Passwordstate User Manual

Table of Contents

1 Introduction

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.

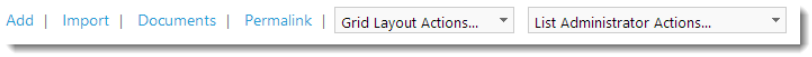
Getting Started - New Users

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. 

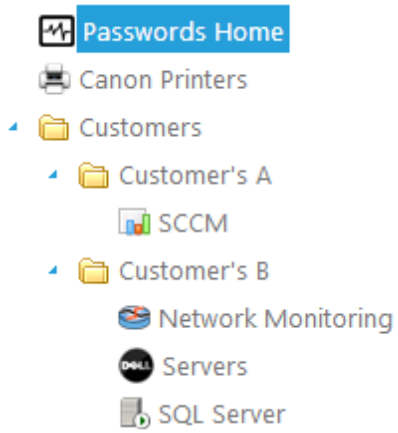
1.2 Quick Start Tutorials

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.

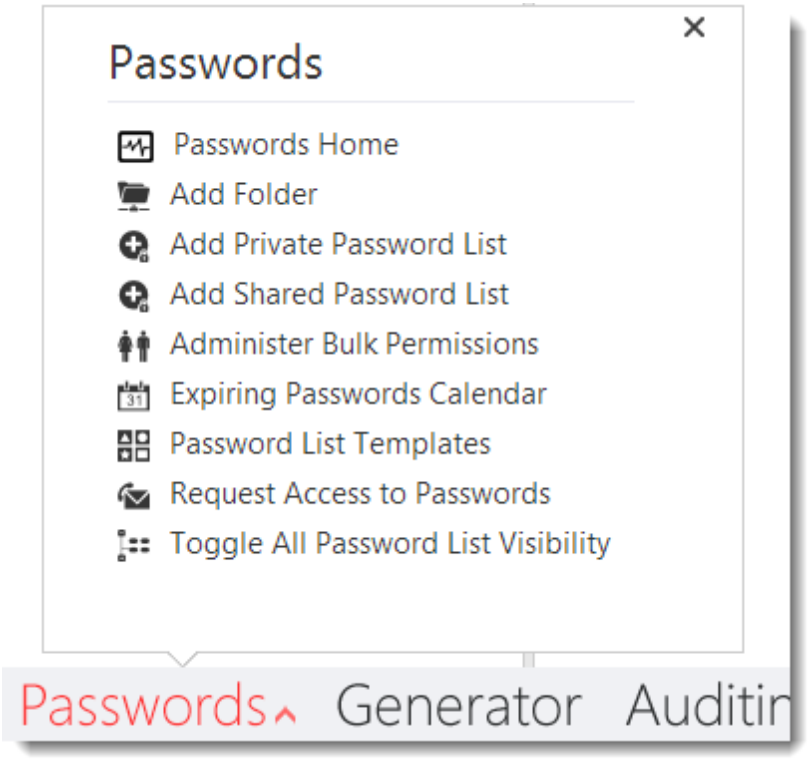
If you want a tree node to be displayed at the root of the navigation tree, simple drag and drop onto the highlighted 'Passwords Home' node you see in this picture.



Navigation Menu Actions

At the bottom of the screen, you will see a 'Passwords' Menu Item. From here you can select multiple sub menu items which allow you to create new Password Lists/Folders, request access to passwords, and manage your Password List Templates.

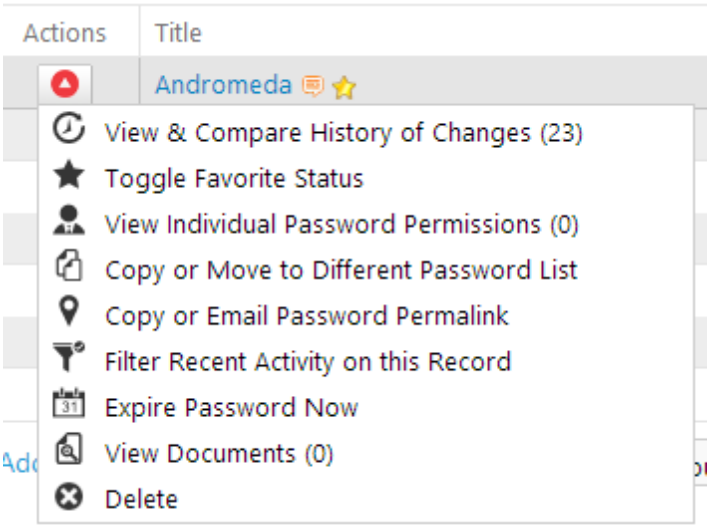
Note: Some of these actions may be disabled by your Security Administrators of Passwordstate.



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.

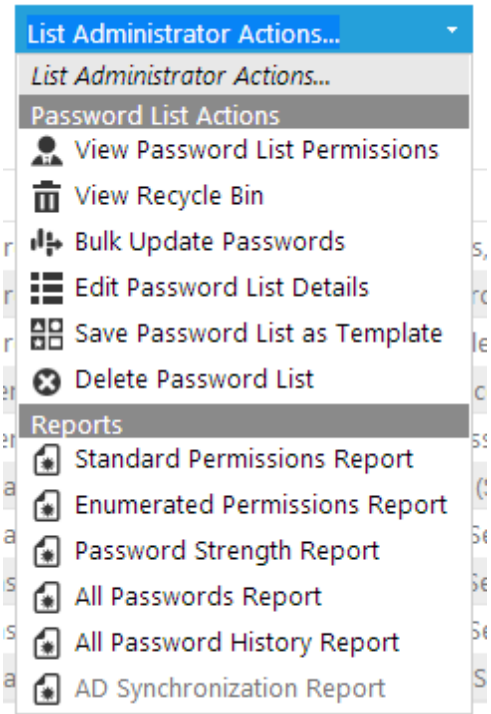
Note: Some of the actions may be disabled depending on some site wide settings, or on your own access rights.



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.



Quick Navigation for Password Lists

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.

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

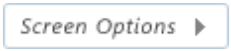
Searching for Passwords

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.

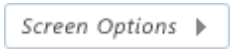
You can also quickly generate a new random Password, by clicking on the icon.

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 'Preferences' Menu Item at the bottom of the screen, you can specify multiple settings which are specific to your account. In particular:

1. Your default home page
2. Various email options
3. Various setting for passwords
4. Any additional authentication options

2 Passwords Menu

The "Passwords Menu" at the bottom of the screen 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 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
Request Access to Passwords	Allows you to request access to either a Password List, or a single password within a Password List
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 Passwords Home

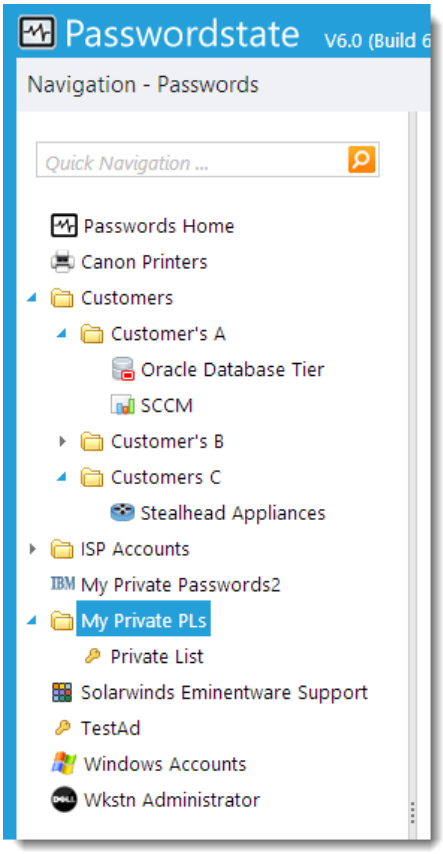
Clicking on Passwords Home will display whatever Password List, or Folder, you have selected as being your default Home Page in the Preferences area.

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 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 **Quick Navigation** 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 perform the following for all nested Password Lists beneath this folder:
  - Search for passwords in any of the nested Password Lists
  - Shows your 'tagged' favorite passwords for any of the nested Password Lists
  - Show audited graphs for all of the nested Password Lists
- 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

2.1.2 Passwords Home and Folders

Clicking on the **Passwords Home** icon, or on a **Password Folder** will display the screen below. This screen will either be a **filtered view** of all Password Lists you have access to (Passwords Home icon), or just the Password Lists nested below the Password Folder you selected.

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:

- Generate a single random password by clicking on the icon
- Search for Passwords
- View your tagged Favorite Passwords
- View statistics
- Customize the screen by clicking on the Screen Options button
- Manager various Folder settings by clicking on the Folder Options button - only available when you click on a Folder and have Admin rights to the Folder, not when you click in Passwords Home
- 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

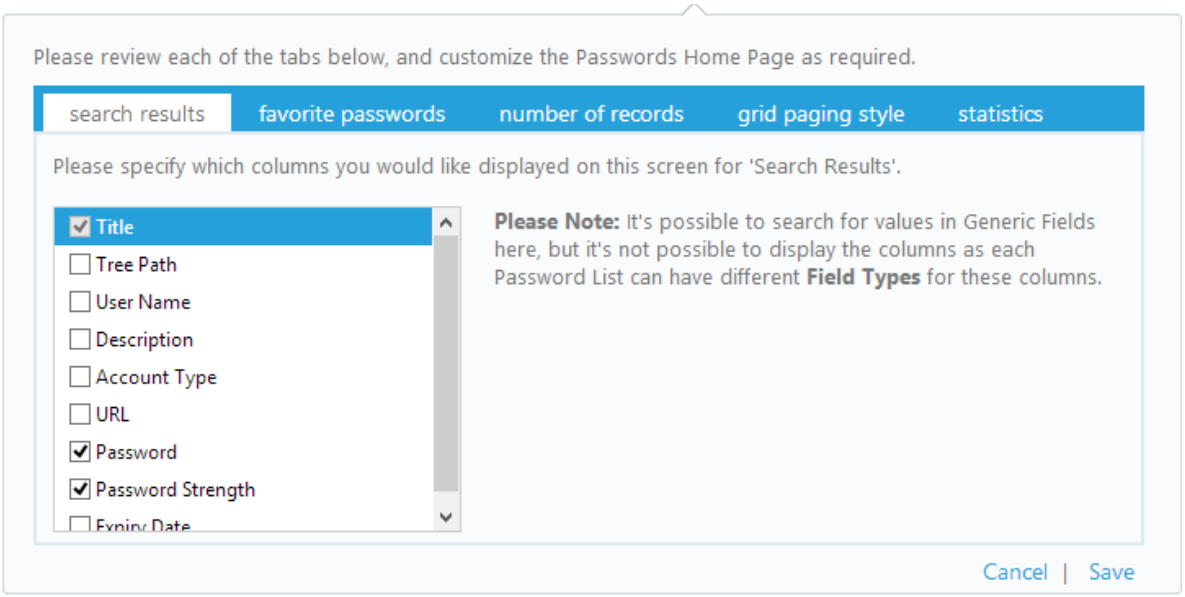
2.1.2.1 Screen Options

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.

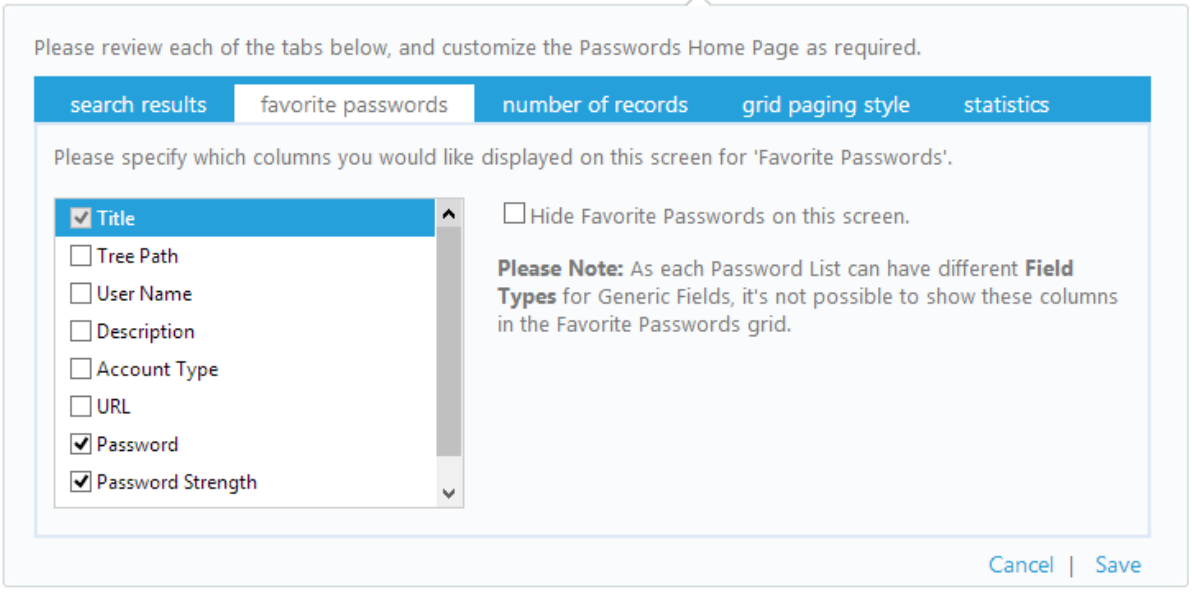
Search Results Tab

The Search Results tab allows you to select which columns are visible when searching for Passwords. For small screen resolutions, it is recommended you only select a minimum number of columns to display is possible.



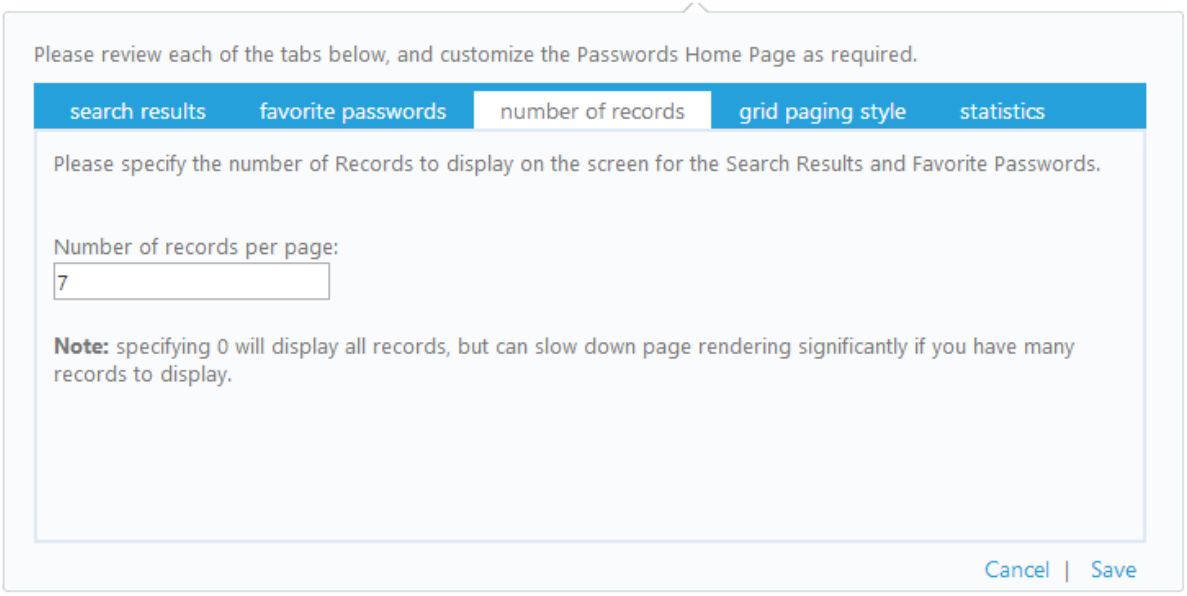
Favorite Passwords Tab

The Favorite Passwords tab allows you to select which columns you want displayed for the Passwords you have tagged as your favorites. You can also choose to hide the Favorites Passwords grid here, which provides more screen real-estate for the search results if required.



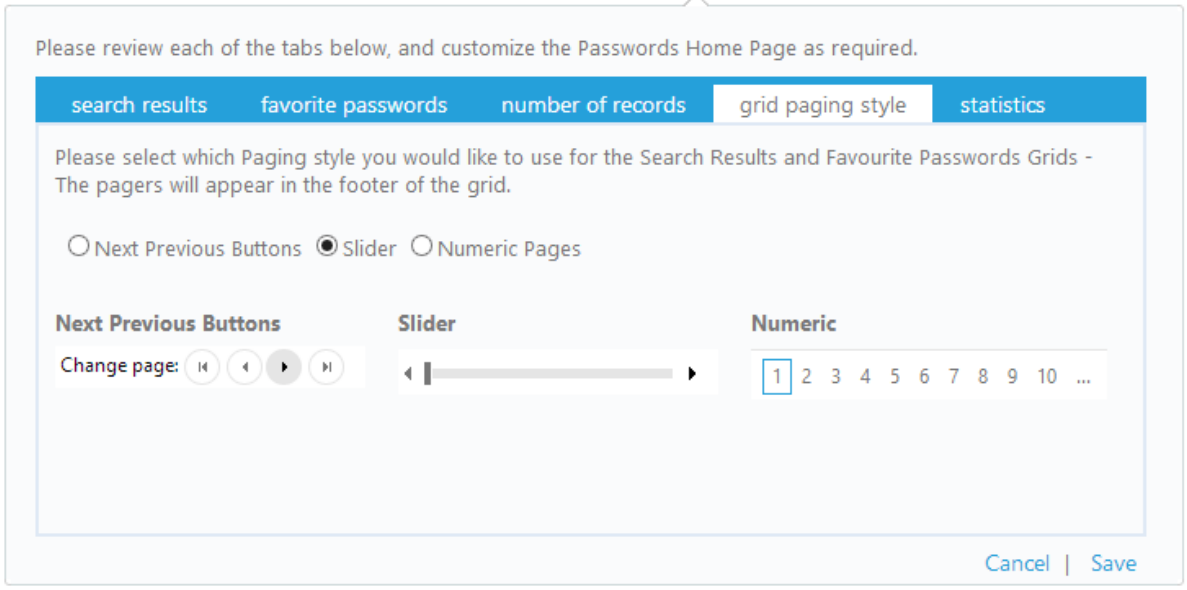
Number of Records Tab

The Number of Records tab simply allows you to specify how many records you would like displayed on the Search Results and Favorite Passwords grids, before the 'paging' controls will be displayed.



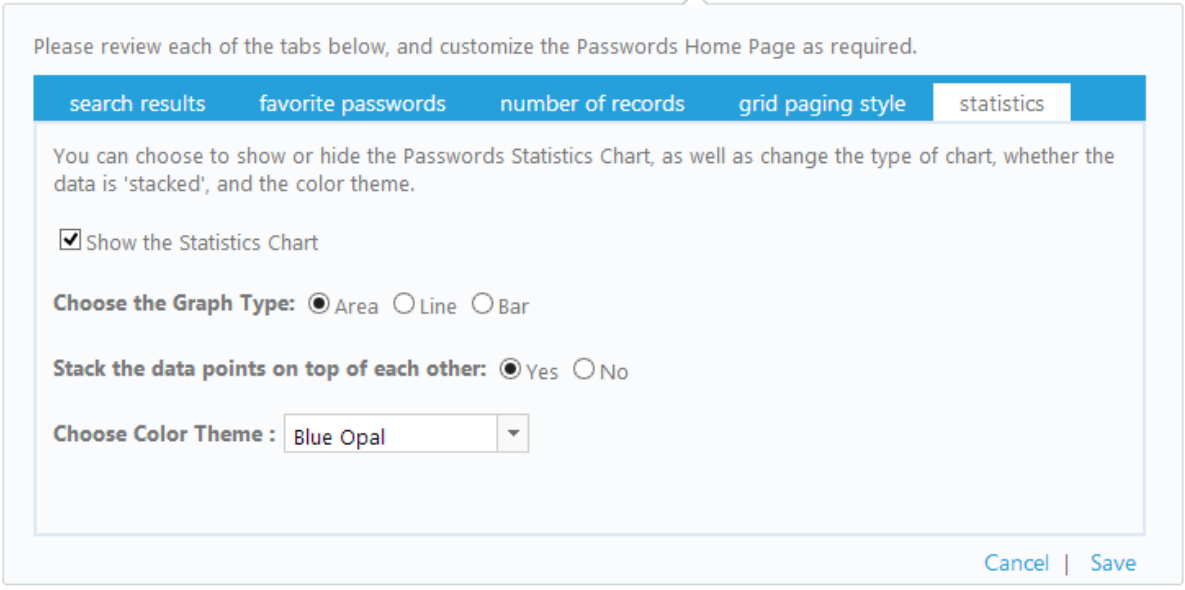
Grid Paging Style Tab

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.



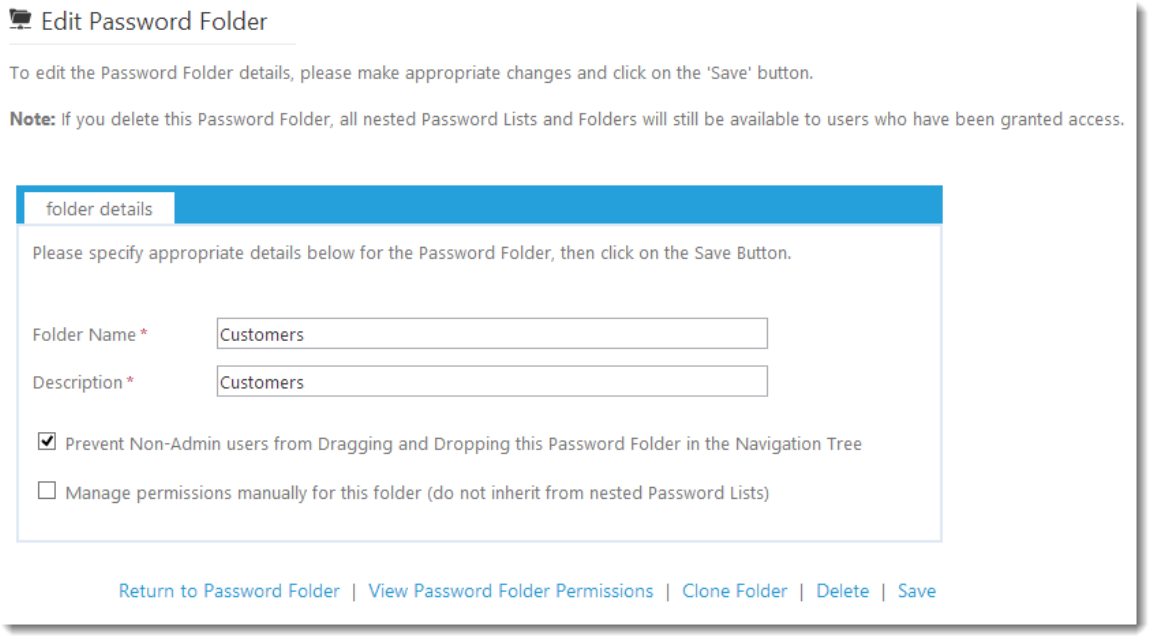
Statistics Tab

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.



2.1.2.2 Folder Options

Folder Options allows you to edit various settings related to the selected Password Folder, as well as various features for permissions and cloning the folder.



Folder Details Tab

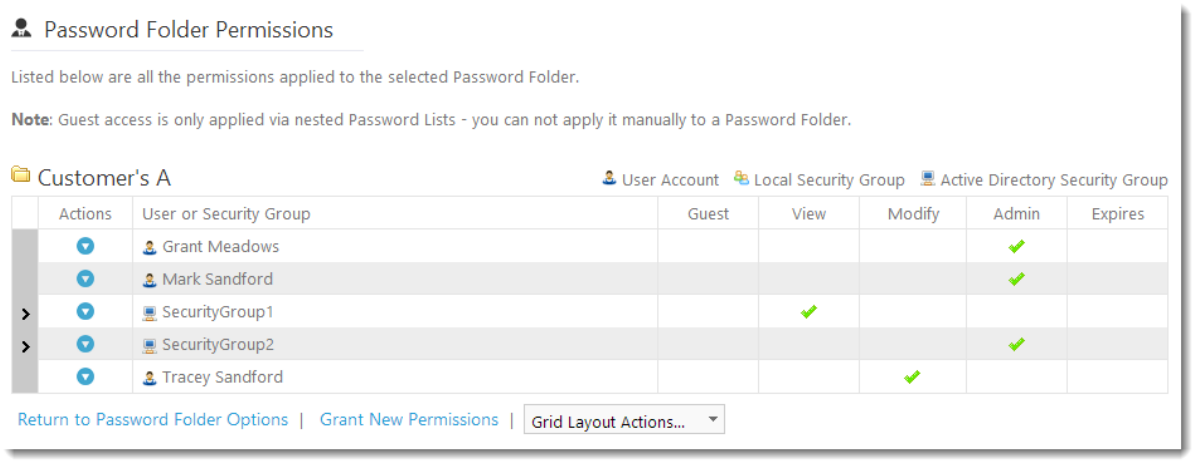
On the Folder Details tab you can:

- 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
- Manage permissions for the folder manually - by default, permissions are generally applied to the Password Lists themselves, as this is where all the sensitive data lives. If a Password List is nested beneath a Folder, as the permissions are applied/changed to the Password List, the changes are propagated upwards to any Folders above it (propagation upwards only occurs on Folders, not other Password Lists). If you choose to manage permissions on Folders manually, then the propagation just spoken of will not occur - this may cause more work applying permissions.

View Password Folder Permissions

By clicking on the 'View Password Folder Permissions' button, you will be able to see what permissions are applied to the folder. If you have chosen to manage permission manually for the Folder, various actions will also be available from the 'Actions' drop-down menu next to each of the records.

Note: The Expires column is only used if managing permissions manually for a Folder. If permissions are set to inherit from Password Lists nested beneath the folder, the Expires value will not be propagated.



Clone Folder

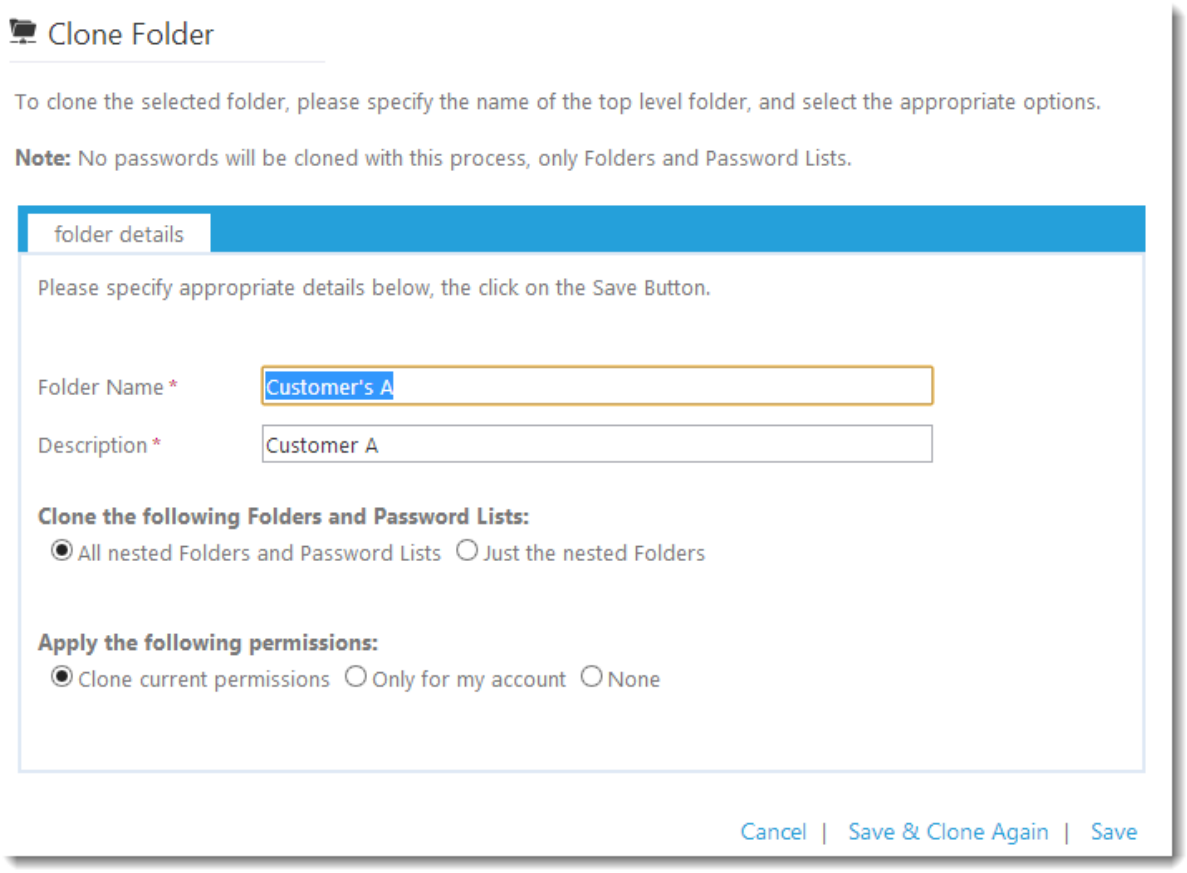
By clicking on the 'Clone Folder' button, there are various options available for you to clone the selected folder. The Options are:

- 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.



2.1.3 Password Lists

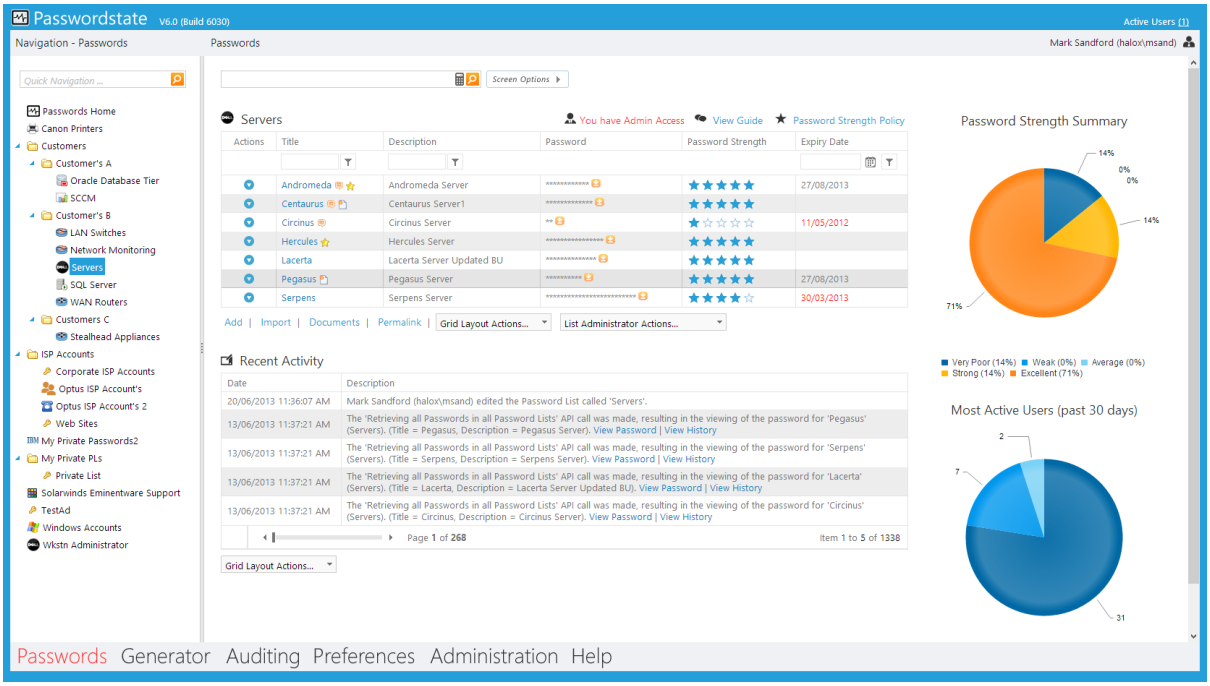
The Password List screen shows you the Passwords stored within the selected Password List. Not all Passwords may be visible to you here, as permissions can be applied to individual records within the Password Lists, as opposed to the whole Password List.

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:

- Generate a single random password by clicking on the icon
- Search for Passwords contained within the selected Password List

- 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 or Import 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



2.1.3.1 Screen Options

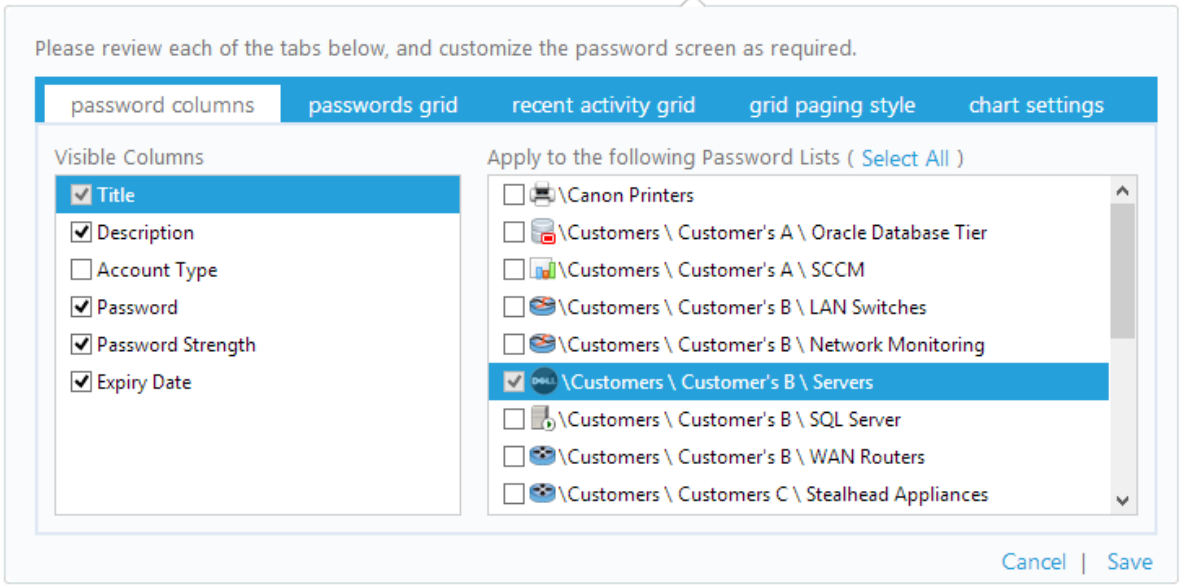
Screen Options allows you to specify various settings for how you would like to see the grids and charts displayed on the screen.

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

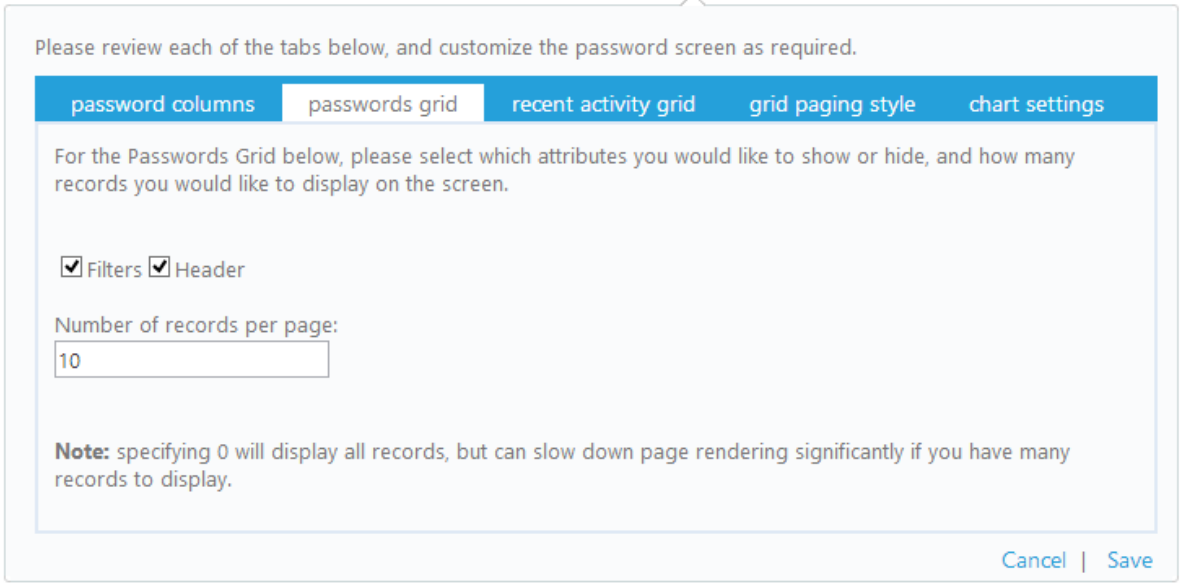
The Password Columns tab allows you to choose which columns are visible in the Passwords grid.

Once you've chosen the columns you want visible, you can also apply the same 'view' to other Password Lists, by selecting them in the 'Apply to the following Password Lists', then clicking 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.



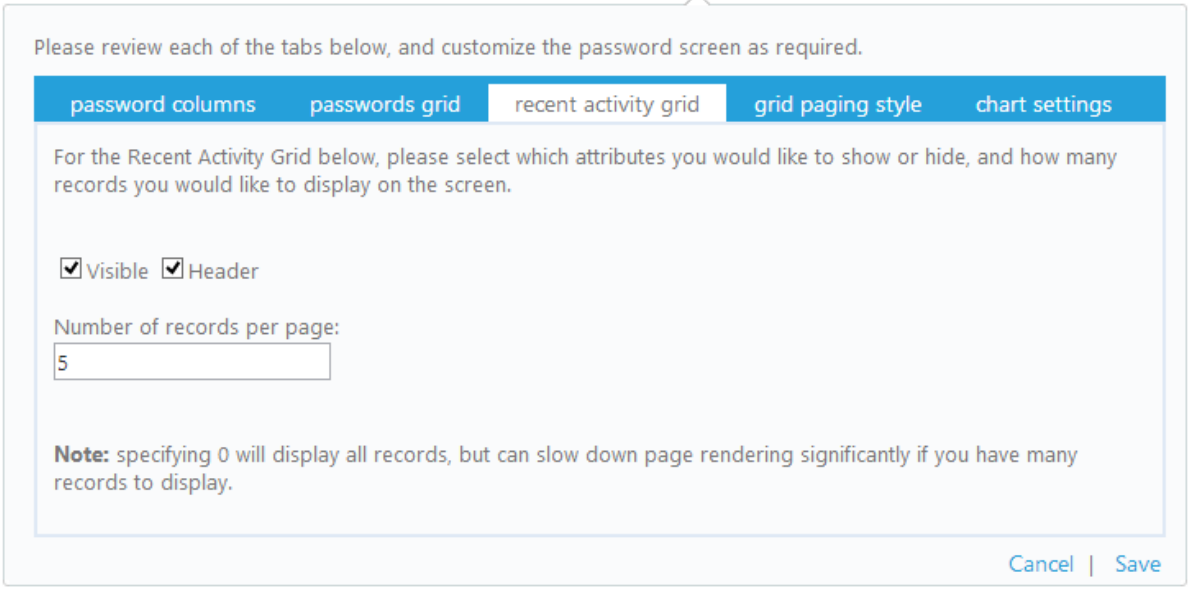
Passwords Grid Tab

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.

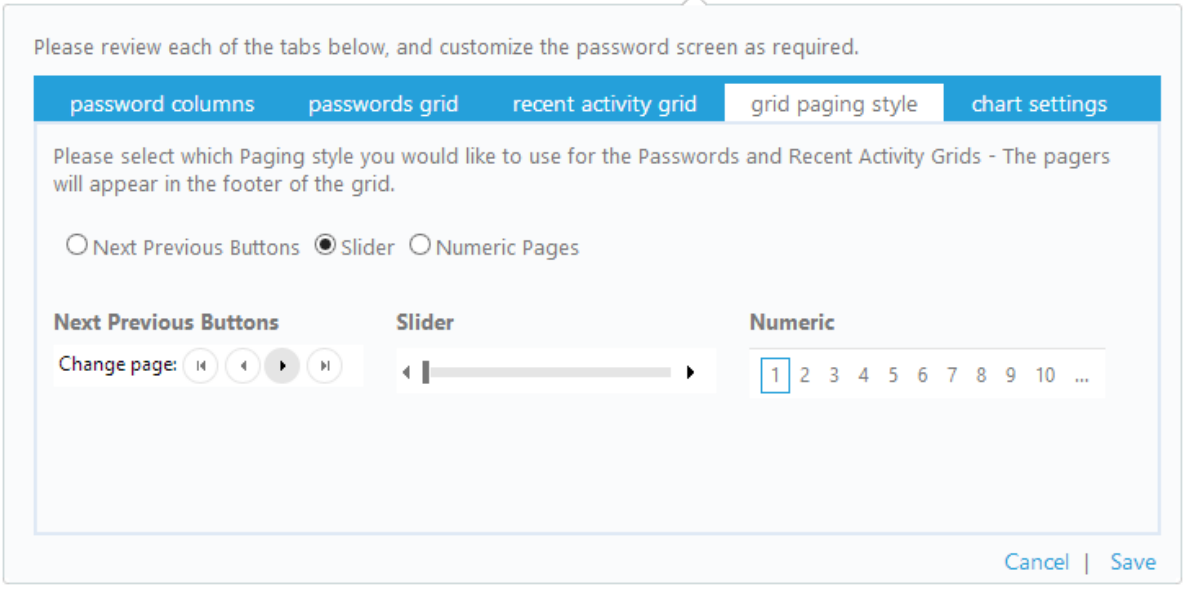
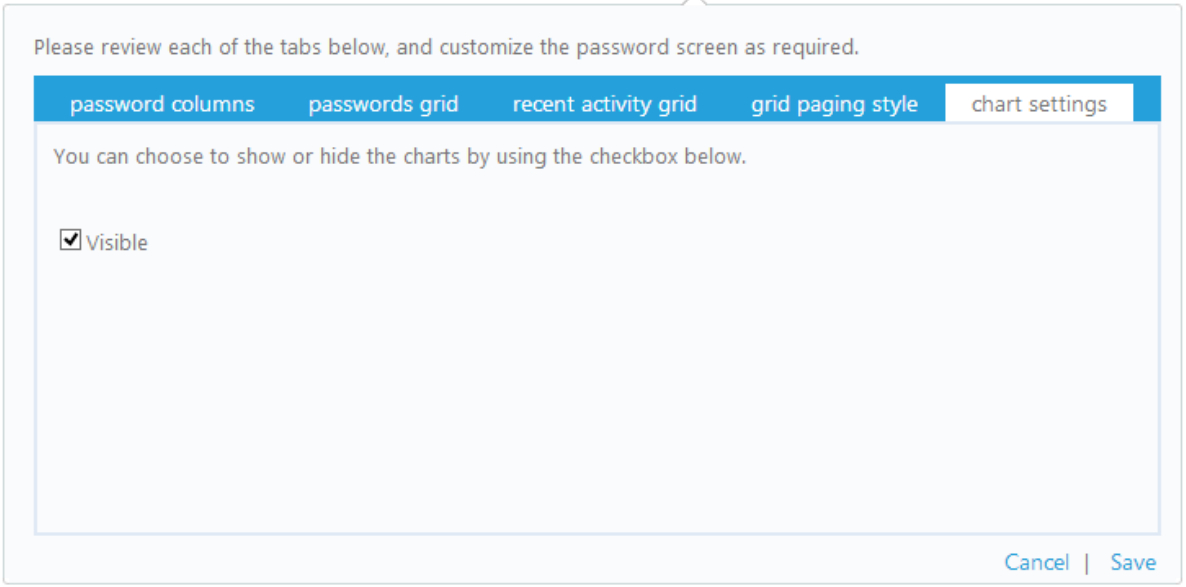


Chart Settings Tab

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.



2.1.3.2 Add Password

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

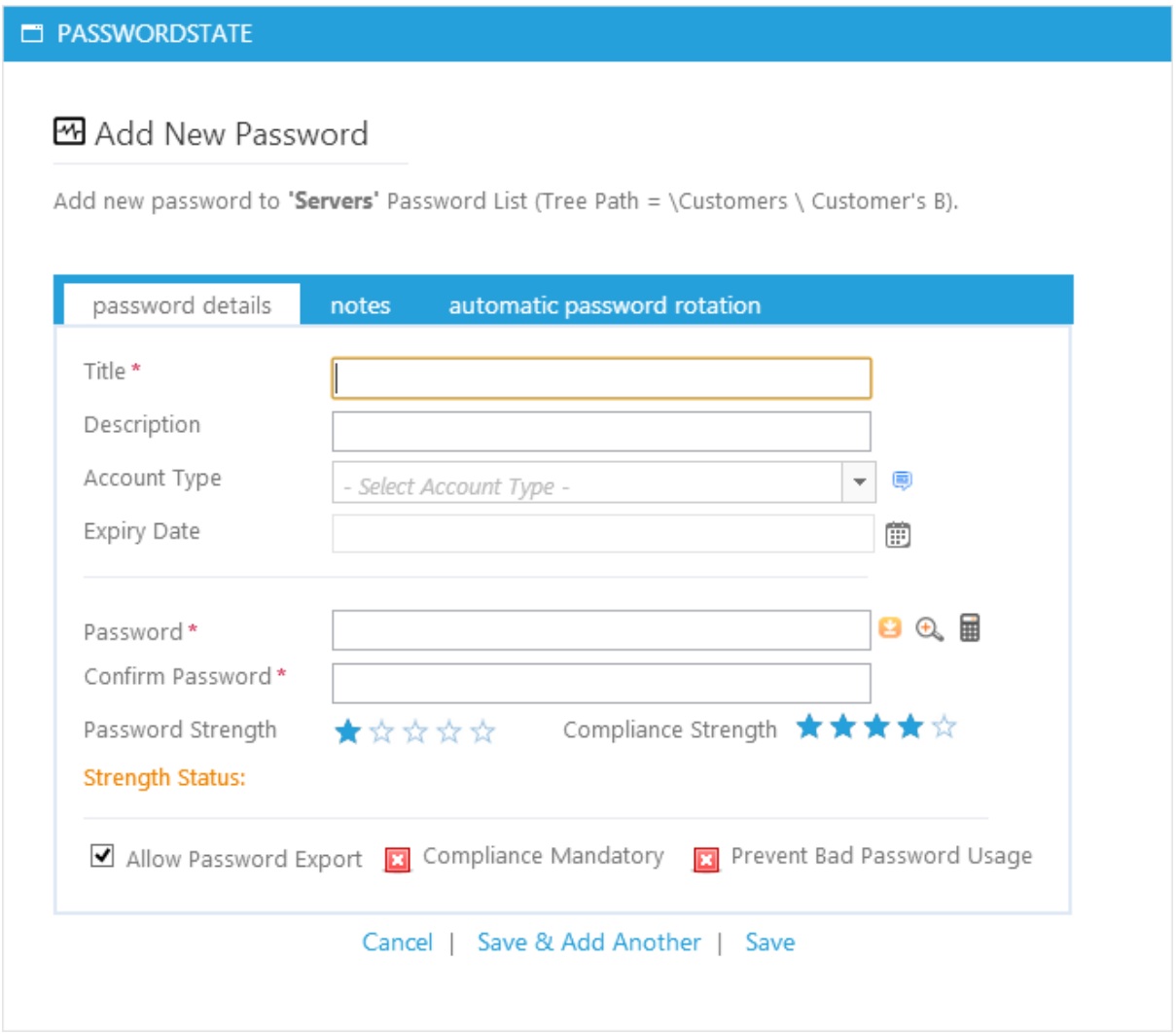
When adding a new password record, the fields visible on the screen can be different for each Password List, as each Password List can be configured to use different fields. There are a total of 9 fixed fields which can be used, and 10 Generic Fields which can take on different field types.

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.

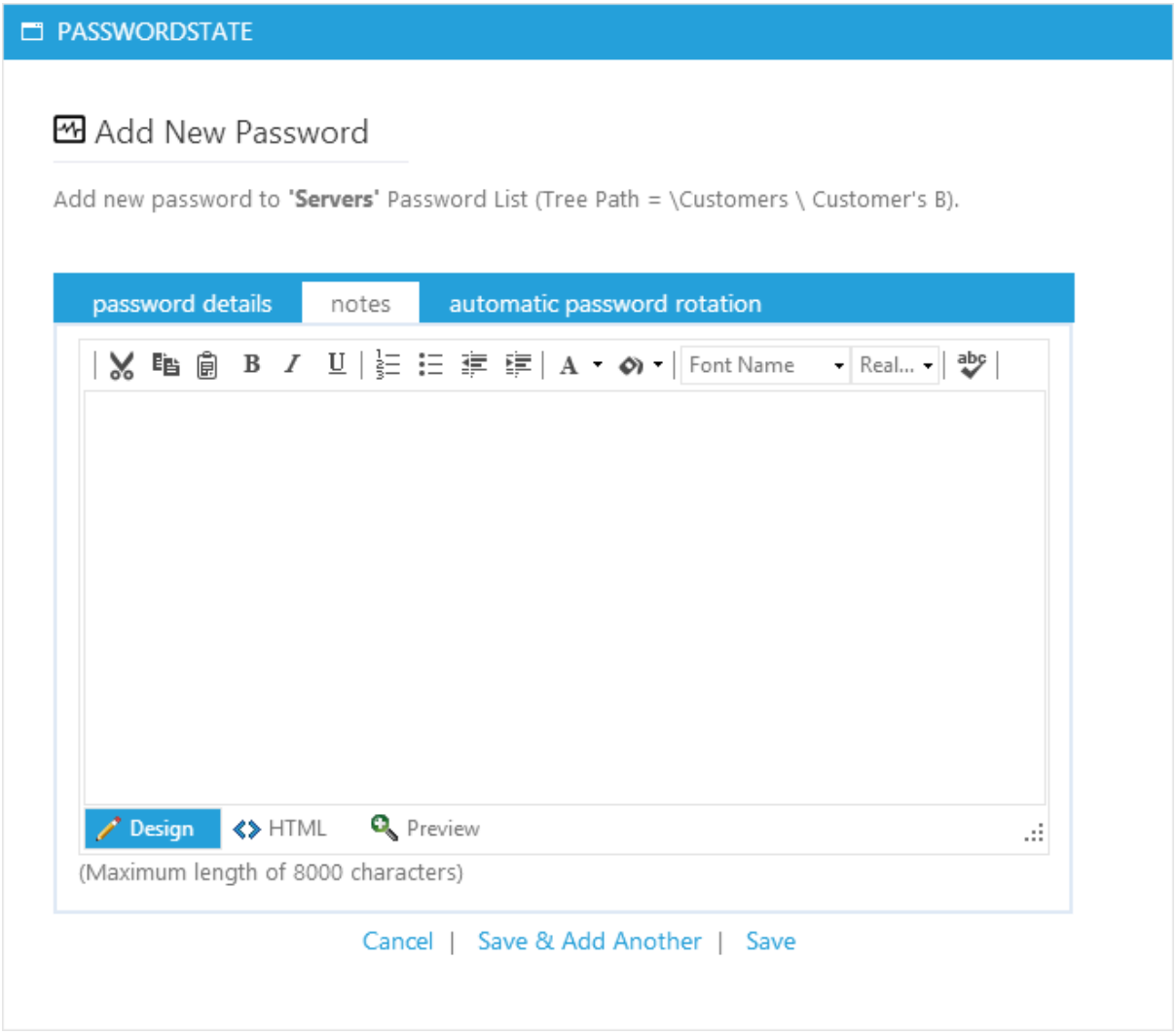
A few things to note on this tab is:

- 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



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.

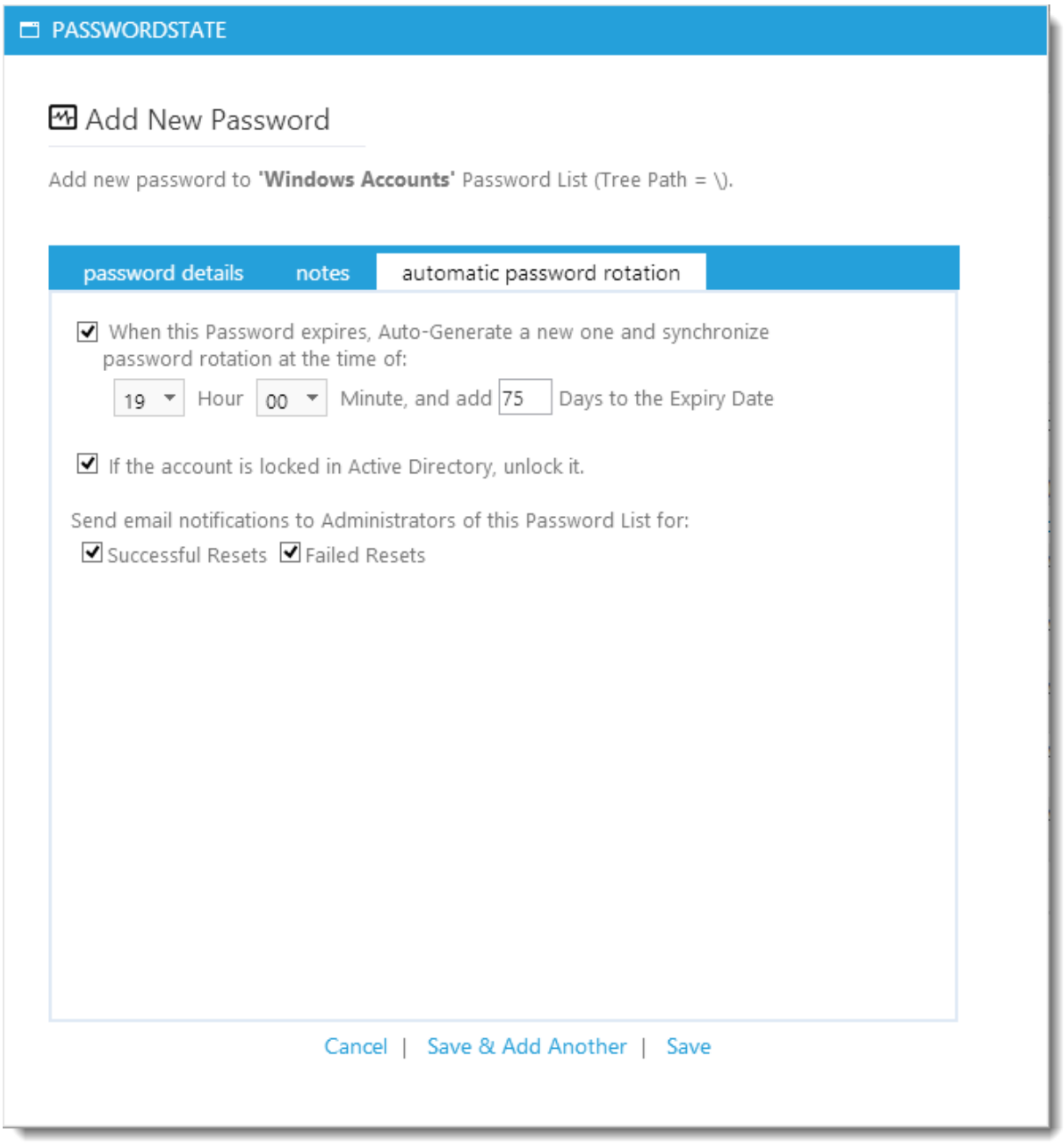


Automatic Password Rotation Tab

The Automatic Password Rotation tab **will only be visible** if the password record is configured to synchronize with Active Directory, or with a local account on a Windows Server. Options available are:

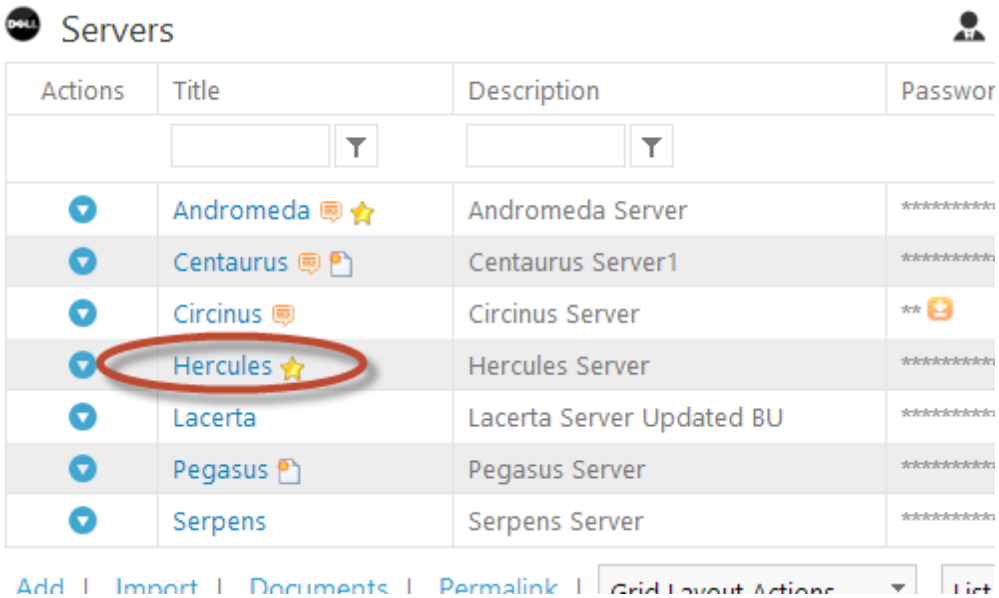
- Whether or not to auto-generate a new password for the record
- At what time of the day should the password be reset, once the Expiry Date has been reached
- How many days should be added to the Expiry Date field, once the password has been automatically reset
- Whether or not emails should be sent to Administrators of the Password List when the reset has succeeded, or failed

The Administrators of the Password List can also set the default options for 'Automatic Password Rotation', and the defaults can be set at the Password List level.



2.1.3.3 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.

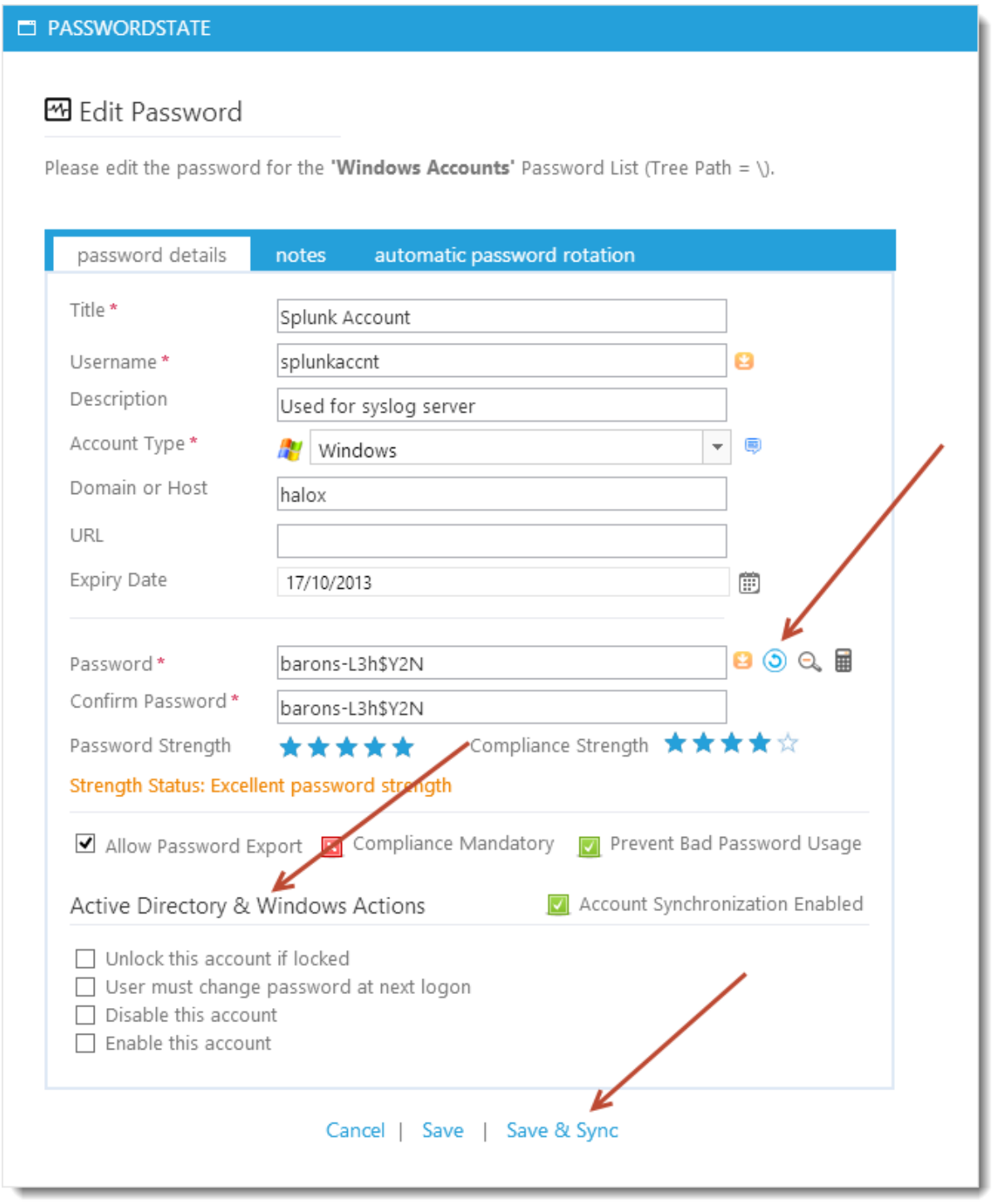
If the Password List is configured to synchronize changes will Active Directory, or local Window Servers, there will be a few additional options available:

Active Directory or Windows Server Account Synchronization Options

On the 'Password Details' tab, the following options may be available:

- The icon allows you to confirm if the password stored in Passwordstate also matches what is stored in Active Directory, or the local Windows Server
- Various 'Active Directory Actions' options may be available if your Administrator of the Password List has enabled them
- The 'Save & Sync' button will also be available, and this allows you to save the new password record in Passwordstate, and also synchronize it with Active Directory, or a local Windows Server

Note: Your Security Administrators must first configure Passwordstate to allow synchronization to occur, and instructions can be found in the Security Administrator manual

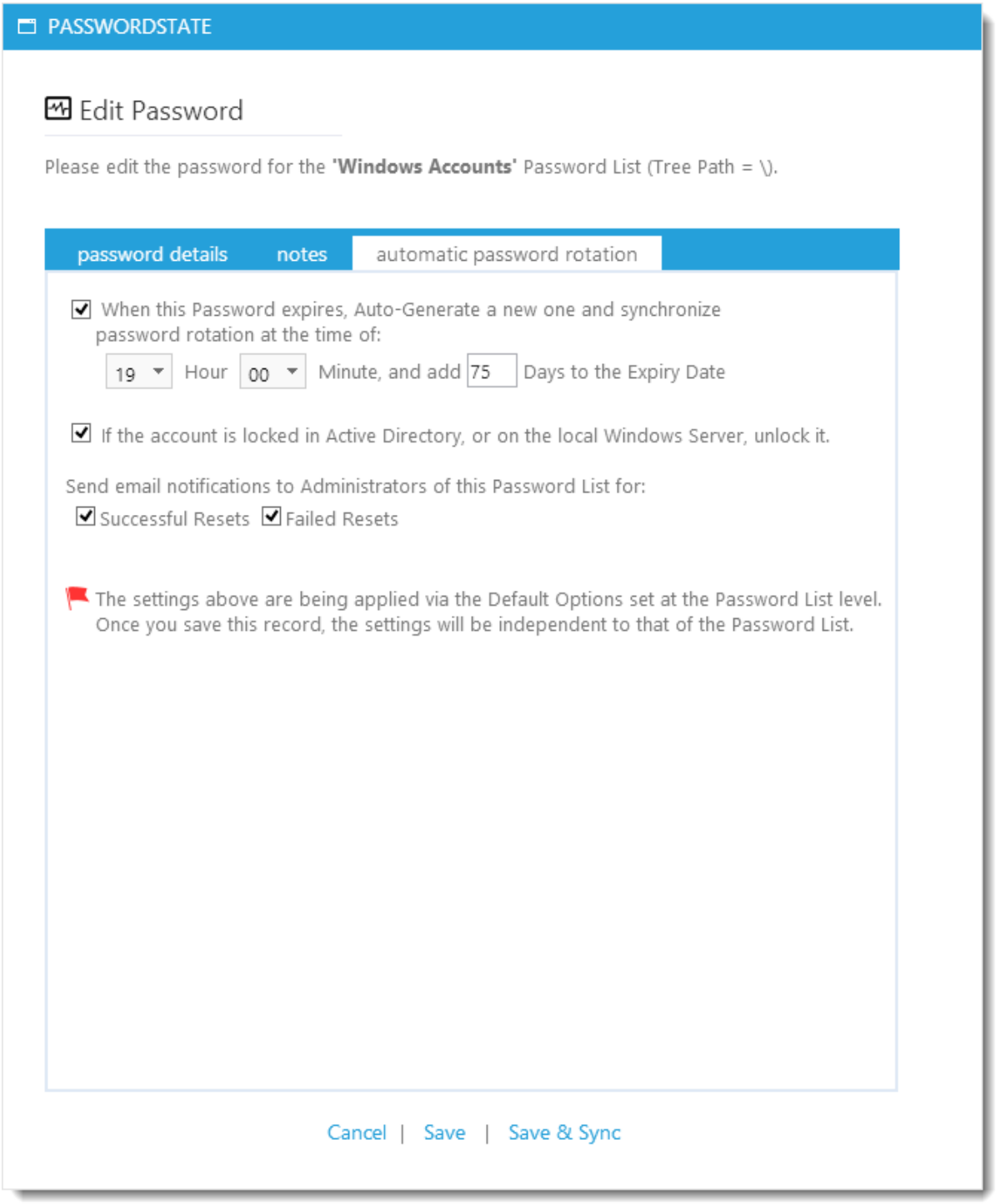


Automatic Password Rotation Tab

On the 'Automatic Password Rotation' tab, you will also have the following options available to automatically reset the password once it expires:

- Resets the password in Passwordstate

- To also synchronize the new password with Active Directory, or the local account on a Windows Server
- If the account is locked in AD or on the local Windows Server, then you can choose to also unlock it



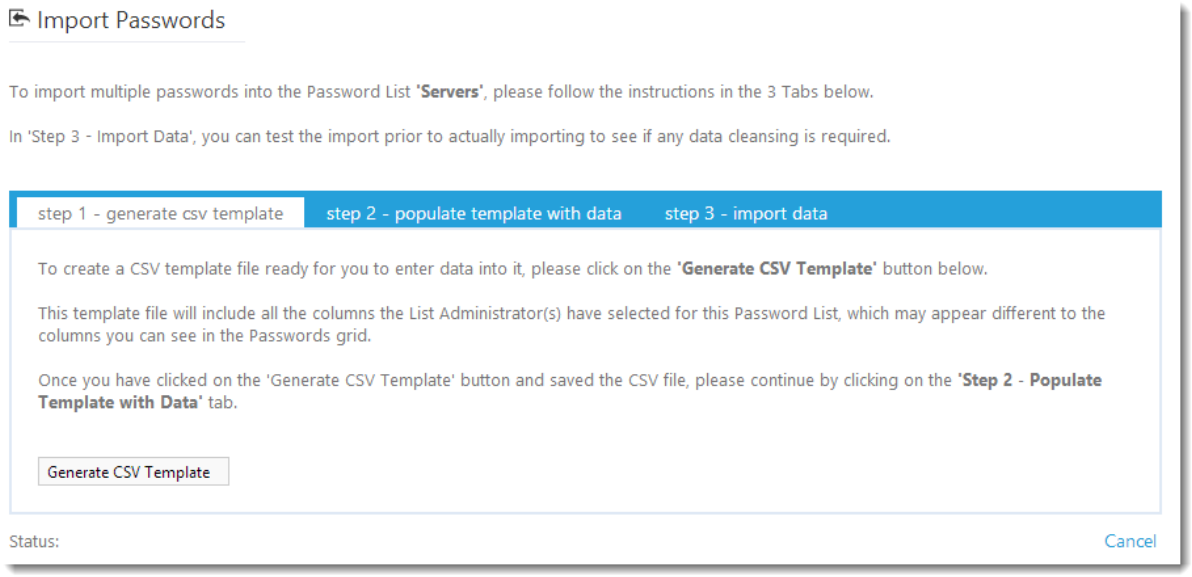
2.1.3.4 Import Passwords

It is possible to import one or more passwords into a Password List via the use of a csv file (comma-separated values). When you click on the Import button, you will be presented with a page which has 3 tabs to guide you through the import process.

Note: Prior to performing the actual import, it is recommended you 'test' the import process first, to ensure all data validation rules are met. You can perform the test in the final tab called 'Step 3 - Import Data'.

Step 1 - Generate CSV Template

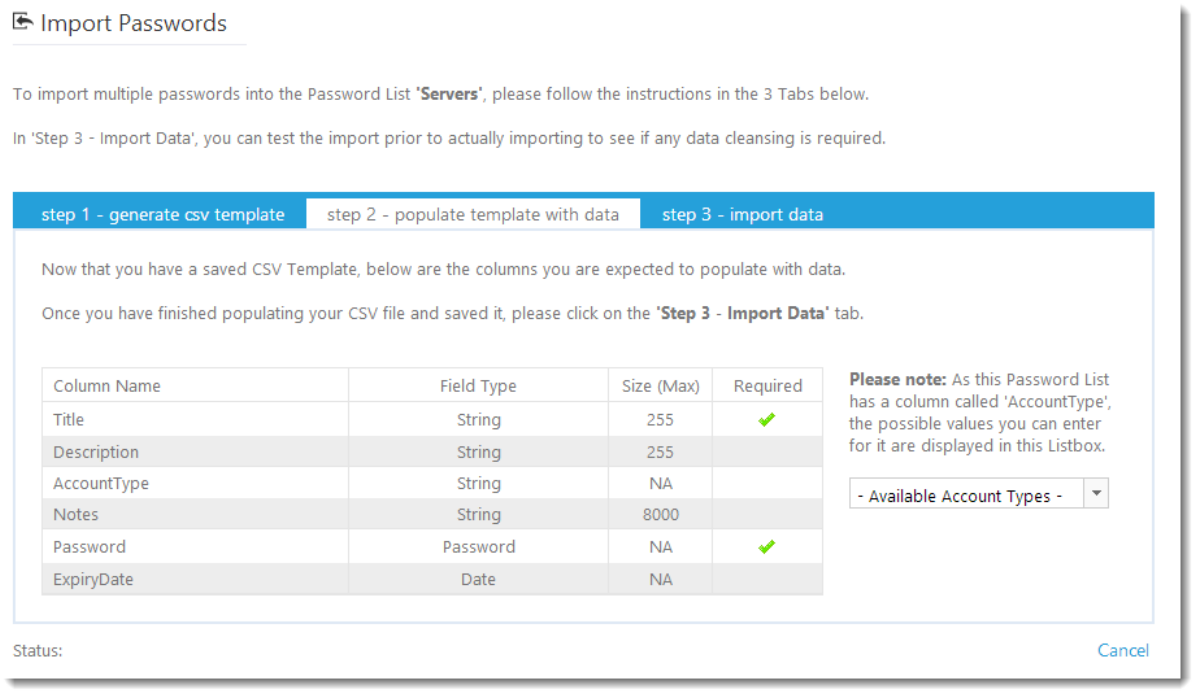
As every Password Lists can have different fields associated with it, it is recommended you use the 'Generate CSV Template' button to generate an empty csv file with the correct headers. Once you have generated your csv file template, you can move onto the tab 'Step 2 - Populate Template with Data'.



Step 2 - Populate Template with Data

The second tab shows you what fields are expected for the Password List, if there are any restrictions on the size of the fields, and which ones are mandatory and must have values. Once you understand the requirements and formatting of the data, you can populate your csv file ready for the test import. Once you have populated your csv file with data, you can move onto the tab 'Step 3 - Import Data'.

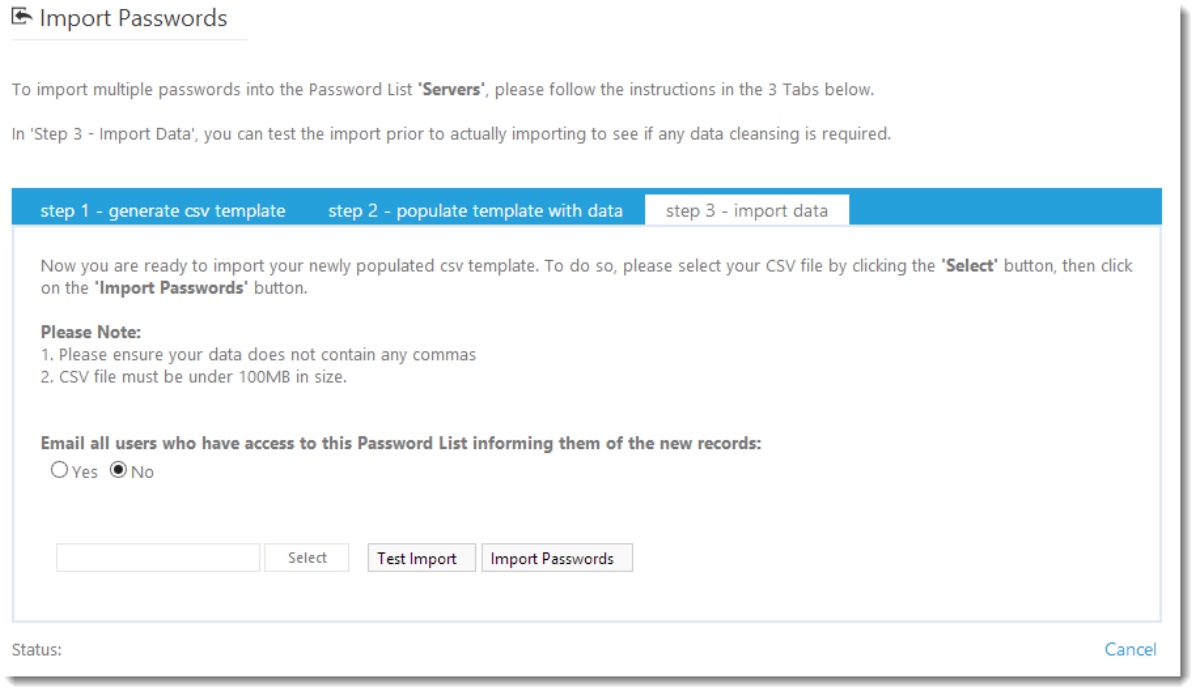
Note: When populating the csv file with data, please ensure the order of the columns is not altered from the generated template, otherwise the import process may fail, or data may be imported into incorrect fields.



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: 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.



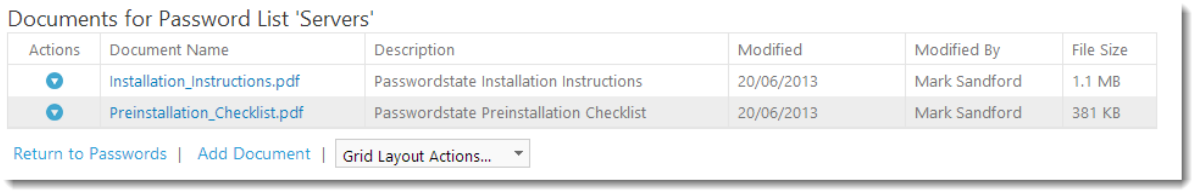
2.1.3.5 Upload Documents

It is possible to upload one or more document/attachments to Passwordstate, and associated them with either the Password List itself, or individual Password records.

When uploading documents, they are stored within the database in binary form, and any file/ document types can be uploaded.

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.

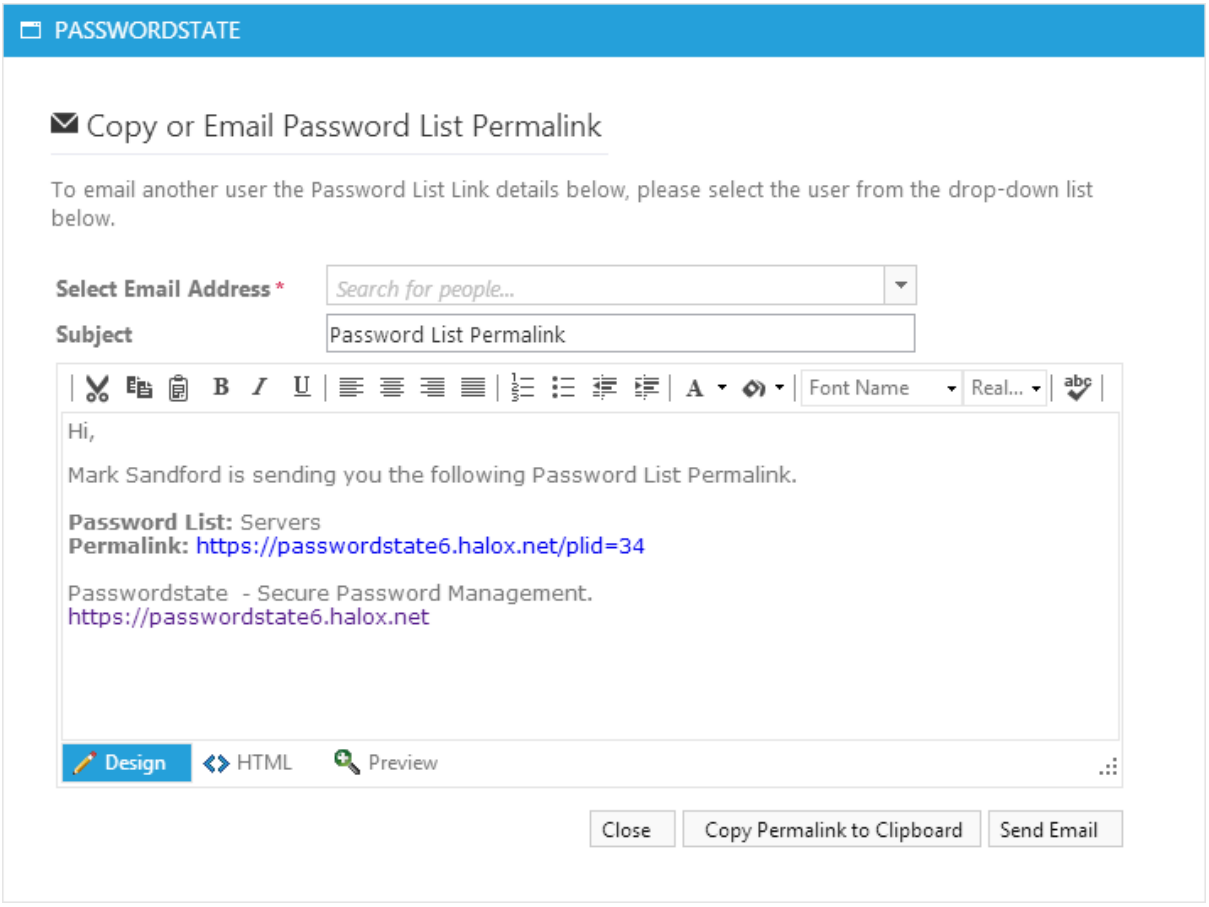


2.1.3.6 Email Permalinks

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.



2.1.3.7 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.

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.
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 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
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
Copy or Email Password Permalink	Similar to Permalinks for Password Lists, you can also copy or email Permalinks for individual Password records
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
Expire Password Now	Selecting 'Expire Password Now' for an individual Password record, will set it's Expiry Date field to the current date
View Documents	You can upload one or more documents/attachments and associate them with individual Password records
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

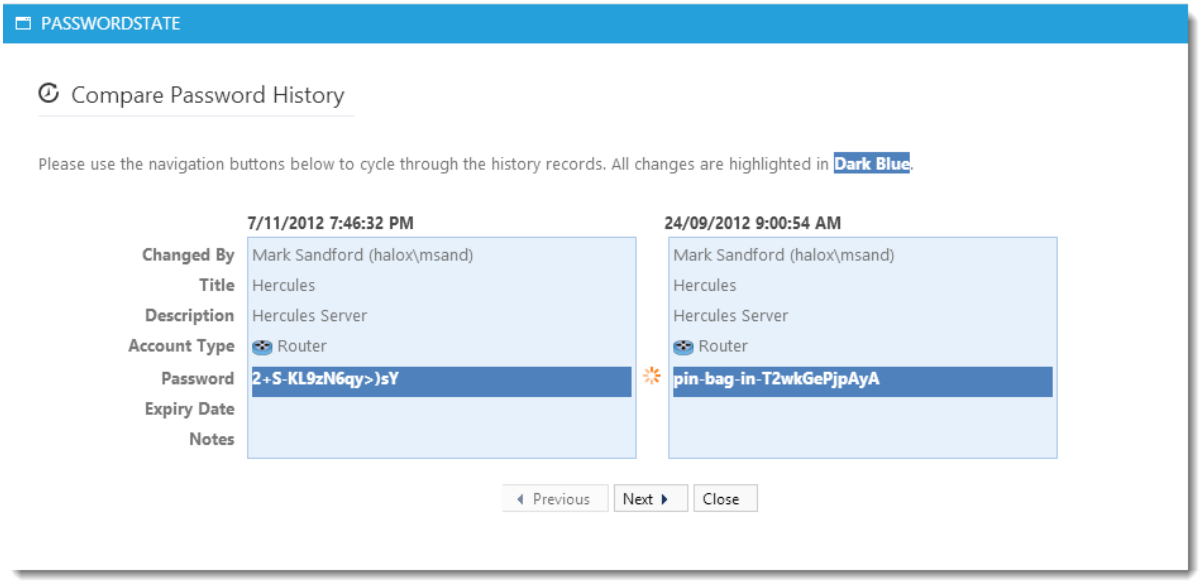
2.1.3.7.1 View & Compare History of Changes

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.



2.1.3.7.2 View Individual Password Permissions

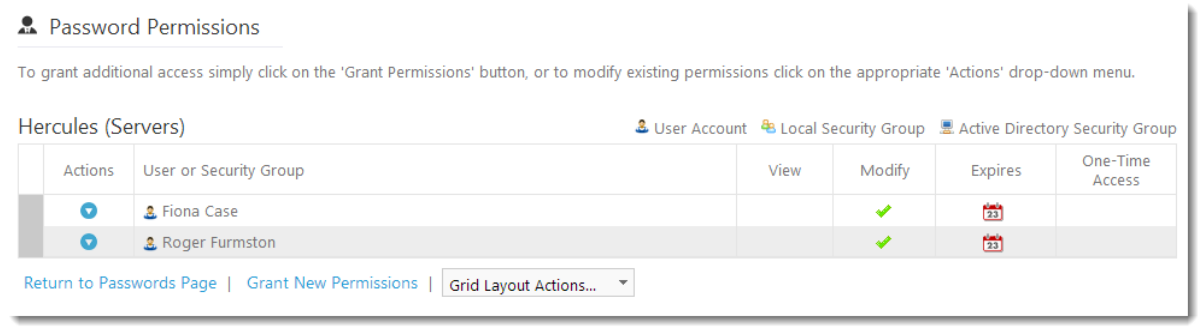
In addition to applying permissions to an entire Password List for users, you can choose to apply permissions just to individual Password records if required. When the user browsers to the Password List, they won't see all the records, just the individual ones they've been given access to

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



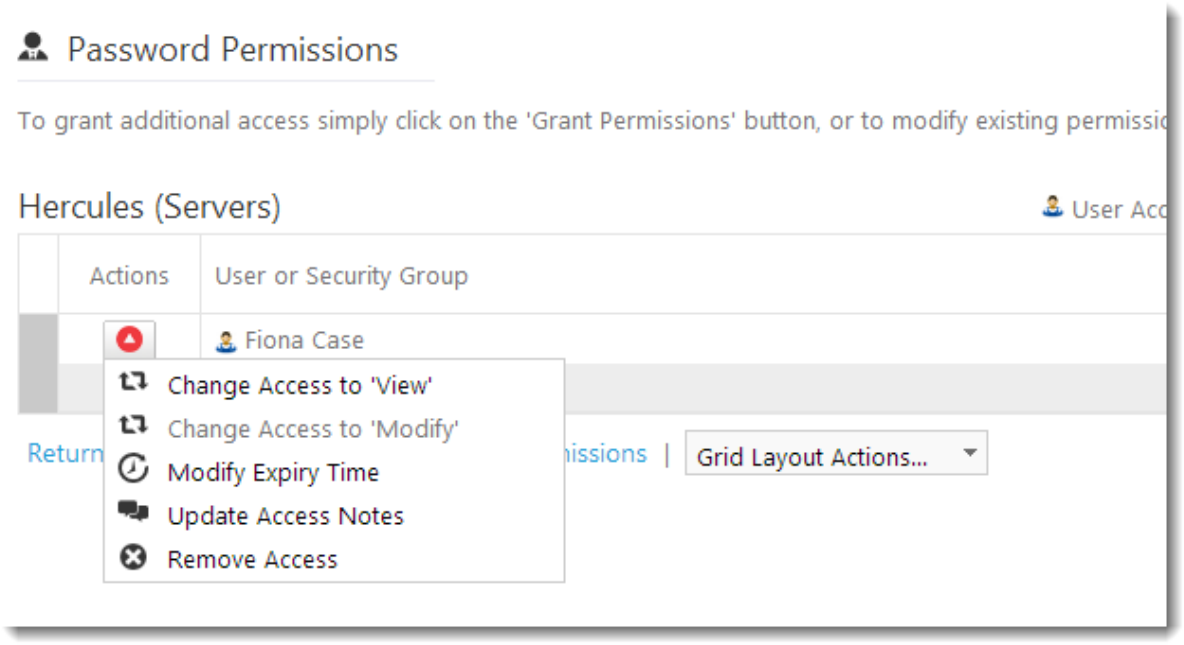
From the 'View Individual Password Permissions' screen, you have the following features

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.

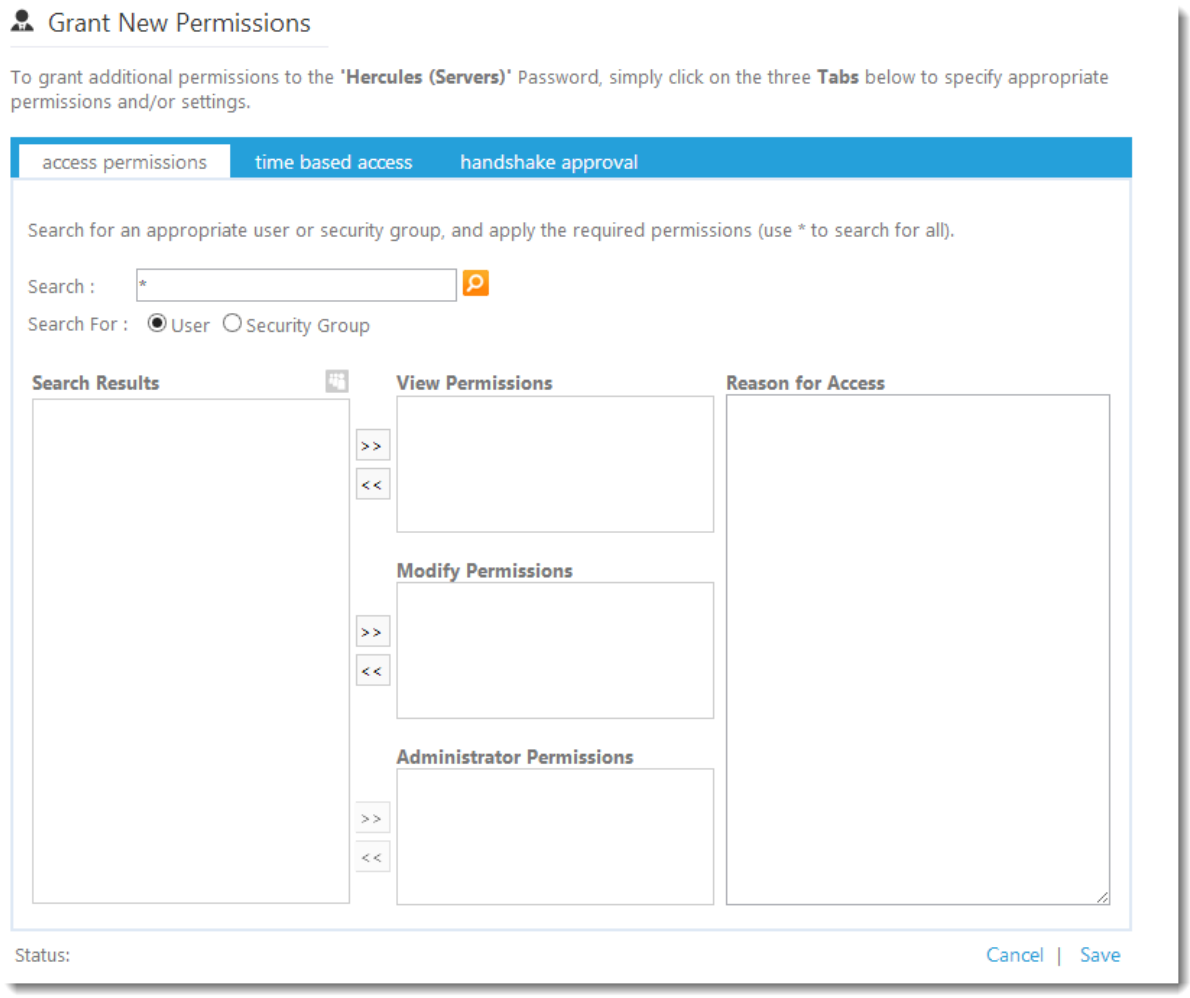
2.1.3.7.2.1 Grant New Permissions

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

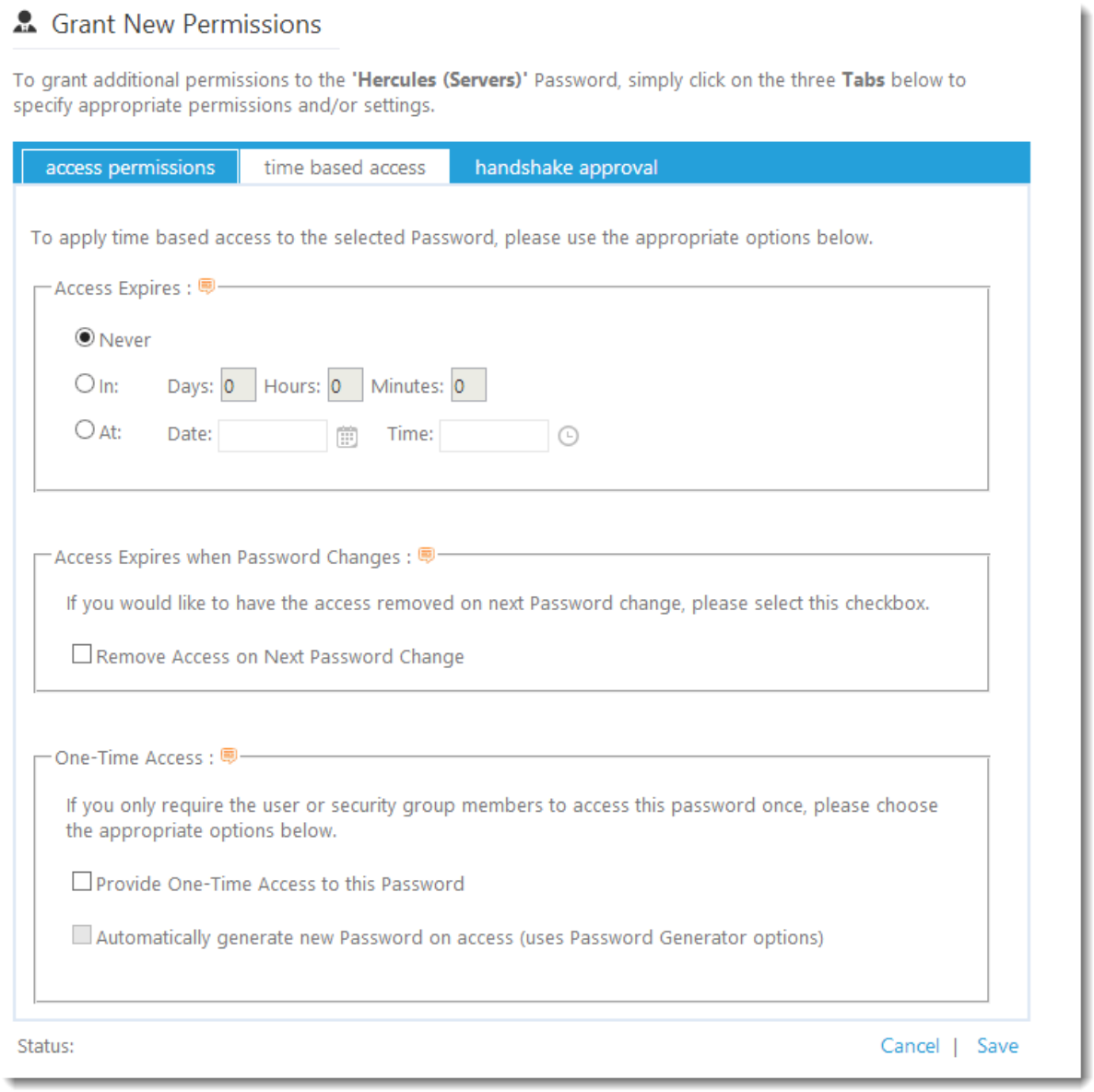


Time Based Access

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.

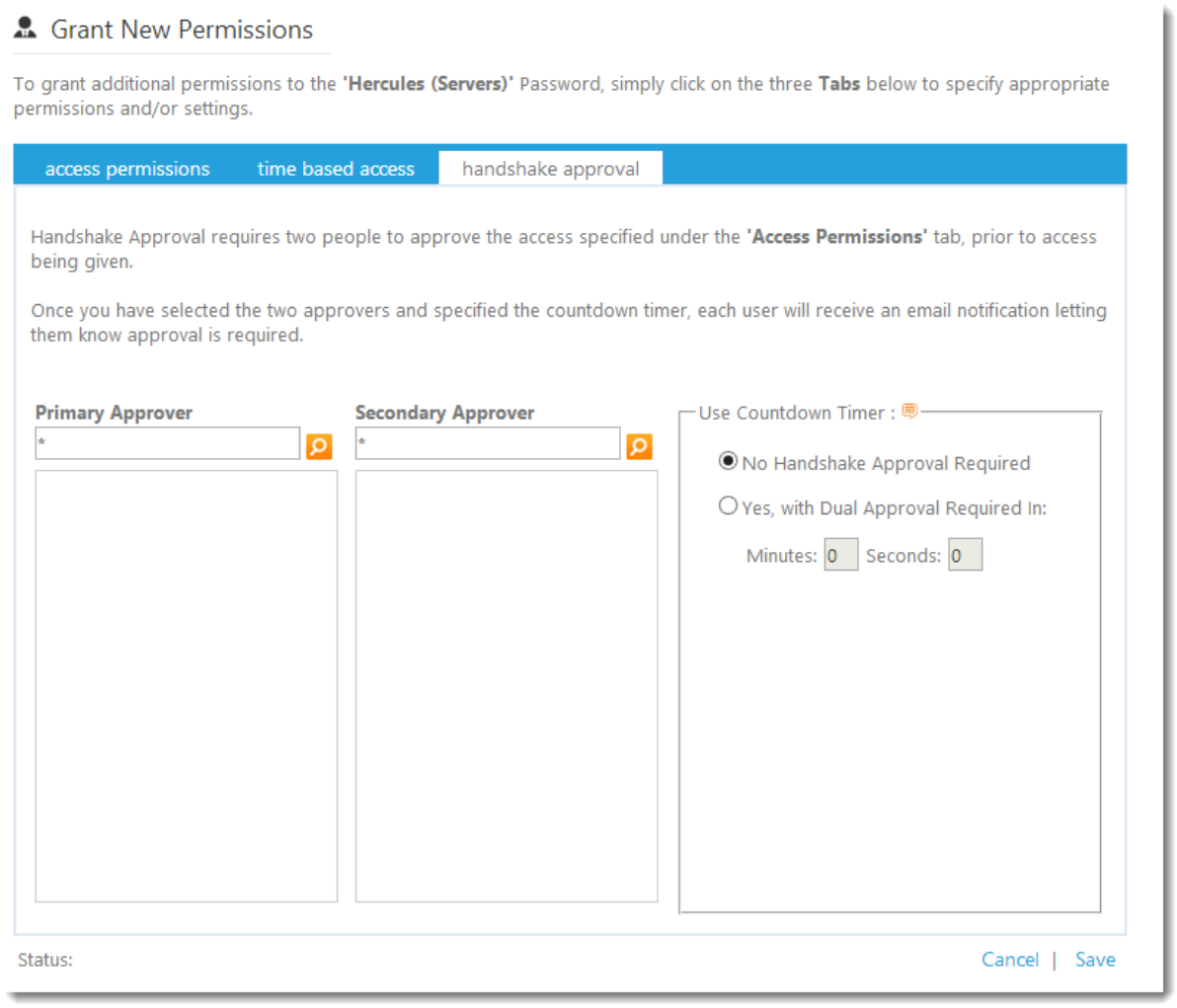


Handshake Approval

'Handshake Approval' can be used for Passwords which are of a various sensitive nature, and requires more than one Password List Administrator to approve access, prior to it being given to the user.

To specify Handshake Approval is require for this Password record, you need to select a Primary

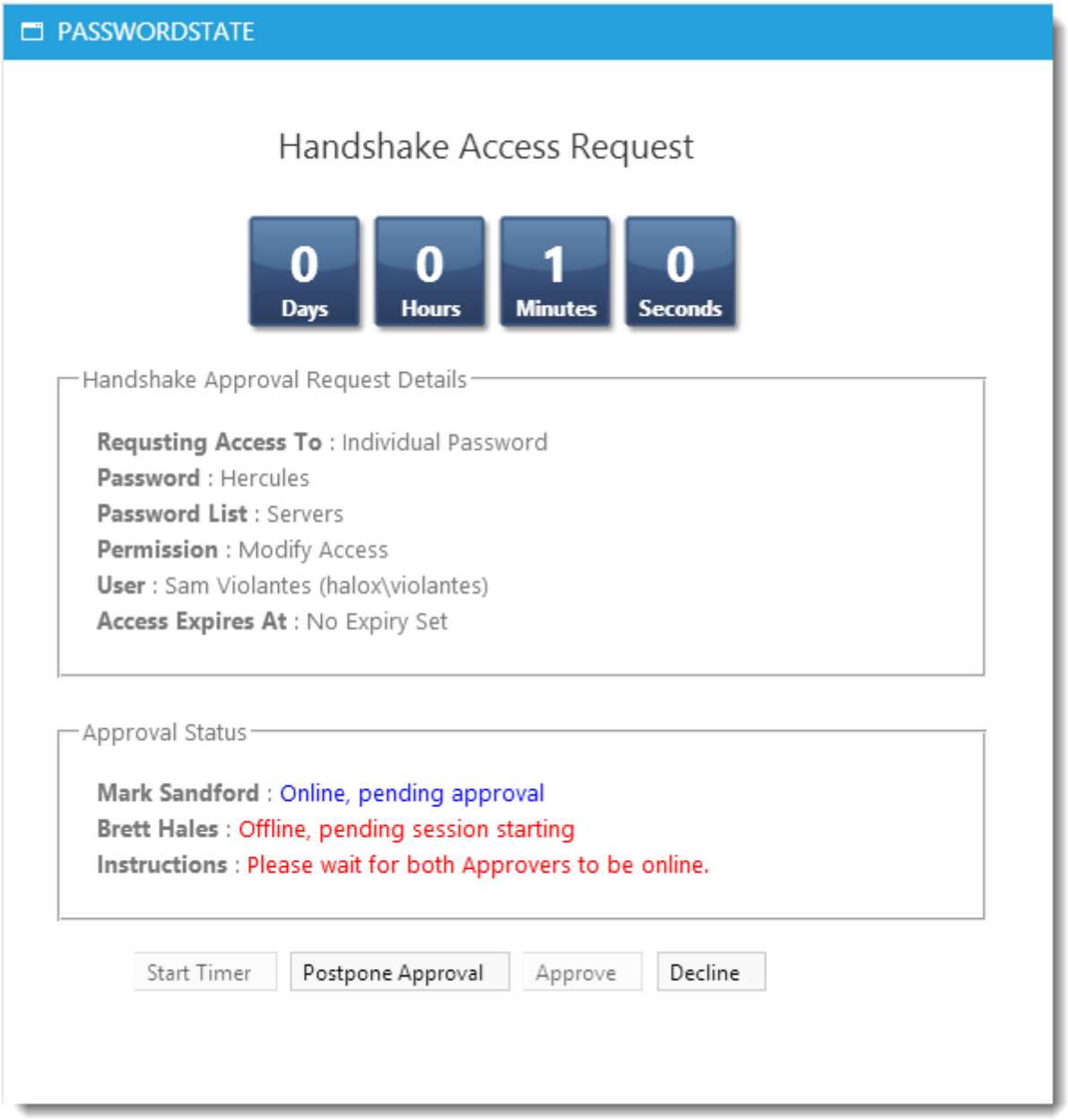
Approver (generally yourself), a Secondary Approver (someone else who has Administrator Access to the Password List), and the amount of time the Handshake Approval Timer will be visible on the screen to the two approvers.



Once the Handshake Approval has been saved, and email will be sent to both approvers asking them to click on a link and approve the access. The screen below will appear when they click on the link.

As soon as both users have this 'Handshake Access Request' screen open, the various buttons will be enabled, and the Primary Approver will then be able to start the timer. Each approver then has a set amount of time to either approve or deny the request.

Note: Administrators of a Password List can choose an to make Handshake Approval mandatory for all access to passwords (or the Password List), in which case the steps above cannot be deliberately ignored, or accidentally overlooked.



2.1.3.7.3 Copy or Move to Different Password List

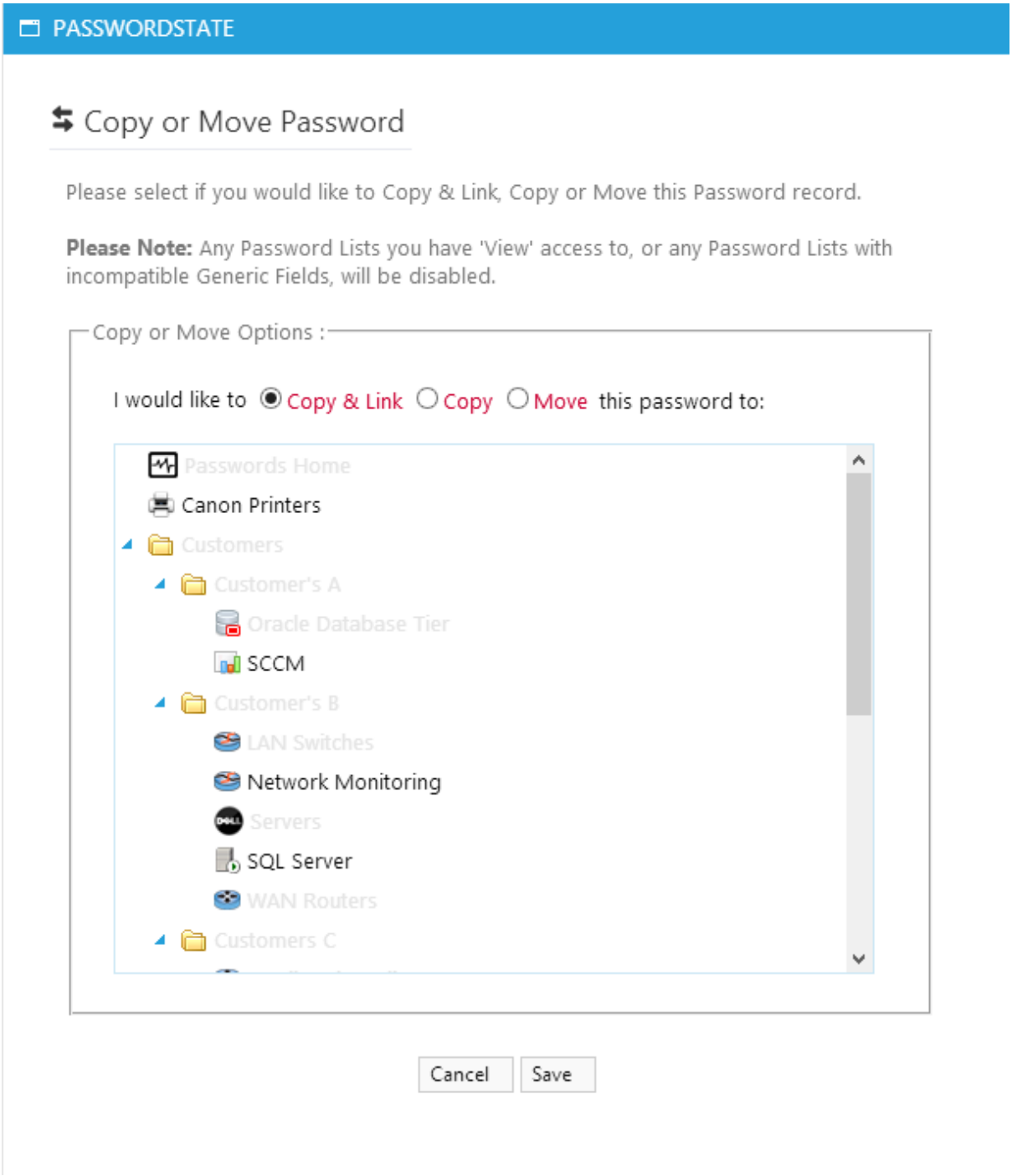
It is possible to copy or move a Password record to a different Password List, but there are a couple of exceptions which may prevent you from doing this:

- 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

If a Password List is grayed out and disabled on the pop-up windows below, then one of the two restrictions above would be the cause.
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

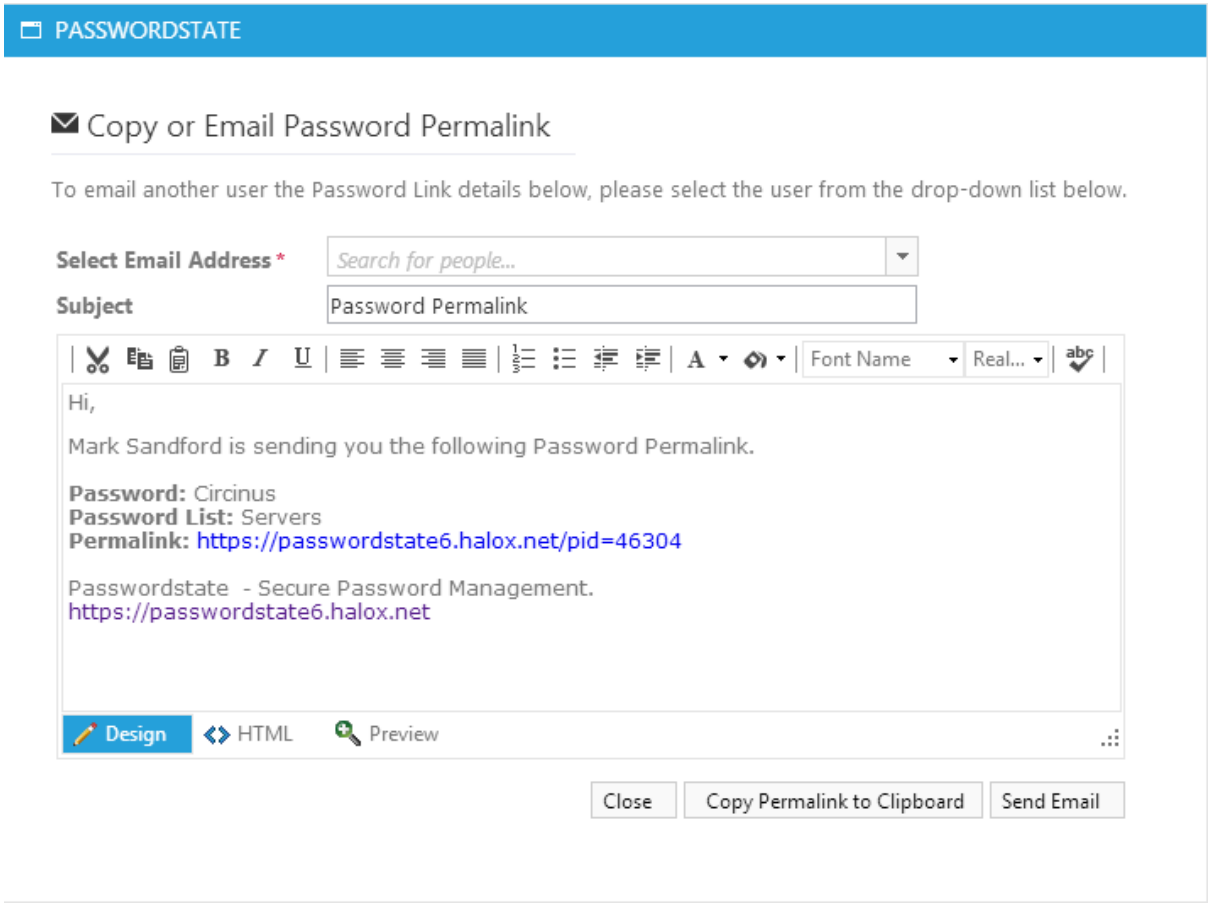
Note: Deleting a Linked Password record will not move it to the Recycle Bin in the other Linked Password Lists.



2.1.3.7.4 Copy or Email Password Permalink

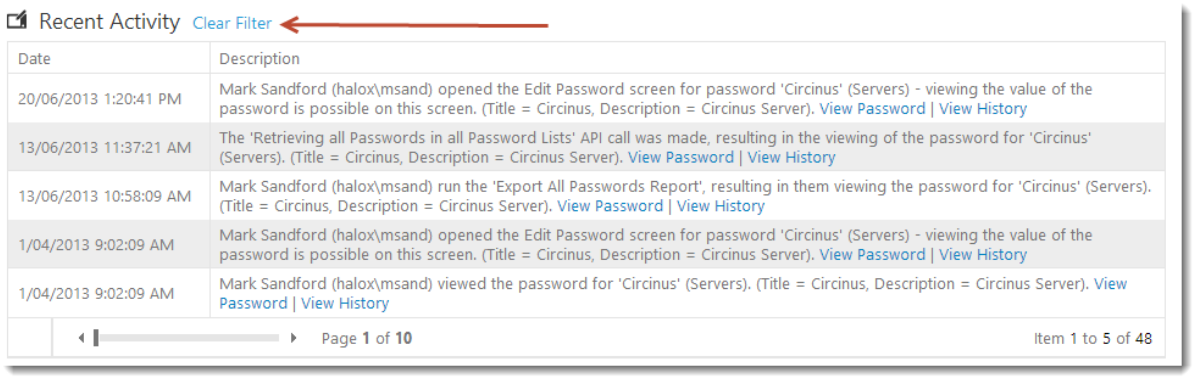
Similar to a Permalink for Password List, you can also copy a Password record's Permalink to the clipboard, or email it to another user.

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.



2.1.3.7.5 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.



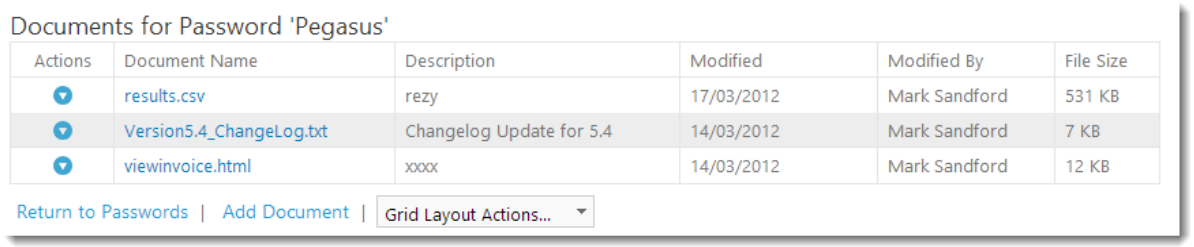
2.1.3.7.6 View Documents

As with Password Lists, it's also possible to upload one or more document/attachments and associated them with an individual Password record.

When uploading documents, they are stored within the database in binary form, and any file/ document types can be uploaded.

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.



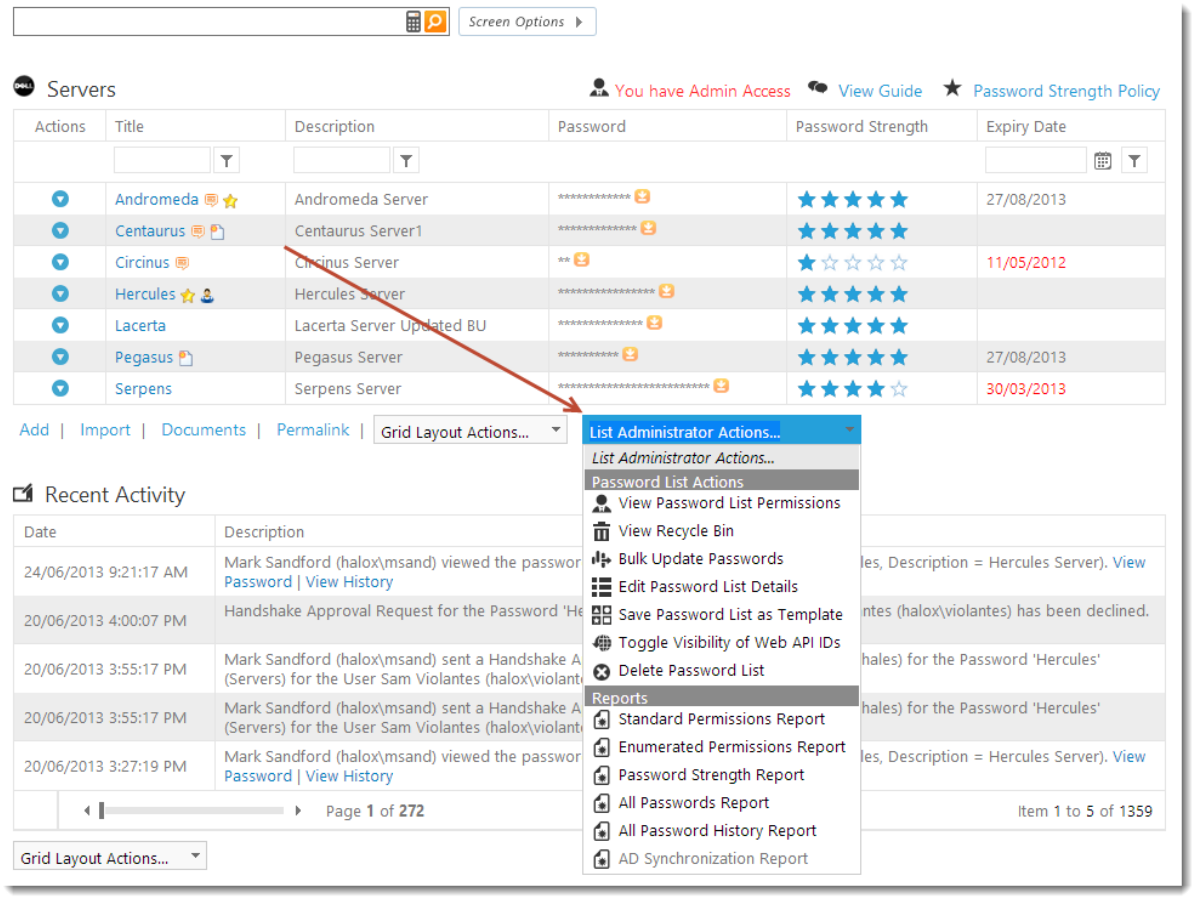
2.1.3.8 List Administrator Actions

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:

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

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
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 Web API IDs	Allows you to see various ID fields required for the Passwordstate API
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
Standard Permissions Report	Will export to csv file a list of permissions applied to the Password List, or any individual Password records
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
All Passwords Report	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
All Password History Report	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
AD Synchronization Report	If the Password List is enabled to synchronize the Passwords with Active Directory, or a local Windows Server, this report will generate a list in real-time as to whether the password values are in sync

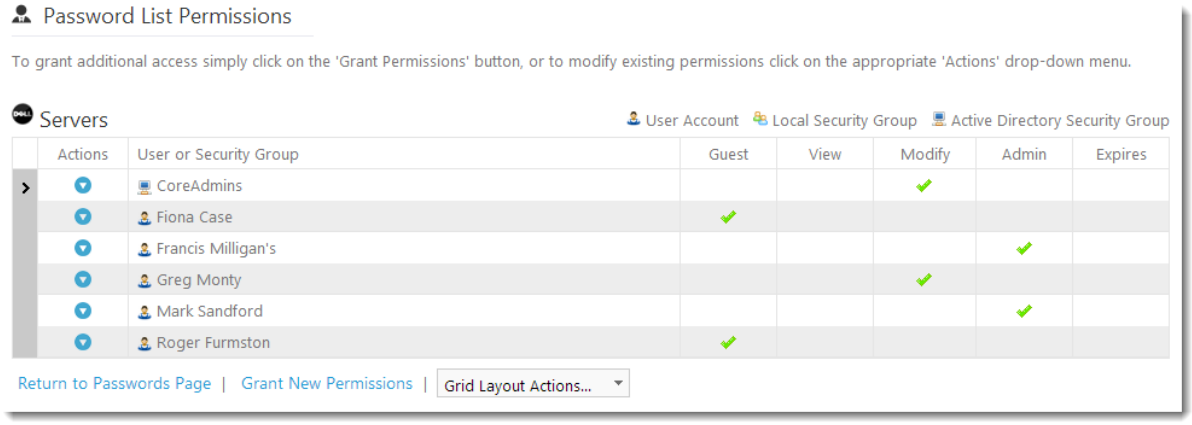


2.1.3.8.1 View Password List Permissions

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, 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

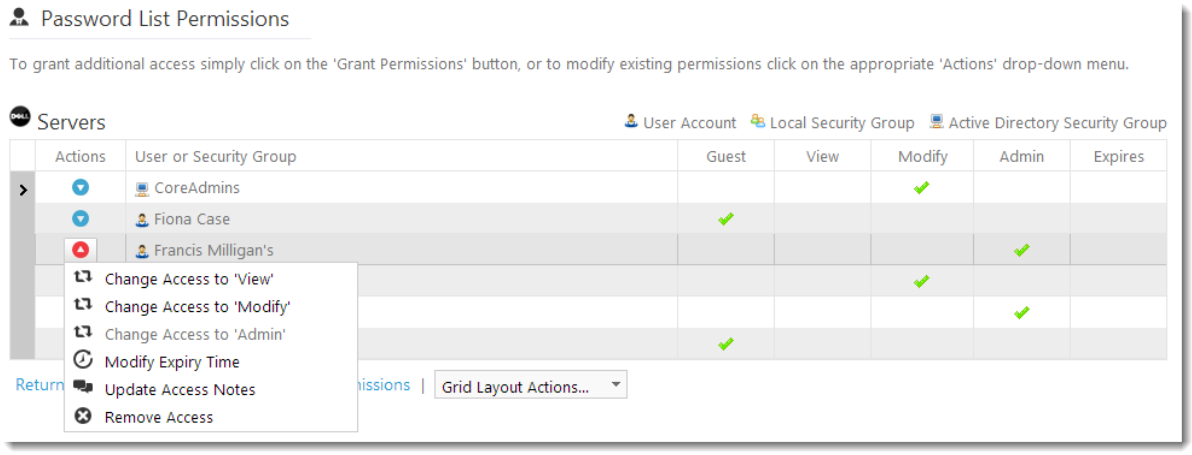


From the 'View Password List Permissions' screen, you have the following features available:

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, Modify or Admin
- 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.

2.1.3.8.1.1 Grant New Permissions

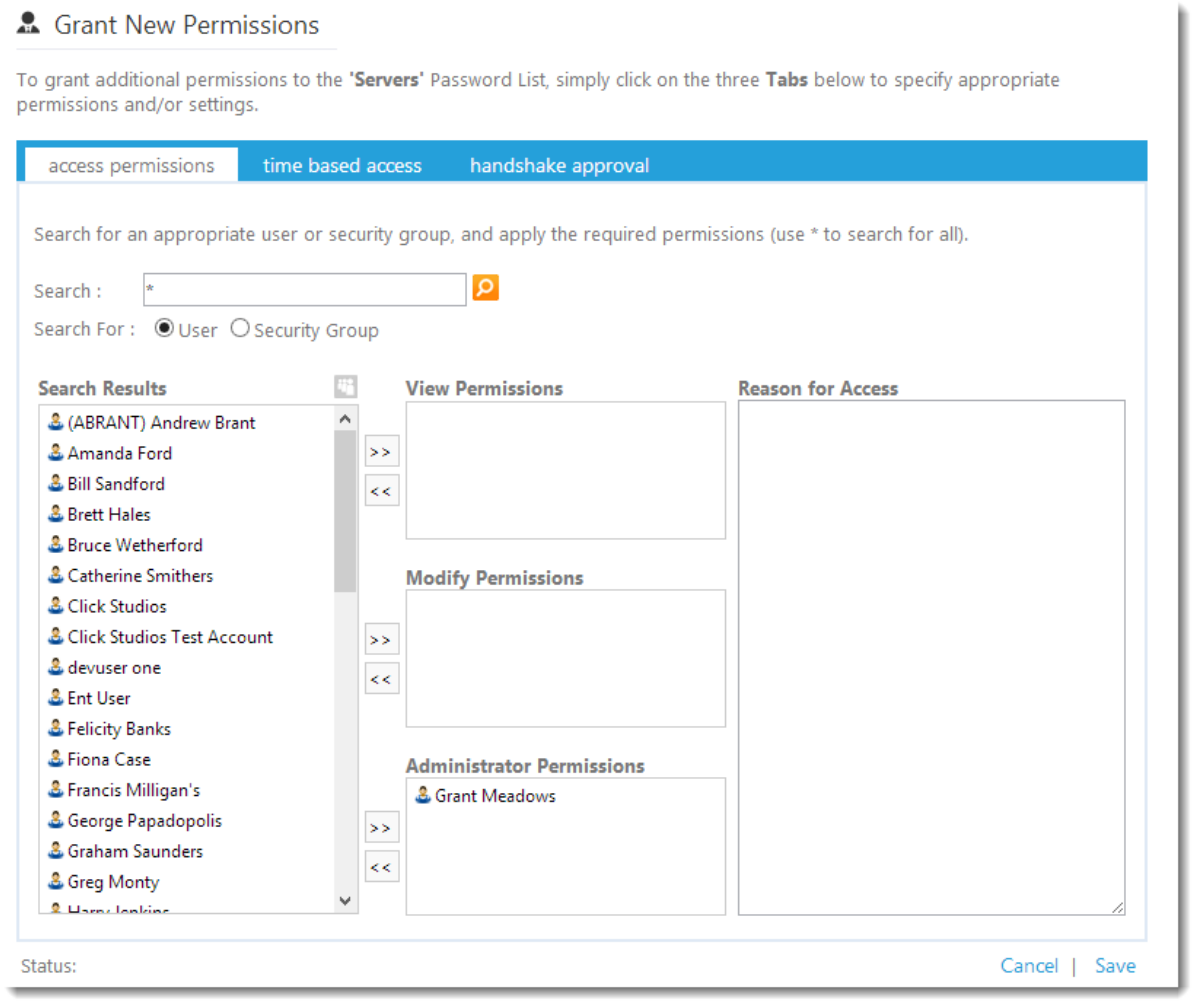
You can grant new permissions to either User Accounts, or members of a Security Group - either local Security Groups within Passwordstate, or Active Directory based Security Groups.

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:

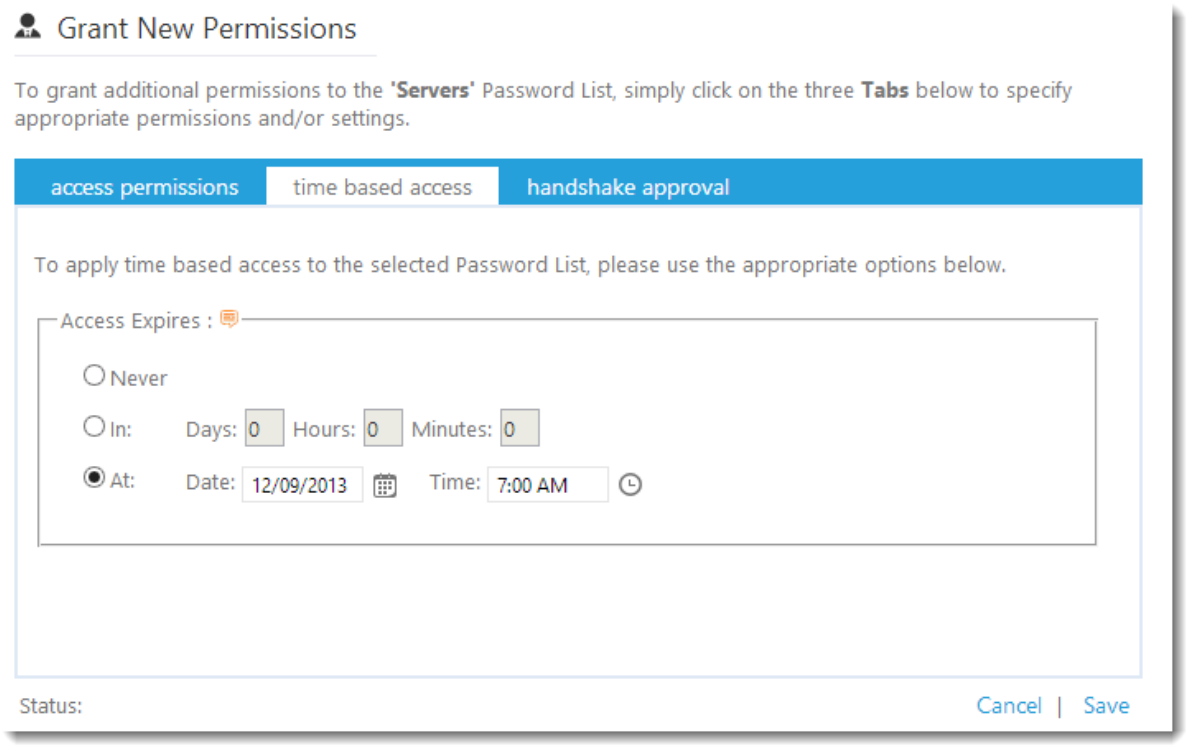
Access Permissions

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



Time Based Access

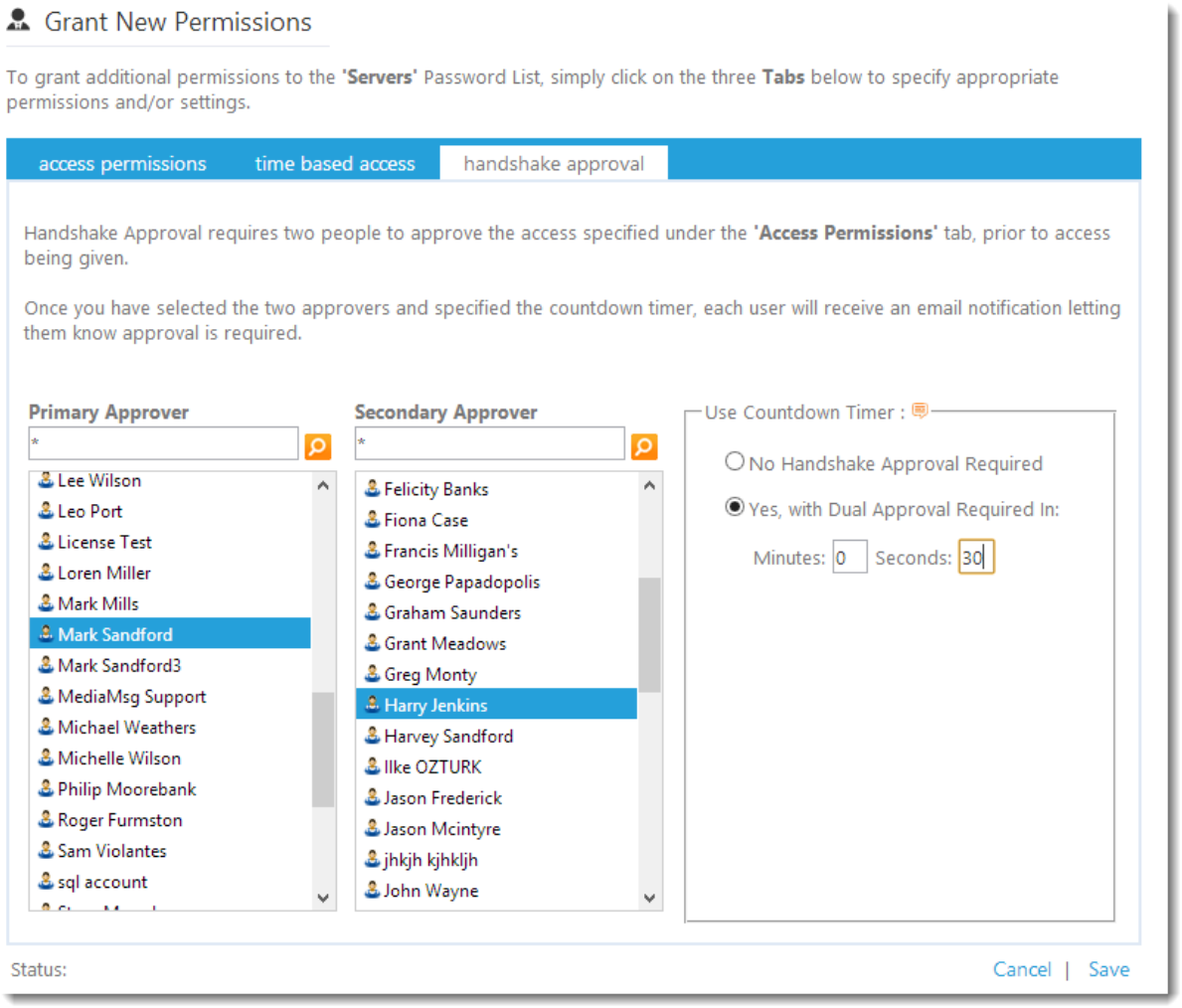
If you require the permissions to be removed after a certain period of time, or at a set time, you can specify the appropriate time period on the 'Time Based Access' tab.



Handshake Approval

'Handshake Approval' can be used for Password List which are of a various sensitive nature, and requires more than one Password List Administrator to approve access, prior to it being given to the user.

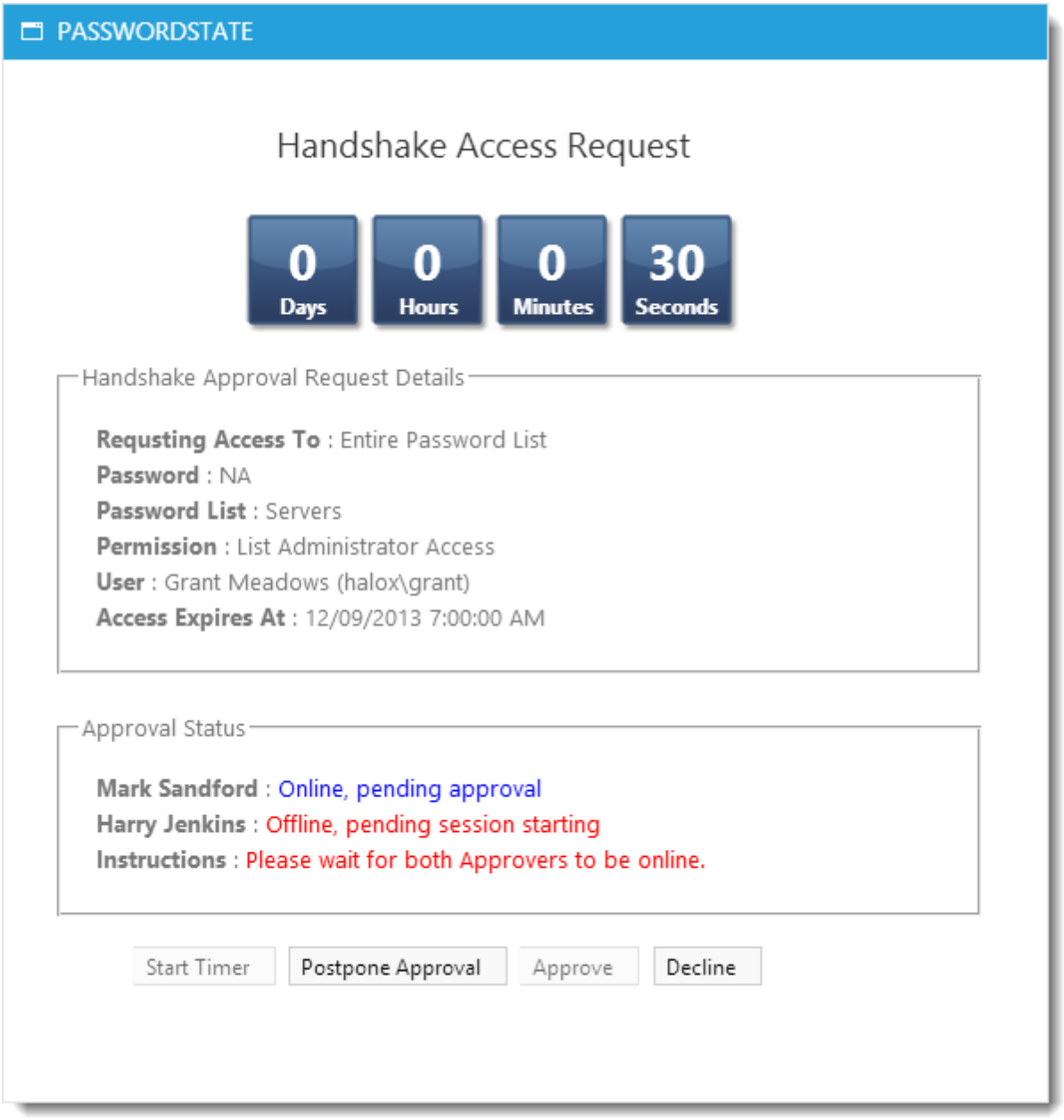
To specify Handshake Approval is require for this Password record, you need to select a Primary Approver (generally yourself), a Secondary Approver (someone else who has Administrator Access to the Password List), and the amount of time the Handshake Approval Timer will be visible on the screen to the two approvers.



Once the Handshake Approval has been saved, and email will be sent to both approvers asking them to click on a link and approve the access. The screen below will appear when they click on the link.

As soon as both users have this 'Handshake Access Request' screen open, the various buttons will be enabled, and the Primary Approver will then be able to start the timer. Each approver then has a set amount of time to either approve or deny the request.

Note: Administrators of a Password List can choose an to make Handshake Approval mandatory for all access to passwords (or the Password List), in which case the steps above cannot be deliberately ignored, or accidentally overlooked.

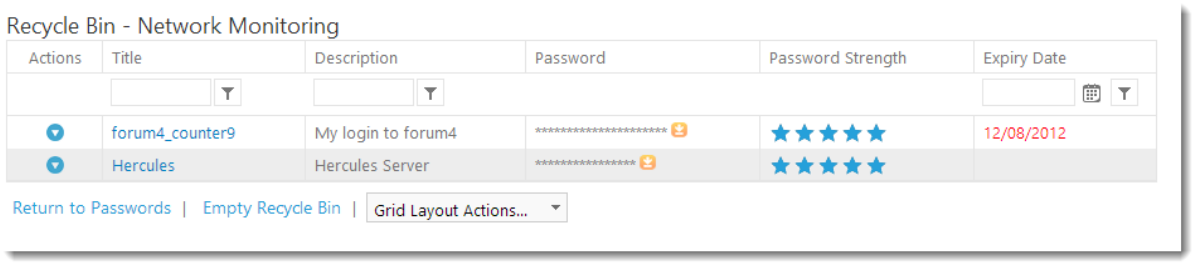


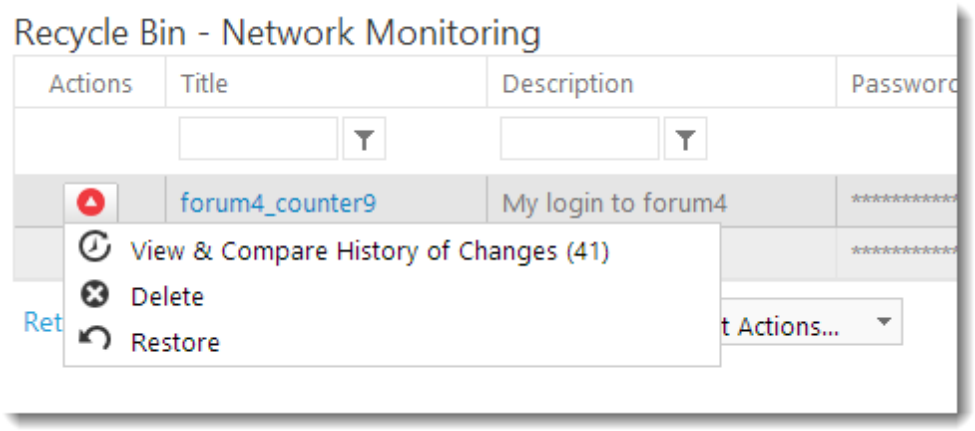
2.1.3.8.2 View Recycle Bin

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), a long 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





2.1.3.8.3 Bulk Update Passwords

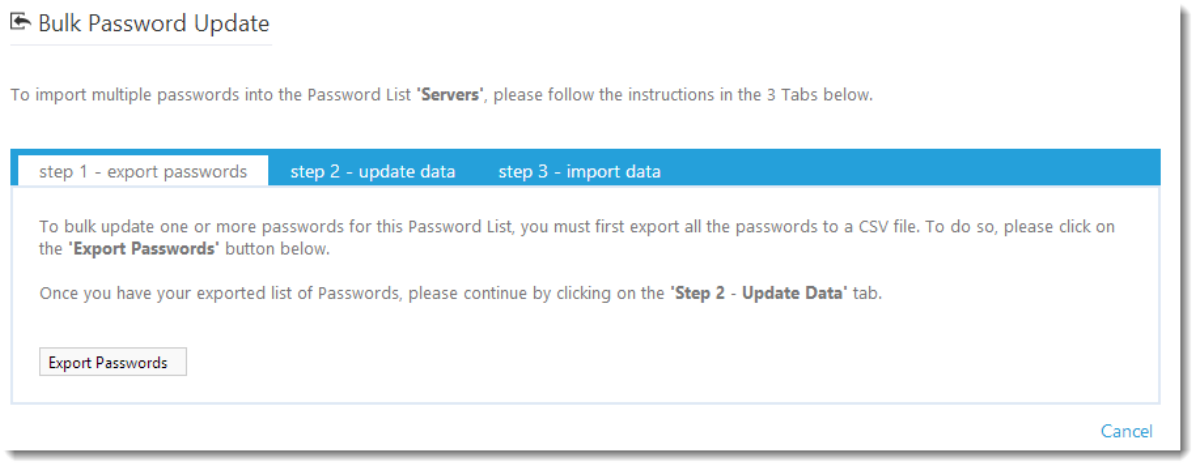
If you have a requirement to update more than one Password record at a time, then you can use the 'Bulk Update Passwords' feature.

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: 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

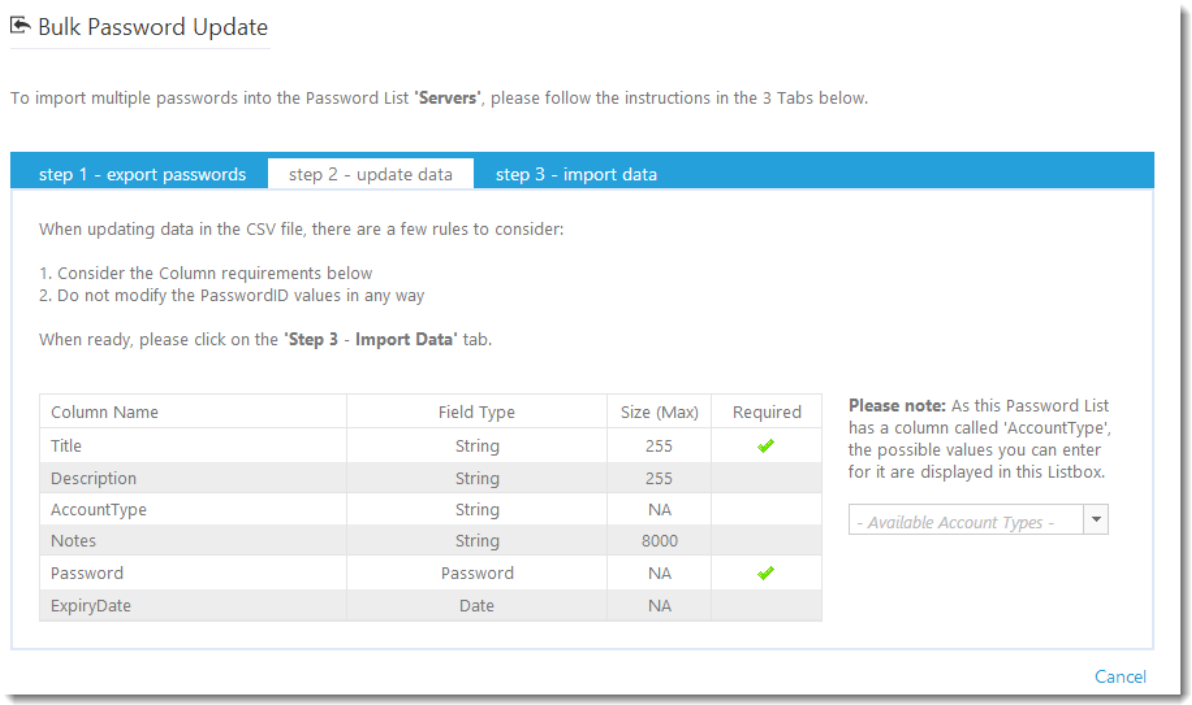
Clicking on the 'Export Passwords' button will export all Password records to a csv file. Once you have your csv file, you can move onto the next tab 'Step 2 - Update Data'.



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'.

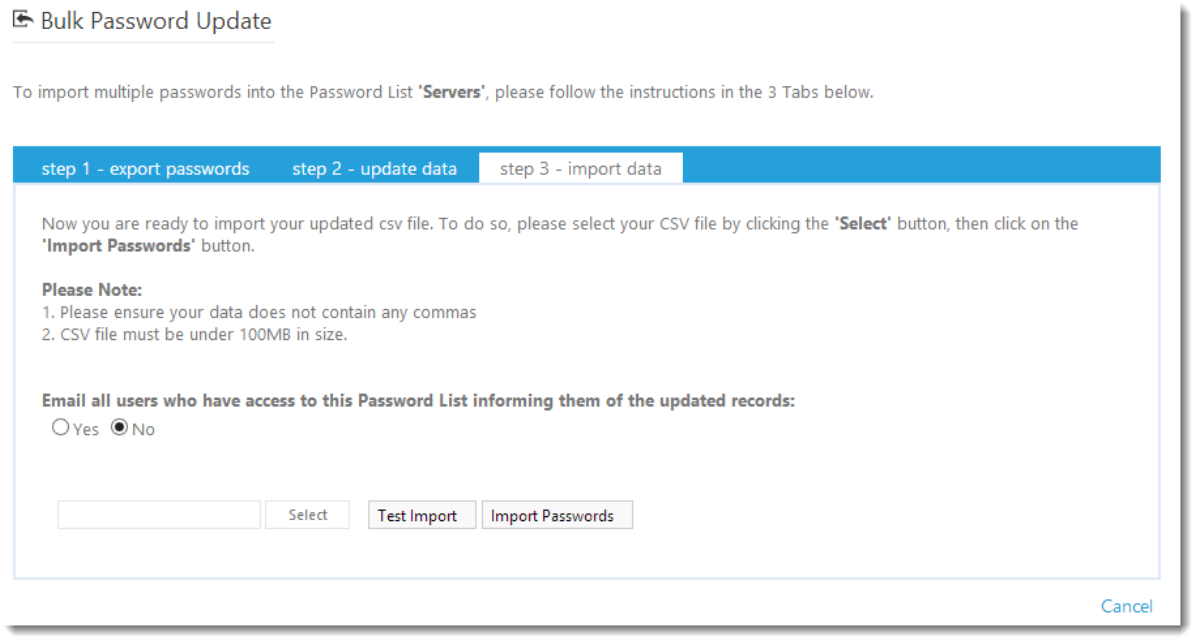
Note: If a field already has data associated with it, but you don't wish to update the data for this field, you simply leave the value as it is - if you remove the data for this field, it will also remove it in the database when the import process occurs



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.



2.1.3.8.4 Edit Password List Details

The Edit Password List Details 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

2.1.3.8.4.1 Password List Details Tab

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.

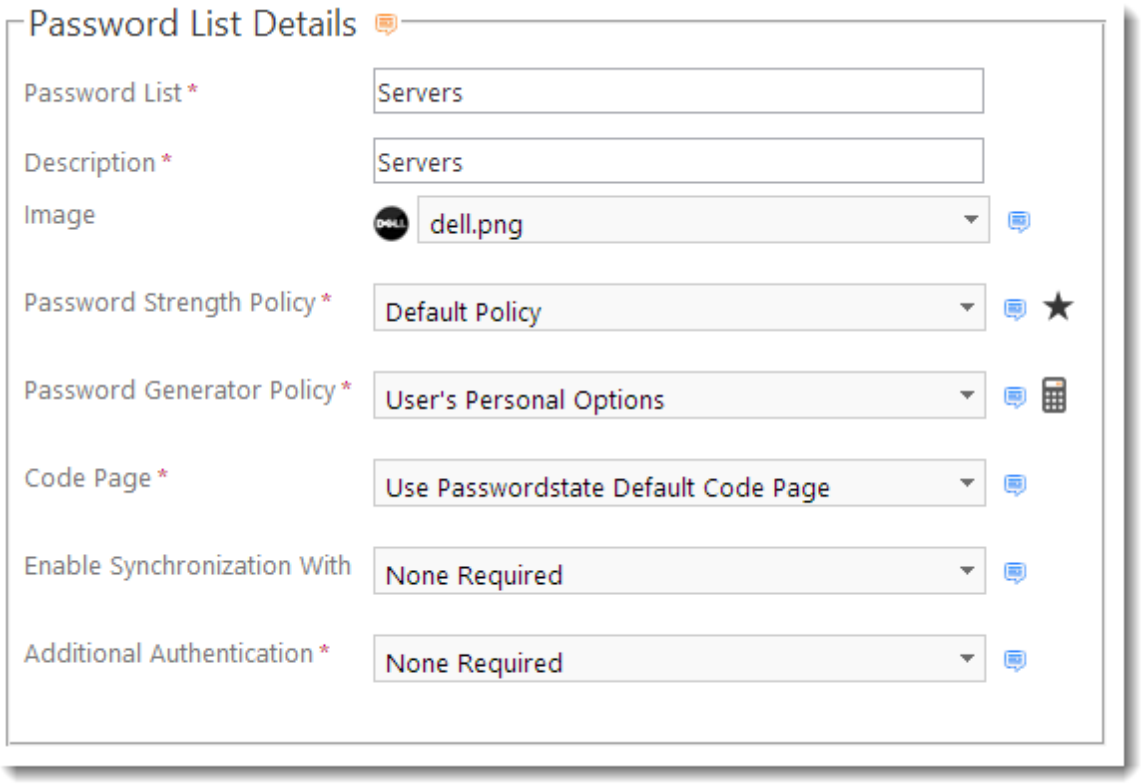
Note: The various Password related options below do not apply to any Generic Fields (Customize Fields Tab) you configure of type 'Password' i.e. prevent password reuse, prevent saving bad password, reset expiry date field, etc.

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:

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
Enable Synchronization With	Select the type of synchronization you would like to occur between Passwords in the Password List, and other systems - currently synchronization with Active Directory or Windows Servers is currently possible, with more to come soon. Selecting an option here will select the 'Generic Fields' required to enable the Password List for synchronization
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

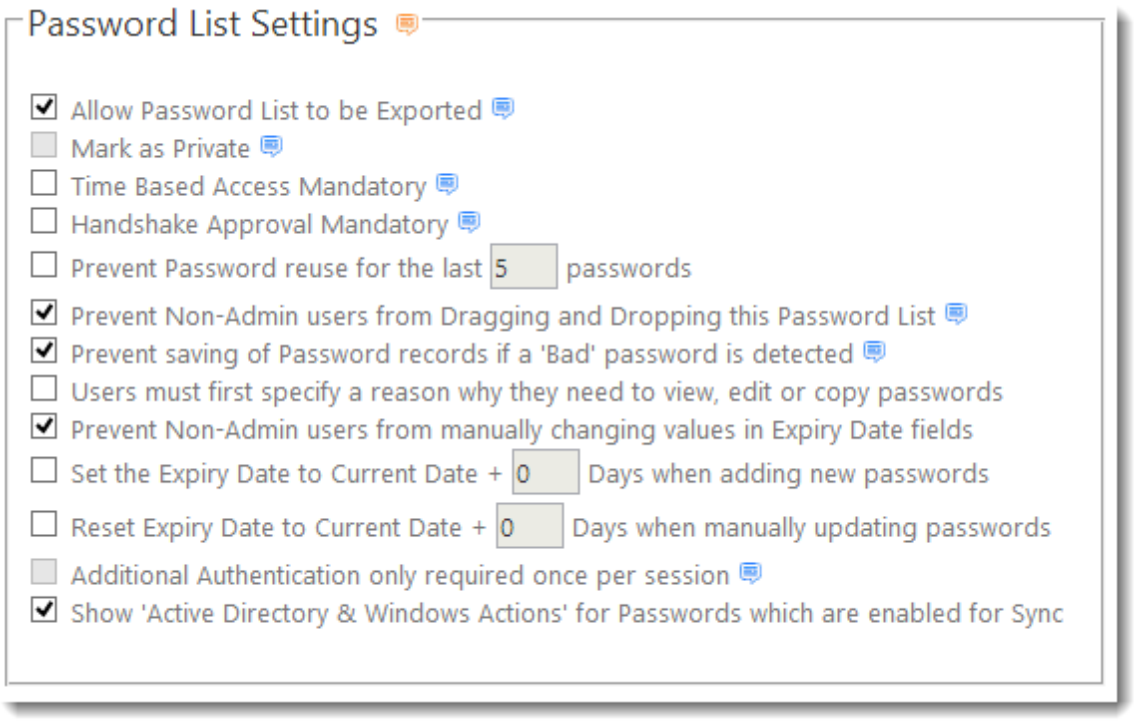


Password List Settings Section

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

Allow Password List to be Exported	Allows or prevents the passwords and their history from being exported
Mark as Private	This option is not selectable - it will be set to True when you create a Private Password List, and False when you create a Shared Password List
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
Handshake Approval 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 who the Primary and Secondary approvers are for Handshake Approval, which must be dual approved prior to access being given
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

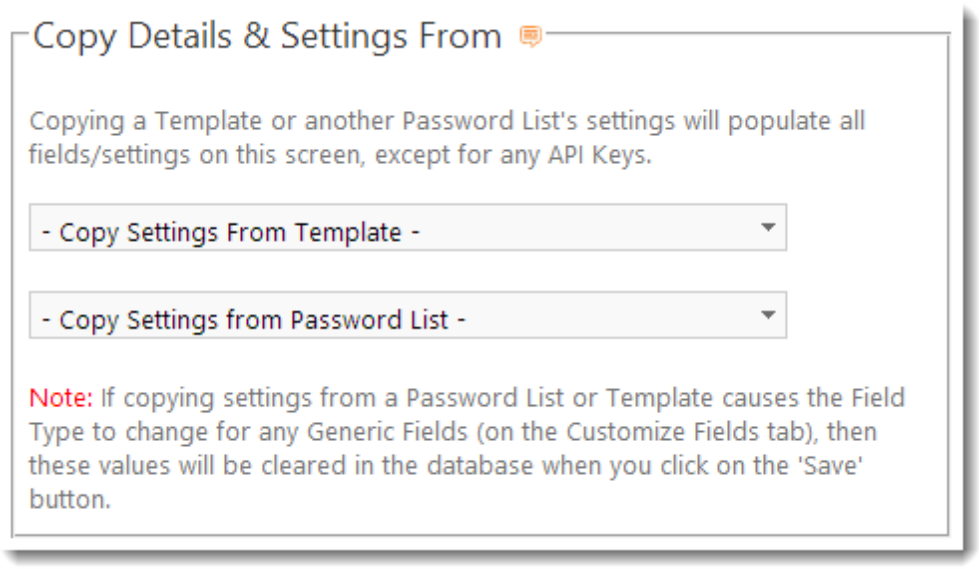
Prevent Non-Admin users from Dragging and Dropping	You can select this option to minimize who can drag and drop the Password List around in the Navigation Tree
Prevent saving of Password records if a 'Bad' password is detected	Your Security Administrators maintain a list of passwords in Passwordstate 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 & Windows Actions' for Passwords which are enabled for Sync	If the Password List is enabled for synchronization with Active Directory or a local Windows Server, enabling this option will provide the following 4 'Actions' which can be performed on the account: • Unlock this account if locked • User must change password at next logon • Disable this account • Enable this account



Copy Details & Settings from Section

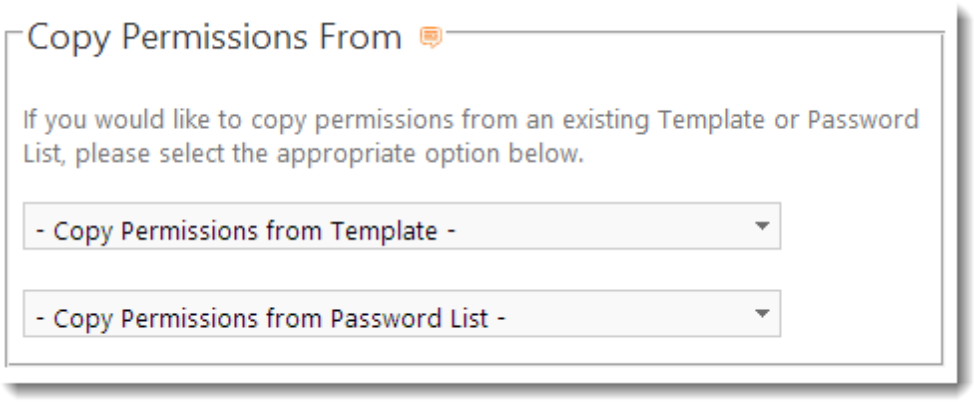
This section allows you to copy Password List settings, and fields to use, from another Password List or Template.

Note: 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.



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.



Default Options for Automatic Password Rotation Section

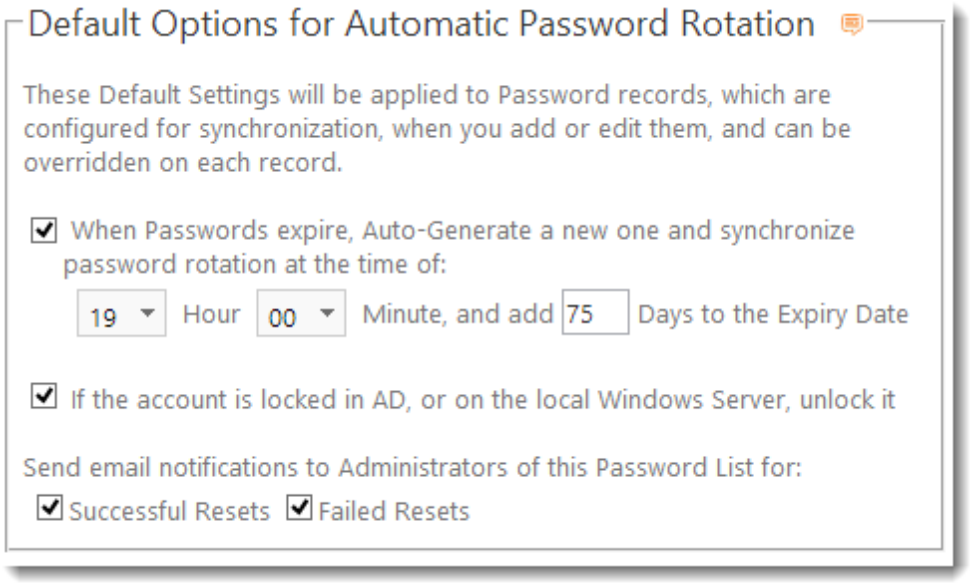
If a Password List is configure to synchronize an account with Active Directory or local Windows Server, you can then set various 'Automatic Password Rotation' settings - used for resetting a Password once the Expiry Date field value is reached.

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

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 Rotation schedules for each of the Passwords stored in a Password List - if required.



2.1.3.8.4.2 Customize Fields Tab

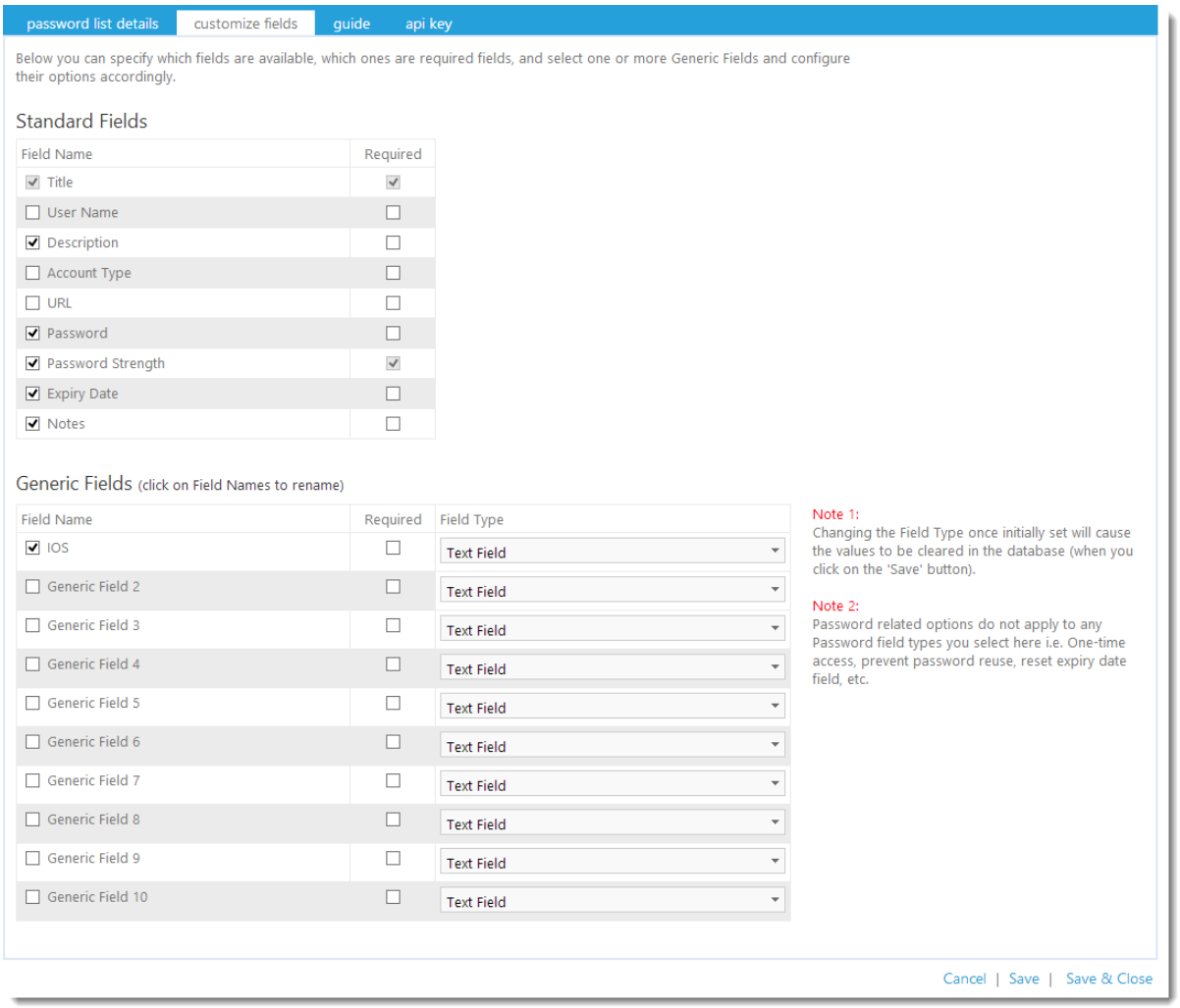
The Customize Fields tab is where you specify which fields you would like to use with the Password List, which of the fields are mandatory, and specify certain 'Field Types' for any one of the 10 Generic Fields.

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

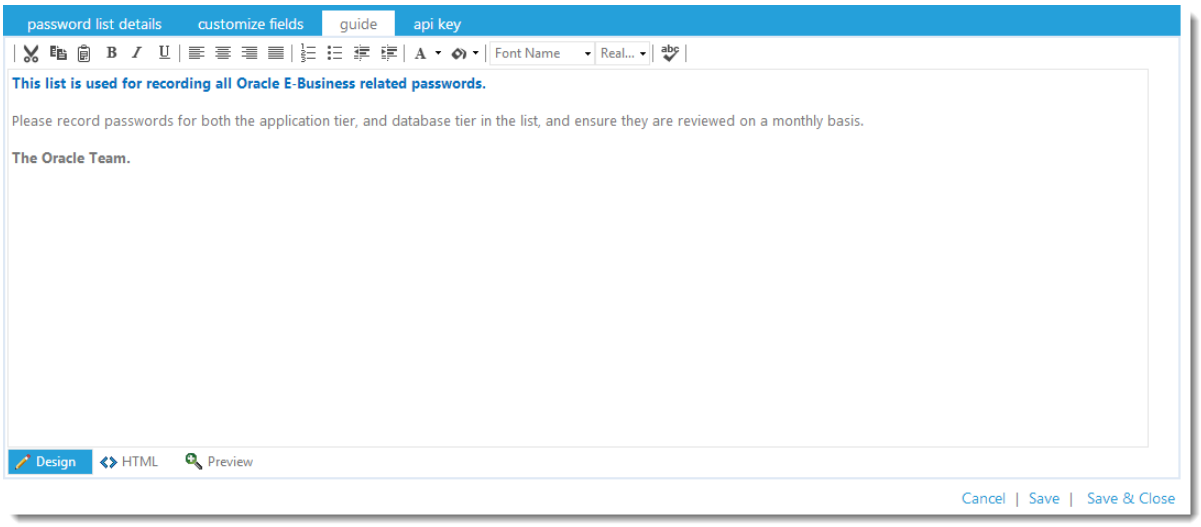
Password Strength	You cannot enter any data for the Password Strength field - it's a graphical representation of how strong the password is, based on the selected Password Strength Poilcy
Expiry Date	All passwords should be reset after a certain period of time. The Expiry Date field can be used to indicate 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


Note: 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.

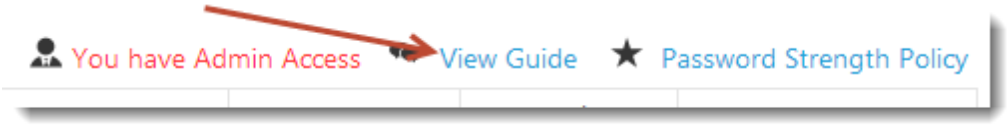


2.1.3.8.4.3 Guide Tab

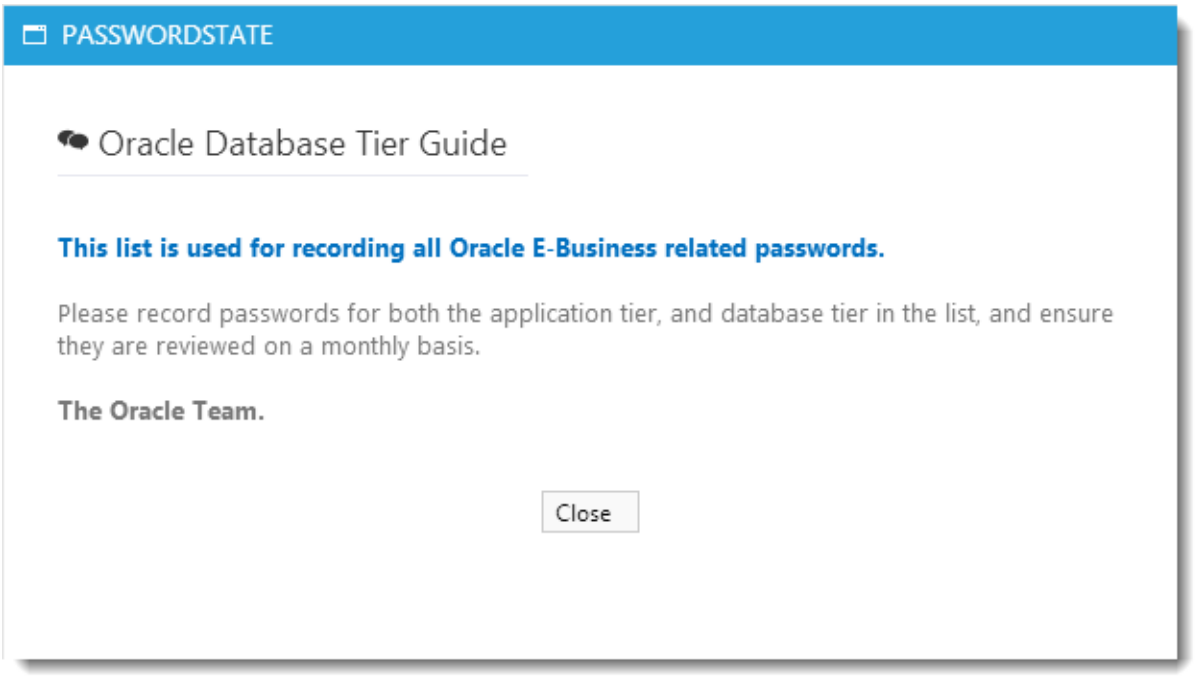
The Guide tab allows you to provide detail as to the intended use of the Password List, and can include some basic HTML style formatting.



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.



2.1.3.8.4.4 API Key Tab

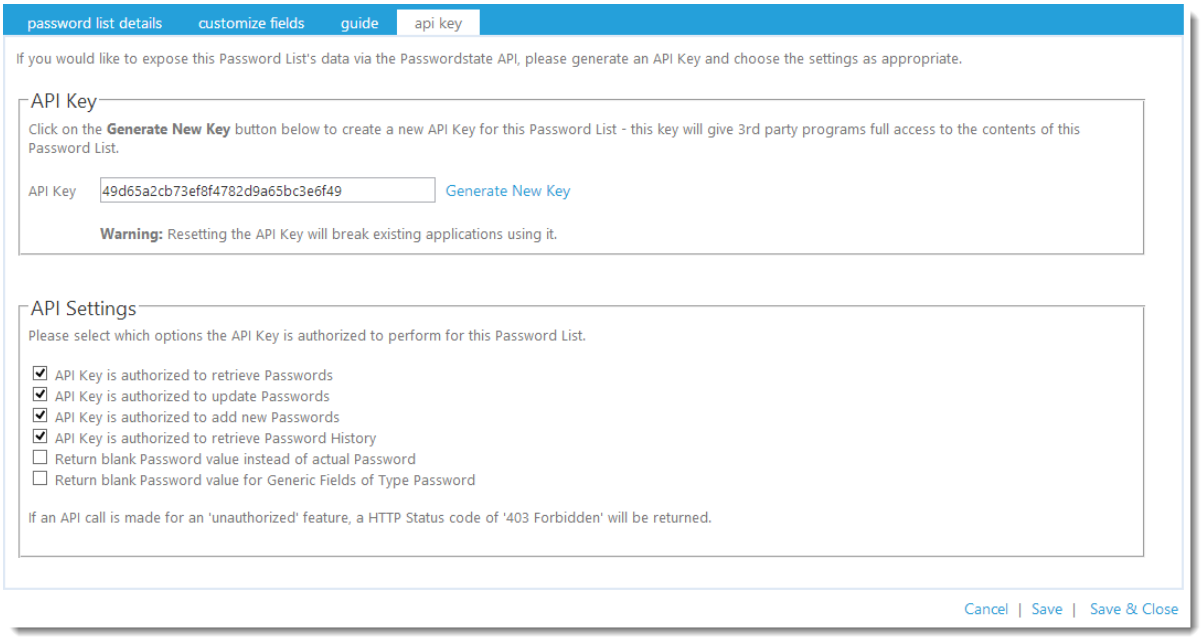
If you would like to expose certain data and features for the Password List to the Passwordstate API (Application Programmable Interface), then you must first create an API Key - each Password List must have it's own unique API Key.

In addition to specifying the API Key, 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.

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.



2.1.3.8.5 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

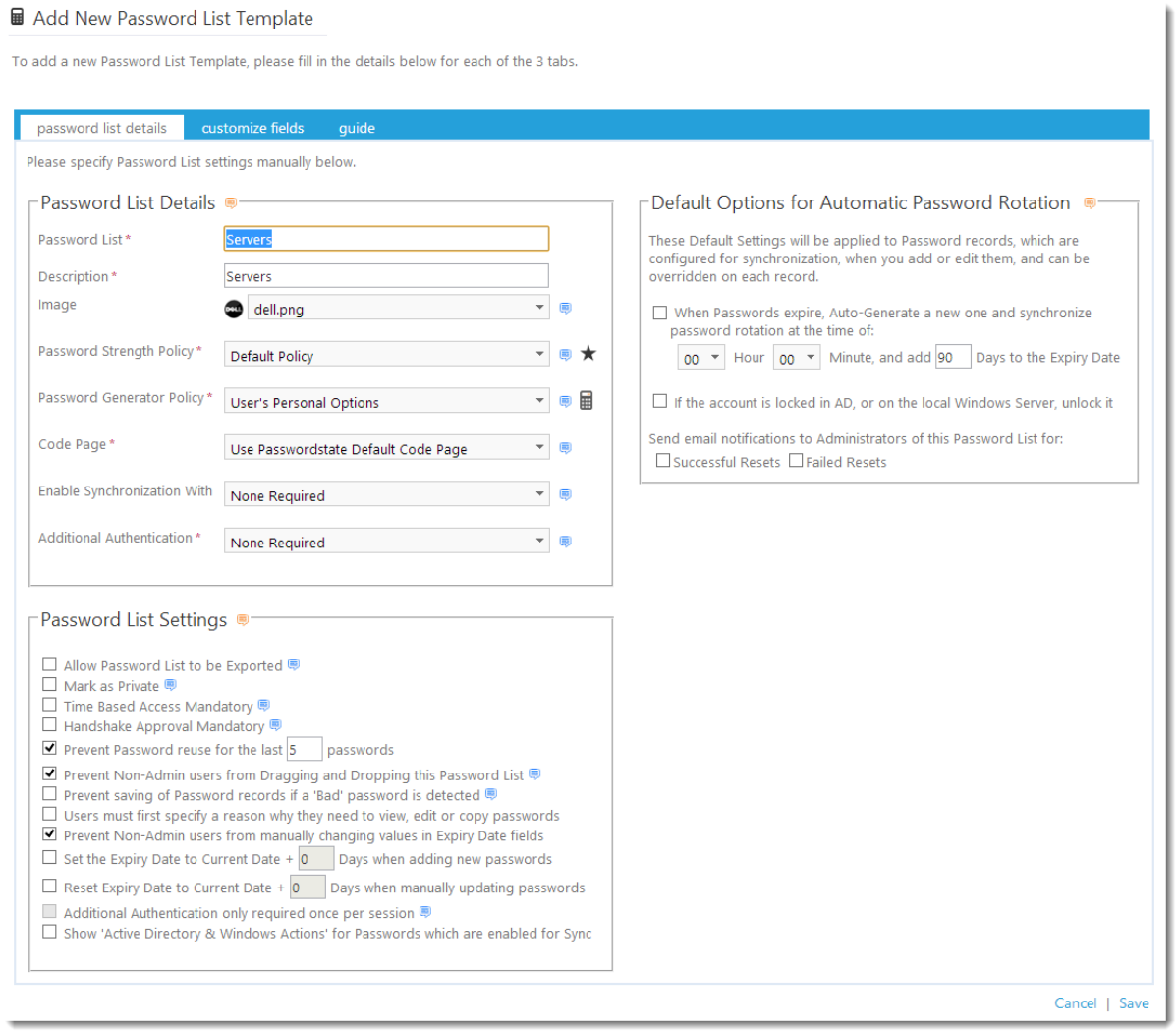
when you link Password Lists to Templates (Linked Password Lists).

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.

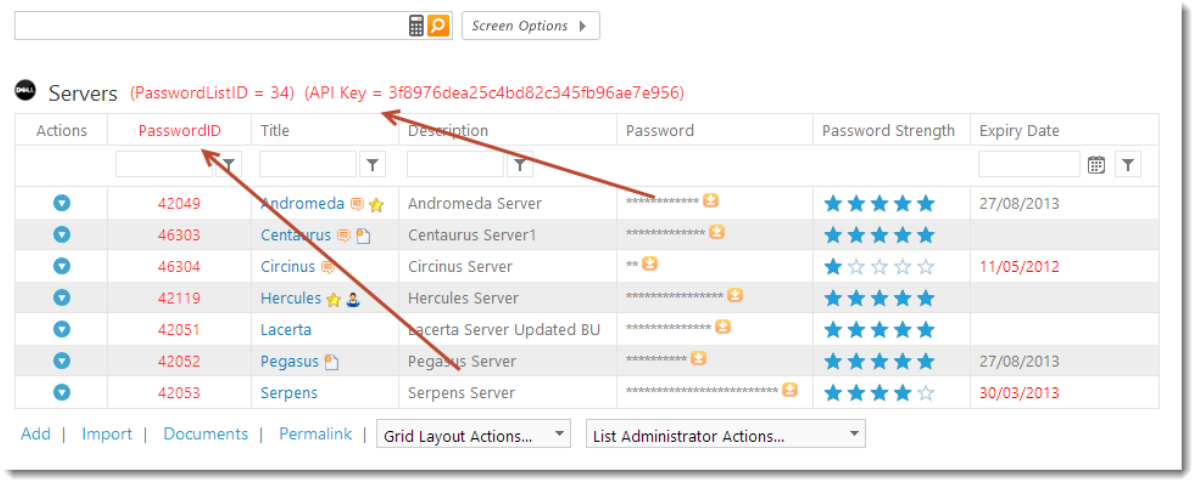


2.1.3.8.6 Toggle Visibility of Web API IDs

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.



2.2 Add Folder

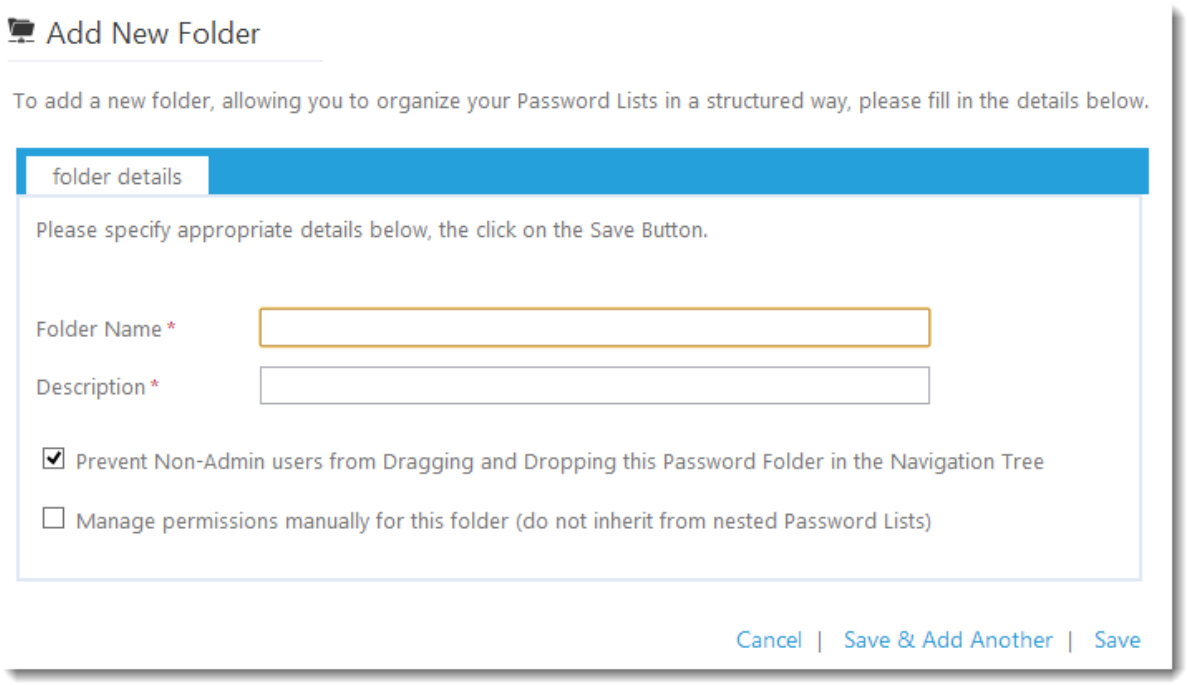
Folders are used to simply logically group other Folders or Password Lists - similar to a directory structure on a file system

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

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
Manage permissions manually for this folder	By default, Folders inherit permissions from the Password Lists which are nested beneath it. You can choose to manage permissions manually for Folders if you like, but every time you make changes to permissions for nested Password Lists, you may need to make changes to the permissions

	of upper-level Folders as well

Note: When you add a new Folder, your account will be granted Admin rights to the Folder, 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 Folder to any position in the Navigation Tree that you like.



2.3 Add Private Password List

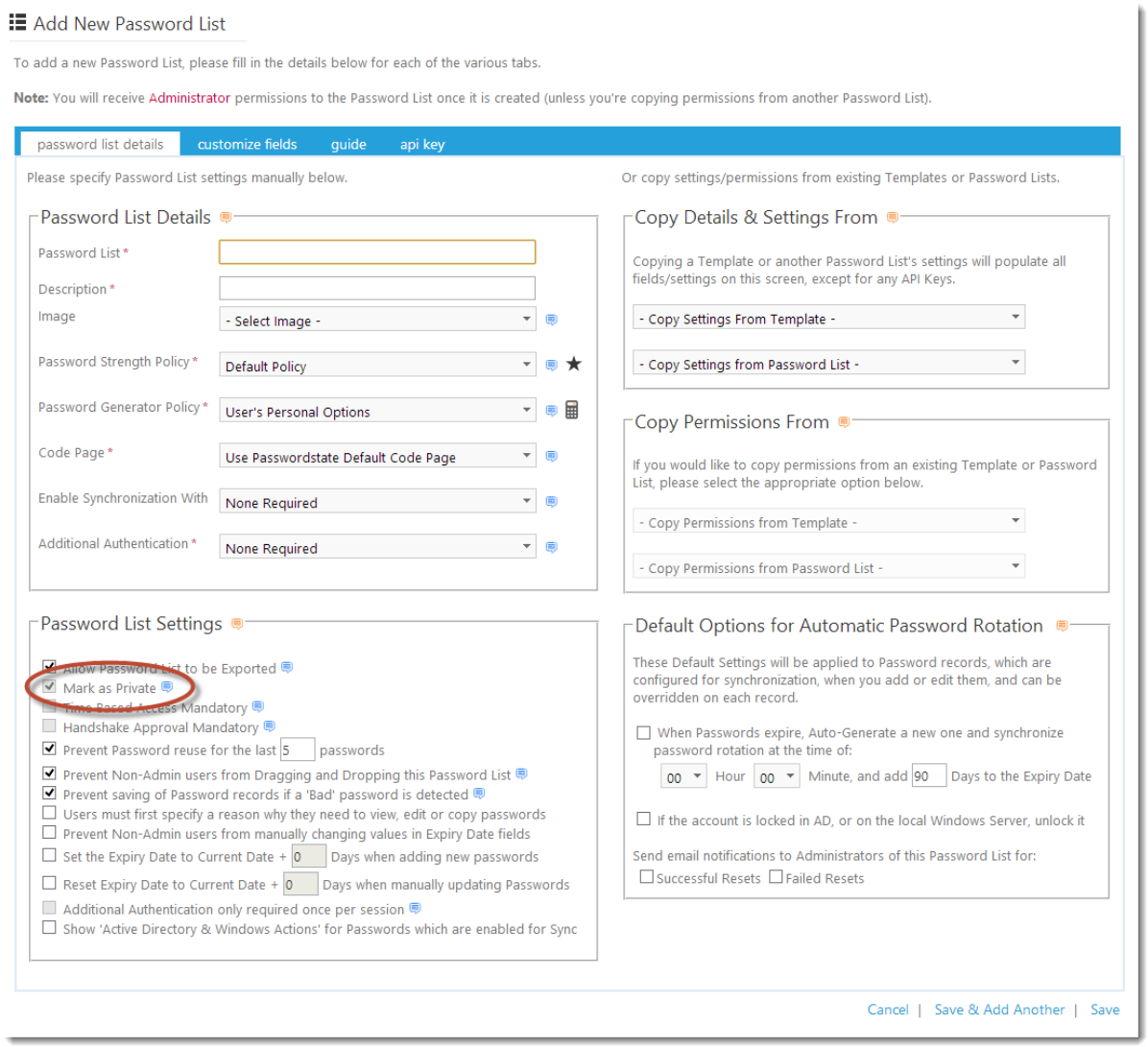
Private Password Lists are almost identical to Shared Password Lists, except the only person who can see a Private Password List and it's contents, is the person who created it - not even Security Administrators of Passwordstate are aware any Private Password Lists exist.

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.

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 Tab.

Note: Be very 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: 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.



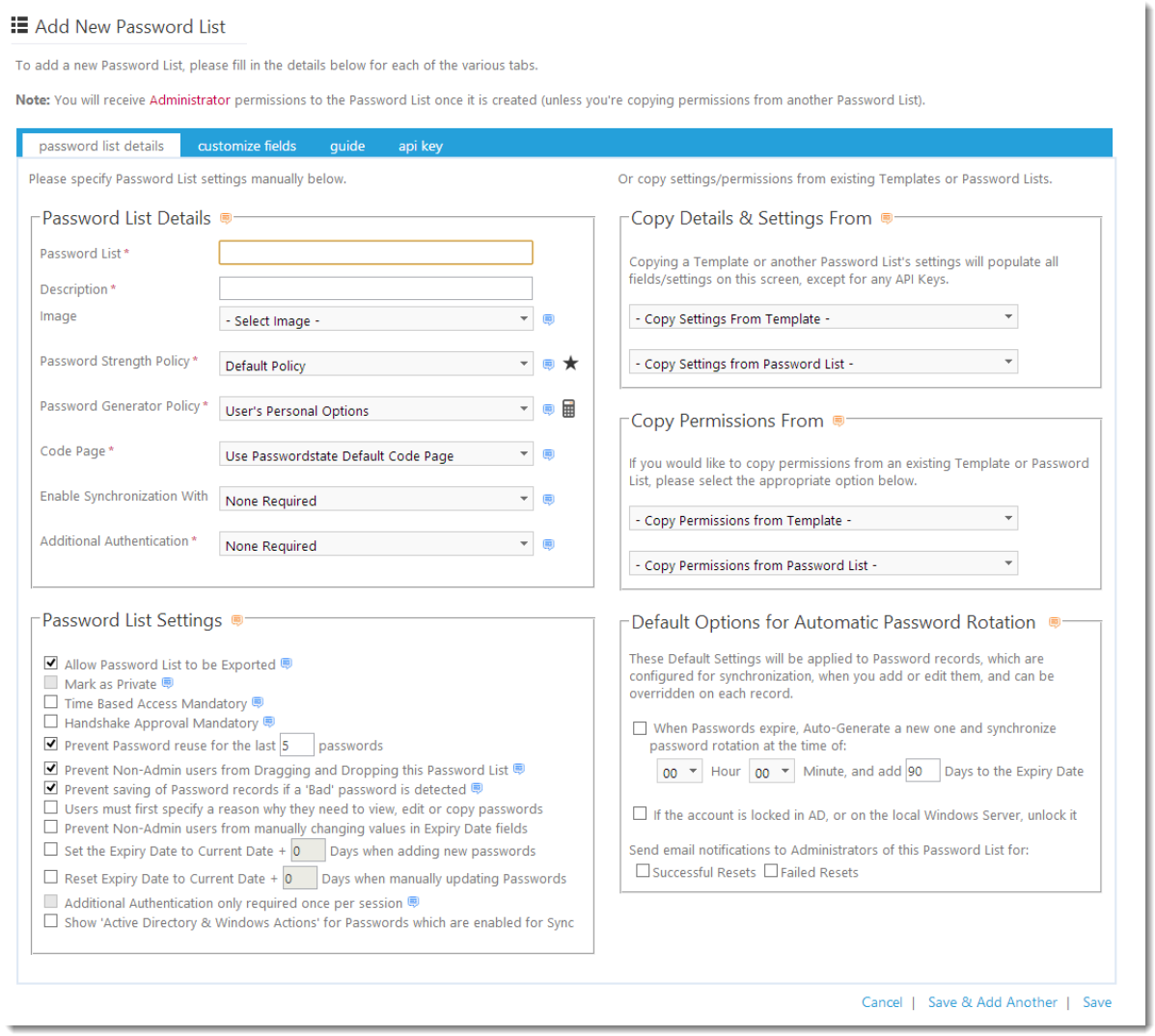
2.4 Add Shared Password List

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.

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 Tab.

Note: 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.



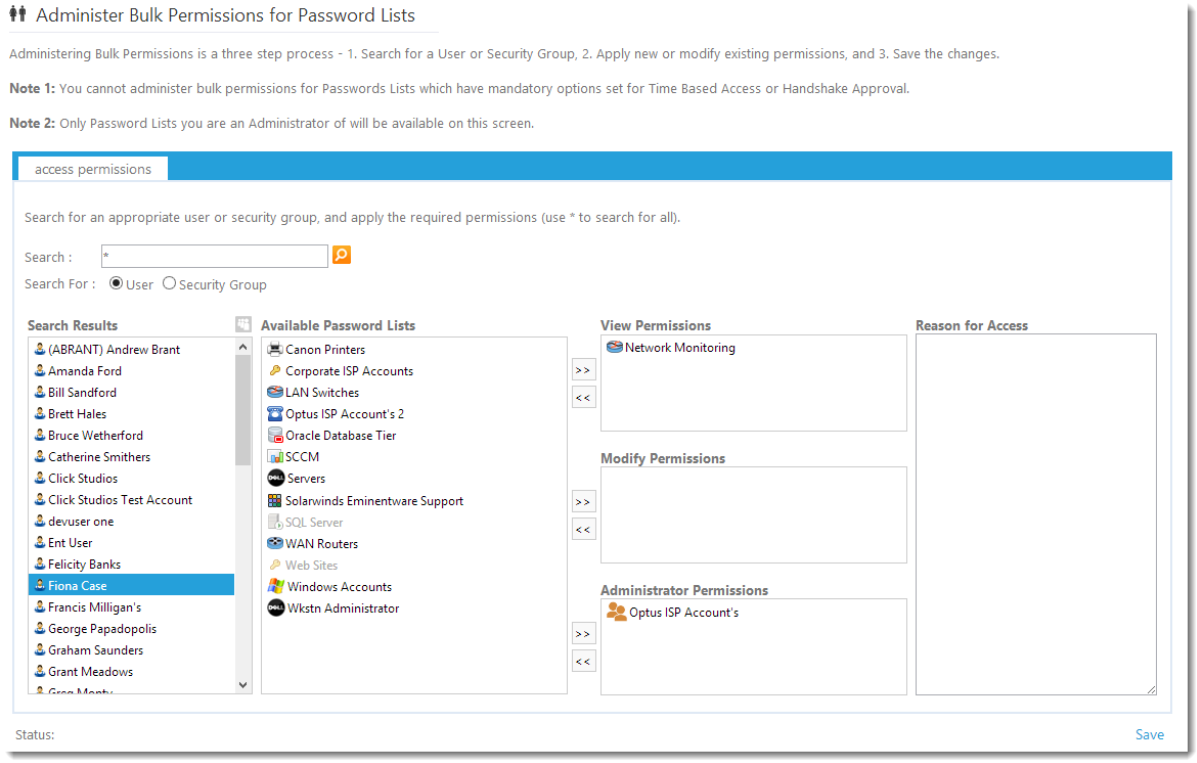
2.5 Administer Bulk Permissions

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 or Handshake Approval set as mandatory, will be disabled in the search results.

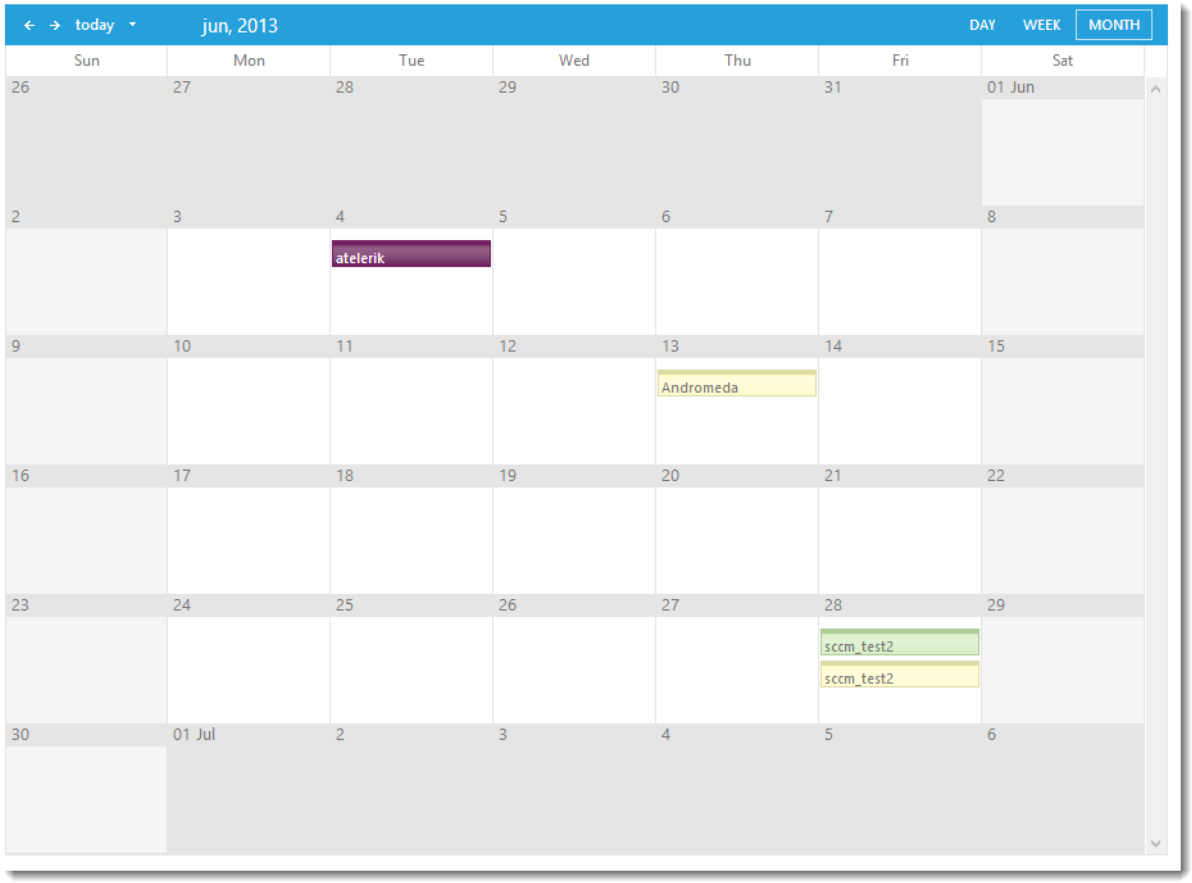


2.6 Expiring Passwords Calendar

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.



2.7 Password List Templates

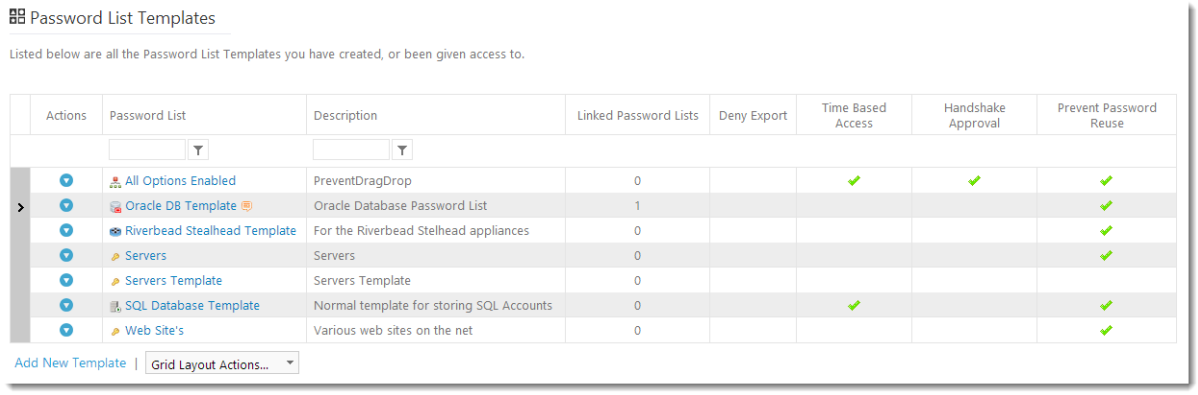
Password List Templates can be used to apply consistency to settings for your Password Lists. They can be used in the following way:

- 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.

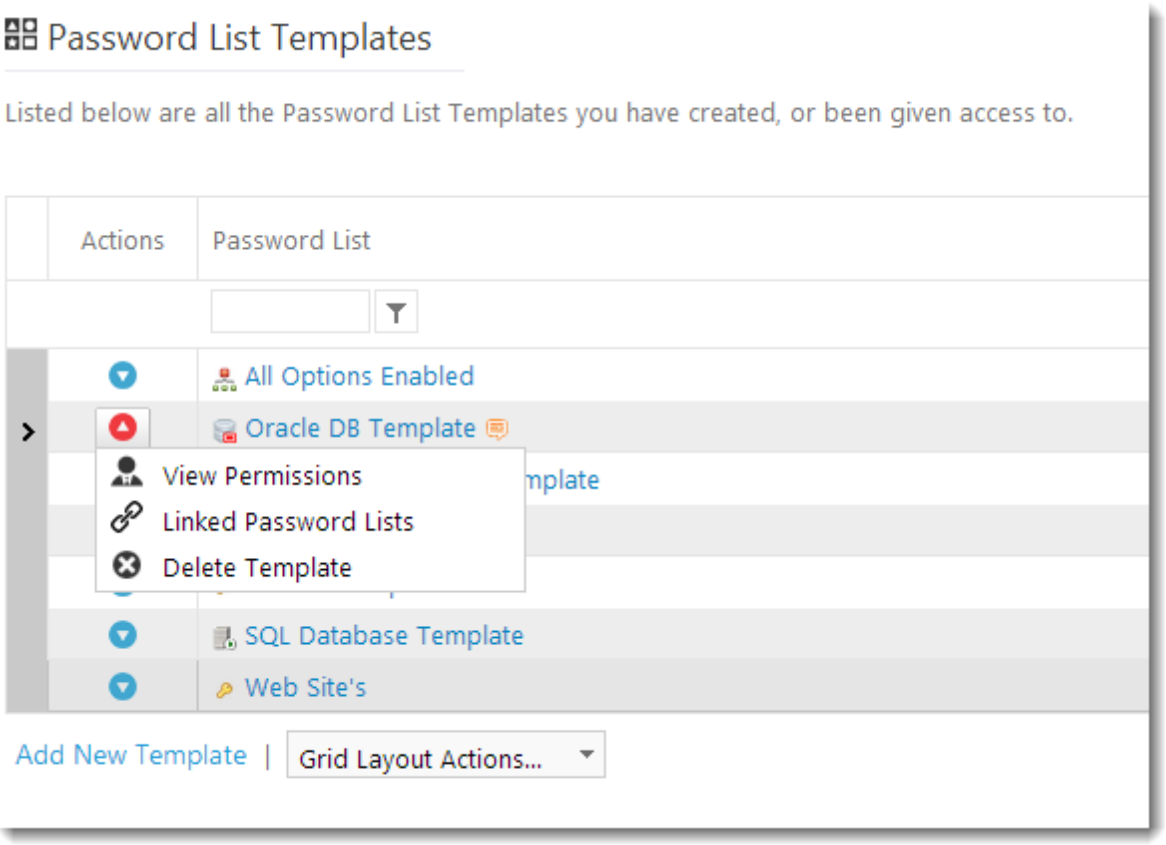
Caution: When editing a Template's settings when it is linked to other Password Lists, if you change any of the Field Types for any Generic Fields, these fields will have their data cleared/ blanked in the database when you click on the 'Save' button. This is because the different Generic Field Field 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

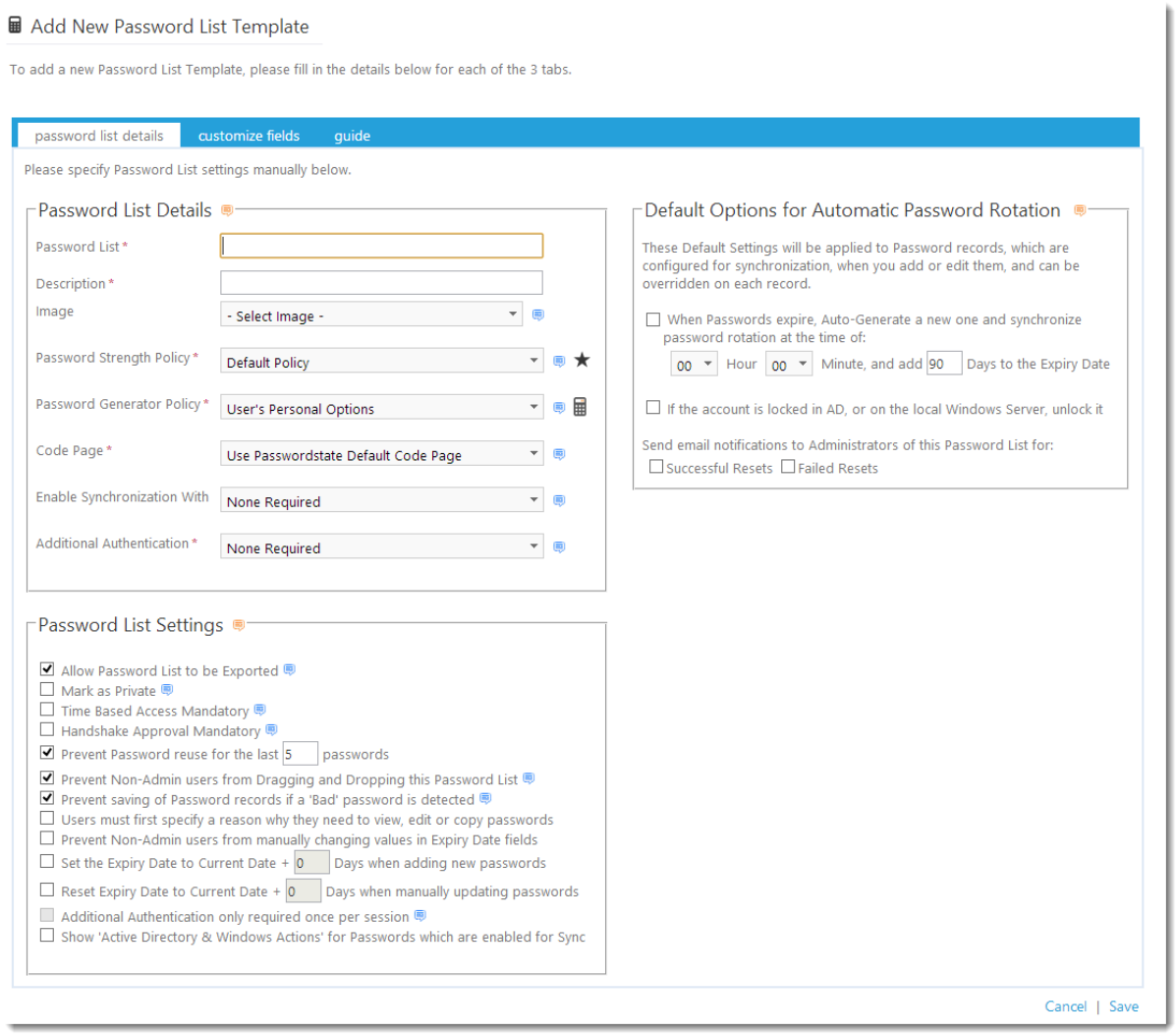
Note: If you delete a Template which is linked to one or more Password Lists, these Password Lists will bet set to use the Templates' settings as there were prior to you deleting the Template. You can then go ahead and modify the settings of the Password Lists as required.



2.7.1 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.

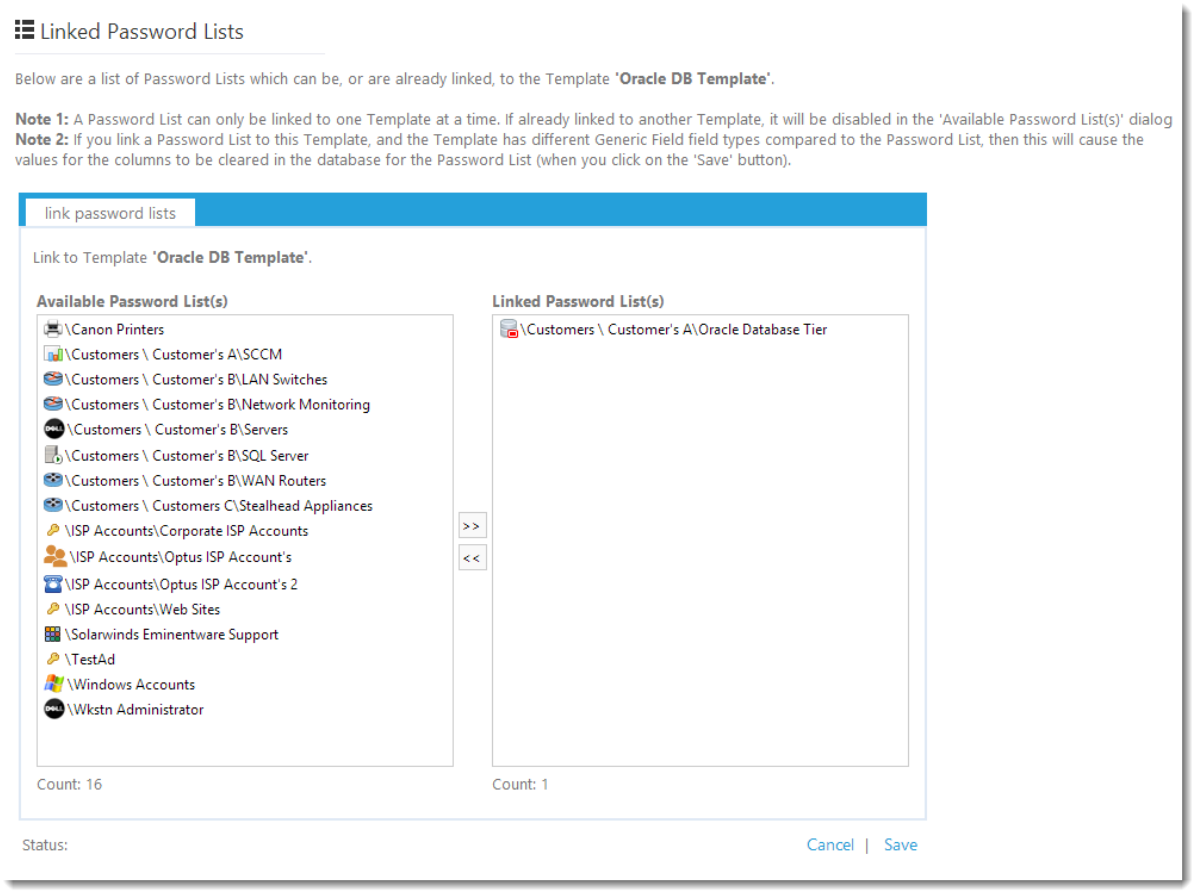


2.7.2 Linked Password Lists

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.

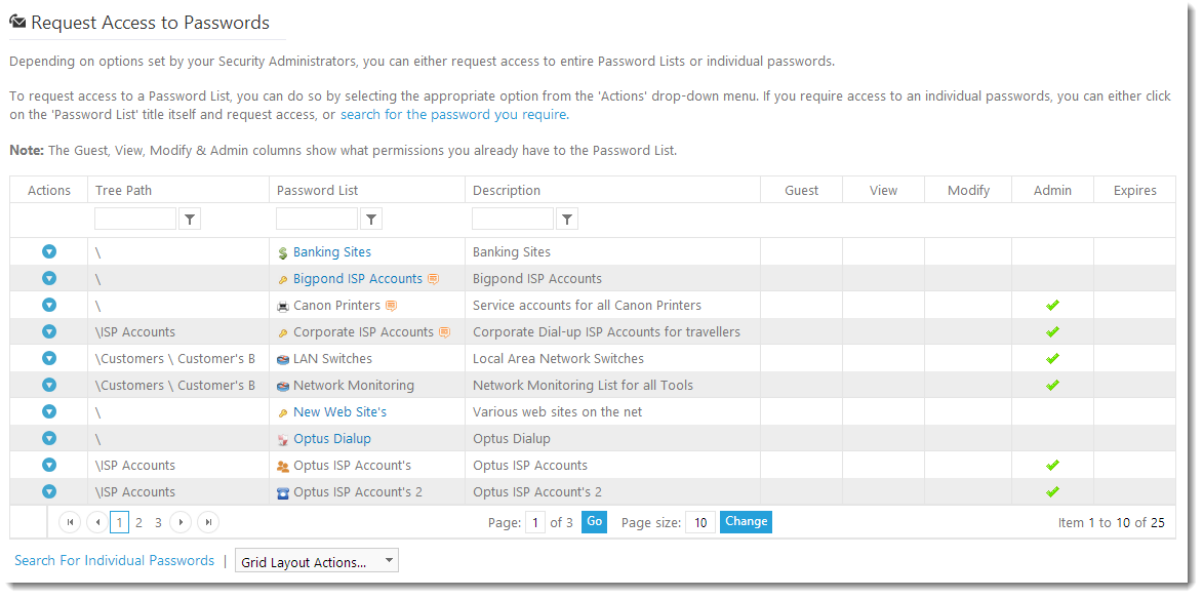
Caution: When linking Password Lists to a Template for the first time, if the Password List has some Generic Fields specified which are different to any Generic Fields specified for the Template, these fields will have their data cleared/blanked in the database when you click on the 'Save' button. This 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.



2.8 Request Access to Passwords

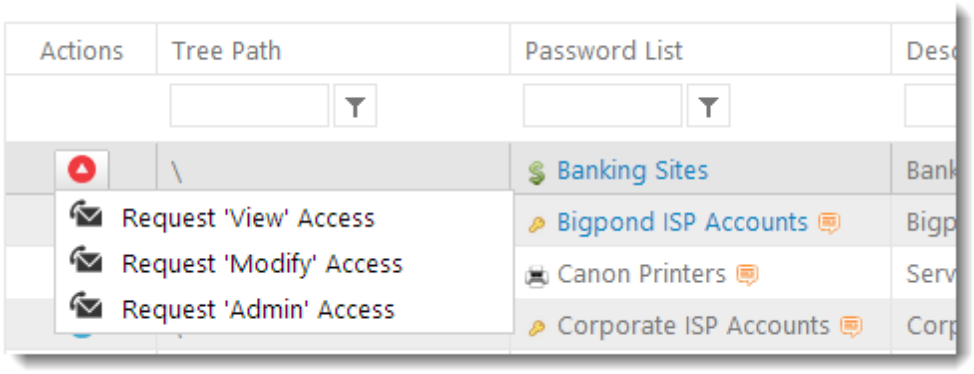
It is possible to request access to a Password List, or individual Password records, if you do not already have access. When requesting access, the email request will be routed to the 'Administrators' of the Password List you are requesting access to - the Administrators will also receive popup reminders when they visit the Passwordstate web site, in case an email is not delivered or is deleted.

The 'Request Access to Passwords' screen shows all the Shared Password List, and what access you already have - if any. From here you can request access to a Password List, or individual Password records.

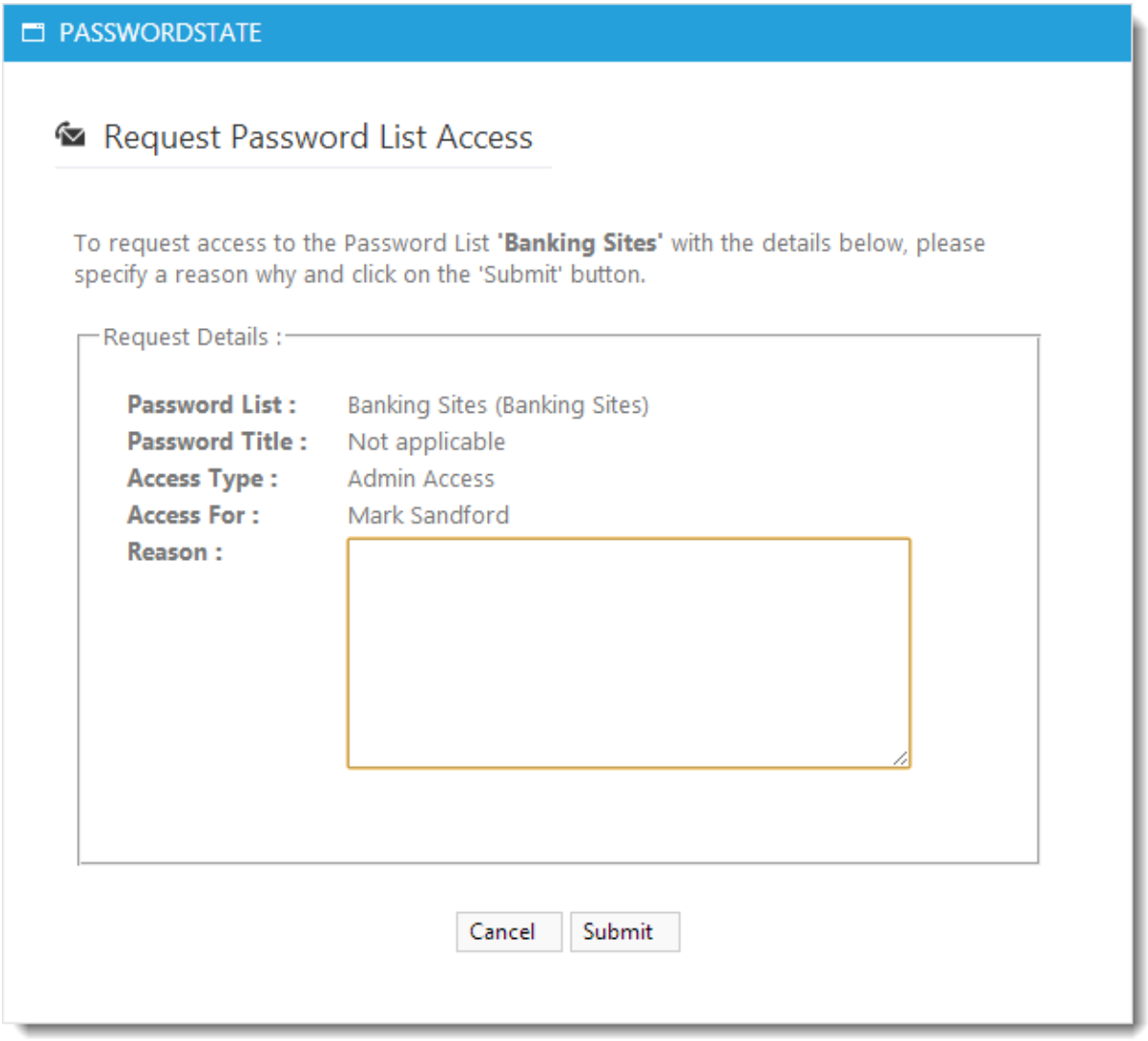


Request Access to a Password List

You can request access to a Password List by selecting the appropriate level of access from the 'Actions' drop-down menu.



You will then be presented with a popup window where you can specify a reason as to why you require access. When you click the 'Submit' button, the request will be routed to the Administrator(s) of the Password List.



Request Access to Individual Password Records

You can request access to individual Password records in a similar fashion to Password Lists, and can be accessed via:

- Clicking on the 'Password List' hyperlink in the Grid, and then accessing via the 'Actions' drop-down menu for the appropriate record
- Or, by clicking on the 'Search for Individual Passwords' button at the bottom of the screen

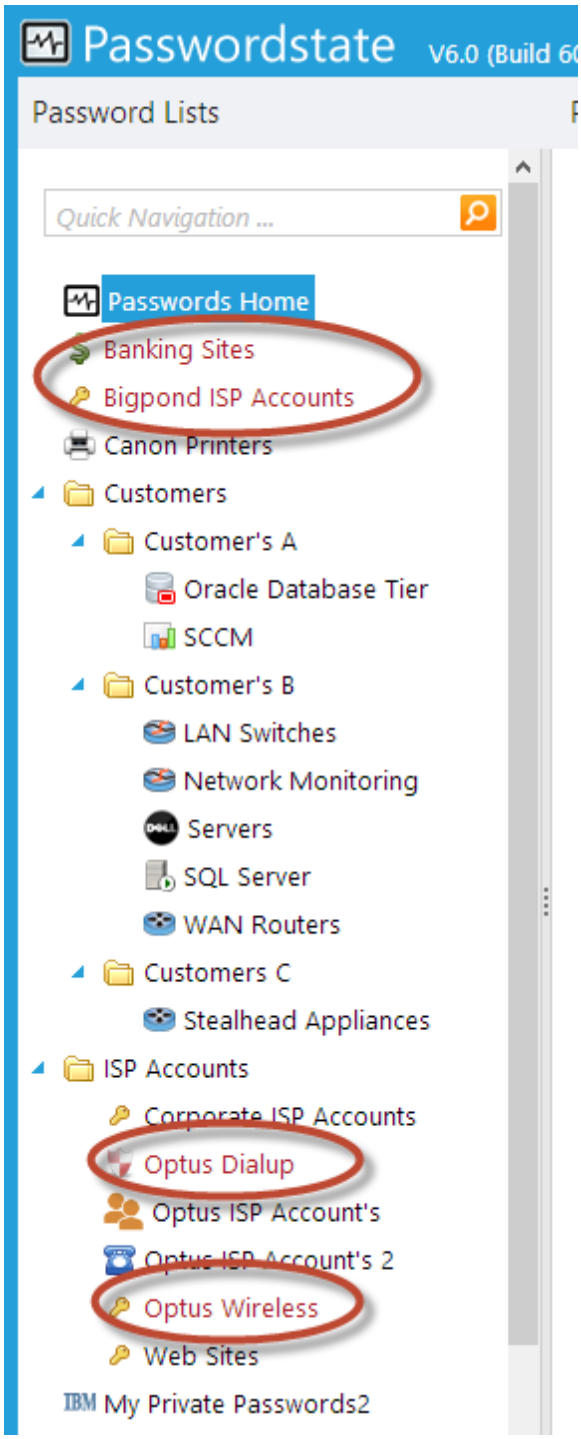
2.9 Toggle All Password List Visibility

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 -> System Settings screen.



3 Generator Menu

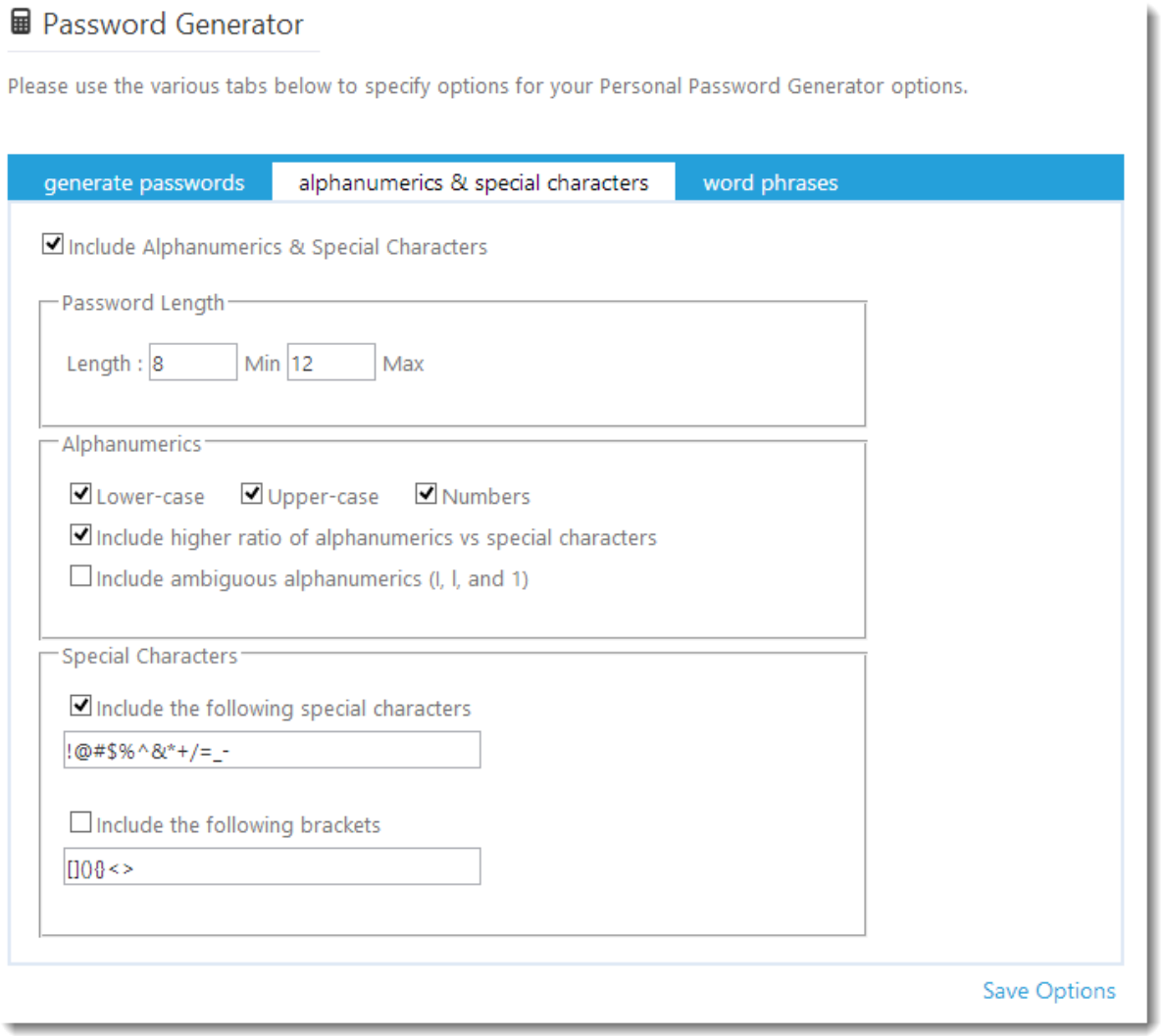
The Generator menu is where you can access your personal settings for the Password Generator built into Passwordstate, and also allows you to generate any number of random passwords with your personal settings.

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

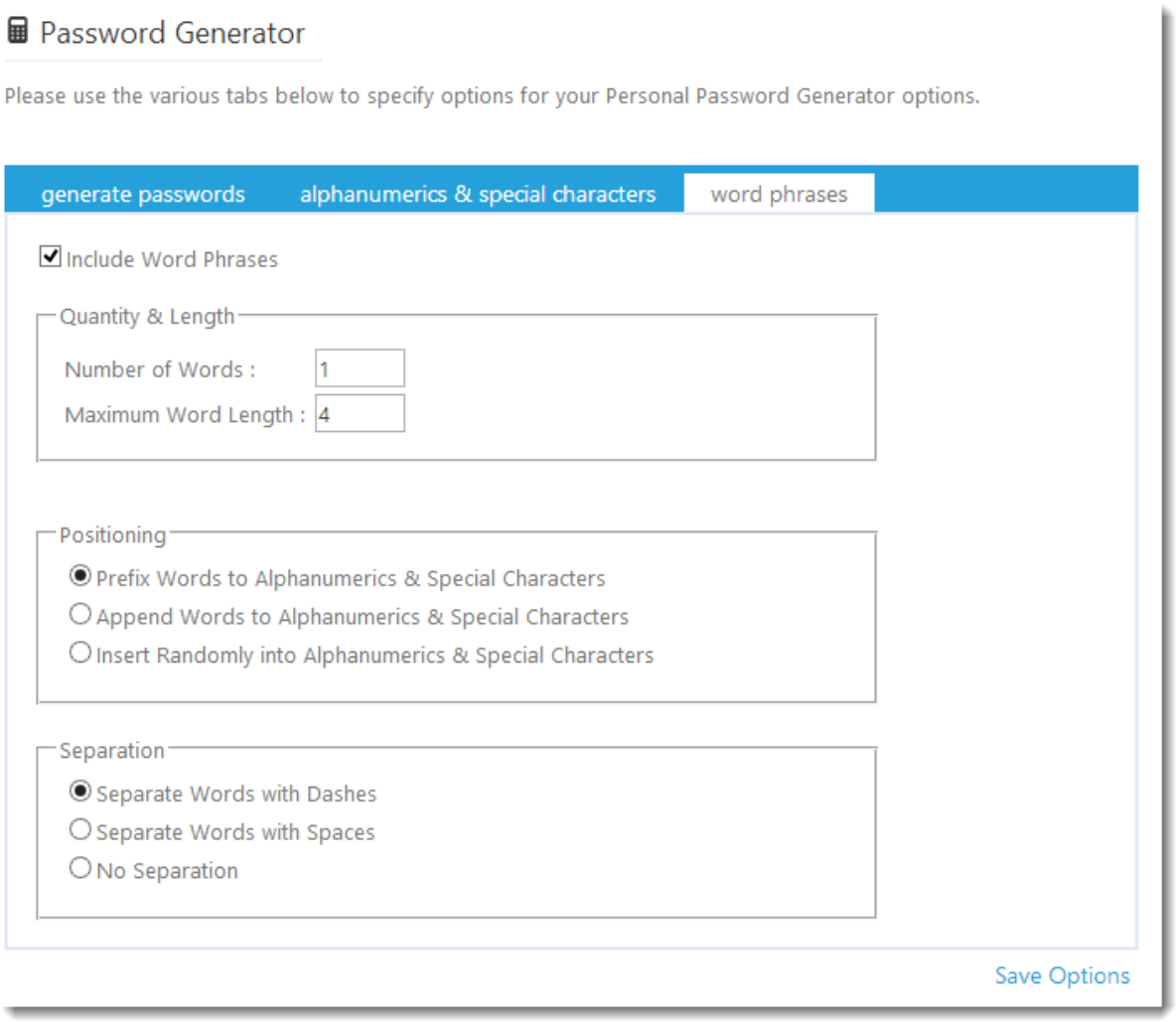
The Alphanumeric & Special Characters tab allows you to specify the desired length of the password you wish to generate, as well as settings for letters, numbers, special characters and various forms of brackets.



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.

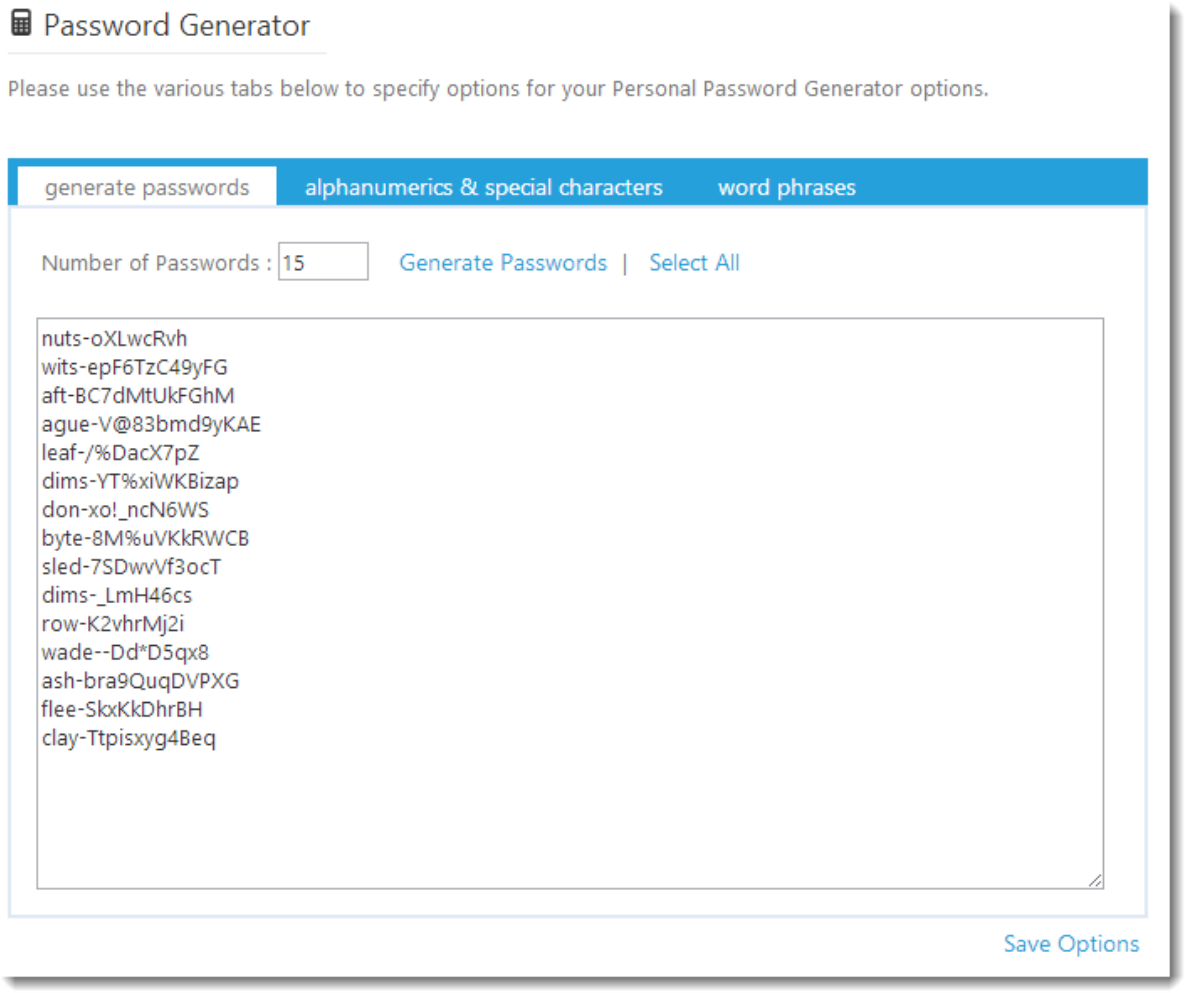


Generate Passwords

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

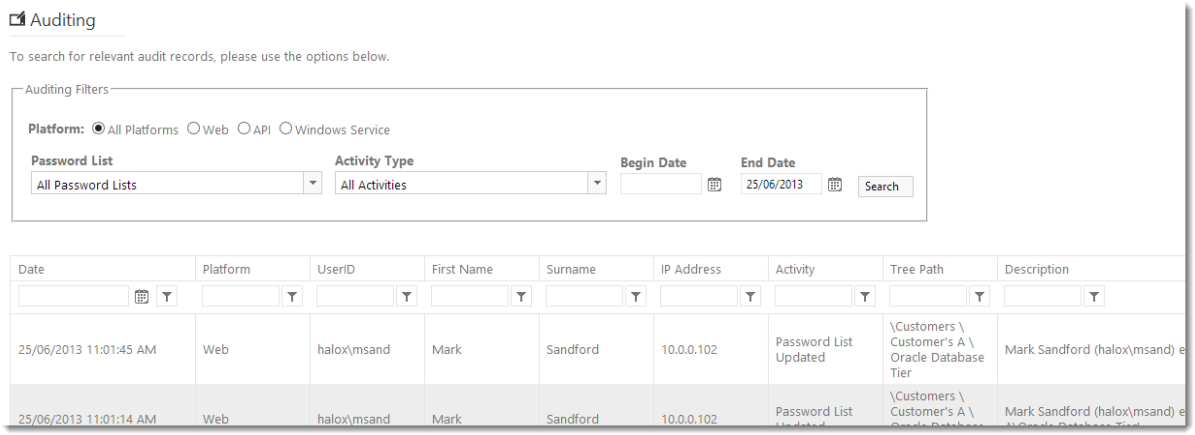
settings for future use.



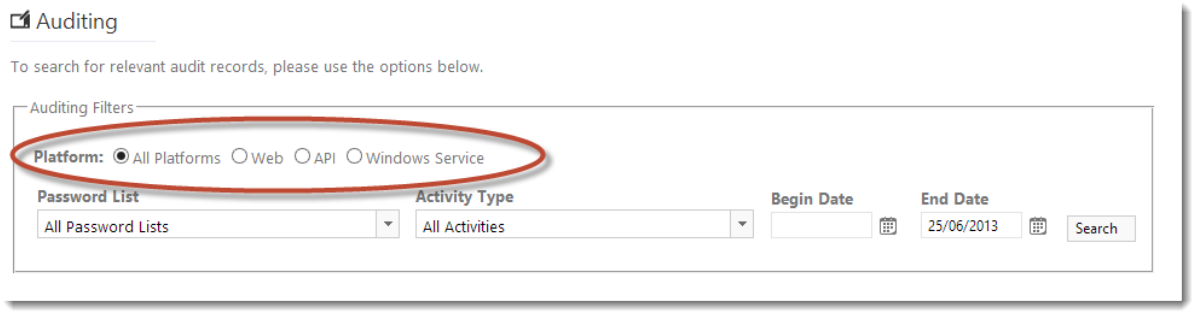
4 Auditing Menu

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.

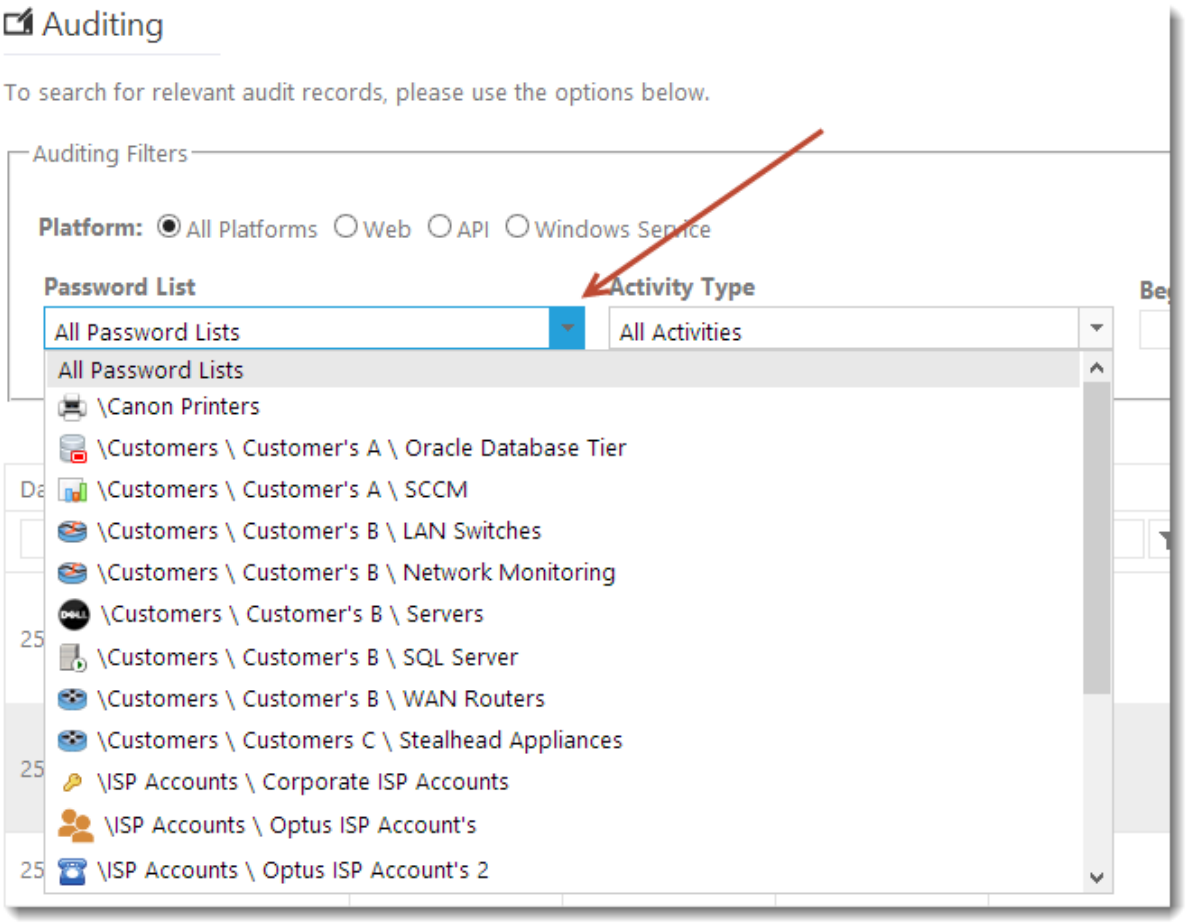
Additional auditing data is also available to Security Administrators of Passwordstate, and can be found on the screen Administration -> Auditing. The additional auditing data relates to certain activities like login failures, user account related, etc.



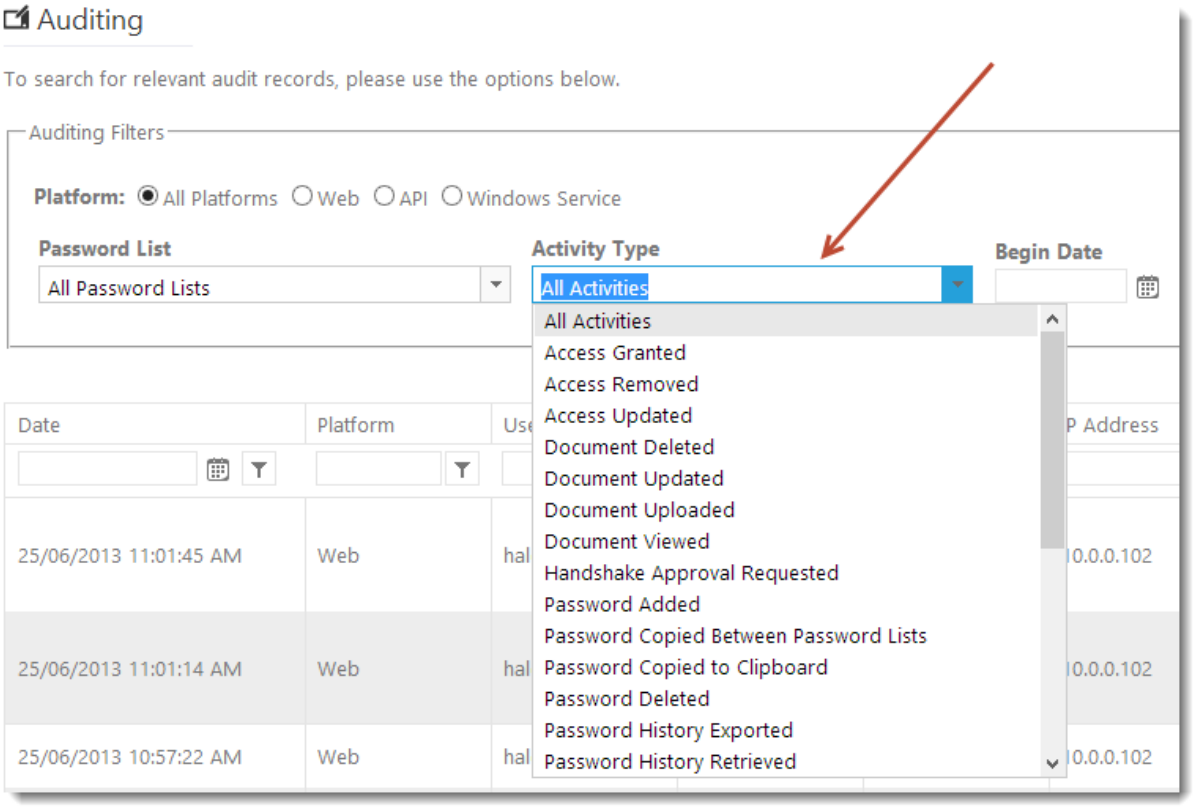
Filter by Platform



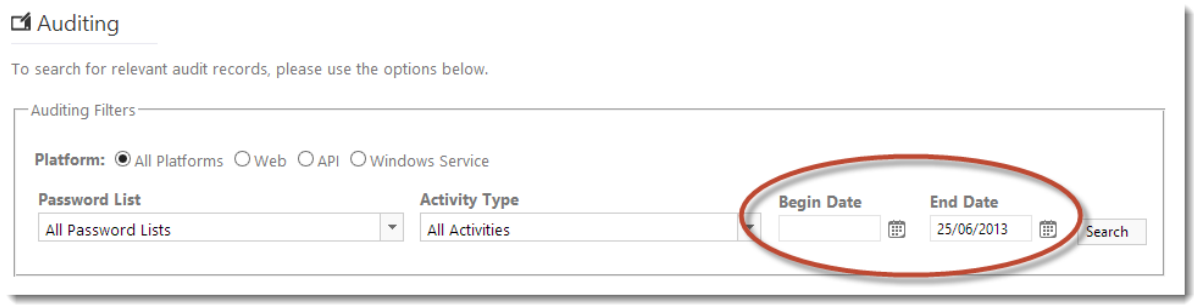
Filter by Specific Password Lists



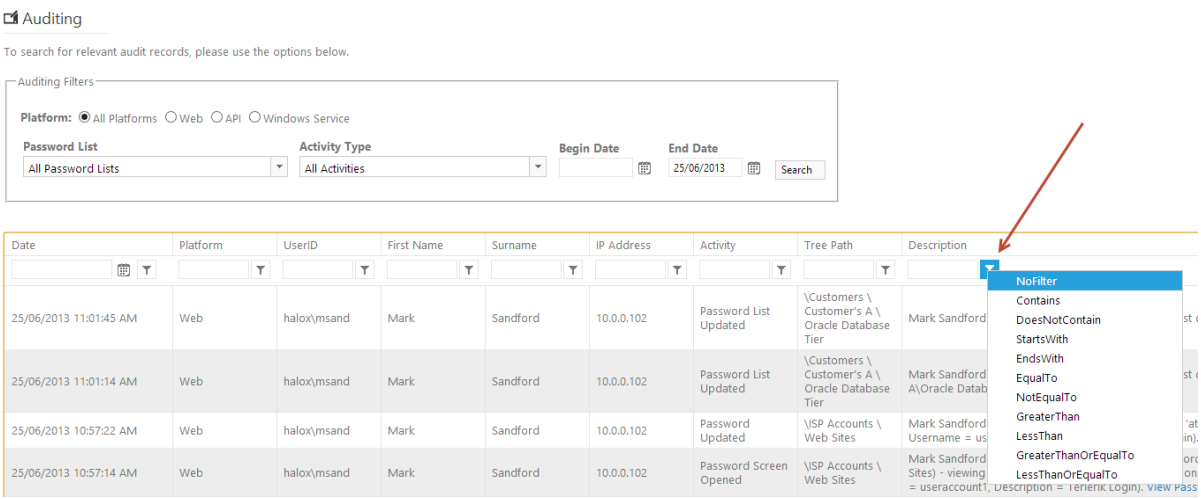
Filter by Specific Activity Type



Filter between Specific Dates



Further Filter by Search Results Contents



5 Preferences Menu

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

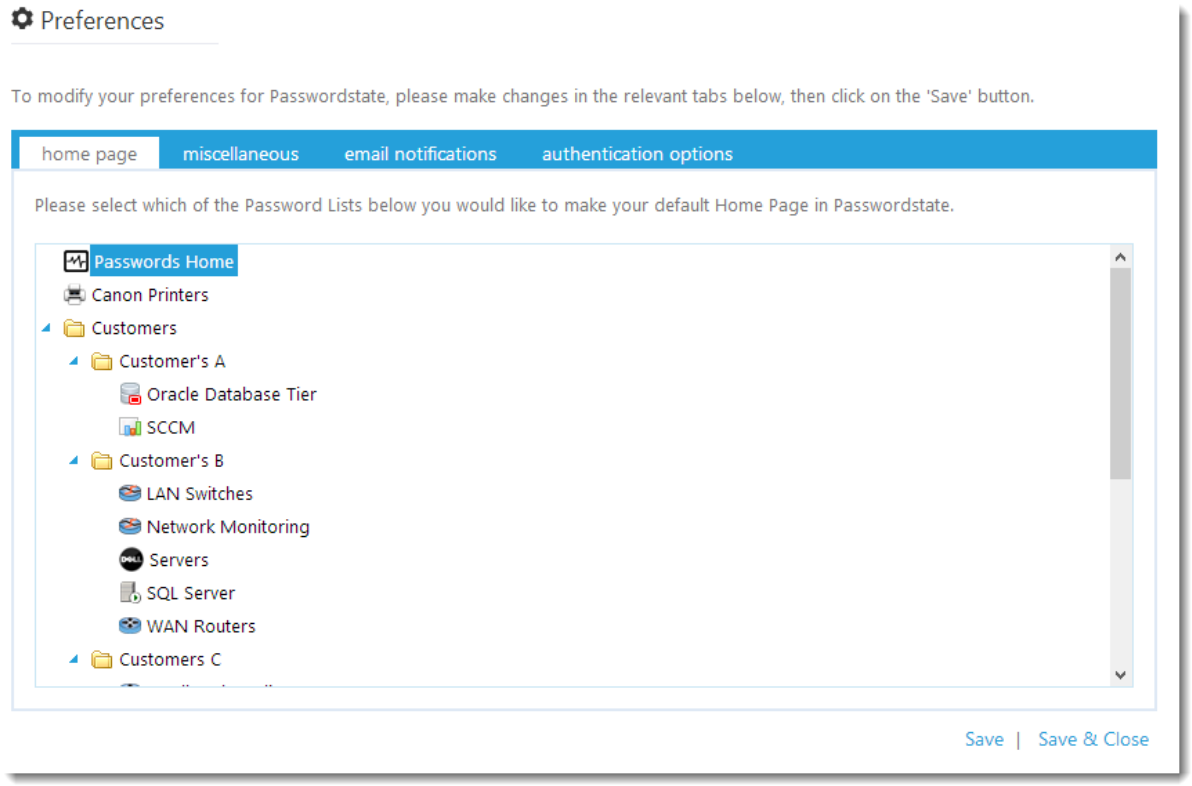
Note: The Security Administrators of Passwordstate can use a feature called 'User Account Policies', which may override any settings you specify here. If a User Account Policy is applied to your account, certain settings on the Preferences screen will be disabled.

The Preferences screen has the following 4 tabs:

Home Page Tab	Allows you to specify which Password List of Folder will first be presented to you when you navigate to the Passwordstate web site
Miscellaneous Tab	A collection of different settings specific for your account
Email Notifications Tab	Allows you to enabled/disabled one or more of the many different email notifications Passwordstate can send you, as well as different report options
Authentication Options Tab	Specify which authentication method you wish to use when first accessing the Passwordstate web site

5.1 Home Page Tab

The Home Page Tab simply lets you select which Password List or Folder you would like displayed for you when you first navigate to the Passwordstate web site.

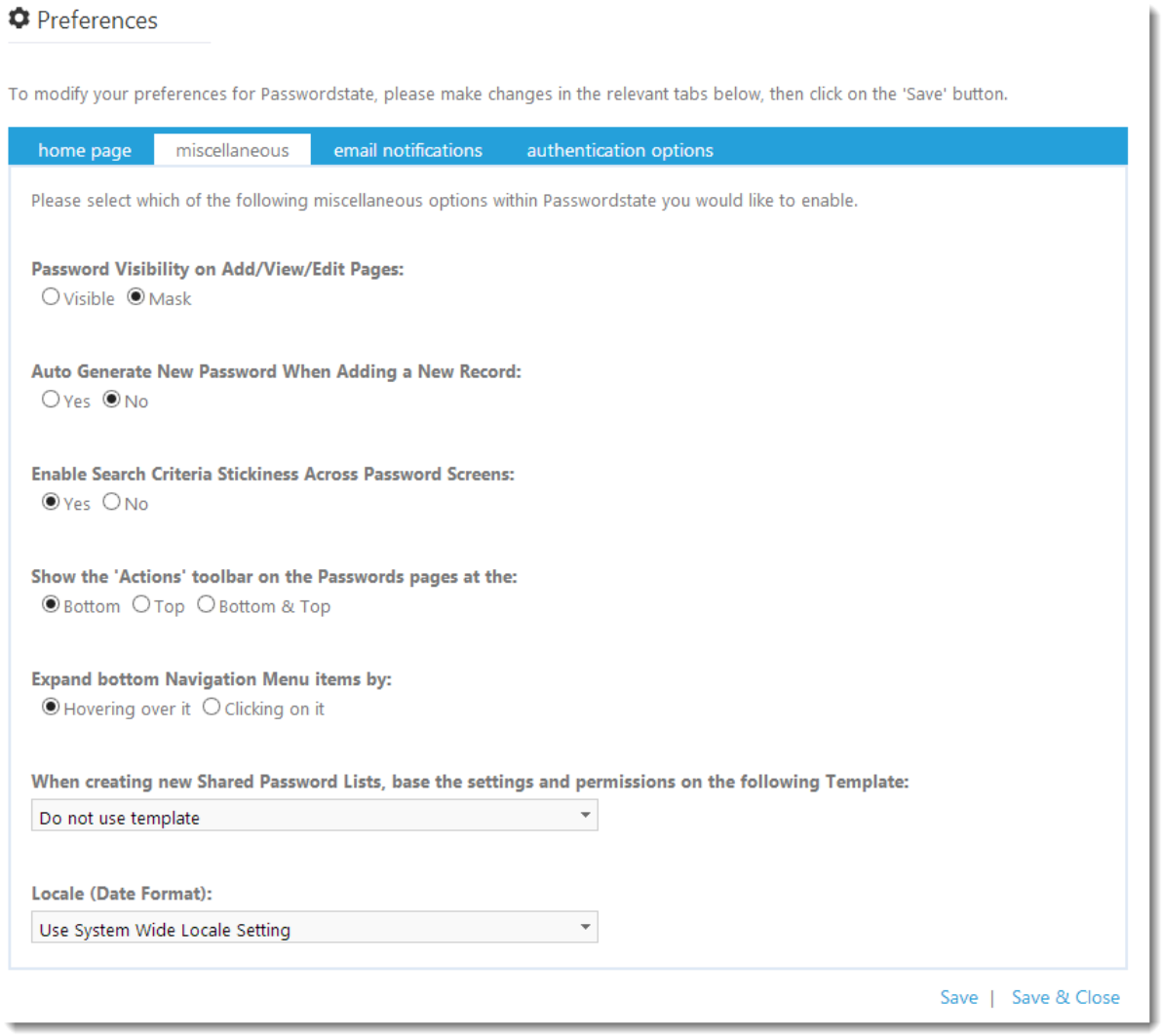


5.2 Miscellaneous Tab

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
Expand bottom Navigation Menu items by	The Navigation Menu at the bottom of the screen can expand certain menus vertically by simply hovering over them. If you choose, you can change this option so you must first click on the Menu item before it expands
When creating new Shared Password Lists, base the settings and permissions on the following Template	When creating new Password Lists, you can choose to automatically specify all the settings based on one of the Templates you select here
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

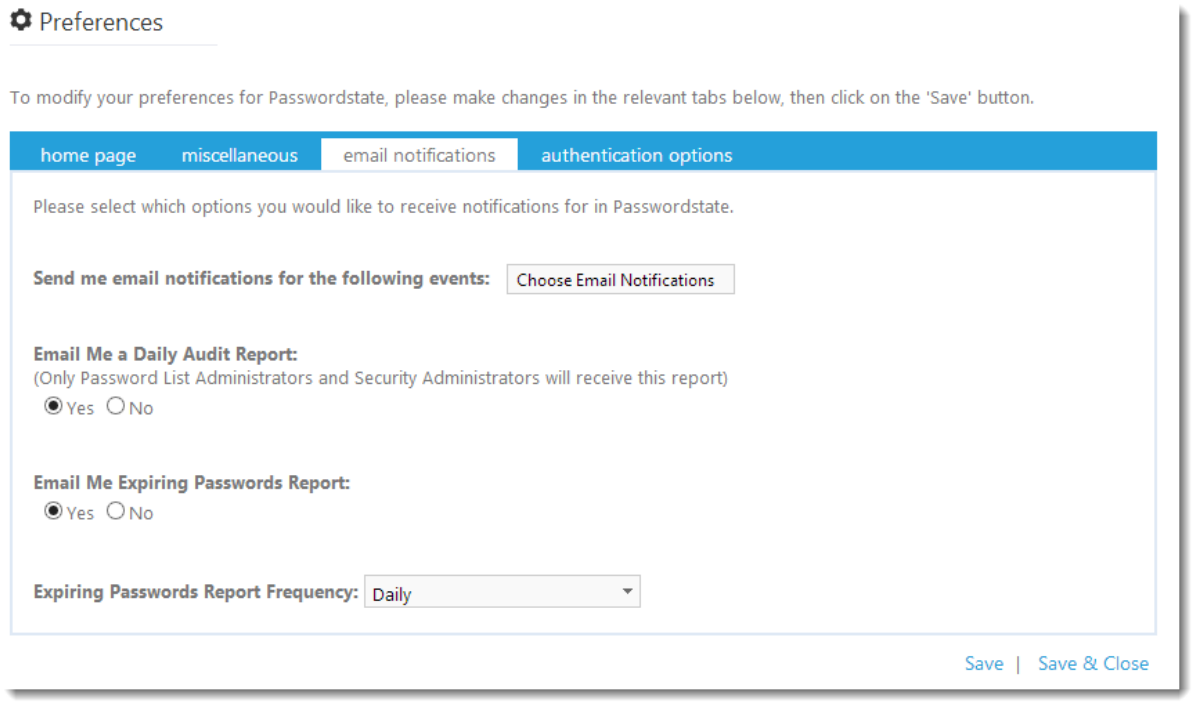


5.3 Email Notifications Tab

The Email Notifications Tab allows you to enabled/disabled one or more of the many different email notifications Passwordstate can send you, as well as different report options.

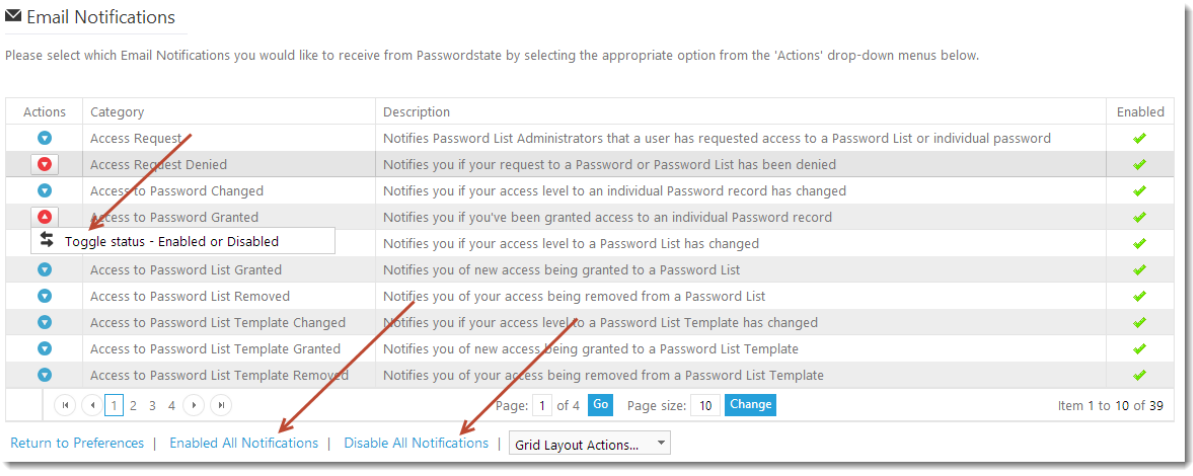
Note: There is a feature called 'Email Notification Groups' which your Security Administrators of Passwordstate can use, and using this feature for your account will cause the 'Choose Email Notifications' button below to be disabled

Note: 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.



Reports

There are also certain reports available to you, which can be emailed at different intervals:

- Daily Audit Report - an email summarizing all activity for Password List you are an Administrator

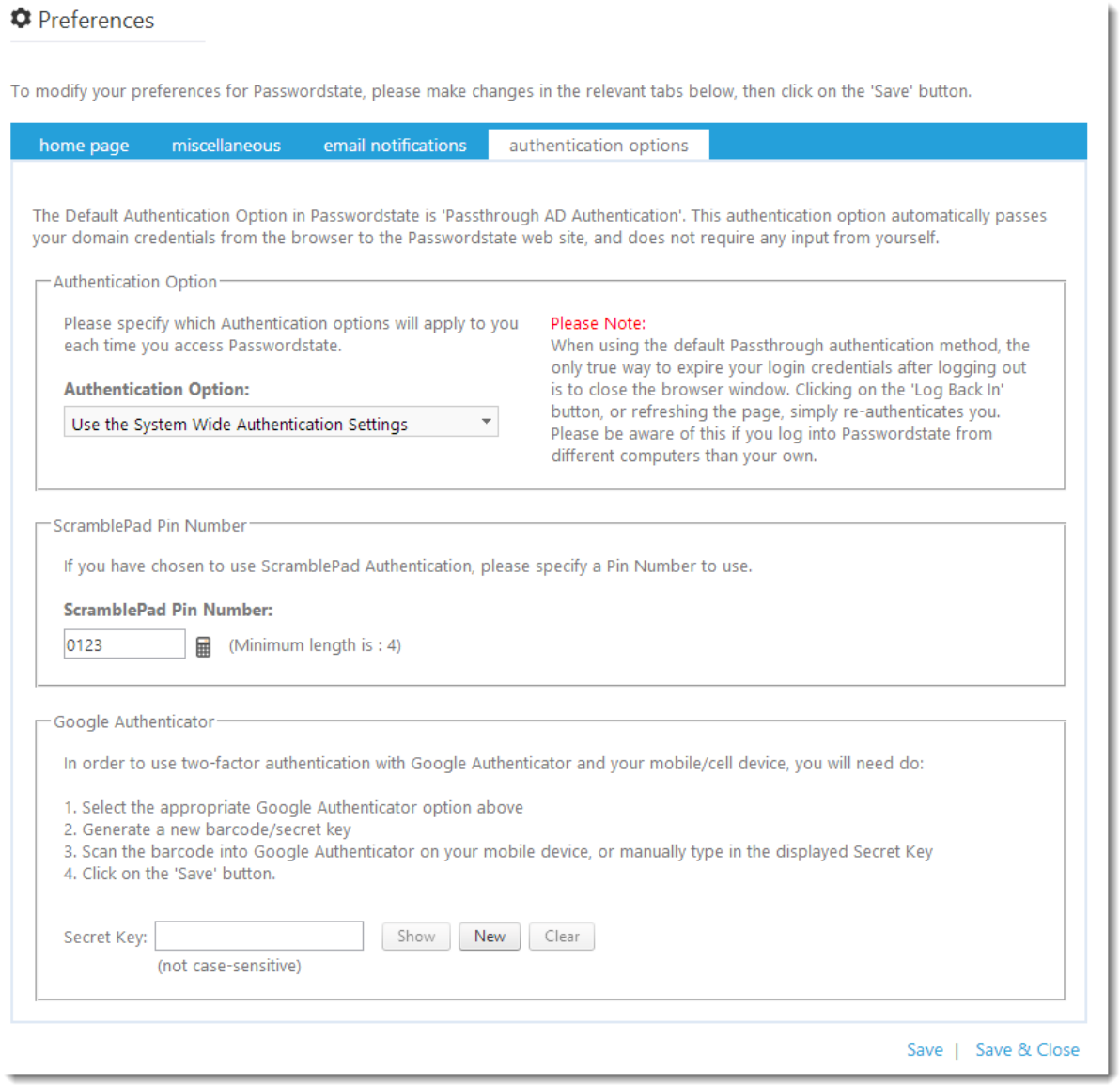
of

- Expiring Passwords Report - a report which shows which Passwords have already expired, or are going to expire within the next 30 days. The report can be sent daily, weekly and monthly, and only applies to Password Lists you have access to

5.4 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

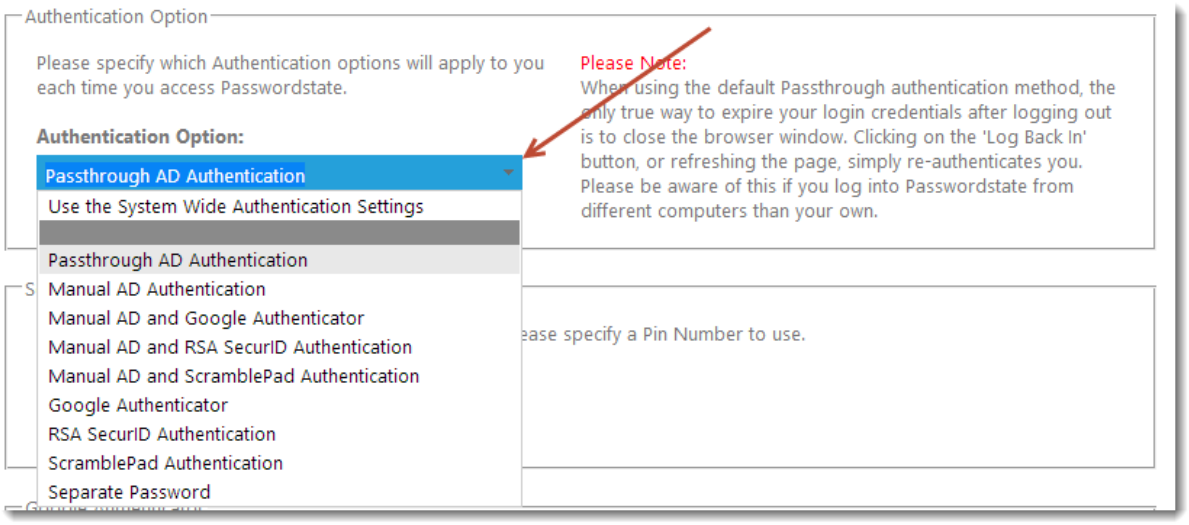
There are multiple authentication options available to you, and they will vary depending on if your are using the Active Directory authentication version of Passwordstate, or the Forms-Based authentication version. The following screen shows the options available when using AD integrated authentication. If using Forms Authentication, none of the 'AD' options will be visible.

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
Passthrough AD Authentication	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
Manual AD 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 AD and Google Authenticator	In additional to manually specifying your AD username and Password, just must also specify a valid Google Verification Code for your Google Authenticator application - see instructions below for this
Manual AD and RSA SecurID	In additional to manually specifying your AD username and Password, just must also specify a valid SecurID Passcode. Your Security Administrators must first follow the provided instructions to prepare Passwordstate for SecurID authentication
Manual AD 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
Google Authenticator	Google Authenticator with Passthrough AD Authentication
RSA SecurID Authentication	RSA SecurID Authentication with Passthrough AD Authentication

ScramblePad Authentication	ScramblePad Authentication with Passthrough AD Authentication
Separate Password	A completely separate password, used in conjunction with Passthrough AD Authentication

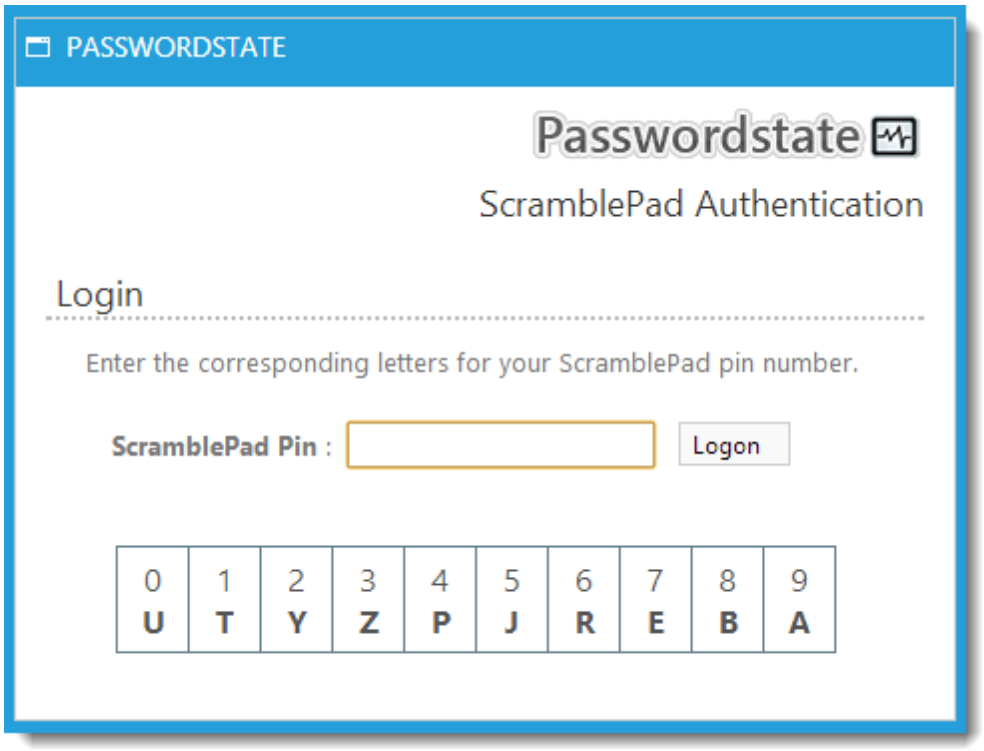
Note: If required, your Security Administrators can reset your Preferences settings, so there is no chance you can permanently lock yourself out of Passwordstate



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.

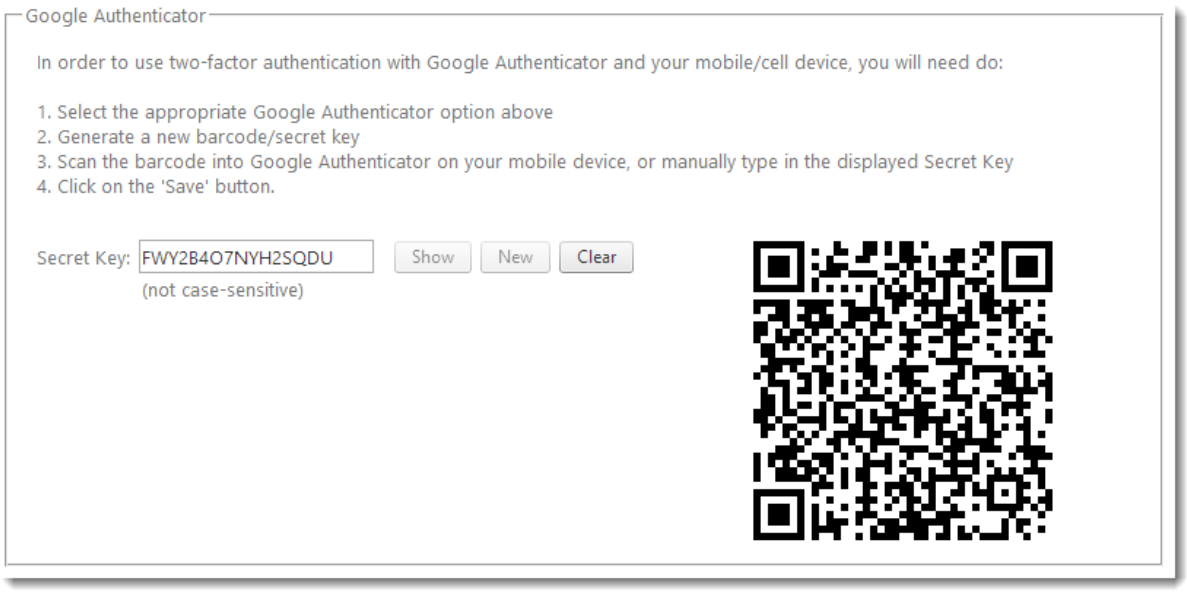
You must match your in number digits, to the randomly generated letters. i.e. If your Pin Number is **1234**, you would need to type **tyzp** to authenticate.



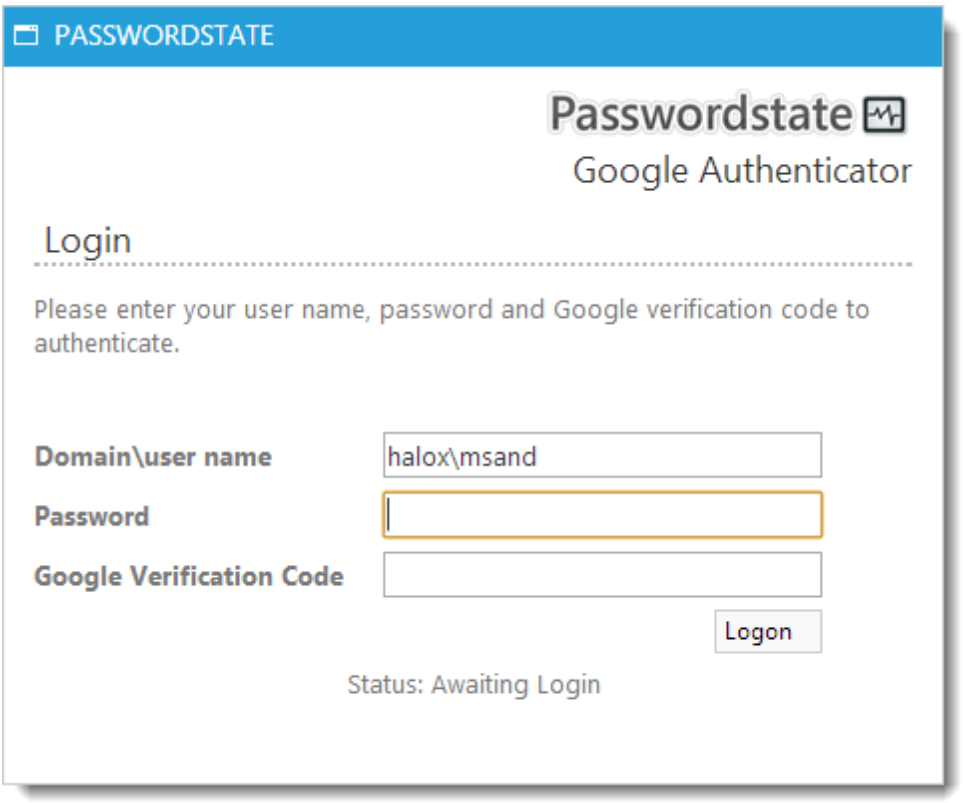
Google Authenticator

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.

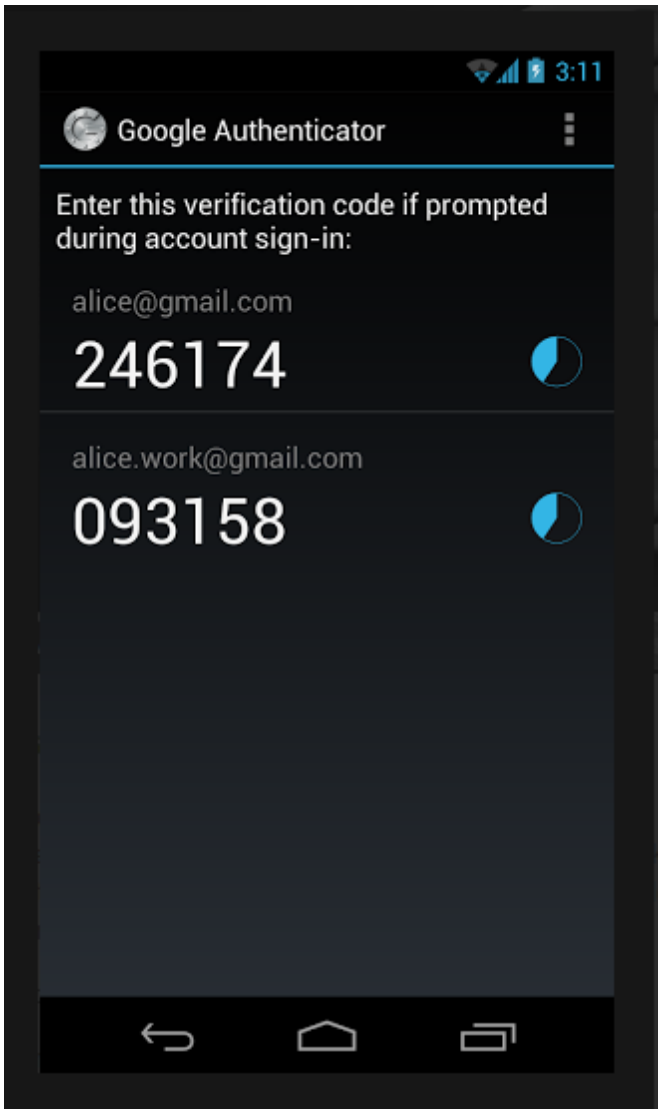


Once you have successfully enabled Google Authenticator with Passwordstate and on your mobile/cell device, then you will be presented with the following login screen next time you visit Passwordstate (this is the screen for 'Manual AD and Google Authenticator').



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.



6 Administration Menu

In order to see the Administration Menu you must be granted one or more of the 15 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.

7 Help Menu

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

1. User Manual (this help file you are referencing now)
2. Guided Tour of Passwordstate - this will show a popup window guiding you through some of the basic functions
3. Security Administrators Manual
4. Web API Documentation

Note: The Security Administrators Manual and Web API Documentation links may be disabled for you by the Security Administrators of Passwordstate.

8 KB Articles

The following is a list of KB Articles for enabling or using certain features in Passwordstate.

Some of the articles show or describe features found in the 'Administration' area of Passwordstate, and if your account is not configured as a 'Security Administrator', you may not have access to these screens.

Synchronize Passwords with Active Directory on Windows Servers
Restoring from an Automatic Backup
How to Clone Folders and Password Lists
Specifying Your Own Custom Fields
Multiple Options for Hiding Passwords
Controlling Settings for Multiple User Accounts

8.1 Synchronize Passwords with Active Directory or Windows Servers

It's possible to synchronize password changes with Active Directory, or with Windows Servers for any local accounts.

In order to perform this synchronization, there's a few permissions and settings which first need to be considered.

Specify Account with Permissions to make Password Changes

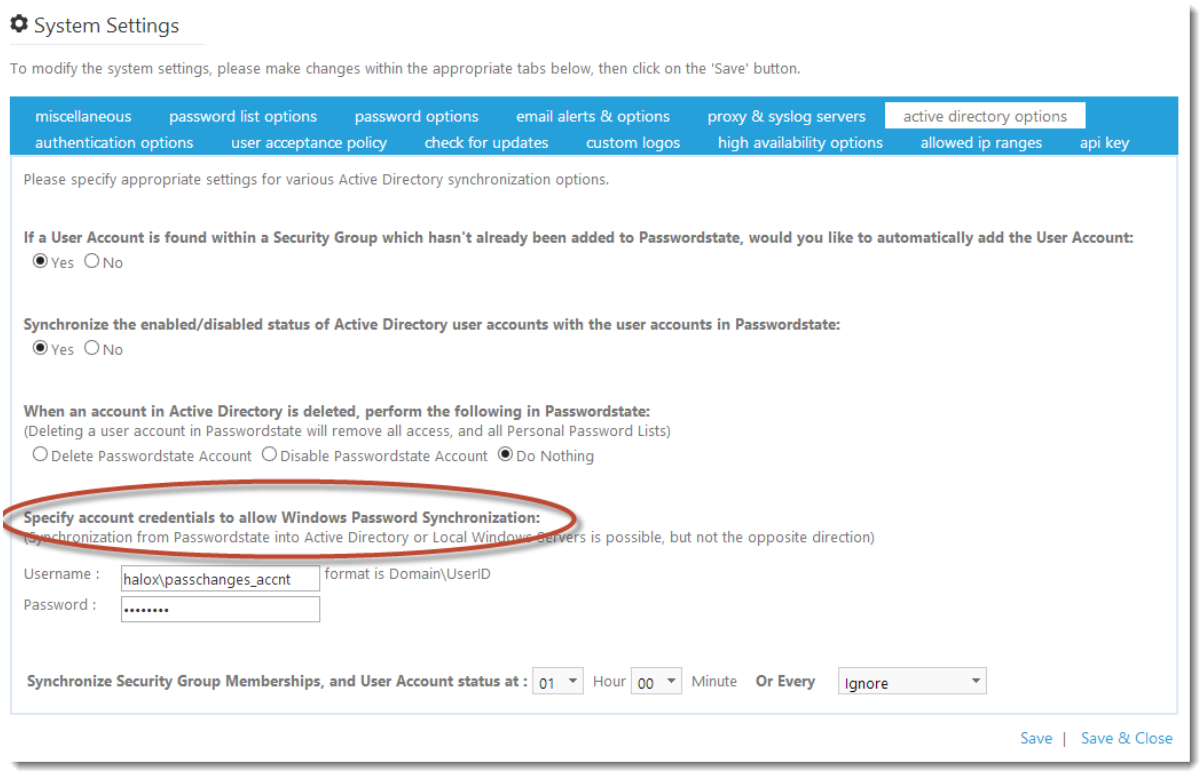
On the screen Administration -> System Settings -> Active Directory Options tab, you can specify an account which will be used to perform the synchronization. This account must have the following minimum permissions:

- Account Operator if changing passwords on the domain (if you need to change passwords for accounts which have Domain Admin rights, then the account you specify here will also need

Domain Admin rights)

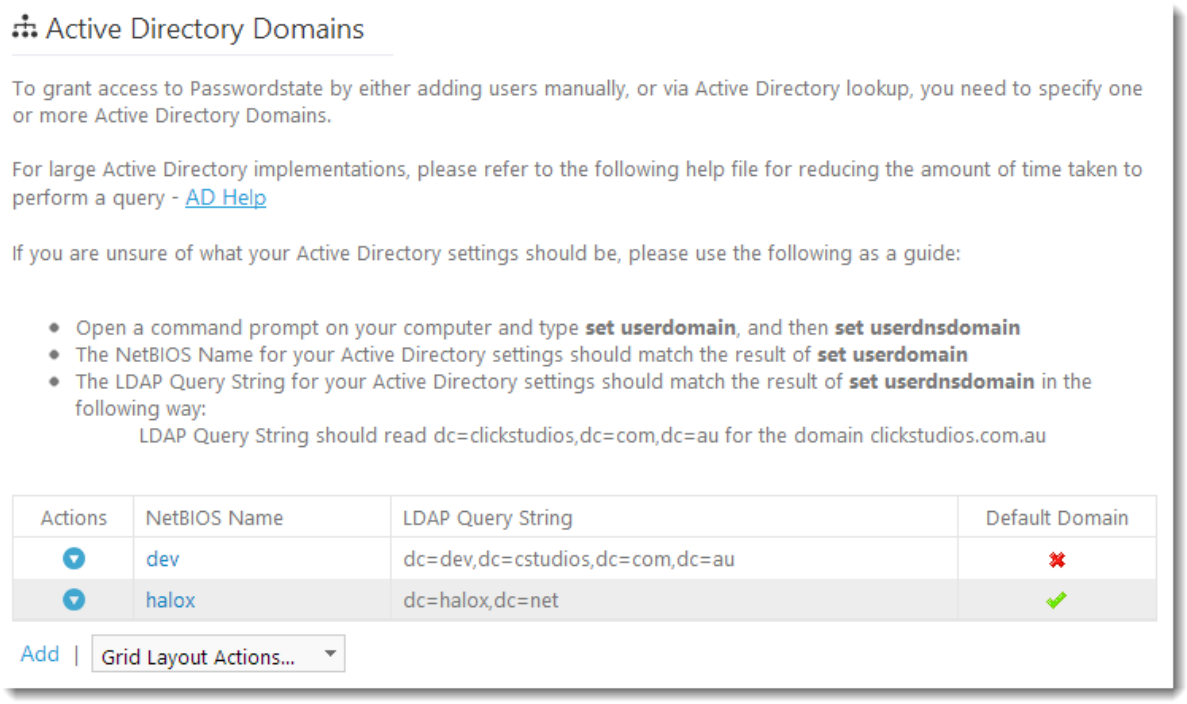
- Local Administrator's group or Local Administrator account if changing passwords for local accounts on Windows Servers

Note: If you change the domain account used here, or modify the permissions for this account i.e. add to a new security group, then it is recommended you restart the Passwordstate Windows Service.



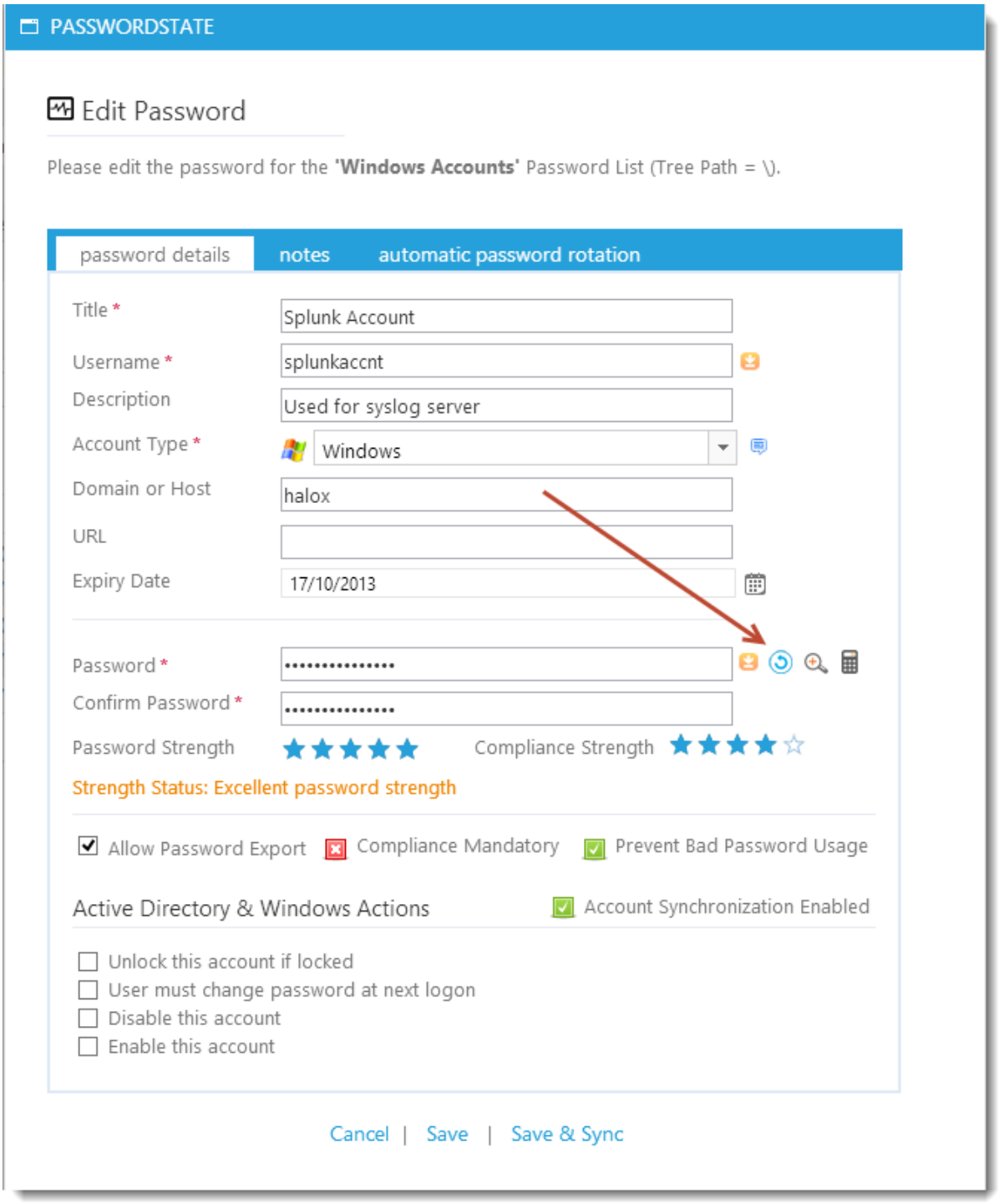
Add Appropriate Domains to the Active Directory Domains Screen

By default, you should already have one Active Directory Domain added to the screen Administration -> Active Directory Domains. If you want to synchronize password changes with other domains which aren't listed, then you must add them to this screen.



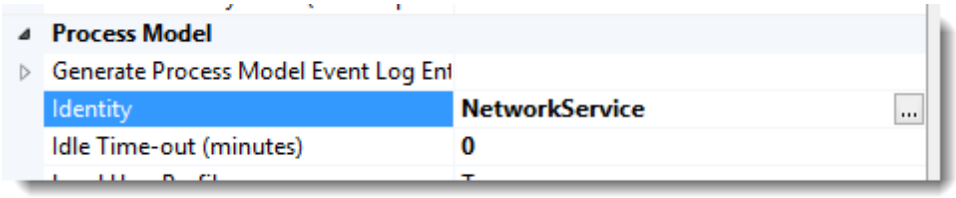
Specify Account with Permissions to Read Active Directory Account Data

When you open the Edit Password screen, the icon can be used to validate the password stored in Passwordstate matches what's stored in Active Directory, or on the Windows Server.

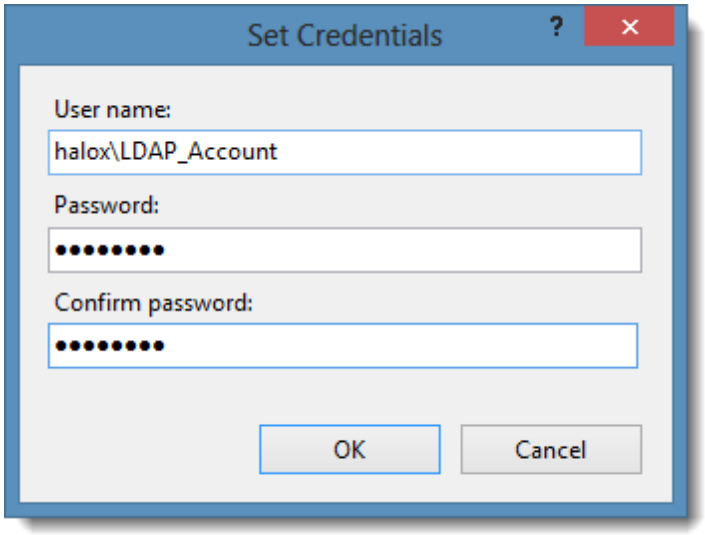


The account used to verify this, plus in other areas of Passwordstate where you can synchronize and look up User Accounts and Security Groups, is configured as part of the Passwordstate Application Pool in Internet Information Services. By default, the Application Pool is configured to use the **'NetworkService'** account, but depending upon any restrictions place on your Active Directory domain, this account may not have sufficient privileges to query Active Directory. If this is the case, you can modify the identity used, and specify a different domain account with

sufficient privileges.



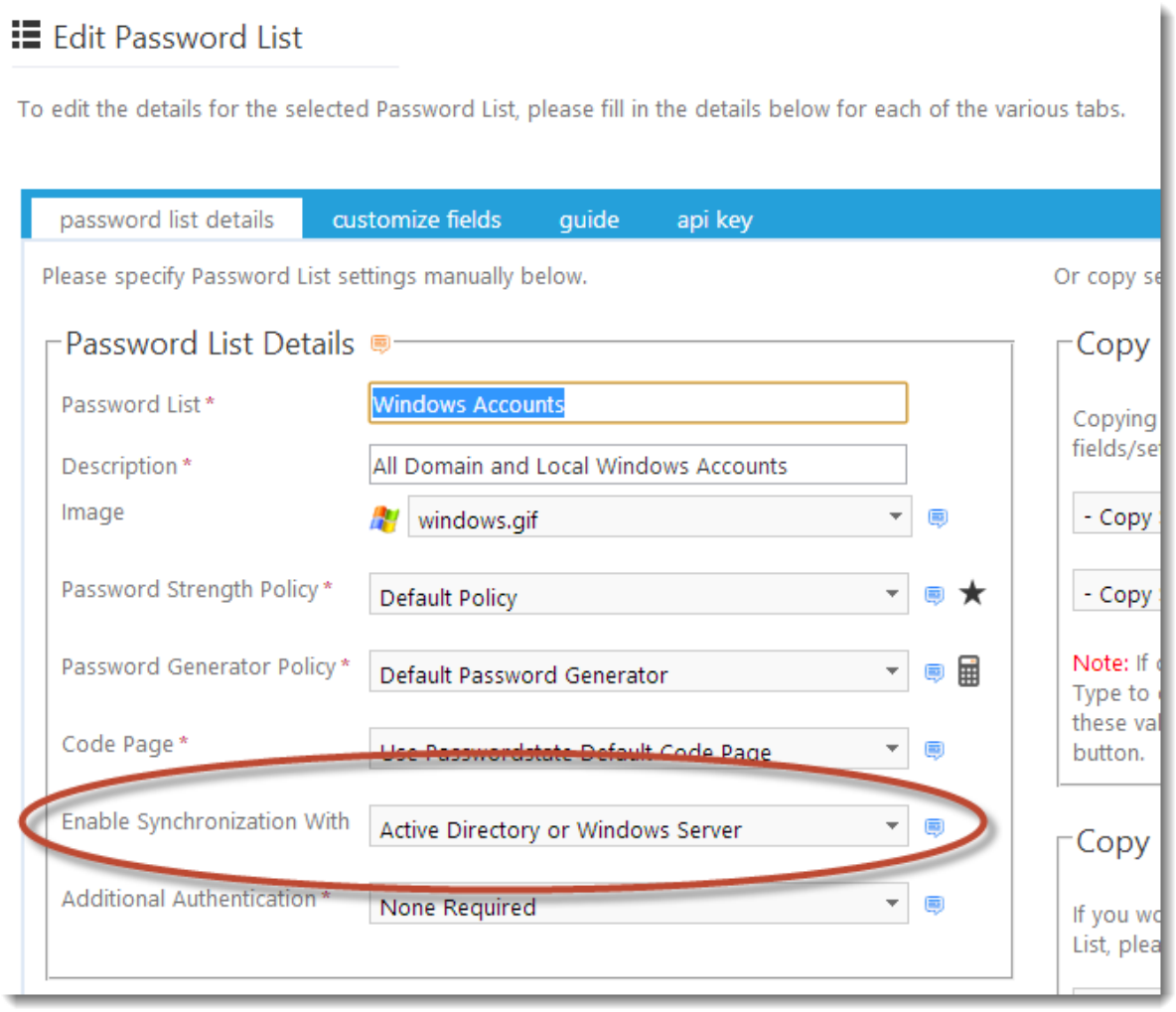
Instead of the **NetworkService** account, specify a different domain account:



Configure a Password List for Synchronization

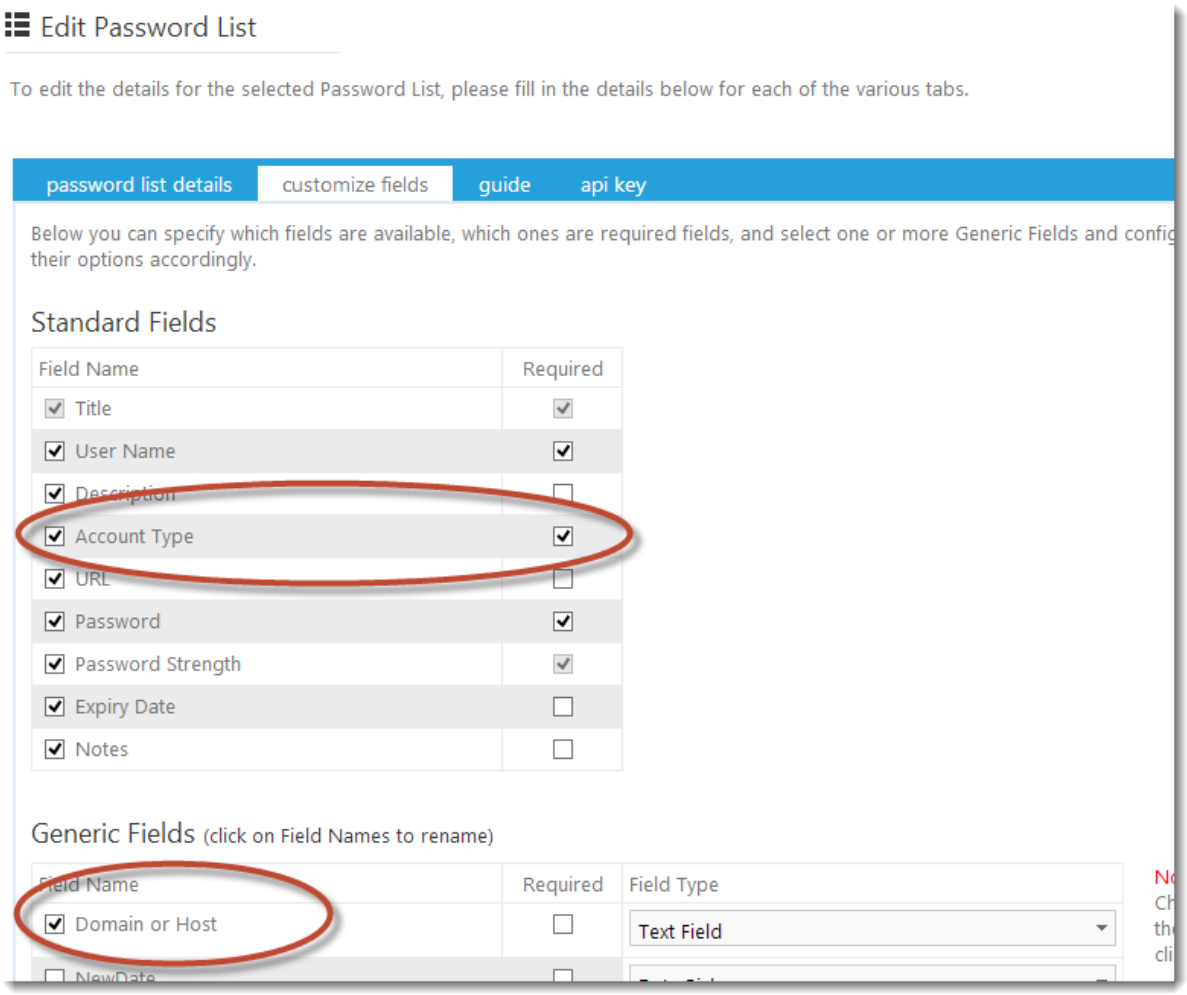
Now that all the permissions should be correct, we need to configure a Password List so that it is enabled for synchronization. To do this you need to:

Select the option **Active Directory or Windows Server** from the **Enable Synchronization With** drop-down list.



And this will make the following changes on the **Customize Fields** tab:

- Select the **Account Type** field
- Select one Generic Field and name it **Domain or Host**



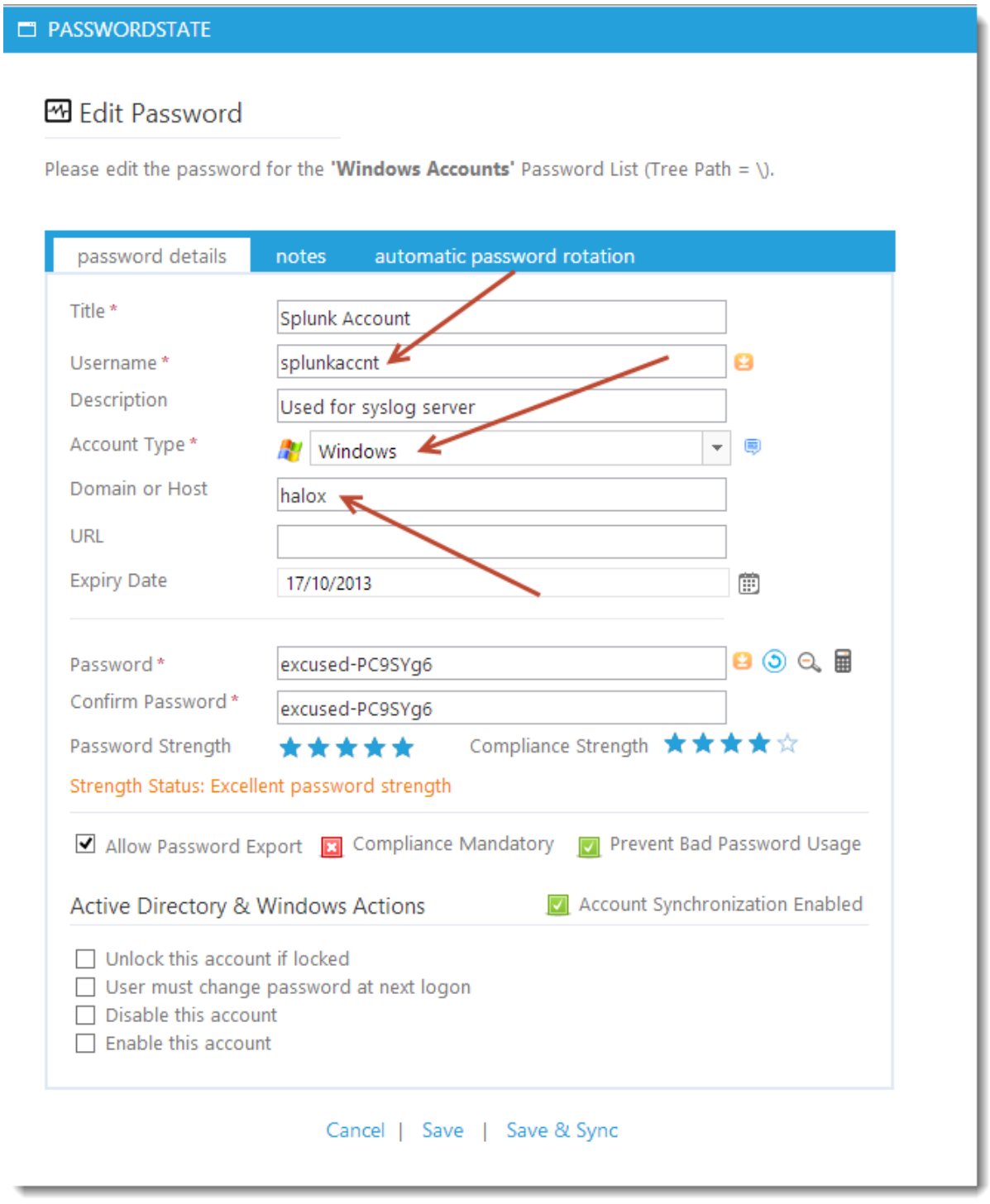
Configure a Password for Synchronization

The last thing required for configuring a password for synchronization is:

- Specify the **Username** of the account
- Select 'Windows' as the **Account Type**
- Specify either the NetBIOS name of the Domain Account you are synchronizing, or the Host Name of the Windows Server you are synchronizing to

Important: If you are wanting to synchronize and Active Directory Account, then it's important the **Domain or Host** value you specify **matches** the domain's **NetBIOS** value you've entered on the screen Administration -> Active Directory Domains. It is this match which determines if we are trying to synchronize an AD account, or not.

Now when you click on the **Save & Sync** button, it will synchronize the password with either Active Directory, or the Windows Server.



8.2 Restoring from an Automatic Backup

This KB article will demonstrate how to restore both the web and database backups as part of the Automatic Backup feature in Passwordstate. The following screens are for SQL Server 2012, and

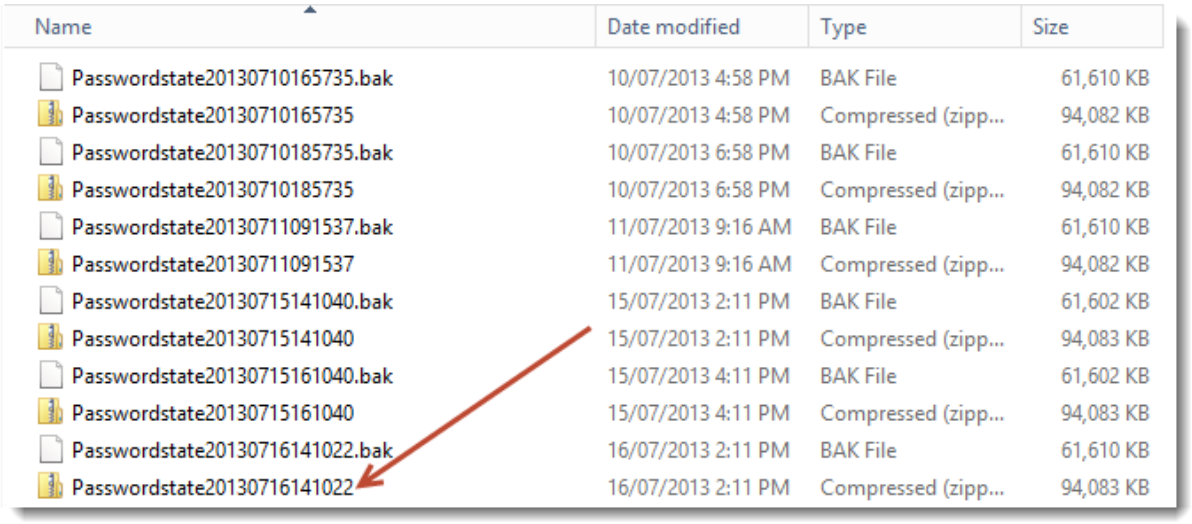
may appear different for other versions of SQL Server.

Restoring the Web Files

Restoring the web files is a 2 step process:

1. Browse to the folder where your backups are stored, and extract the latest Passwordstate<xxxxx>.zip file to the location of where your Passwordstate installation is
2. Ensure the Passwordstate folder, and all nested files/folders have modify permissions for the **Network Service** & **IIS_IUSRS**

Note: If for some reason your Passwordstate installation no longer exists, i.e. you had to rebuild your server, you can perform a fresh install of Passwordstate and then simply restore just the web.config file from the backup zip file - all other data is stored in the database. You can obtain the latest and previous downloads of Passwordstate from http://www.clickstudios.com.au/previous-builds.html

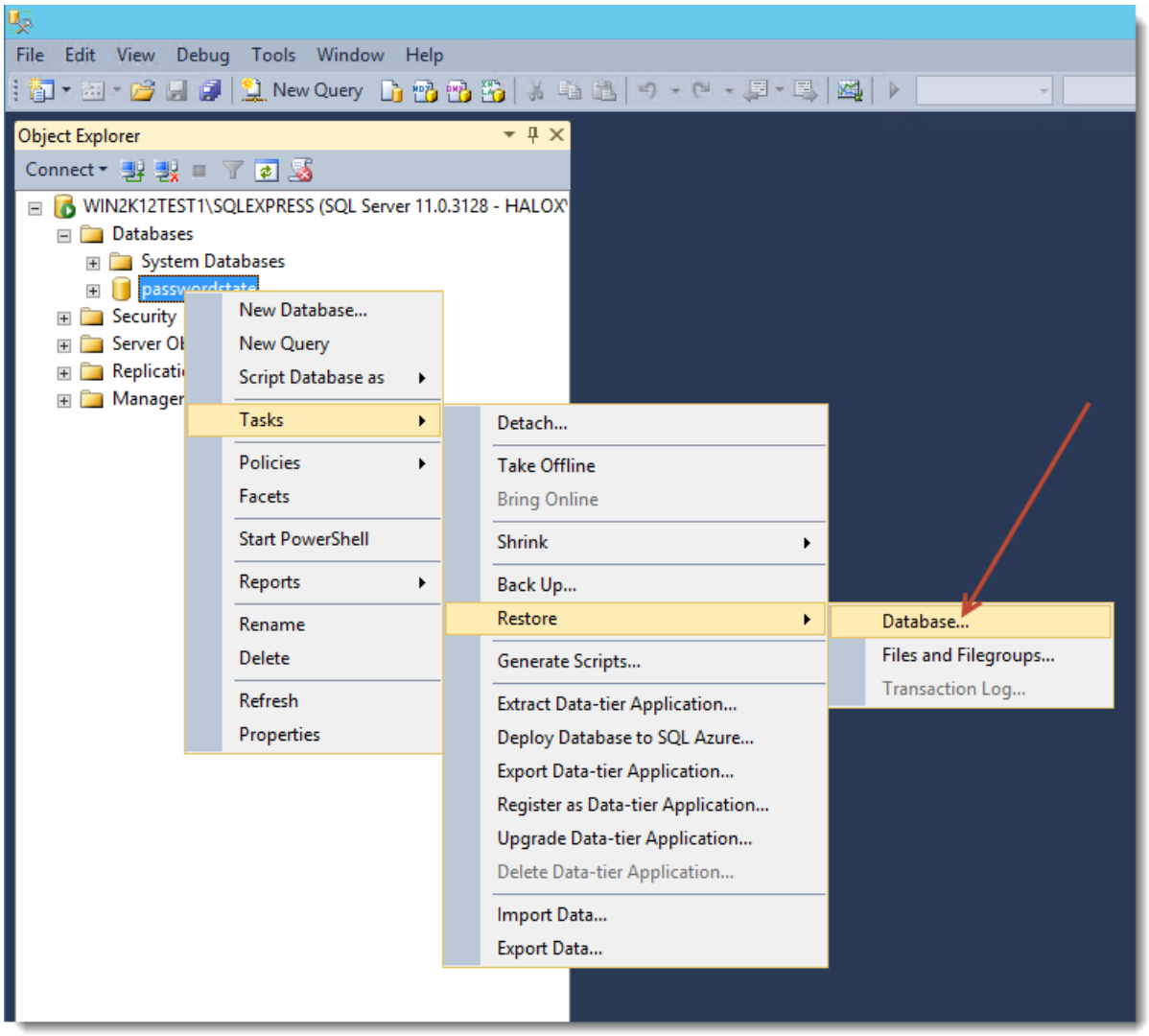


Restoring the Database Backup

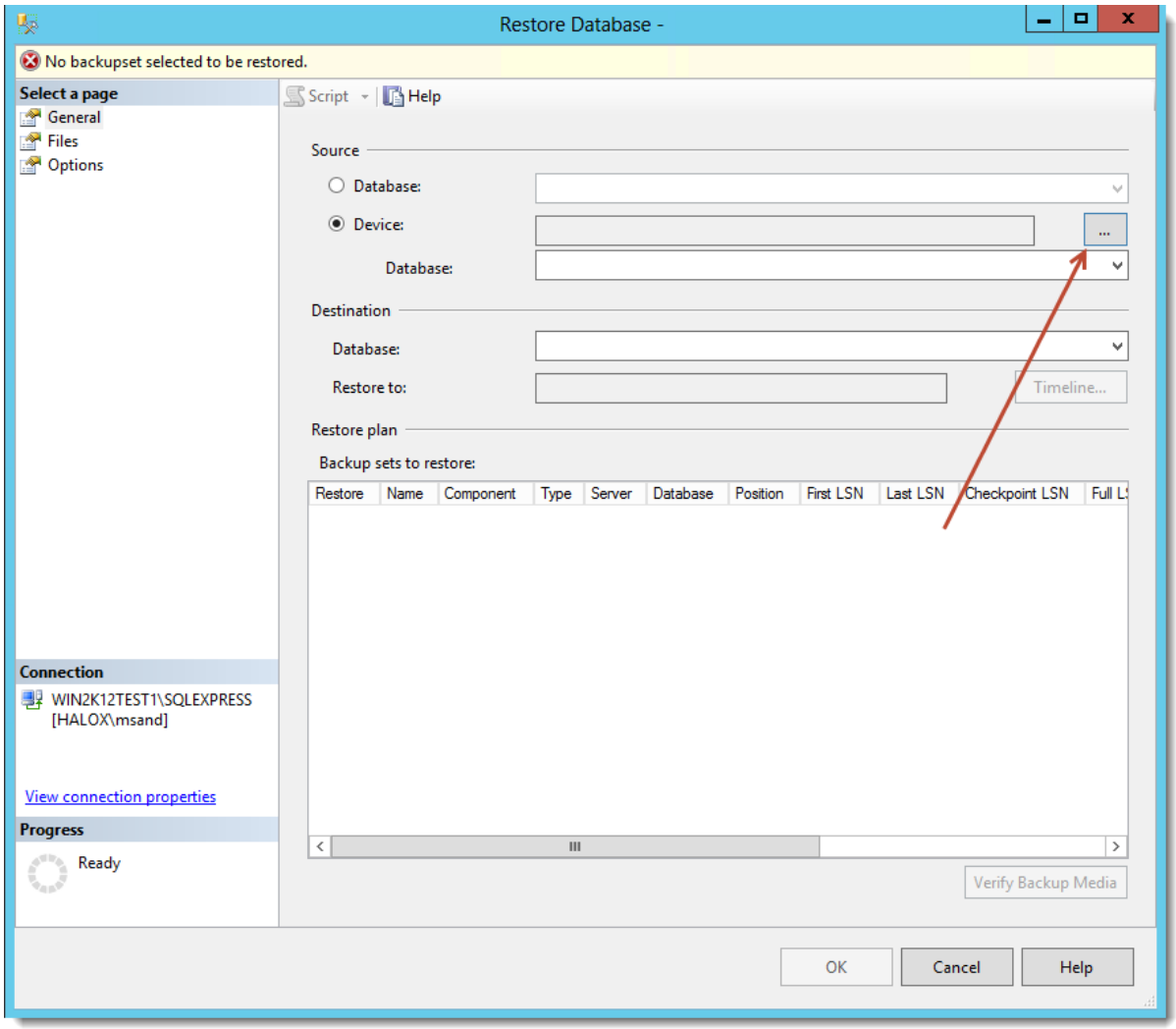
To restore a copy of the Passwordstate database, you must have appropriate database administrator access. Please follow these steps:

Open SQL Server Management Studio, and make a connection to your database server

Right click on the Passwordstate database select **Tasks -> Restore -> Database**

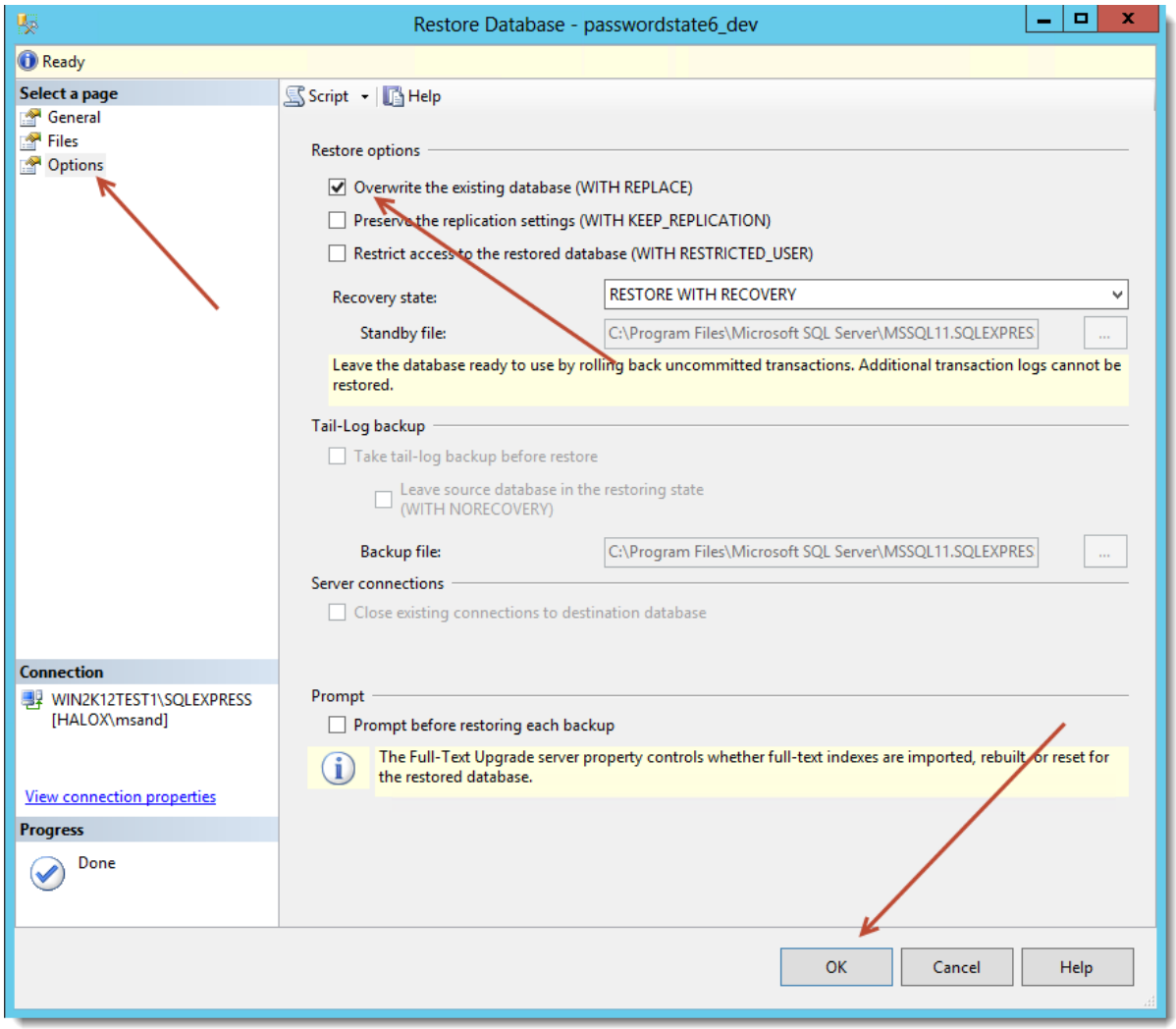


Click on **Device** as the **Source,** then click on the eclipse button and browse and select the latest database backup file



Once the backup file is showing in the 'Backup sets to restore' window, click on the **Options** page option, select the restore option of 'Overwrite the existing database (WITH REPLACE), and click on the OK button

Note: If you receive an error during the install about the database being in use, you may need to restart SQL Server to remove any locks - this can be done by right clicking on the server name in the **Object Explorer**, and selecting R**estart**.



Passwordstate_user SQL Account

If you are restoring the database to the same SQL Server, and over the top of an existing Passwordstate database, then the SQL Account used to connect the Passwordstate web site to the database (passwordstate_user) should require no modifications in any way. If however you are restoring to a different SQL Server, or the passwordstate_user SQL Account no longer exists for some reason, the following information may be helpful.

- During the initial installation of Passwordstate, an SQL account called passwordstate_user was created
- The passwordstate_user SQL account should have db_owner rights to the Passwordstate database
- If you look in the web.config file, located in the root of the Passwordstate folder, there is a database connection string which details which SQL server host the Passwordstate web site should be connecting to, and what the password for this account is meant to me - you can use this password value to reset the password in SQL Server if required.

```
<connectionStrings>
 <add name="PasswordstateConnectionString" connectionString="Data Source=win2k12test1\sqlexpress;Initial Catalog=passwordstate;
  User ID=passwordstate_user;Password=randompassword" providerName="System.Data.SqlClient"/>
</connectionStrings>
```

8.3 How to Clone Folders and Password Lists

If you need to create multiple Password Lists, the Clone Folder feature might be useful for you.

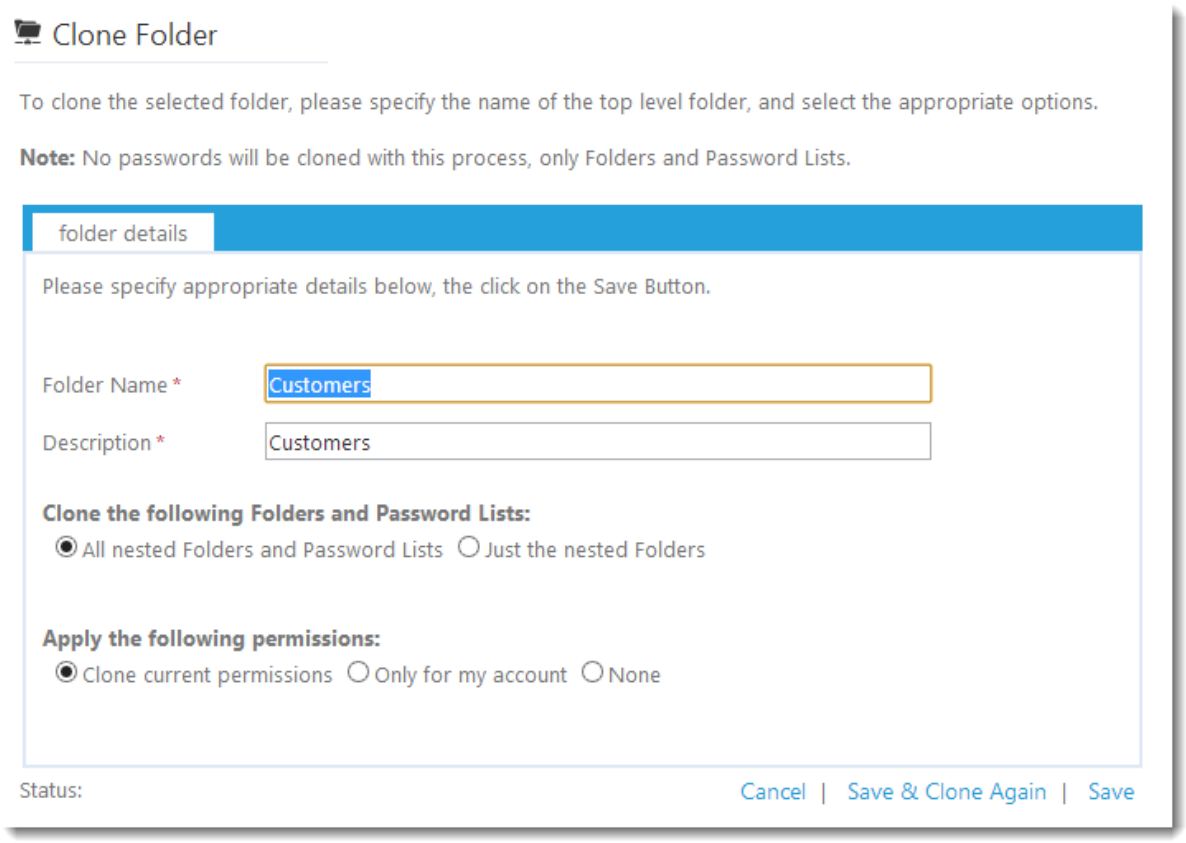
The Clone Folder feature allows you to pick a Folder, and clone all the Folders and Password Lists nested beneath it. The intention is to create a folder structure, with a base set of Password Lists and settings, and then duplicate this structure.

To clone a folder, you first need to click on it in the Navigation Tree, then click on the 'Folder Options' button at the top of the screen, and then you will see the 'Clone Folder' link. From here you have the following options available to you:

- Specify the new name of the folder to be cloned
- Choose whether you want to clone all Folders and Password Lists nested below the chosen folder, or just clone Folders only
- Choose what permissions you would like to apply to the new Folders and Password Lists – either clone the current permissions, apply permissions just for yourself, or don't apply any permissions at all

When you have finished cloning the folder, it will place the structure in the root of the Navigation Tree.

Note 1: Standard processing occurs when cloning folders i.e. appropriate audit events are logged, and email notifications are sent informing users they have access to one or more new Password Lists.
Note 2: Cloning Password Lists will not clone any of the passwords contained within them – only settings, customizations and permissions will be cloned.



8.4 Specifying Your Own Custom Fields

When you create or edit a Password List, the standard fields which can be used are:

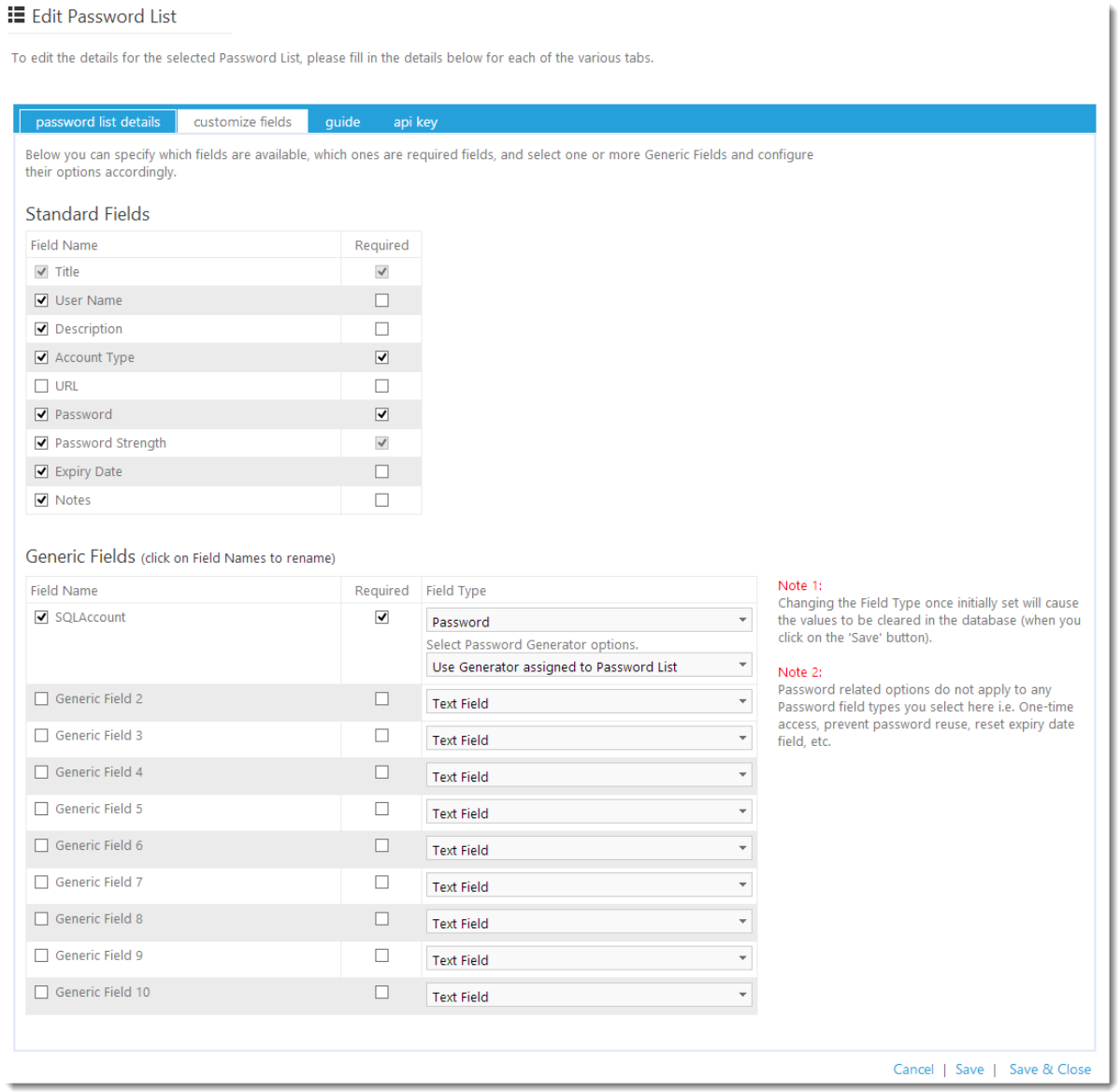
Field Name	Length	Description
Title	255	A title which describes the password
User Name	255	A username which is normally used as part of the authentication process for the password
Description	255	A longer description describing the password's use
Account Type	NA	A graphical icon to help identify the record type
URL	255	If the password relates to a web site login, or FTP login, etc, you can specify the URL
Password	NA	The password itself
Password Strength	NA	Not a field to store any data - a graphical representation of the strength of the password
Expiry Date	NA	A data in which the value of the password should be reset
Notes	8000	Any general notes about the password

In addition to the Standard Fields, you can select up to 10 different custom fields, and the custom fields can be named to anything you want, and have the following data types:

- Text Field – just a standard text field

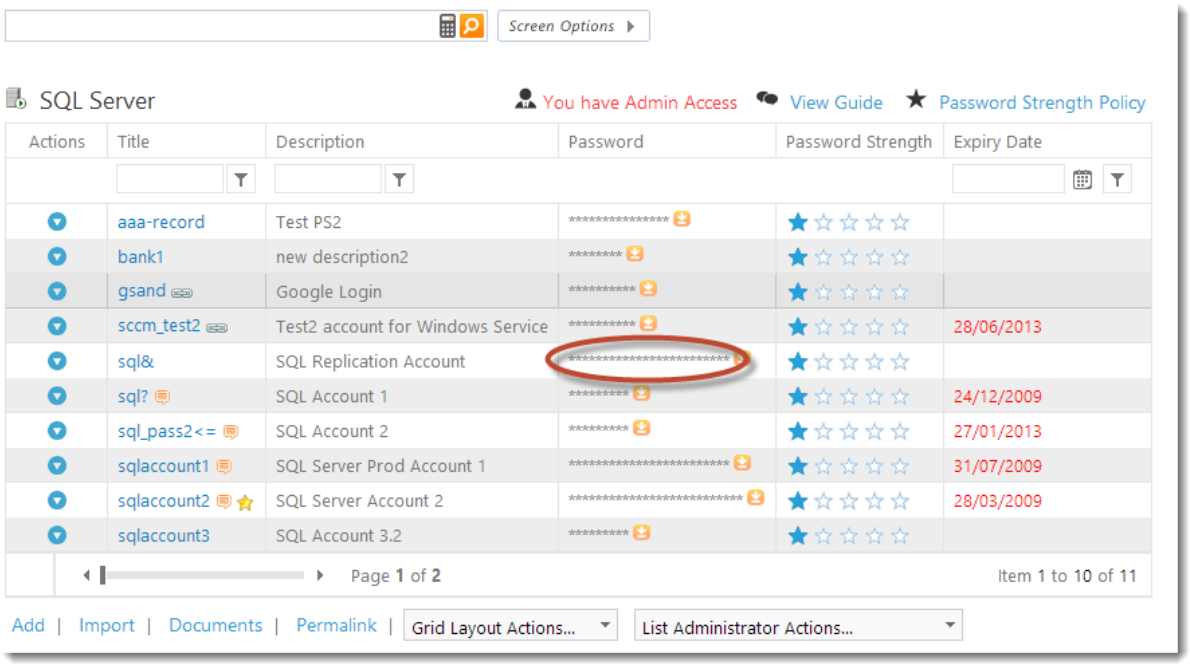
- Free Text Field – an unlimited text field for entering larger bodies of text
- Password – an encrypted password field (encrypted and salted in the database), and allows you mask the contents as per a normal Password field i.e. ******, and you can also copy to clipboard as per normal
- Select List – allows you to specify multiple fixed values, which shows as a drop-down list
- Radio Buttons – allows you to specify multiple fixed values, which shows as a Radio Button
- Date Picker – similar to the Expiry Date field, this one gives you a popup calendar for specifying date values

Caution: If you have a requirement to change the Field Type of an existing in-use Generic Field, this will cause the values to be cleared in the database as some of the Generic Fields need to their data stored differently, and also processed differently when displayed on the site.



8.5 Multiple Options for Hiding Passwords

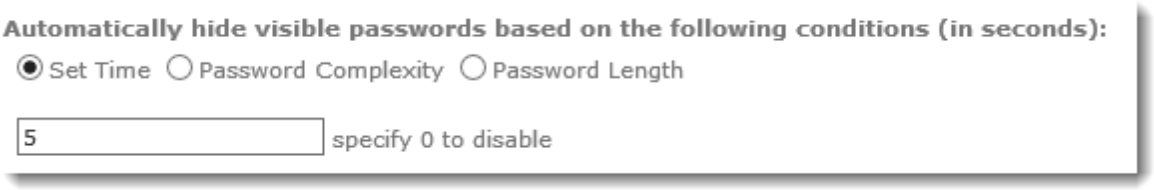
On each of the Password Lists screens, there is a 'Password' column which shows the masked password and provides a image for you to click on copy the Password to the clipboard – see image below. There are three options for how long the Password will stay visible on the screen when you click the masked password text.



To select one of the three different time options, you can do so on the screen Administration -> System Settings -> Passwords Options Tab. The options are:

Option 1 – Hide Based on a Set Time

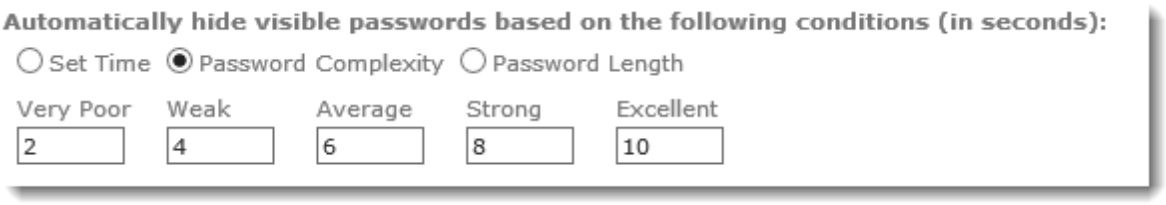
Regardless of the length or complexity of the Password, you can hide the Password based on a set time interval – in seconds.



Option 2 – Hide Based on Complexity of the Password

As you're aware, each Password is deemed to be of a certain 'Strength', and this strength can differ depending on which 'Password Strength Policy' is assigned to the Password List. You can set

a specific time interval for each of the 5 different Password Strengths – Very Poor, Weak, Average, Strong & Excellent



Option 3 – Hide Based on Password Length

It can be very difficult to read an unmasked Password in it's entirety if it is a long password – more than likely it will be hidden before you've finished typing the password into a different screen somewhere. To overcome this, you can hide the Password based on different set time intervals, for three different Password Lengths – of which, all can be customized to your liking. Note that **Length 3** is **greater than or equal to**, whereas the other two options are **less than or equal to**. This means you should set Length 3 to be one value greater than Length 2.

8.6 Controlling Settings for Multiple User Accounts

With the use of the **User Account Policies** feature, you can specify multiple settings for User's Preferences, their Password List Screen Options, and also their Home Page and Folder Screen Options. These settings can then be applied to either multiple user accounts, or multiple security groups.

You can access the User Account Policies from the screen Administration -> User Account Policies, and when you add/edit a policy, you can control the following settings:

User Preferences

Mask Password Visibility on Add/View/Edit Pages
Auto Generate New Password When Adding a New Record
Enable Search Criteria Stickiness Across Password Screens
Show the 'Actions' toolbar on the Passwords pages at the
Expand the bottom Navigation Menu items by
Locale (Date Format)

Specify which Authentication option will apply to the user's account

Password List Screen Options

Show the 'Header' row on all Passwords Grids
Show the 'Filter' controls in the Header of the Passwords Grids
Show the 'Header' row on all Recent Activity Grids
Make the Recent Activity Grid visible to the user
Selects the Paging Style controls for Password and Recent Activity grids
Make the Pie Charts visible to the user

Home Page and Folder Screen Options

Show the Favorites Passwords Grid
Show the Password Statistics Chart
Choose the Style of the Password Statistics Chart
Stack the data points on top of each other for the Password Statistics Chart
Select the color theme for the Password Statistics Chart

Note 1: When you first add a new User Account Policy, it is disabled by default. It is recommended that before you enable the policy, you apply the permissions required, then click on the 'Check for Conflicts' button. The Check for Conflicts process will ensure that there are no two settings with different values assigned to a user's account - this could cause confusion for the user, and for Security Administrators if this is the case.
Note 2: You can have more than one policy applied to a user's account, but you should use the **Check for Conflicts** button after applying permissions to the policy.

When a User Account Policy is in effect for a user, the option will be disabled for them, and they will see a little red flag notification, informing them a policy is in effect. In the following graphic, a policy is set for the 'Page Style' used for the grids.