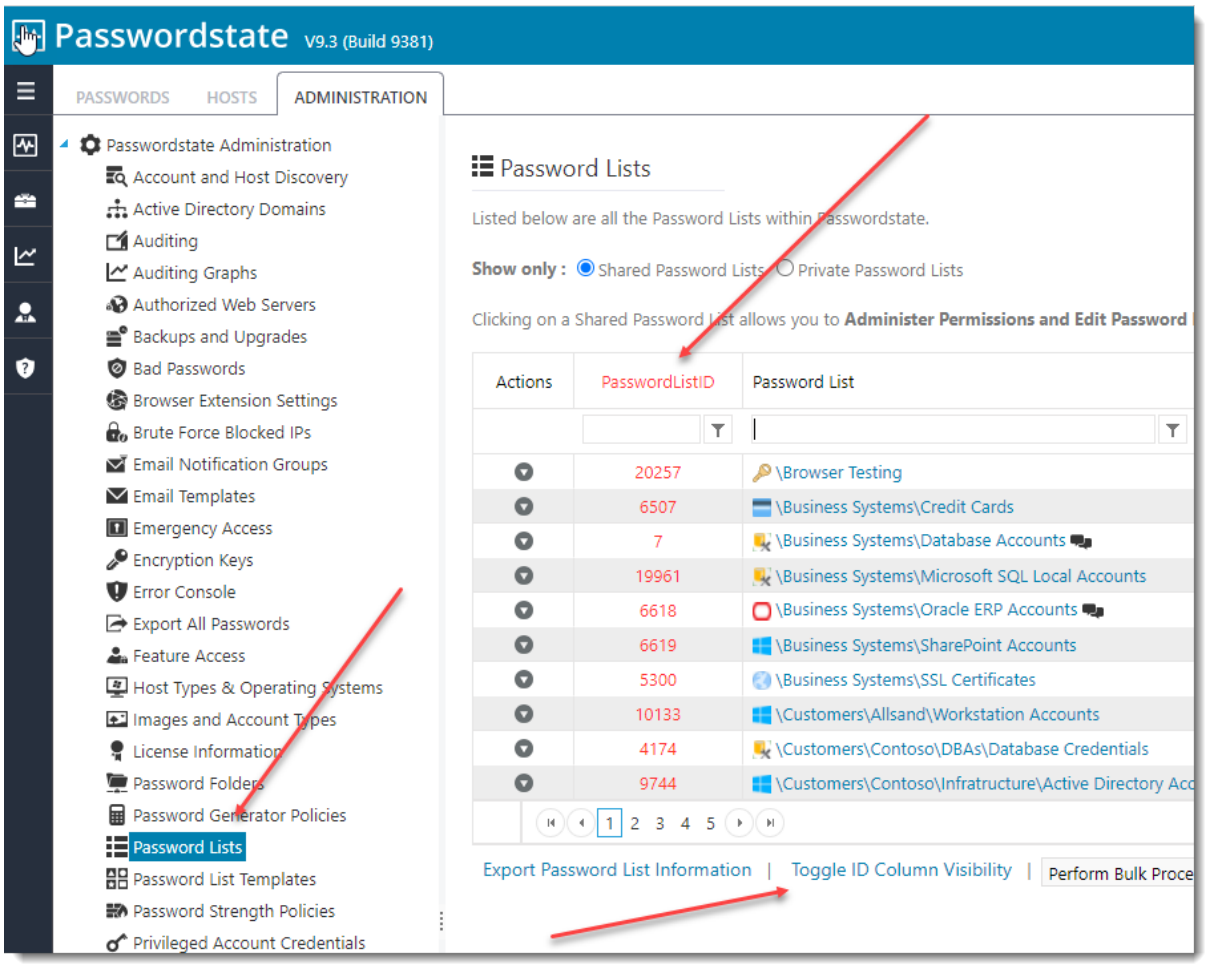
Note 1: For the CSV imports, you must have created the Password Lists already to import into. And when importing into Multiple Password Lists, you must know the PasswordListID values for each Password List, as you need to specify these in the import CSV file. Please see instructions below of 'Determining PasswordListID's for CSV Imports' for how to determine these ID's
Note 2: When using the 'CSV file into Multiple Password Lists', you must be a Security Administrator of Passwordstate, which has the Password Lists Security Administrator role. This restriction is in place to prevent standard user accounts from importing data into Password Lists which they have not been given access to.
Note 3: For importing from the 4 different products listed above, the Base URL of your Passwordstate web site must be recorded correctly in Passwordstate, so the API can be used to perform this import



Determining PasswordListID's for CSV Imports

The PasswordListID's can be viewed on a per Password List level, as per the first screenshot below, or you can view them in bulk as per the second screenshot below.

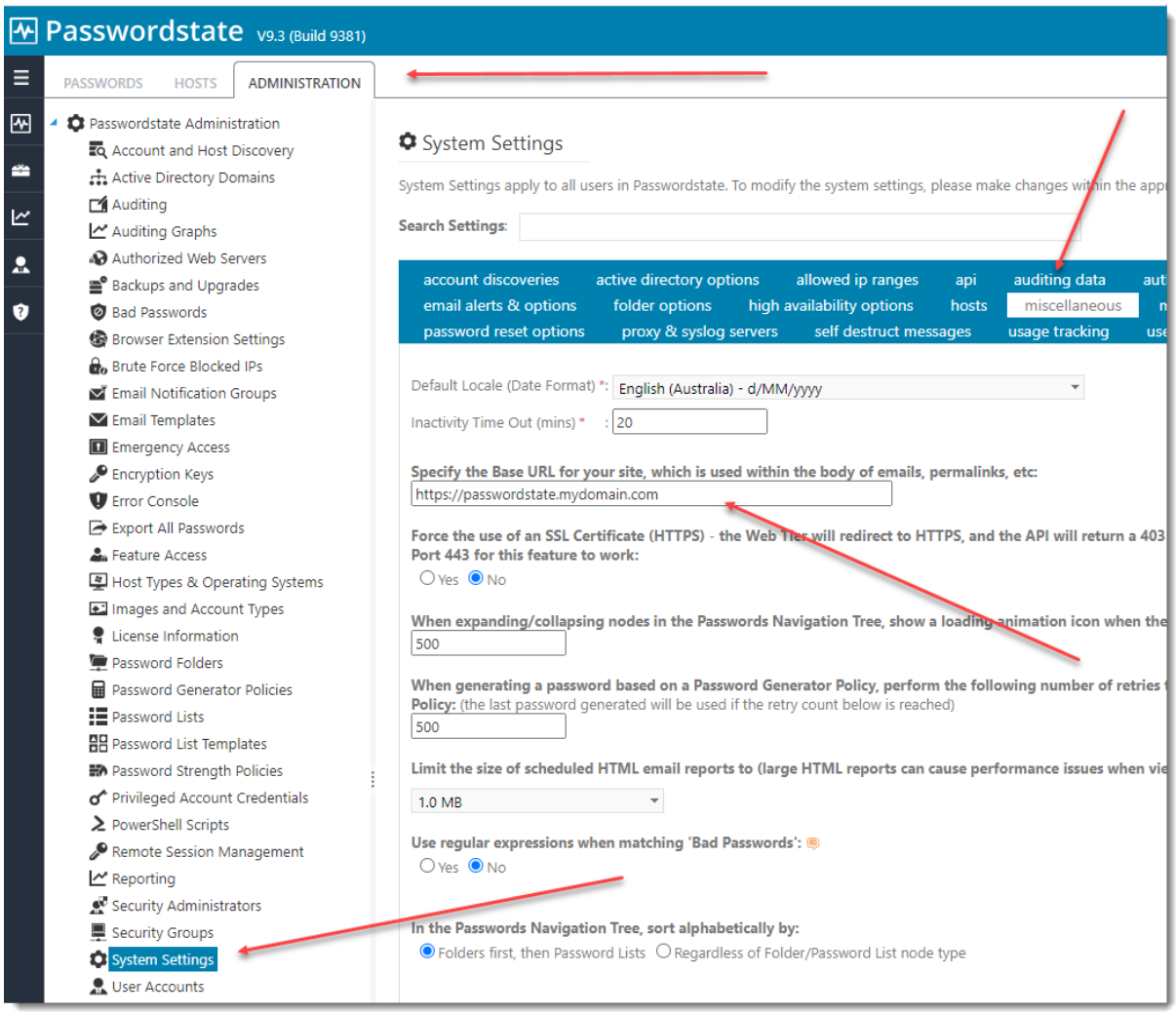




Determining PasswordListID's for CSV Imports

For the imports of KeePass, LastPass, Thycotic Secret Server & Password Manager Pro, each of these need to communicate to the API in Passwordstate, in order to perform the import.

Please check the Base URL you see in the screenshot below is accurate, and please test this by running on the pre-defined reports on the screen Administration -> Reporting, to confirm API connectivity is working.



2.2.4 Password Generator

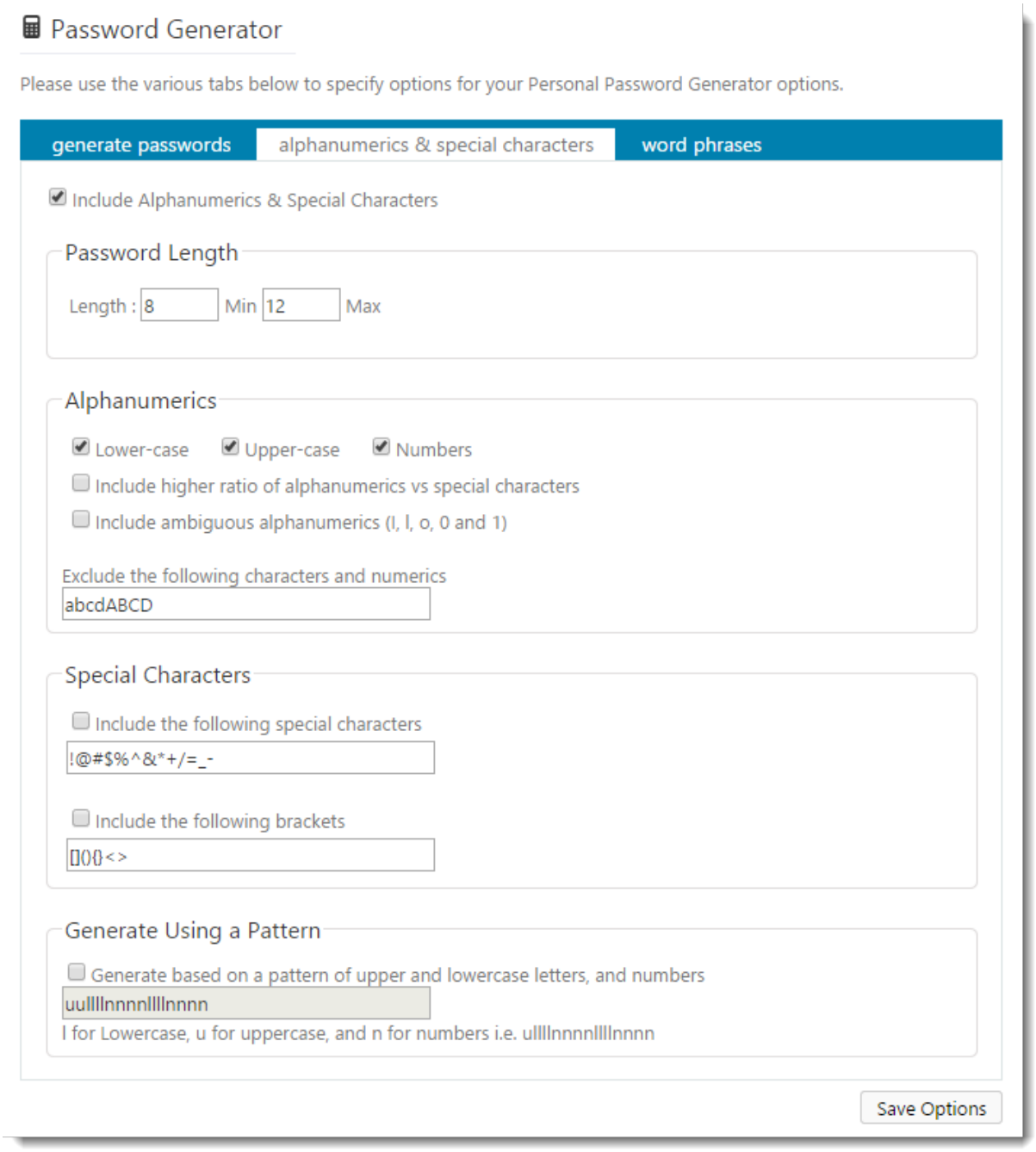
The Generator menu is where you can access your personal settings for the Password Generator built into Passwordstate, and also allows you to generate any number of random passwords with your personal settings.

Note: The Security Administrators of Passwordstate can create different Password Generator Policies and apply them to various Password Lists, so if you generate a new random password when adding/editing a Password record, the password does not seem to conform to your personal settings, then most likely a different Password Generator has been applied to the Password List.

The Password Generator screen comprises of three tabs - two for specifying the settings, and one for generating the random passwords.

Alphanumeric & Special Characters

The Alphanumeric & Special Characters tab allows you to specify the desired length of the password you wish to generate, as well as settings for letters, numbers, special characters and various forms of brackets.

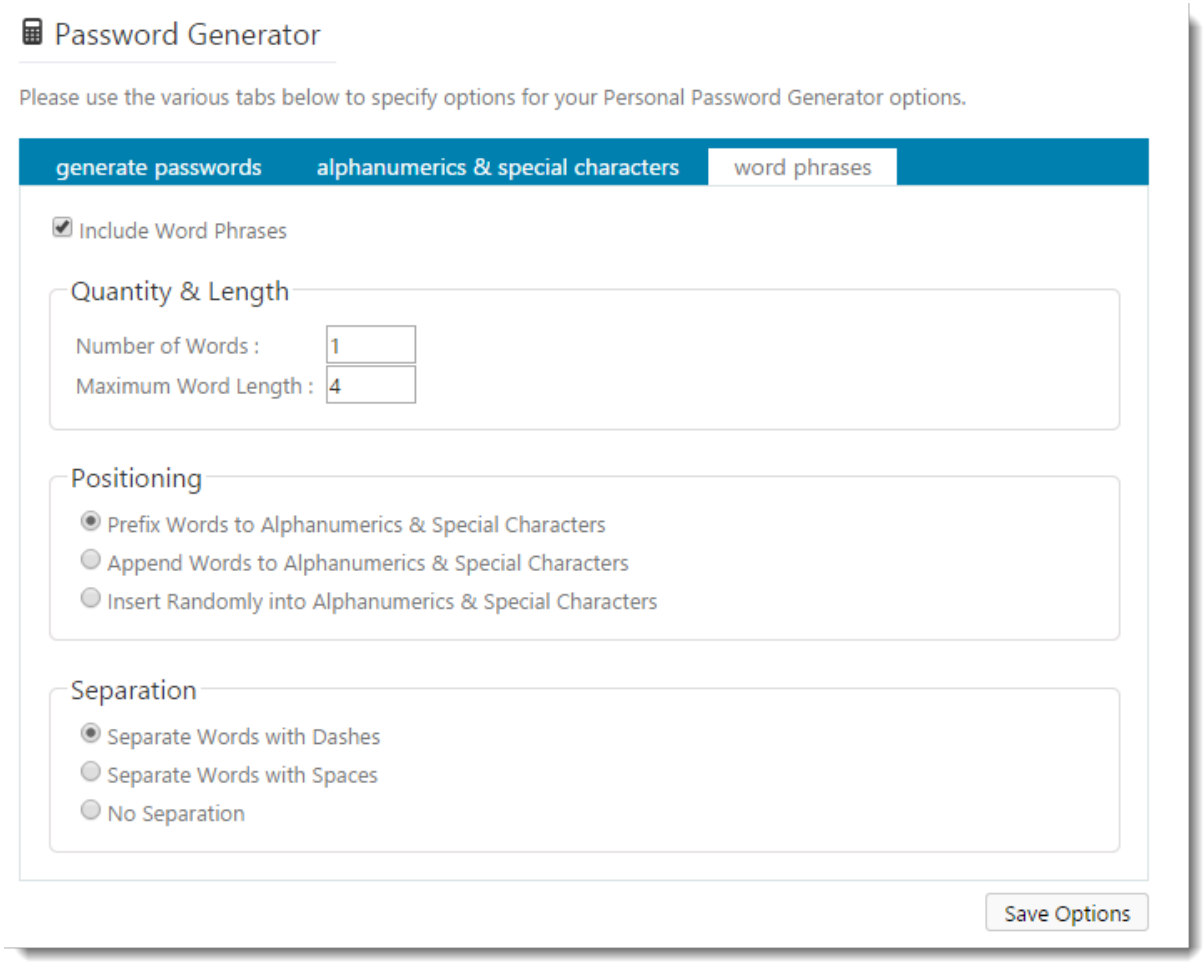


Word Phrases

The Word Phrases tab allows you to insert a random word at the beginning of the password, somewhere in the middle, or at the end. You can specify how many words to create, what length,

and what form of separation you would like between the word and the rest of the random password - either dashes, spaces or nothing.

Passwordstate has 10,000 different words it can choose from, all of different lengths.

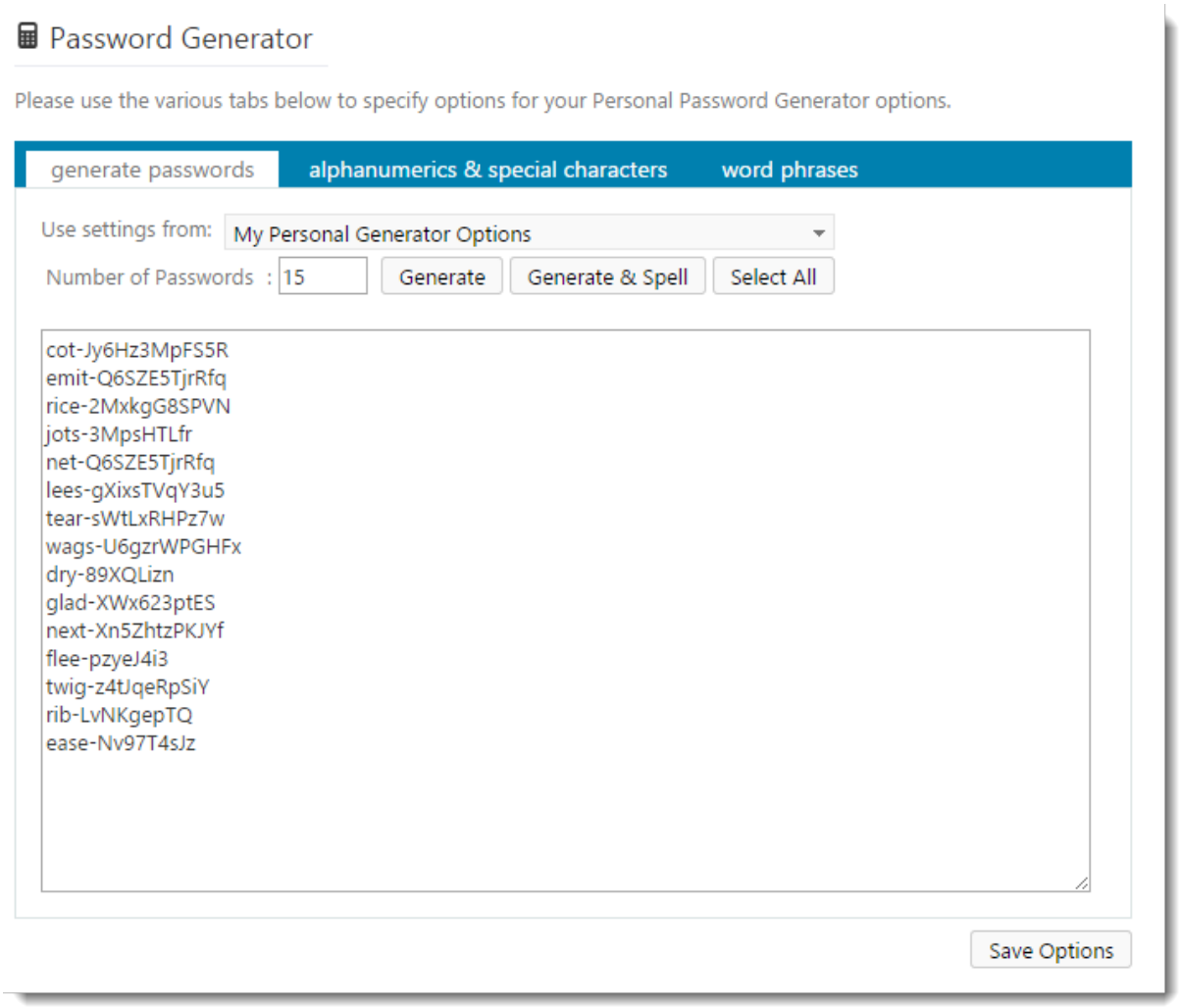


Generate Passwords

The Generate Passwords tab is where you specify the number of random passwords you want to generate.

It's not necessary to click on the 'Save Options' button if you simply want to test different options under the two other tabs, but you will need to click on this button if you want to retain these settings for future use.

Note 1: You can also generate some random passwords based on the settings of a Password Generator Policy by selecting a policy from the dropdown list on this screen.
Note 2: The 'Generate & Spell' button will spell out passwords for you in the format of tango echo yankee foxtrot, etc

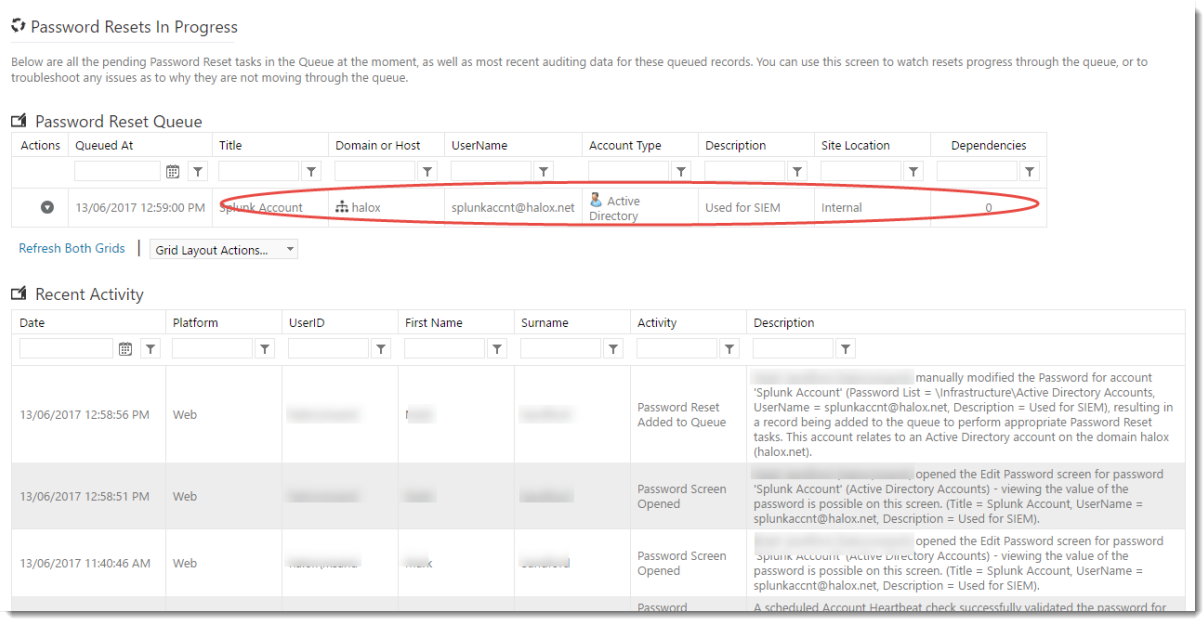


2.2.5 Password Resets in Progress

The Password Resets in Progress screen shows any accounts which are sitting in the queue, pending processing.

The auditing data on the screen is a filtered view of only the records currently sitting in the queue. It can be used to troubleshoot any potential issues as to why resets are not progressing through the queue.

Note: Password Resets for Site Location of "Internal" should be processed within 1 minute from the Passwordstate Windows Service, but any other Site Locations will stay in the queue longer as it depends on what polling time has been configured for each of the Remote Site Location agents.



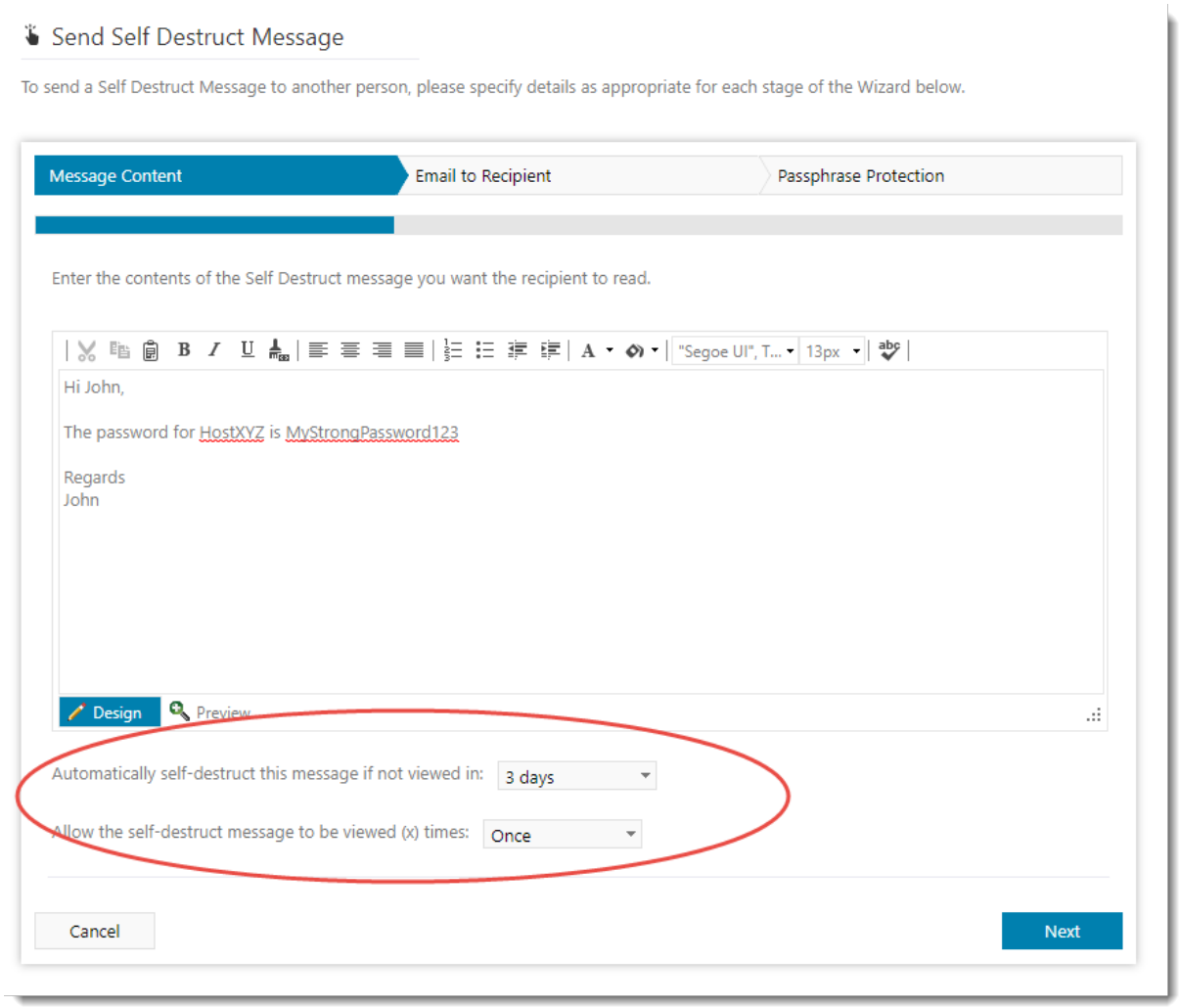
2.2.6 Self Destruct Message

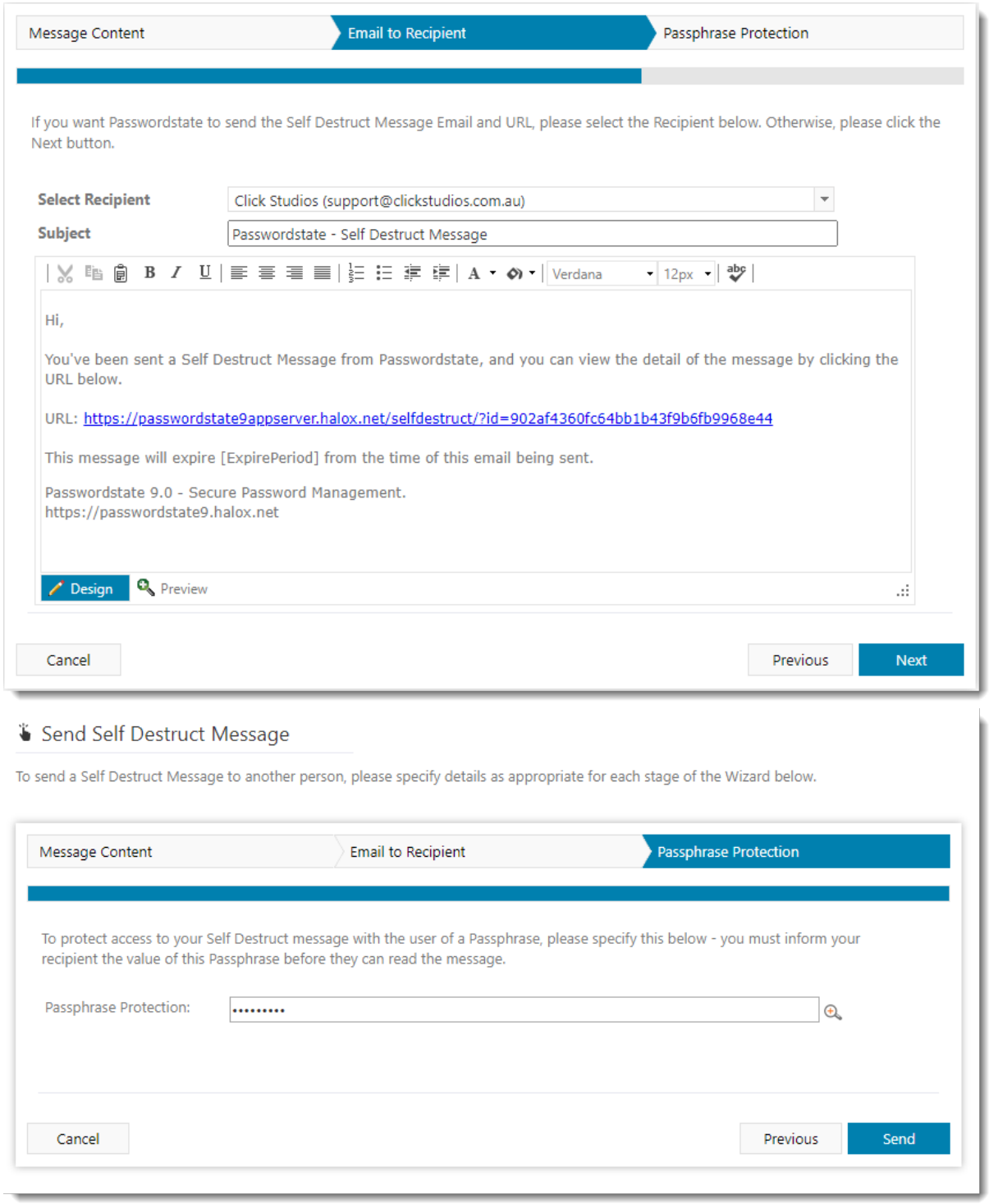
The Self Destruct Message menu allows you to generate and send a Self Destruct email message to another user - the message expires after the set time period, if not read.

Creating a Self Destruct message is a three step process:

1. Specify the message, how long the message will be active for, and how many times the message can be viewed
2. Choose the user you want to send the message to - this can either be another user of Passwordstate, or a recipient from the Address Book, or someone else simply by typing their email address
3. And specify any Passphrase protection you might want - there is a default Passphrase value which can be configured by your Security Administrators on the screen Administration -> System Settings -> Self Destruct Messages, or contacts in the Address Book Book can also have their own Passphrase. The intended recipient need to know what this Passphrase is prior sending them messages

The message will no longer be available for viewing either when the user has viewed it the specified number of times, or the message has expired.





2.3 Reports Menu

The Reports Menu allows you to access audit data for Password Lists you have access to, and also schedule the email delivery of various reports.

Auditing	Allows you to view all the auditing data applicable to the Password Lists you have access to
Auditing Graphs	Allows you to view basic charts representing various audit activities over time
Scheduled Reports	Allows you to schedule one or more reports to be emailed to your account

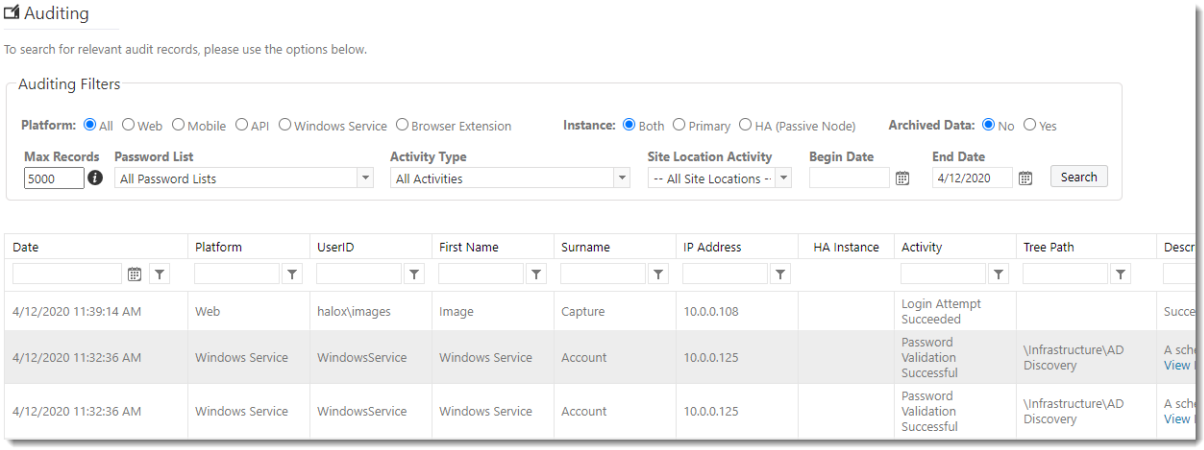
2.3.1 Auditing

The Auditing menu allows you to view all the auditing data applicable to the Password Lists you have access to. It allows you to filter the data in multiple ways, as well as export the contents of the search results to a csv file for further analysis if required.

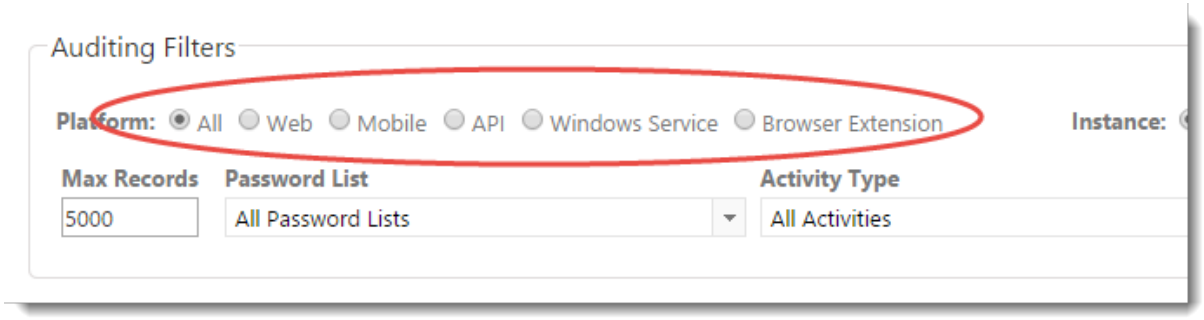
Additional auditing data is also available to Security Administrators of Passwordstate, and can be found on the screen Administration -> Auditing. The additional auditing data relates to certain activities like login failures, user account related, etc.

Note: The Telerik Grid and Filter controls here prevent filtering while using special characters - for security reasons. If you're wanting to filter using a backslash (\) here, simply type the backslash twice i.e. domain\\userid

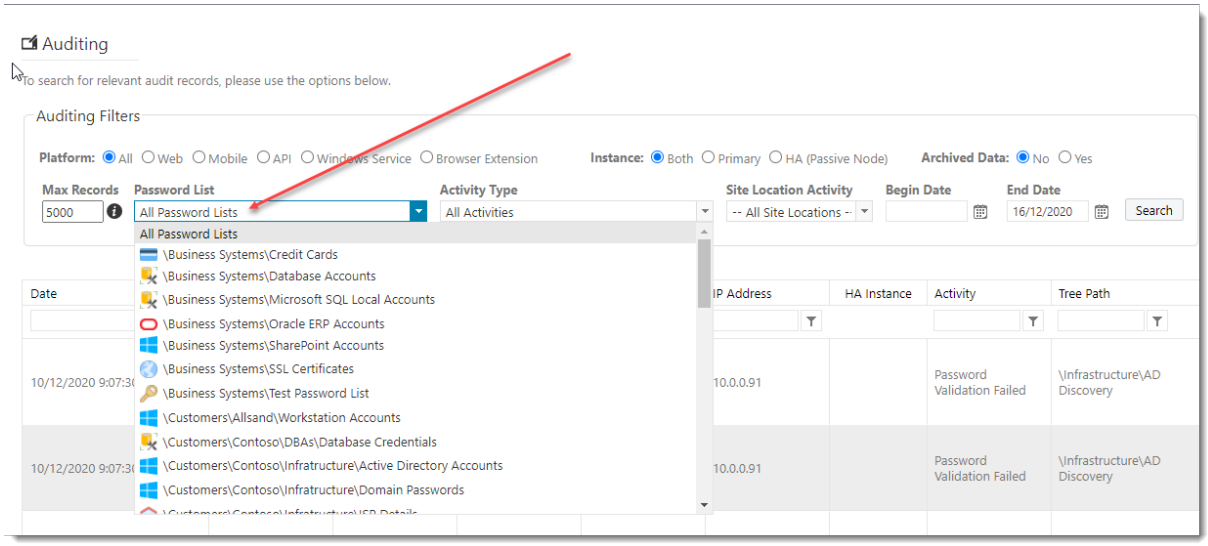
Performance Considerations: Please note that on this screen, only auditing records for Password Lists you have access to will be displayed here. This means there could be a potential performance impact, if you have thousands of Password Lists - permission checks are done on Password Lists for your User Accounts, and Security Groups, as well as for individual password records. If you find a performance impact on this screen, please use the screen Administration -> Auditing if you have access to it.



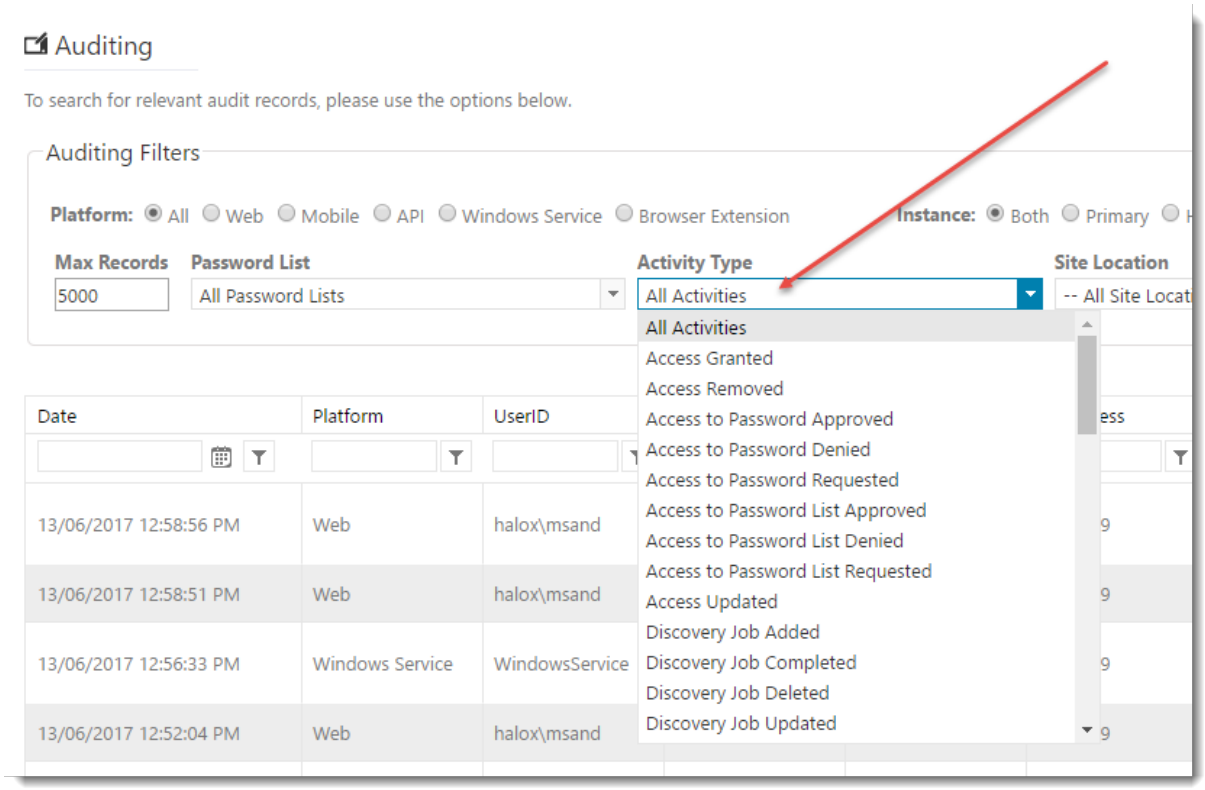
Filter by Platform



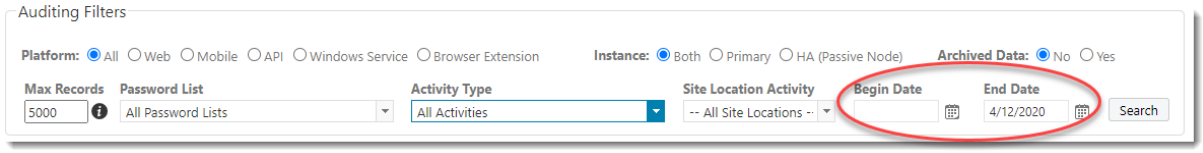
Filter by Specific Password Lists



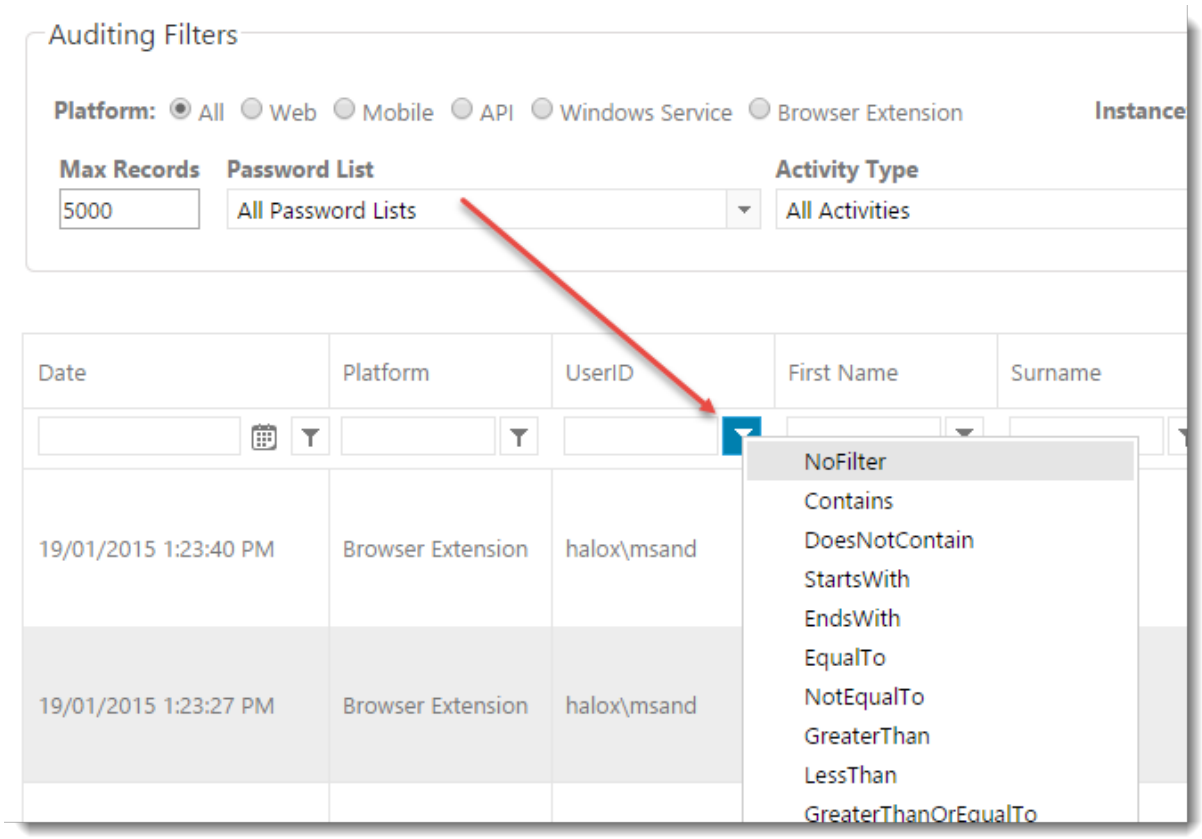
Filter by Specific Activity Type



Filter between Specific Dates

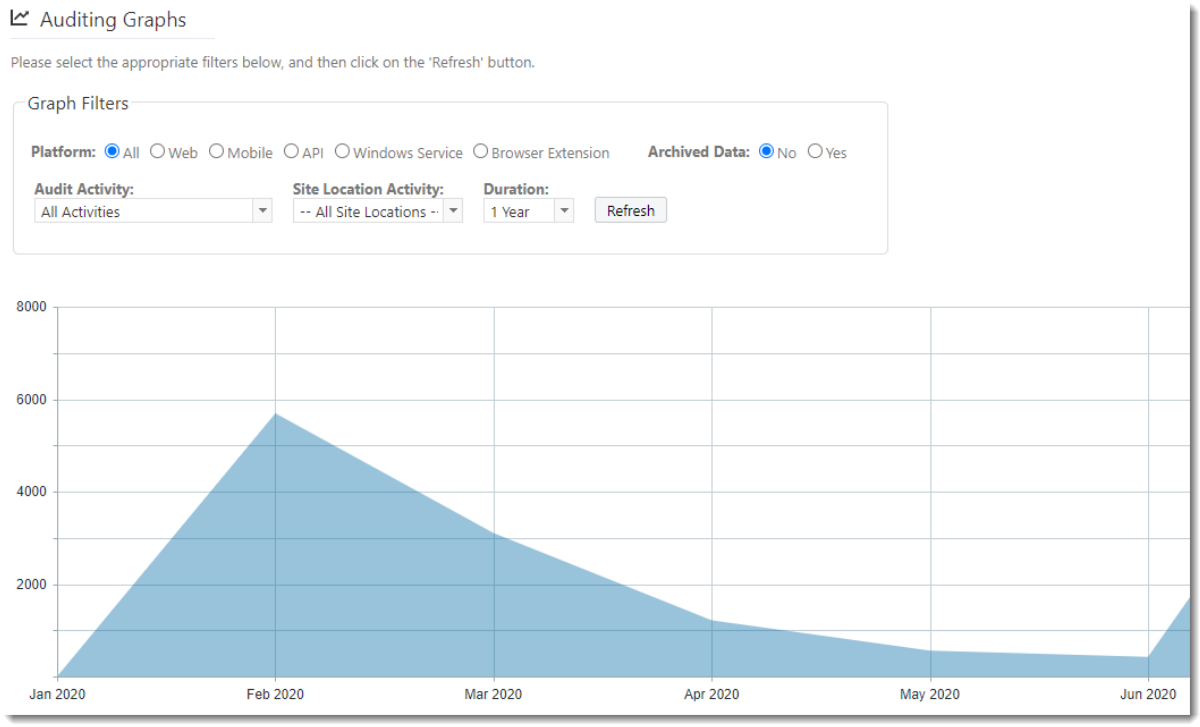


Further Filter by Search Results Contents



2.3.2 Auditing Graphs

The Auditing Graphs menu simply allows to to see a graphical representation of auditing events over a time-line you specify. You can filter by Platform, Audit Activity and Duration.



2.3.3 Scheduled Reports

The Reports Menu allows you to schedule one or more reports to be emailed to your account, either as an embedded HTML report within the email, or as a CSV attachment.

Choosing The Report Type

As a standard user account, there are two types of reports available:

- Custom Auditing Report - Allows you to specify a custom filter for reporting on audit activities for Password Lists that your account has access to
- Expiring Passwords - produces a report of password records which have already expired, or are about to expire within the next number of days you specify - for password credentials your account has got access to

If your account has also been granted the 'Reporting' Security Administrator's role, then there are many more reports available in addition to the Custom Auditing and Expiring Passwords report. If you are a Security Administrator and select Custom Auditing or Expiring Passwords, then all Shared Password Lists will be available to you.

Below are a list of all the Security Administrator reports available as well:

User Reports

- What passwords can a user see?
- What passwords does a user still know? (Last Access vs Viewed)
- What has a user been doing lately? (all auditing data for the user)
- What Failed login attempts have there been?

- Who hasn't logged in recently?
- Who has one or more Security Administrator roles?
- What Remote Sessions has a user been doing lately?
- What user accounts are currently disabled?
- What user accounts are set to expire?
- Which users have logged in using the Emergency Access account?
- What user account impersonation has been occurring?

Passwords Reports

- What passwords have failed Heartbeat?
- What passwords have failed Reset?
- What passwords require checkout?
- What passwords are currently checked out?
- What passwords require a Reason to be specified for access?
- What passwords are expiring soon?
- What passwords have recently been reset?
- What password values have been reused?
- What passwords have not been used lately? (Aged Password Report)
- What Passwords are not being synced?
- Passwords Strength Compliance Status

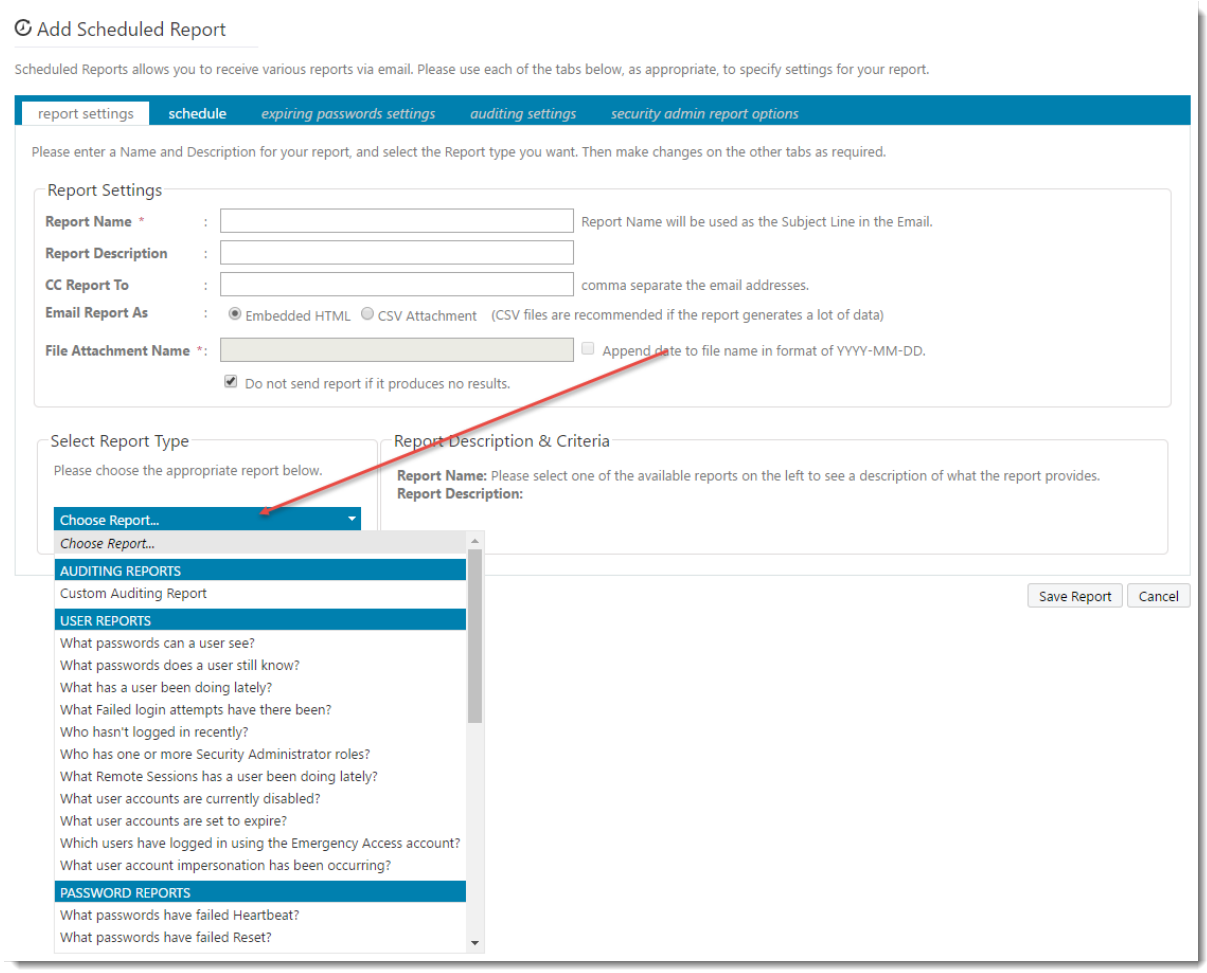
Permissions Reports

- What permissions exist (all users and security groups)?
- What permissions exist for a user?
- What Permissions exist for a Security Group?
- What permissions have changed recently?
- Who has been approved access to passwords recently?
- Who has been denied access to passwords recently?

Audit Activity Reports

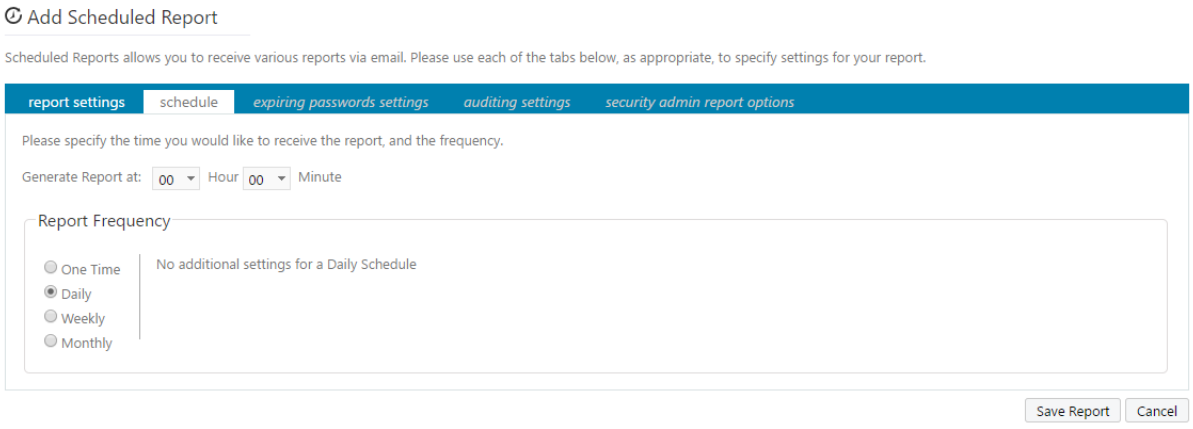
- Remote Session Launcher Activity
- Browser Extension Activity
- Mobile App Actviity
- API Activity
- Self Destruct Activity
- Passive High Availability Module Activity

Once you've chosen the required type of report, you must specify a schedule for when the report is sent, and also any other additional settings for the Expiring Passwords report, Custom Auditing or Security Admin Reports.



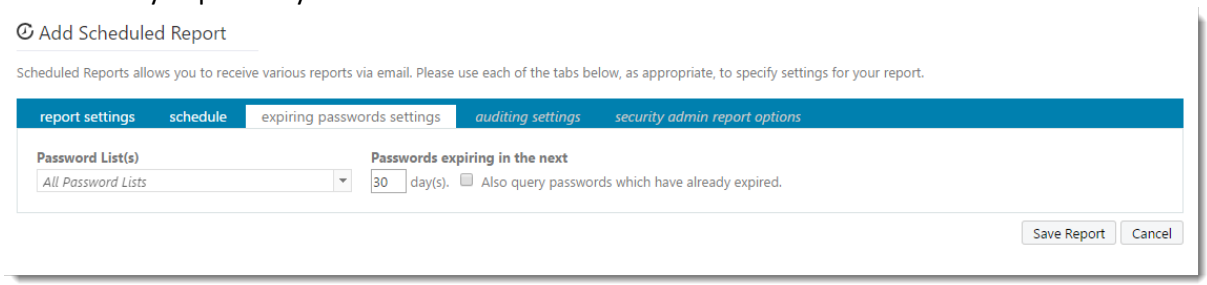
Setting The Schedule

When setting the schedule, you can choose the time of the day the report is sent, and also the frequency - Daily, Weekly, or Monthly. A One-Time option is also available, which can be repeated at different intervals as well.



Expiring Passwords Settings

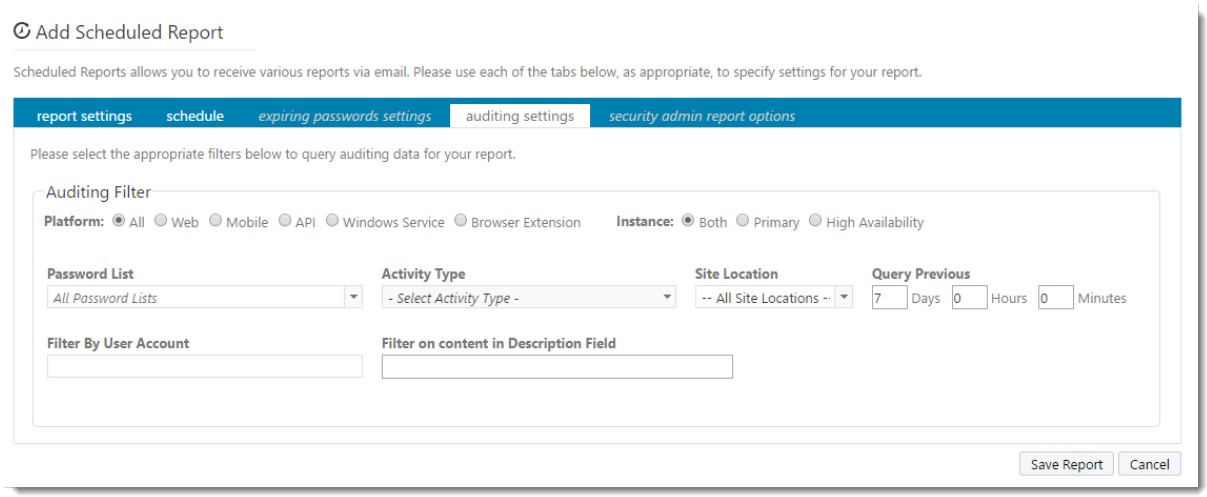
If you have chosen the Expiring Passwords Report, you can choose how many days ahead to look for passwords which are due to Expire - this is based on the value of the Expiry Date Field. This report will look ahead the number of days you've specified, and also include any passwords which have already expired if you choose.



Auditing Settings

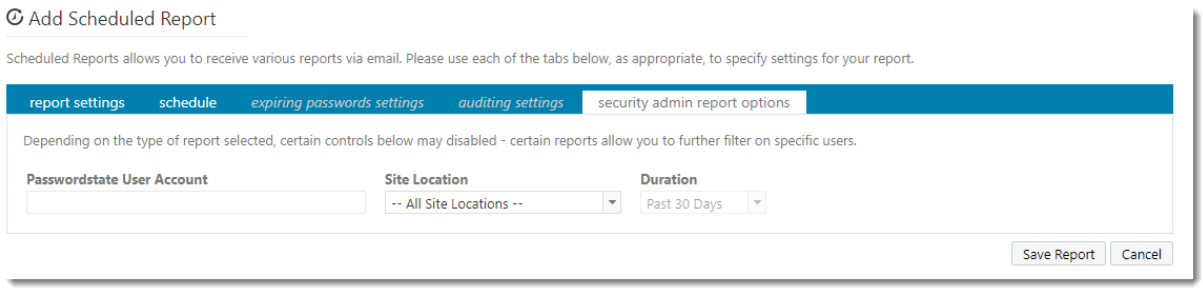
If you have chosen one of the 'Custom Auditing Reports', you can create your own filter for the auditing data, and specify how many days, hours and minutes into the past you wish to query the data.

Note: You can select one or more Password Lists or Audit Activities by checking the appropriate options in each of the relevant dropdown lists.



Security Admin Report Options

Depending on which Security Administrator's report you have selected, various fields will either be enabled or disabled on the 'Security Admin Report Options' tab, allowing filtering as required.



2.4 Preferences Menu

The Preferences Menu allows you to set various settings for your Passwordstate account, set various email notifications.

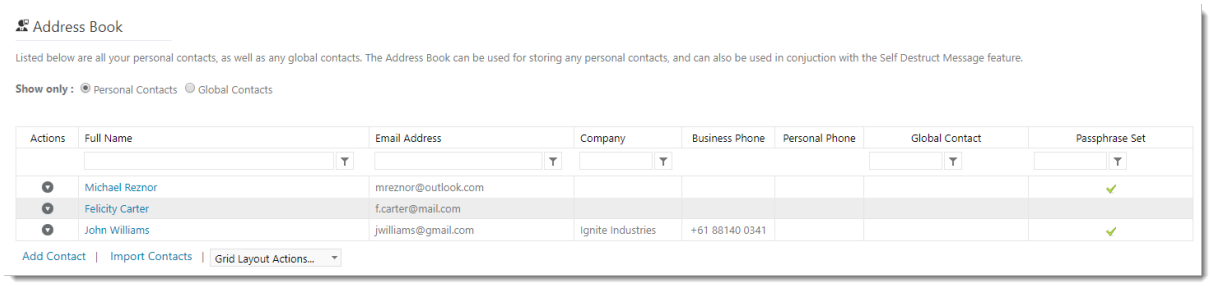
Address Book	An Address Book which can be used to store contact details, and can be used in conjunction with the Self Destruct Message feature
Preferences	Specify various settings for your Passwordstate account
Email Notifications	Select which Email Notifications you would like to receive, or block

2.4.1 Address Book

The address book is used primarily for two features:

- A simply address book to store contact information
- Or to be used with the Self Destruct Message feature, so you can send messages to the recipients in the Address Book

Each user can add their own contacts in the Address Book, and they will only be visible to them. Global contacts can also be added, and these contact types will be visible to all users in Passwordstate. It is possibly to specify who is allowed to manage Global Contacts on the screen Administration -> Feature Access -> Miscellaneous tab.



2.4.2 Preferences

The Preferences screen is where you can specify many different settings specific to just your Passwordstate user account.

Note: The Security Administrators of Passwordstate can use a feature called 'User Account Policies', which may override any settings you specify here. If a User Account Policy is applied to your account, certain settings on the Preferences screen will be disabled.

The Preferences screen has the following 8 tabs:

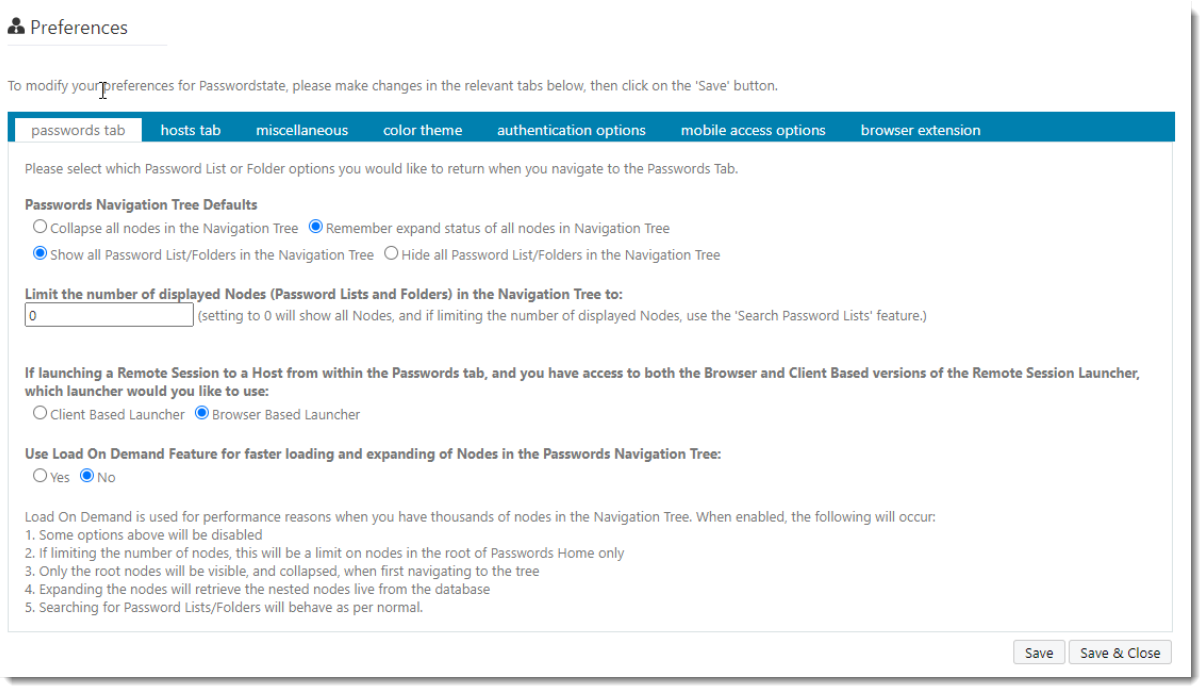
Passwords Tab	The Passwords Tab allows you to select various options for the Passwords Navigation Tree
Hosts Tab	Specify a couple of settings for features available under the Hosts tab
Miscellaneous Tab	A collection of different settings specific for your account
Color Theme Tab	Allows you to customize the colors for Passwordstate
Authentication Options Tab	Specify which authentication method you wish to use when first accessing the Passwordstate web site
Mobile Access Options Tab	Allows you to specify various settings for the Mobile App version of Passwordstate, and also the Pin Number used for you to authenticate.
Browser Extension	The Browser Extension tab allows you to specify various settings for the Chrome Browser Extension, which is used to automatically form-fill web site logins
API	Allows you to set a 2FA secret to be used with the Windows Integrated API

2.4.2.1 Passwords Tab

The Passwords Tab allows you to select various options for the Passwords Navigation Tree.

If you have thousands of Folders and Password Lists showing in the Passwords Navigation Tree, it is recommended you either limit the number of nodes displayed, and/or select the Load On Demand feature . The Load On Demand feature will only show the Password Lists/Folders in the root of the Navigation Tree, and when you expand a Folder, it will retrieve nested objects from the database at that time - dramatically improving performance.

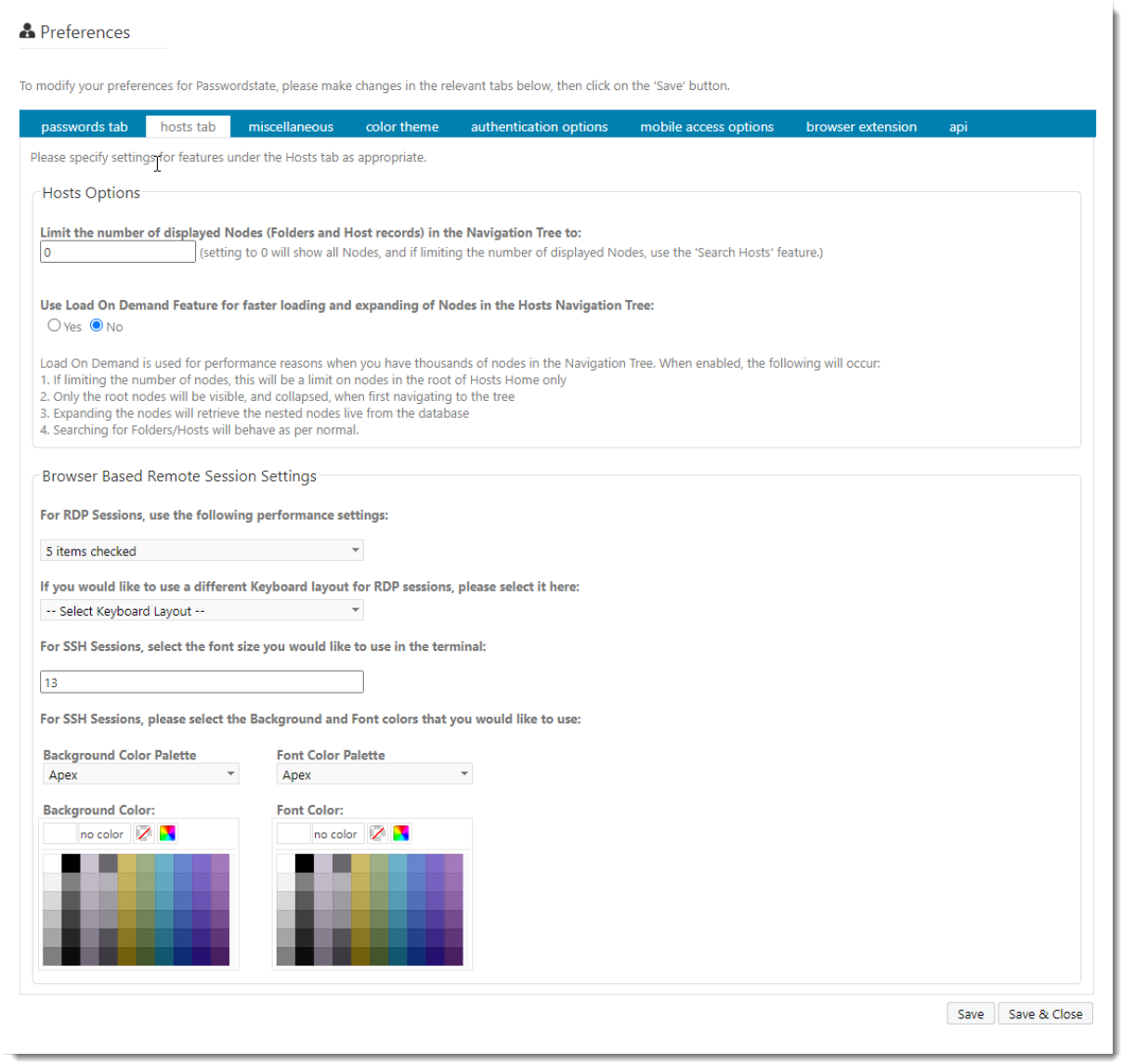
These options are recommended, because downloading and rendering all the HTML required for thousands of nodes, can cause performance issues.



2.4.2.2 Hosts Tab

The Hosts Tab allows you to select various options for the Hosts Navigation Tree under the Hosts tab.

In particular, you can limit the number of Nodes displayed in the Hosts Navigation Tree, or use the Load On Demand feature, similar to the Passwords Navigation Tree.

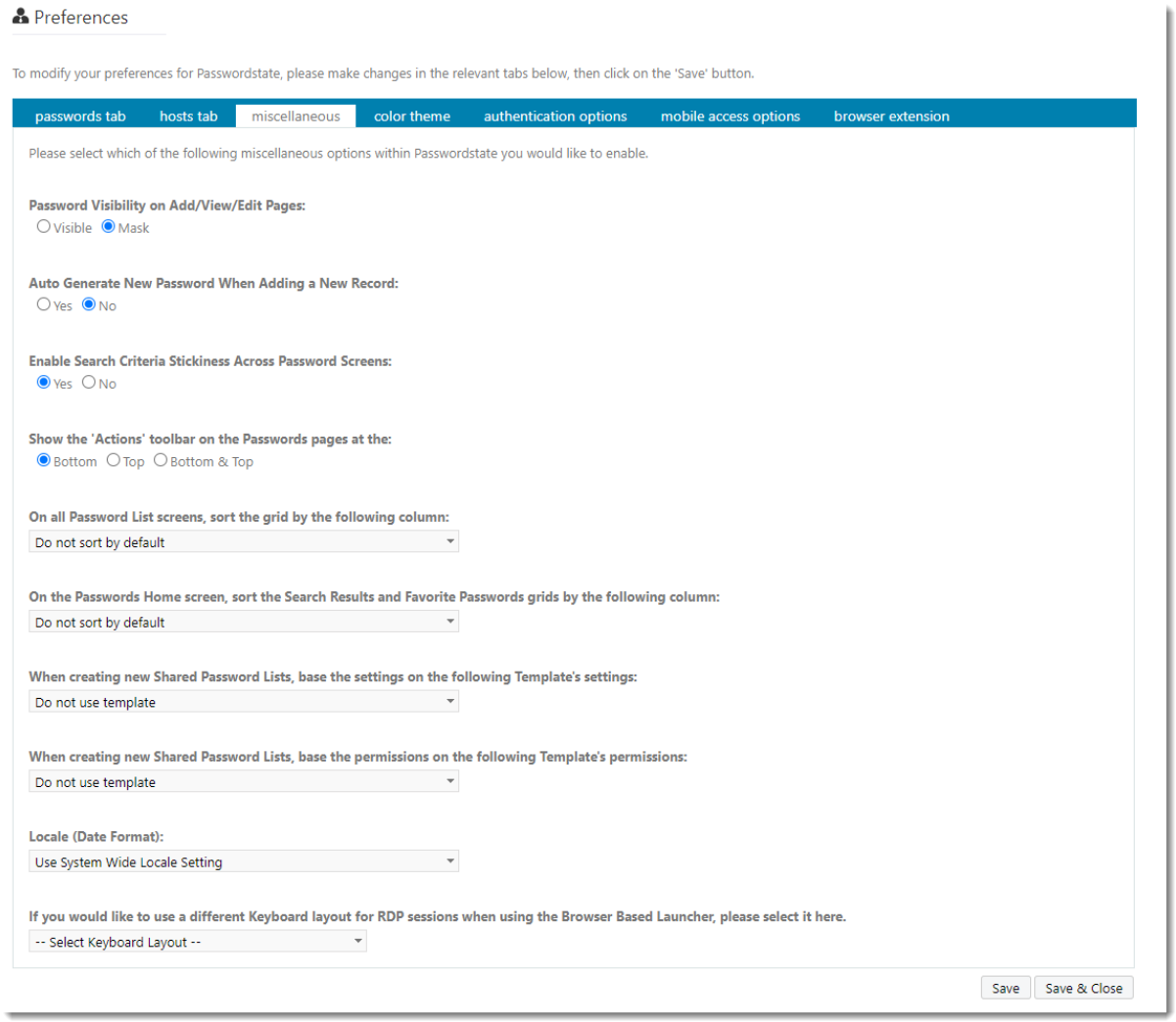


2.4.2.3 Miscellaneous Tab

The Miscellaneous Tab has the following settings you can choose for your account:

Password Visibility on Add/View/Edit Pages	When you add a new Password or edit an existing one, by default the password value is masked i.e. ****** If you choose, you can instead show the password value instead of the masked one
Auto Generate New Password When Adding a New Record	When adding a new Password record, you can automatically generate a new random password instead of having to specify one yourself. The format/complexity of the new random password will be determined by which Password Generator Policy is applied to the Password List

Enable Search Criteria Stickiness Across Password Screens	When using the search textbox found at the top of most Password screens, you can choose to make this search value you type sticky across different Password Lists i.e. if you search for 'test' in one Password List, when you click on another Password List in the Navigation Tree, the contents of the Passwords grid will also be filtered by the term 'test'. You can also clear the search criteria by clicking on the  icon
Show the 'Actions' toolbar on the Passwords pages at the	At the bottom of every Passwords grid there are certain buttons/controls for adding passwords, importing them, viewing documents, etc. With this option, you can choose to display the 'Actions' toolbar at the bottom of the Passwords grid, at the top, or both
On all Password List screens, sort the grid by the following column	If you would like all Password grids to be sorted by default on a selected column, you can choose the column here. Note: this will override you manually sorting a column and then selecting the save the Grid layout
On the Passwords Home screen, sort the Search Results and Favorite Passwords grids by the following column	Similar to the option above, but this sort order applies to the Search Results and Favorite Passwords grids on the Passwords Home page
When creating new Shared Password Lists, base the settings on the following Template's settings	When creating new Shared Password Lists, you can choose to automatically specify all the settings based on the selected Template
When creating new Shared Password Lists, base the permissions on the following Template's permissions	When creating new Shared Password Lists, you can choose to automatically apply permissions based on the permissions set on the selected Template
Locale (Date Format)	Allows you to specify a date format for any date fields - you may need different format based on your region, compared to that of what Passwordstate is current set to use system wide
RDP Keyboard Layout	When using the Browser Based Remote Session Launcher, the default keyboard used is United States (English). This default can be change for all users on the screen Administration -> Feature Access -> Remote Sessions tab, or individual users can change it here on their Preferences screen

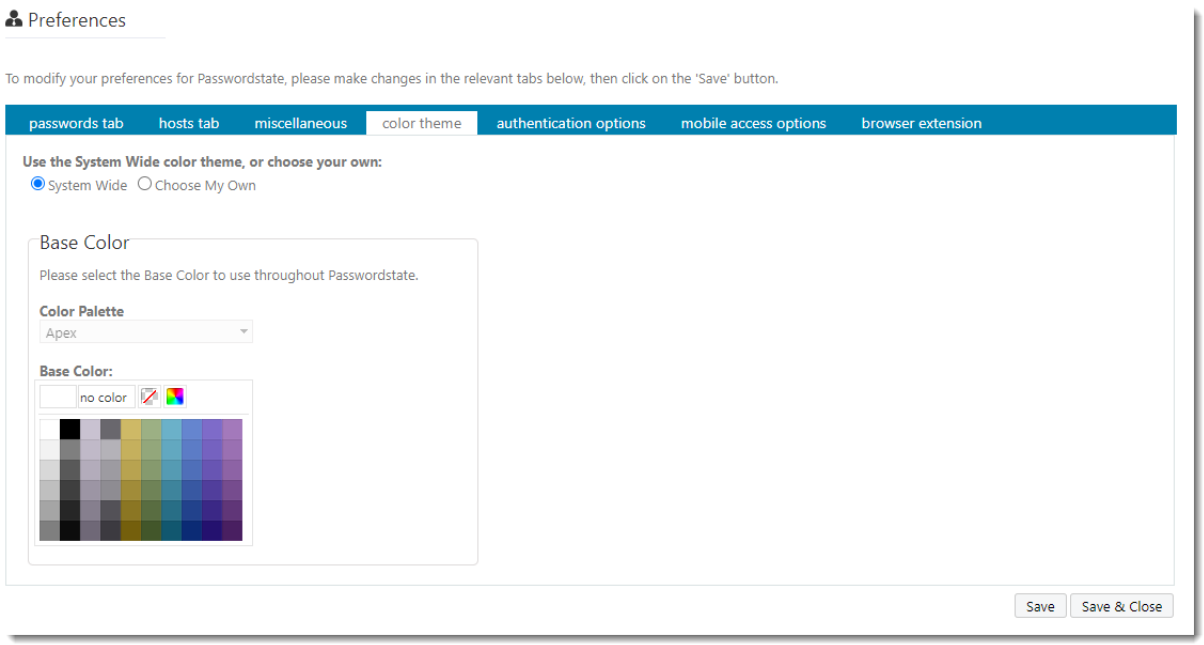


2.4.2.4 Color Theme Tab

The Color Theme Tab allows you to customize the colors for Passwordstate.

You can use the default colors as specified by you Passwordstate Security Administrator(s), or you can pick your own.

Note: The Security Administrators of Passwordstate can use a feature called 'User Account Policies', which may override any settings you specify here.



2.4.2.5 Authentication Options Tab

There are a variety of different Authentication Options available when you first browse to the Passwordstate web site. By default you will use the 'System Wide' authentication option as specified by your Security Administrators, but you can elect to use a different authentication option if you like by specifying it as part of your Preferences.

Note: The Security Administrators of Passwordstate can use a feature called 'User Account Policies', which may disable any authentication options you have specified for your Preferences.

Authentication Option

There are multiple authentication options available to you, and they will vary depending on whether your Passwordstate Administrators have enabled Active Directory Single Sign-On for the Passwordstate web site.

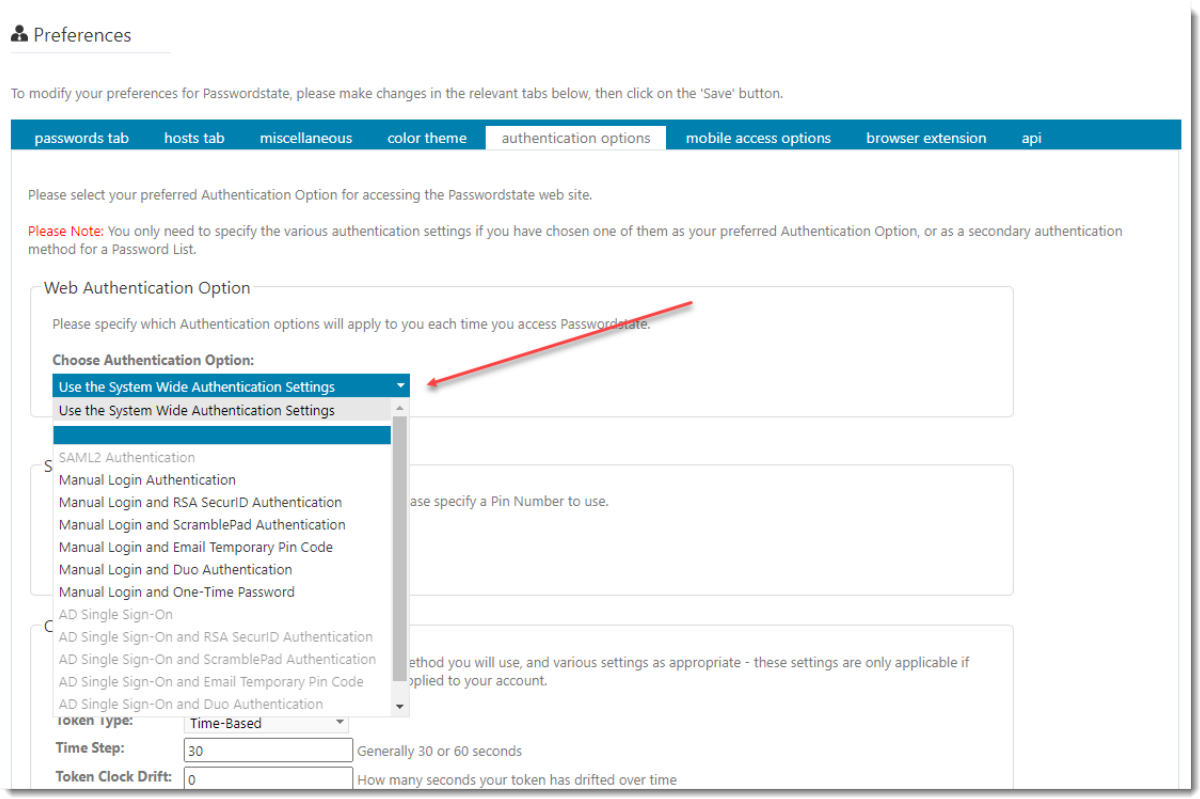
The following table describes each of the Authentication Options:

Use the System Wide Authentication Settings	Any one of the below authentication options as set by your Security Administrators
SAML2 Authentication	Authenticate against a SAML 2.0 provider. Note: Your Passwordstate email address must match what's configured for your account on the SAML2 provider's web site
Manual Login Authentication	This options will present you with a screen where you can manually specify your domain username and

	password. Passwordstate will then validate this against Active Directory.
Manual Login and Google Authenticator	In additional to manually specifying your AD username and Password, you must also specify a valid Google Verification Code for your Google Authenticator application - see instructions below for this
Manual Login and RSA SecurID	In additional to manually specifying your AD username and Password, you must also specify a valid SecurID Passcode. Your Security Administrators must first follow the provided instructions to prepare Passwordstate for SecurID authentication
Manual Login ScramblePad Authentication	ScramblePad Authentication requires you to match a pin number which is assigned to your account, to a randomly generated string of letters - see below for a screenshot
Manual Login and Email Temporary Pin Code	This authentication option will send you a temporary Pin Code to any email address you specify - which could also be an SMS Gateway if required. The temporary Pin Code expires after a set period, set by the Security Administrator(s) of Passwordstate, and cannot be reused after it expires. This authentication option requires you to validate both your Active Directory account credentials, plus the temporary Pin Code
Manual Login and Duo Authentication	In additional to manually specifying your AD username and Password, you must also specify your Duo Username, which then allows you to use the various Duo Authentication options
Manual Login and One-Time Password	In additional to manually specifying your AD username and Password, you can use a software or hardware based On-Time Password Authentication option, based on either the TOTP or HOTP algorithms
Manual Login and RADIUS Authenication	Authenticate your AD Account, as well as to a RADIUS server
Manual Login and YubiKey Authentication	In additional to manually specifying your AD username and Password, you can also authentication using YubiKey Authentication - either Yubico Cloud OTP, or TOTP & HOTP
AD Single Sign-On	If Passwordstate is installed and configured correctly, you should not be prompted with a browser authentication window when using this option. The browser should "passthrough" your domain credentials to the IIS web site, and the 'Windows Authentication' within IIS will validate your credentials against AD. If you are being prompted to enter your username and

	password, please ask your Security Administrators to investigate
AD Single Sign-On and Google Authenticator	Google Authenticator with Passthrough AD Authentication
AD Single Sign-On and RSA SecurID Authentication	RSA SecurID Authentication with Passthrough AD Authentication
AD Single Sign-On and ScramblePad Authentication	ScramblePad Authentication with Passthrough AD Authentication
AD Single Sign-On and Email Temporary Pin Code	This authentication option will send you a temporary Pin Code to any email address you specify - which could also be an SMS Gateway if required. The temporary Pin Code expires after a set period, set by the Security Administrator(s) of Passwordstate, and cannot be reused after it expires.
AD Single Sign-On and Duo Authentication	You must specify your Duo Username, which then allows you to use the various Duo Authentication options
AD Single Sign-On and One-Time Password	You must specify your One-Time Password based on the use of either a software or hardware token, for either the TOTP or HOTP algorithms
AD Single Sign-On and RADIUS Authentication	Authenticate against a RADIUS server
AD Single Sign-On and YubiKey Authentication	Authentication using YubiKey Authentication - either Yubico Cloud OTP, or TOTP & HOTP

Note: If required, your Security Administrators can reset your Preferences settings, so there is no chance you can permanently lock yourself out of Passwordstate



ScramblePad Pin Number

You must associate a ScramblePad Pin Number with your account if you wish to use ScramblePad Authentication. When a pin number is set, and the authentication option is selected, your login screen will look similar to the screenshot below.

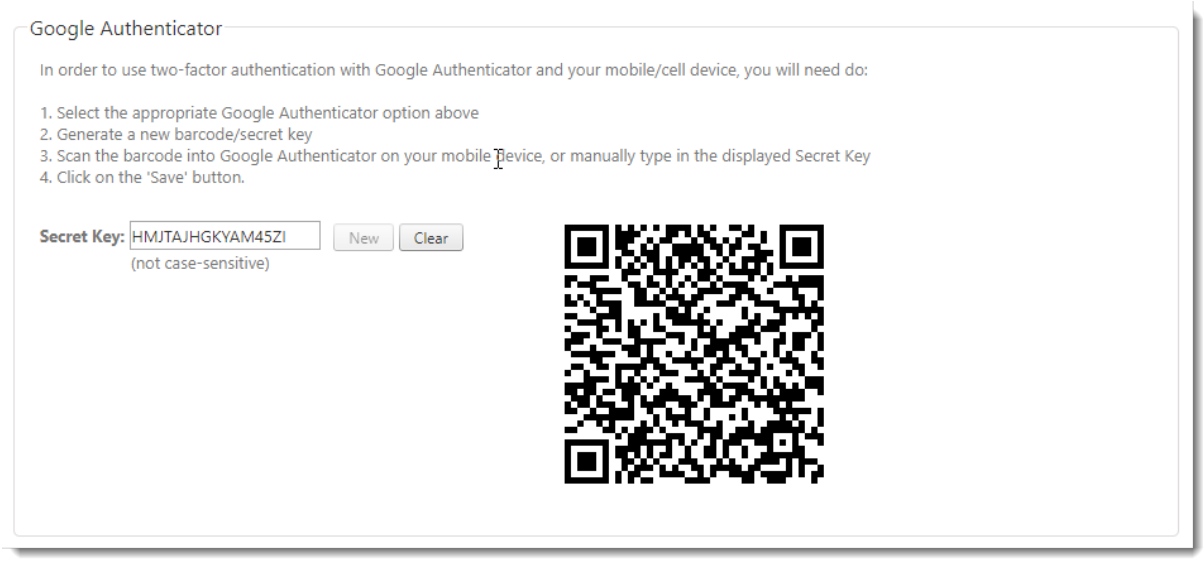
You must match your in number digits, to the randomly generated letters. i.e. If your Pin Number is **1234**, you would need to type **tyzp** to authenticate.

wylu

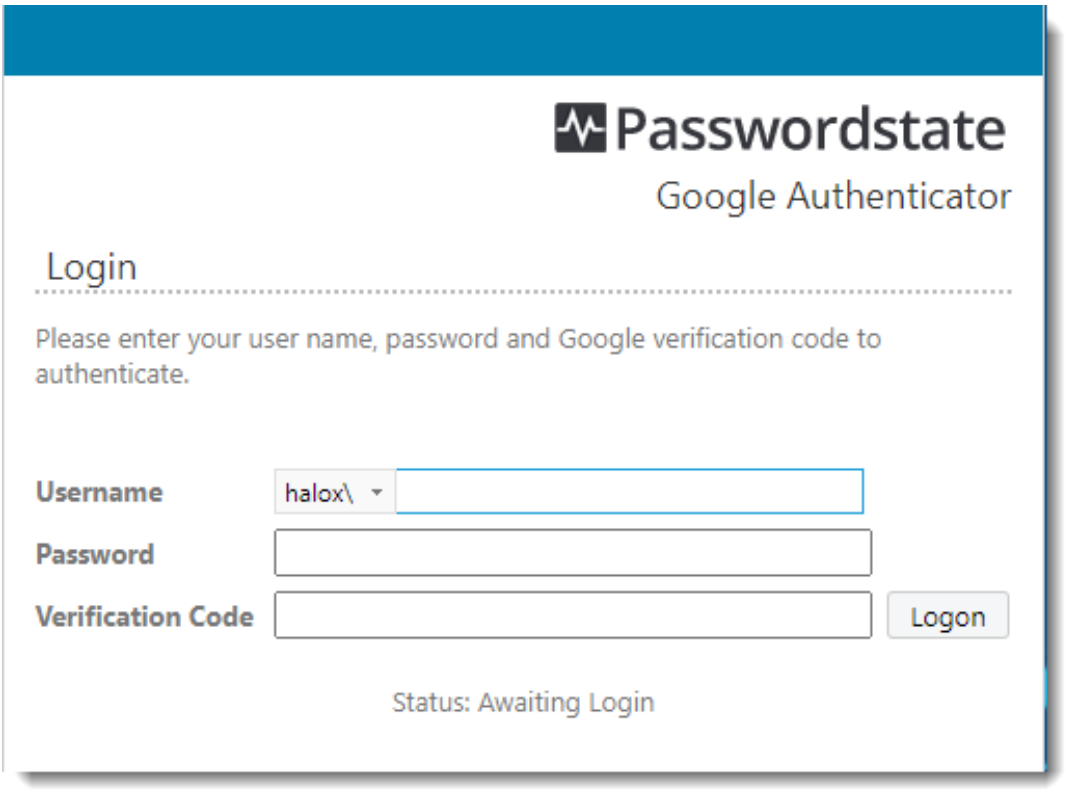
Google Authenticator

Prior to using Google Authenticator, you must first generate a new secret key for your account. To do so, you can follow these instructions:

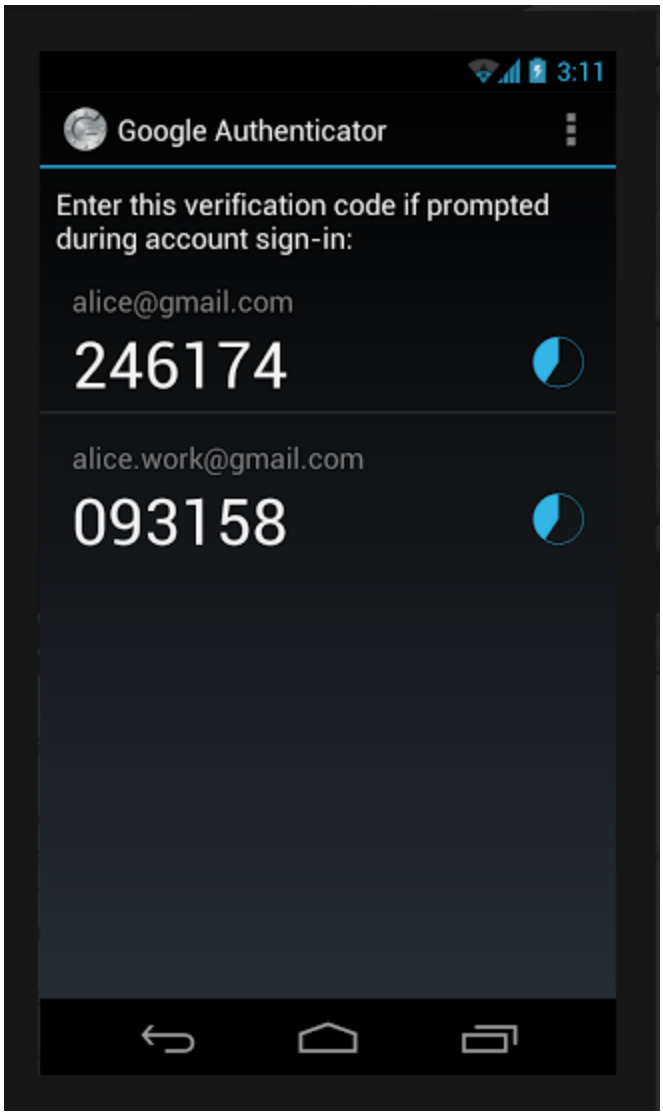
- First install Google Authenticator on your mobile device – Android, iOS & Windows Phone
- Generate a new barcode/secret key
- Scan the barcode into Google Authenticator on your mobile device, or manually type in the displayed Secret Key
- Click on the 'Save' button.



Once you have successfully enabled Google Authenticator with Passwordstate and on your mobile/cell device, then you will be presented with the following login screen next time you visit Passwordstate (this is the screen for 'Manual AD and Google Authenticator').



You will now have a maximum of 60 seconds to copy the verification code from your mobile/cell device (image below), into Passwordstate. After 60 seconds, a new verification code will appear on your device.

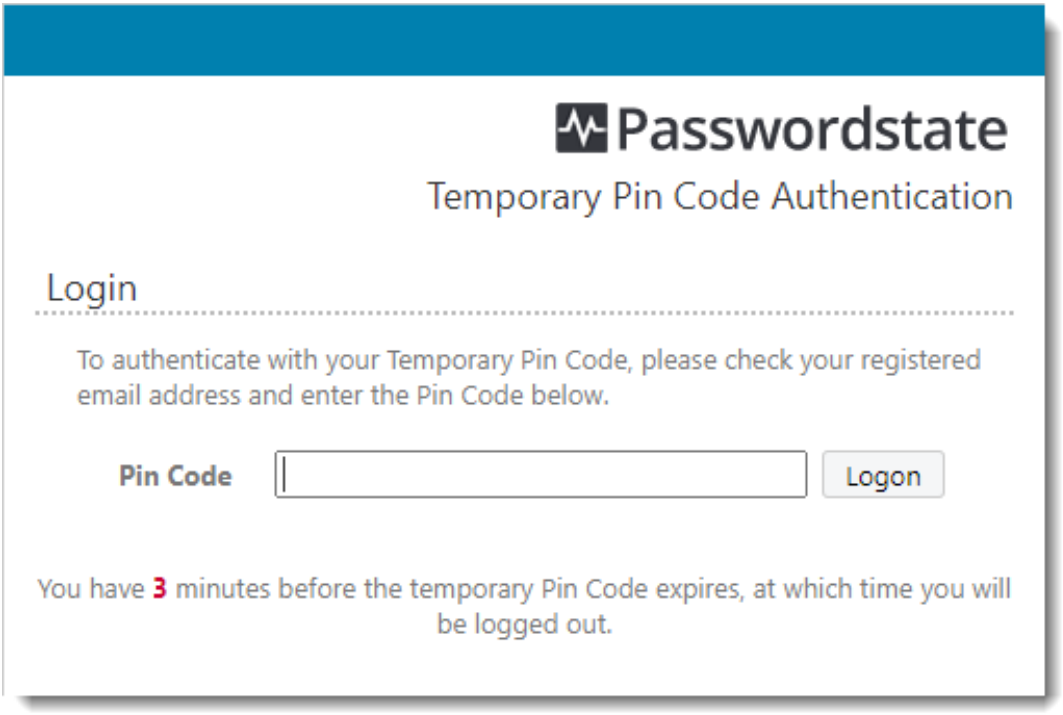


Email Temporary Pin Code

When you select a Temporary Pin Code Authentication option, you must also specify the email address where you want the Pin Code sent to. This email address could either be your work email address, a personal one, or the email address of an SMS Gateway so you can receive the Pin Code via a SMS message.

Once you have configured your account in Passwordstate, you will see the following type of screen when you first authentication to the Passwordstate web site:

Note: The Expiry Time, and length of the Pin Code can be modified by your Passwordstate Security Administrator(s).



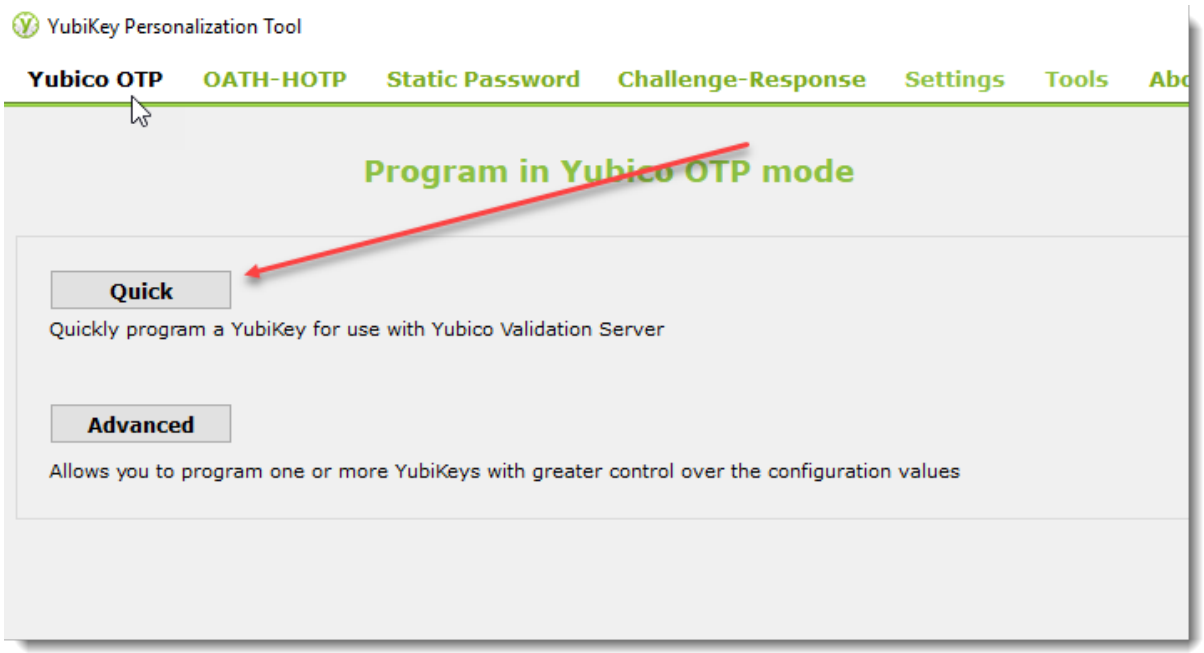
YubiKey Authentication

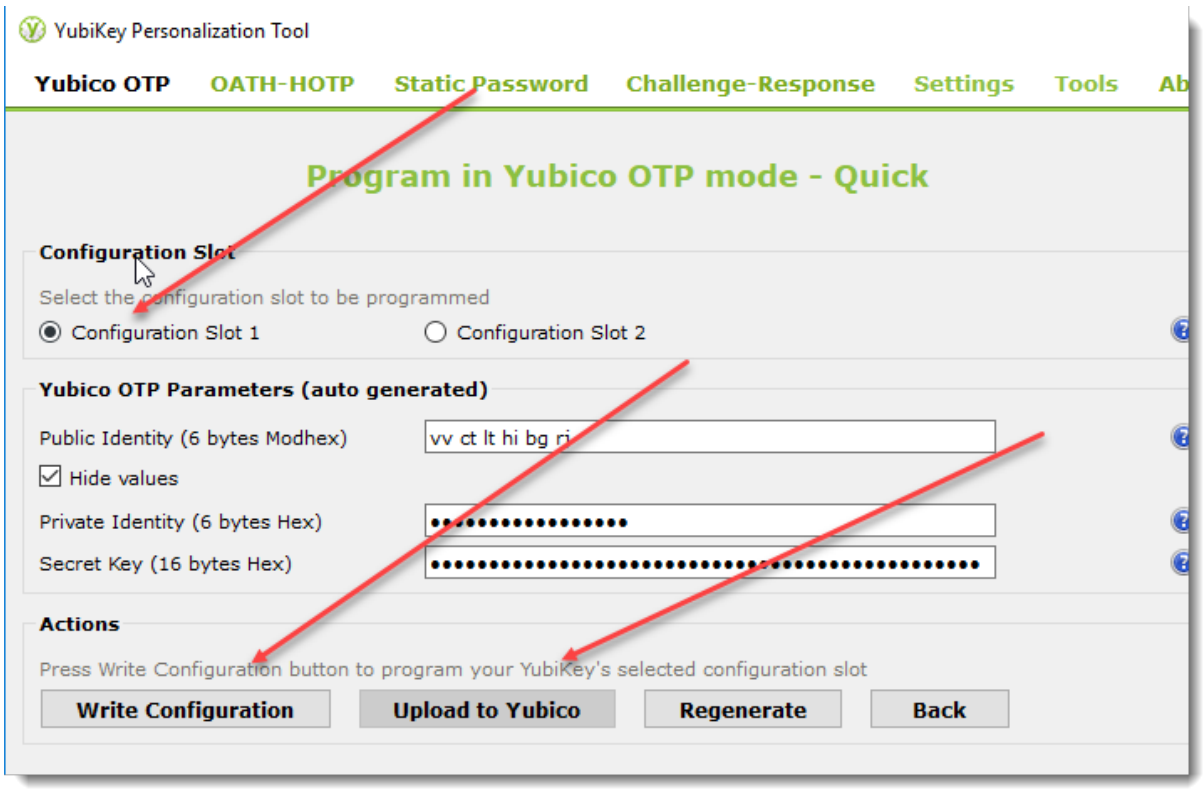
Passwordstate can support the following YubiKey authentication methods:
- Yubico OTP (this queries Yubico's API on the internet)
- OATH - HOTP (couner-based algorithm which does not require internet connectivity)
- OATH - TOTP (time-based algorithm which does not require internet connectivity)

By default, new YubiKey's are configured for Yubico OTP, but the configuration can be changed using Yubico tools. Below are instructions for configuring your YubiKey for each of the authentication options above. The following tools will need to be downloaded and installed on your desktop:
- To configure for Yubico OTP or HOTP, you need this tool - https://www.yubico.com/products/services-software/download/yubikey-personalization-tools/
- To configure and authenticate using TOTP, you need this tool - https://www.yubico.com/products/services-software/download/yubico-authenticator/

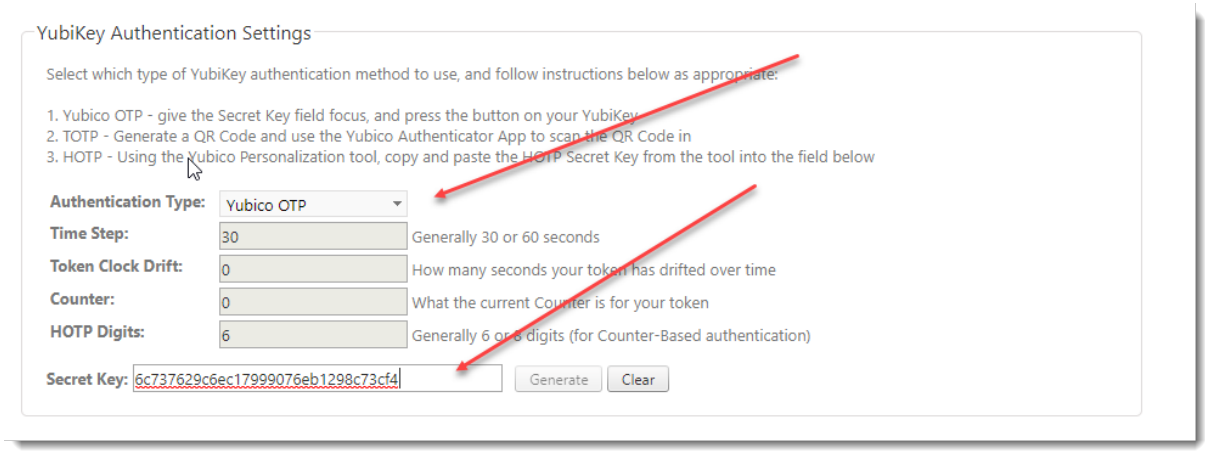
Configure YubiKey for Yubico OTP Support
As mentioned, this step may not be required as your YubiKey should be configured for this option by default. Follow the instructions below if this is required, and changing the Identities here on your YubiKey requires you to upload those changes to Yubico's web site.

You also need to select which Slot you want the configuration written to.



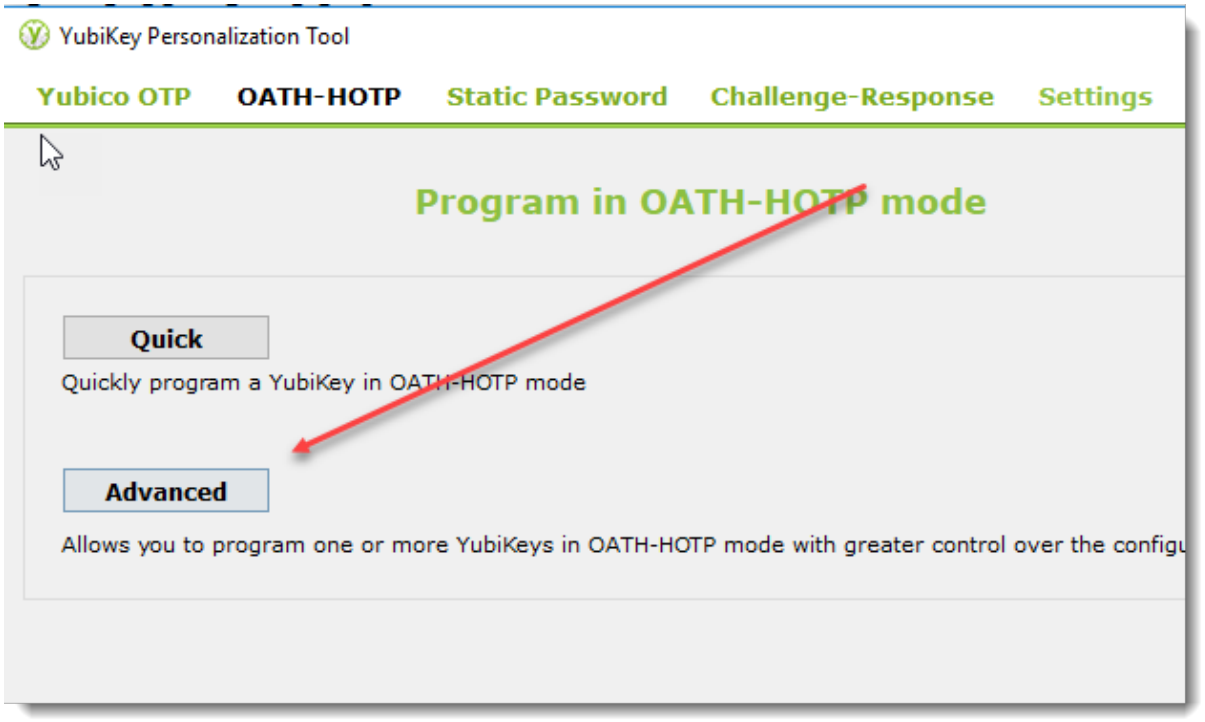


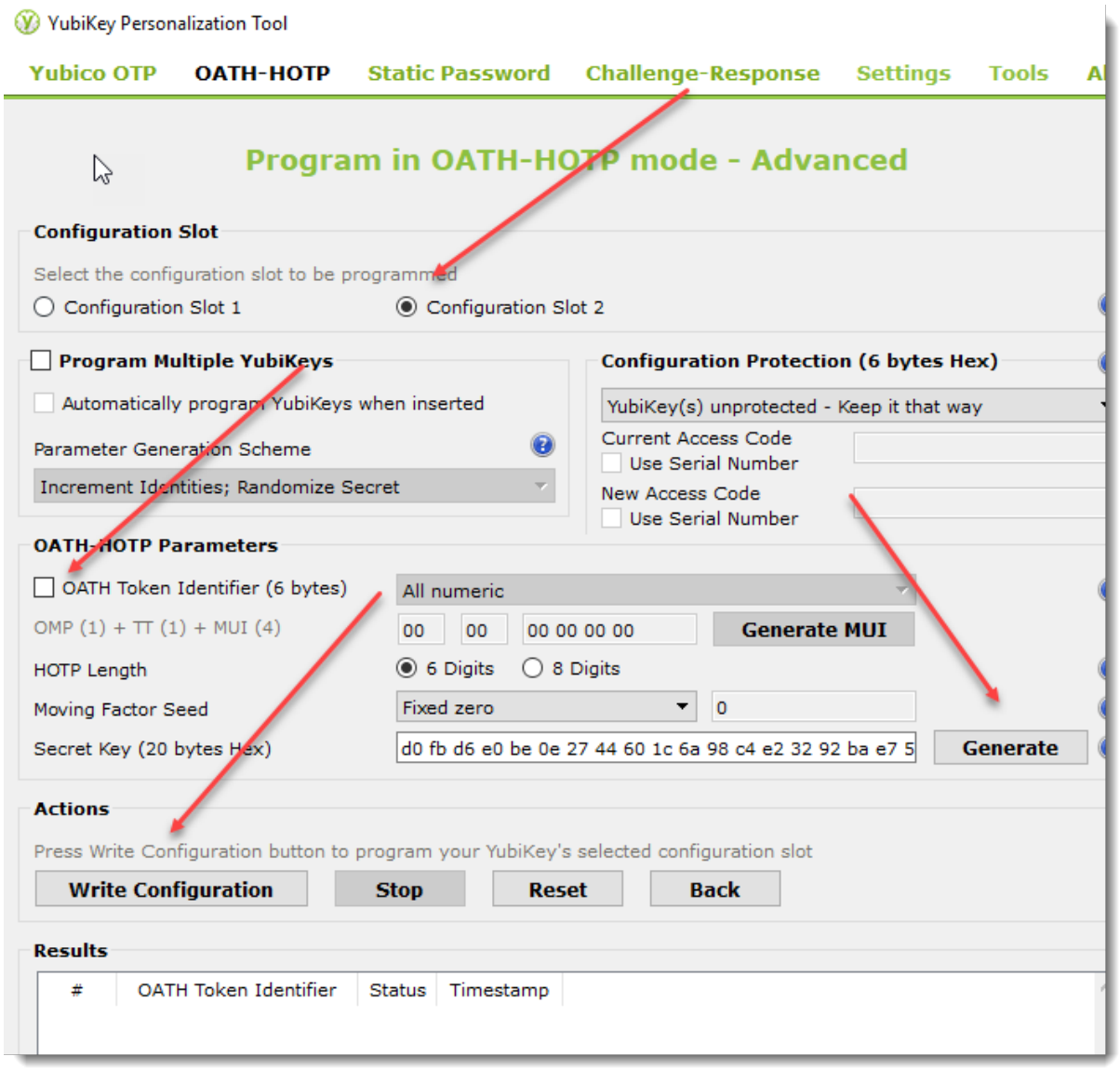
And then in Passwordstate, on your Preferences screen, you select Yubico OTP, select the Secret Key field, and then press the button on your YubiKey to populate your secret key - and 'Save' your Preferences.



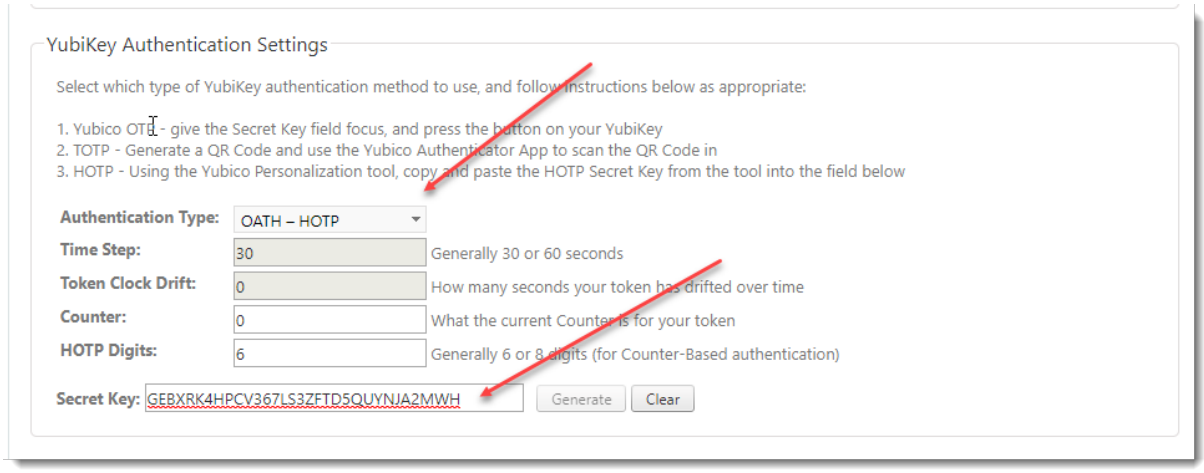
Configure YubiKey for OATH - HOTP Support

To configure your YubiKey for HOTP support, you need to click the 'Advanced' button, as per the screenshot below, as you need to deselect the 'OATH Token Identifier (6 bytes) option. Generate your Secret Key, and then write the configuration to the required Slot.





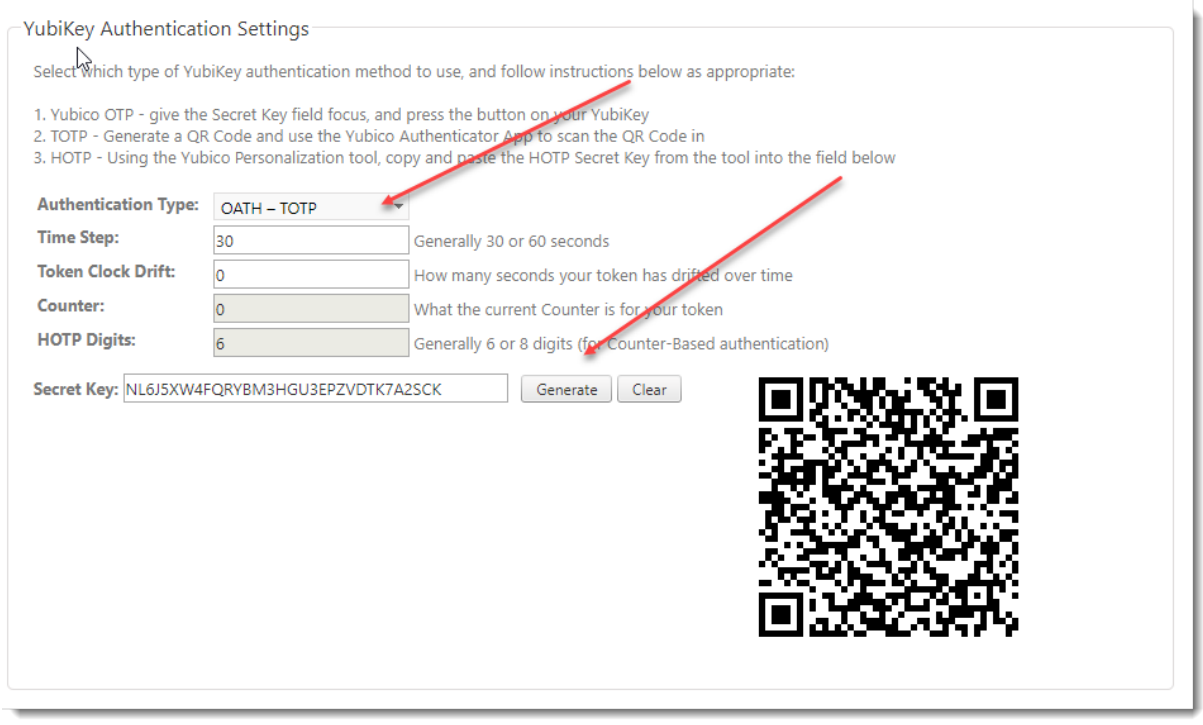
And then in Passwordstate, on your Preferences screen, you select OATH - HOTP, and copy and paste the 'Secret Key (20 bytes Hex)' you see in the screenshot above, into the Secret Key field below - and 'Save' your Preferences.



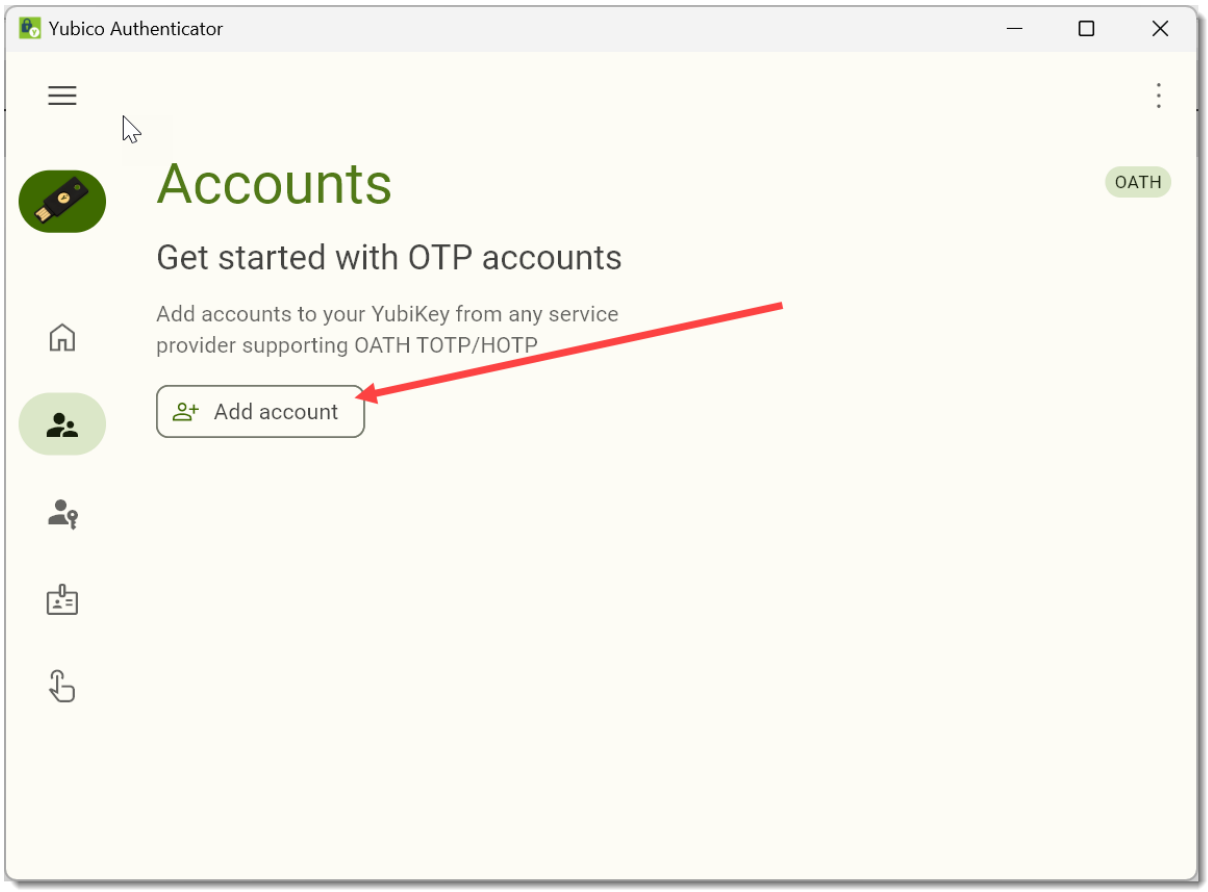
Configure YubiKey for OATH - TOTP Support

To configure your Yubikey for OTP support, you need to use the Yubico Authenticator application. It is also this application which is used to generate your One-Time Passwords for authentication.

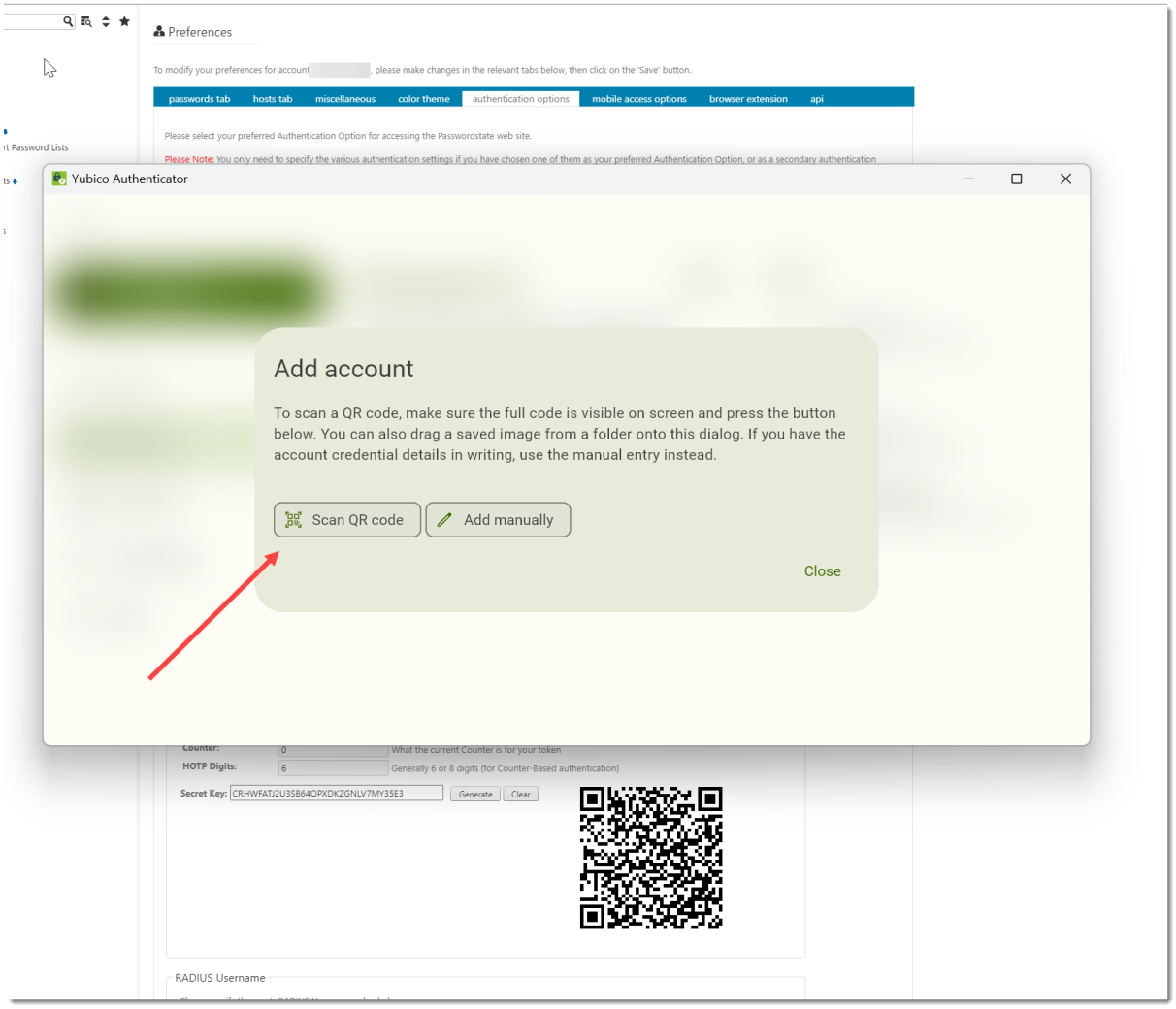
In Passwordstate, on your Preferences screen, you need to select 'OATH - TOTP', and click then **Generate** button so the QR Code is displayed. Do not save these changes just yet.



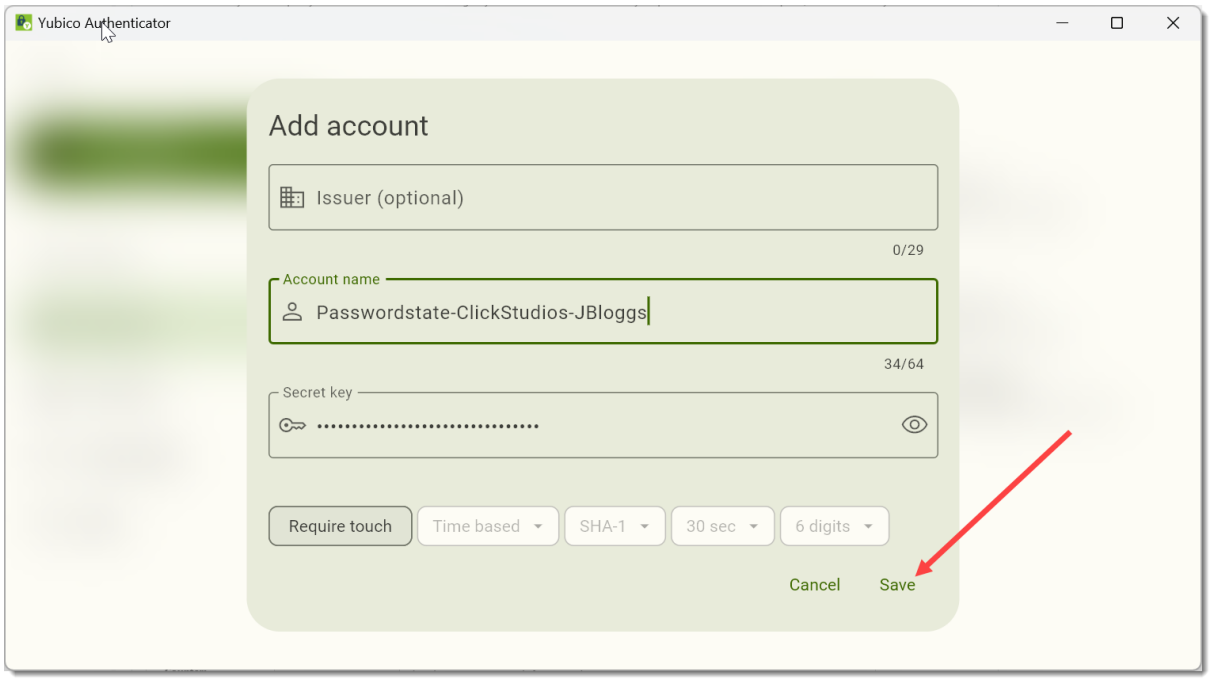
Insert your Yubikey into your workstation, launch the Yubikey Authenticator software and select **Accounts** -> **Add Account**:



Make sure the QR code form your Passwordstate preferences screen is visible somewhere on the screen and click the **Scan QR Code** button:



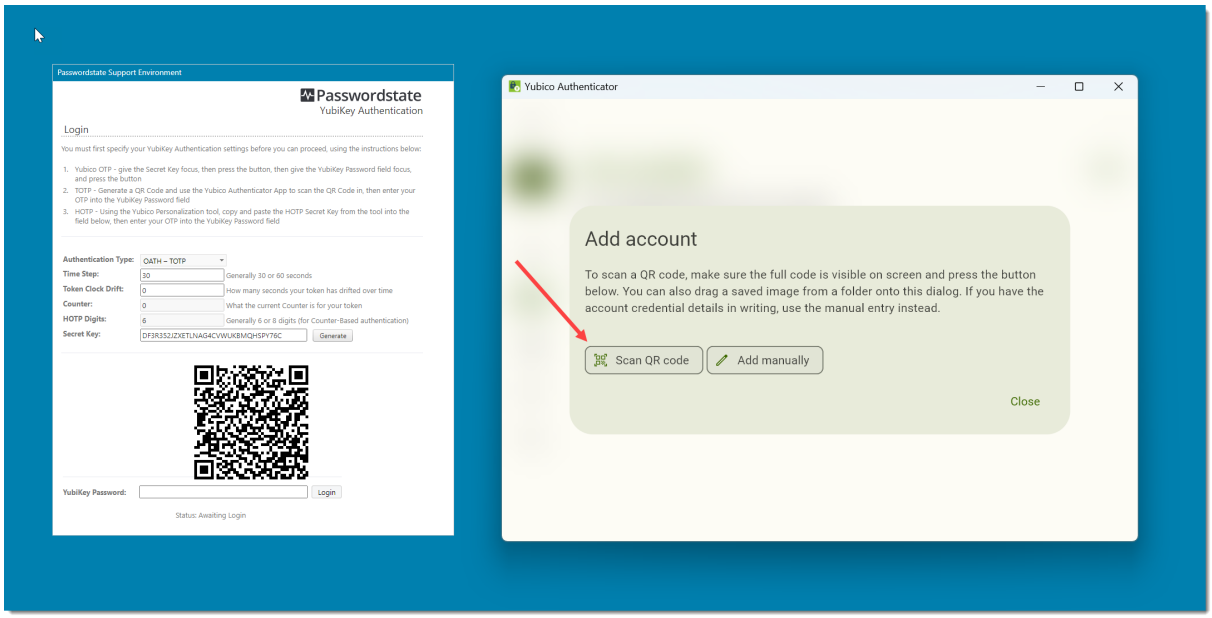
Click **Save**

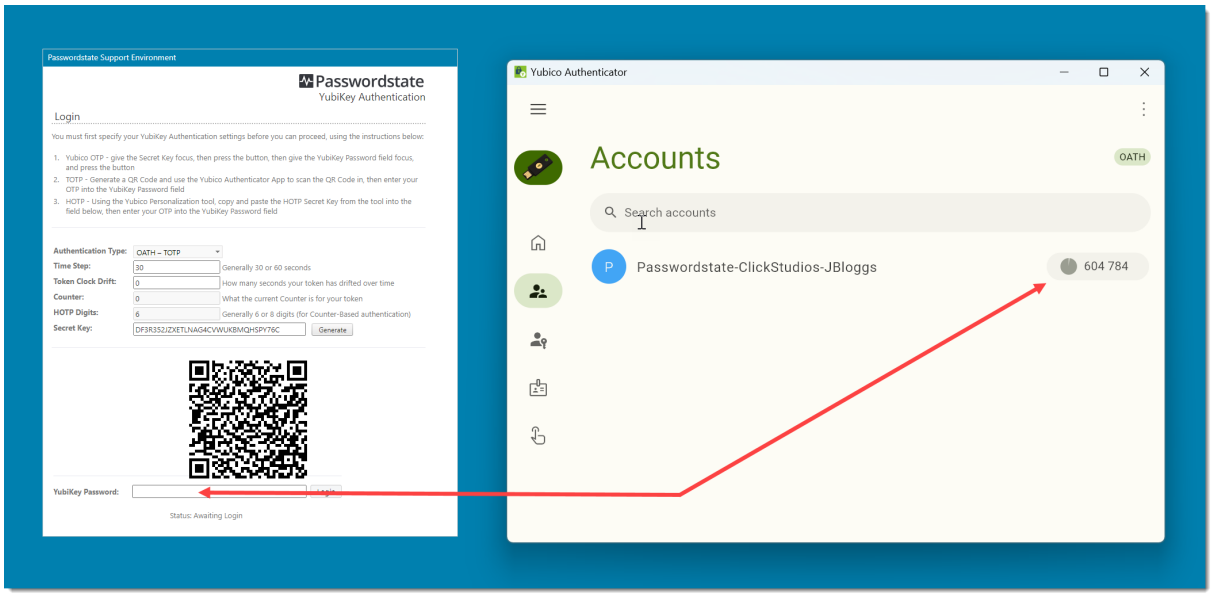


Back in Passwordstate, click save on your Preferences screen to save that Secret key/QR code that you generated in the step above.

Next, change the authentication option in Passwordstate to use Yubikey Authentication. You can set this in a few different areas which depends on which Passwordstate users you want to force Yubikey authentication for. This blog post explains where you can make this change according to your requirements: https://blog.clickstudios.com.au/specifying-authentication-options/. When you next try to log into Passwordstate, you will be required to copy the One Time Code from the YubiKey App and paste it into your Passwordstate login screen to gain access to the system.

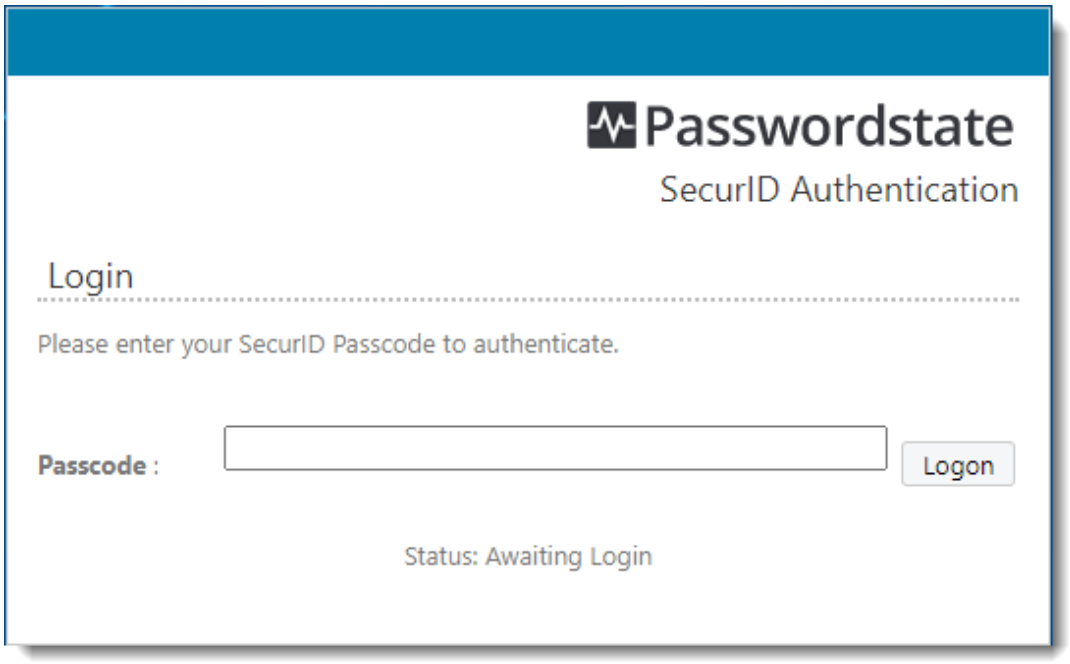
If you do not configure your personal preferences in Passwordstate as outlined above before enabling Yubikey Authentication, you will be presented with the equivalent information on your Passwordstate login screen. Use the Yubikey Authenticator App to scan the QR code as a once off process, and then you can use the One Time Codes from the Yubikey App to authenticate.





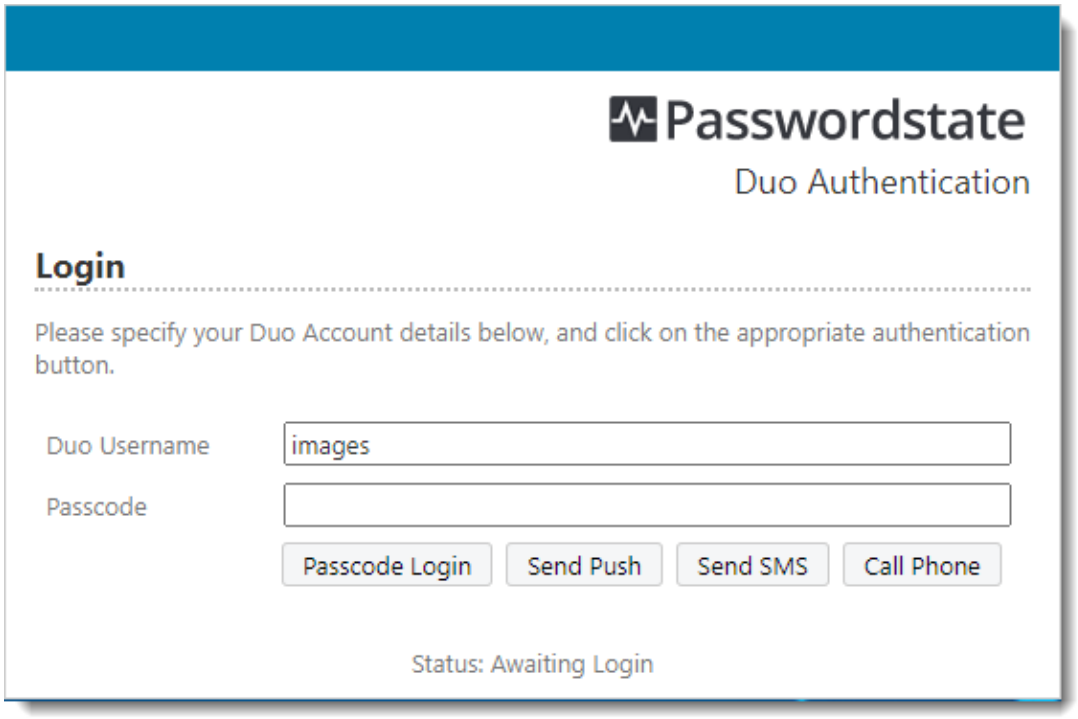
SecurID Authentication

You must specify your SecurID User ID on this Preferences screen, and then you can begin to use this two-factor authentication method. You Passcode is a combination of your Pin, plus the Tokencode.



Duo Authentication

You must specify your Duo Username, and then you can use one of the multiple Duo Authentication options. If you have more than one device assigned to your Duo account, then you will be presented with a list of devices to use.



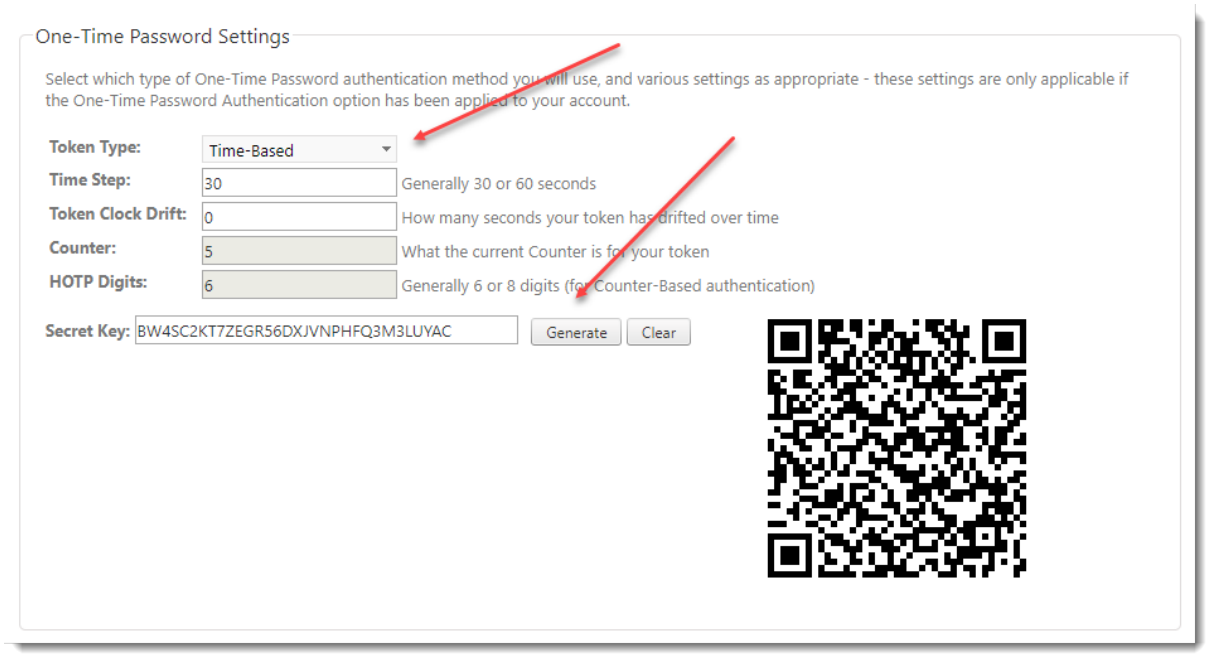
One-Time Password

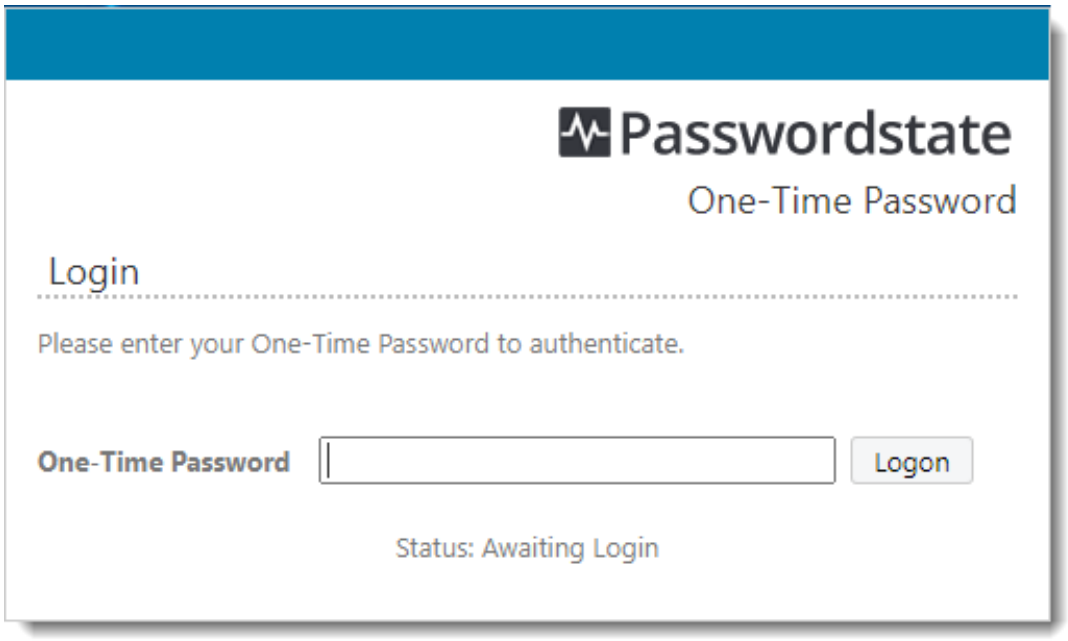
One-Time Password authentication supports the TOTP and HOTP algorithms - TOTP being time-based, and HOTP being counter-based. Both hardware and software tokens can be used for this authentication method

In order to use this authentication option, you must select the Password Type, and then select various settings for your token.

The Secret Key needs to be specified in Base32 format, which is a string of 32 characters in length. If you are using a software token, then you can generate a random Secret Key in Passwordstate, and then specify this key in your software token software. If you are using hardware tokens, you should be been provided with the Base32 Secret Key when you were provided your token.

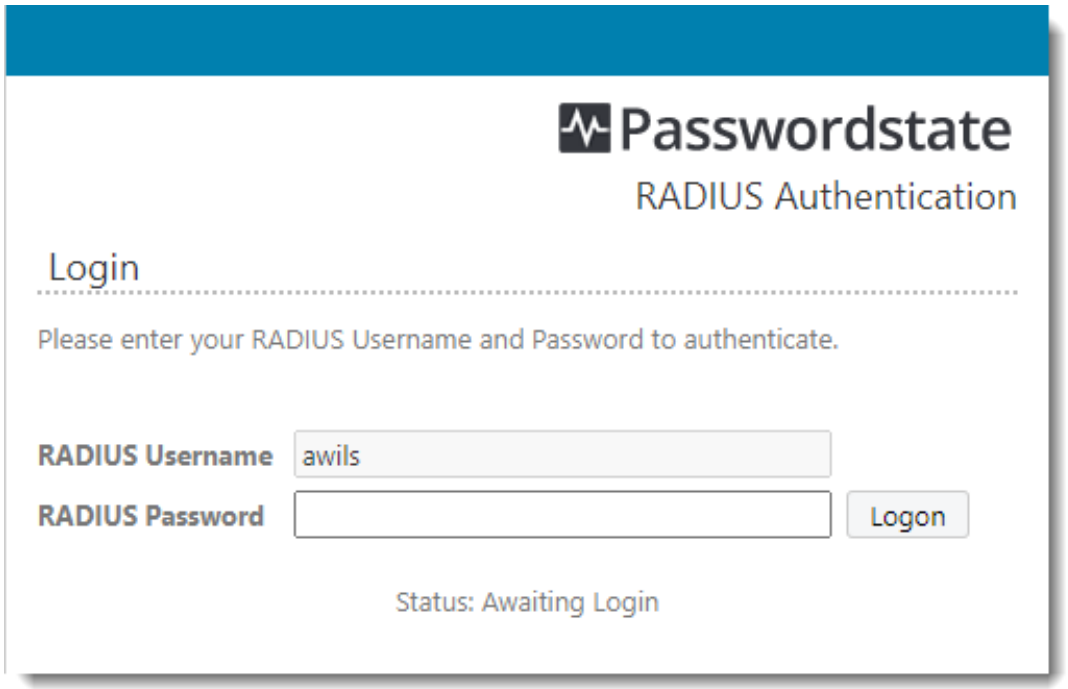
Note: If someone enables this authentication method for you, but you have not configured the settings below, you will be prompted to configure them when you first try and authenticate to the Passwordstate web site.





RADIUS Authentication

RADIUS Authentication allows you to authenticate against a RADIUS server, where the RADIUS server can be configured for different types of authentication per user - even various two-factor methods.

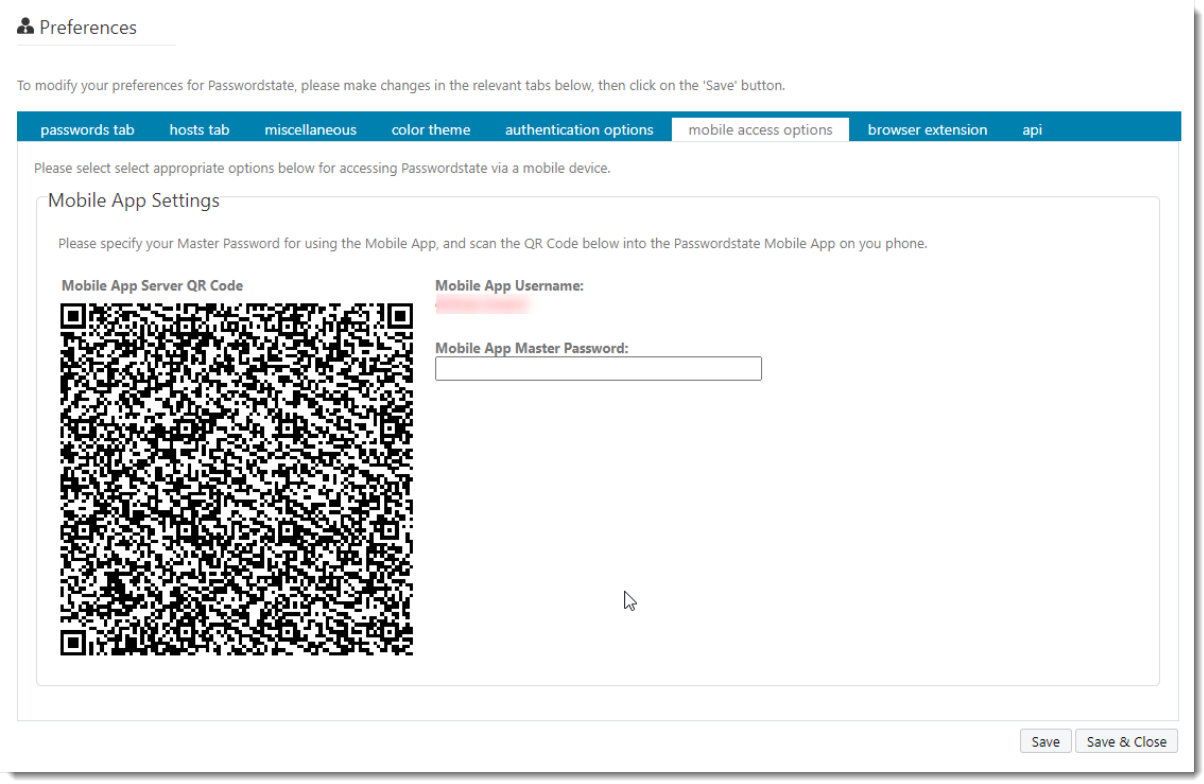


2.4.2.6 Mobile Access Options Tab

The Mobile Access Options tab allows you to specify various settings for the Passwordstate native iOS and Android Apps, and to scan the Mobile App QR code so you can being using the App.

Note: Please ensure you use a strong Master password for the Mobile App authentication.

Full instructions for the Mobile App can be found under the Help Menu in Passwordstate - the menu is called Mobile App Manual.



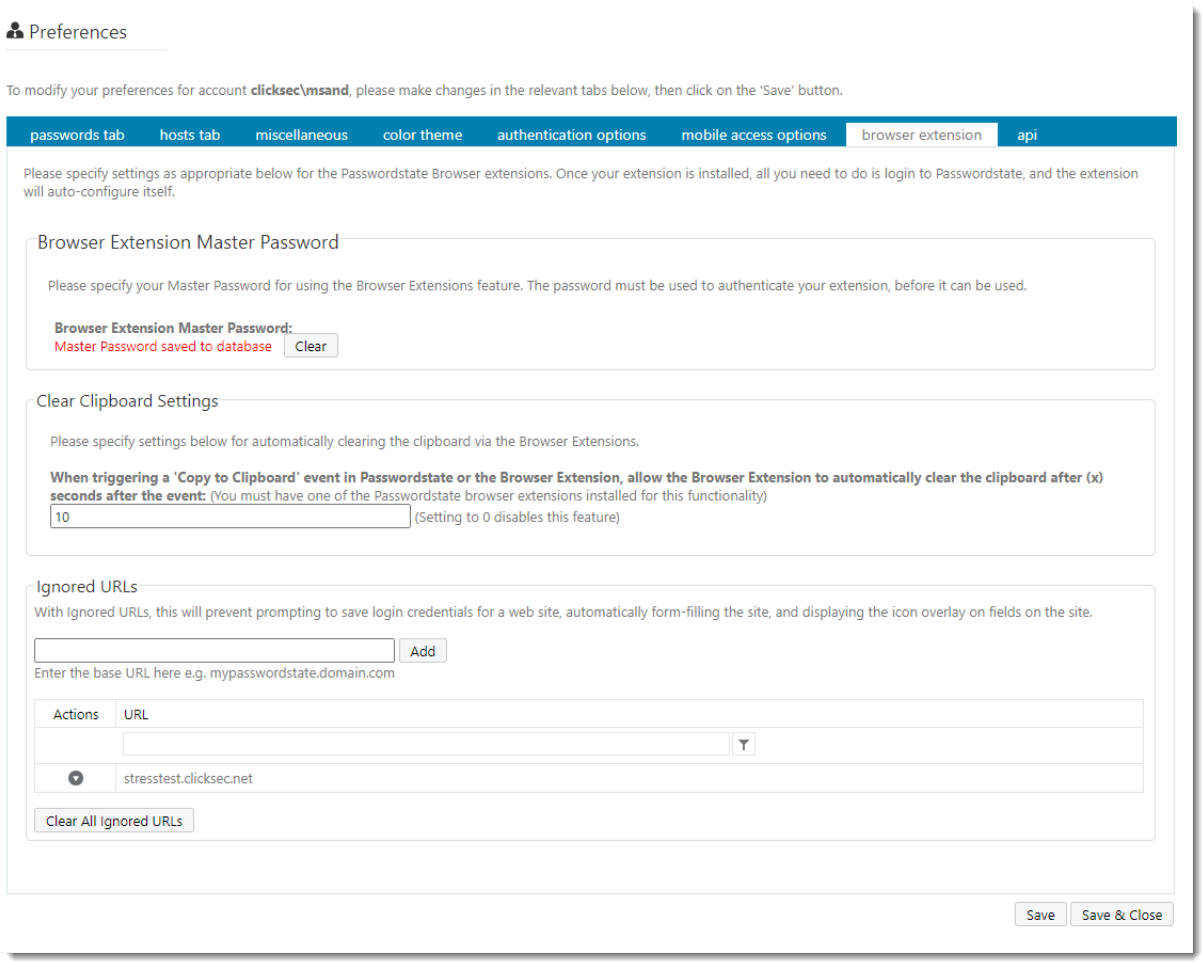
2.4.2.7 Browser Extension

The Browser Extension tab allows you to specify various settings for the Chrome Browser Extension, which is used to automatically form-fill web site logins.

In particular you can:

- Specify your Master Password to be used with the browser extensions
- Specify which URLS will be ignored by the Browser Extension, so that it doesn't prompt you to save login credentials, form-fill the sites, or show the icon overlay
- The browser extension can also be used to automatically clear any contents in your clipboard at a set interval.

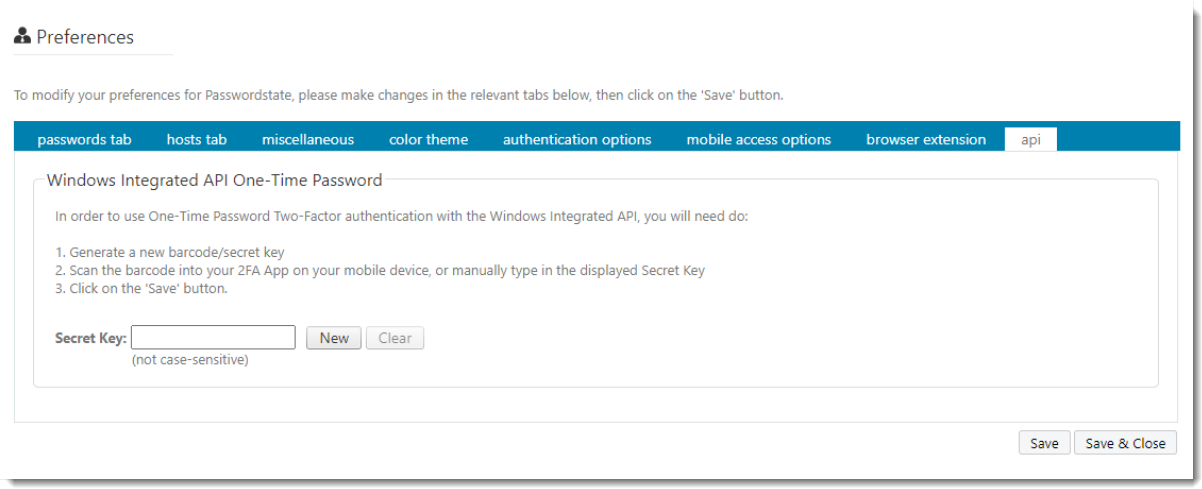
Please refer to the Browser Extension Manual for further instructions.



2.4.2.8 API

Your Security Administrator's of Passwordstate can require Two-Factor Authentication when making calls to the Windows Integrated API.

If so, on the API tab on your Preferences screen, you can create the required 2FA Secre and scan the QR Code into your mobile device, or any other compatible app.



2.4.3 Email Notifications

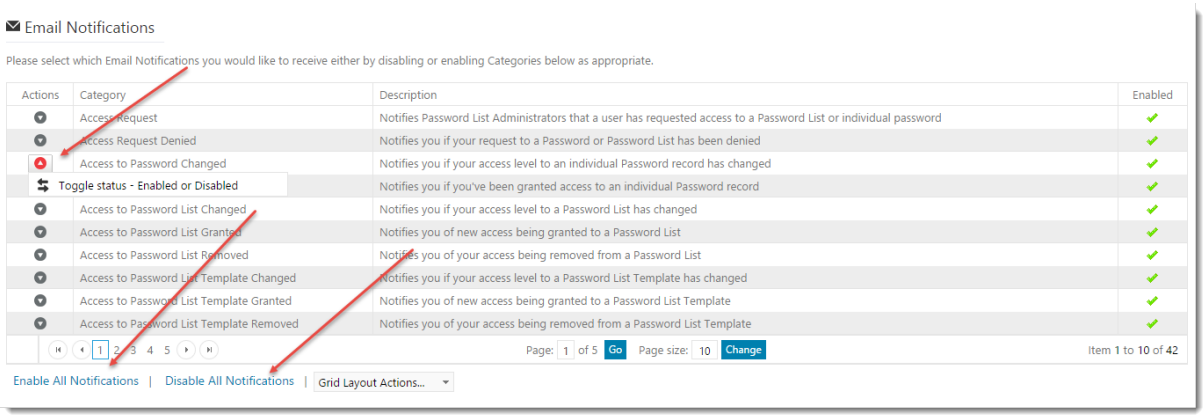
The Email Notifications screen allows you to enabled/disabled one or more of the many different email notifications Passwordstate can send you.

Note 1: There is a feature called 'Email Notification Groups' which your Security Administrators of Passwordstate can use, and using this feature for your account will cause the 'Choose Email Notifications' button below to be disabled

Note 2: Security Administrators can also disable one or more Email Notifications system wide, so if you are not receiving emails you are expected to, please speak with one of your Security Administrators

Choose Email Notifications

By Clicking on the 'Choose Email Notifications' button, you will be presented with a list of email categories, which can either be enabled or disabled. There is also an option to enable or disable all email notifications with the buttons at the bottom of the grid.



3 Hosts

Within the Hosts tab, there are two primary functions which can be used:

- Adding Hosts records into the system so that accounts on them can be managed (account discoveries, password resets and account heartbeats)
- Use the Remote Session Launcher utility. With the Remote Session Launcher utility, there are two different types available:

Browser Based
- Runs from within your Browser - can be used on all Operating Systems
- RDP & SSH Sessions
- All sessions are initiated (proxied) from the Passwordstate web server
- Session Recording and Playback

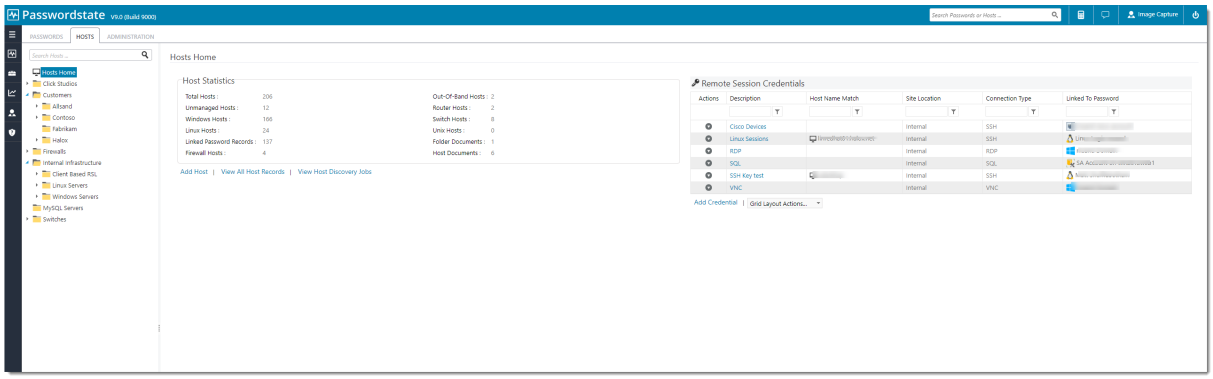
Client Based
- Requires Client Install - Windows Operating Systems only
- RDP, SSH, Telnet, VNC, SQL and Teamviewer Sessions
- All sessions are initiated from the user's PC
- No Session Recording

Note 1: By default, all users have access to all features under this Hosts tab. It is recommended a Security Administrator of Passwordstate visit the page Administration -> Passwordstate Administration -> Feature Access -> Hosts tab and Remote Sessions tab, and review each of the varying levels of access, and modify permissions as appropriate.
Note 2: Microsoft have removed the ability to pass a SQL Server account password value to SQL Server Management Studio via the command line, in Management Studio 2018. Authenticating with Active Directory accounts works with Management Studio 2018, but if you wish to use SQL Accounts you will instead need to use Management Studio 2017.

3.1 Hosts Home Screen

When you click on the Hosts Home icon, you will be presented with a screen were you can see some statistics regarding the number of Host records which have been added to Passwordstate, as well as any Remote Session Credentials your account has access to.

From this screen you can:
- Click on View All Host Records to see all Host records, and manage them
- Click on View Host Discovery Jobs to manage Discovery Jobs for querying Active Directory for Host records - and import them into Passwordstate
- And manage Remote Session Credentials which can be used with the Remote Session Launcher Utility.



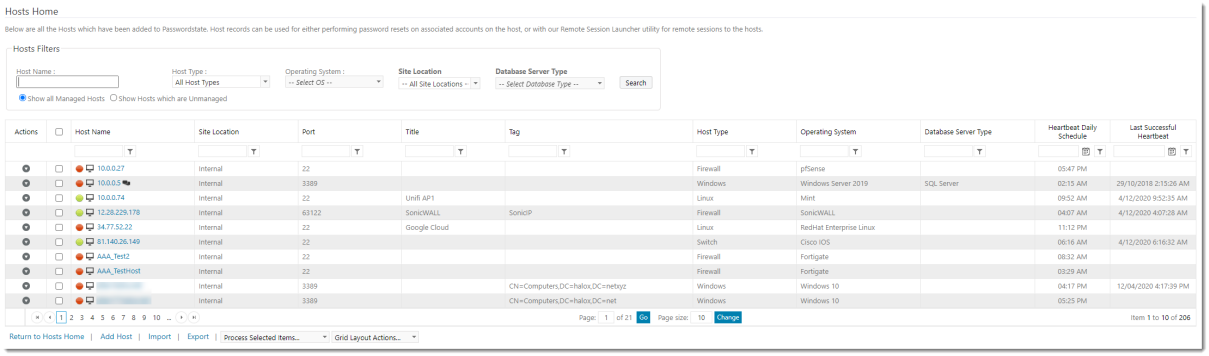
3.1.1 View All Host Records

On the View All Host Records screen, you can Add/Import/Edit hosts into Passwordstate, so they can be used to perform Password Resets for accounts on the Hosts, or so they can be used for the Remote Session Launcher feature.

On this screen there are various features available to you, in particular:

- Adding Hosts manually
- Importing Hosts via a CSV file
- Exporting Hosts to a CSV file
- Setting a Host to 'Unmanaged' status - setting an Host to unmanaged means no Password Resets account occur for accounts on the Host
- Send a Heartbeat request to the Host to see if it is available on the network (You can also set the time frame in which regular scheduled Heartbeats occur for different operating systems, on the screen Administration -> Host Types & Operating Systems
- And deleting a Host

Note: It is also possible to import Hosts via the Passwordstate API, or use a Discovery Job to import them from Active Directory

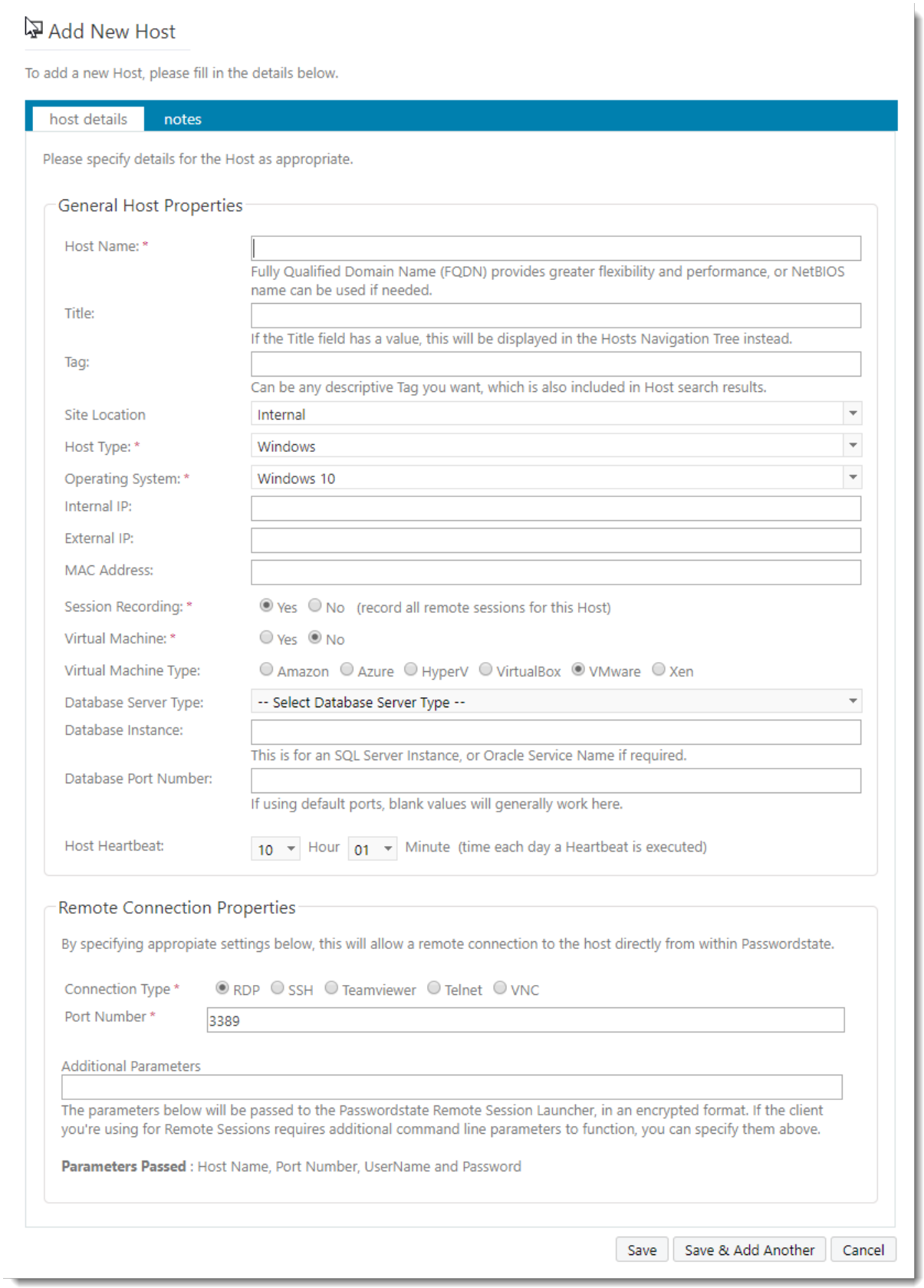


Adding New Hosts Manually

When adding new Hosts, there are a few things to consider:

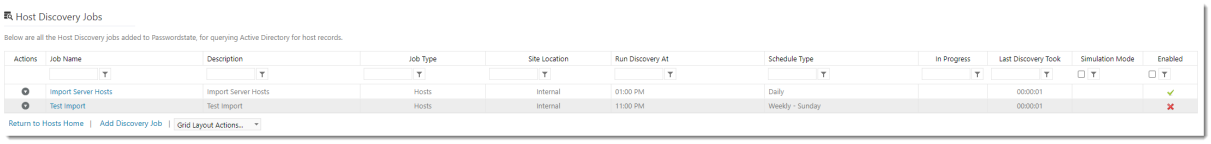
- Specifying the FQDN for the host name results in improved performance when resetting passwords, and launching Remote Sessions. It also offers greater flexibility for non-trusted Active Directory Domains, as you can apply Password Reset Scripts, Password Validation Scripts, or Remote Session Credentials, based on the domain name the host is joined to
- The Tag field can be any value you like, and is included in the search results when searching for the 'Host Name'. If using a Discovery Job for searching for Hosts in Active Directory, there's an option to include the Host's OU in the Tag field
- If the Host is a MS SQL, MySQL Server or Oracle Server, you can specify Instance details and port numbers if needed, so Passwordstate can connect to it to execute Password Reset Scripts
- If using the Remote Session Launcher utility, you can specify various properties for launching remote sessions i.e. Connection Type, Port Number, and possibly any other Remote Session Parameters needed for the Remote Session client program you're using

Note: As Telnet traffic is unencrypted, it is recommended you avoid using Telnet for connectivity if possible.



3.1.2 View Host Discovery Jobs

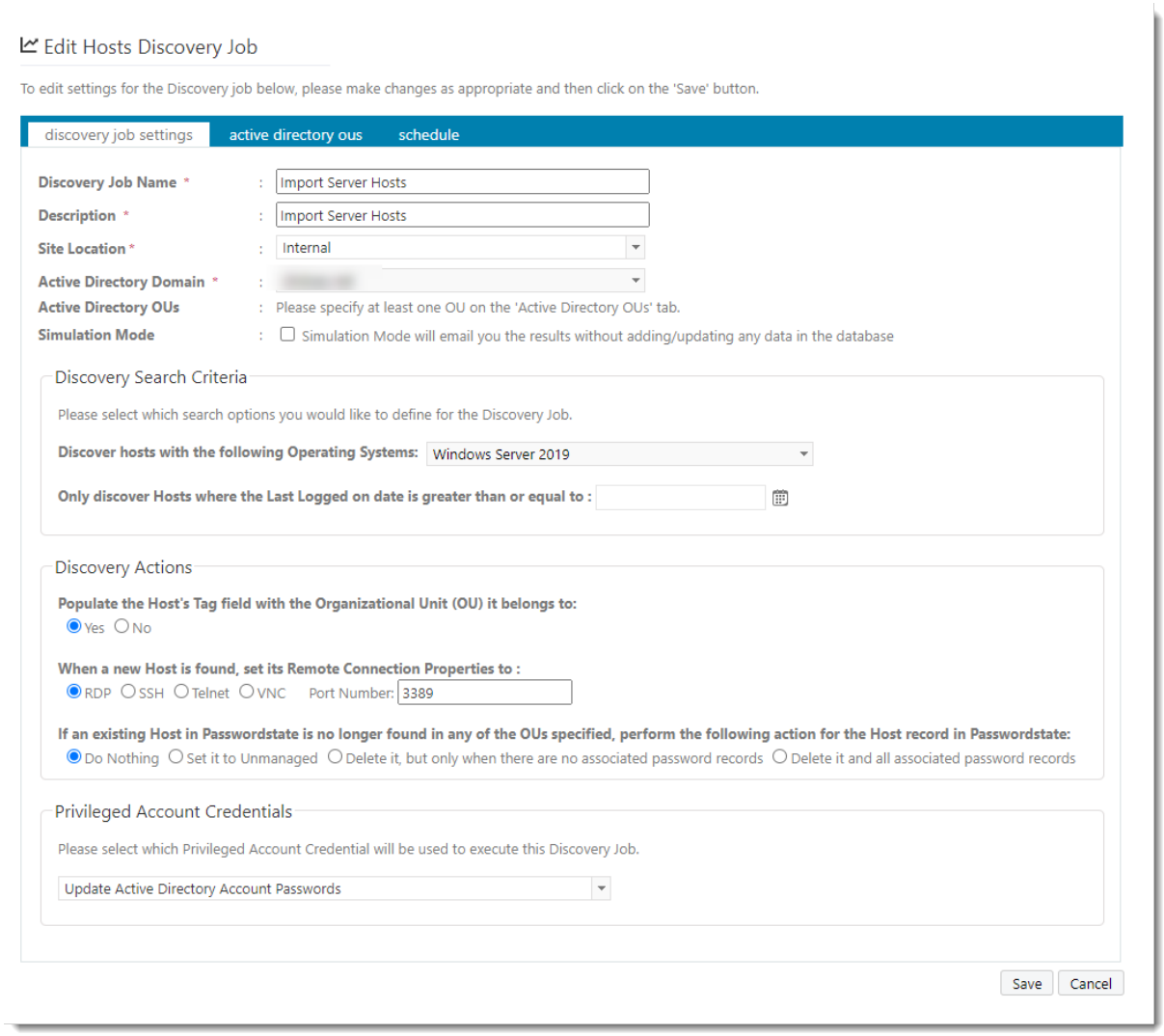
Discovering Windows & Linux Hosts on your network is simply a query of your Active Directory domain - Passwordstate does not "go out" into your network discovering host using things like route tables at all. Because of this, no specify system requirements are necessary, except for a domain account with privileges to query Active Directory.



When discovering new Windows & Linux Hosts, you have the following options available to you:

- Which Active Directory domain to query
- To query specific AD OUs, you can click on the 'Active Directory OUs' tab and specify them here
- Which type of Hosts you want to discover, based on the Operating System Level
- Only discover Hosts which have been logged into based on a set date i.e. only machines logged into since July 2014
- You can also set the Tag field for a Host to be the value of the Active Directory OU it belongs to
- As users in Passwordstate need to be given permissions to Hosts in order to use them for various features, you can set permissions on the 'Permissions' tab
- You also need to specify the 'Privileged Account' identity which will be used to query your Active Directory Domain. These Privileged Account Credentials can be added/editing/updated on the screen Administration -> Privileged Account Credentials
- And finally the schedule for how often you want the Discovery Job to be executed
- When applying permissions to the Job after it is created, whoever is given access can then administer the job, as well receive an emails with the results of the job execution

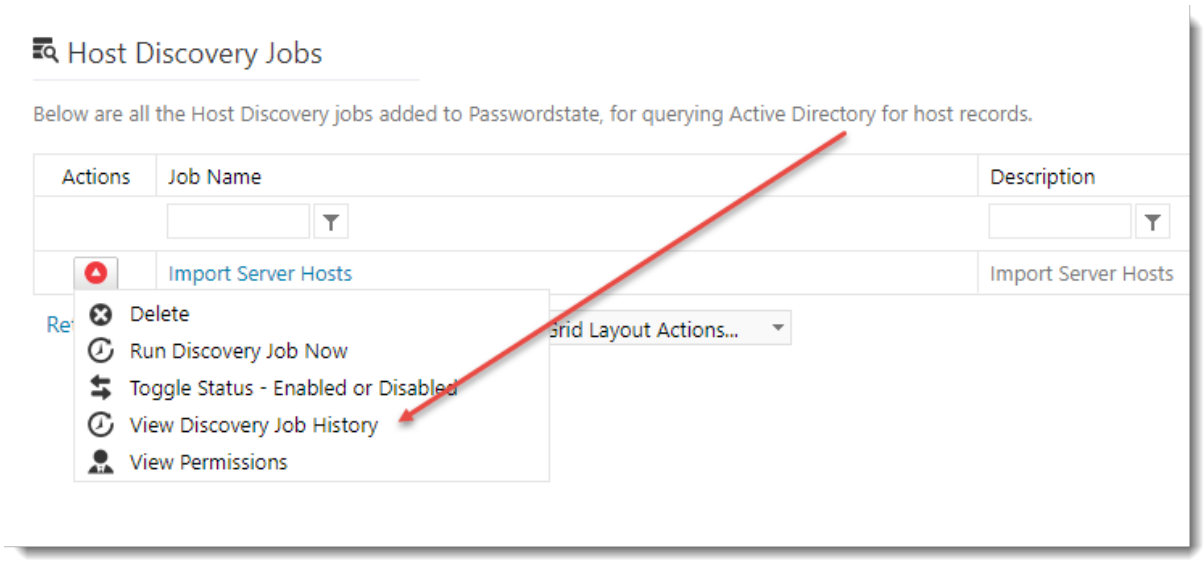
Note: When query Active Directory for Hosts, it is the value of the OperatingSystem AD Attribute which is queried. If you go to the screen Administration -> Passwordstate Administration -> Host Types & Operating Systems, you can see what attribute is currently set for each different operating system.



Discovery Job History

In addition to the emails you will received for results of Discovery Jobs, a History of all changes to the database are also recorded and can be viewed anytime - as per the screenshot below.

If your Discovery Job does not actually find any Hosts though, then it will not record any data i.e. You may have a Host filter set on the Discovery Job that does not find any Host records in Active Directory, or possibly you have specified an OU to query which does not have any computer objects in it.



3.2 Remote Session Management

For full instructions of how to install/configure and use either of the two Remote Session Launchers available in Passwordstate, please refer to the 'Remote Session Management' menu under the Help Menu in Passwordstate, or download the document Passwordstate_Remote_Session_Management_Manual.pdf

4 Administration

In order to see the Administration Tab you must be granted one or more of the different types of Security Administrators roles.

If you are a Security Administrator of Passwordstate, please reference the 'Security Administrators Manual', available from the Help menu.

5 Help Menu

The Help Menu provides various forms of Help to general users of Passwordstate, or Security Administrators. The Help available is:

1. Browser Extension Manual - for form-filling web site logins
2. Guided Tour of Passwordstate - this will show a popup window guiding you through some of the basic functions
3. Mobile App Manual - for using the Passwordstate native iOS and Android apps
4. Online Help - this links back to the Support page at Click Studio's web site
5. Password Reset Portal User Manual - shows a User based guide for the Self Service Password Reset Portal
6. Privileged Account Management - information about Account Discoveries, Password Resets and Password Validations
7. Remote Session Management - information for both the Client Based, or Browser Based, remote session management features

8. Remote Site Agent Manual - Showing instructions for how to deploy and use Agents for the Remote Site Location module
9. Security Administrators Manual
10. User Manual (this help file you are referencing now)
11. Web API Documentation
12. What's New - this shows the change-log for Passwordstate

Note: Some or all of these menus may be disabled or hidden from you, depending on options configured by your Passwordstate Security Administrator(s)