Passwordstate User Manual

© 2017 Click Studios (SA) Pty Ltd

Table of Contents

© 2017 Click Studios (SA) Pty Ltd

© 2017 Click Studios (SA) Pty Ltd

Part IX KB Articles 160

© 2017 Click Studios (SA) Pty Ltd

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

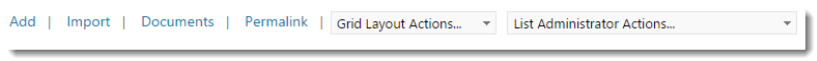
If you are new to Passwordstate, please study the Quick Start Tutorials to familiarize yourself with the basics.

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

© 2017 Click Studios (SA) Pty Ltd

	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

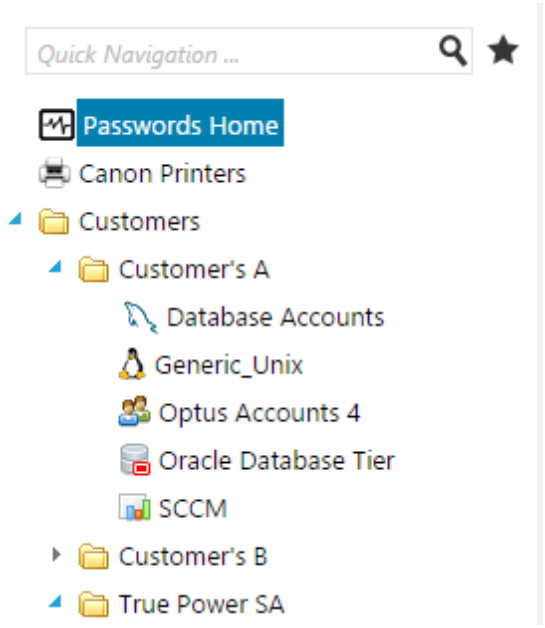
The following is a few quick tips to get you familiar with the Passwordstate interface, and some of the features it offers.

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.

© 2017 Click Studios (SA) Pty Ltd

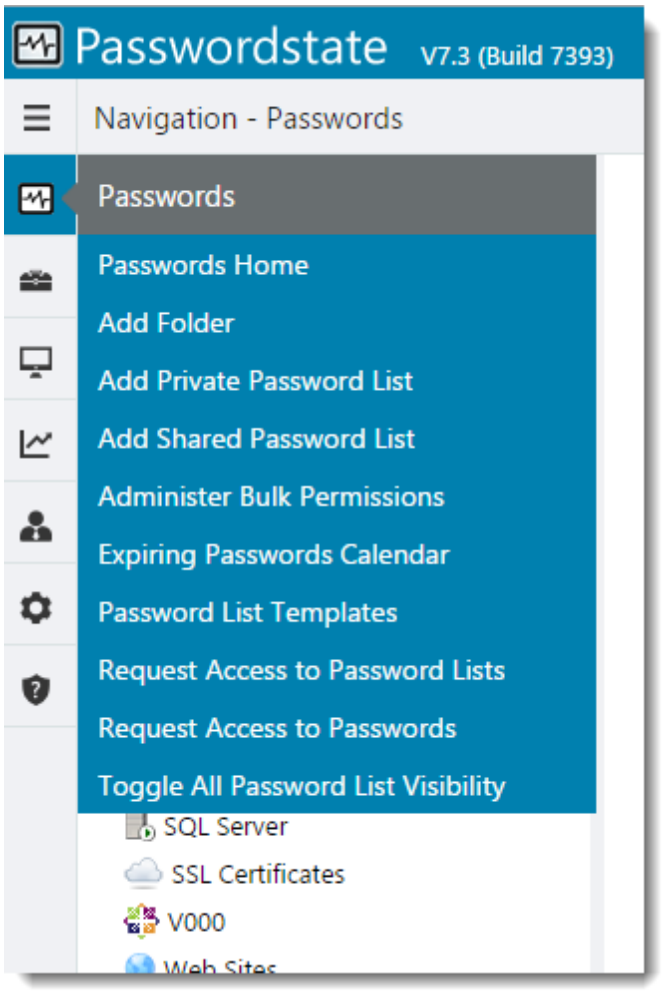


Navigation Menu Items

There are two types of Main Navigation Menus available - a Vertical one on the left hand side of the screen, or a Horizontal one at the bottom of the screen. Each of these Menus have sub-menus providing access to the core functionality within Passwordstate.

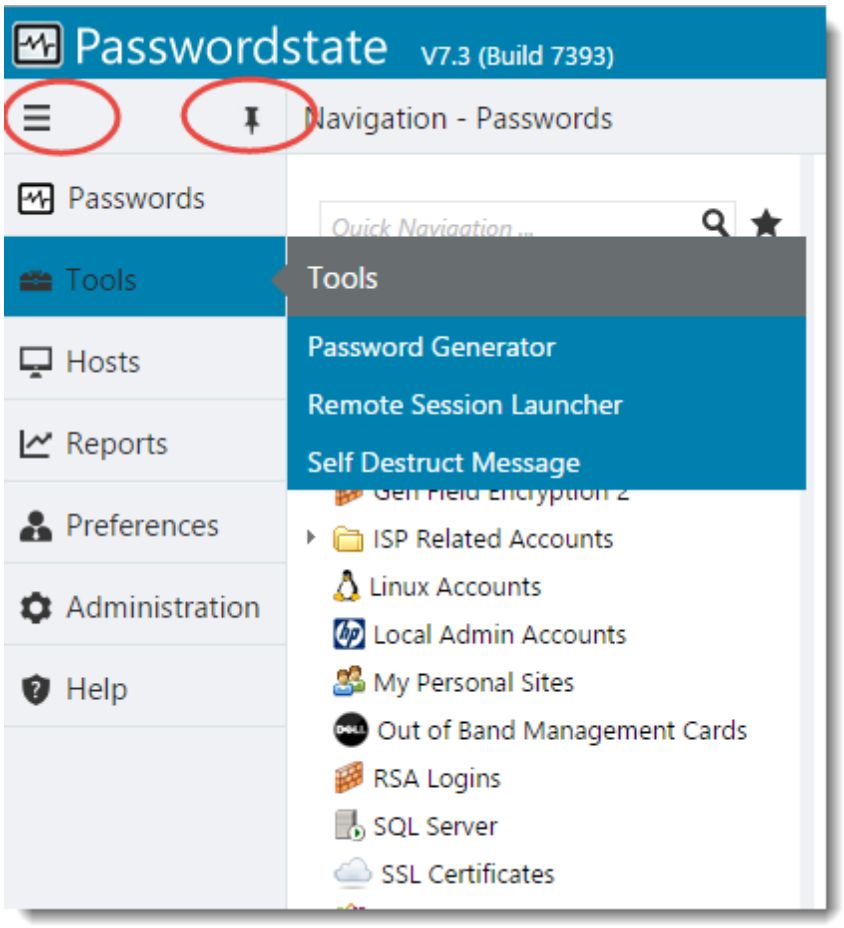
Note: Some of these actions may be disabled by your Security Administrators of Passwordstate.

© 2017 Click Studios (SA) Pty Ltd

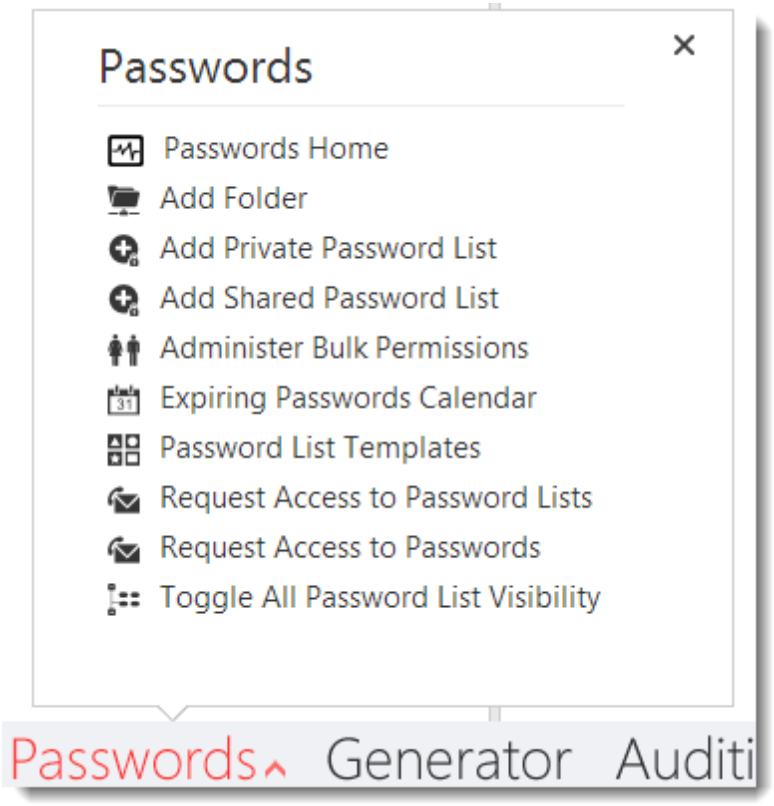


You can also expand and pin the Vertical Menu.

© 2017 Click Studios (SA) Pty Ltd



© 2017 Click Studios (SA) Pty Ltd

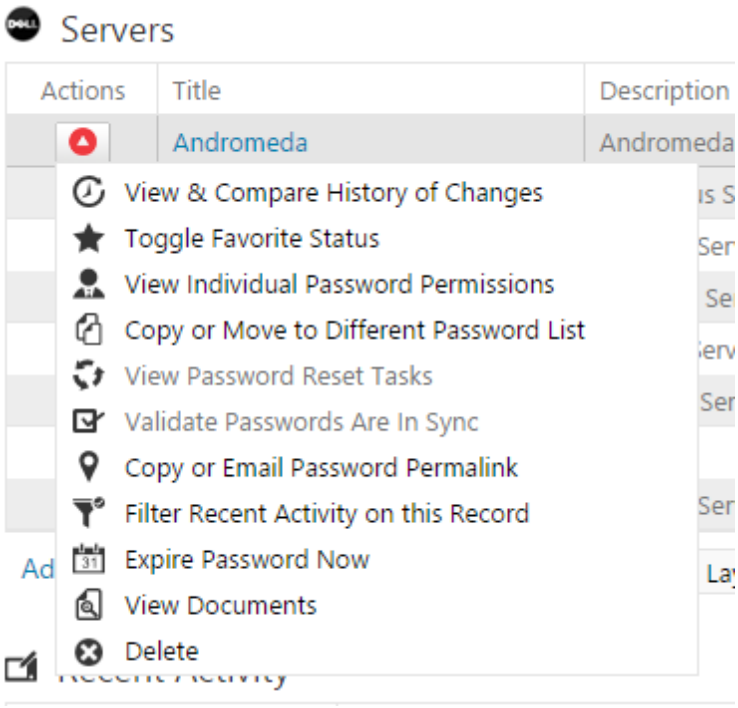


Grid Actions Drop-down Menus

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.

© 2017 Click Studios (SA) Pty Ltd

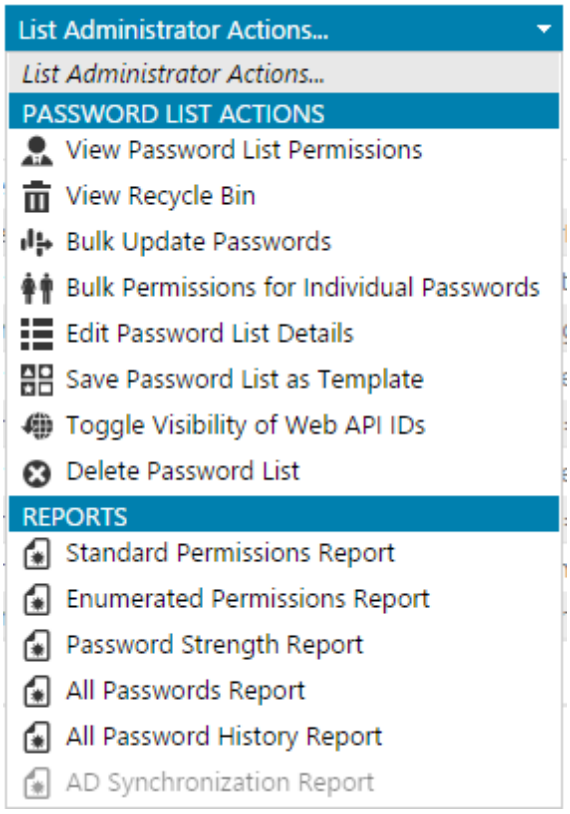


Password List Administrator Actions

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.

© 2017 Click Studios (SA) Pty Ltd



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. The Star symbol also allows you to filter any Password Lists you have marked as being your 'Favorites'.

Resizing the Navigation Tree Pane

You can re-size the Navigation Tree pane by simply dragging the following re-size divider.

Resizing the Navigation Pane is also automatically saved for the next time you use Passwordstate.

View or Copy Password to Clipboard

© 2017 Click Studios (SA) Pty Ltd

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

Both of these actions will add an audit event record.

Password and Password List Permissions

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

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

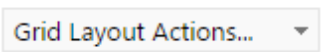
Searching for Passwords

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

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

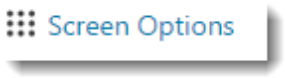
Resetting Number of Rows in Grids

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



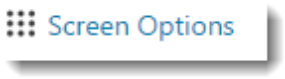
© 2017 Click Studios (SA) Pty Ltd

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



Screen Options

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



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

Reordering and Resizing Grid Columns

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

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

Generate a Random Password

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

Preferences

By clicking on the main 'Preferences' Menu Item, you can specify multiple settings which are

© 2017 Click Studios (SA) Pty Ltd

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
5. Color Themes
6. API Keys for various features

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 Password Lists	Allows you to request access to one or more Password Lists

© 2017 Click Studios (SA) Pty Ltd

Menu Item	Description
Request Access to Passwords	Allows you to search for individual password records, and then request access to them - this is intended to be used when you don't require access to an entire 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.

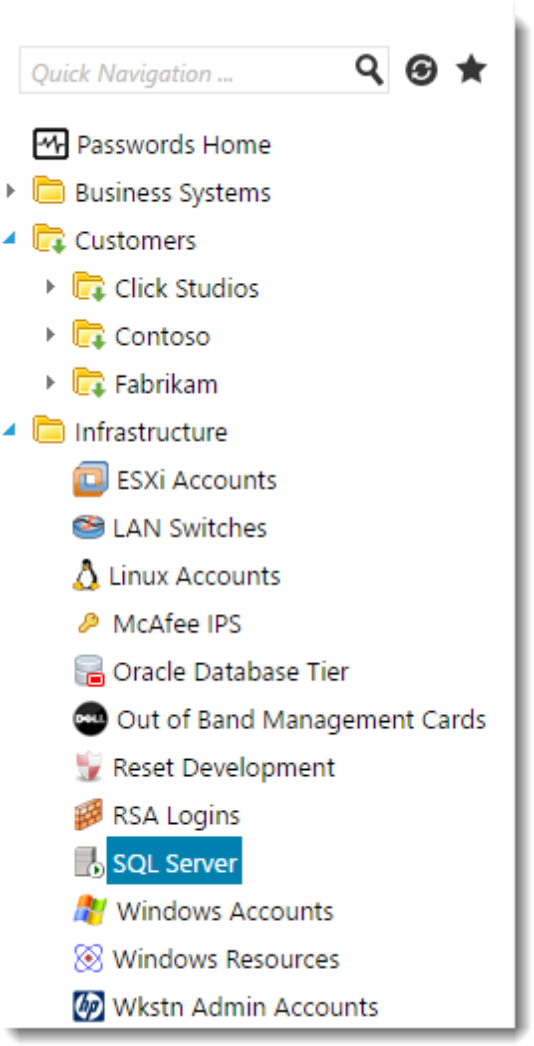
Some of the features of the Navigation Tree are:

- 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

© 2017 Click Studios (SA) Pty Ltd

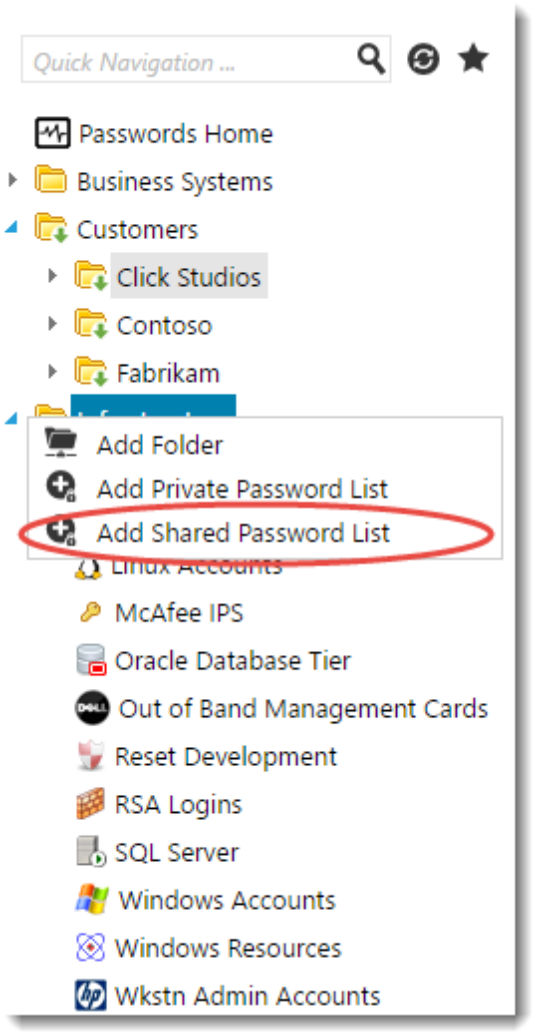
the same access

- When expanding/collapsing tree nodes, if you hold down the Control Key while doing so, it will expand/collapse all nested Password Lists/Folders beneath the one you are clicking on
- The Star symbol also allows you to filter any Password Lists you have marked as being your 'Favorites'.



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

© 2017 Click Studios (SA) Pty Ltd



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.

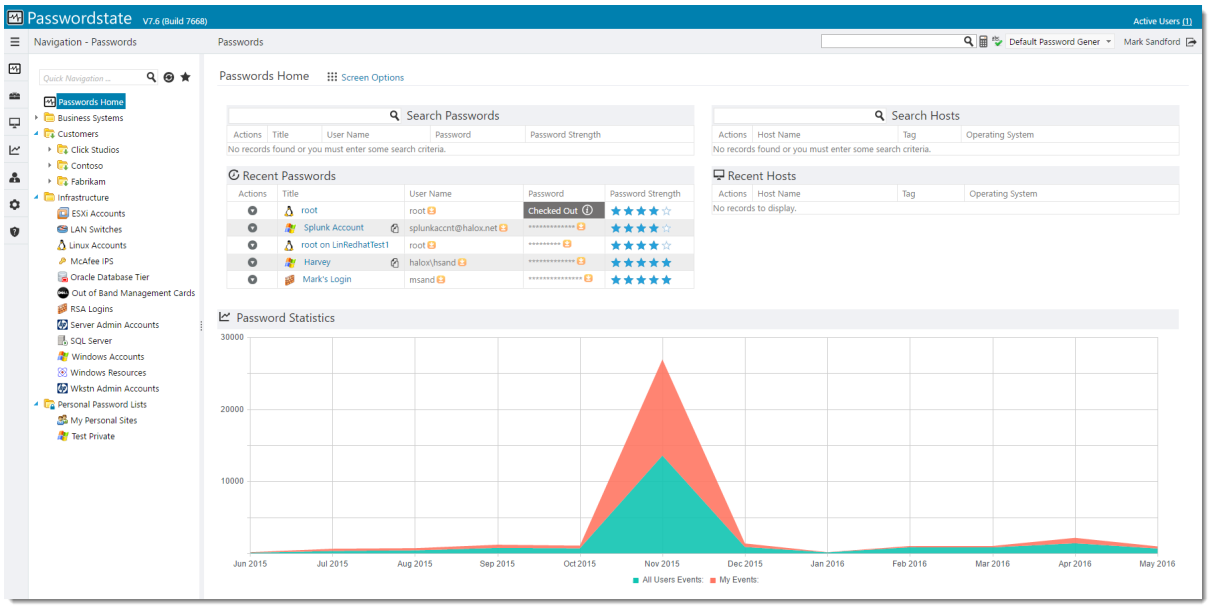
Note: Some of these features detailed below may be hidden or disabled for you, depending on your access rights, and what settings have been applied to the various Password Lists you have access to.

On this screen you can:

- Search for Passwords across all the Password Lists you have access to (from Passwords Home), or all passwords within the selected Folder. Note: To perform an exact match search, enclose your search term in double quotes i.e. "root_admin"
- View and access Passwords you've recently used i.e. viewed/editing/copied to clipboard, etc
- View your tagged Favorite Passwords

© 2017 Click Studios (SA) Pty Ltd

- Search for Hosts and launch a Remote Session to the host i.e. RDP, SSH, Telnet or VNC
- View Hosts you've recently launched a Remote Session to
- View your tagged Favorite Password Lists
- Generate a single random password by clicking on the icon
- View some basic auditing statistics 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

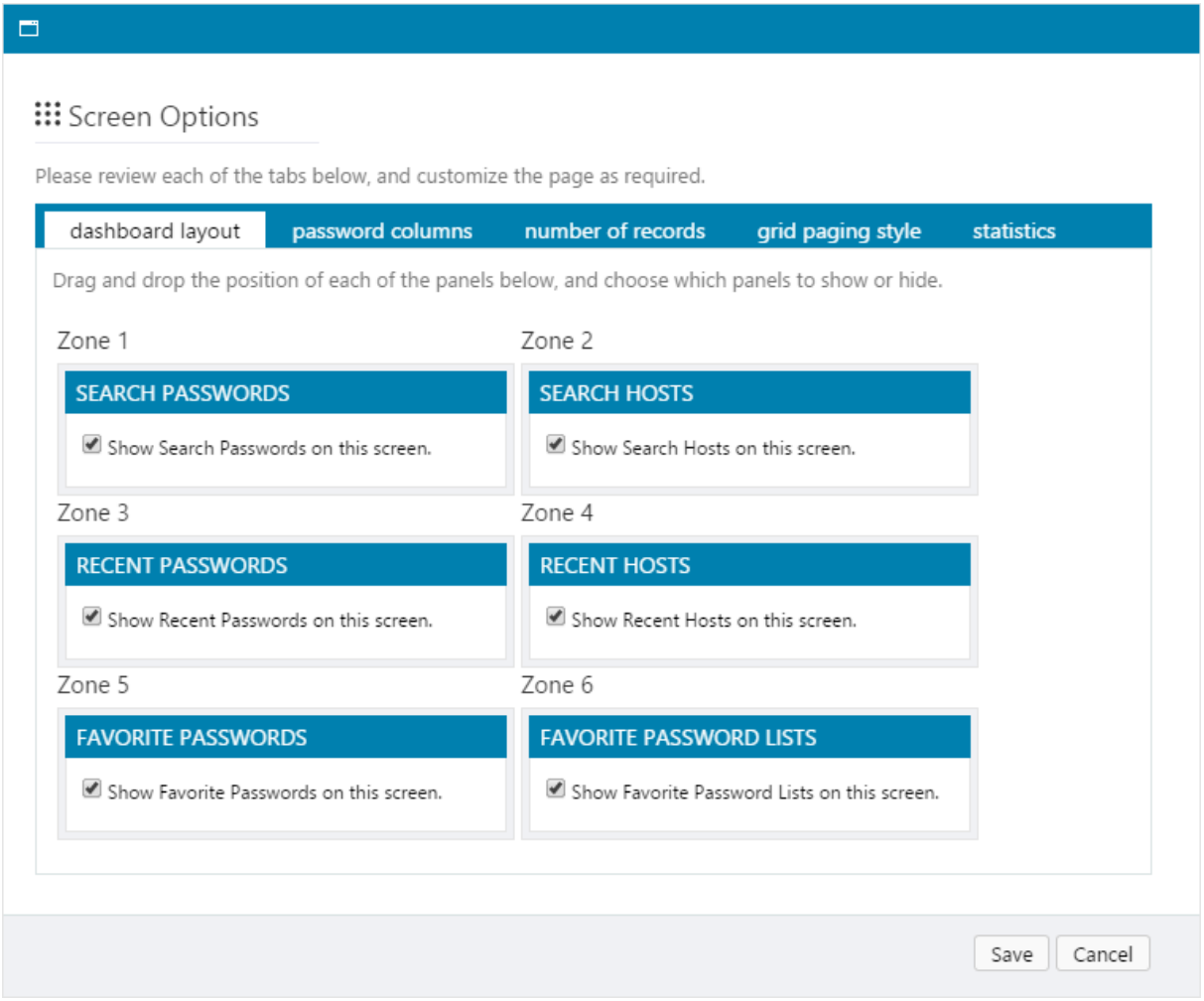
Screen Options allows you to specify various settings for how you would like to see the grids and charts displayed on the screen.

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.

Dashboard Layout Tab

© 2017 Click Studios (SA) Pty Ltd

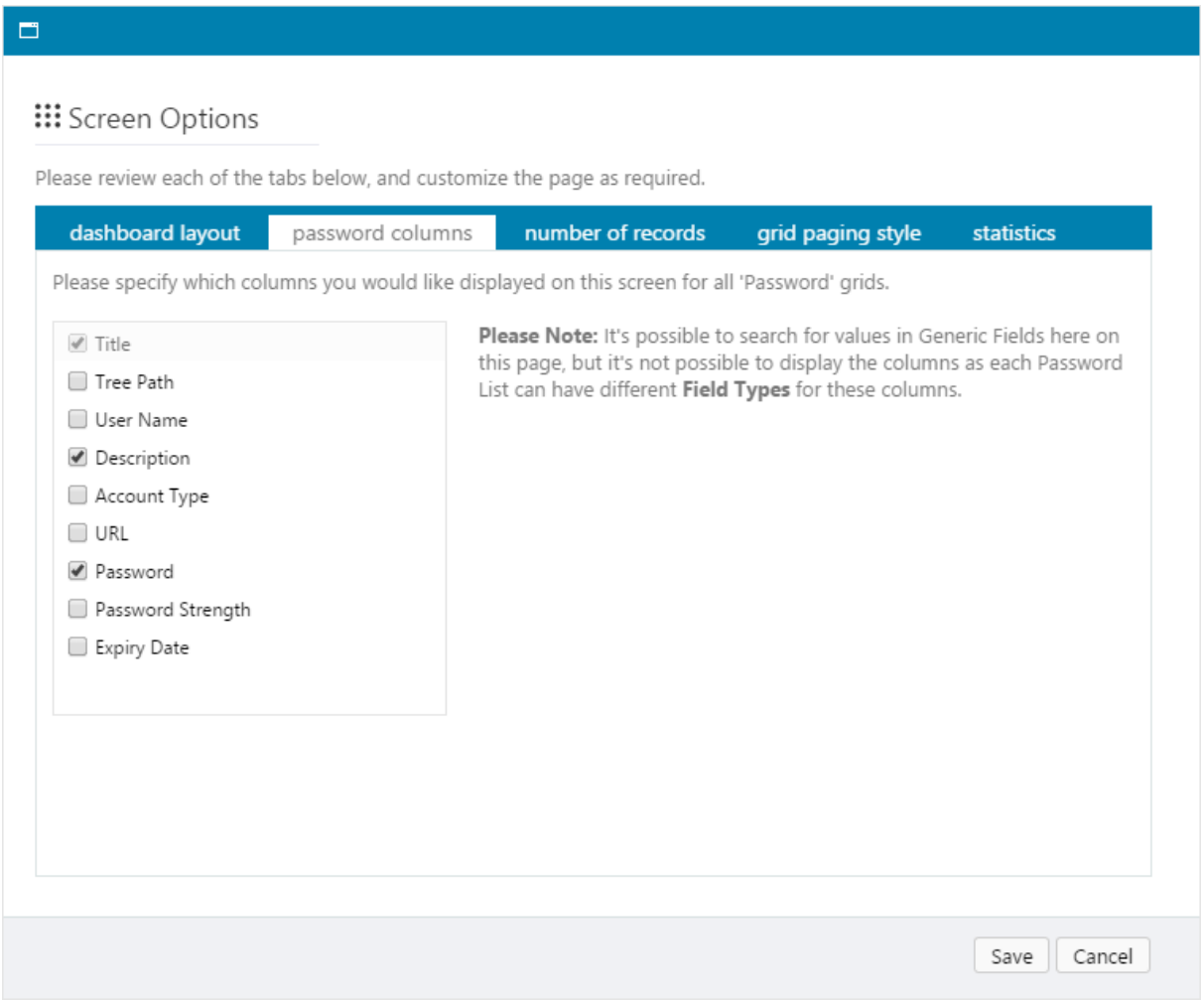
The Dashboard Layout tab allows you to select which Panels you would like to display, and in which Zone position. You can drag-n-drop the Panels around within the different Zones, so they appear in the position you like.



Password Columns Tab

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

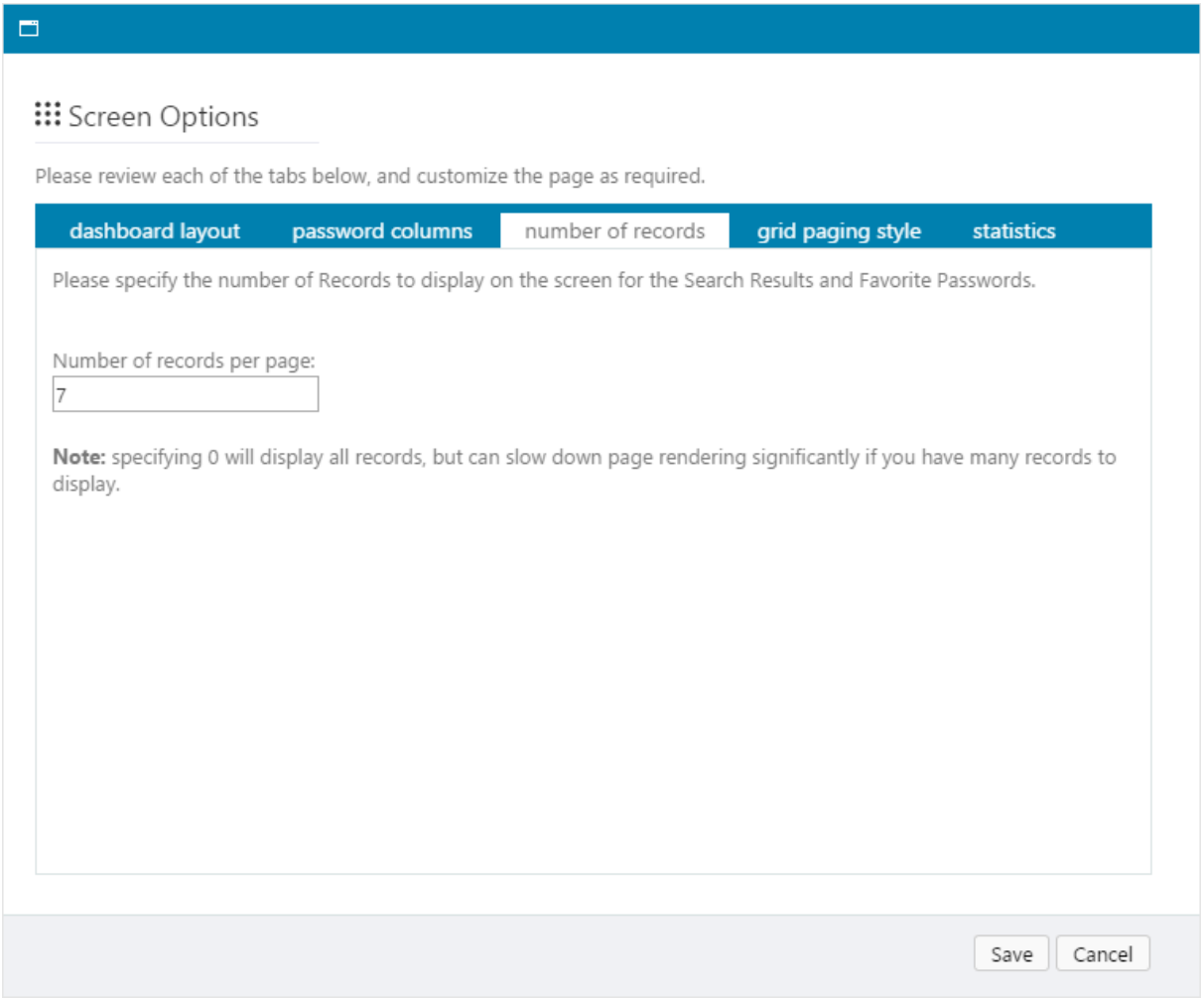
© 2017 Click Studios (SA) Pty Ltd



Number of Records Tab

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

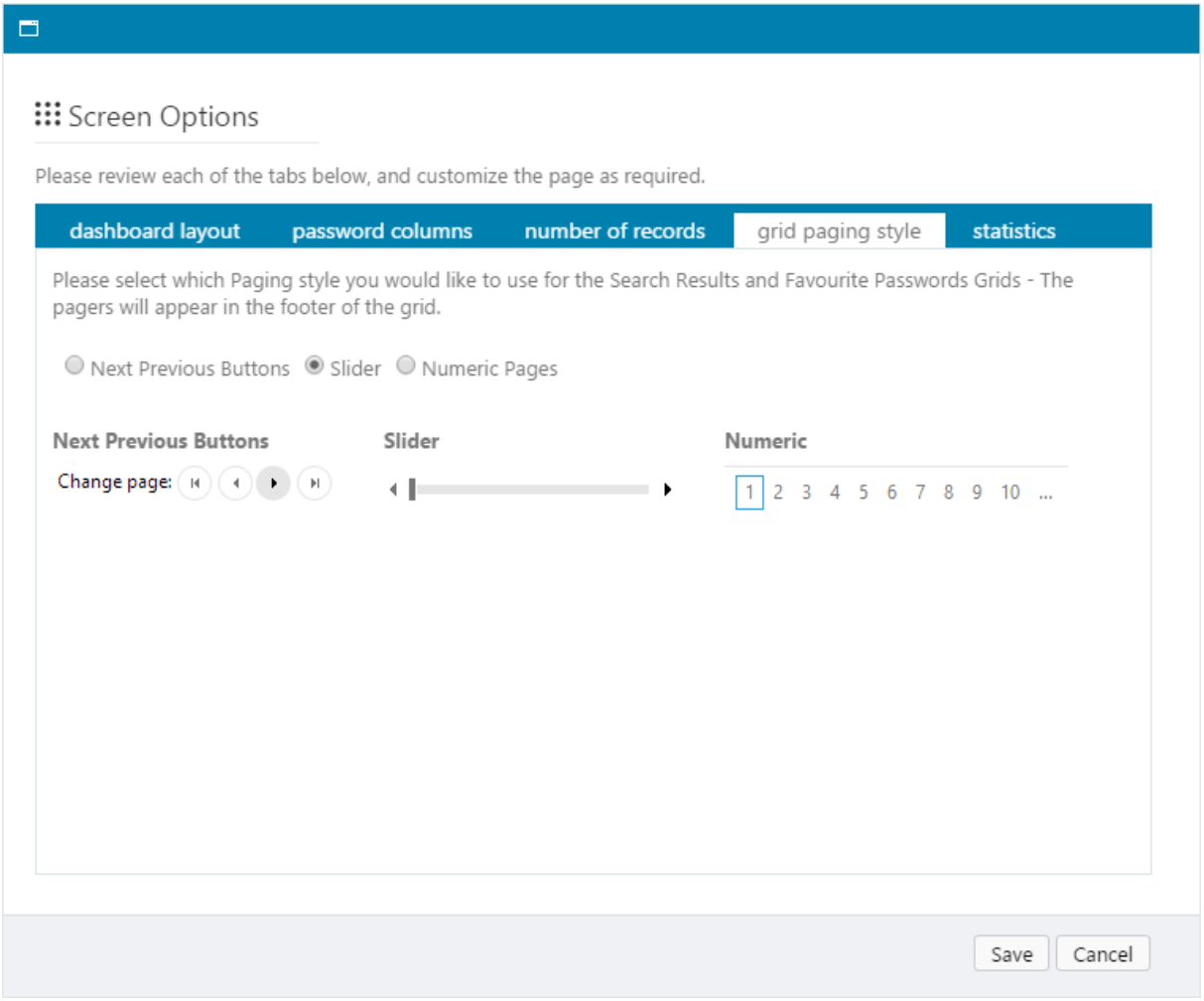
© 2017 Click Studios (SA) Pty Ltd



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.

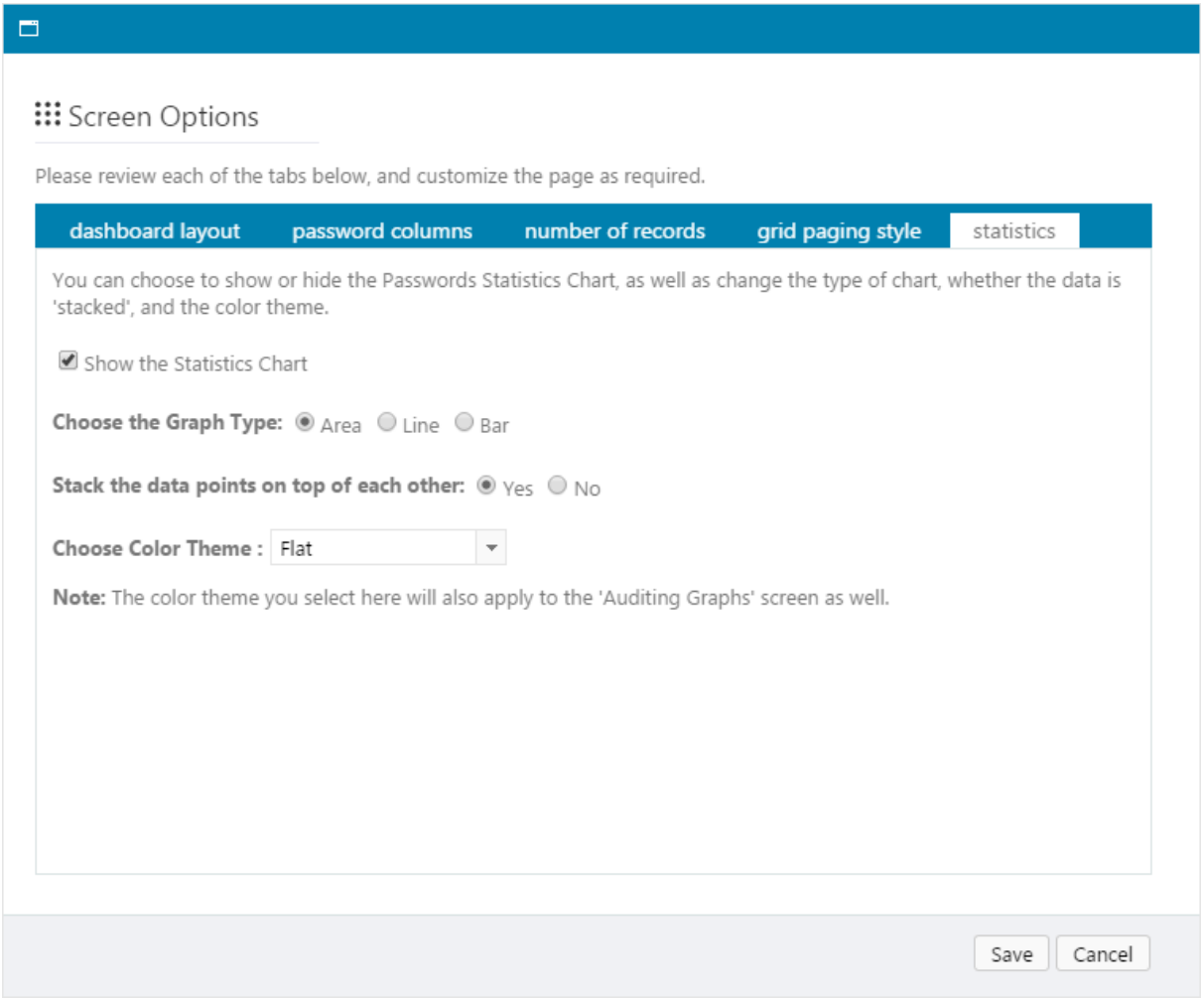
© 2017 Click Studios (SA) Pty Ltd



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.

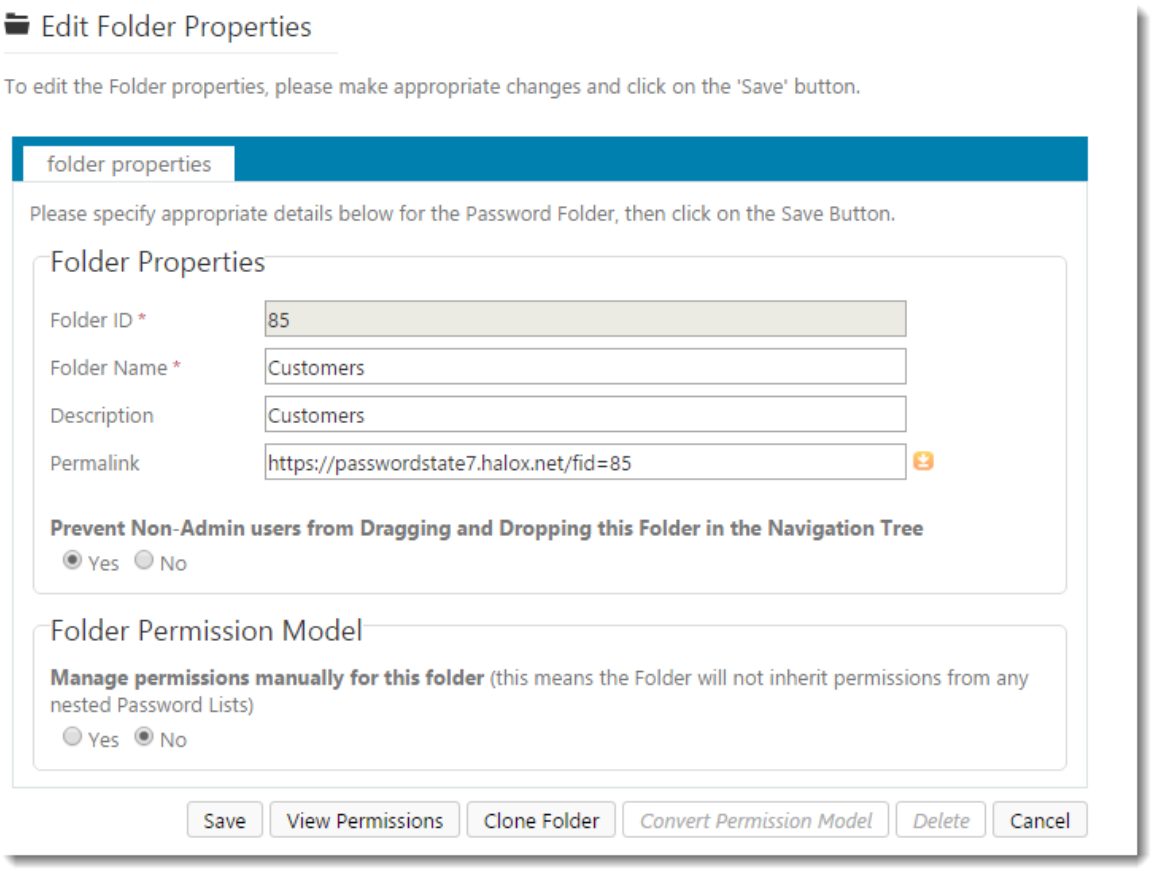
© 2017 Click Studios (SA) Pty Ltd



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.

© 2017 Click Studios (SA) Pty Ltd



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
- The Permalink allows someone to click on the URL specified, and navigate directly to the Folder

Clone Folder

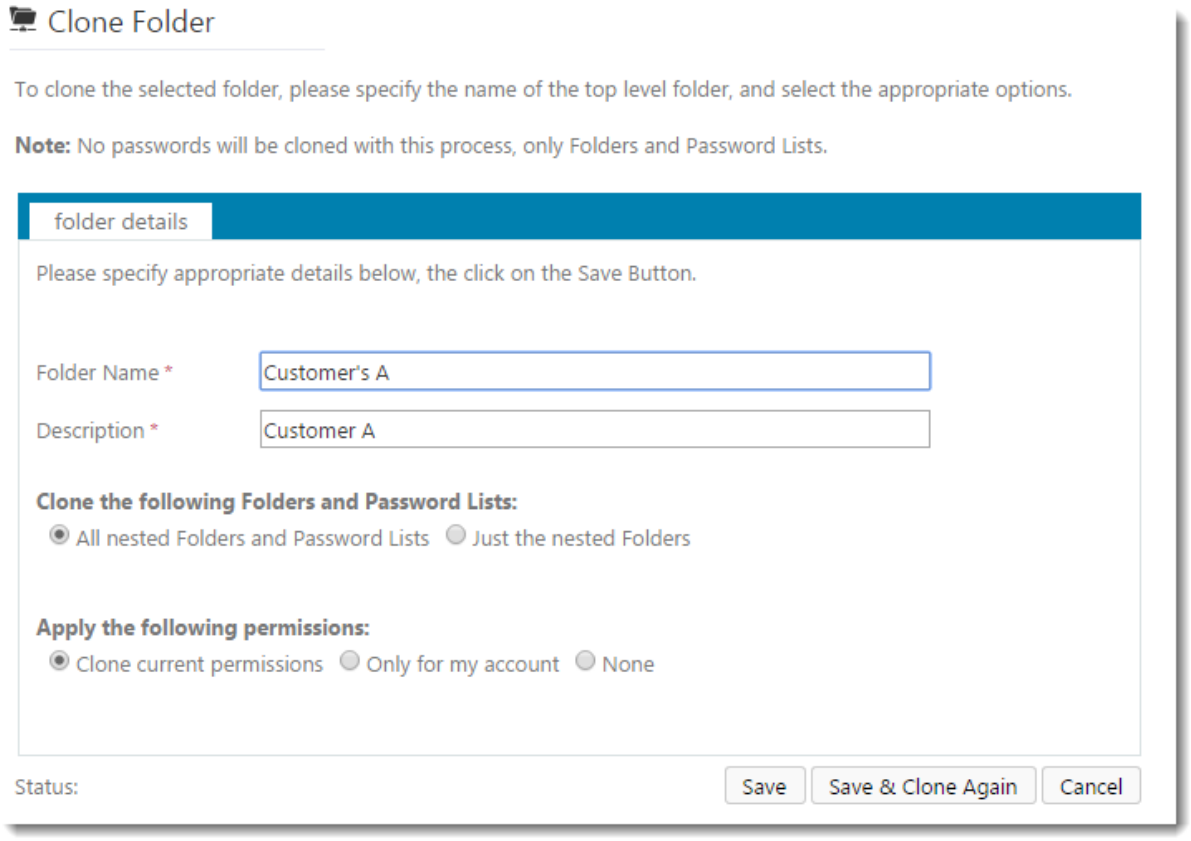
By clicking on the 'Clone Folder' button, there are various options available for you to clone the selected folder. The Options are:

- 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

© 2017 Click Studios (SA) Pty Ltd

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.

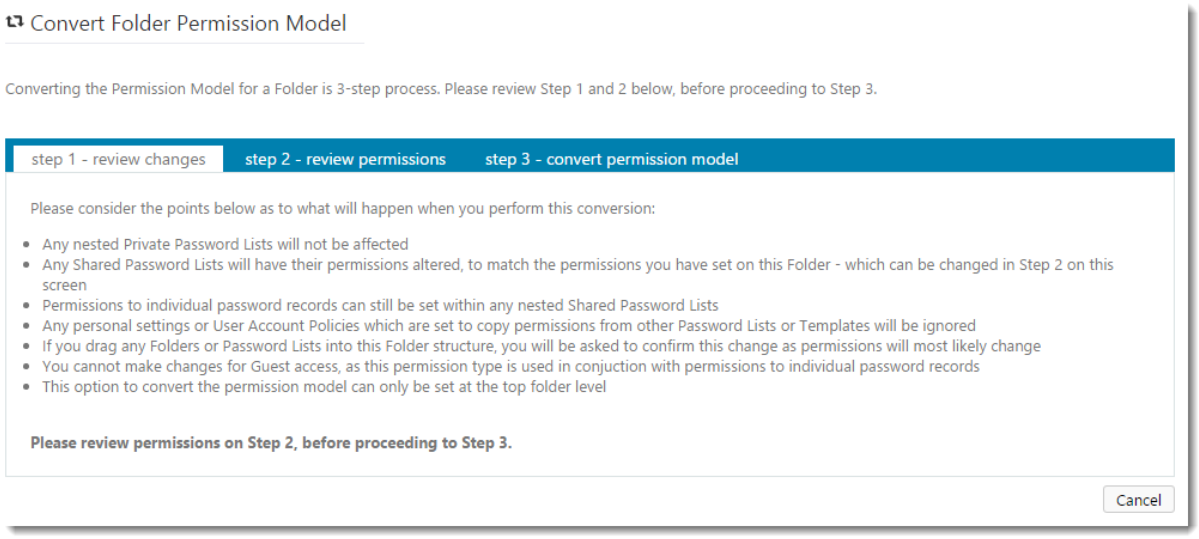


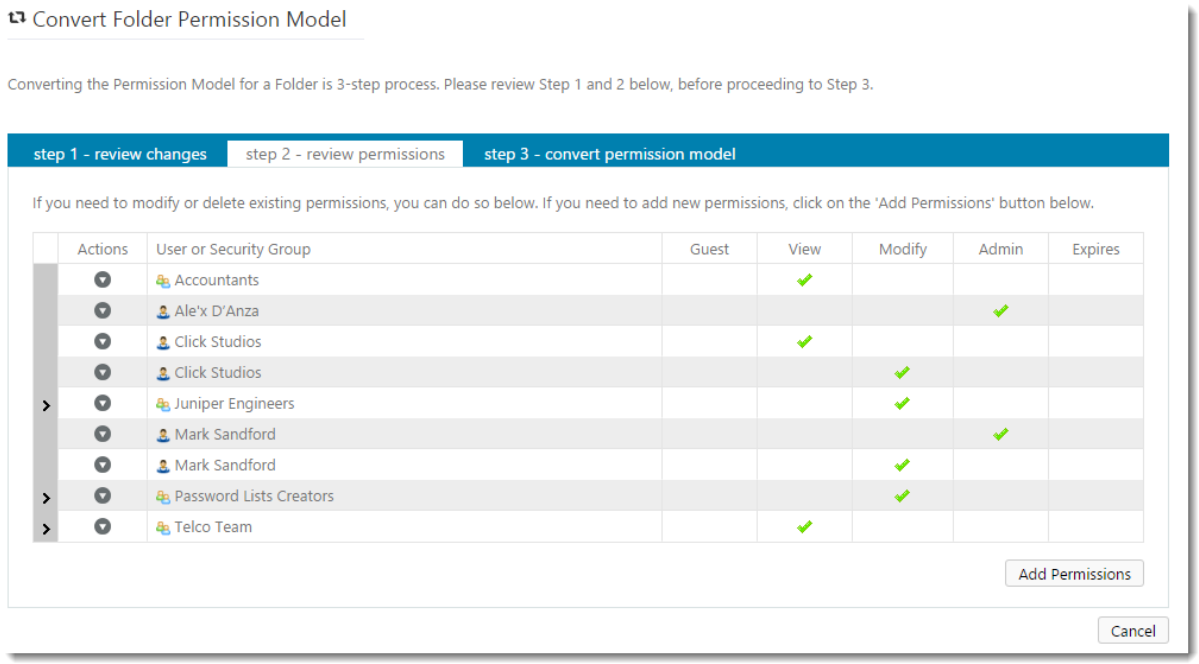
Convert Permissions Model

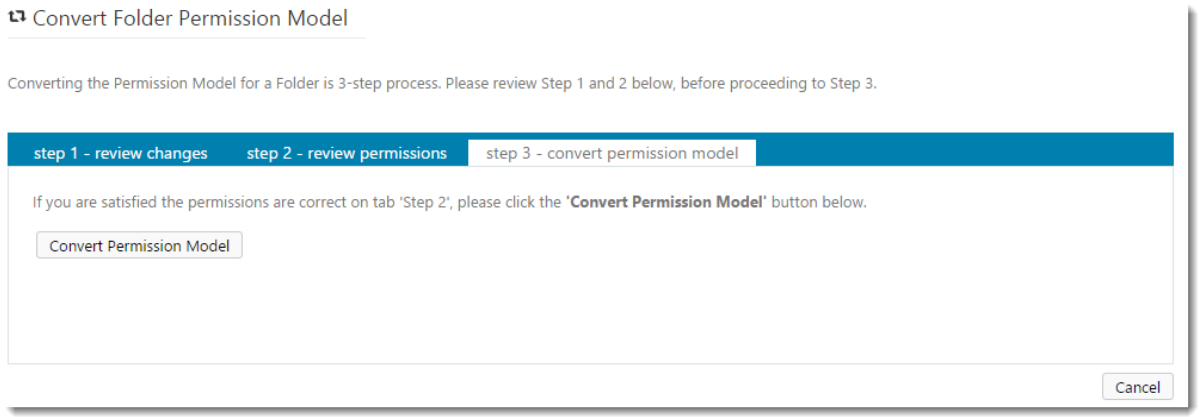
The default permissions model in Passwordstate is for Password Lists to propagate their permissions up to all upper level Folders. This can be changed so a top level Folder can propagate permissions down to all nested Password Lists and Folders. Please refer to the section Add Folder for certain restrictions when using this model.

You can convert between models by using the 'Convert Permission Model' button, but you must first check the 'Manage Permissions Manually for this Folder' option. When you do, you will be presented with a screen which asks you to confirm the permissions on the Folder, prior to propagating these down to all nested Password Lists and Folders.

© 2017 Click Studios (SA) Pty Ltd







© 2017 Click Studios (SA) Pty Ltd

2.1.3 Password Lists

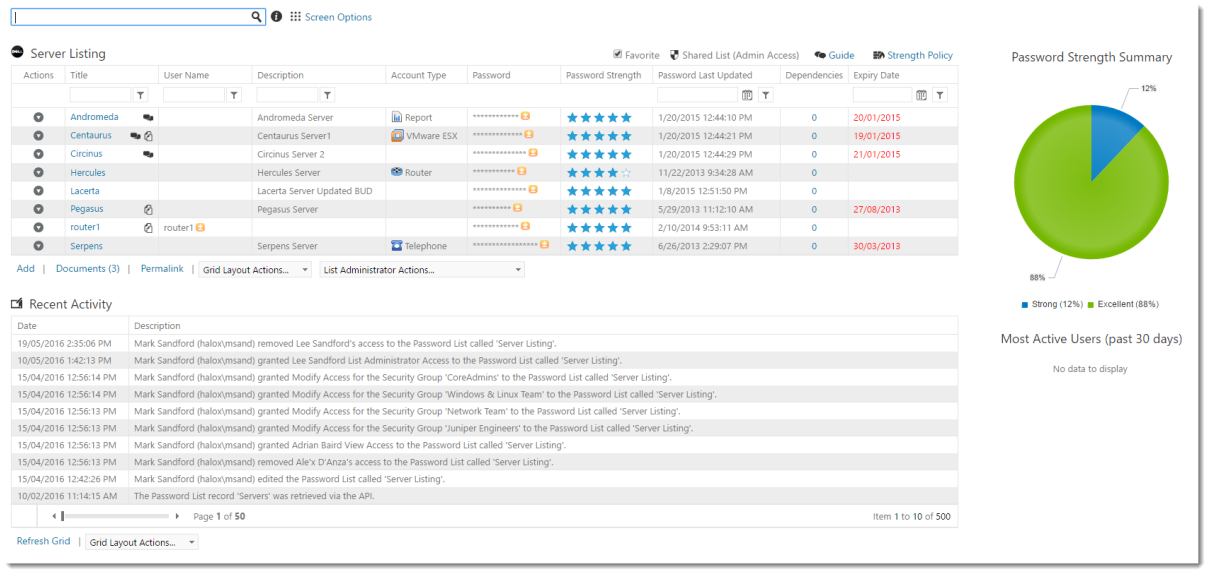
The Password List screen shows you the Passwords stored within the selected Password List. Not all Passwords may be visible to you here, as permissions can be applied to individual records within the Password Lists, as opposed to the whole Password List.

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:

- Search for Passwords contained within the selected Password. Note: To perform an exact match search, enclose your search term in double quotes i.e. "root_admin"
- View various statistics about the selected Password List
- Customize the screen by clicking on the Screen Options button
- View what access you have to the Password List, and 'Guide' which has been added for the Password List, and also the specific Password Strength Policy settings which have been applied
- View Auditing data related to the Password List (Recent Activity)
- You can edit/view a password by clicking on the hyperlink in the **Title** column
- You can view a password on the screen by clicking the masked ******* (the speed at which the password is again hidden can be control by your Security Administrators)
- You can copy a password to the clipboard by clicking on the icon (if using Internet Explorer, the clipboard can be cleared after a set time, which is set by your Security Administrators)
- You can perform various Password Actions by selecting the appropriate menu option from the Actions drop-down menu
- Add Passwords, view Uploaded Documents, or Email Permalinks
- If you have Admin privileges to the Password List, there will also be multiple options available to you via the List Administrator Actions Actions drop-down list
- By clicking on one of the segments in the 'Password Strength Summary' pie chart, you can filter the results in the Passwords grid
- By clicking on one of the segments in the 'Most Active Users' pie chart, you can filter the results in the Recent Activity grid

© 2017 Click Studios (SA) Pty Ltd



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.

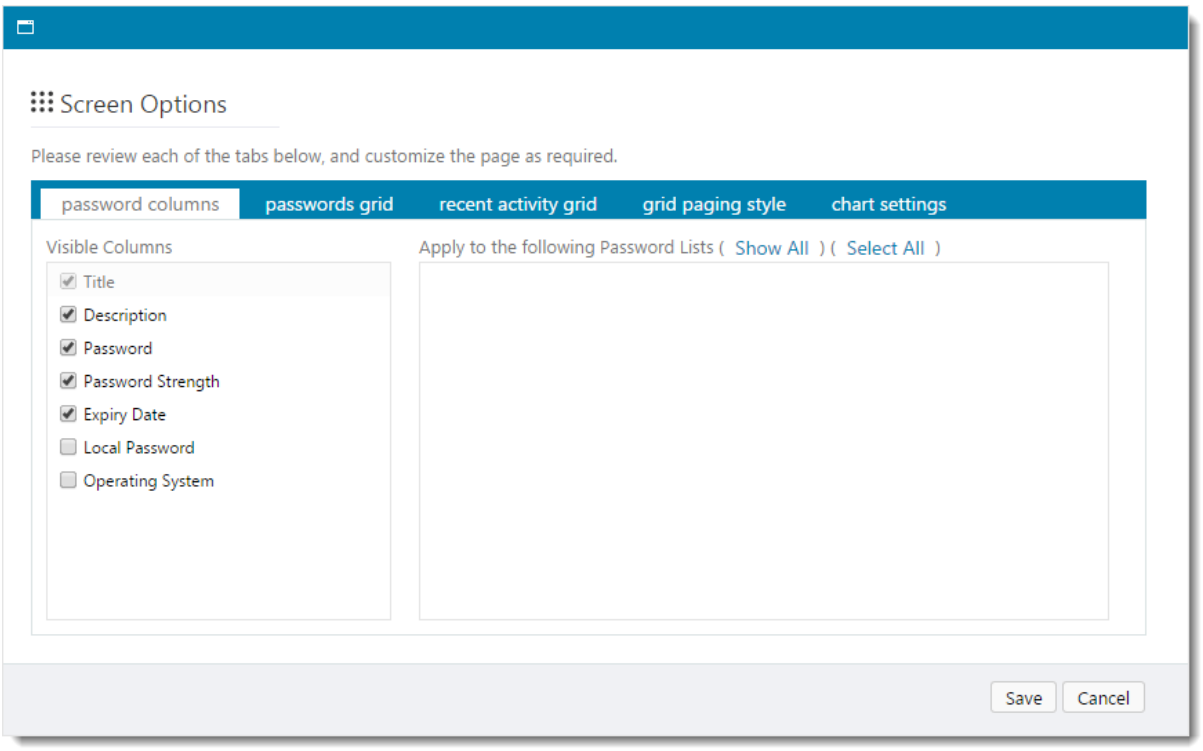
Please note that some of these settings may be set by your Security Administrator(s) of Passwordstate, and if so the controls will be disabled. You will see an icon like  , and message telling you if this is the case.

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

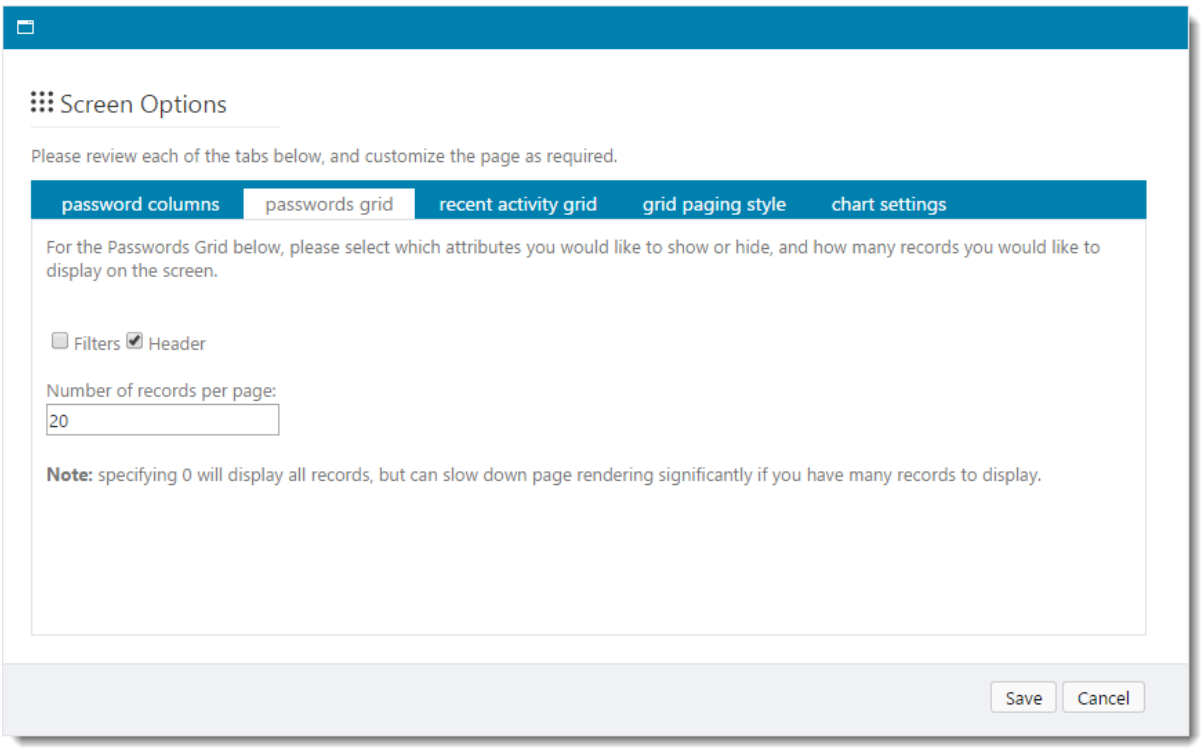
© 2017 Click Studios (SA) Pty Ltd



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.

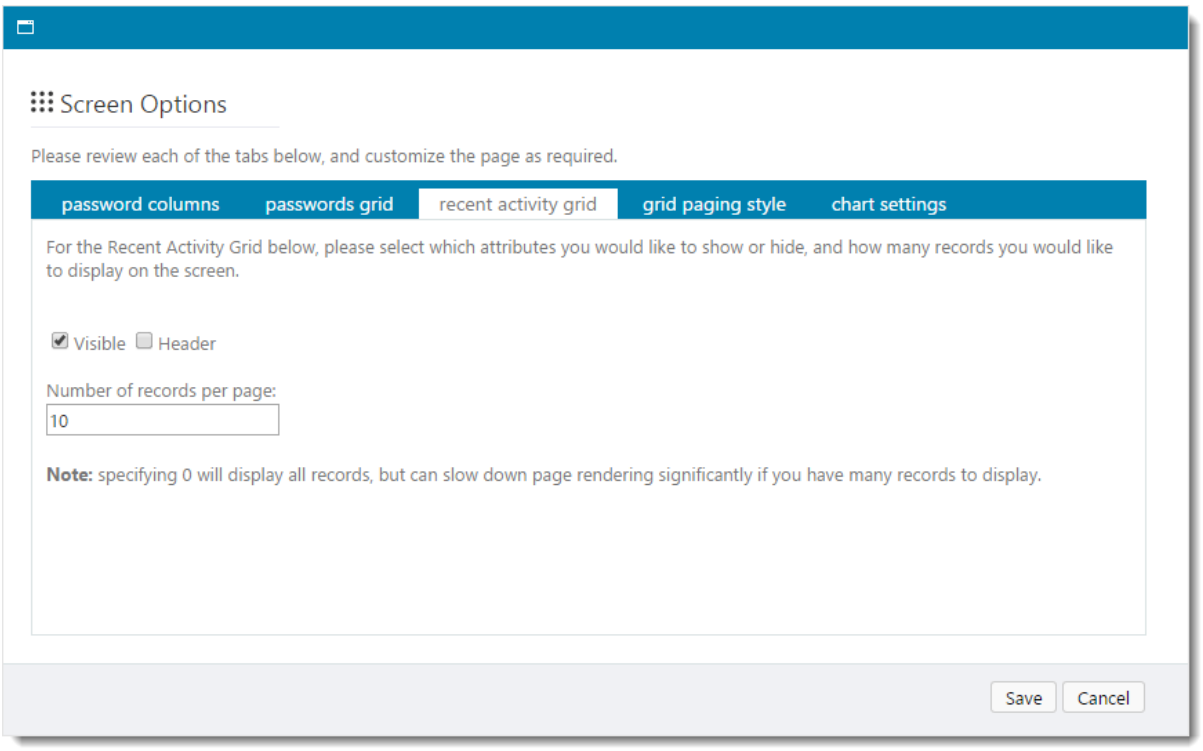
© 2017 Click Studios (SA) Pty Ltd



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.

© 2017 Click Studios (SA) Pty Ltd



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.

© 2017 Click Studios (SA) Pty Ltd

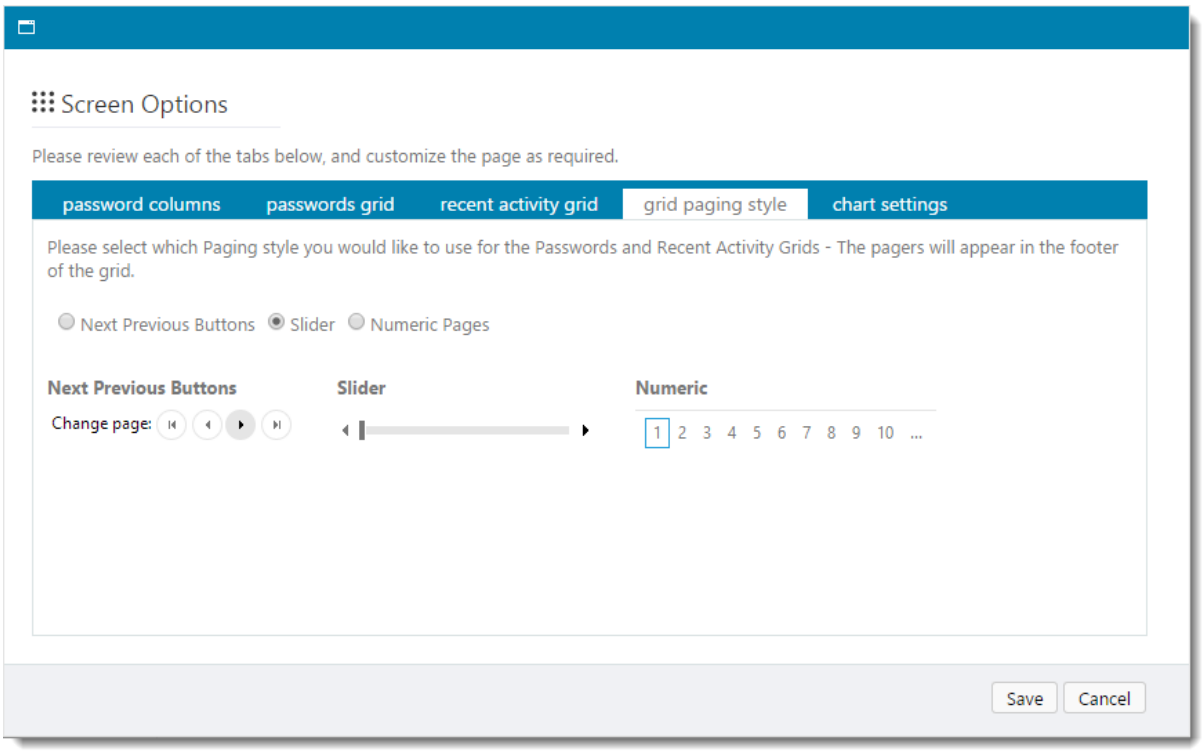
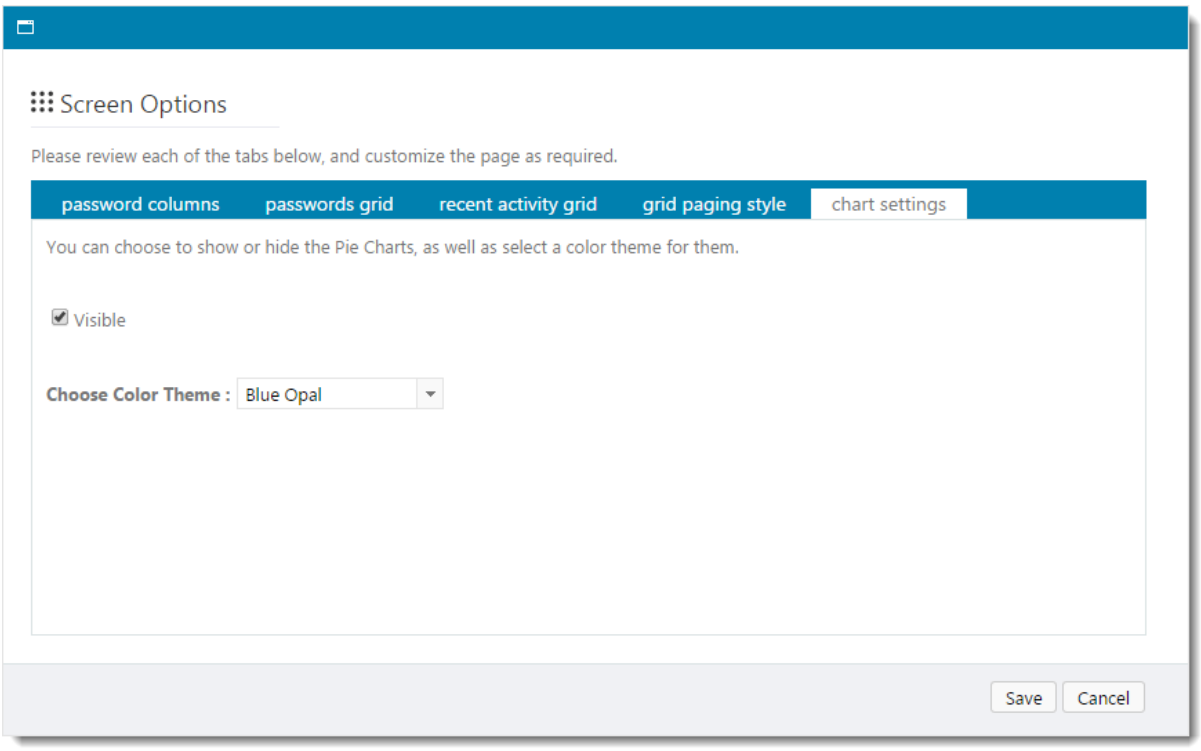


Chart Settings Tab

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

© 2017 Click Studios (SA) Pty Ltd



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:

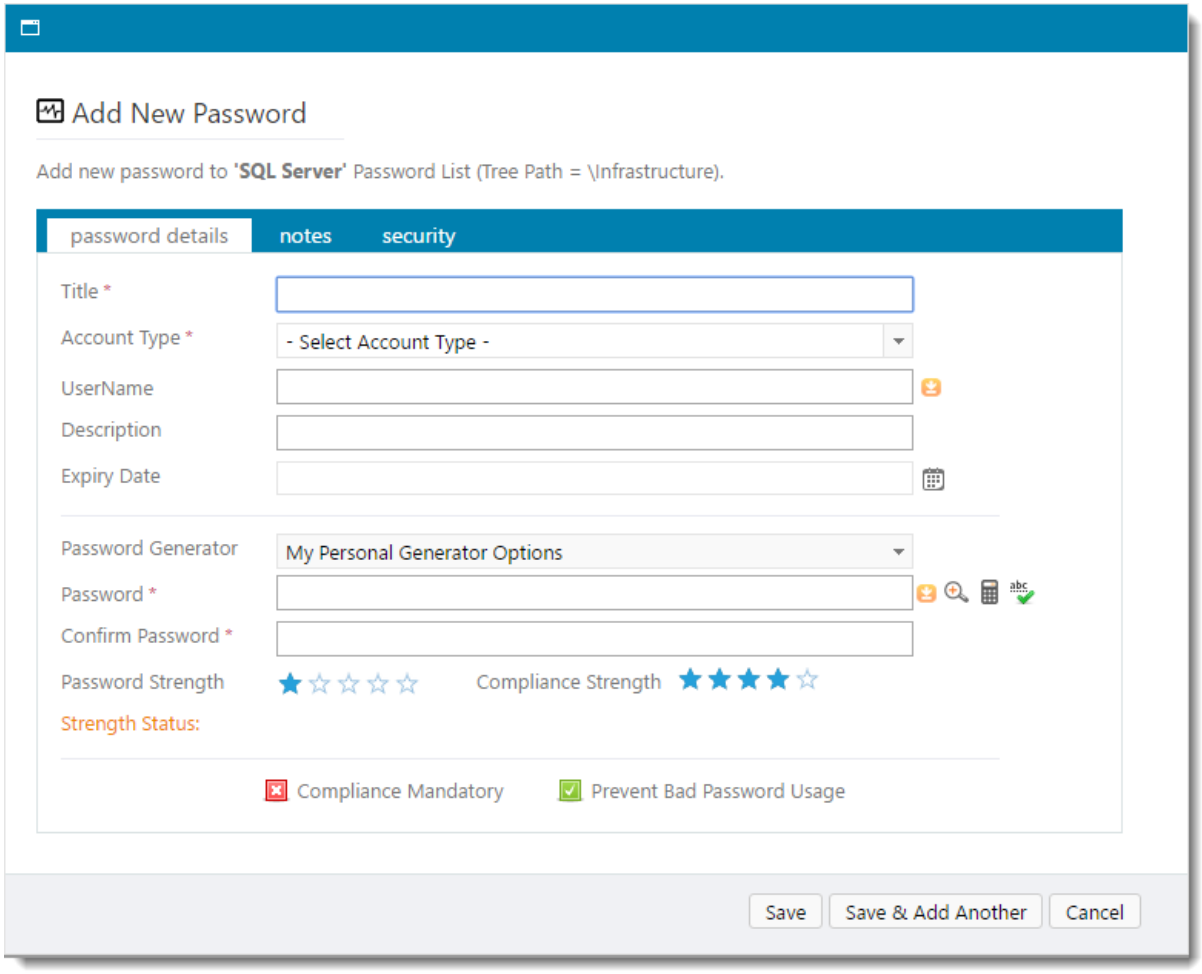
- Any fields which are denoted with * are mandatory fields, and you must specify a value for them
- The Password Strength indicators and text at the bottom of the screen only apply to the 'password' field - they do not apply to any Generic Fields which may be configure of type Password
- You can choose 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

© 2017 Click Studios (SA) Pty Ltd

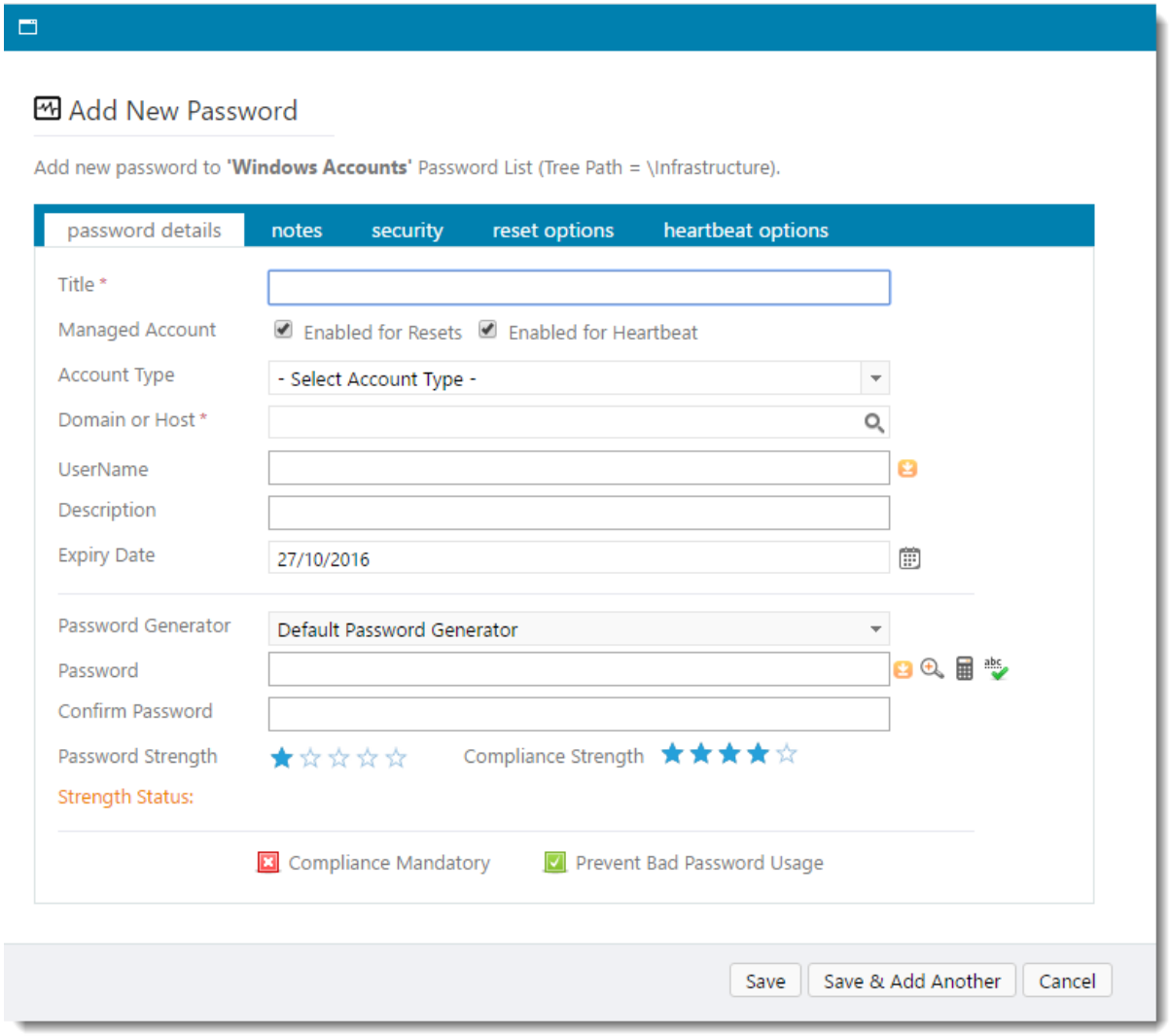
record, like a certain Password Strength must bet met before the record can be saved, or that passwords deemed as 'Bad' cannot be used. You will need to refer to one of the Administrators of the Password List to understand what settings and restrictions have been applied

- The Spell Check type icon shows a popup window which spells out the password in the format of 'PAPA alpha sierra sierra whiskey oscar romeo delta'

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



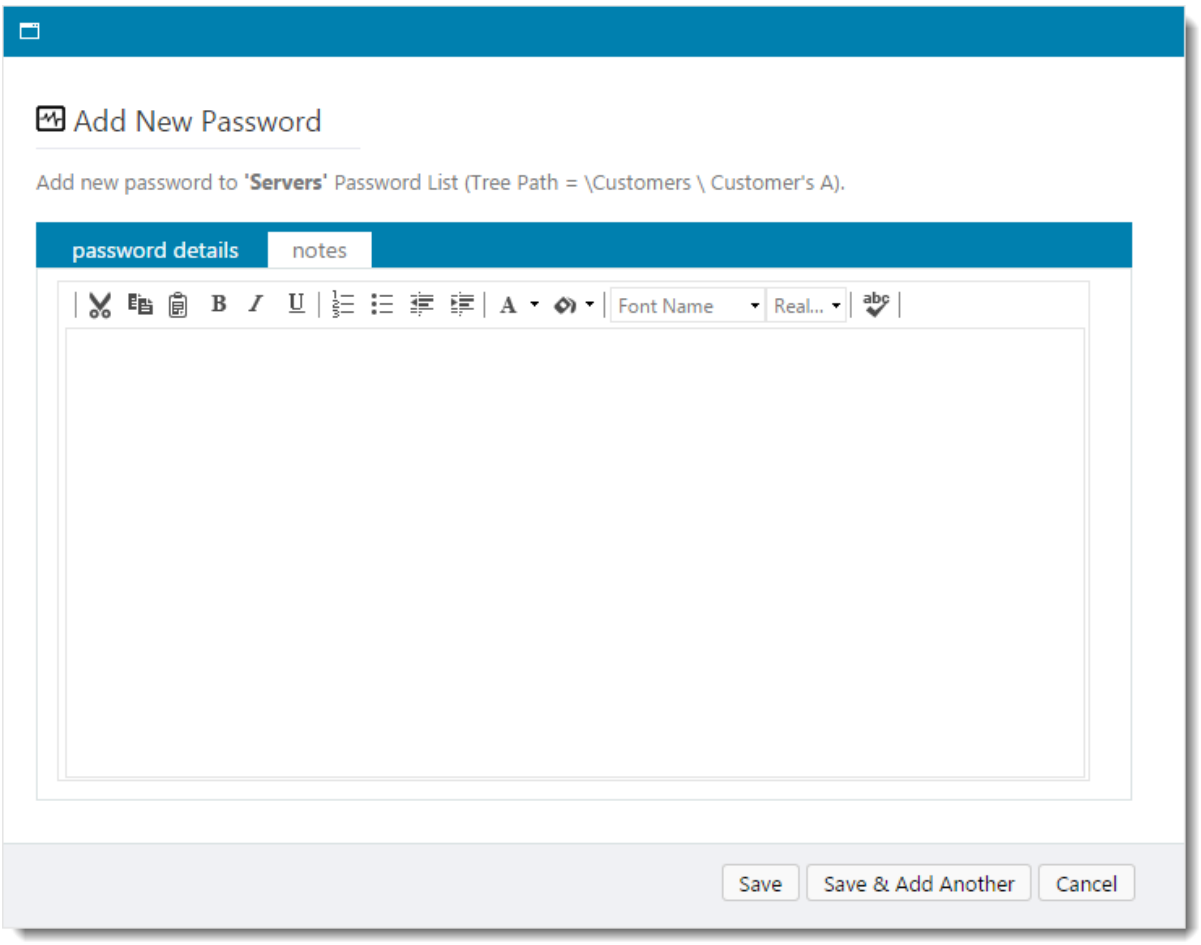
© 2017 Click Studios (SA) Pty Ltd



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.

© 2017 Click Studios (SA) Pty Ltd

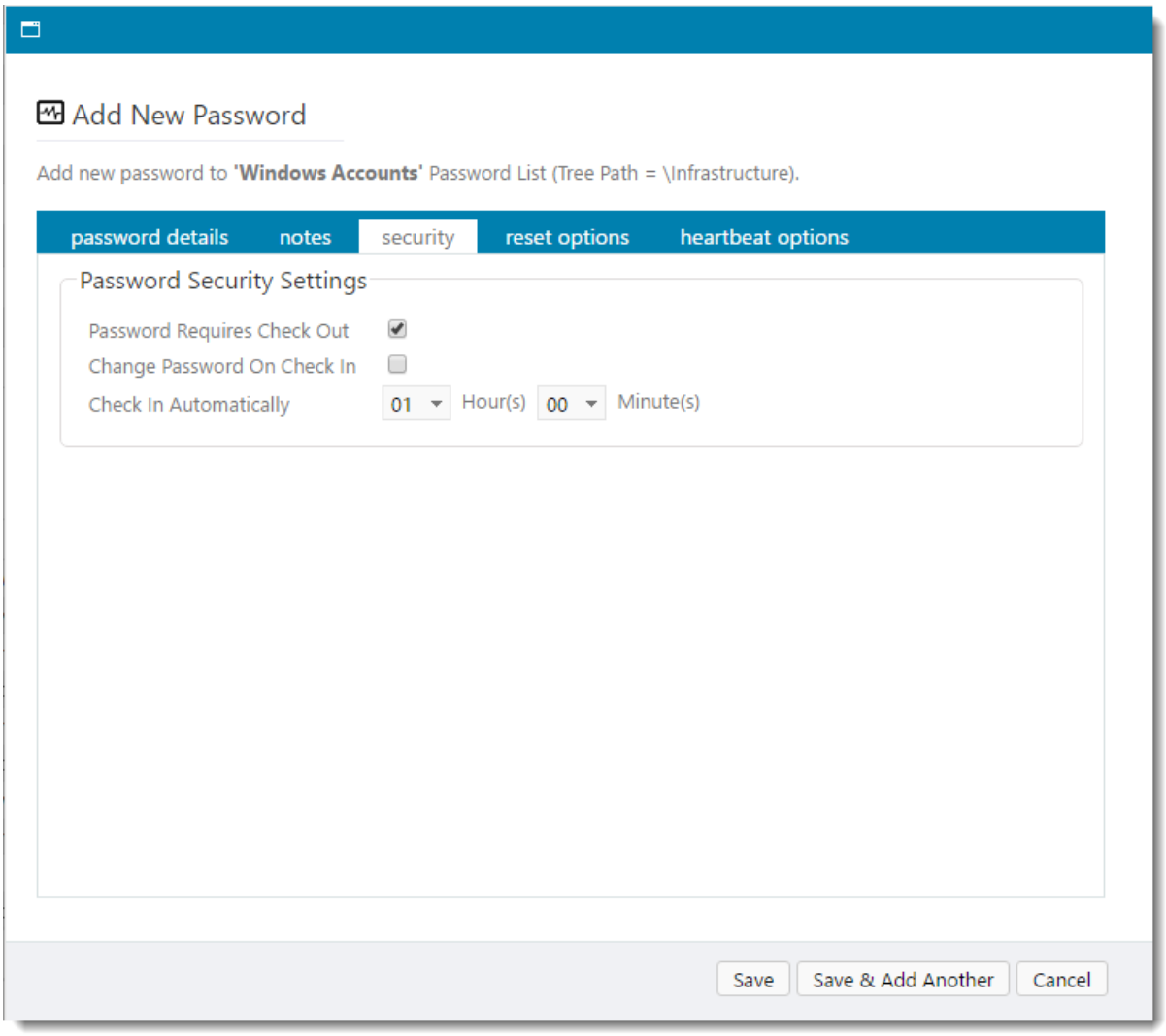


Security Tab

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

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

© 2017 Click Studios (SA) Pty Ltd



Reset Options and Heartbeat Options Tabs

The Reset Options and Heartbeat options tabs **will only be visible** if the password record has been configured to perform password resets. For a complete example of how to configure a password for resets, please read the following kb article - Password Reset Example

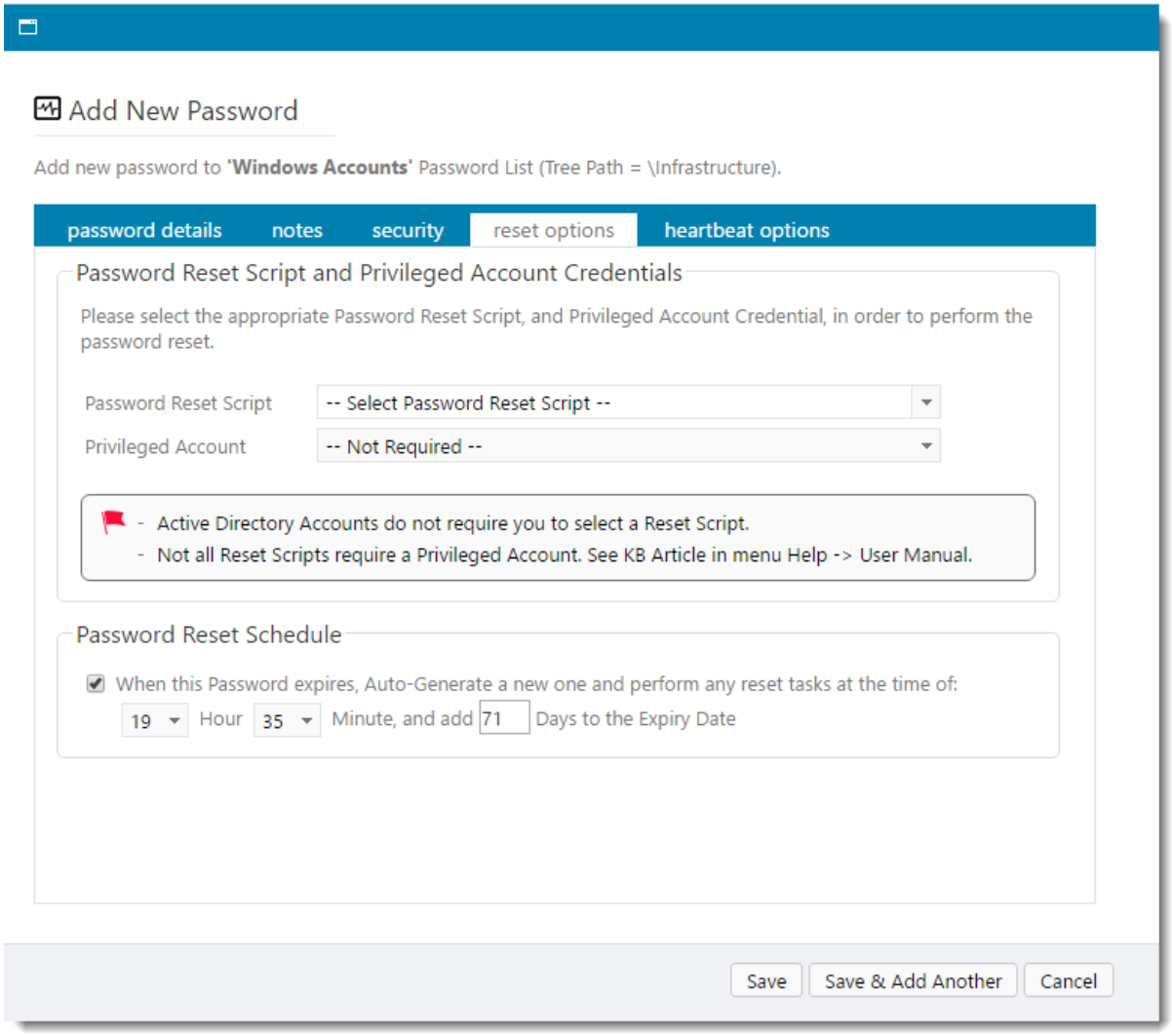
Options available are:

- The Password Reset Script to be used for this account
- The Privileged Account Credential to associate with the record so a Password Reset can occur - not all Reset Scripts require this, so please refer to the following kb article for more information - Password Reset Scripts and Requirements
- 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

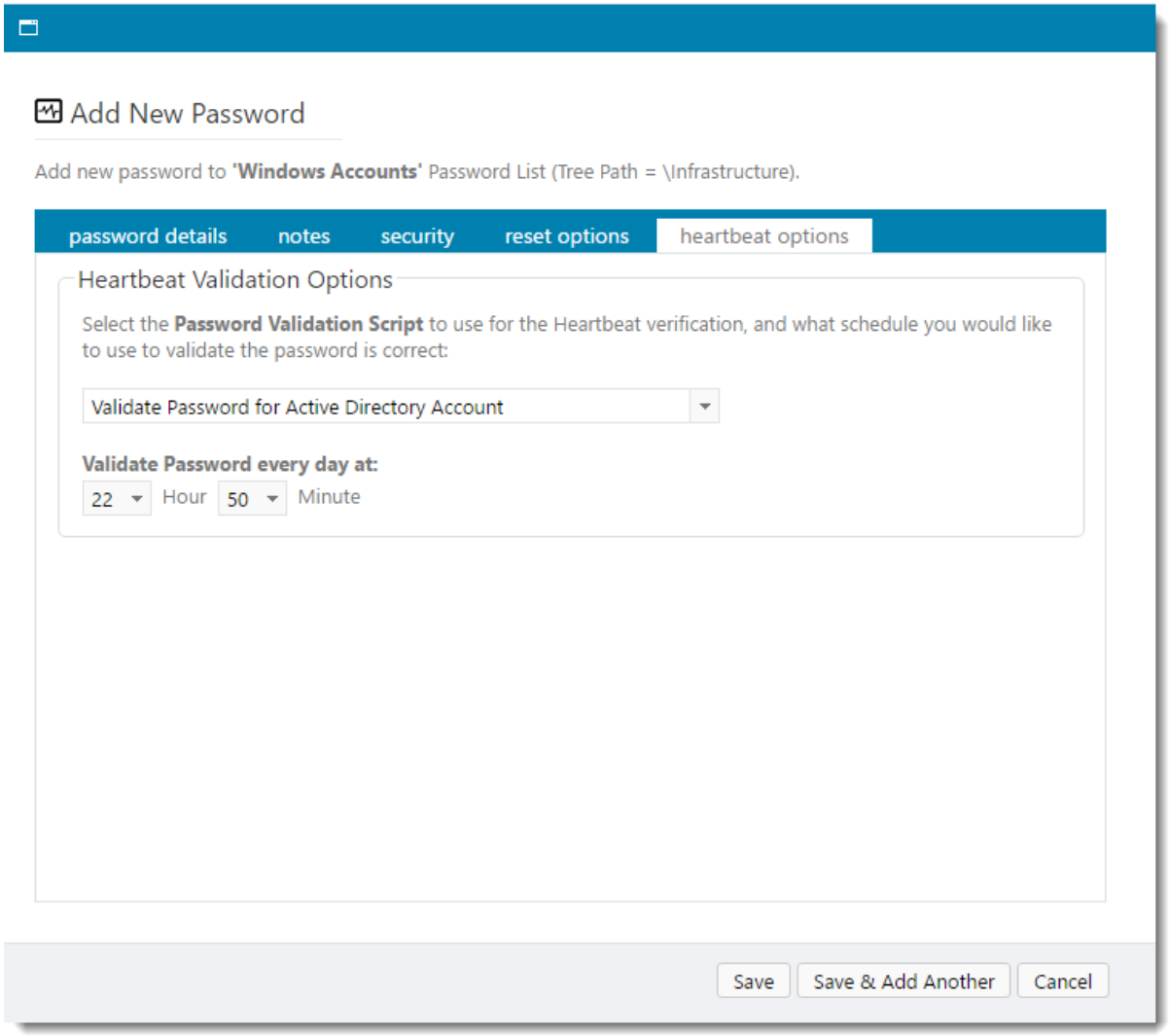
© 2017 Click Studios (SA) Pty Ltd

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

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



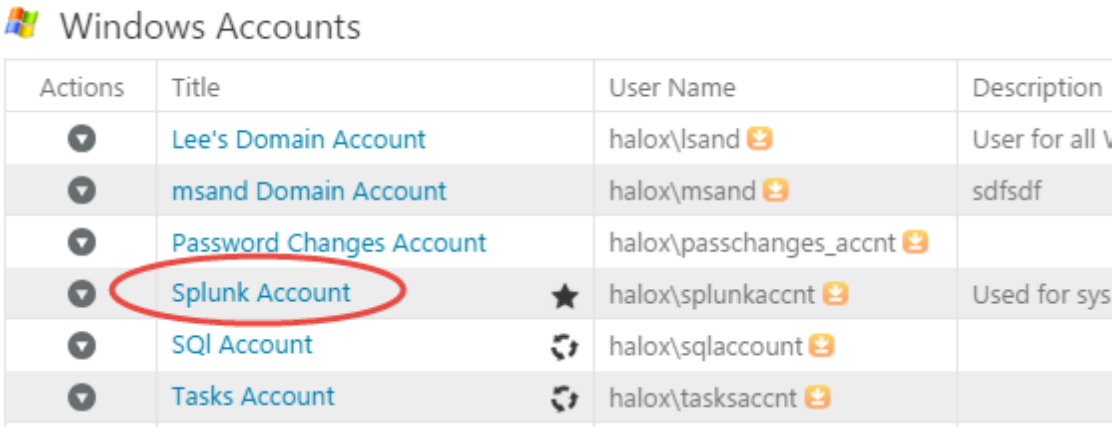
© 2017 Click Studios (SA) Pty Ltd



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.

© 2017 Click Studios (SA) Pty Ltd



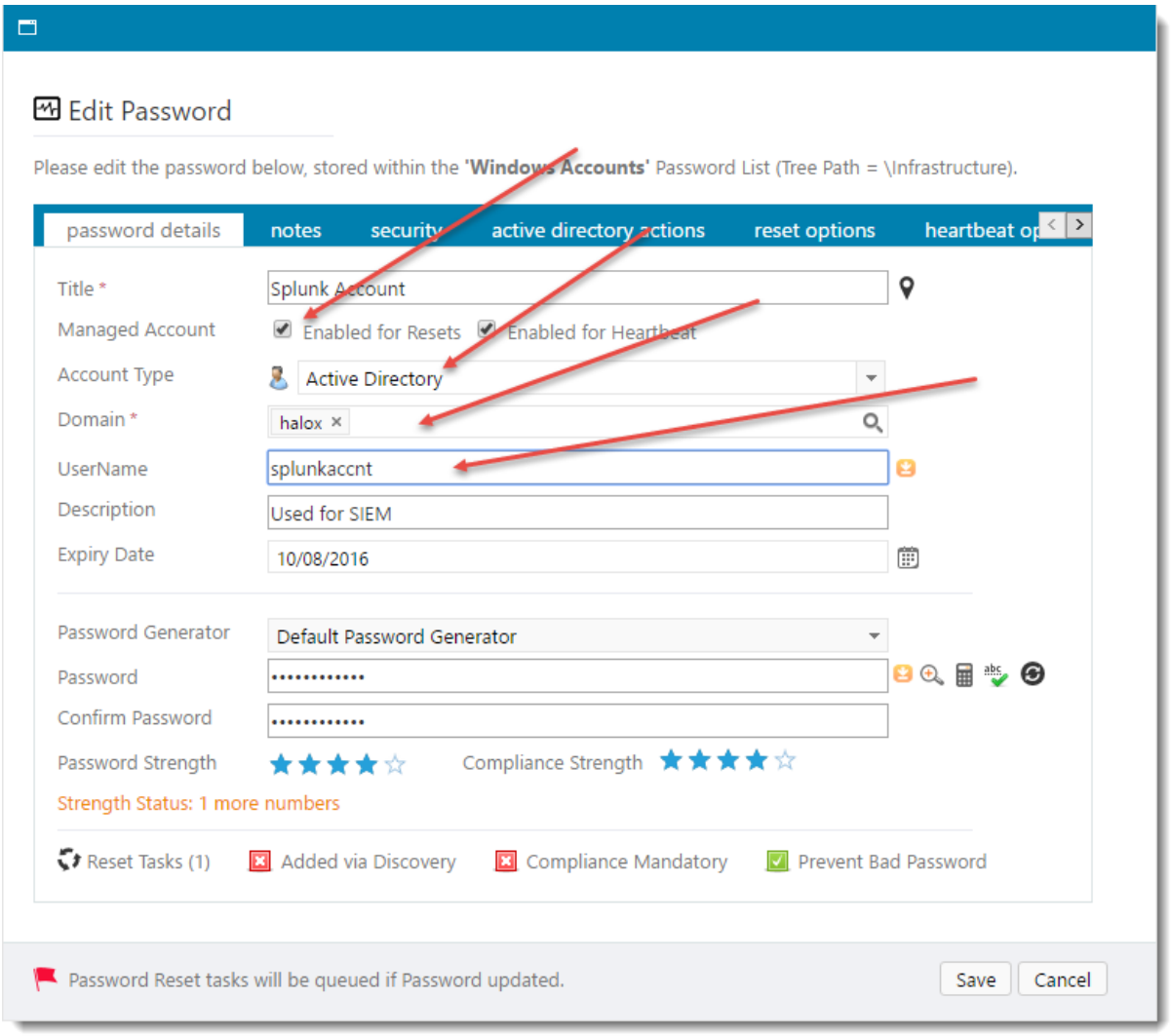
Once the Edit Password screen is open, each of the fields and options on the Tabs is similar to the Add Password screen.

Password Details tab

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

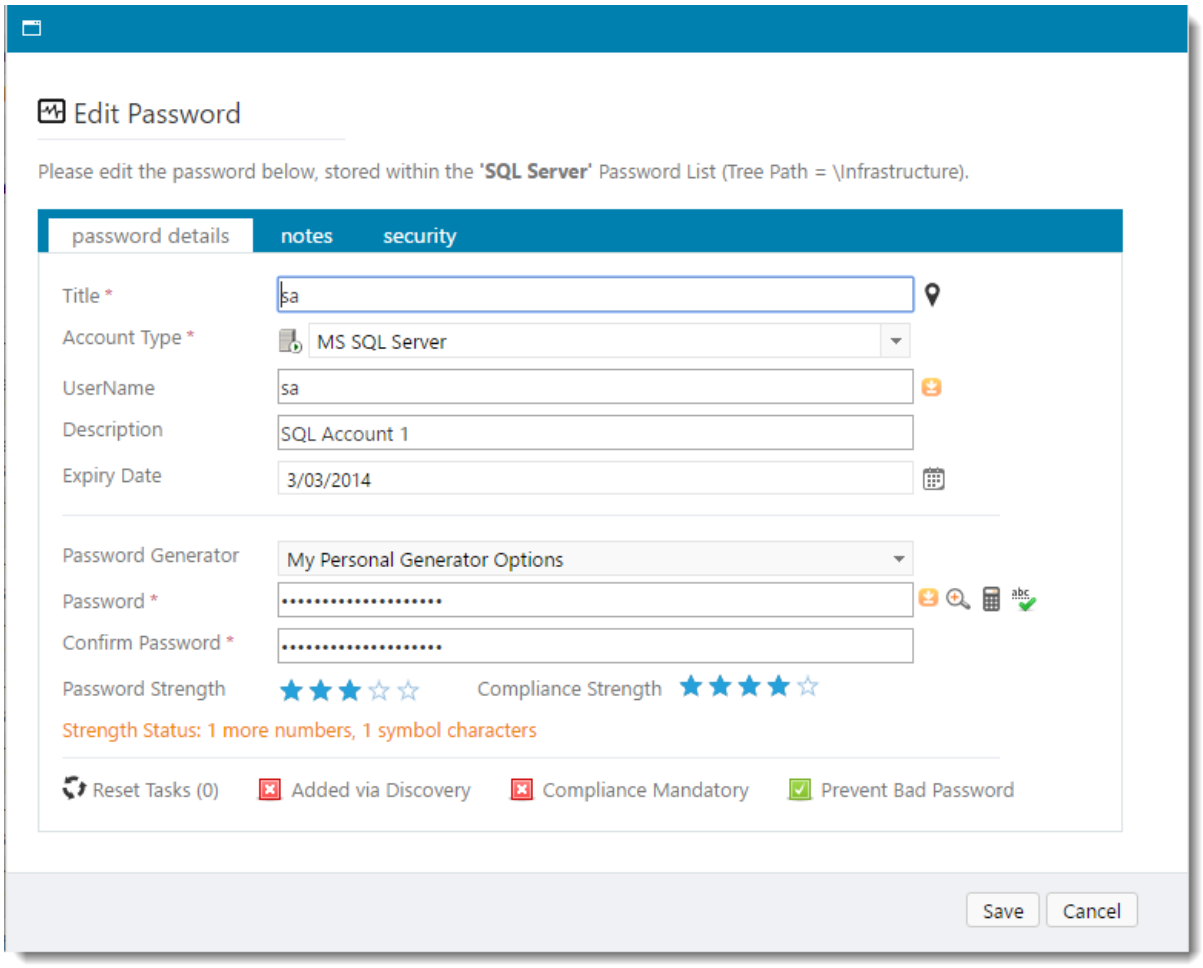
Note: Please refer to the KB Article Password Resets Explained for all the detail and requirements for resetting passwords on remote hosts

© 2017 Click Studios (SA) Pty Ltd



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

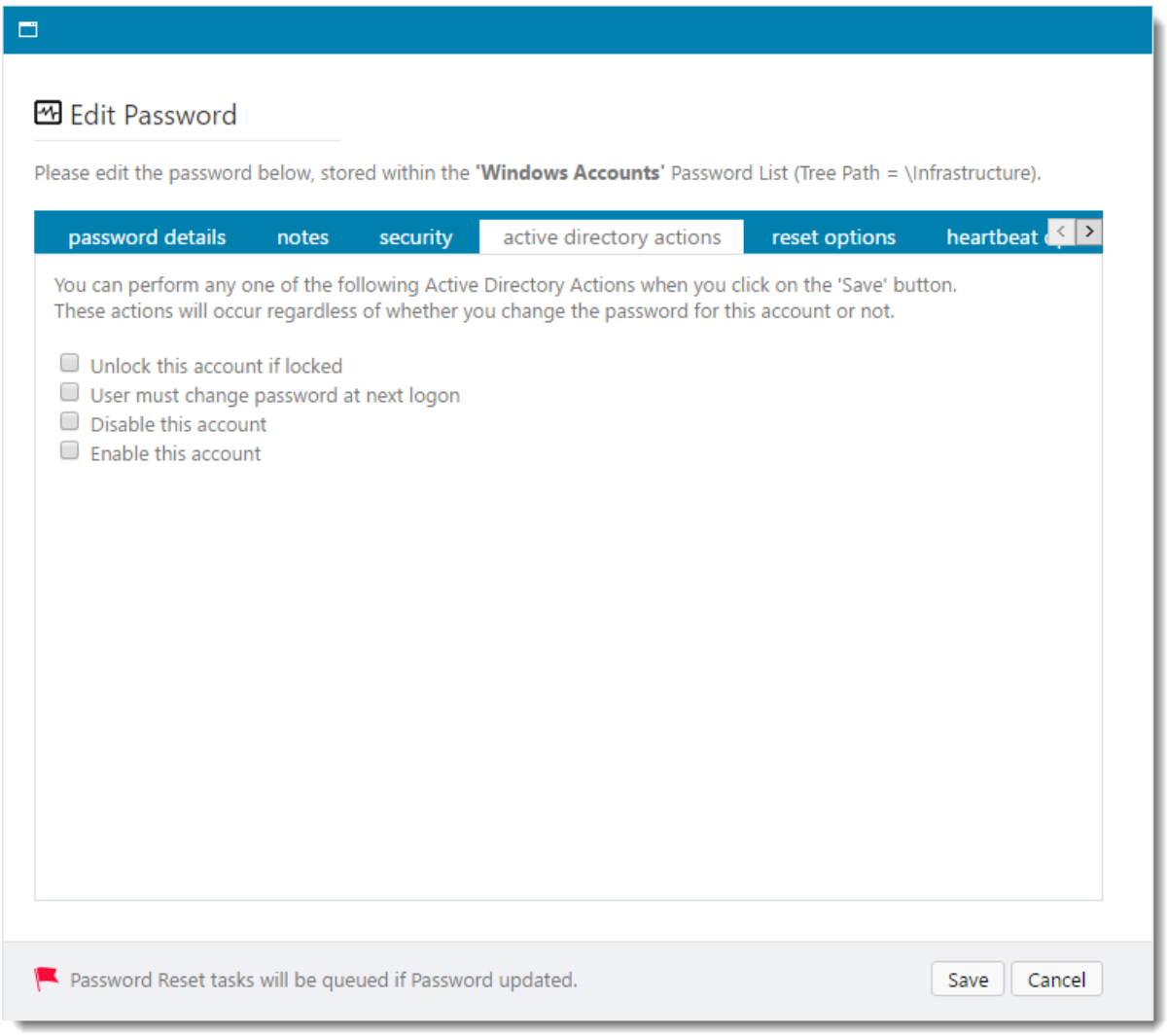
© 2017 Click Studios (SA) Pty Ltd



Active Directory Actions tab

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

© 2017 Click Studios (SA) Pty Ltd



Reset Options and Heartbeat Options Tabs

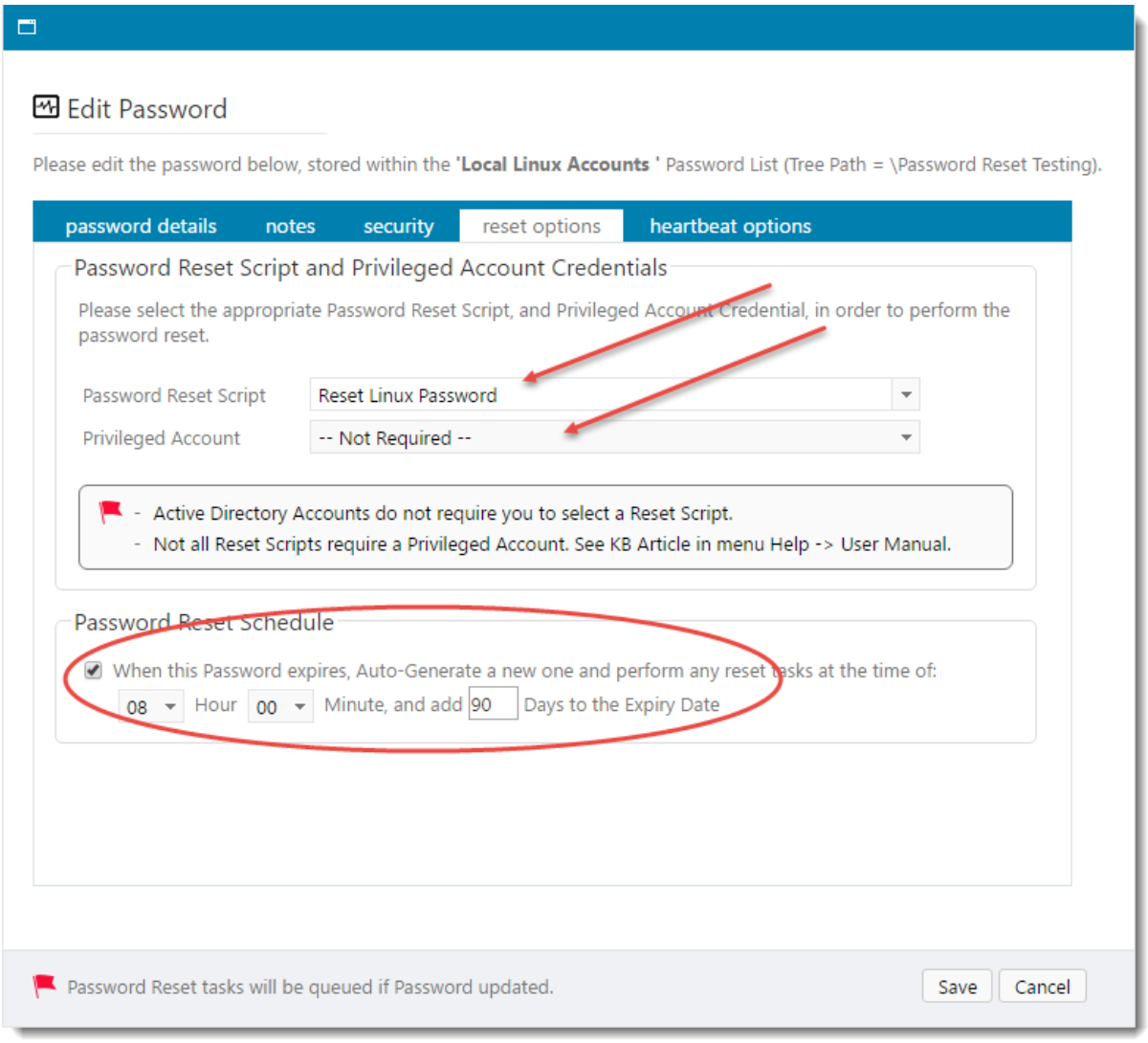
The Reset Options and Heartbeat options tabs **will only be visible** if the password record has been configured to perform password resets. For a complete example of how to configure a password for resets, please read the following kb article - Password Reset Example

Options available are:

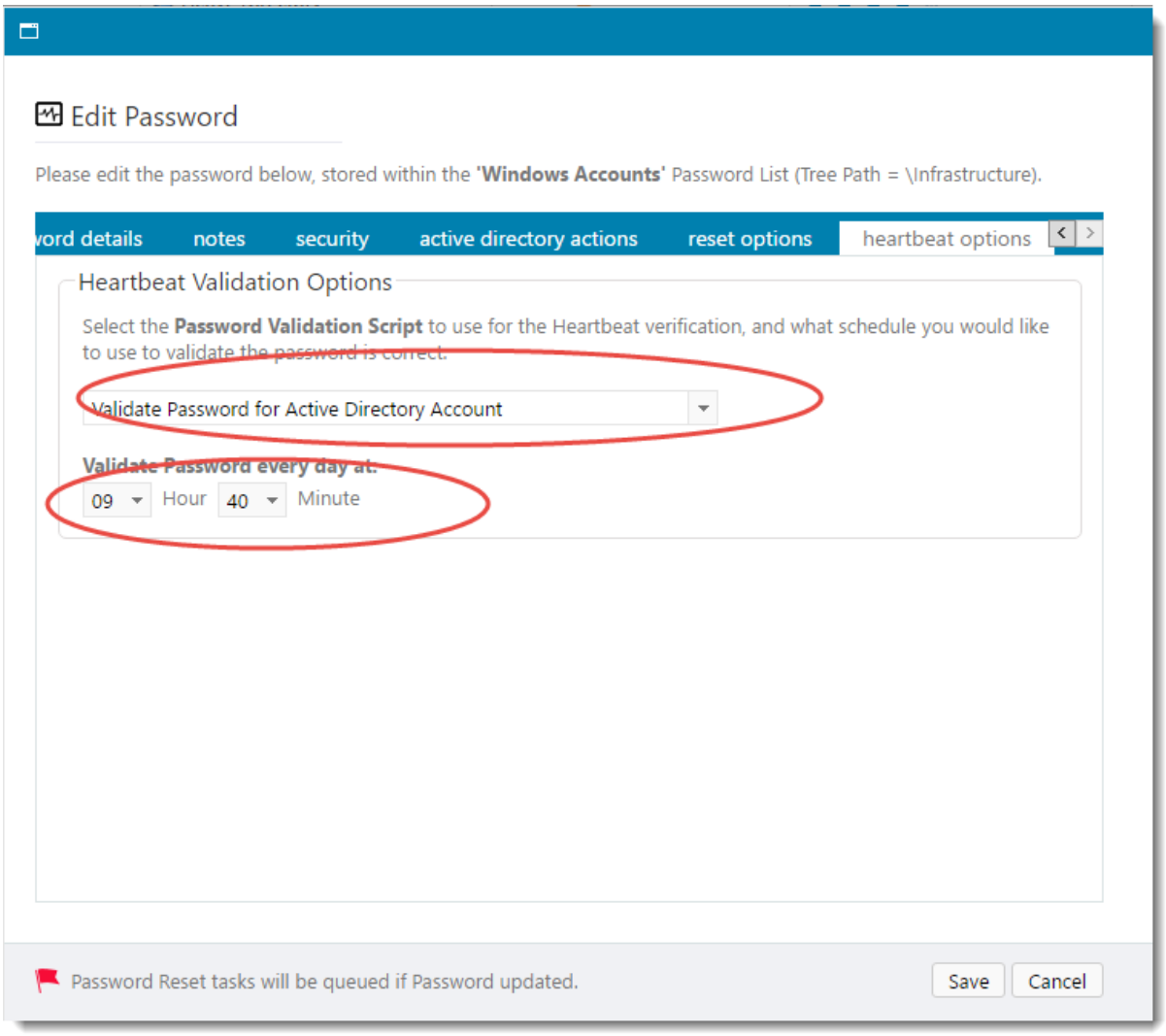
- The Privileged Account Credential to associate with the record so a Password Reset can occur - not all Reset Scripts require this, so please refer to the following kb article for more information - Password Reset Scripts and Requirements
- Whether or not to auto-generate a new password for the record
- At what time of the day should the password be reset, once the Expiry Date has been reached
- How many days should be added to the Expiry Date field, once the password has been automatically reset
- And what Validation Script and schedule to use for the Heartbeat process

© 2017 Click Studios (SA) Pty Ltd

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



© 2017 Click Studios (SA) Pty Ltd



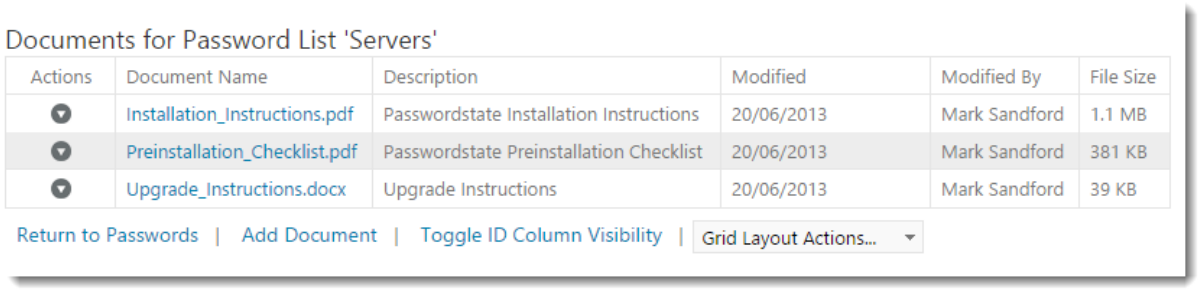
2.1.3.4 Upload Documents

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. Uploaded documents are also encrypted within the database, using the same type of 256bit AES encryption as other encrypted data.

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

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

© 2017 Click Studios (SA) Pty Ltd

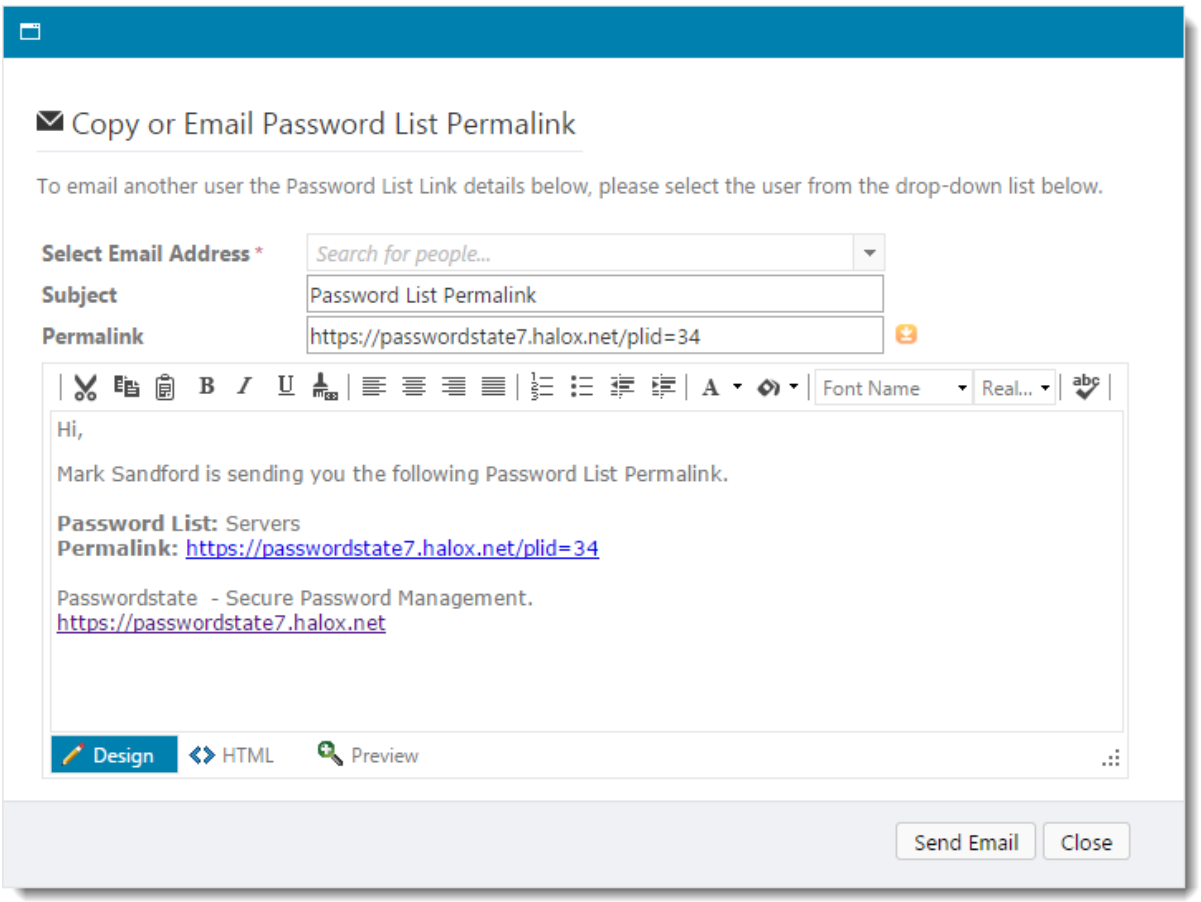


2.1.3.5 Email Permalinks

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

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

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



© 2017 Click Studios (SA) Pty Ltd

2.1.3.6 Password Actions

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

Check-In Password	Allows a user to check a record back in, after they have checked it out for exclusive use
Copy or Email Password Permalink	Similar to Permalinks for Password Lists, you can also copy or email Permalinks for individual Password records
Copy or Move to Different Password List	It's also possible to copy or move individual Password records between Password Lists, and it's even possible to link them - so all changes are synchronized between Password Lists
Delete	When you delete an individual Password record, it is moved to the Recycle Bin for the Password List. Administrators of the Password List can restore back from the Recycle Bin if required
Expire Password Now	Selecting 'Expire Password Now' for an individual Password record, will set it's Expiry Date field to the current date, and trigger any associated Password Reset tasks as well
Filter Recent Activity on this Record	If you need a quick method of filtering the audit data (Recent Activity) for an individual Password record, you can use the 'Filter Recent Activity on this Record' menu option
Remote Session Launcher with these Credentials	This menu option allows you to use the password credentials to launch a Remote Session to a designated host.
Send Account Heartbeat Request	If the password record has the option enabled to perform account Heartbeats, to validate the password is correct against the remote Host or Active Directory, then you can use this menu option to perform the validation real-time.
Send Self Destruct Message	This menu option allows you to send a Self Destruct Message, with the contents being details for the selected Password record.
Toggle Favorite Status	If you have Password records which you use frequently, you can tag them as your favorites and they will show up in the 'Favorite Passwords' grids on the Password Home page, or any of the Password Folder pages. A Favorite password is also denoted by the ★ icon on the Passwords grid
View & Compare History of Changes	Every change made to a Password record retains a history

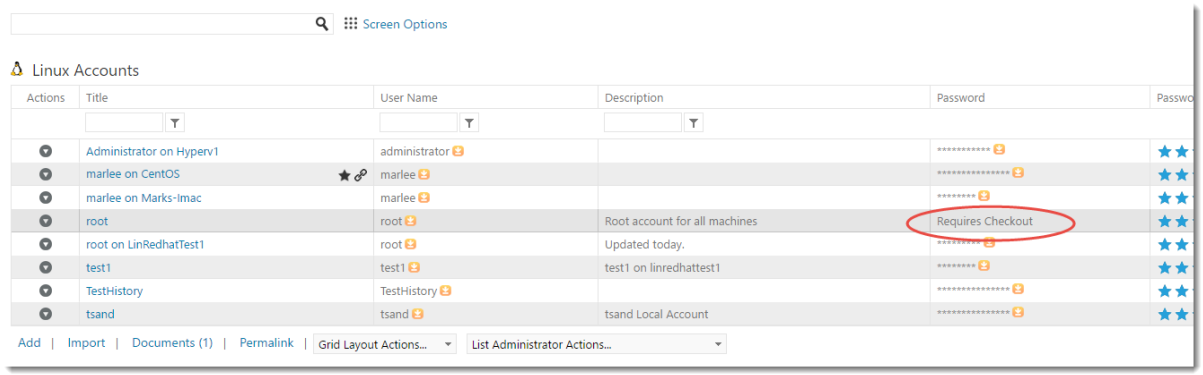
© 2017 Click Studios (SA) Pty Ltd

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

2.1.3.6.1 Check-In Password

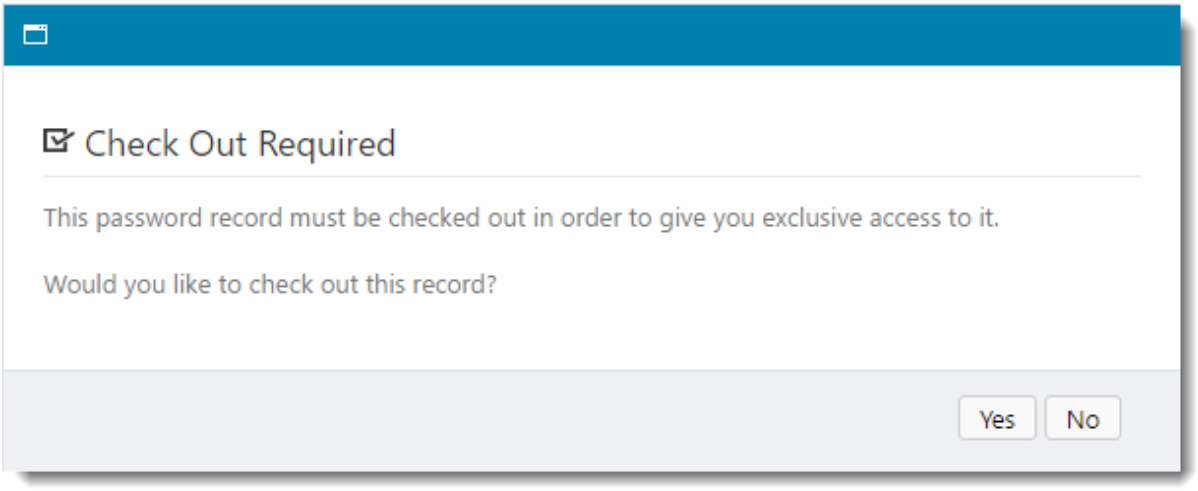
When a password is configure to require exclusive access via the Check-In/Check-Out process, and menu item called 'Check-In Password' will be visible when the password is checked out. This menu item will only be available to the user who checked the record out.

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

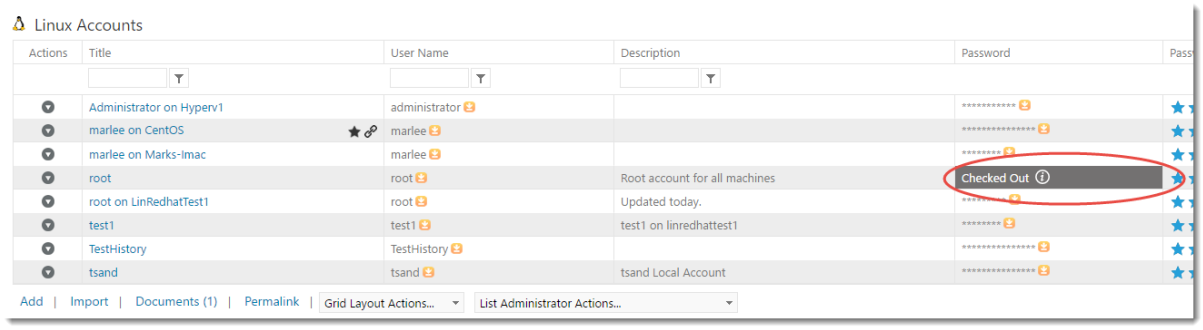


When you click on the Title for the record to access it, you will be asked to check the record out.

© 2017 Click Studios (SA) Pty Ltd

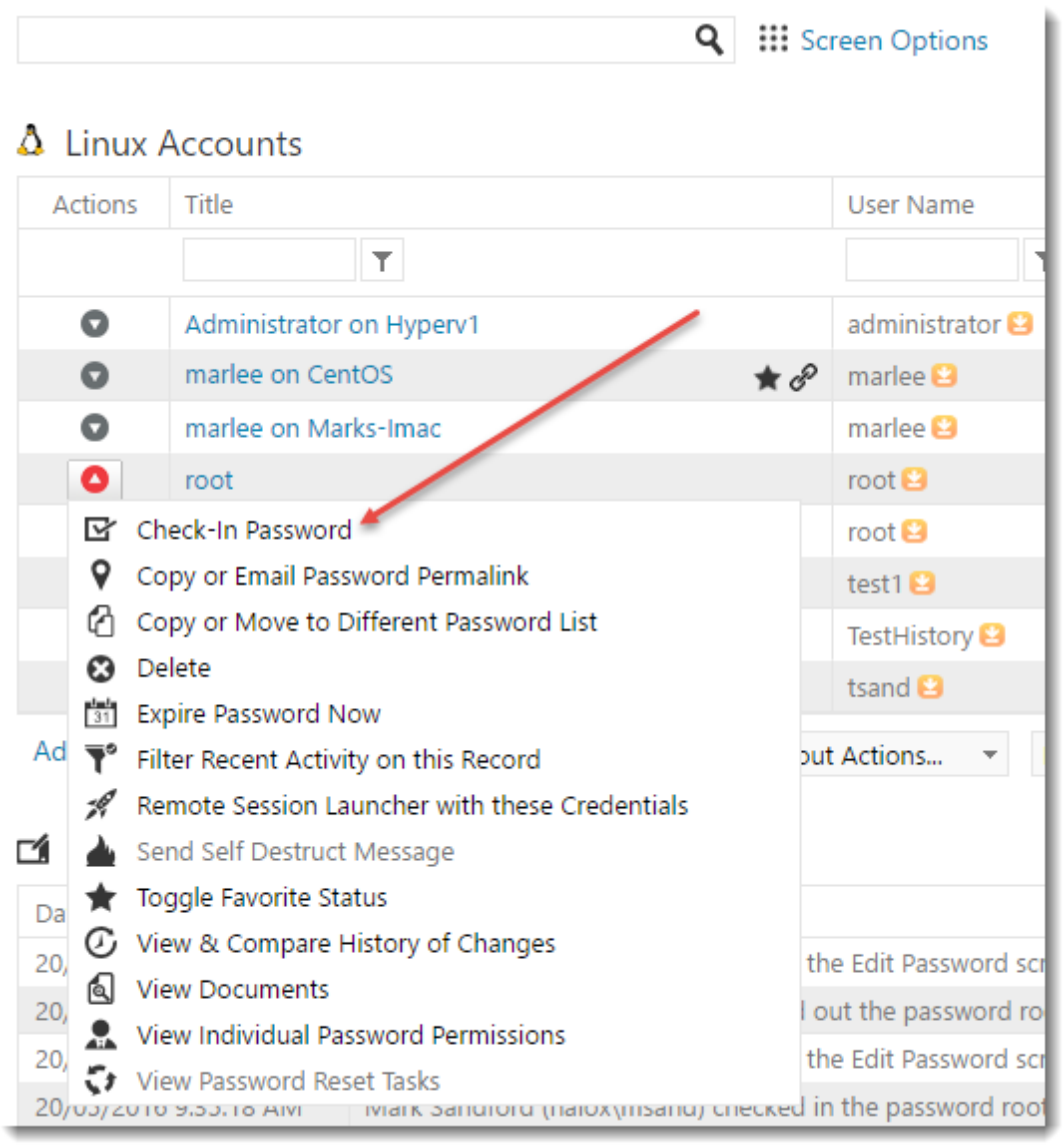


When checked out, it also indicates this in the password grid, and no other users can access the password until it is checked back in.



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

© 2017 Click Studios (SA) Pty Ltd

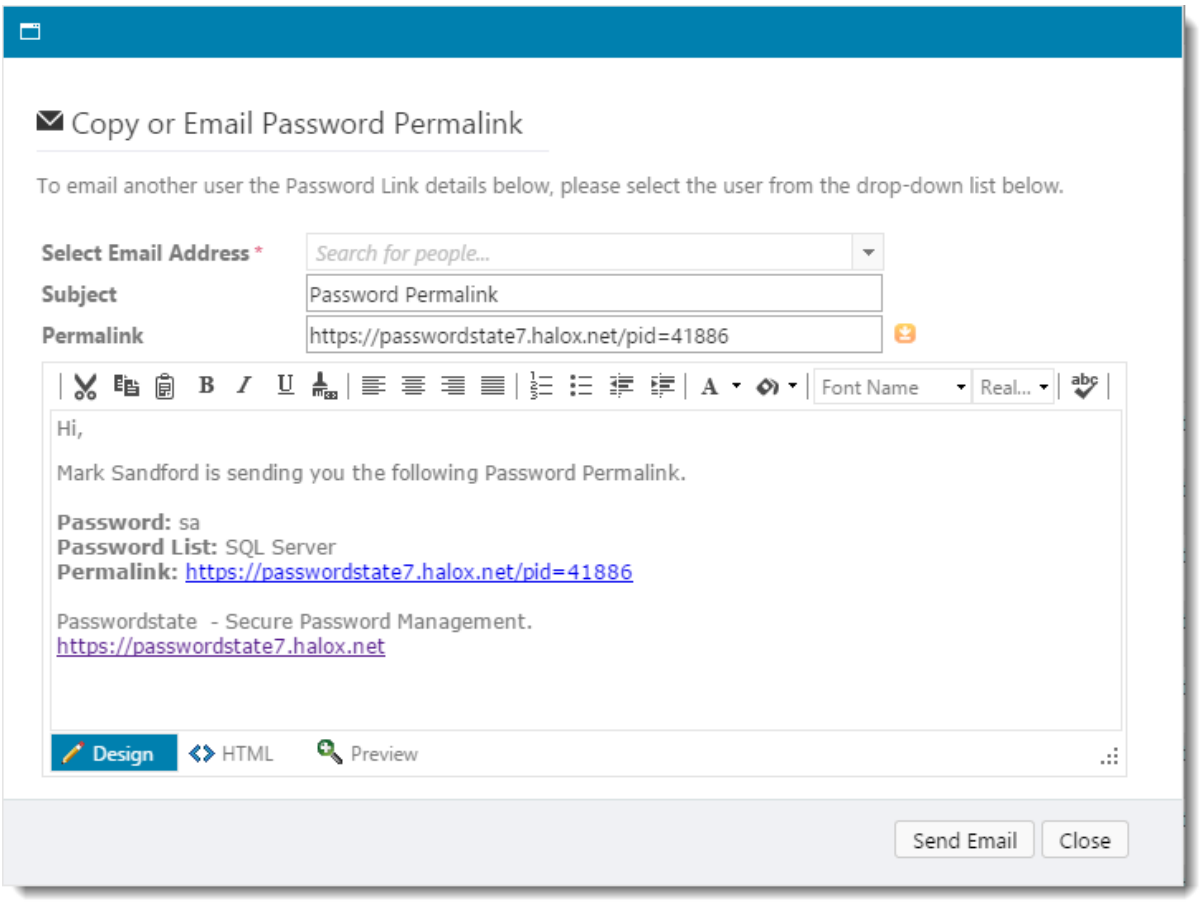


2.1.3.6.2 Copy or Email Password Permalink

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

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

© 2017 Click Studios (SA) Pty Ltd



2.1.3.6.3 Copy or Move to Different Passw ord List

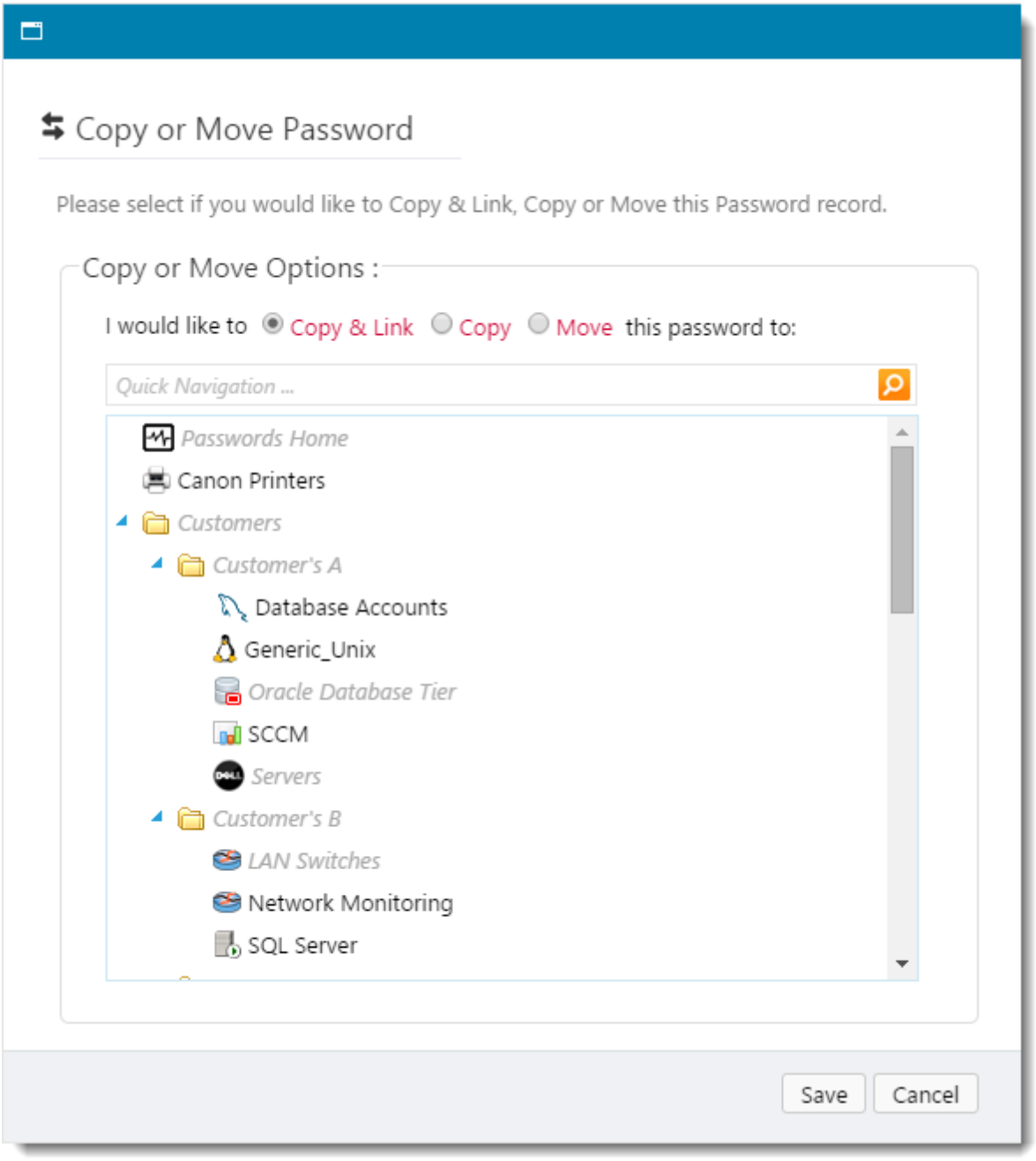
It is possible to copy or move a Password record to a different Password List, but there are a couple of exceptions which may prevent you from doing this:

- 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.

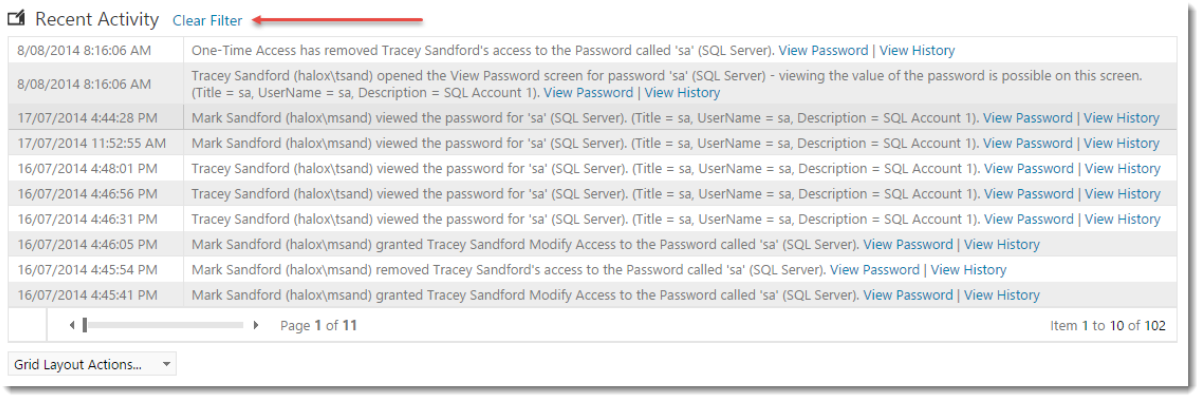
© 2017 Click Studios (SA) Pty Ltd



2.1.3.6.4 Filter Recent Activity on this Record

Sometimes it might be useful to quickly filter all the auditing data on information relevant to a single Password. When selecting 'Filter Recent Activity on this Record', all contents of the Recent Activity grid will be filtered, and the 'Clear Filter' button will be displayed, allowing you to remove the filter.

© 2017 Click Studios (SA) Pty Ltd

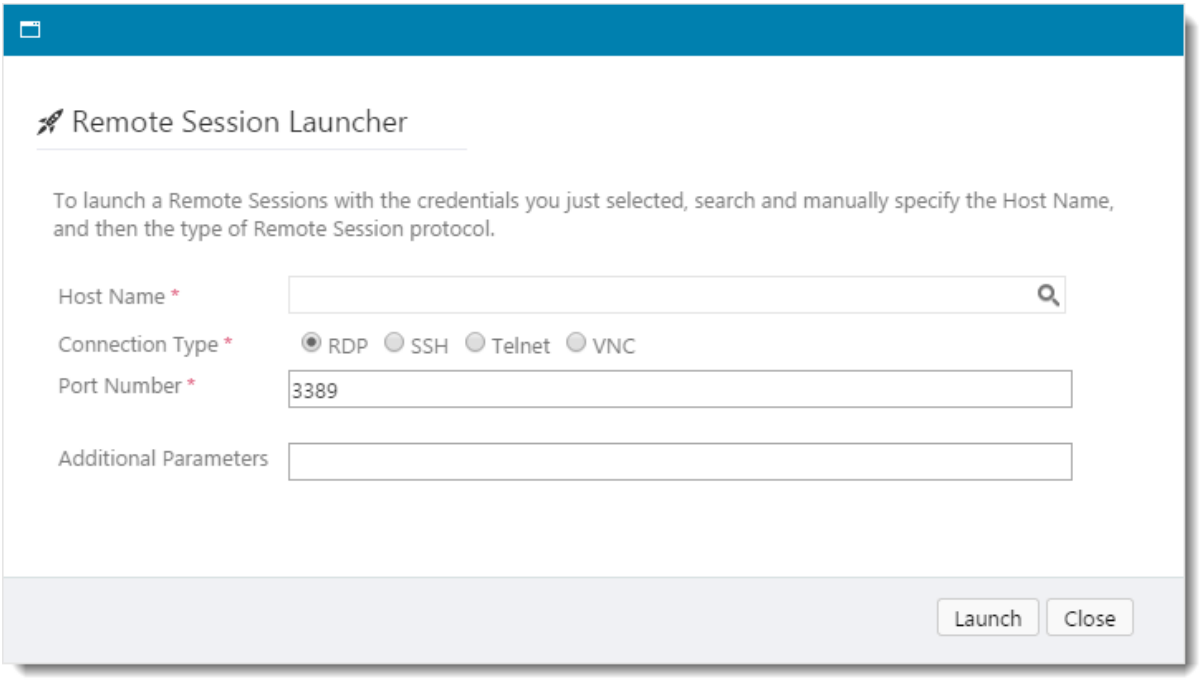


2.1.3.6.5 Remote Session Launcher with these Credentials

This menu option allows you to use the password credentials to launch a Remote Session to a designated host.

You can either search for a Host that you already have access to, or you can type in the name of the Host manually.

Note 1: Search for the Host also searches the Tag field for the Host as well.
Note 2: This menu option can be hidden on the screen Administration -> System Settings -> Password Options tab



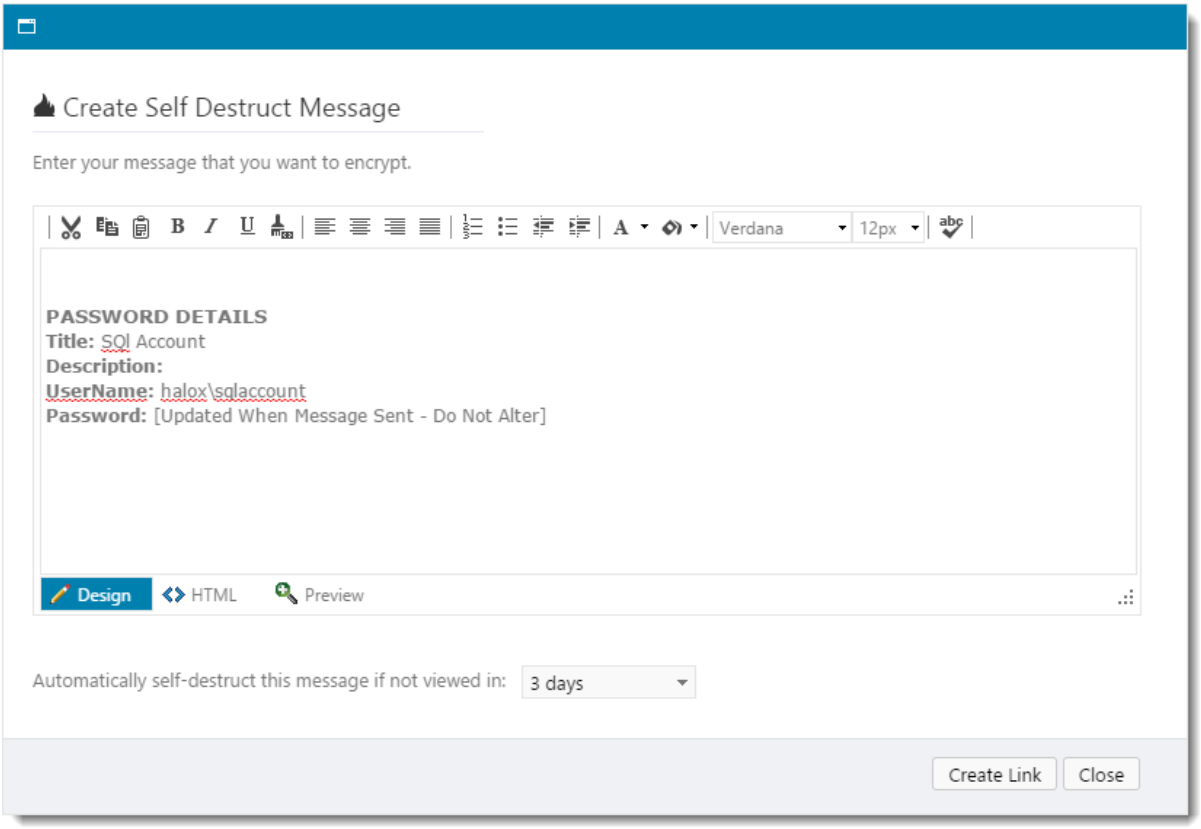
2.1.3.6.6 Send Self Destruct Message

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

© 2017 Click Studios (SA) Pty Ltd

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

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



2.1.3.6.7 View & Compare History of Changes

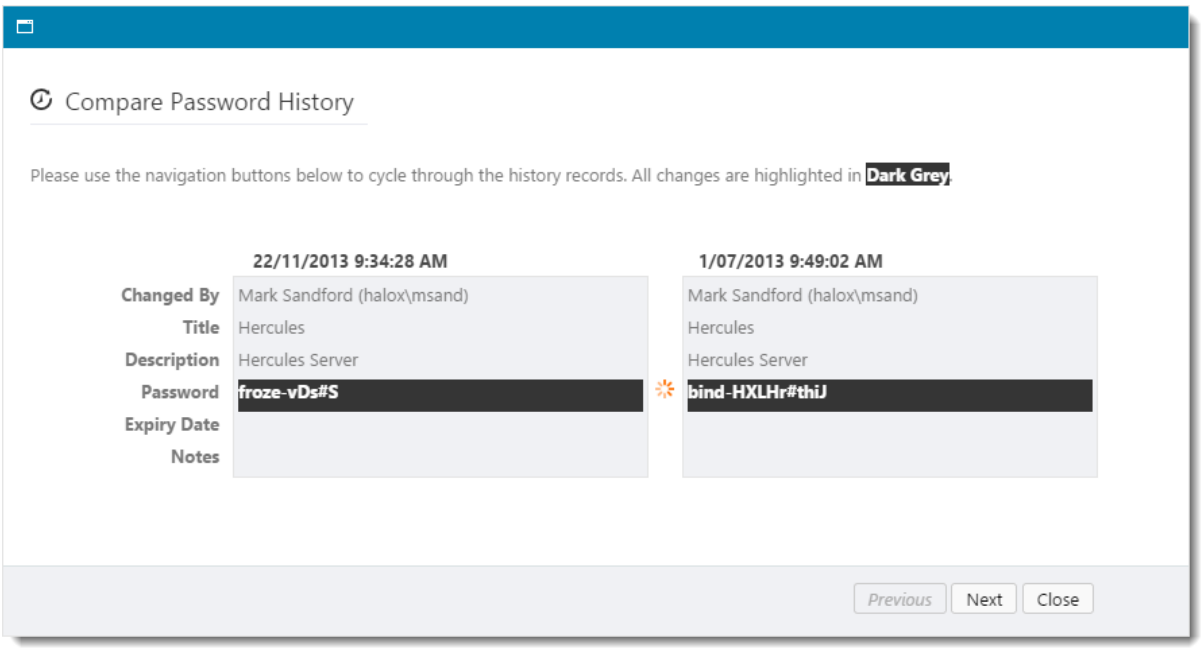
Any changes made to a Password record will not only generate an audit log record, but also the history of changes will be maintained so you can easily compare what has change, when, and by whom

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

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

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

© 2017 Click Studios (SA) Pty Ltd

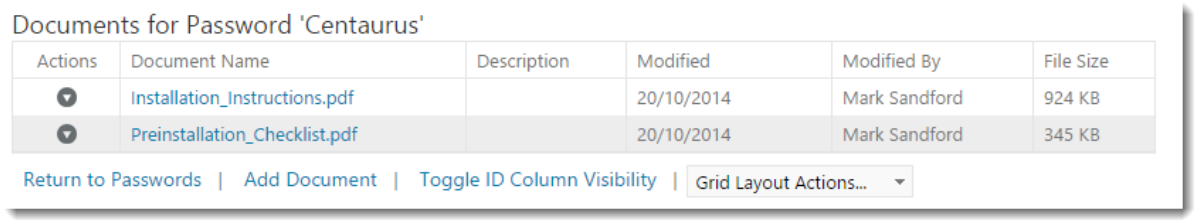


2.1.3.6.8 View Documents

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

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

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



2.1.3.6.9 View Individual Password Permissions

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

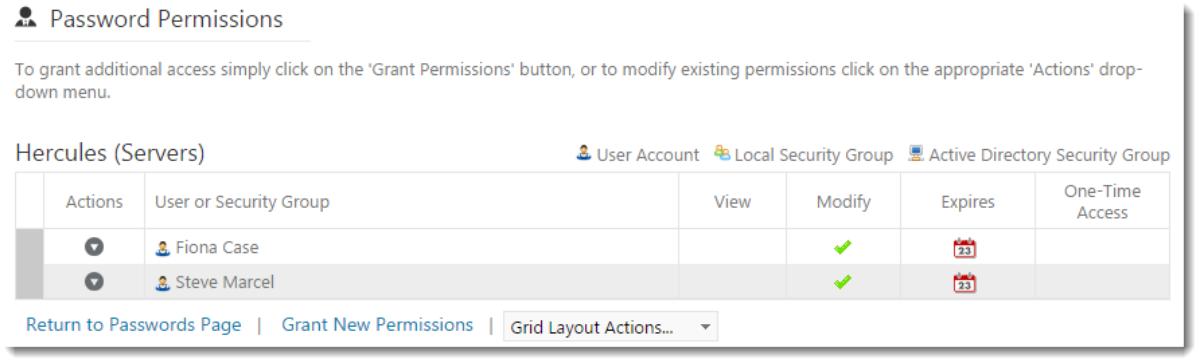
When you click on the 'View Individual Password Permissions' menu item, you will be directed to a screen which shows what permissions have been applied to the individual Password record.

© 2017 Click Studios (SA) Pty Ltd

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



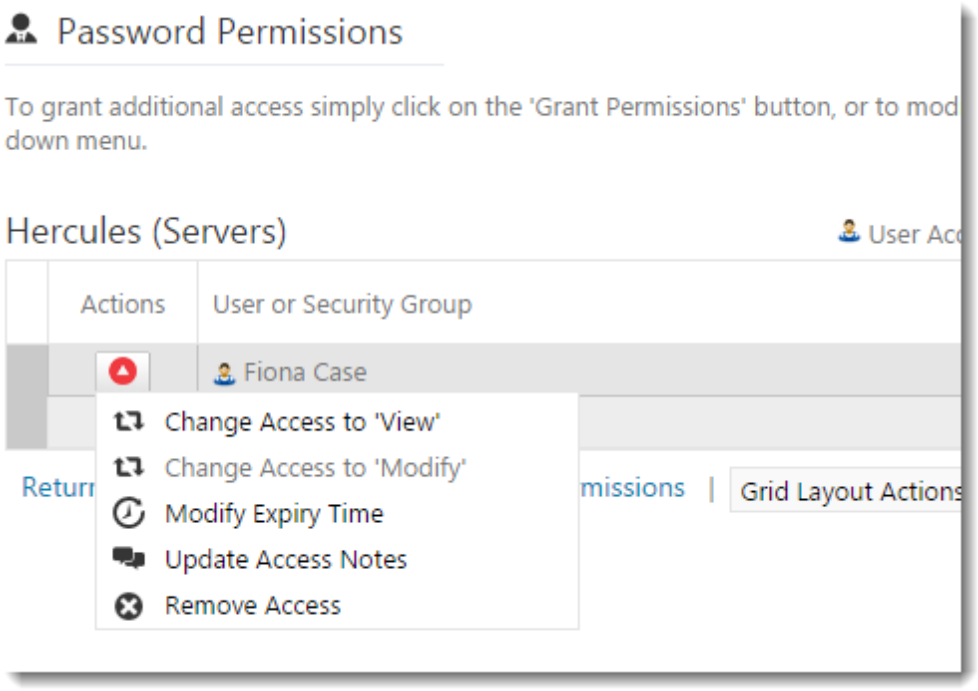
From the 'View Individual Password Permissions' screen, you have the following features available:

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

© 2017 Click Studios (SA) Pty Ltd



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.

2.1.3.6.9.1 Grant New Permissions

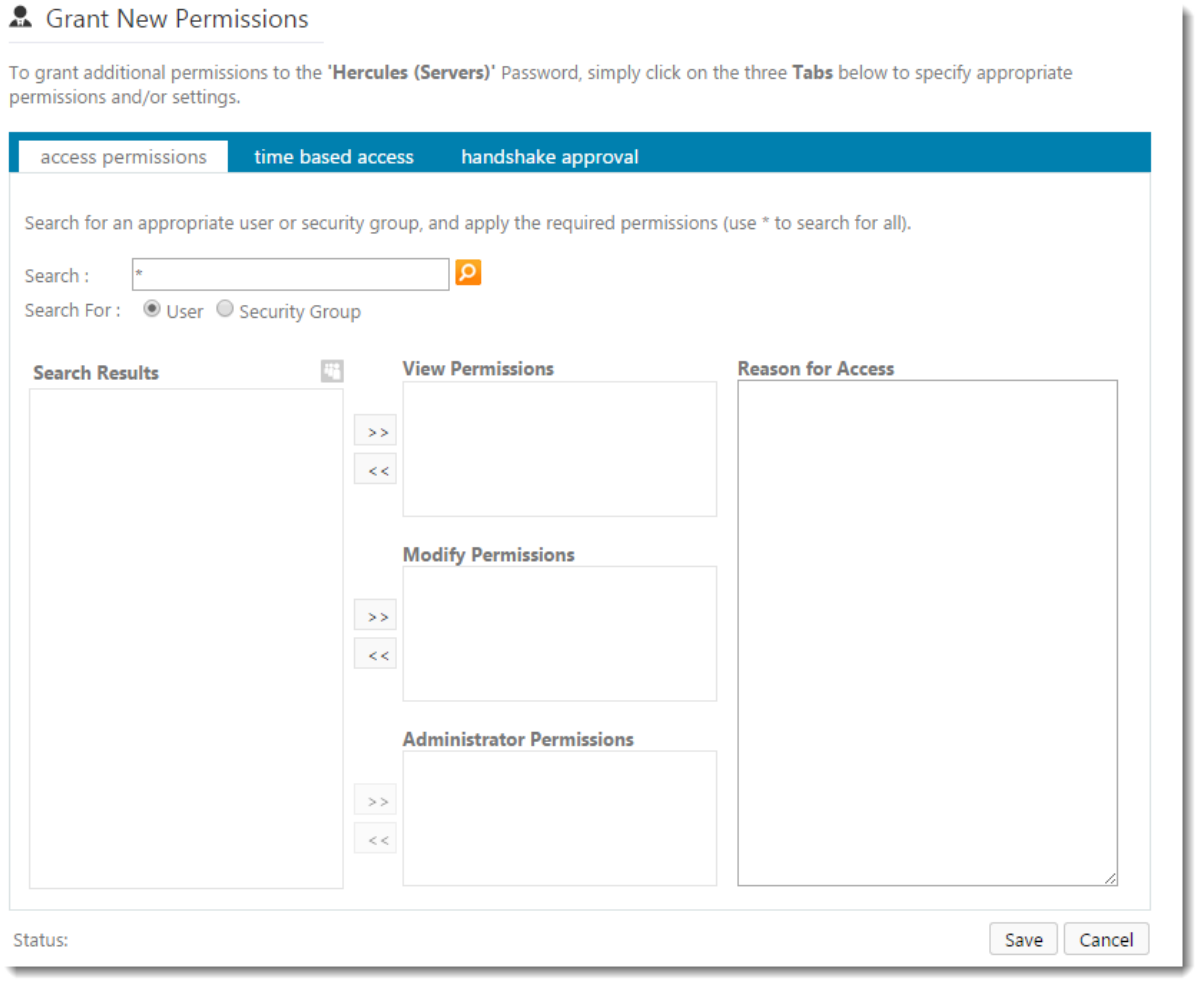
When granting new permissions (access) to a Password record, there are three tabs of features available to you:

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

© 2017 Click Studios (SA) Pty Ltd

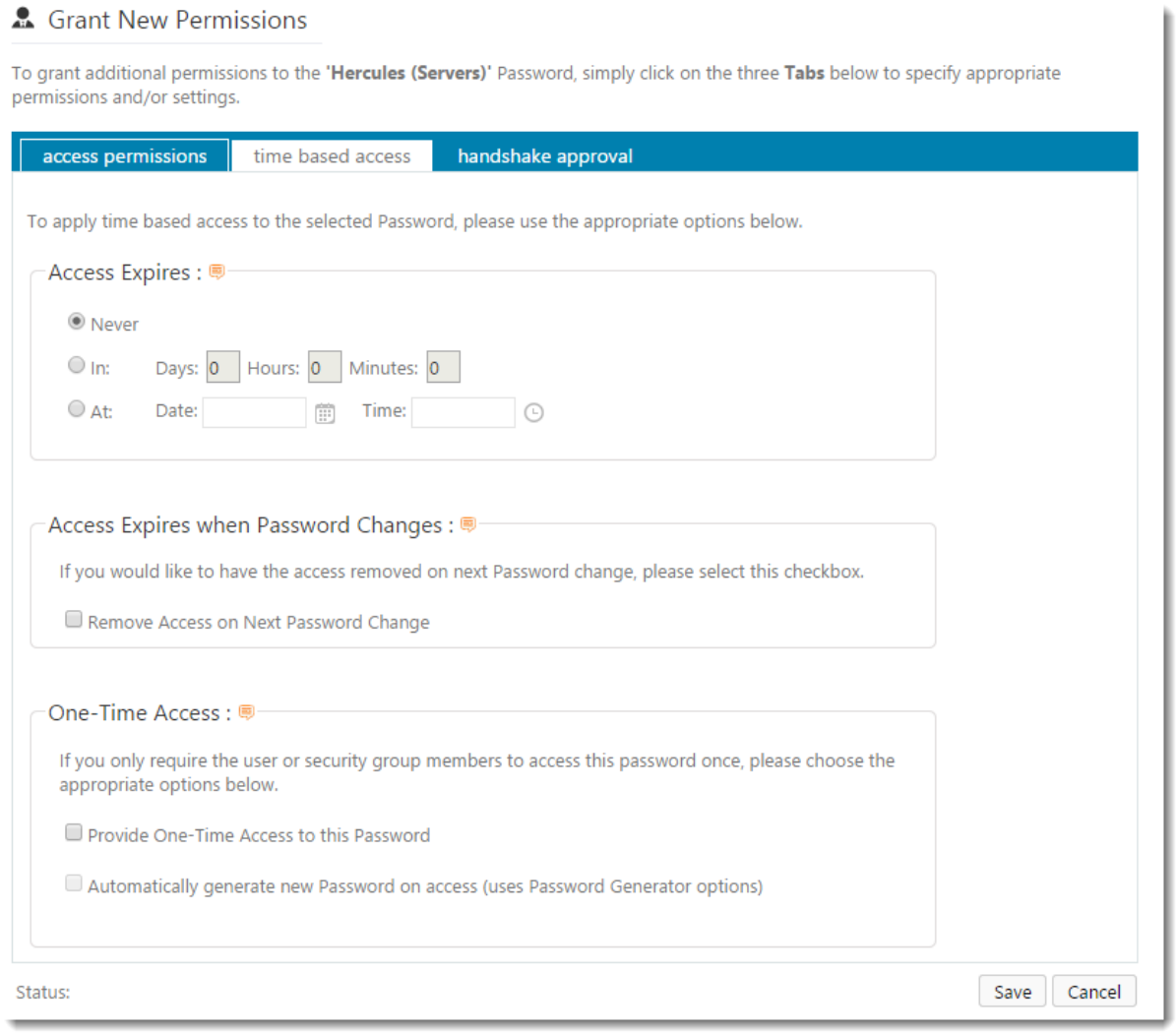


Time Based Access

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.

© 2017 Click Studios (SA) Pty Ltd

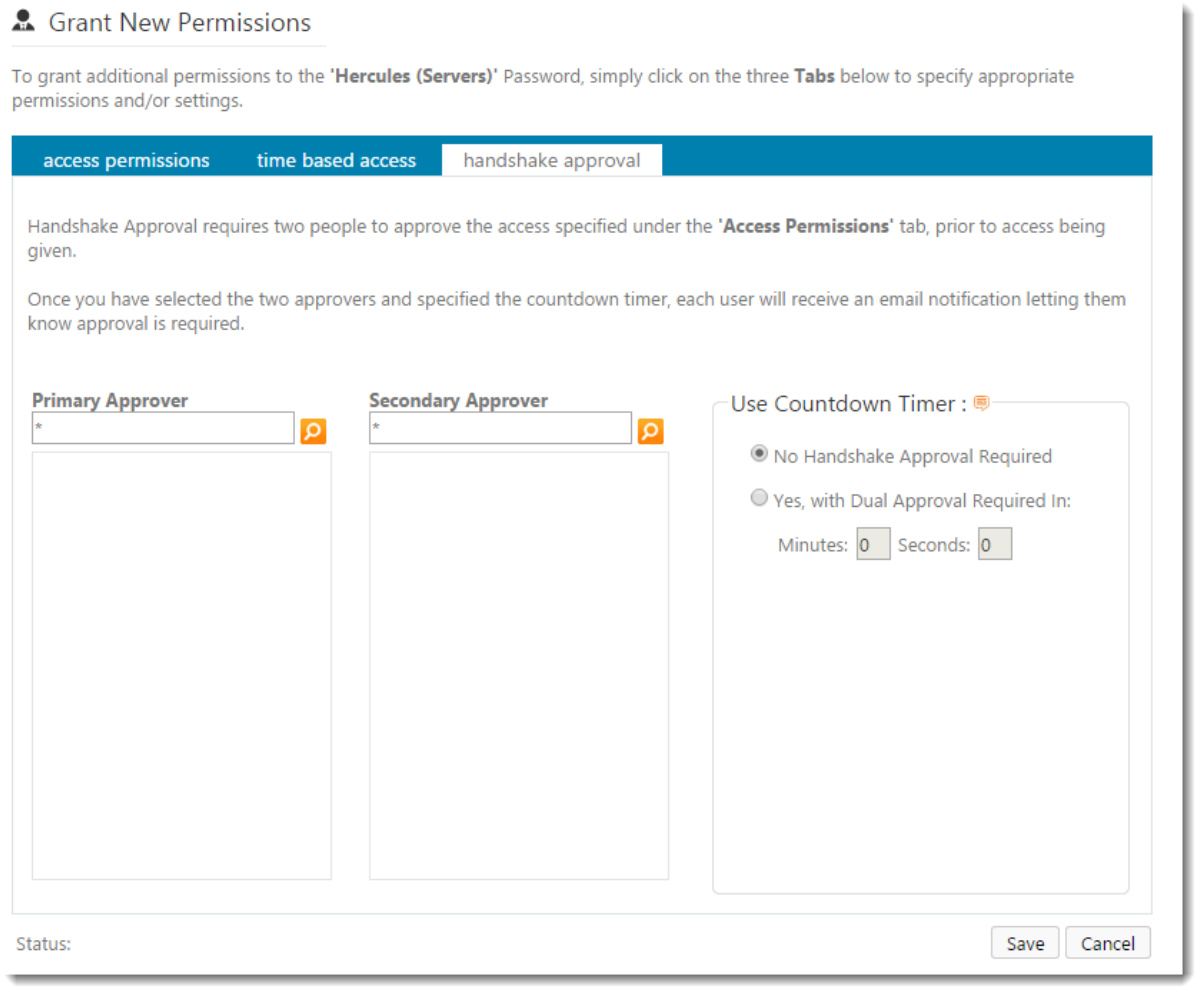


Handshake Approval

'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.

© 2017 Click Studios (SA) Pty Ltd

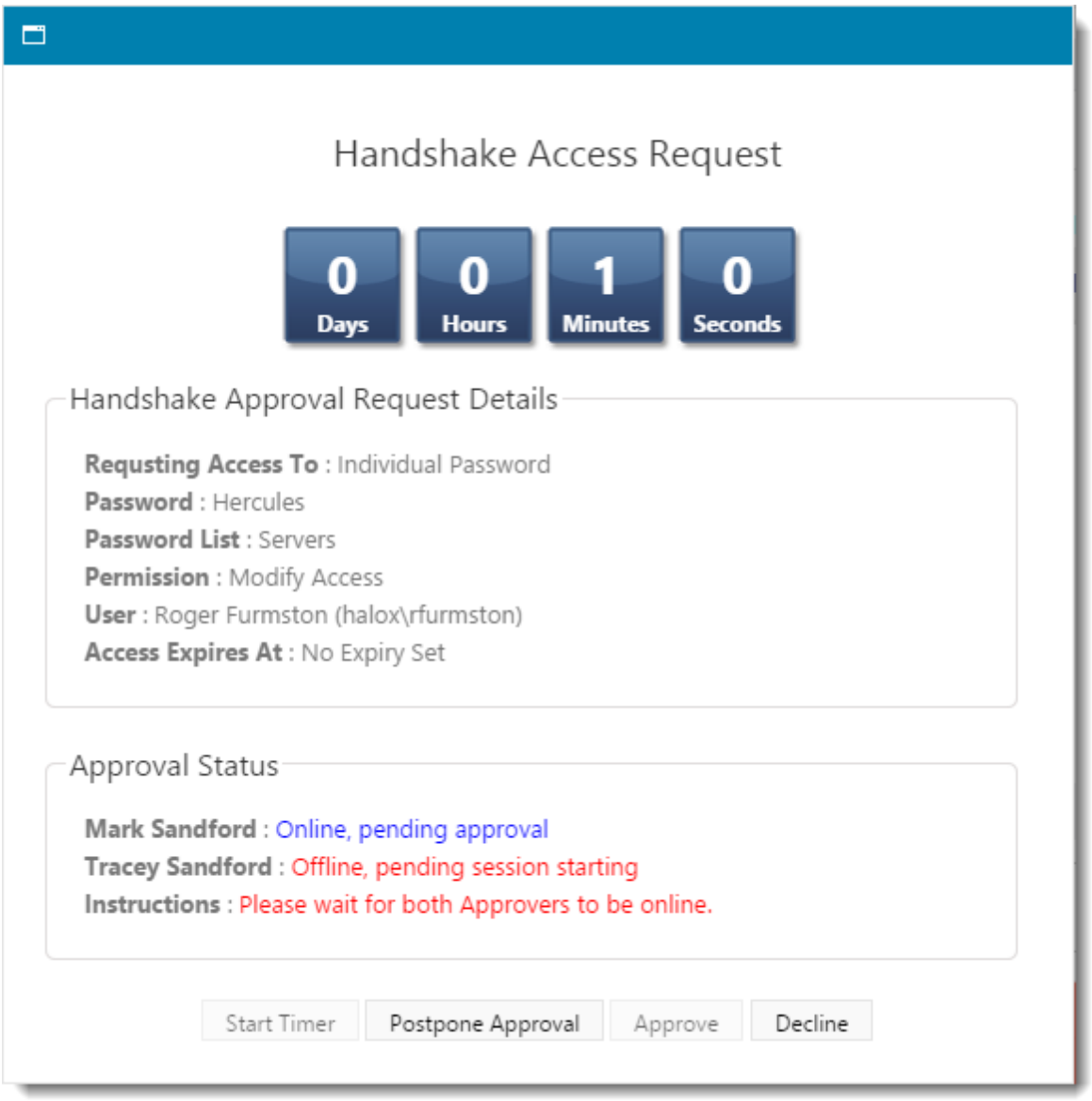


Once the Handshake Approval has been saved, and email will be sent to both approvers asking them to click on a link and approve the access. The screen below will appear when they click on the link.

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.

© 2017 Click Studios (SA) Pty Ltd



2.1.3.6.10 View Password Reset Dependencies

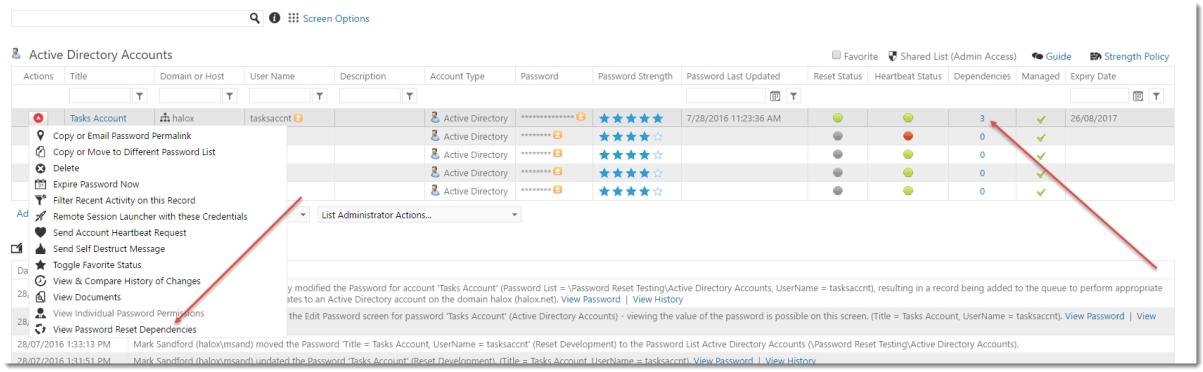
In addition to performing Password Resets for accounts, you can also add various 'dependencies' to a password record, which can also trigger a Password Reset script after the password for the account has been reset.

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

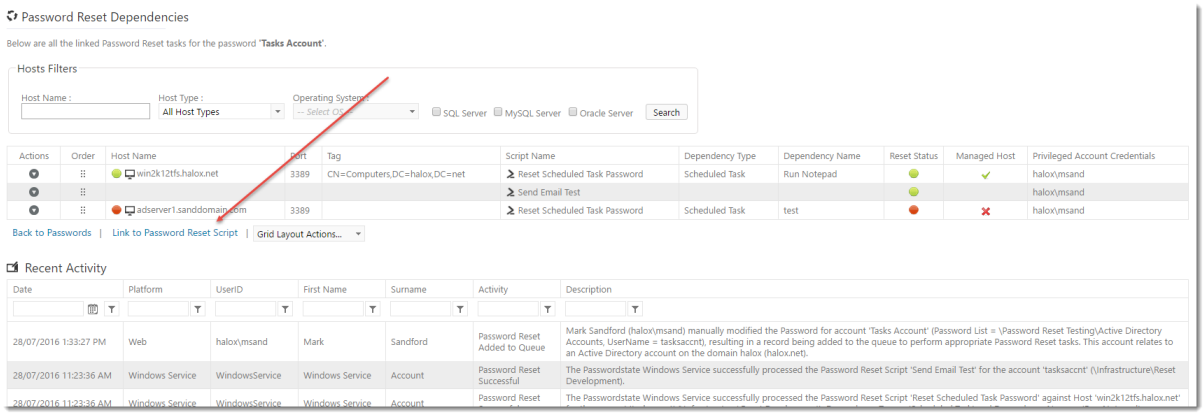
It is also possible to execute any custom type of PowerShell script you want as well, and the script does not necessarily have to be associated with a Host record.

© 2017 Click Studios (SA) Pty Ltd

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



Then you click on the 'Link to Password Reset Script' button.



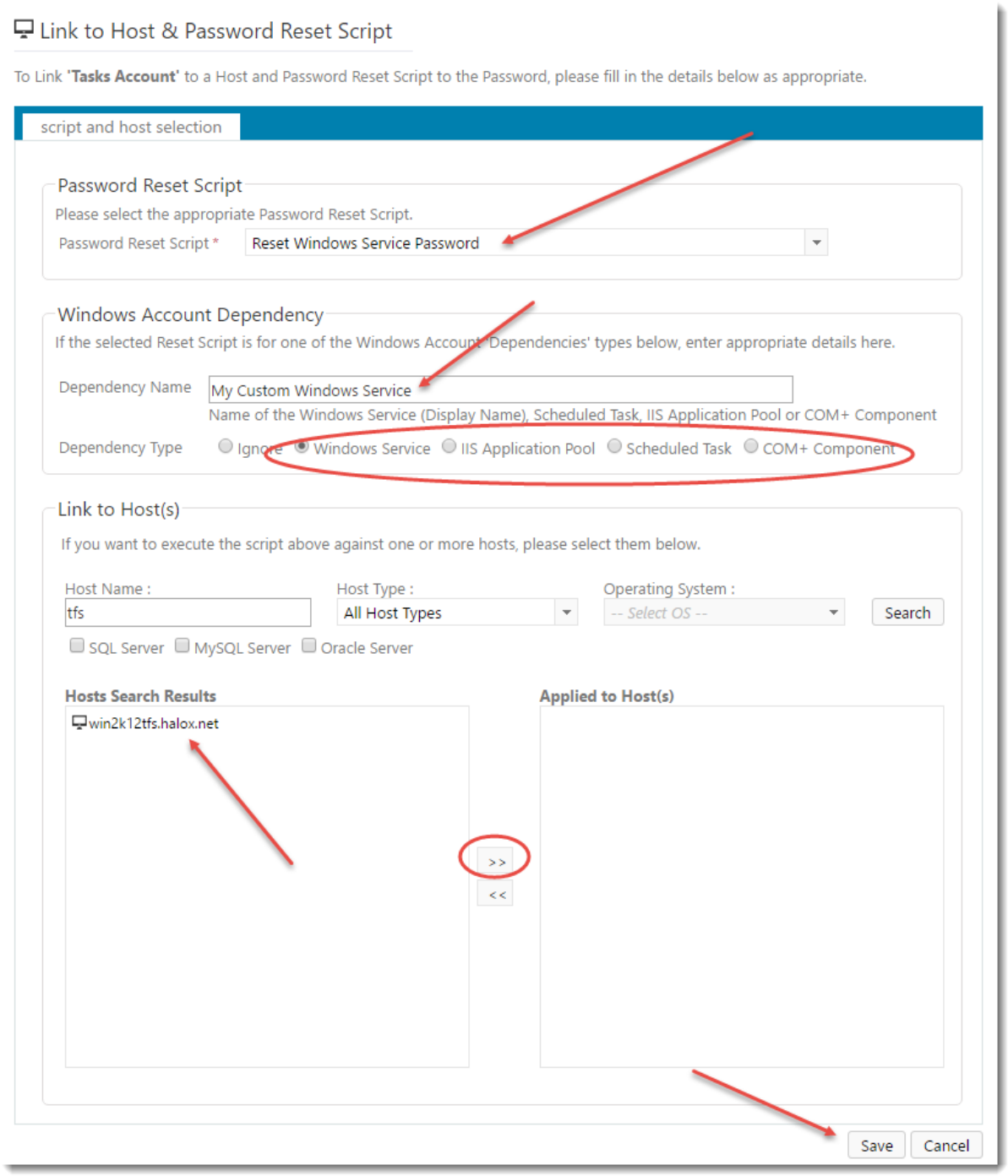
And then select the following options as appropriate:

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

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

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

© 2017 Click Studios (SA) Pty Ltd



2.1.3.7 List Administrator Actions

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

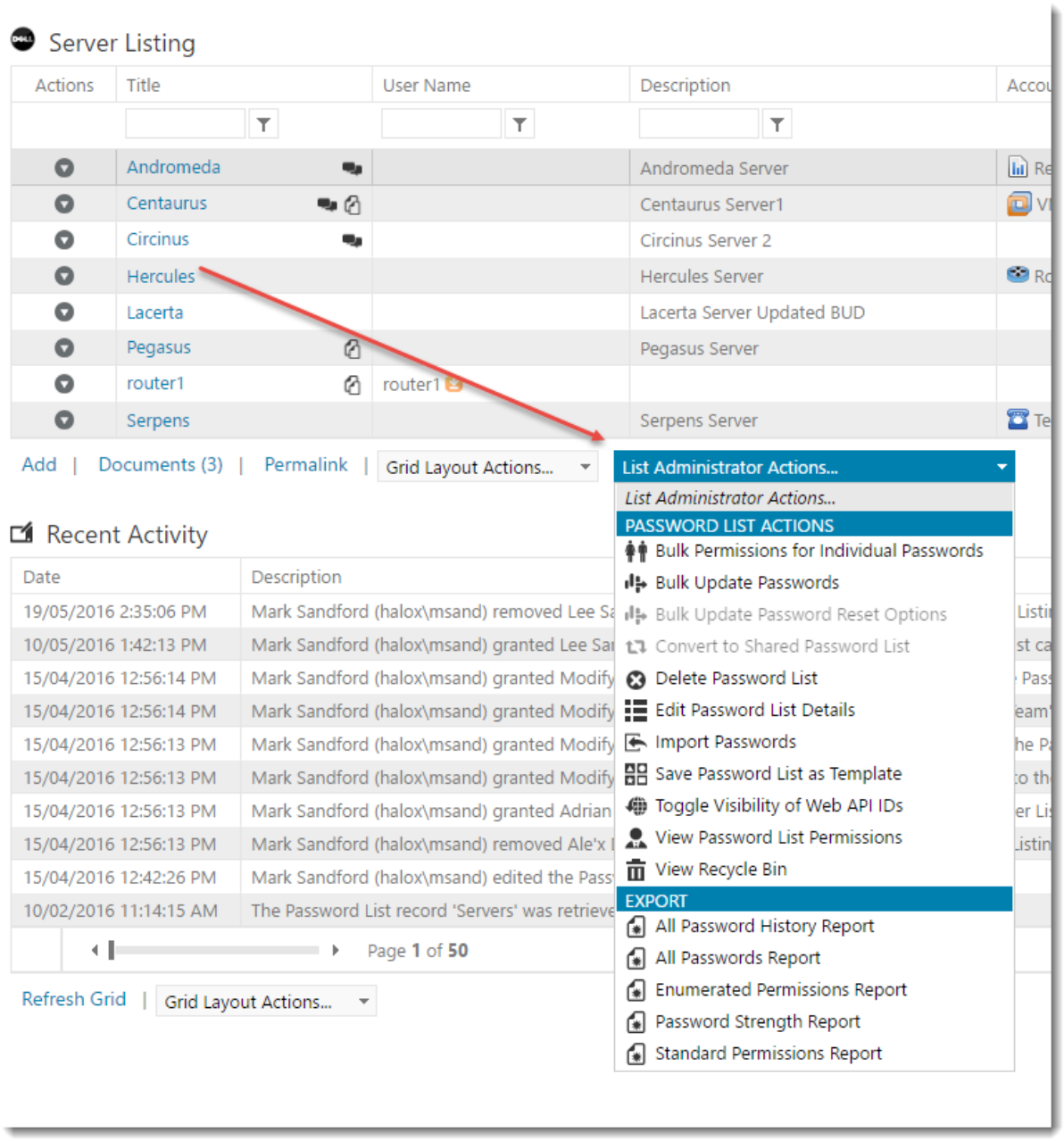
A summary of the features are:

© 2017 Click Studios (SA) Pty Ltd

Bulk Permissions for Individual Passwords	Allows you to apply permissions for a User's Account, or a Security Group, to multiple individual passwords records at once
Bulk Update Passwords	Instead of editing data/fields for a single Password record, 'Bulk Update Passwords' allows you to use a CSV file to update many records at once
Bulk Update Password Reset Options	When you have a Password List enabled to perform Password Resets, you can use this feature to change multiple "reset" options for one or more password records i.e. schedules, Privileged Account Credentials, etc
Convert to Shared Password List	If the Password List is a Private one, and you wish to convert it to a Shared one, then you can use this menu option.
Delete Password List	Deleting a Password List will delete the List itself and all related data. Note: There is no Recycle Bin for a Password List, so please use this feature with caution
Edit Password List Details	Allows you to modify existing settings for the Password List, change which fields you would like to use, and create an API key so records in the Password List can be queried or manipulated via the Passwordstate API
Import Passwords	Allows you to install passwords via CSV files
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
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
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
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
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

© 2017 Click Studios (SA) Pty Ltd

Standard Permissions Report	Will export to csv file a list of permissions applied to the Password List, or any individual Password records



2.1.3.7.1 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.

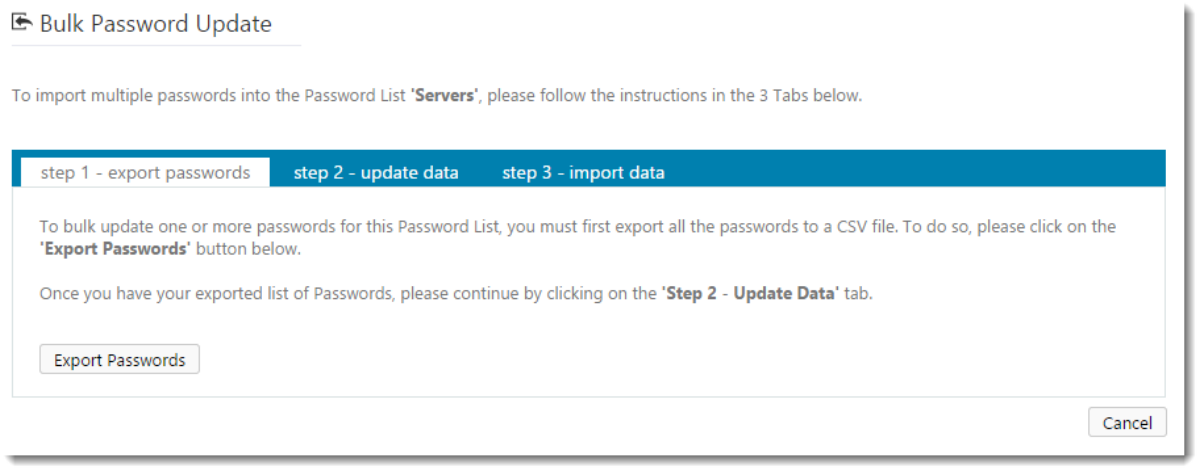
This feature will allow you to export all the passwords to a csv file, which you can then update as appropriate, and then re-import back into the Password List.

© 2017 Click Studios (SA) Pty Ltd

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

Step 1 - Export Passwords

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

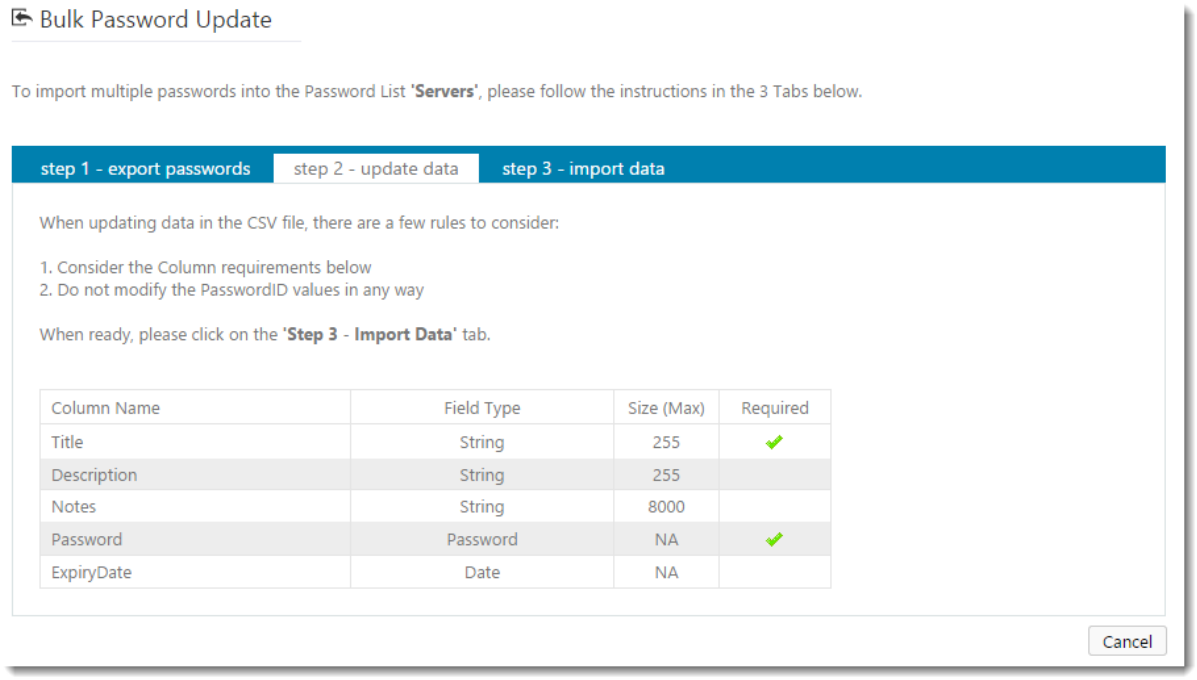


Step 2 - Update Data

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

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

© 2017 Click Studios (SA) Pty Ltd



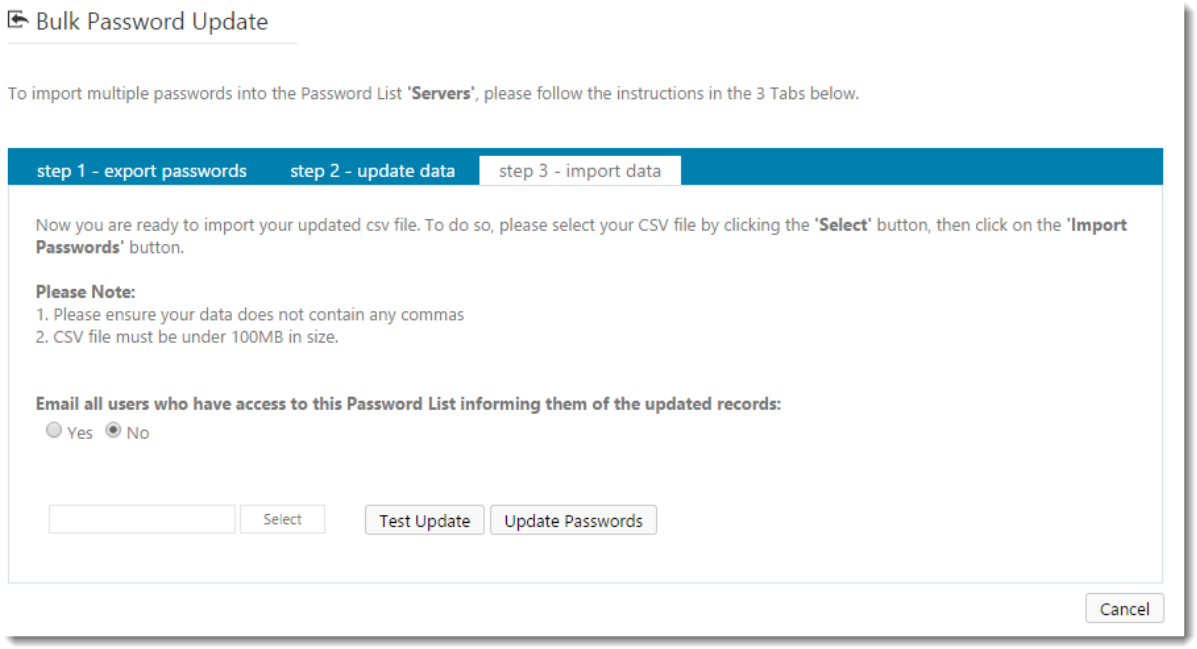
Step 3 - Import Data

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.

© 2017 Click Studios (SA) Pty Ltd

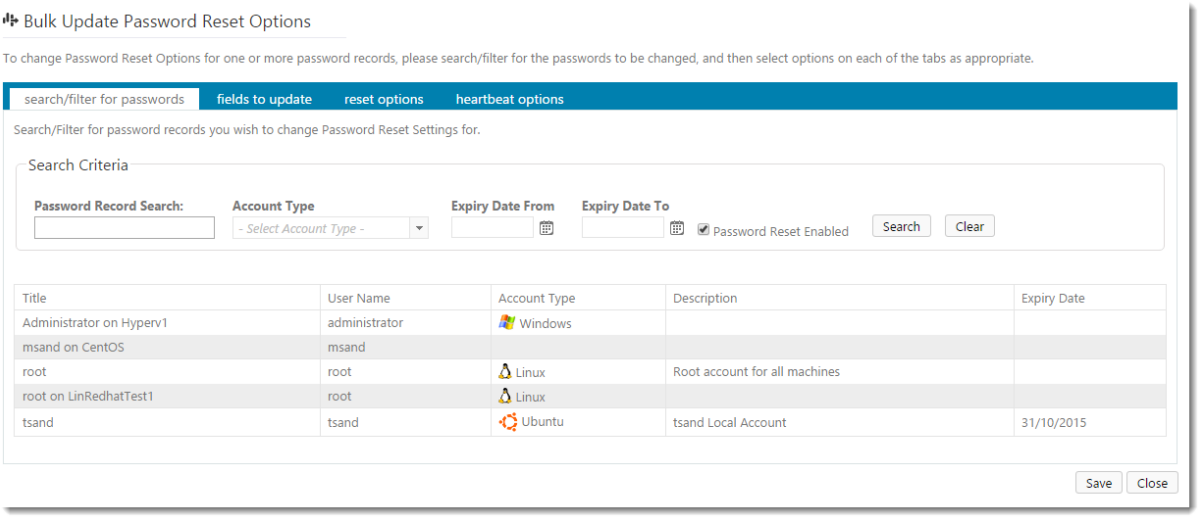


2.1.3.7.2 Bulk Update Passw ord Reset Options

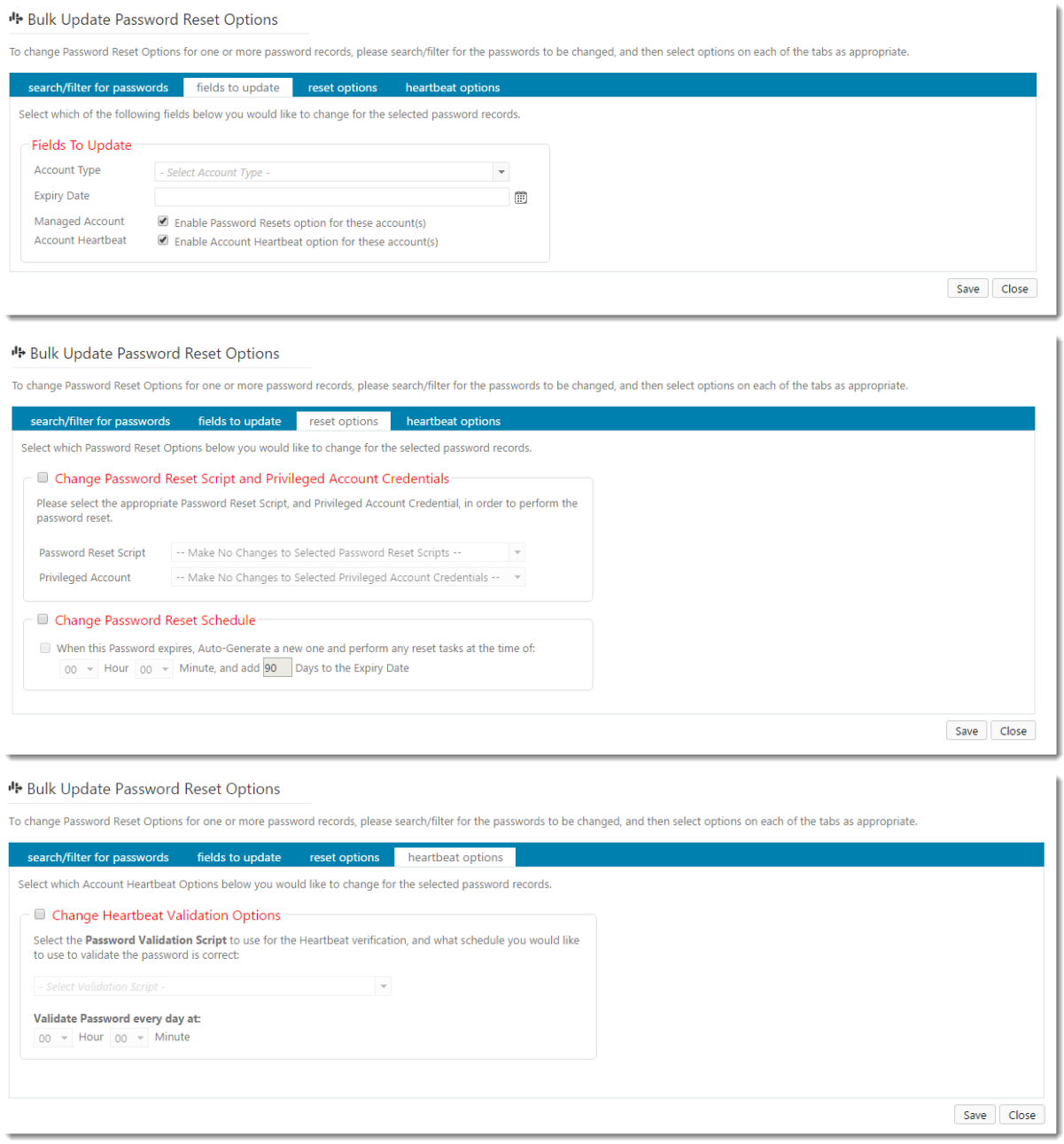
If you need to update Password Reset settings for more than one password record at a time, then you can use the 'Bulk Update Password Reset Options' available from the 'List Administrators Actions' dropdown list on each Password List.

With this feature you can:

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



© 2017 Click Studios (SA) Pty Ltd



2.1.3.7.3 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.

© 2017 Click Studios (SA) Pty Ltd

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

2.1.3.7.3.1 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.

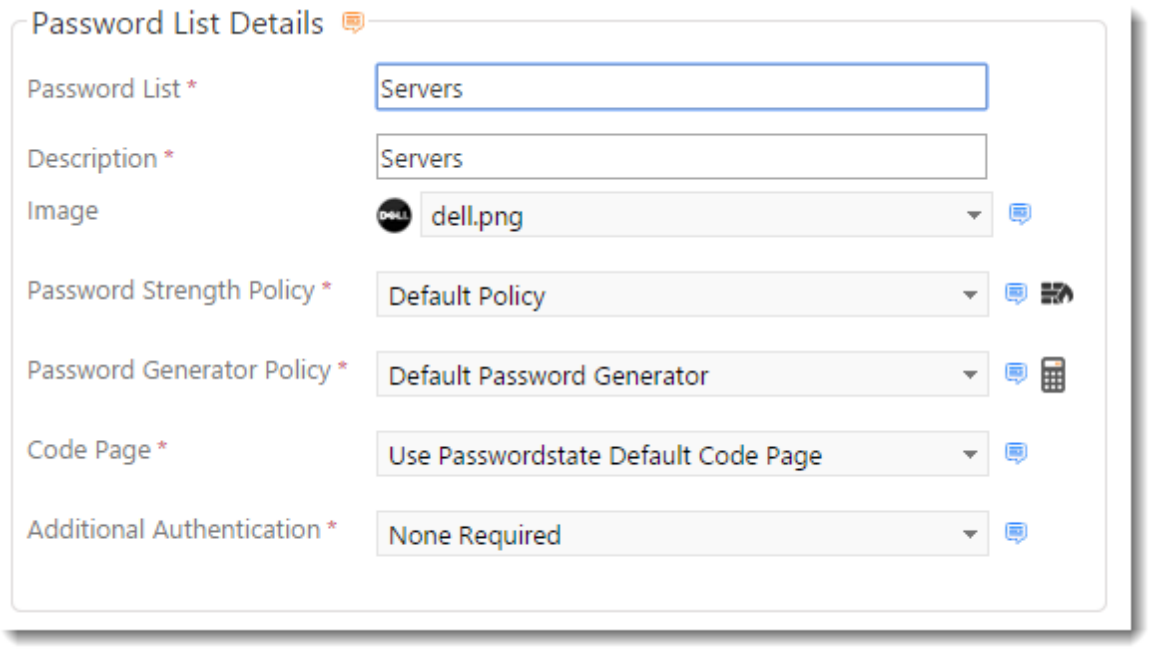
Below is some detail for each of the sections in the Password List Details tab.

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
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

© 2017 Click Studios (SA) Pty Ltd



Password List Settings Section

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

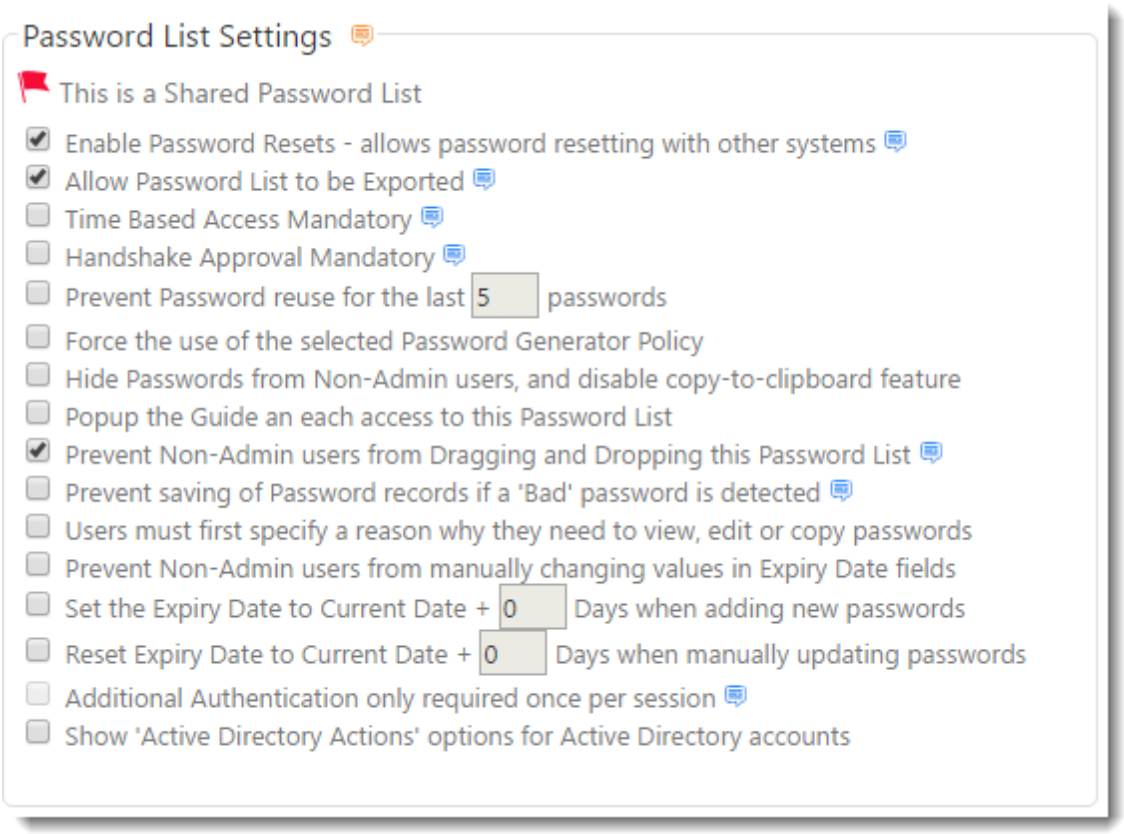
Allow Password List to be Exported	Allows or prevents the passwords and their history from being exported
Time Based Access Mandatory	If this option is set, any time new permissions are applied to the Password List for user accounts or security groups, you must specify a future date/time when the permission 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
Enable Password Resets	Allows passwords stored within the Password List to perform Password Resets on other remote systems/hosts
Do not send Email Notifications for Scheduled Password Resets	This option is useful if you have a Password List configured to store all Local Administrator Accounts for many workstations. When 'discovering' Local Administrator accounts, if you chose the option to add one password record for every workstation, you may not want to receive reset emails for each record - it could cause a lot of emails to be generated
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

© 2017 Click Studios (SA) Pty Ltd

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

© 2017 Click Studios (SA) Pty Ltd

	• User must change password at next logon • Disable this account • Enable this account

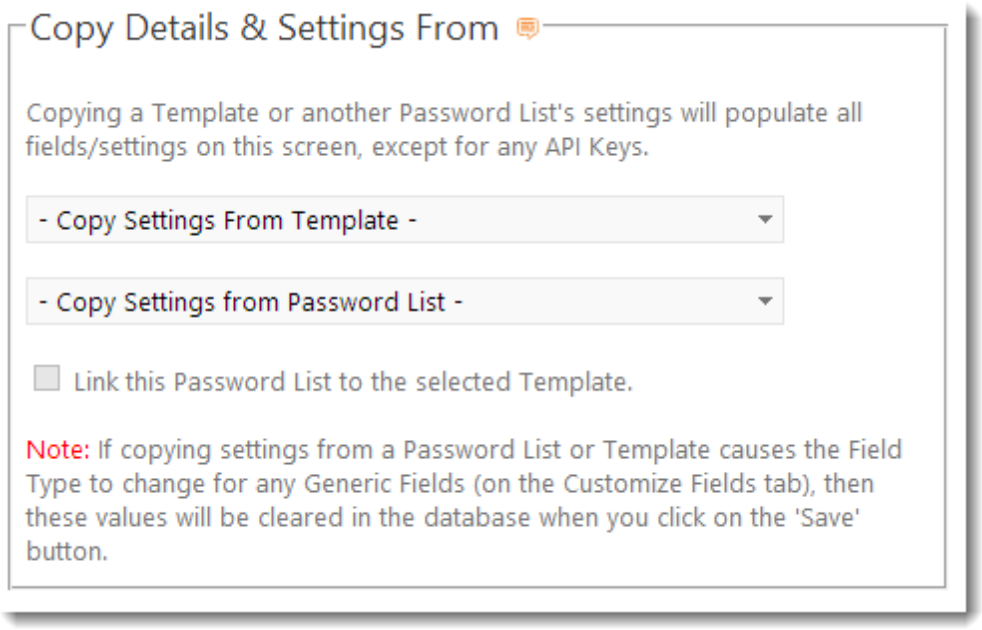


Copy Details & Settings from Section

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

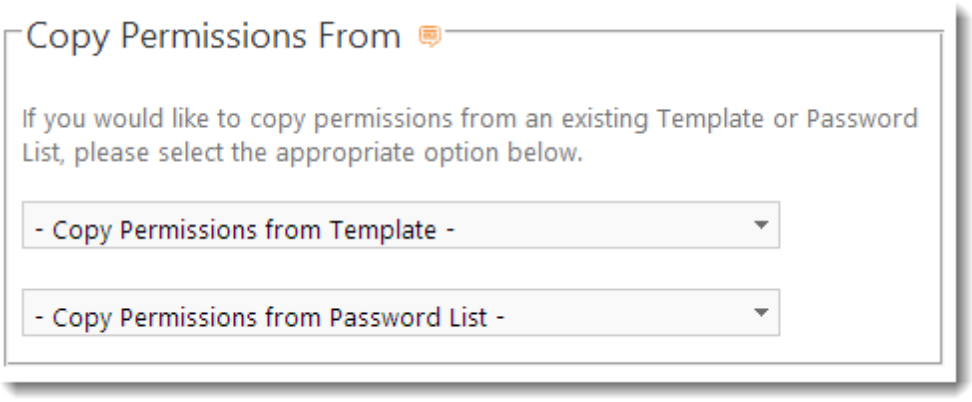
Note 1: When copying settings from another Password List or Template, you need to be aware of incompatible field types for Generic Fields. If a selected Generic Field in one Password List/ Template is of type 'Text Field', and of type 'Password' in the Password List you are editing, then the values in the Password List you are editing will be erased/blanked in the database - this is because you cannot mix different Generic Field data types. There are multiple warning messages within the Passwordstate as well for this, so please be aware.
Note 2: If you select to copy settings from a Template, you can also link the Password List to the Template at the same time. By doing this, all subsequent changes to settings and fields needs to be done on the Template itself, and not on the Password List

© 2017 Click Studios (SA) Pty Ltd



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 Password Reset Schedule

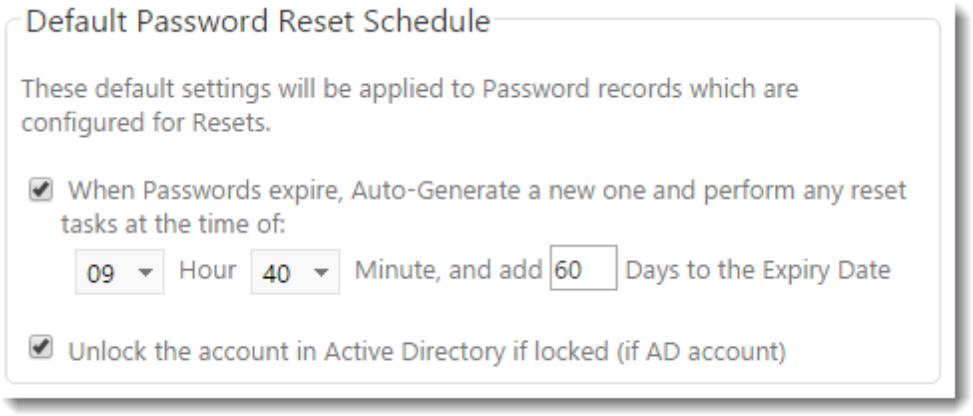
If a Password List is configure to perform Password Resets with other systems/hosts, you can then set various Automatic Password Reset settings - used for resetting a Password once the Expiry Date field value is reached.

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

© 2017 Click Studios (SA) Pty Ltd

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

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



2.1.3.7.3.2 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

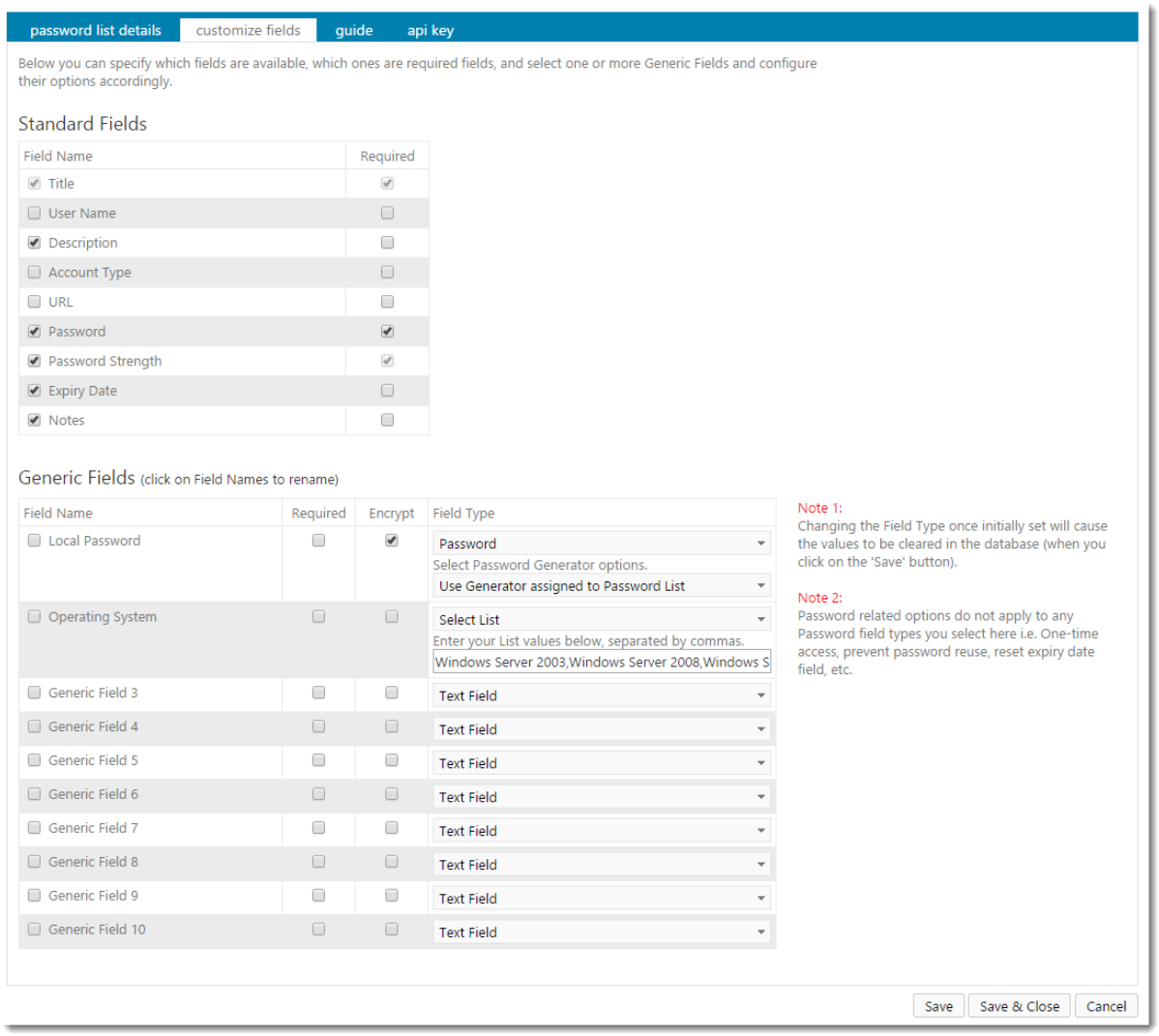
© 2017 Click Studios (SA) Pty Ltd

	selected Password Strength Poilcy
Expiry Date	All passwords should be reset after a certain period of time. The Expiry Date field can be used to indicate when this time is, and can be used for reporting purposes, or for Automatic Password resetting
Notes	Allows you to specify longer HTML formatted text for any general notes you need to maintain for the record
Generic Fields (1 to 10)	Generic Fields can be configured for any purpose you like, and also named any way you like. The following Field Types are available for Generic Fields: • Text Field — A single line text field • Free Text Field — Multiple line text field • Password — An encrypted password field • Select List — A vertical drop-down list of predefined values • Radio Buttons — A horizontal checklist of predefined values • Date Picker — A popup calendar style control for picking date values • URL Field — Allows you to click on the URL in the Grid view and launch the web site

Note 1: If you change a Generic Field's Field Type after the fields have been populated with data, then the values for the changed field will be erased/blanked in the database when you click on the 'Save' button - this is because the different Generic Field Field Types need to have their data treated differently. There are multiple warning messages within the Passwordstate as well for this, so please be aware.

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

© 2017 Click Studios (SA) Pty Ltd



2.1.3.7.3.3 API Key & Settings 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:

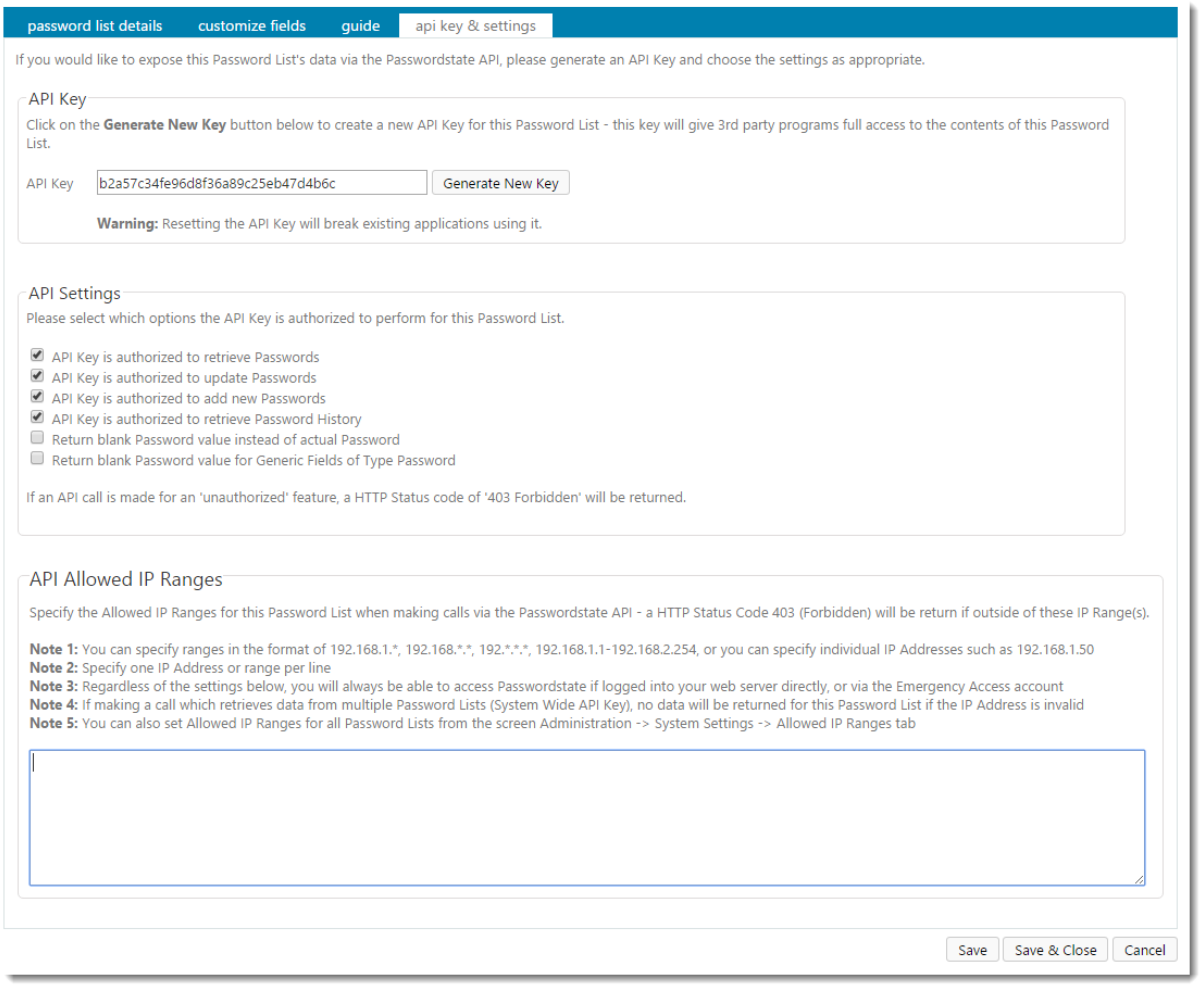
- To retrieve Passwords or Password History from the API
- To update Passwords via the API
- To add new Password records via the API
- To return blank values for Password fields, instead of returning plain-text Passwords - some customers may find this useful for additional security, where they can write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

© 2017 Click Studios (SA) Pty Ltd

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'

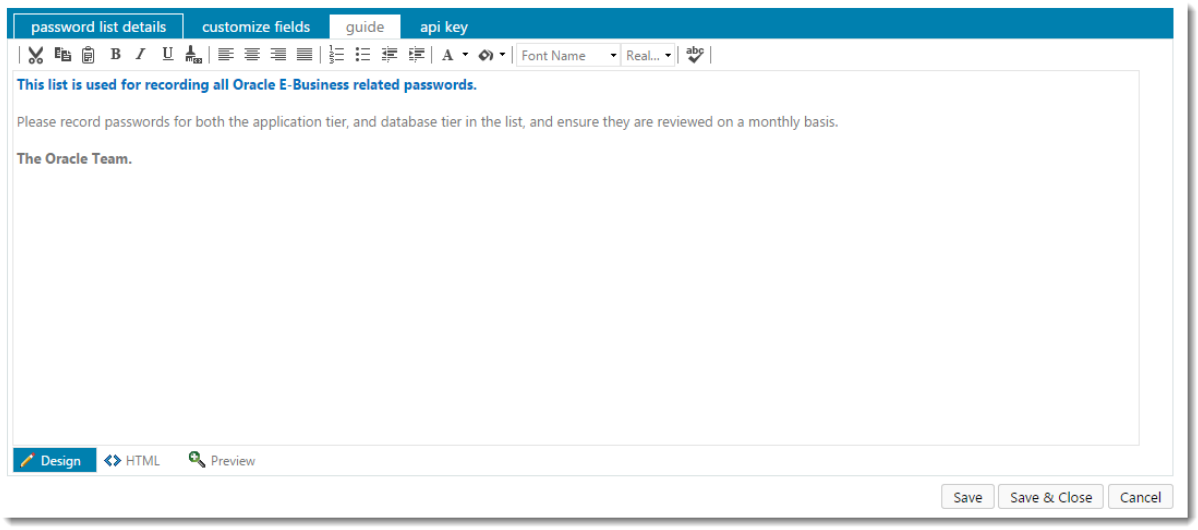
For more information about the functions the Passwordstate API can perform, please reference the 'Web API Documentation' from the Help navigation menu within Passwordstate.



2.1.3.7.3.4 Guide Tab

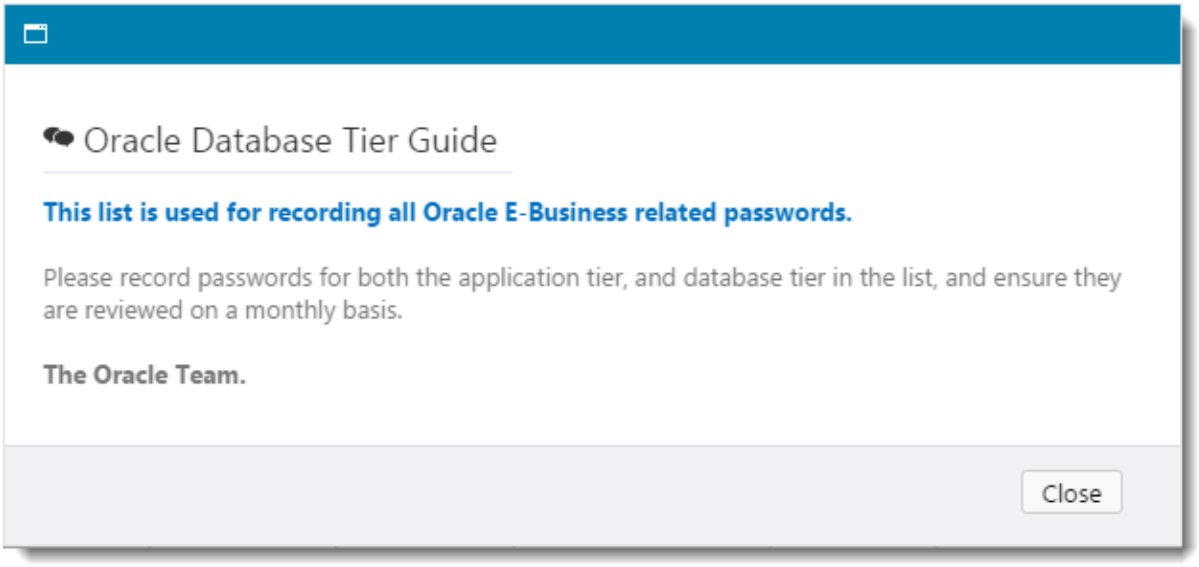
The Guide tab allows you to provide detail as to the intended use of the Password List, and can include some basic HTML style formatting.

© 2017 Click Studios (SA) Pty Ltd



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.



2.1.3.7.4 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

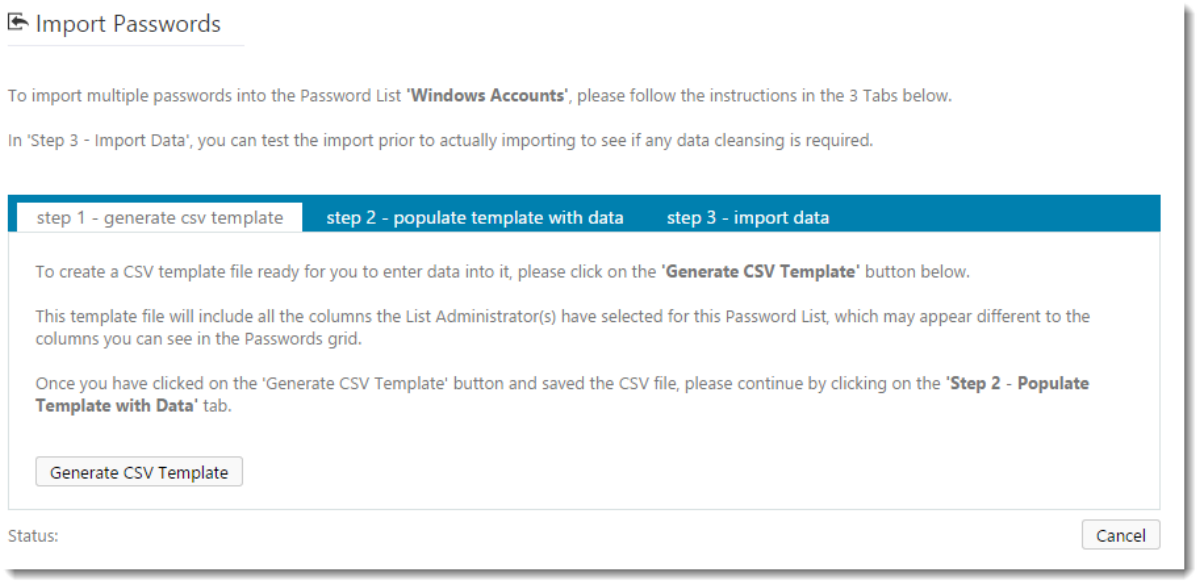
© 2017 Click Studios (SA) Pty Ltd

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'.

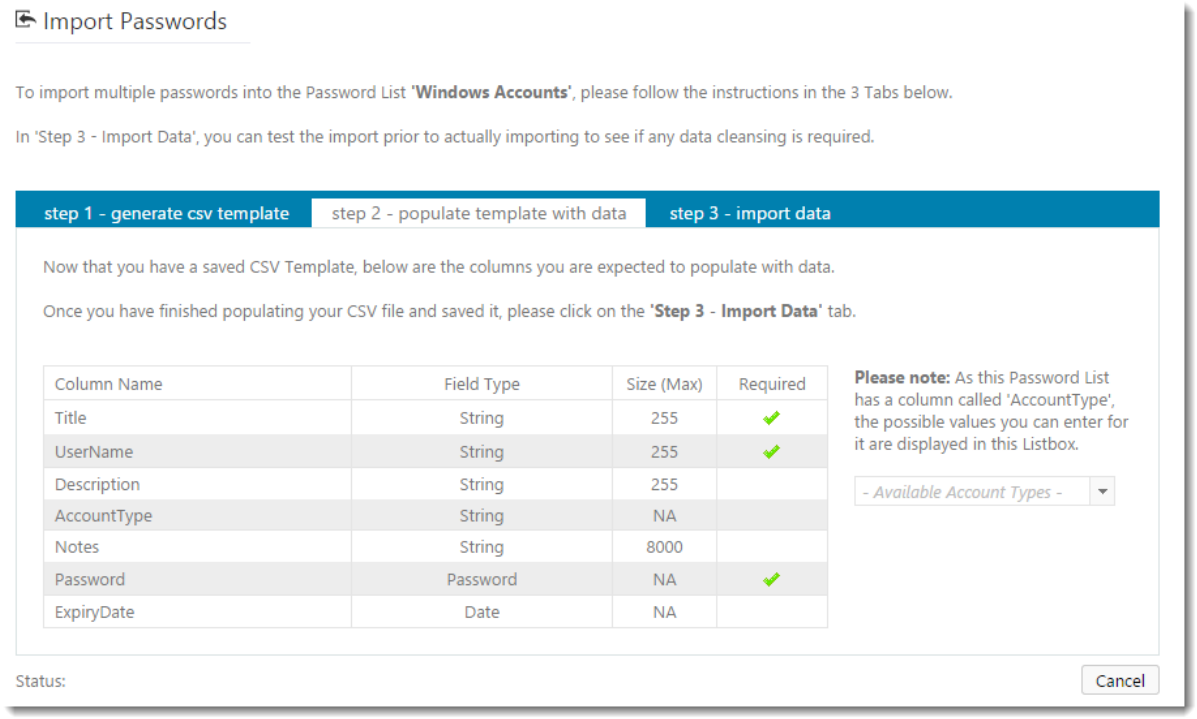


Step 2 - Populate Template with Data

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.

© 2017 Click Studios (SA) Pty Ltd

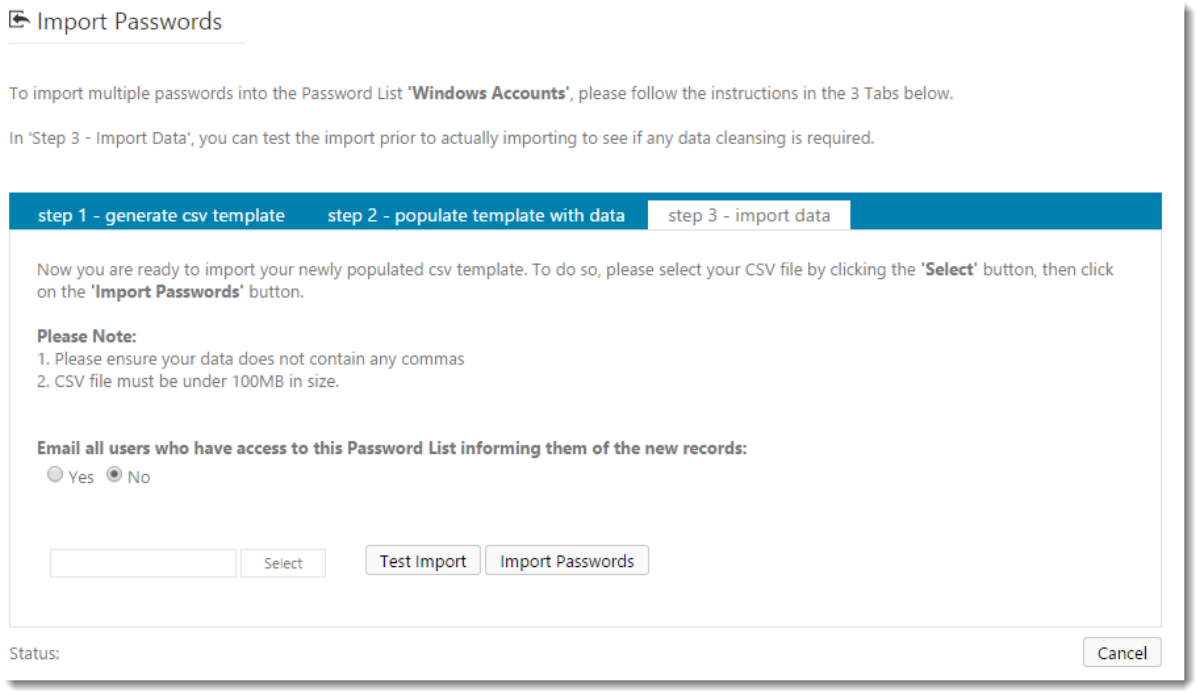


Step 3 - Import Data

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.

© 2017 Click Studios (SA) Pty Ltd



2.1.3.7.5 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).

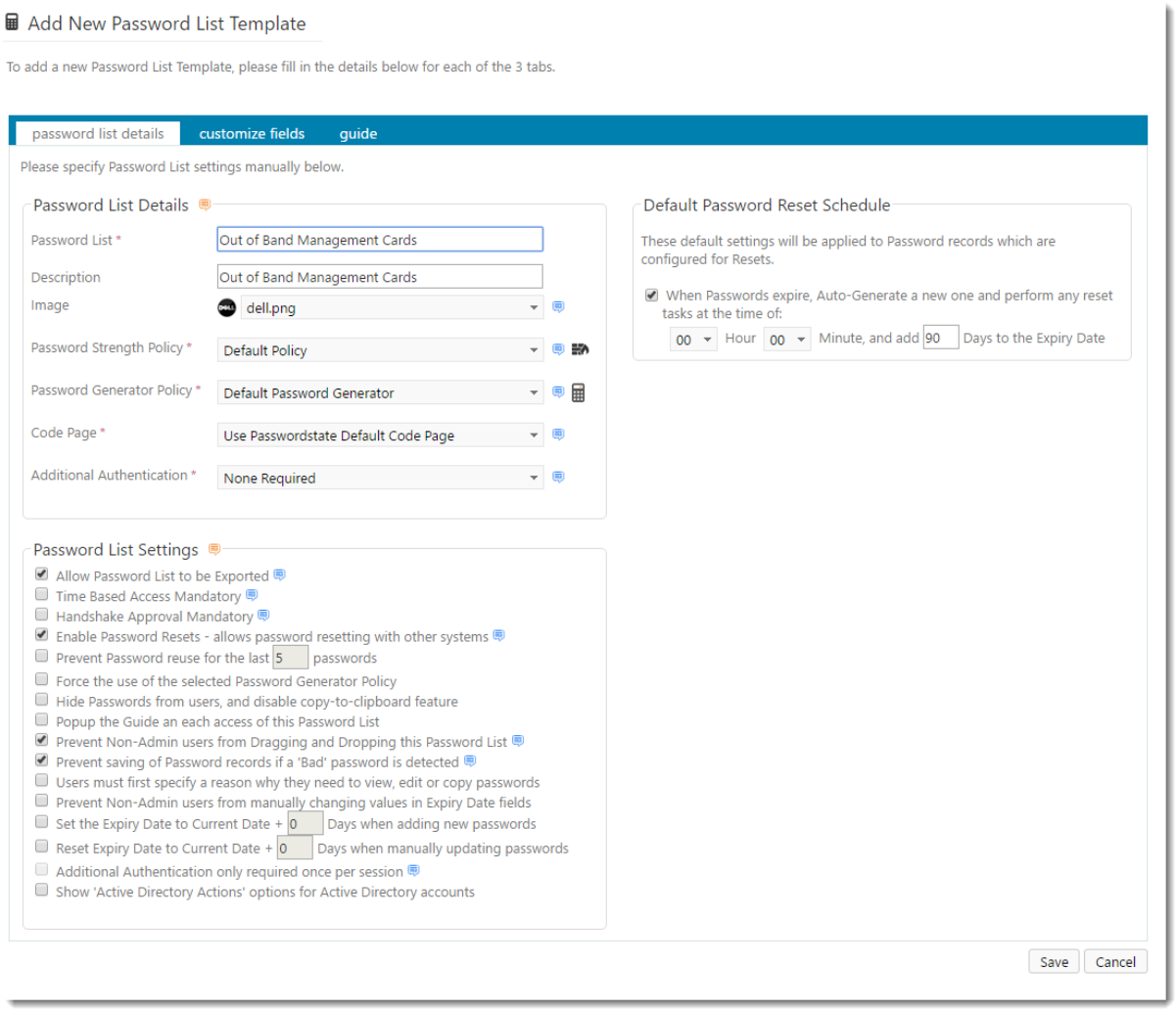
When you click on the menu item 'Save Password List as Template', you will see a screen very similar to the Add/Edit Password List screen, with a few small exceptions:

- 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.

© 2017 Click Studios (SA) Pty Ltd



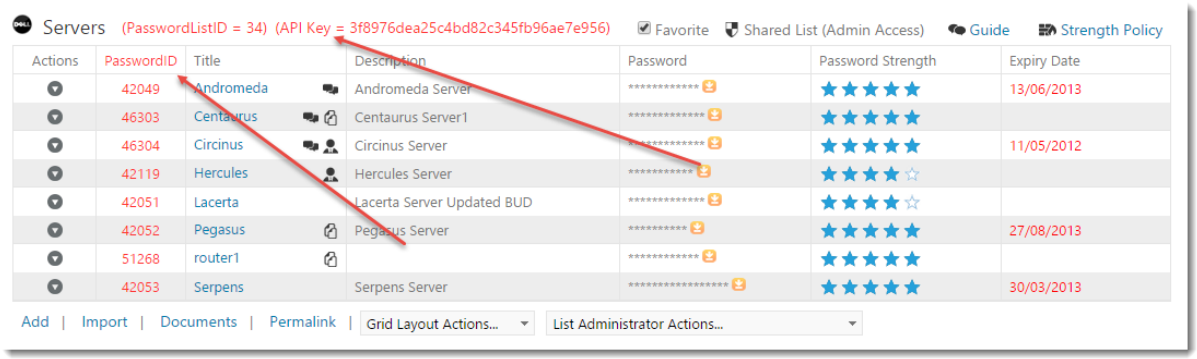
2.1.3.7.6 Toggle Visibility of Web API IDs

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.

© 2017 Click Studios (SA) Pty Ltd

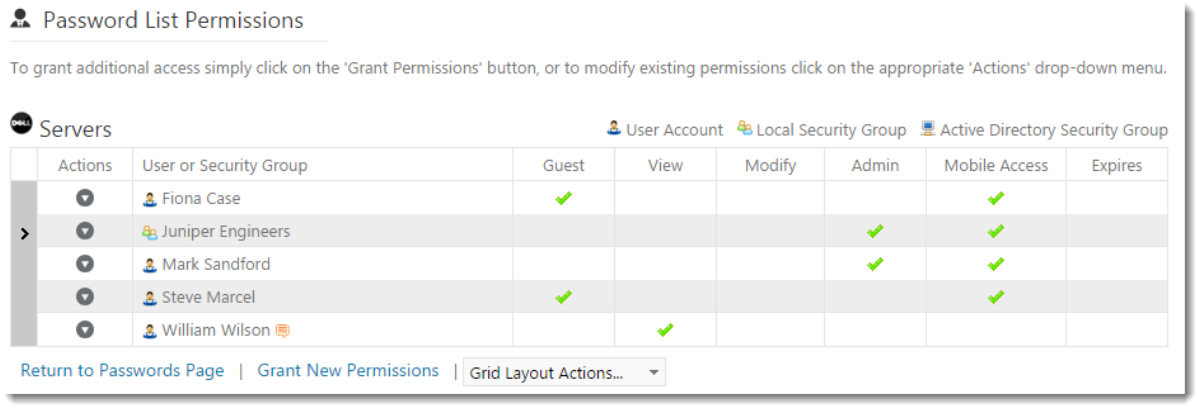


2.1.3.7.7 View Password List Permissions

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
- Mobile Access - In addition to access Password Lists through the web interface, you can also grant Mobile Client Access for each of the different permissions as well



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

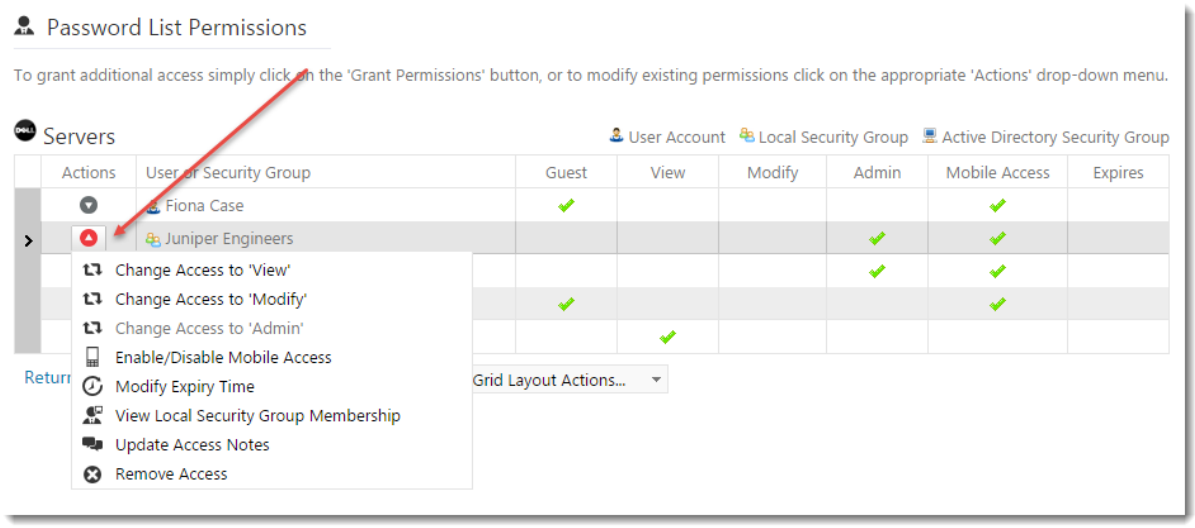
Password List Permission Actions

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

© 2017 Click Studios (SA) Pty Ltd

group, you can:

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



Grant New Permissions

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

2.1.3.7.7.1 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.

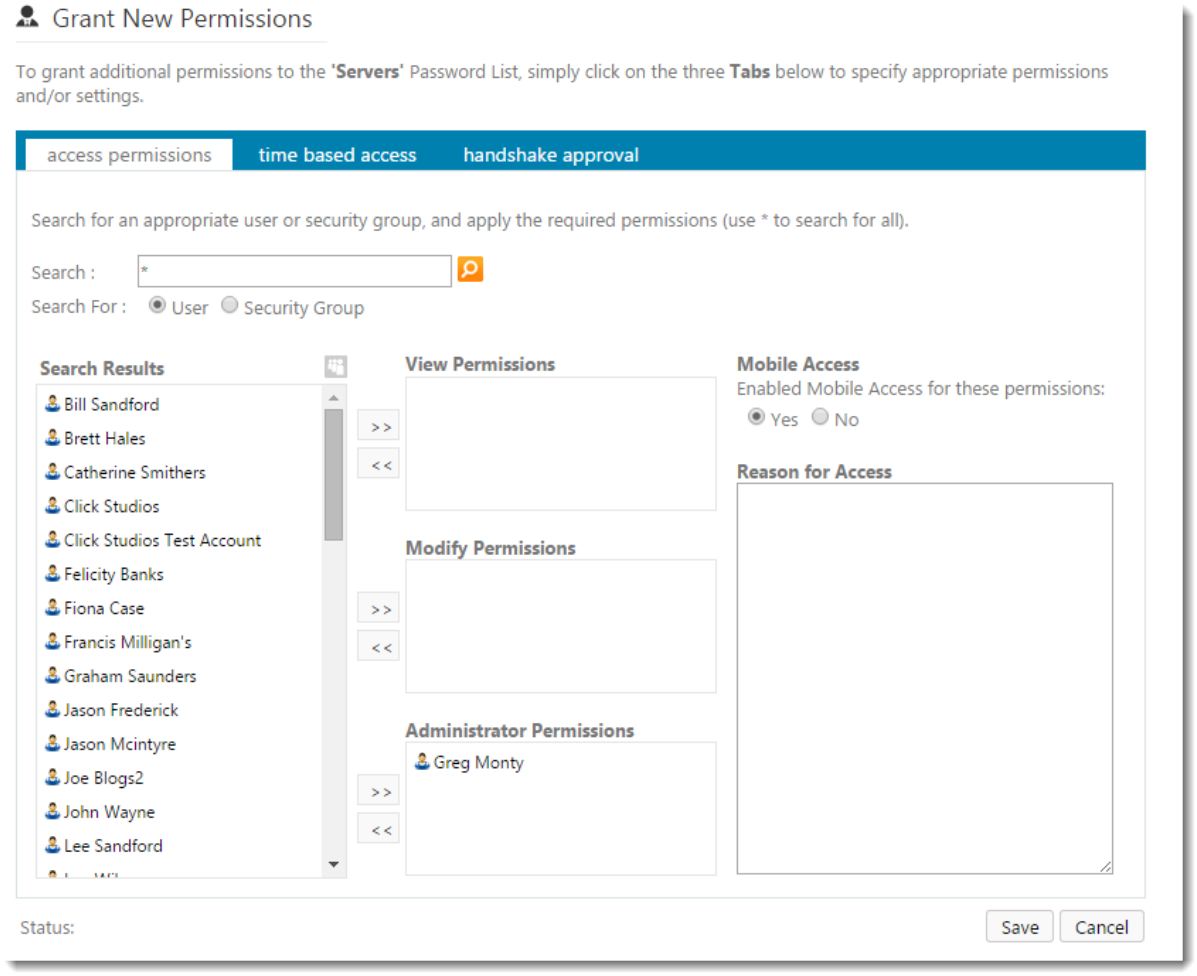
As you apply new permissions for users, they will also be granted permissions to any upper-level Password Folders the Password List may be nested beneath - there may be an exception to this if a Folder is configured to manager permissions manually, but this is the default setting.

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. You can also enable or disable Mobile Client Access for any permissions added here.

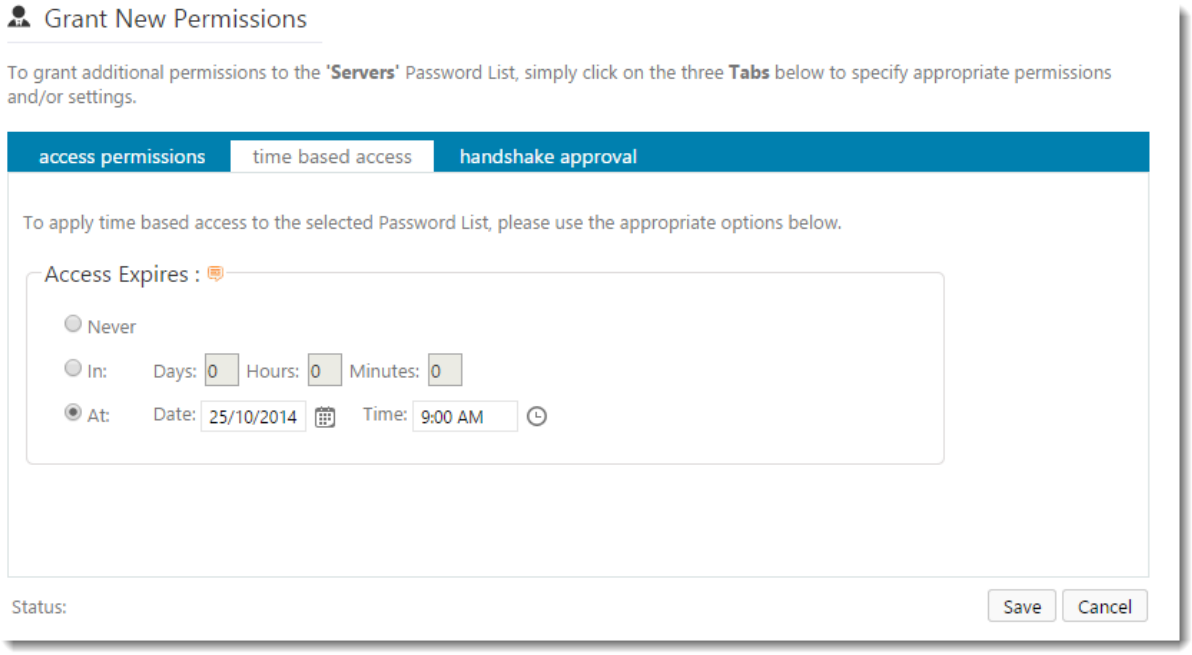
© 2017 Click Studios (SA) Pty Ltd



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.

© 2017 Click Studios (SA) Pty Ltd

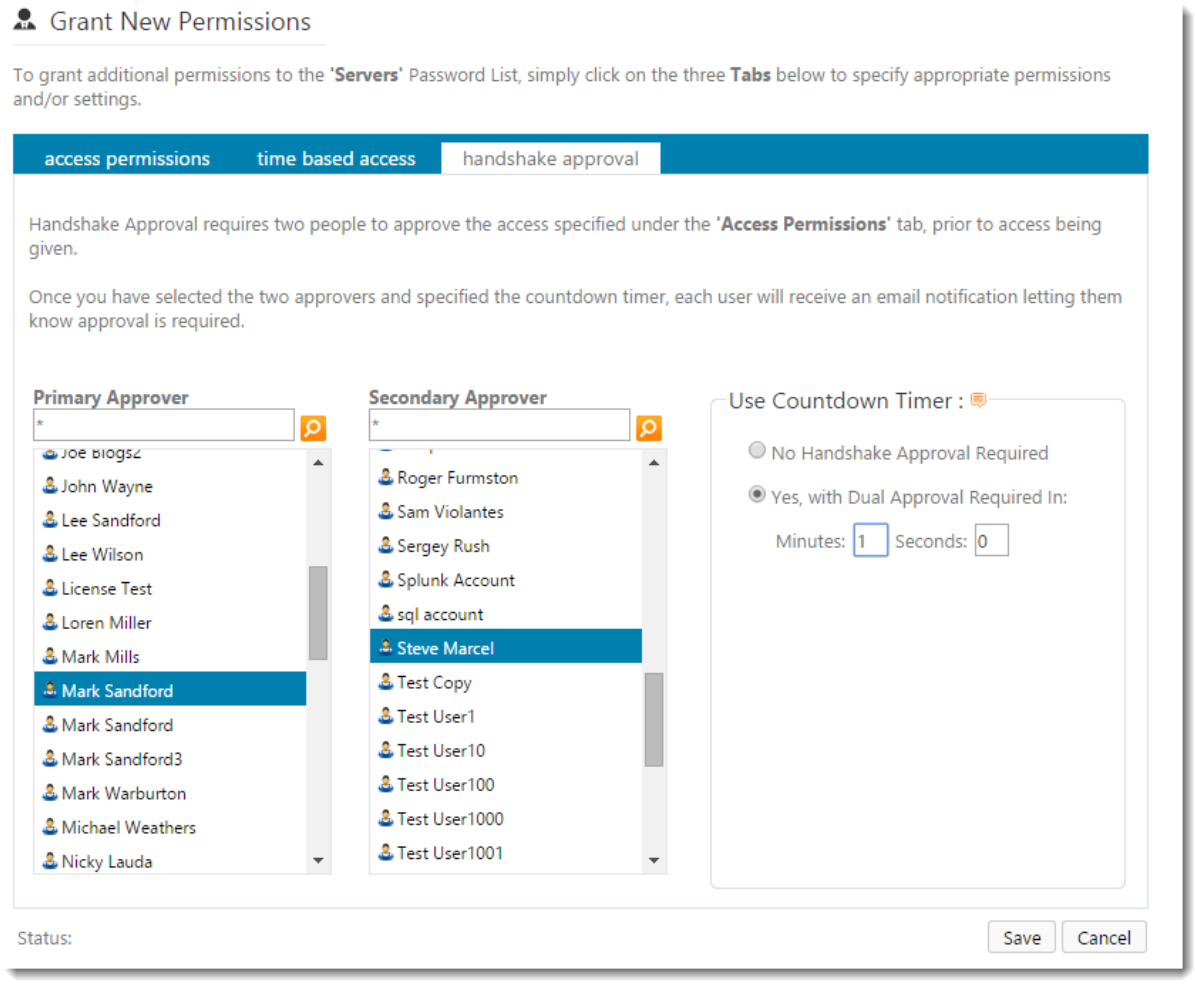


Handshake Approval

'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.

© 2017 Click Studios (SA) Pty Ltd

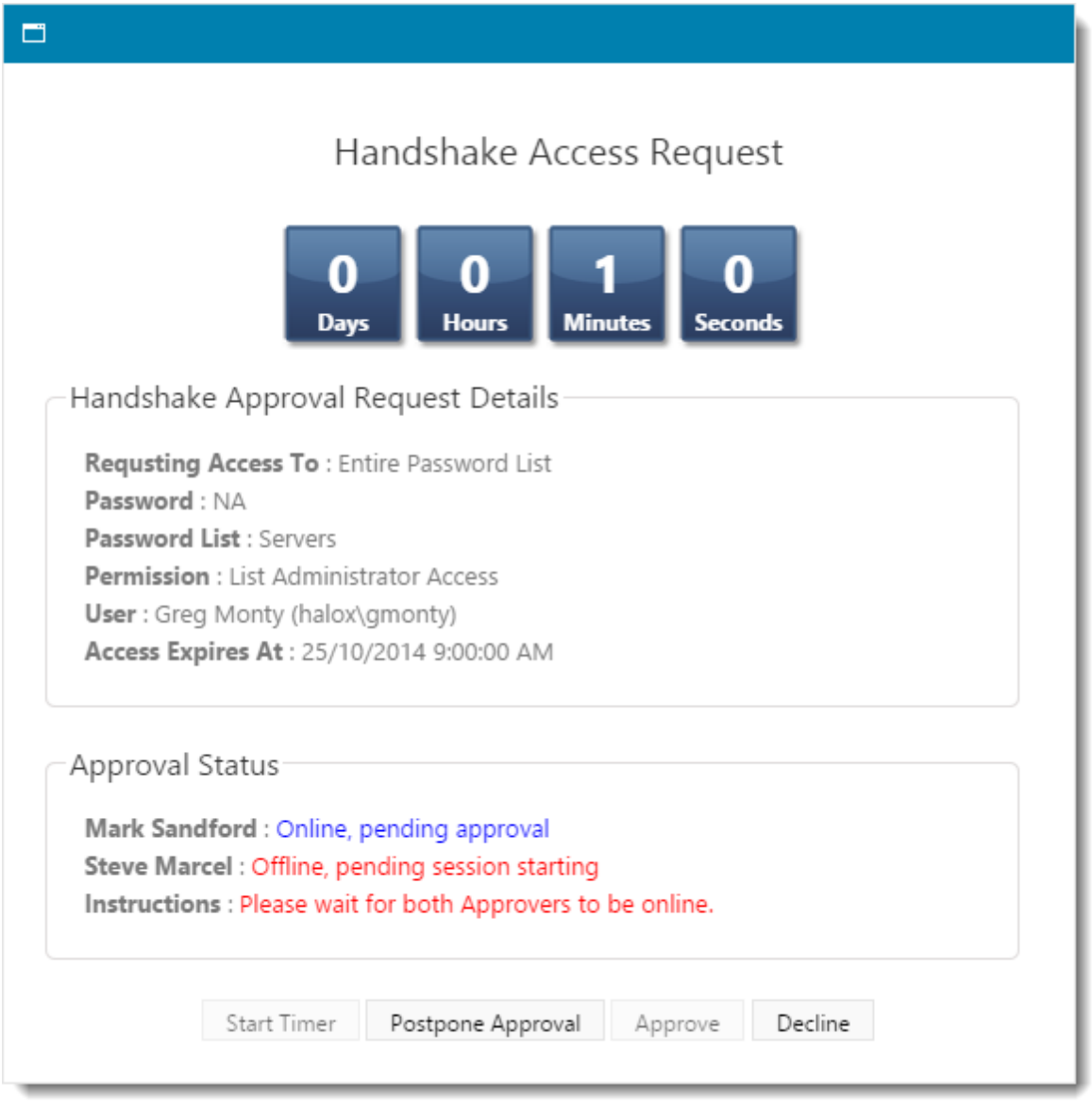


Once the Handshake Approval has been saved, and email will be sent to both approvers asking them to click on a link and approve the access. The screen below will appear when they click on the link.

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.

© 2017 Click Studios (SA) Pty Ltd

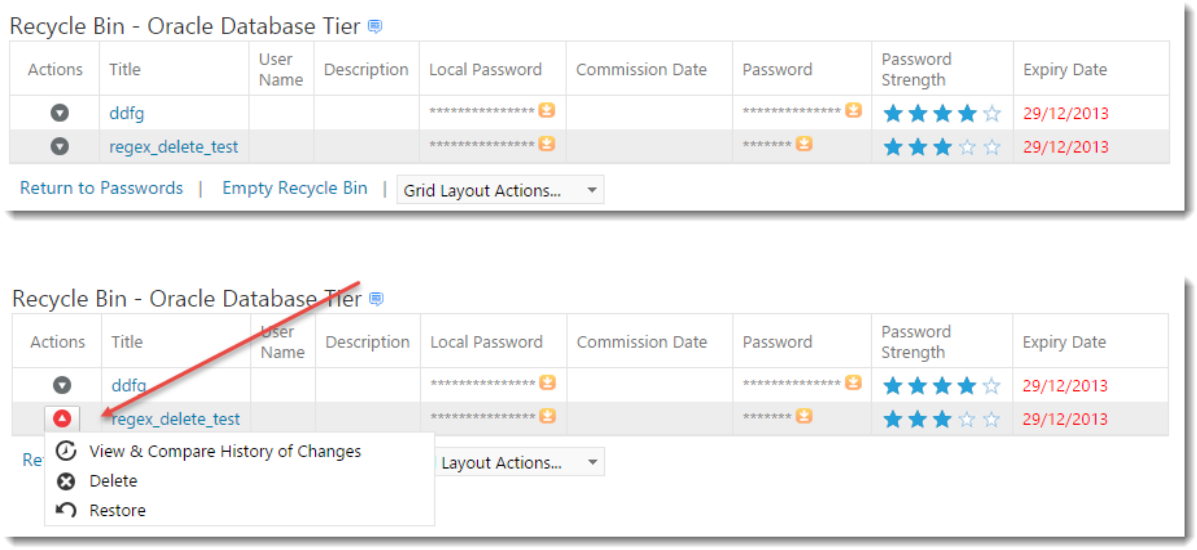


2.1.3.7.8 View Recycle Bin

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

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

© 2017 Click Studios (SA) Pty Ltd



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. When doing this, any 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 - unless you select the option below to Propagate any permissions on the folder to nested Folders and Password Lists beneath it
Propagate Permission Downwards	This option allows you to manage permissions at the folder level, and all the permissions added/ modified will be propagated down to any nested Password Lists or Folders

© 2017 Click Studios (SA) Pty Ltd

Permission Model Overview

There are two ways permissions can be managed for Folders and Password Lists:

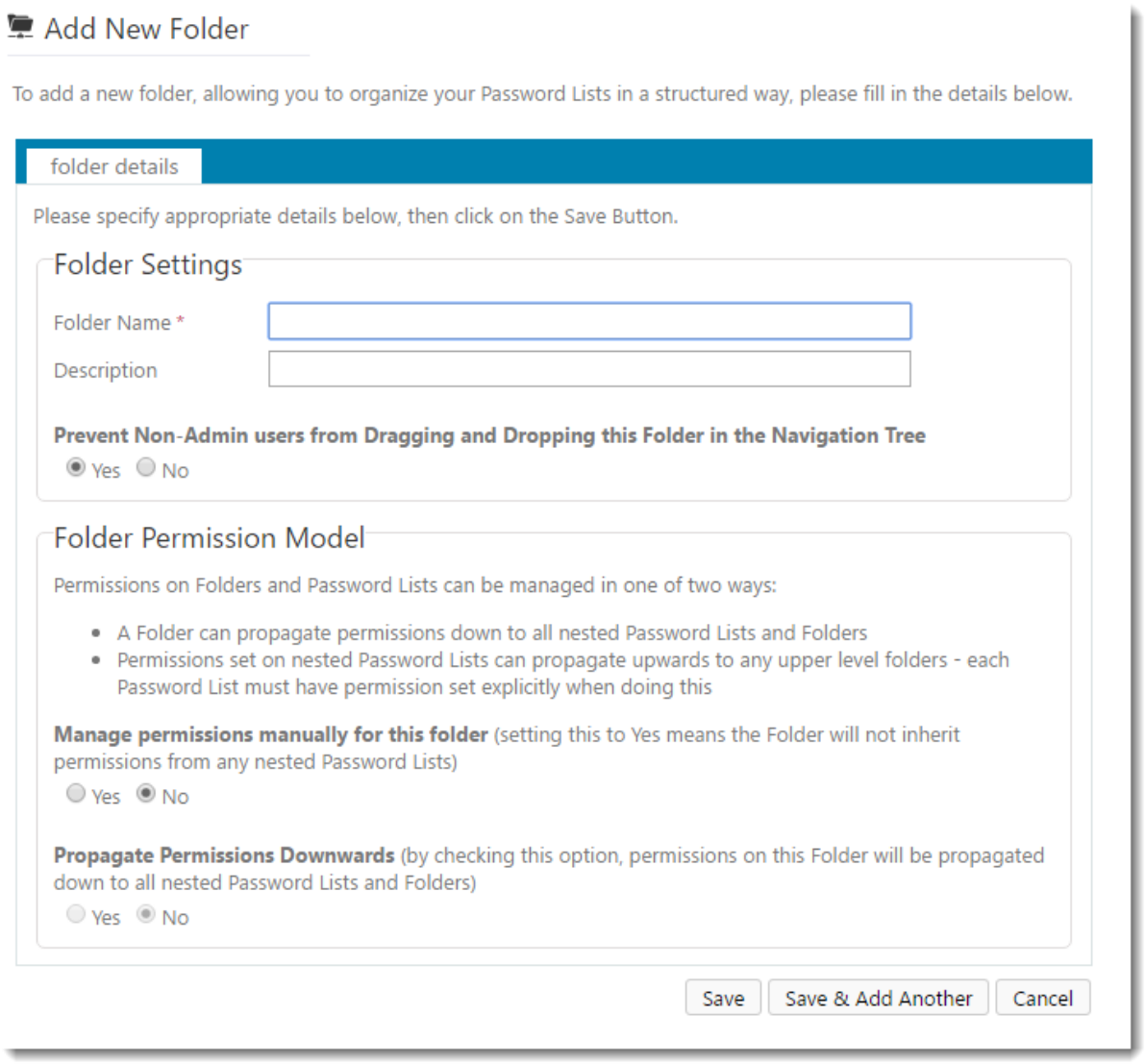
- Permissions are managed at the individual Password List level, and any changes to permissions on the Password Lists are propagated up to any upper level Folders
- For a top level Folder, you can choose to manage permissions at this level, and propagate those permissions down to any nested Password Lists or Folders

Propagating Permission Restrictions

If you choose to propagate permissions from the Folder down, there are a few restrictions you need to be aware of:

- Private Password Lists cannot be nested beneath a Folder which is propagating permissions down
- The 'Bulk Permissions' feature cannot be used for any Password Lists which are inheriting permissions from an upper-level Folder
- If dragging and dropping Folders and Password Lists around in the Navigation Tree, you will be warned and ask to confirm if any changes to permissions to Password Lists will occur
- A couple of System Settings options for applying permissions to newly created Password Lists will be ignored
- When adding or editing a Password List, the options to clone permissions from other Password Lists or Templates will be disabled

© 2017 Click Studios (SA) Pty Ltd



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 its contents, is the person who created it .

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

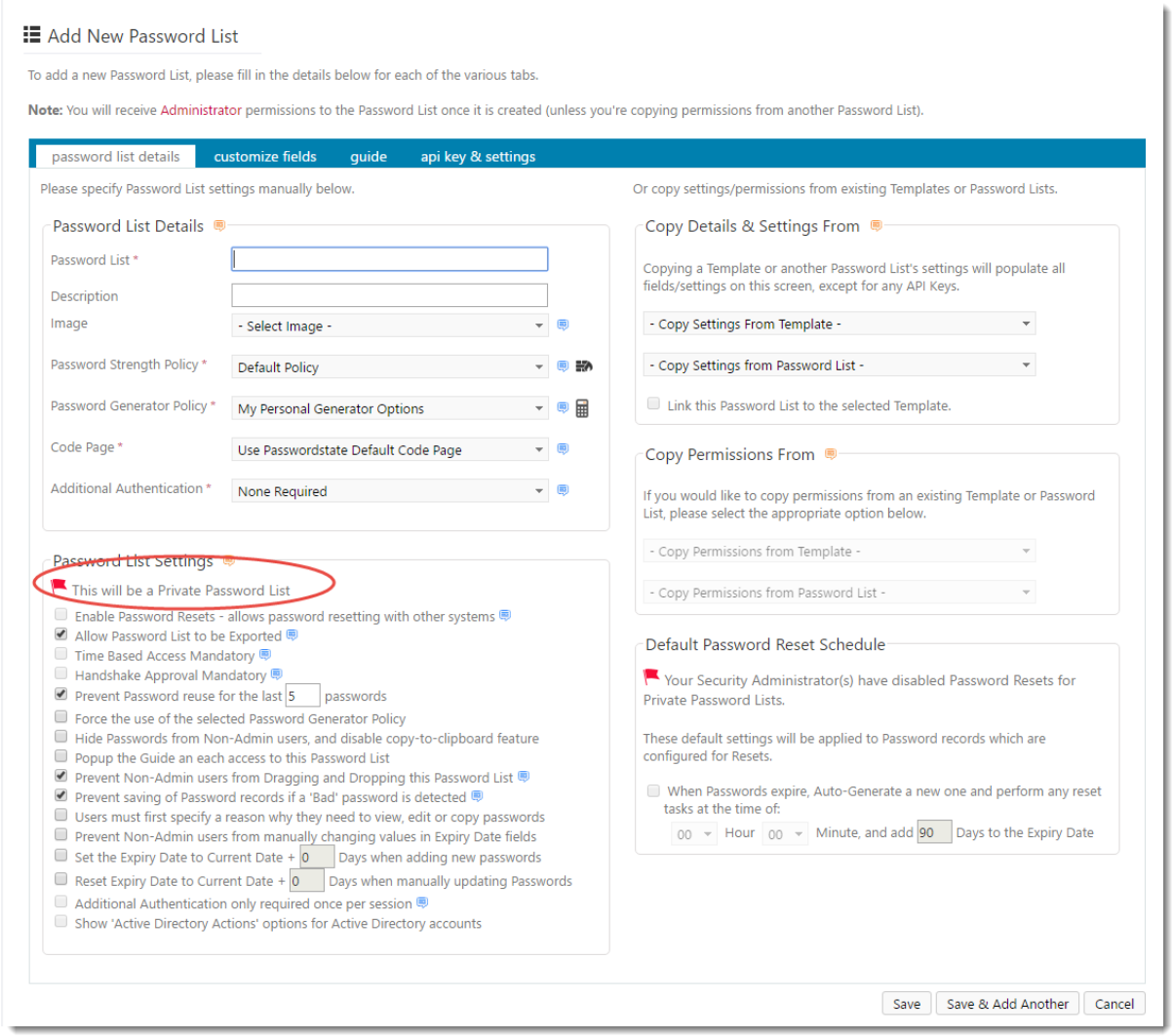
As the majority of settings and features available when creating a Private Password List are the same as Adding/Editing a Shared Password List, you can view the documentation for each of the tabs here - Password List Details Tab, Customize Fields Tab, Guide Tab & API Key & Settings Tab.

Note: 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

© 2017 Click Studios (SA) Pty Ltd

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

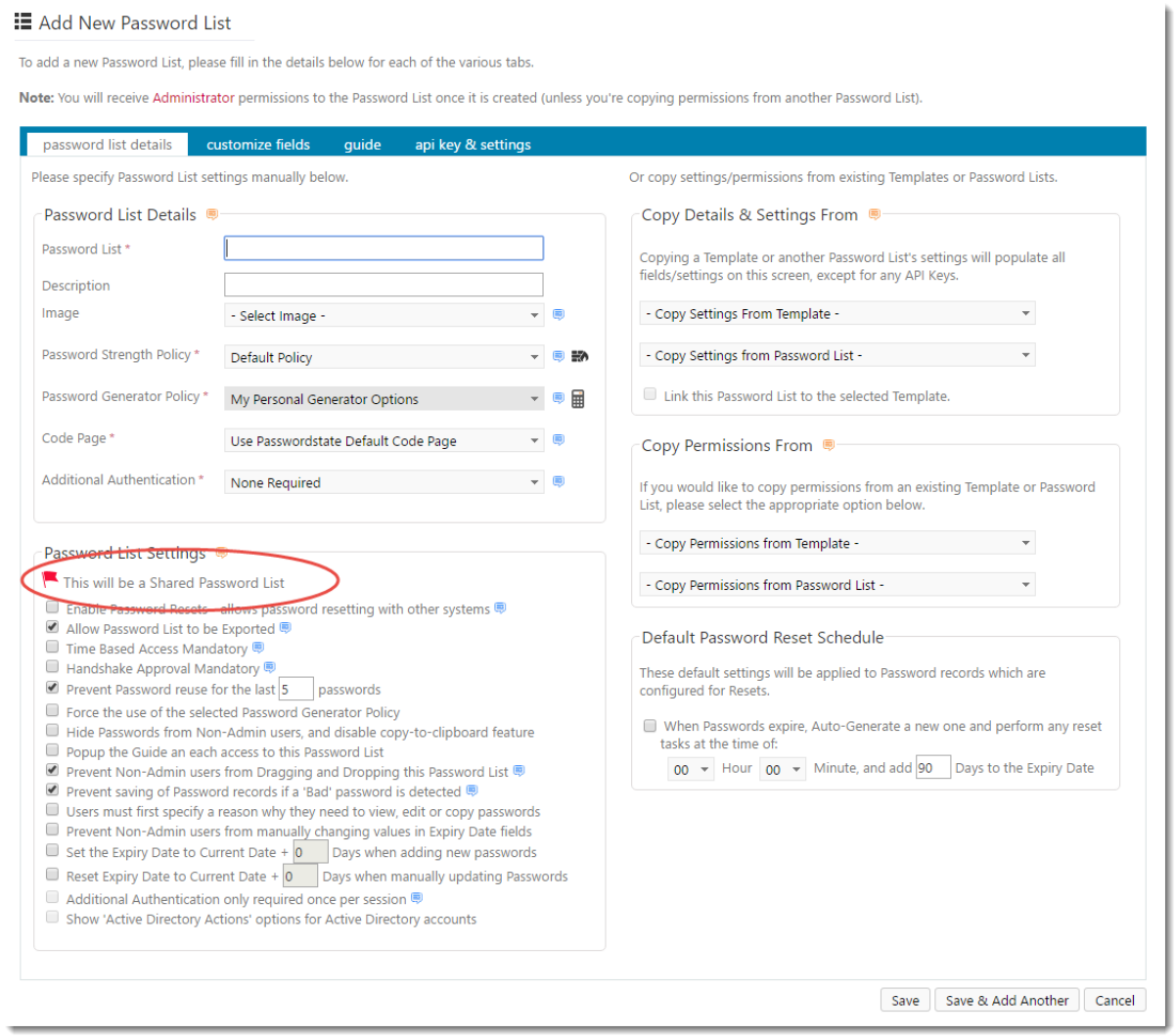
Shared Password Lists are used to share Passwords with teams of people, and allows various types of permissions to be applied - View, Modify or Administrator.

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 & Settings Tab.

© 2017 Click Studios (SA) Pty Ltd

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

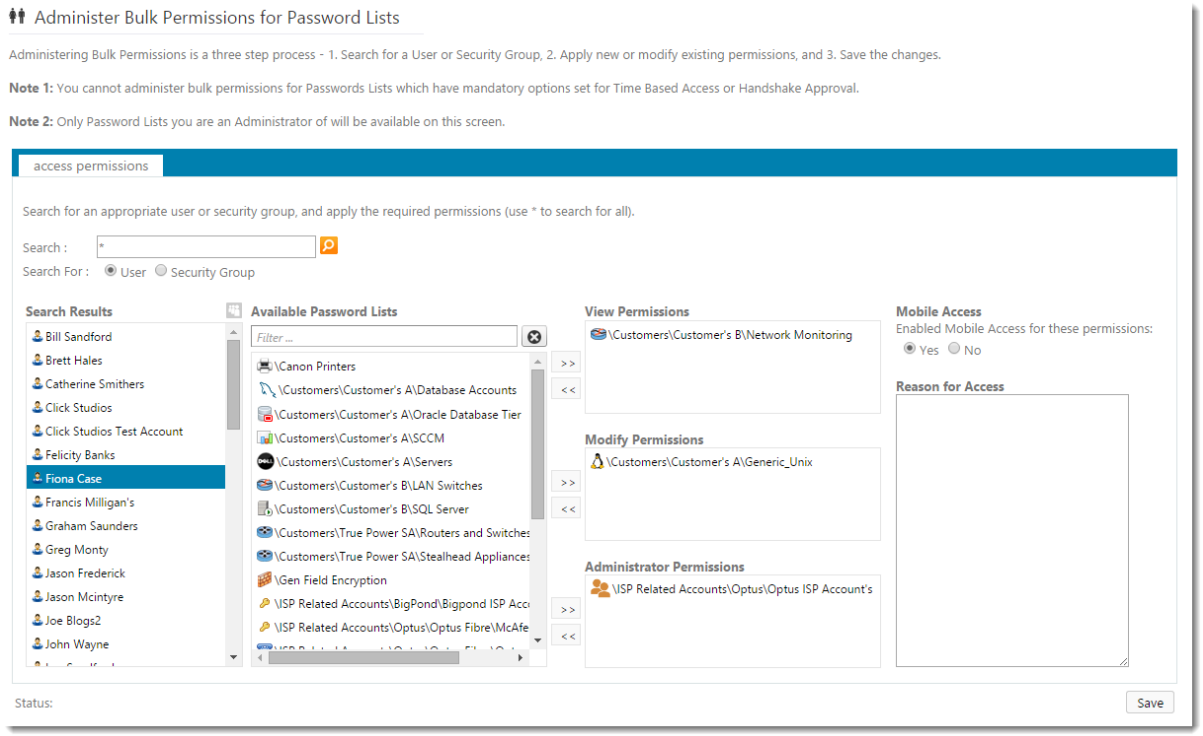
The standard method of apply permissions to a Password List is via the Grant New Permissions button for each individual Password List.

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

© 2017 Click Studios (SA) Pty Ltd

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.



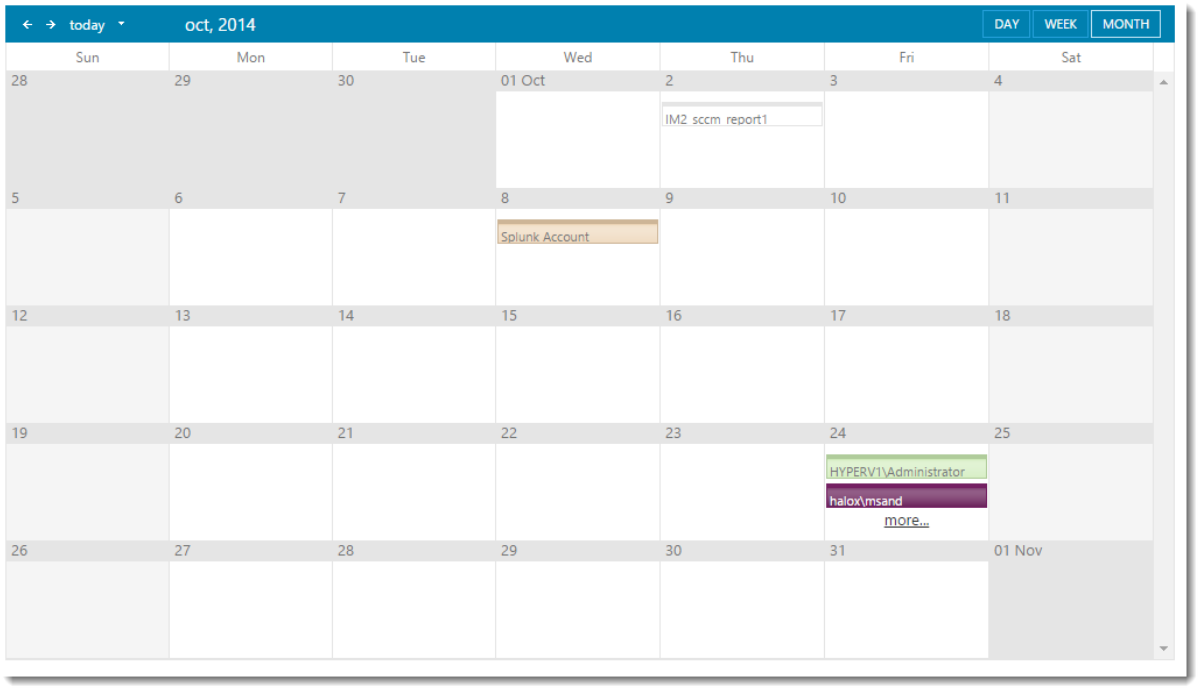
2.6 Expiring Passwords Calendar

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.

© 2017 Click Studios (SA) Pty Ltd



2.7 Password List Templates

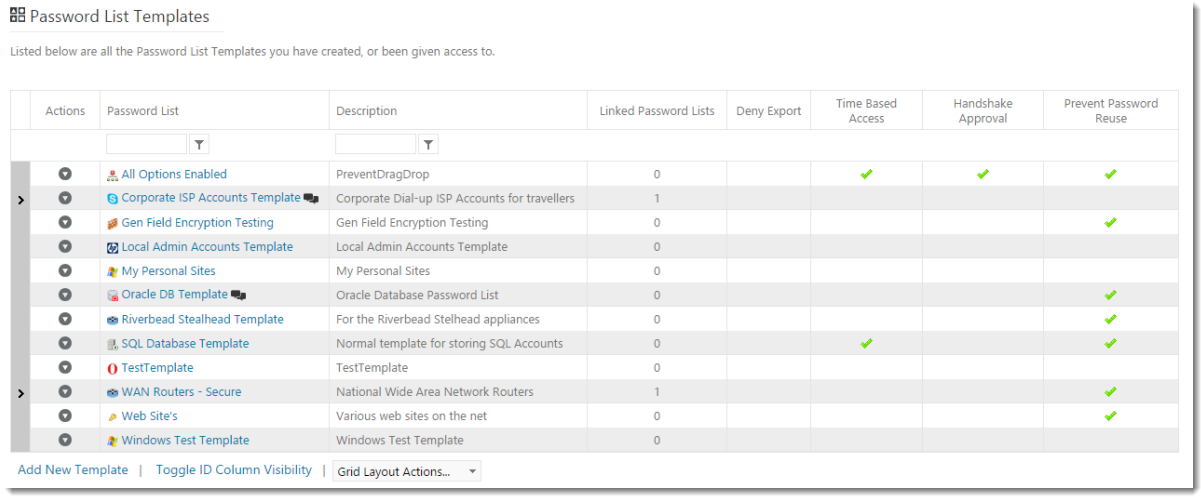
Password List Templates can be used to apply consistency to settings for your Password Lists. They can be used in the following way:

- 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.

© 2017 Click Studios (SA) Pty Ltd



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.

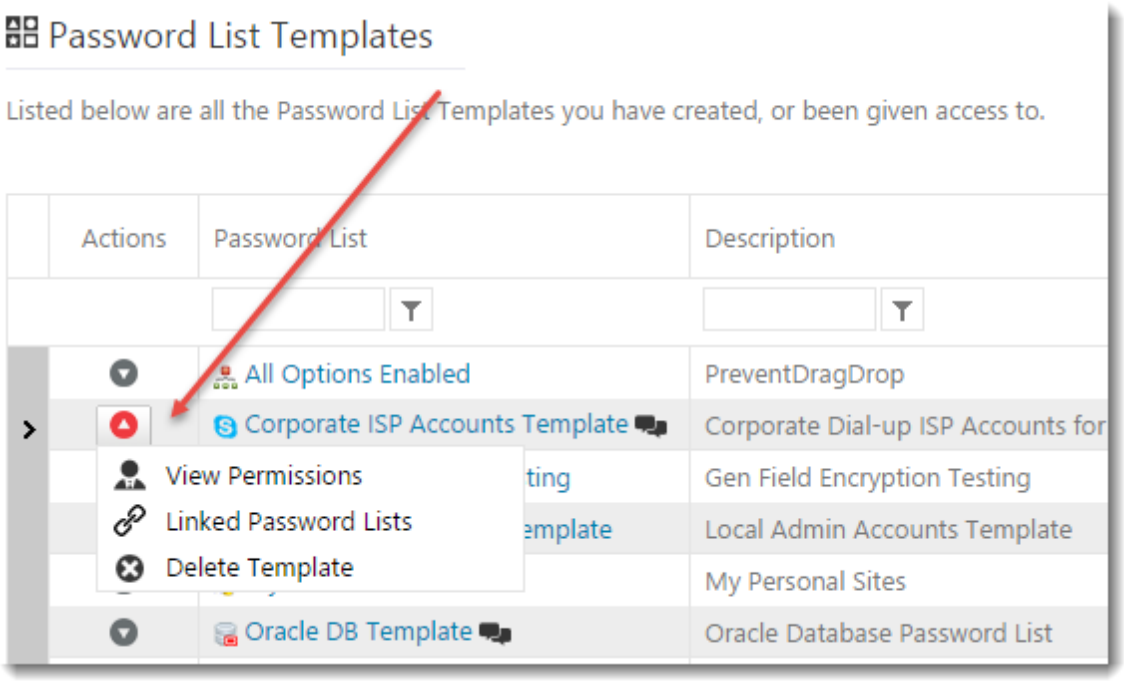
Password List Template Actions

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.

© 2017 Click Studios (SA) Pty Ltd

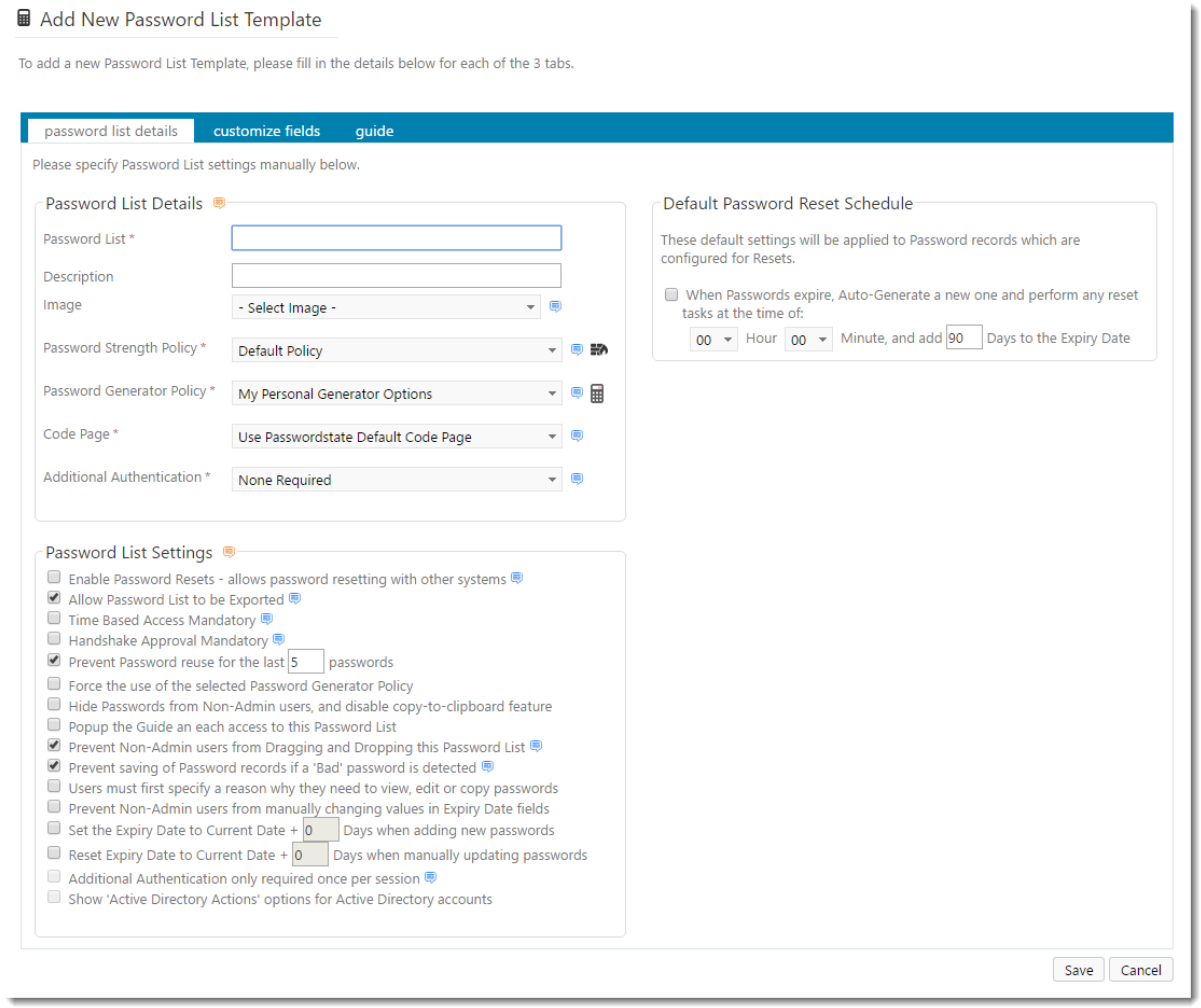


2.7.1 Add New Template

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.

© 2017 Click Studios (SA) Pty Ltd



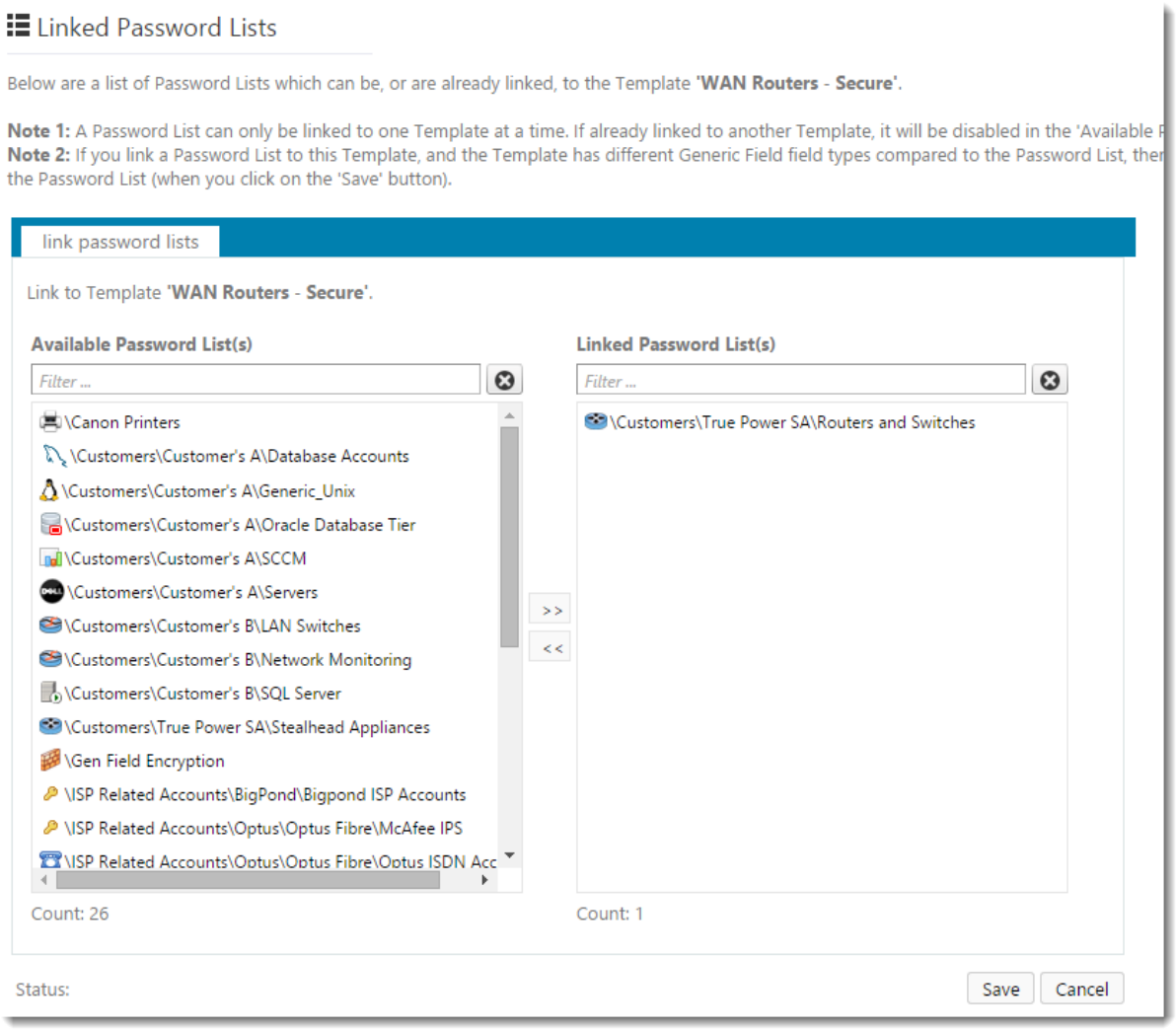
2.7.2 Linked Password Lists

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.

© 2017 Click Studios (SA) Pty Ltd

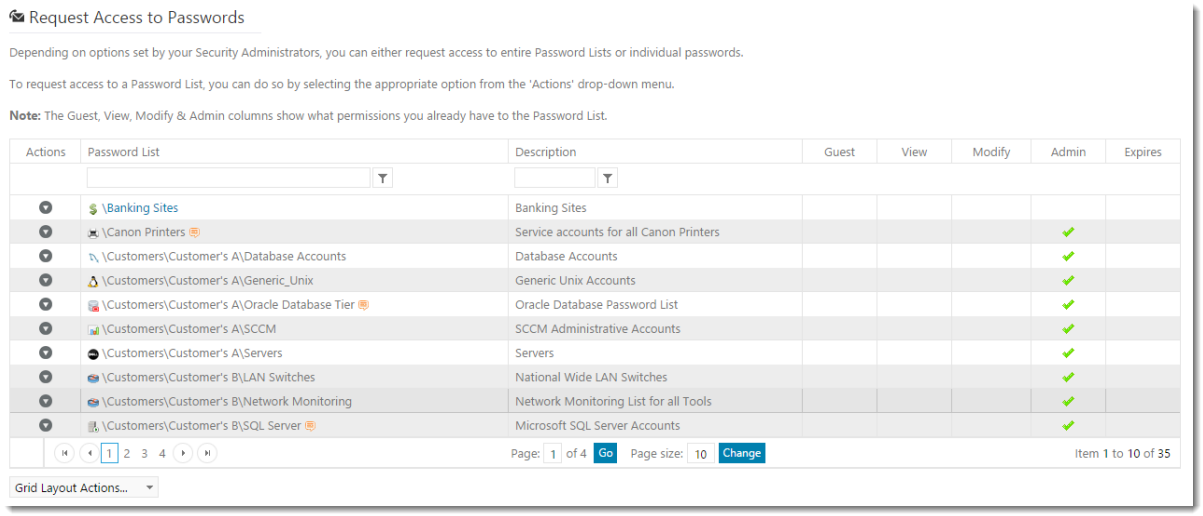


2.8 Request Access to Password Lists

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.

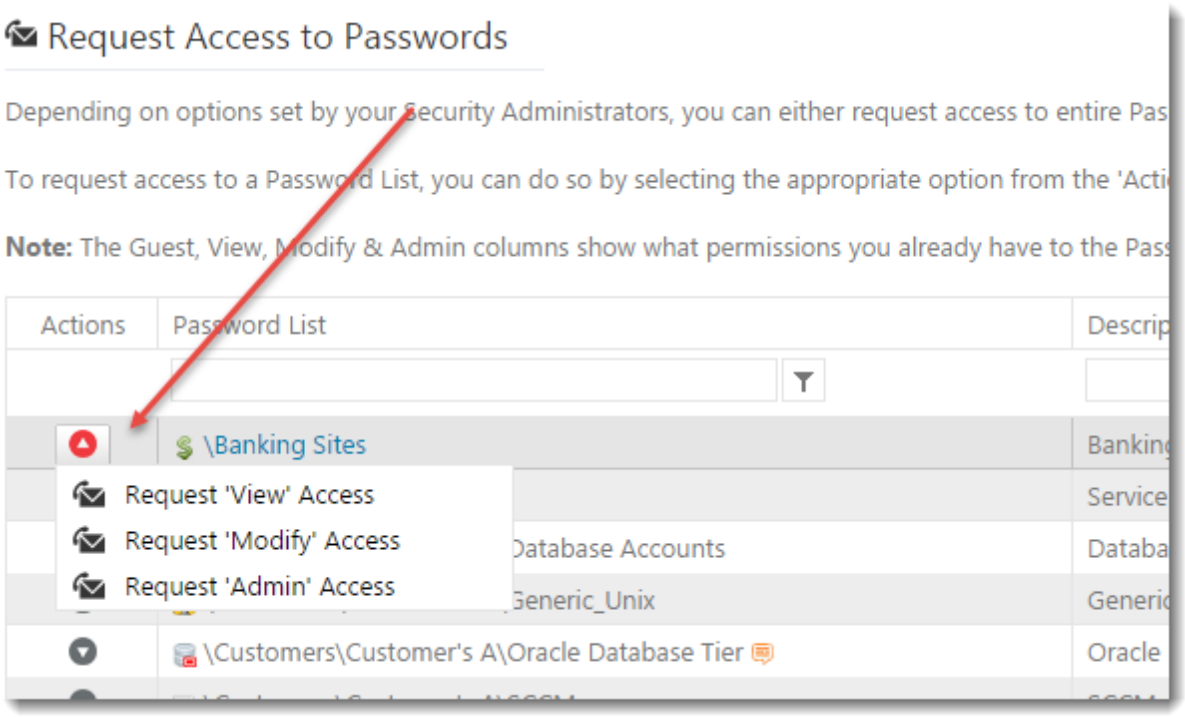
The 'Request Access to Password Lists' screen shows all the Shared Password Lists, and what access you already have - if any. From here you can request access to a Password List, or access to an individual password within a List by clicking on the appropriate link in the 'Password List' column.

© 2017 Click Studios (SA) Pty Ltd



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.

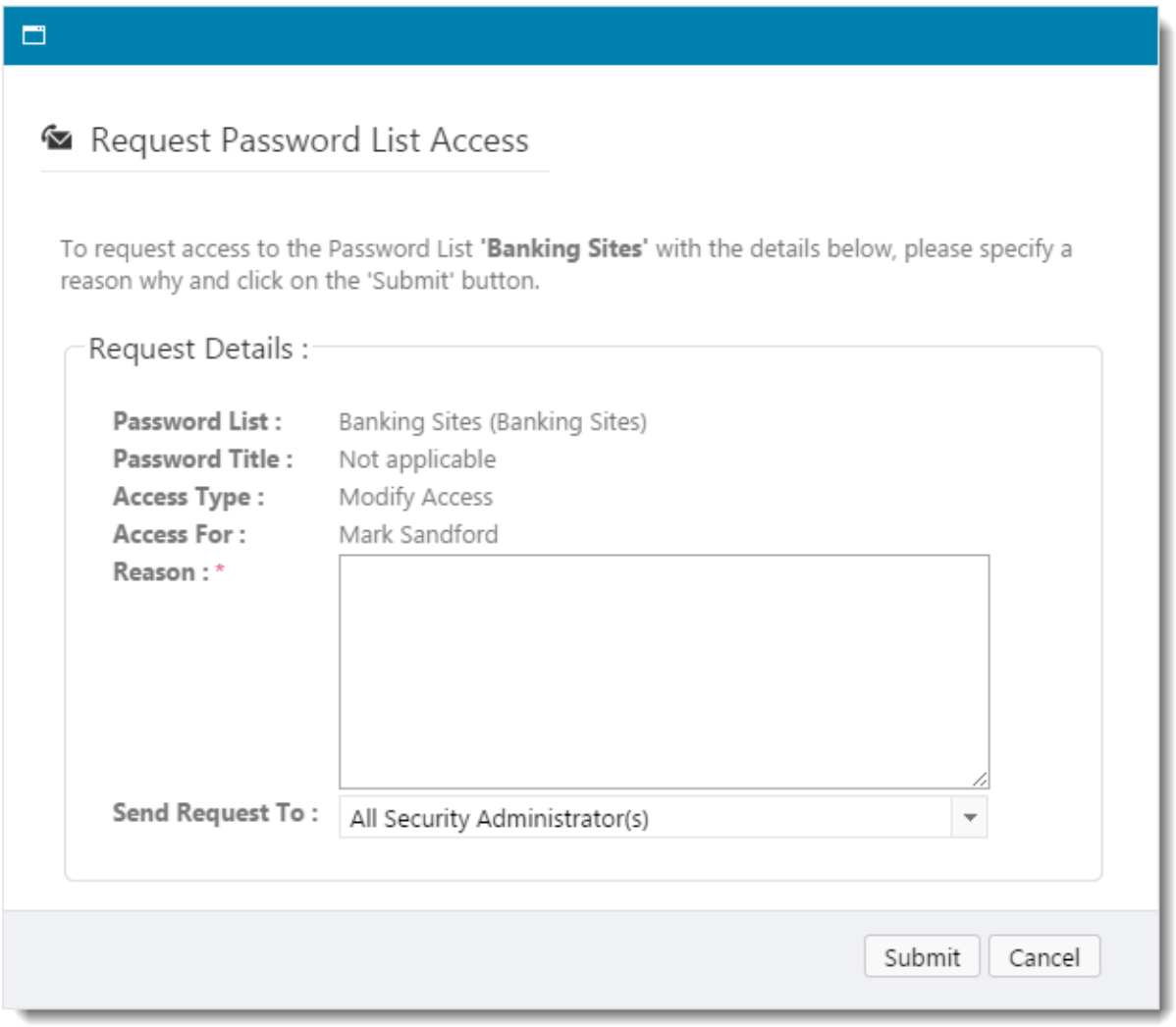


You will then be presented with a popup window where you can specify a reason as to why you require access. When you click the 'Submit' button, the request will be routed to the Administrator(s) of the Password List.

When requesting access, you can send the request to all Administrators of the Password List, or

© 2017 Click Studios (SA) Pty Ltd

you can pick a specific Administrator to send the request to.

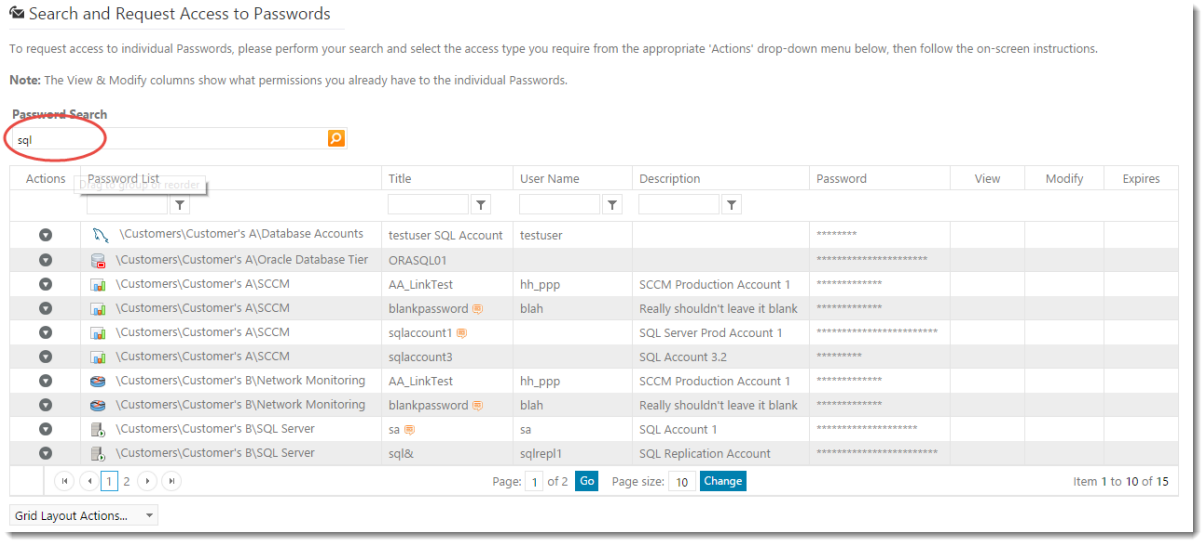


2.9 Request Access to Passwords

If you only require access to one or more individual password records, and not an entire Password List, the 'Request Access to Passwords' menu allows you to search for the password you require, and then request access from the Password List Administrator(s).

Once you have found the password you require access to, simply choose the preferred access level from the appropriate 'Actions' menu, and then submit your request.

© 2017 Click Studios (SA) Pty Ltd



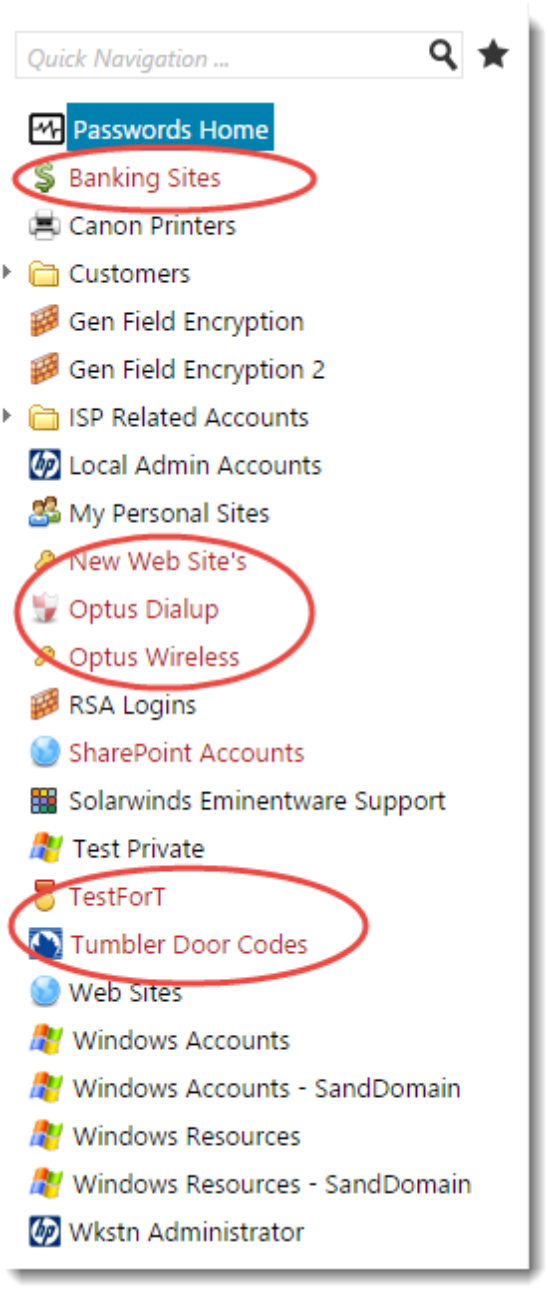
2.10 Toggle All Password List Visibility

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

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

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

© 2017 Click Studios (SA) Pty Ltd



3 Tools Menu

There are three options available under the Tools menu.

Password Generator	Allows you to generate one or more randomly generated passwords
Remote Session Launcher	Opens a separate browser window, which will not log you out, that allows for remote session launching to hosts i.e. RDP, SSH, Telnet and VNC

© 2017 Click Studios (SA) Pty Ltd

Self Destruct Message	Allows you to generate and send a Self Destruct email message to another user

3.1 Password Generator

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

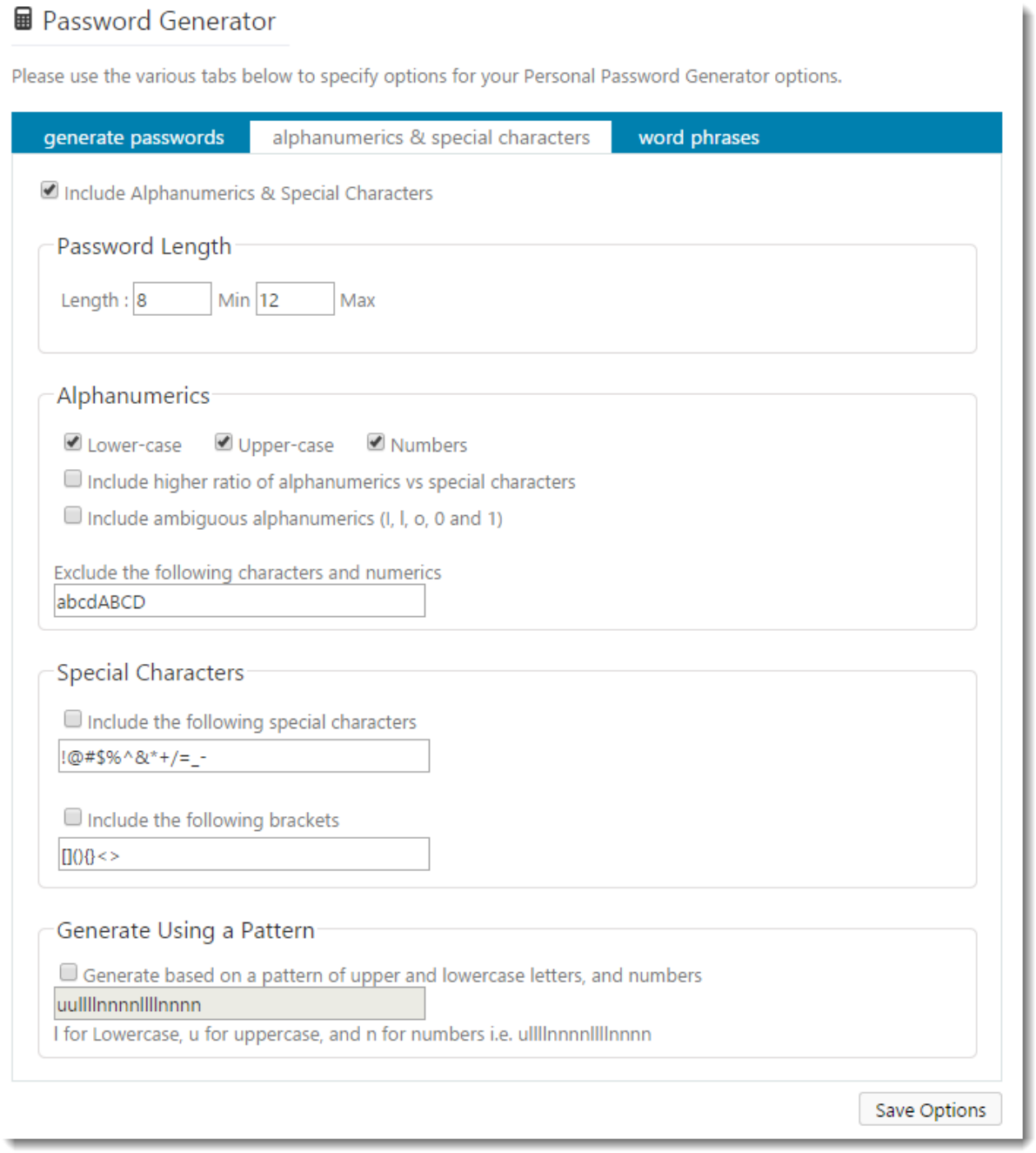
Note: The Security Administrators of Passwordstate can create different Password Generator Policies and apply them to various Password Lists, so if you generate a new random password when adding/editing a Password record, the password does not seem to conform to your personal settings, then most likely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

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

Alphanumeric & Special Characters

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

© 2017 Click Studios (SA) Pty Ltd

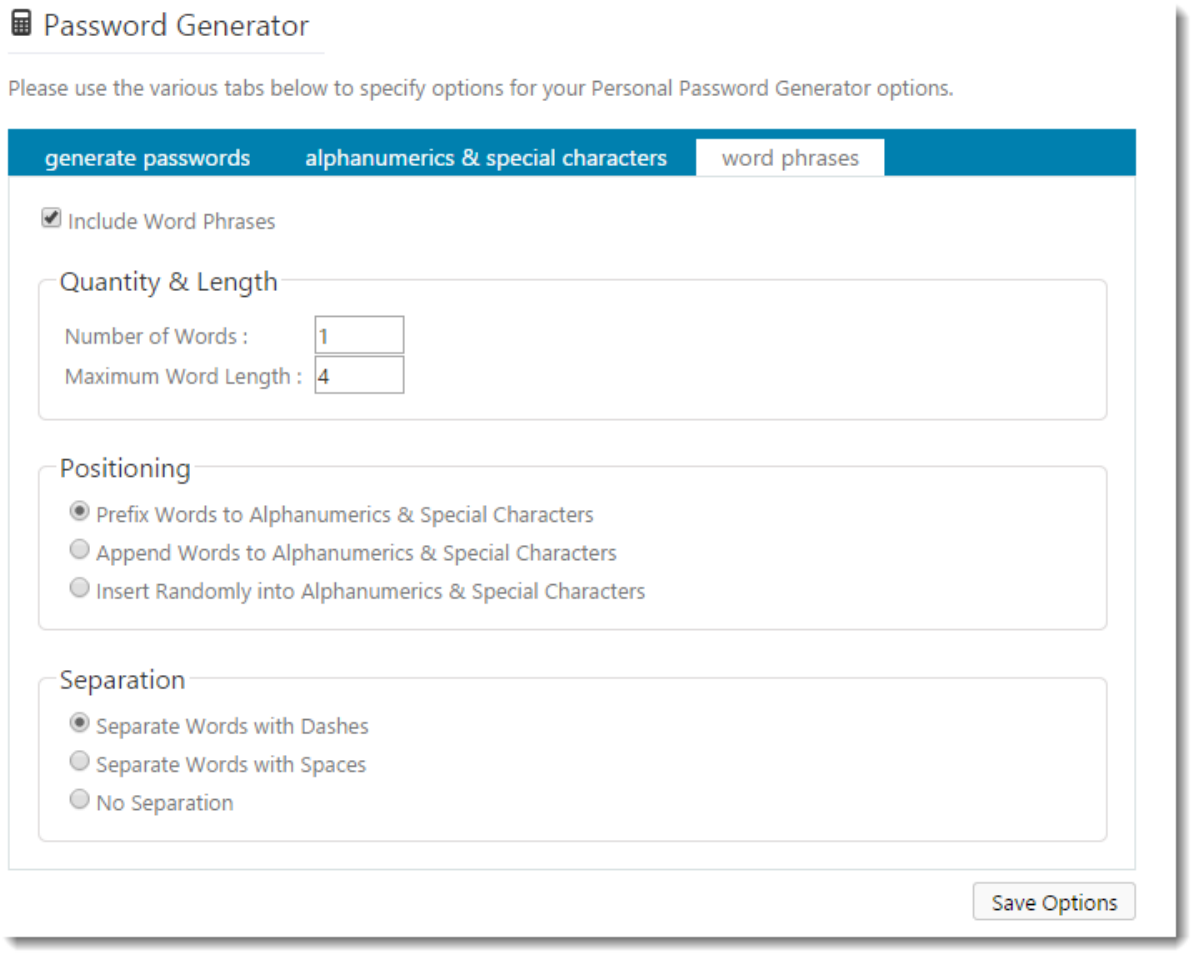


Word Phrases

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.

© 2017 Click Studios (SA) Pty Ltd



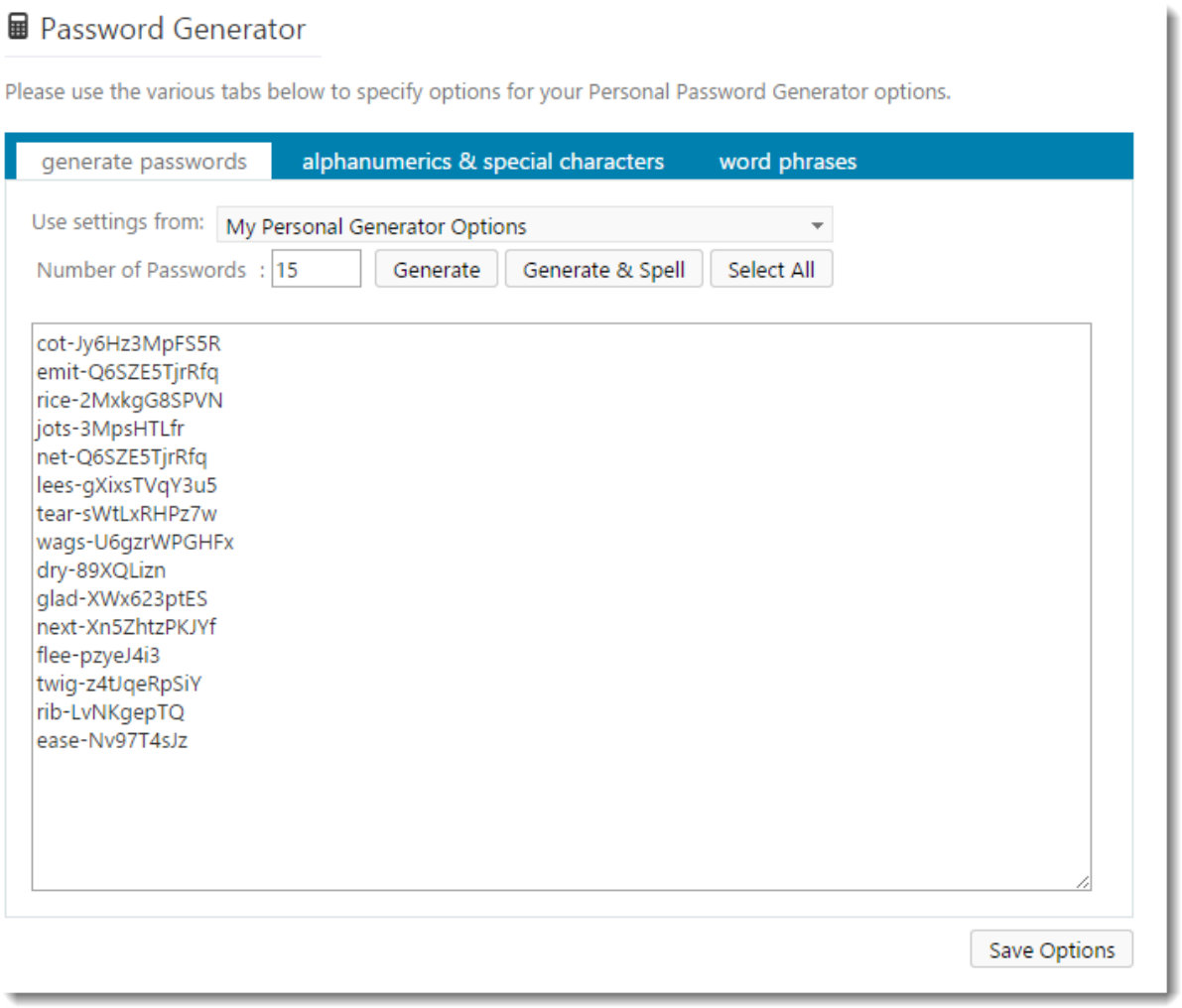
Generate Passwords

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

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

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

© 2017 Click Studios (SA) Pty Ltd



3.2 Remote Session Launcher

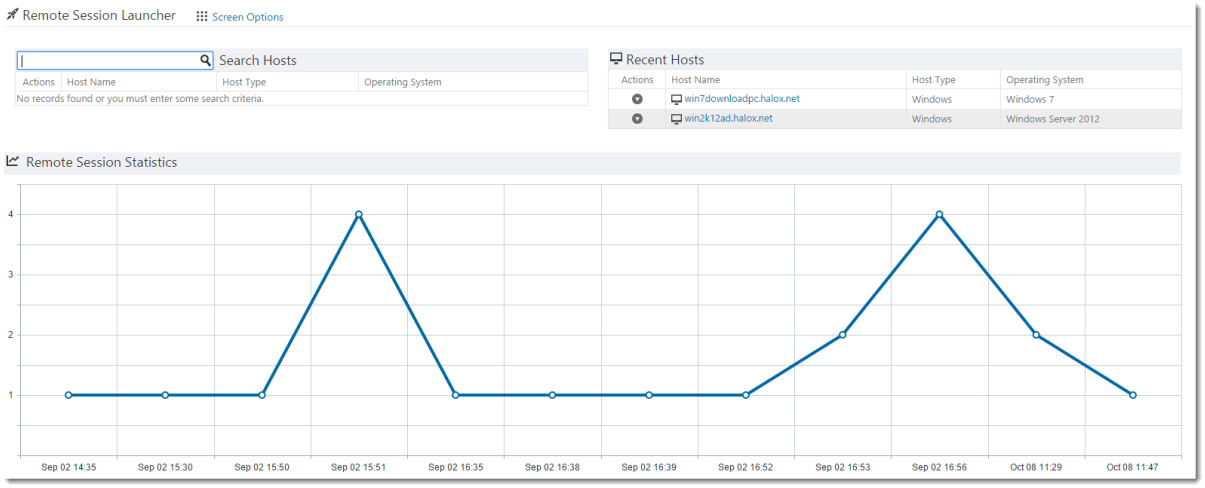
The 'Remote Session Launcher' menu allows for remote session launching to hosts using RDP, SSH, Telnet or VNC. If your session in Passwordstate times out while on this screen, you will be returned back to it when you next login.

Note: Remote Session Launching is only available from Windows Hosts

In order to use the Remote Session Launcher feature, the following is required:

- You must have PowerShell 3.0 or above installed on your desktop computer, and the Passwordstate Remote Session Launcher utility
- You must have added/imported/discovered the Hosts you want to initiate the Remote Session with, and have been give access (permissions) to the Hosts - Hosts and Resources
- You must have created one or more Remote Session Credentials queries, so the automatic logins will occur - Remote Session Credentials

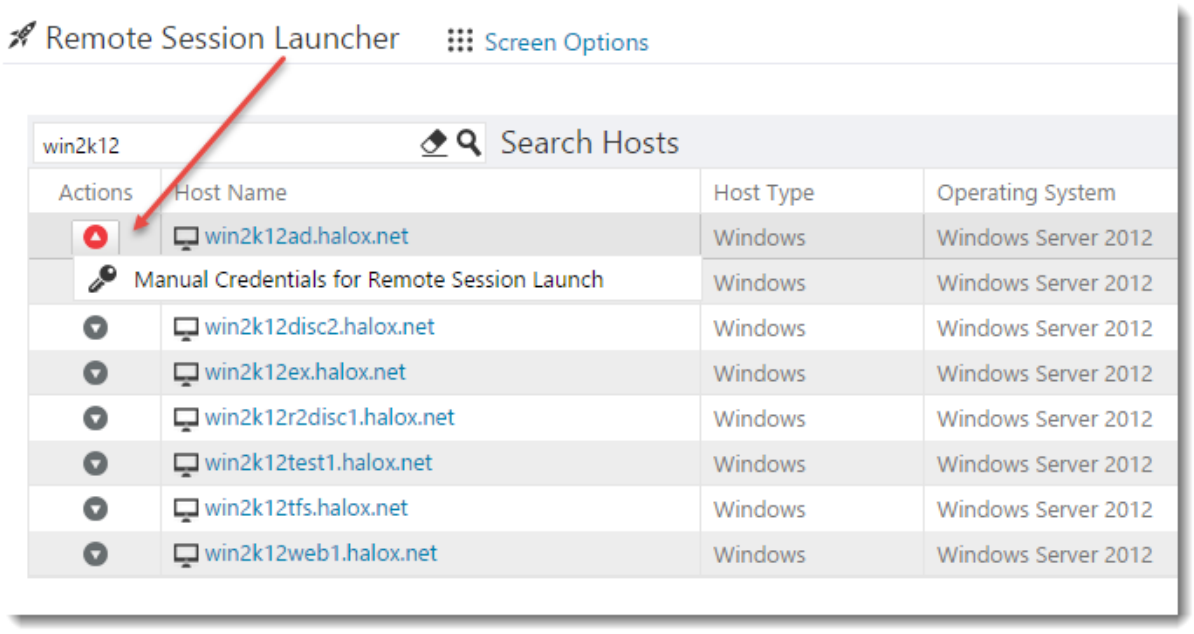
© 2017 Click Studios (SA) Pty Ltd



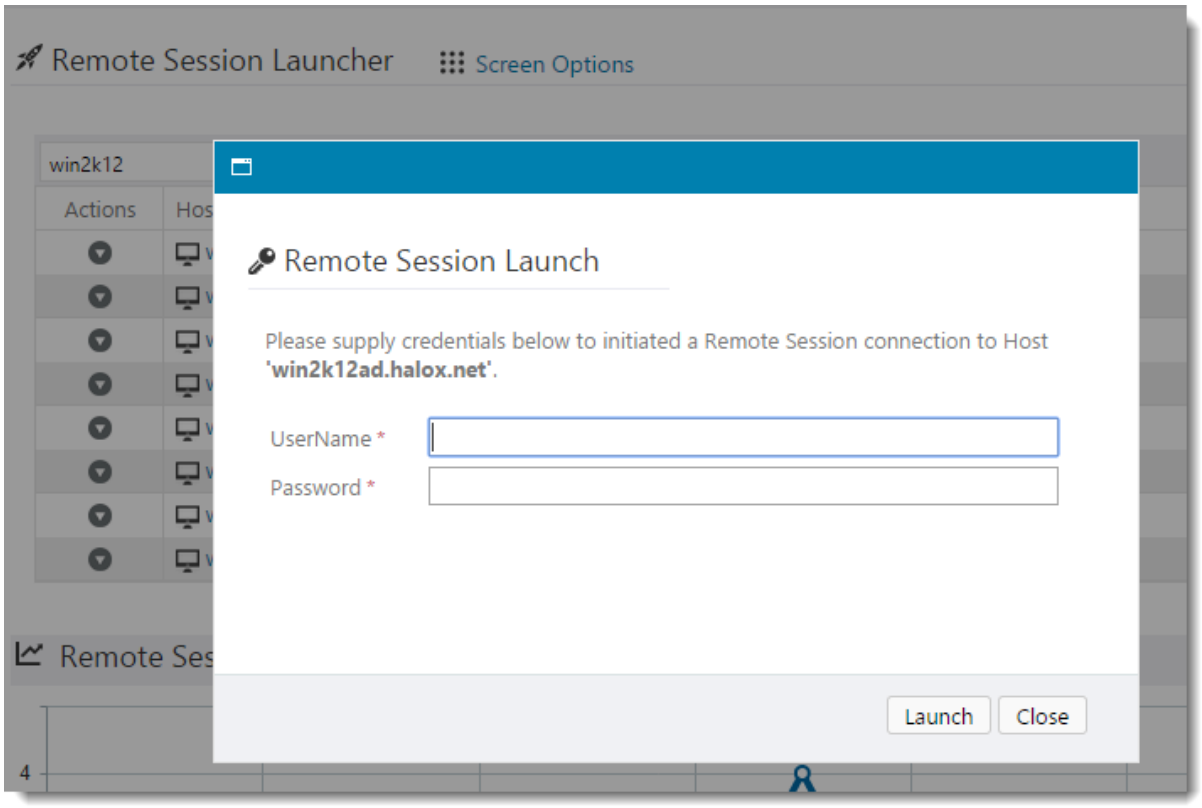
Authentication Options

There are several possibilities for supplying credentials for the Remote Session login:

- If only one credential is found from the query/queries you have created on the Remote Session Credentials page, then simply clicking on the Host in either of the 'Search Hosts' or 'Recent Hosts' grid will launch the remote session and log in for you automatically
- If more than one credential is found from the query/queries you have created on the Remote Session Credentials page, then you will be presented with a popup page asking you to choose which credential to authenticate with
- If you simply want to specify the authentication credentials manually, then you can do so using the 'Manual Credentials for Remote Session Launch' menu option as per the screenshot below



© 2017 Click Studios (SA) Pty Ltd



3.3 Self Destruct Message

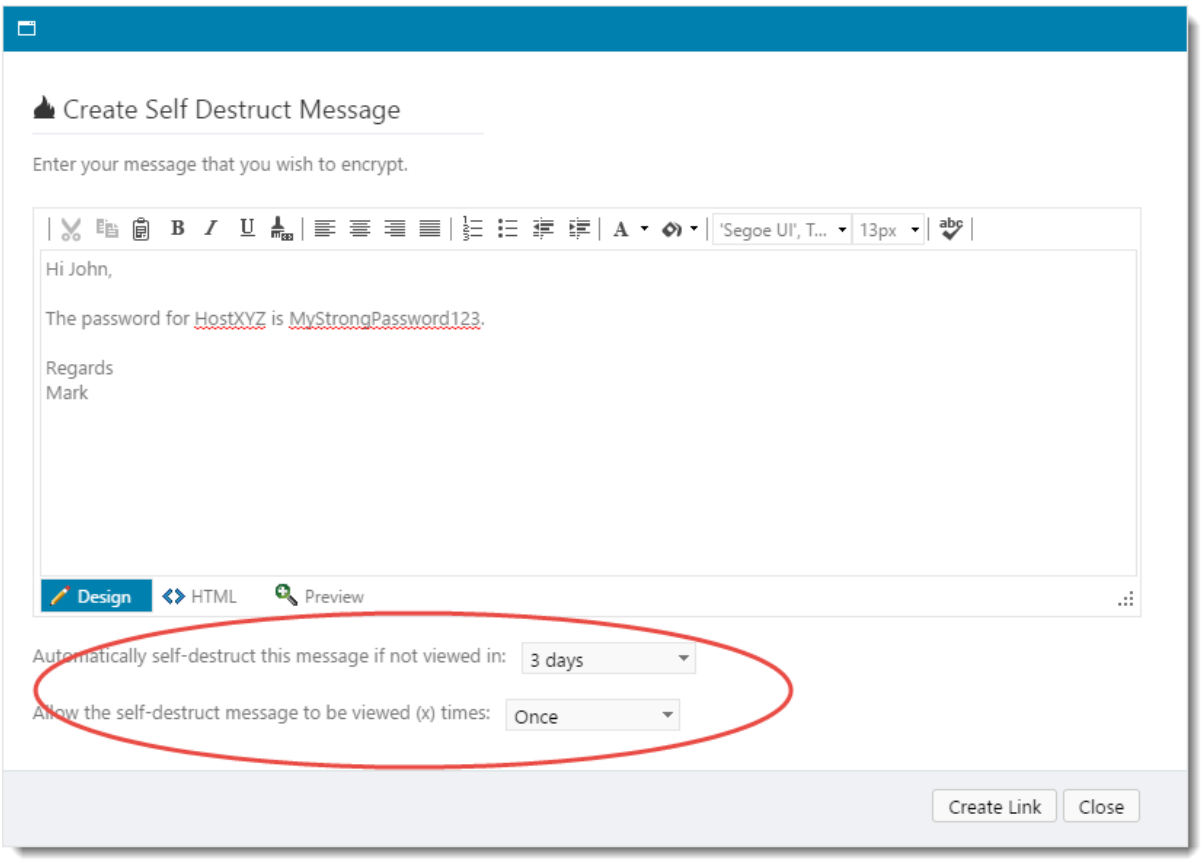
The Self Destruct Message menu allows you to generate and send a Self Destruct email message to another user - the message expires after the set time period, if not read.

Creating a Self Destruct message is a two step process:

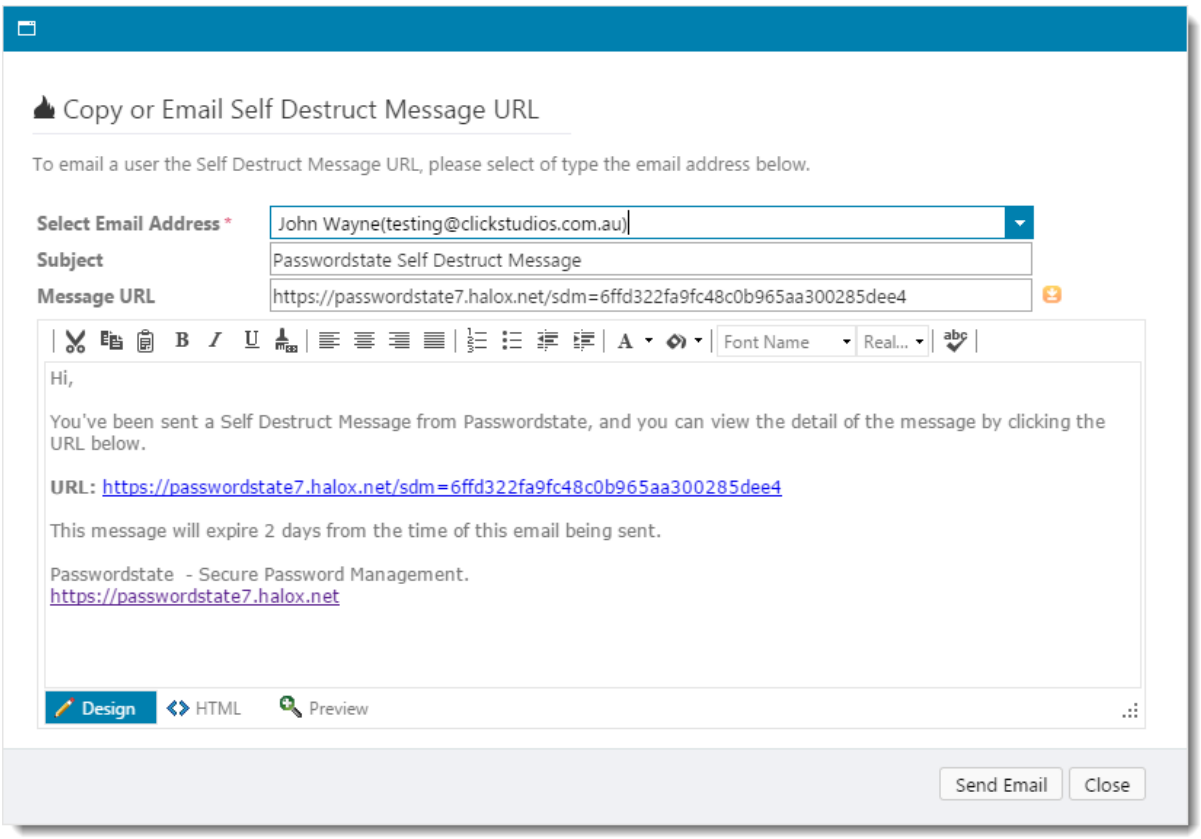
1. Specify the message, how long the message will be active for, and how many times the message can be viewed
2. Then choose the user you want to send the message to

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

© 2017 Click Studios (SA) Pty Ltd



© 2017 Click Studios (SA) Pty Ltd



4 Resets Menu

The Resets menu contains the bulk of the features which allows for Password Resets to occur on remote Hosts, Remote Sessions to be launched (RDP, SSH, Telnet and VNC), and to validate passwords stored in Passwordstate match what is currently in use on the remote Hosts/Systems.

Hosts	Add/Import/Edit hosts
Hosts and Account Discovery	Allows you to discovery Windows Hosts, Local Admin Accounts, and Windows Services/IIS Application Pools/Scheduled Tasks which are using a domain account as their identity
Queued Password Resets	Shows any records which are currently sitting in the queue to perform password resets
Scripts - Account Discovery	Shows the two default scripts for perform various types of account discovery on your network
Scripts - Password Resets	Shows all the default, and any custom, PowerShell scripts for performing password resets on AD accounts, and any accounts on remote Hosts
Scripts - Password Validation	Shows all the default, and any custom, PowerShell scripts for performing account password validation in AD and on remote Hosts

© 2017 Click Studios (SA) Pty Ltd

4.1 Hosts

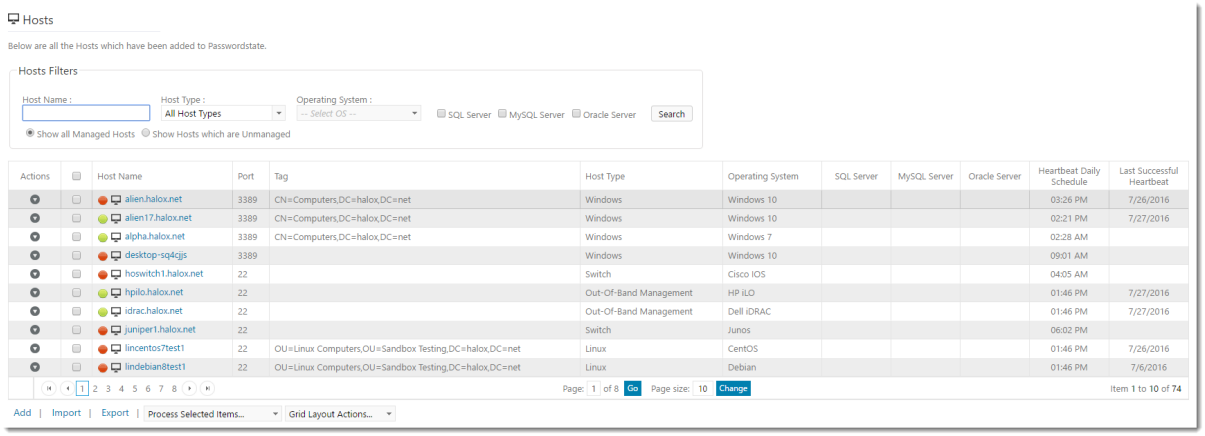
The Hosts Menu allows you to Add/Import/Edit hosts into Passwordstate, so they can be used to perform Password Resets for accounts used on the Hosts, or so they can be used for the Remote Session Launcher feature.

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

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

Note 1: By default, all users of Passwordstate has access the Hosts area. If you want to restrict this, it can be done via the screen Administration -> Menu Access, where you can hide the entire menu. If you want your users to see all the Host records, but make no changes to them, then you can restrict this access via the screen Administration -> System Settings -> Host tab

Note 2: On the screen Administration -> System Settings -> Hosts, there are various settings you can configure for the Host Heartbeat polling process, including setting a Host to Unmanaged, or deleting the Host record, if it's not seen on the network for a set period



Adding New Hosts Manually

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

- Specifying the FQDN for the host name results in improved performance when resetting passwords, and launching Remote Sessions. It also offers greater flexibility for non-trusted

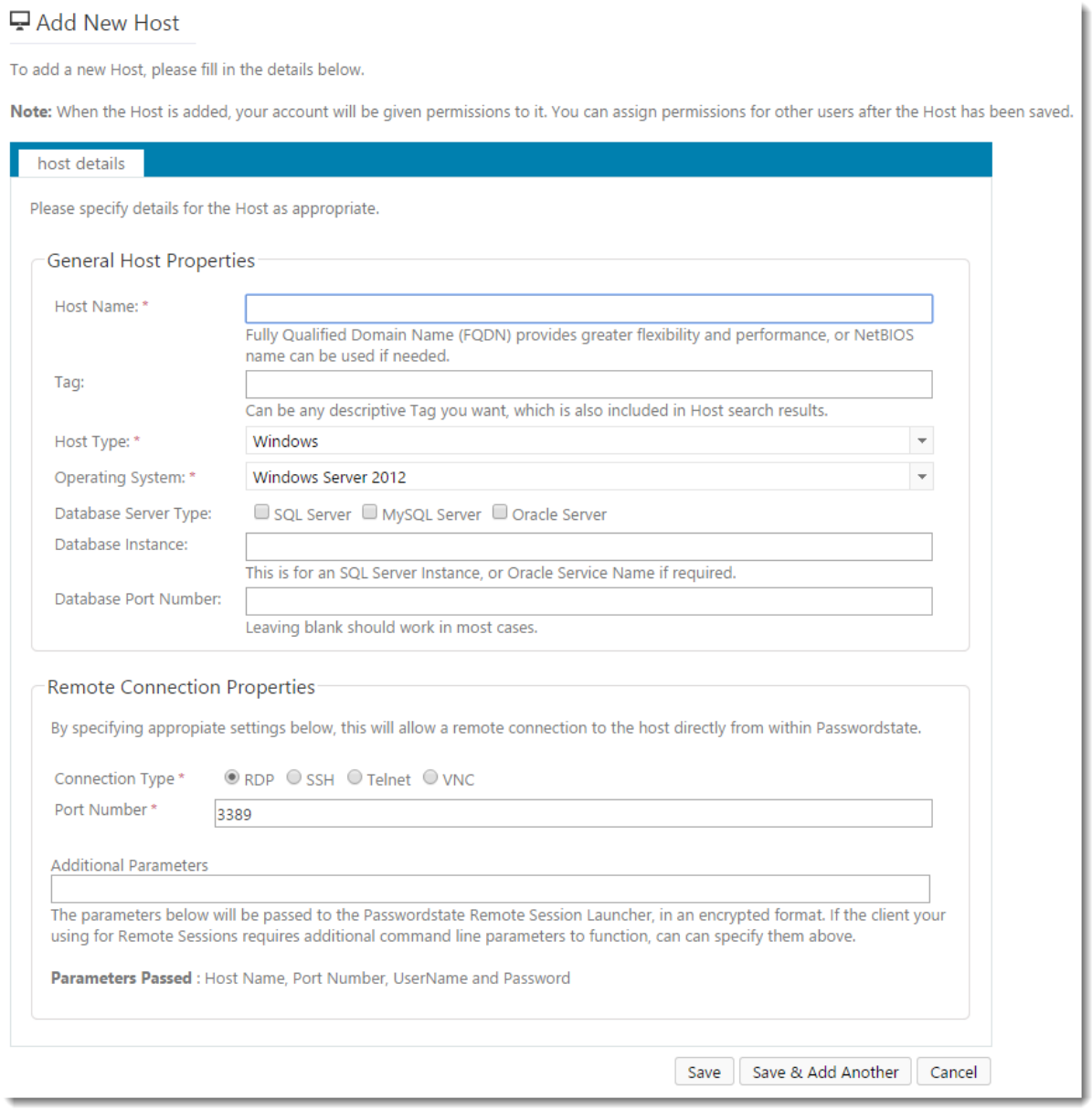
© 2017 Click Studios (SA) Pty Ltd

Active Directory Domains, as you can apply Password Reset Scripts, Password Validation Scripts, or Remote Session Credentials, based on the domain name the host is joined to

- The Tag field can be any value you like, and is included in the search results when searching for the 'Host Name'. If using a Discovery Job for searching for Hosts in Active Directory, there's an option to include the Host's OU in the Tag field
- If the Host is a MS SQL, MySQL Server or Oracle Server, you can specify Instance details and port numbers if needed, so Passwordstate can connect to it to execute Password Reset Scripts
- If using the Remote Session Launcher utility, you can specify various properties for launching remote sessions i.e. Connection Type, Port Number, and possibly any other Remote Session Parameters needed for the Remote Session client program you're using

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

© 2017 Click Studios (SA) Pty Ltd



4.2 Hosts and Account Discovery

The Hosts and Account Discovery Menu allows you to discovery Windows Hosts on your network, Local Admin Accounts, and Windows Services/IIS Application Pools/Scheduled Tasks which are using a domain account as their identity.

There are 3 categories for Discovery on your network:

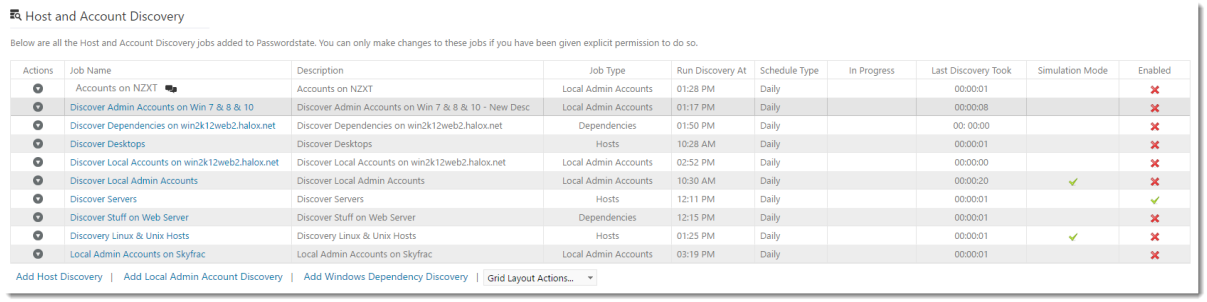
1. Discovering Windows Hosts
2. Discovering Local Administrator Accounts on Windows Servers/Desktops
3. Discovering Windows Dependencies - Windows Services, IIS Application Pools and Scheduled Tasks which are configure to use a domain account as their identity

© 2017 Click Studios (SA) Pty Ltd

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

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

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



Discover Windows Hosts

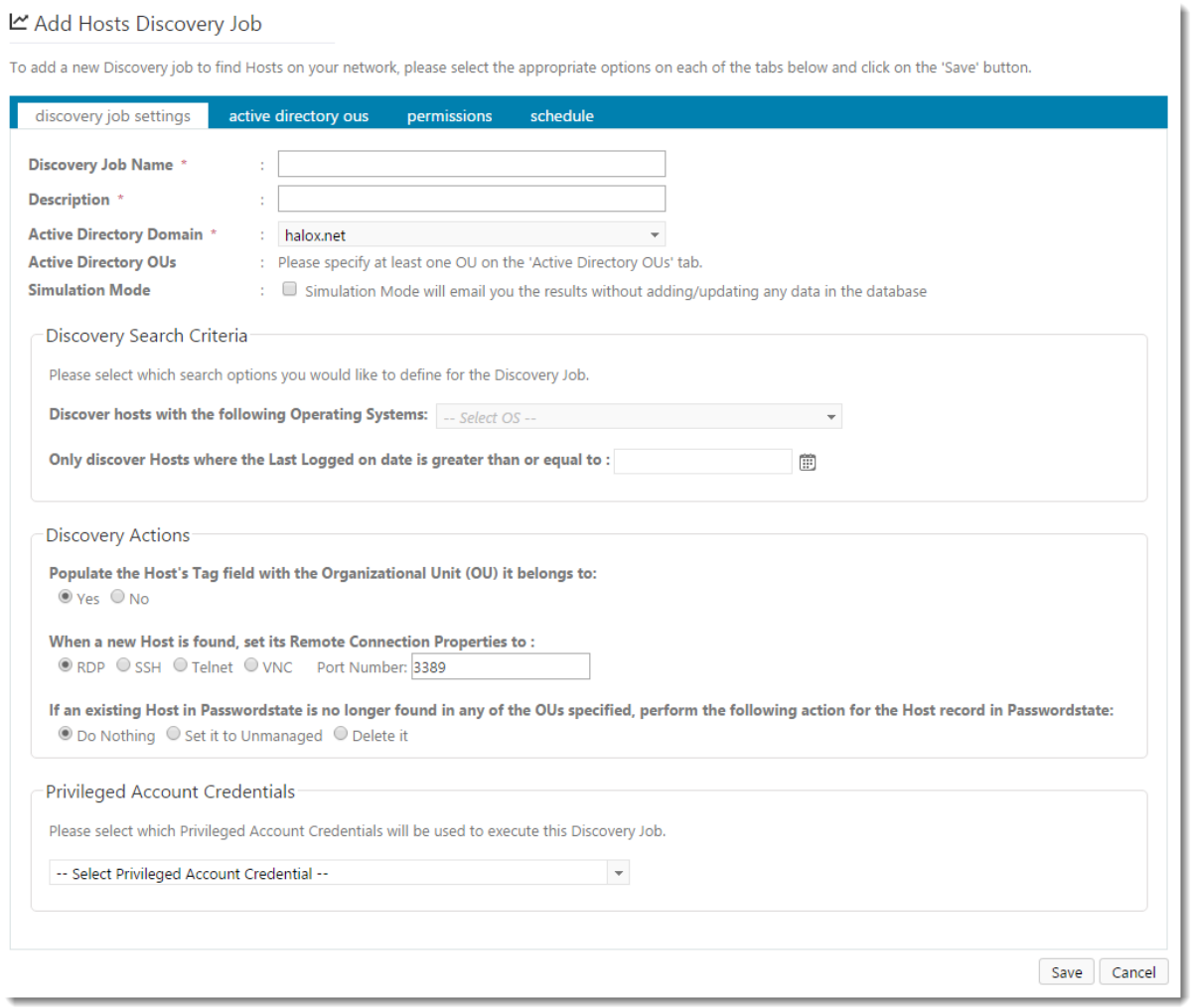
Discovering Windows & Linux Hosts on your network is simply a query of your Active Directory domain - Passwordstate does not go out into your network discovering host by host manually. Because of this, no specify system requirements are necessary, except for a domain account with privileges to query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

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

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

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

© 2017 Click Studios (SA) Pty Ltd



Discover Local Administrator Accounts

When discovering Local Administrator Accounts on Windows Hosts on your network, there are many options available to you. In particular:

- You can filter on the type of Hosts you want to query, based on the Operating System type, or any sort of Host Name wildcard match - this queries the Hosts found on the screen Hosts
- If a new Local Administrator's account is found, you can specify which Password List to store the password record into. If the account is found in another Password List when the discovery executes, it will not add in a duplicate record
- As it's not possible to decrypt Windows Passwords, you will need to specify what password will be recorded in Passwordstate initially for the Local Admin account, or you can generate a random one. You also have the option to perform a password reset for any newly discovered accounts, and the password value for these accounts will be set to what's selected here - either a static password, or a randomly generated one
- When new records are added to the selected Password List, you have the option to also specify

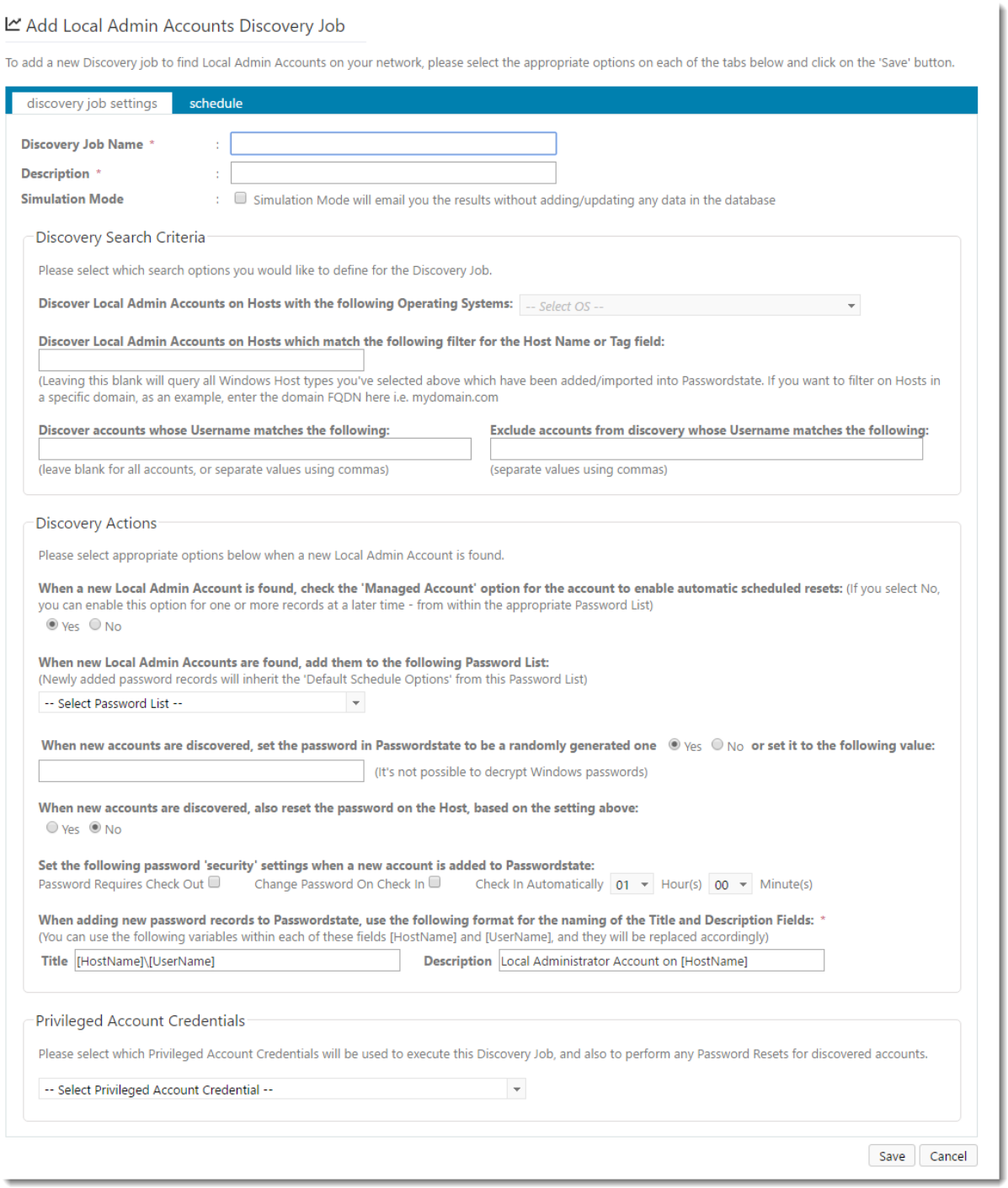
© 2017 Click Studios (SA) Pty Ltd

some detail for the Title and Description fields.

- You also need to specify the Privileged Account Credentials to use when interrogating your Windows Hosts on the network - this account will need sufficient privileges to query the membership of the Administrator's Security Group
- If you do not wish to automatically configure the discovered accounts to perform scheduled resets, you can set the 'Managed Account' option to No. Then later within the Password List, you can enable this option for one or more records at a time - either by editing individual records, or using the Bulk Update Password Reset Options feature
- There are also various options you can set the the Check In/Out feature aswell

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

© 2017 Click Studios (SA) Pty Ltd



Discover Windows Dependencies

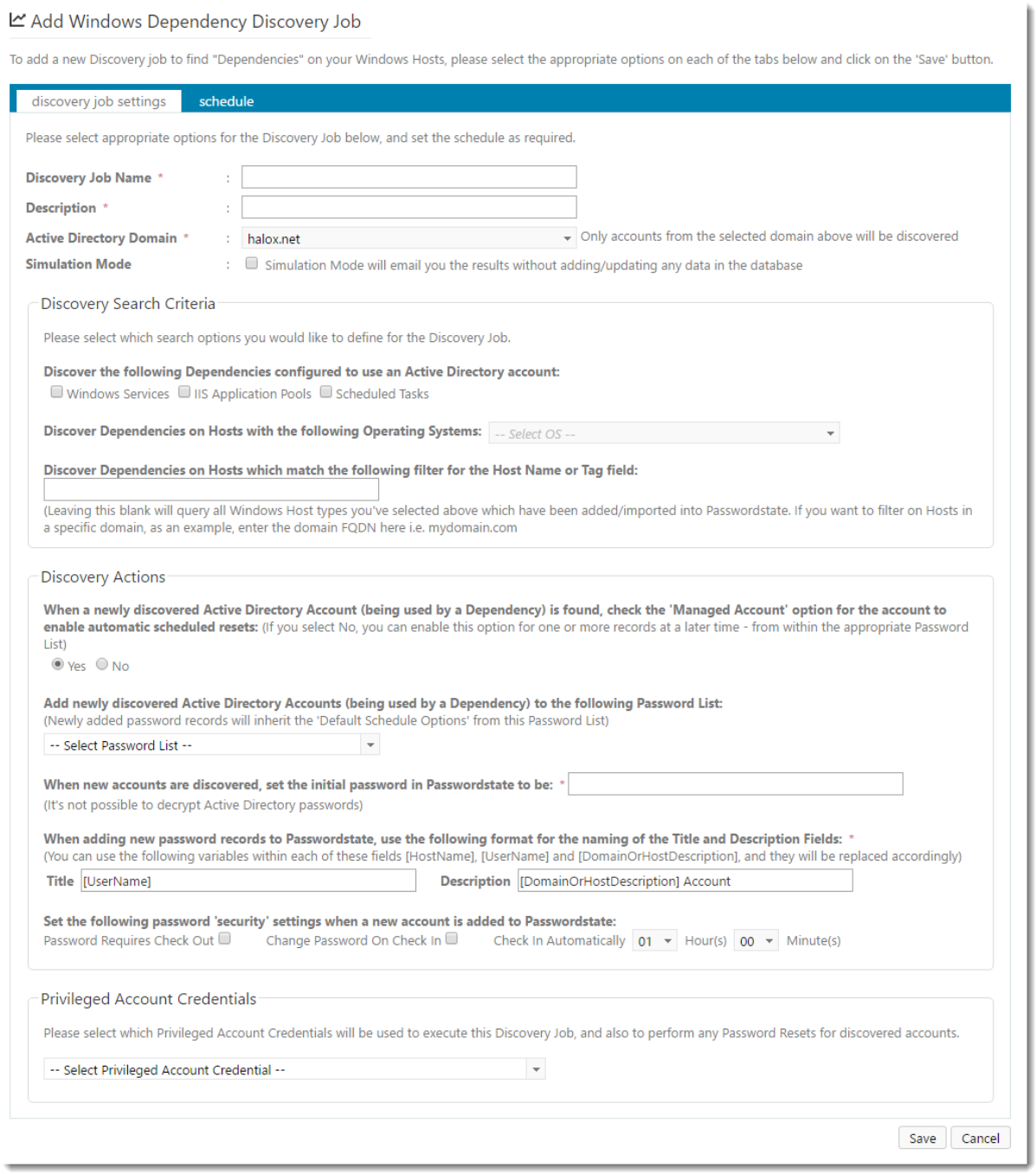
It's possible to also discovery various 'Windows Dependencies on your network that are using domain accounts as their identity to run under i.e. Windows Services, IIS Application Pools & Scheduled Tasks. When setting up such a Discovery Job, the following options are available:

© 2017 Click Studios (SA) Pty Ltd

- You need to select which 'Dependencies' you want to try and discover - Windows Services, IIS Application Pools or Scheduled Tasks - can you select all of them as part of the same Discovery Job if you want
- The rest of the options are very similar to discovery of Local Admin Accounts
- If you do not wish to automatically configure the discovered accounts to perform scheduled resets, you can set the 'Managed Account' option to No. The later within the Password List, you can enable this option for one or more records at a time
- And don't forget to set the Schedule

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

© 2017 Click Studios (SA) Pty Ltd

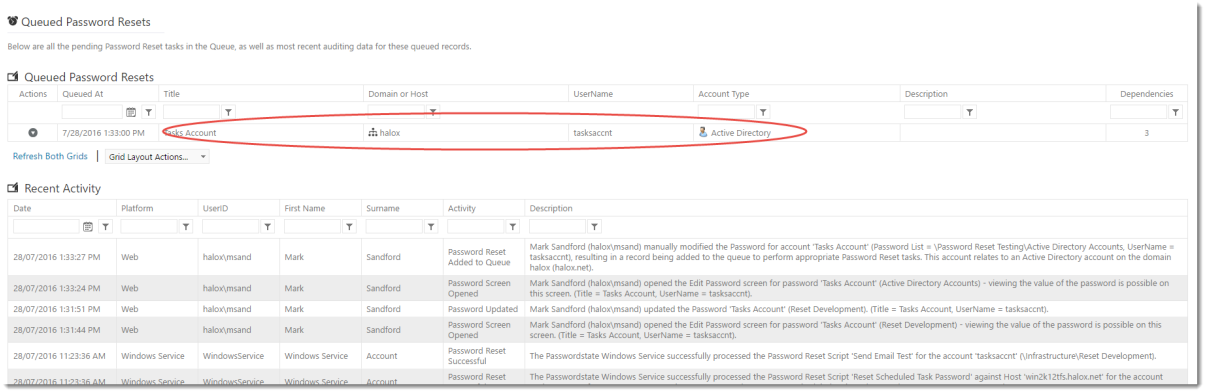


4.3 Queued Password Resets

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

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

© 2017 Click Studios (SA) Pty Ltd



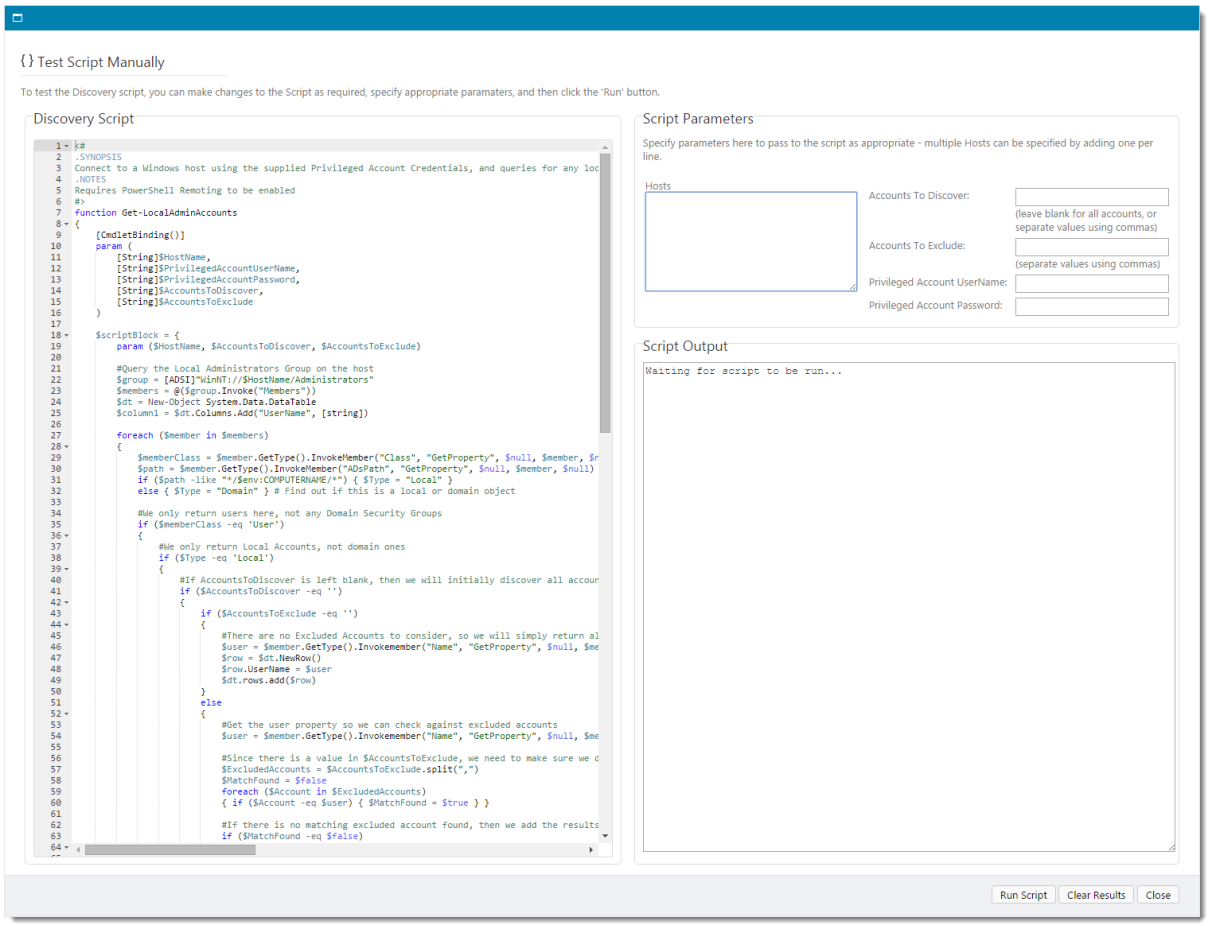
4.4 Scripts - Account Discovery

The two Discovery Jobs 'Local Administrator Accounts' and 'Dependencies' both use a PowerShell script to query Hosts for the existence of accounts.

On this screen, you can manually test each of these discovery scripts without changing any data in the database. Simply specify what Hosts you wish to query, and various parameters as appropriate.

Note: Modifying the Discovery Scripts through the web interface is not possible, but you can restore the script from the file system on the path /setup/scripts. If for any reason you need to change these scripts, please first contact Click Studios.

© 2017 Click Studios (SA) Pty Ltd



4.5 Scripts - Password Resets

The Password Resets Scripts menu allows you to modify the default supplied PowerShell scripts for resetting passwords, or to create your own.

Note 1: Most Password Reset Scripts, and associated Password records, requires a Privileged Account Credential to be associated with it, and these can be created on the screen Administration -> Privileged Account Credentials. You also need to apply permissions to these credentials, so they can selected on the Add/Edit Password screen. See the following KB article for which scripts require a Privileged Account - Password Reset Scripts and Requirements

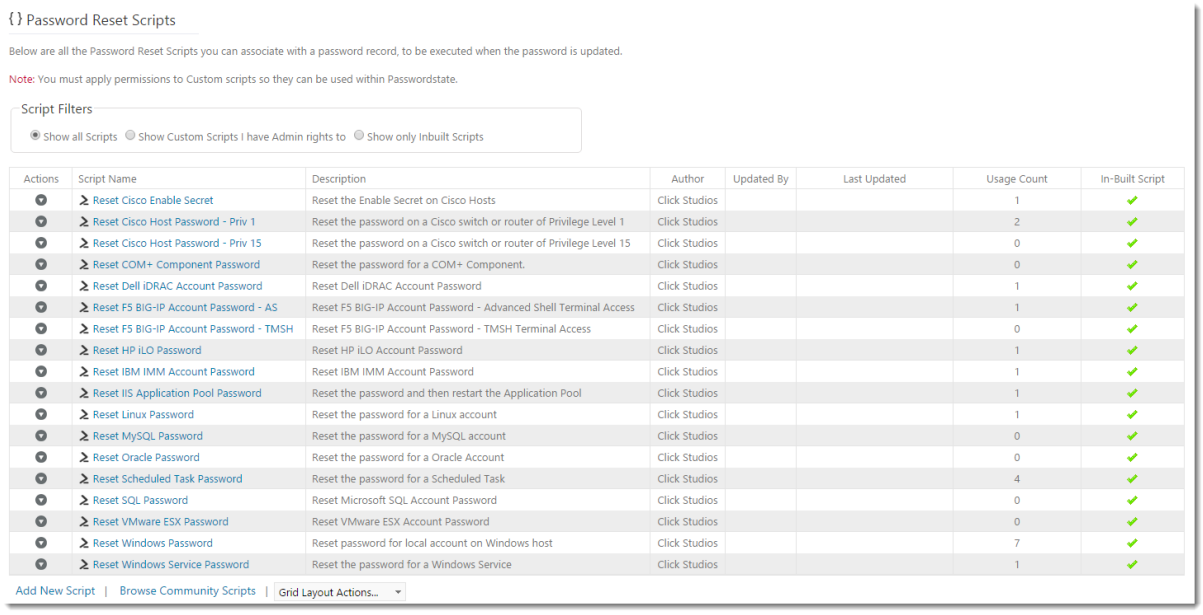
Note 2: Click Studios provides various default PowerShell scripts for performing various Password Resets. As you're also able to create your own, it's recommended you test these scripts outside of Passwordstate prior to using them in your production environment - you can use such tools as PowerShell ISE or PowerShell Studio by http://www.sapien.com/

Note 3: Please refer to the document 'Password Discovery Reset & Validation Requirements.pdf' for system requirements for the Discovery Process to work - it relies on PowerShell in your environment to function

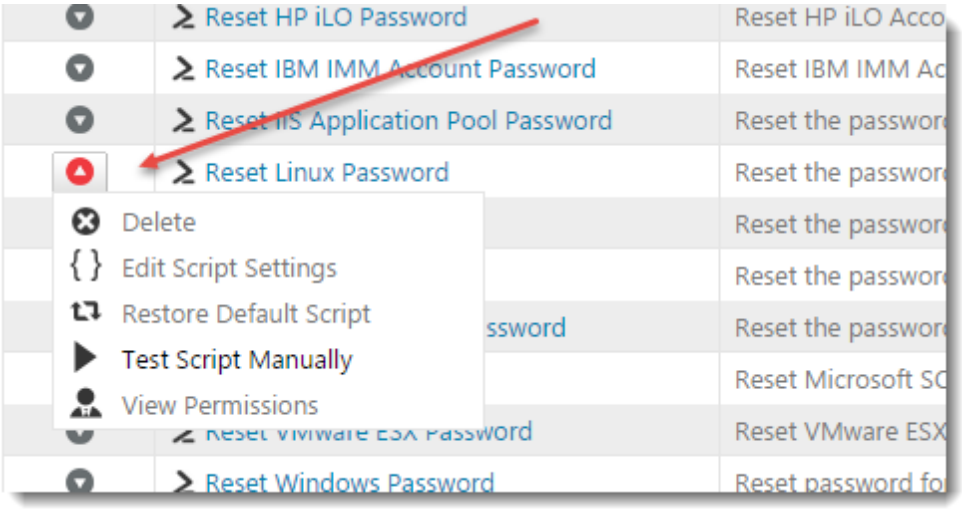
If you want to create your own scripts, have a look at the following KB article to explain the structure of PowerShell Scripts provided - Structure of a Password Reset Script. It is recommended

© 2017 Click Studios (SA) Pty Ltd

that when you create your own script, you clone one of the default scripts Click Studios provides



When clicking on the 'Actions' dropdown menu for each script, most menu items will be disabled for the default inbuilt scripts Click Studios provides, but generally are available for scripts you have created yourself:



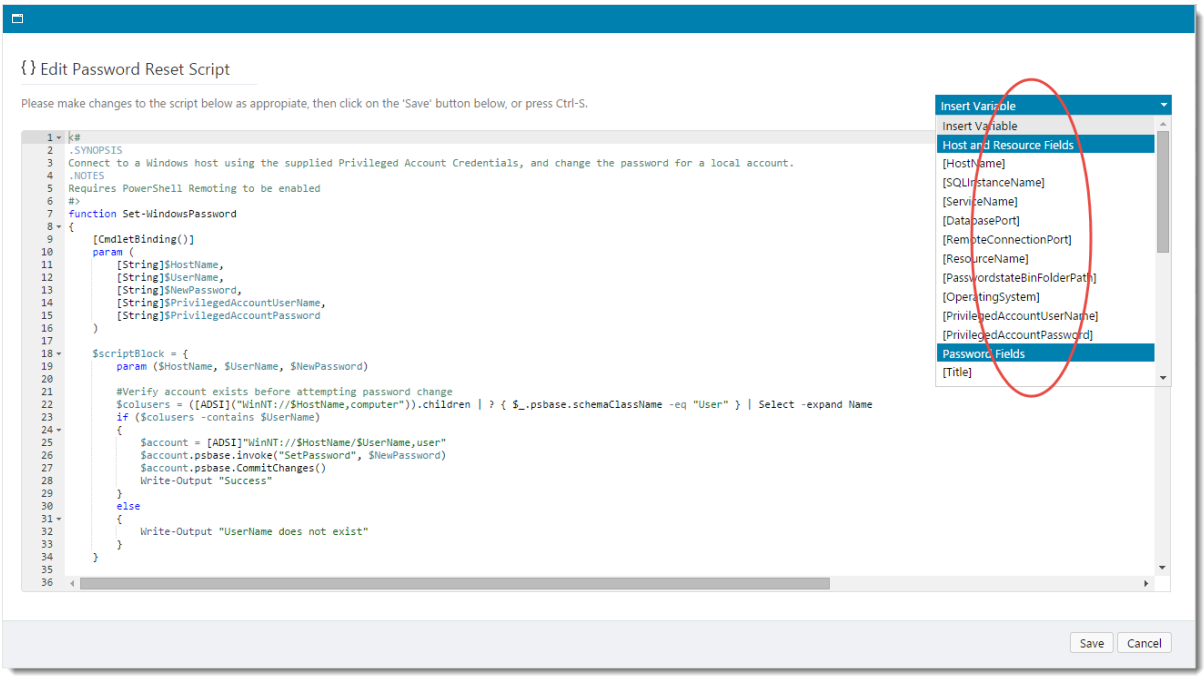
When you click on the 'Script Name' within the Grid view, it will open a window allowing you to make changes to scripts you have added yourself. There are a few things to note about these PowerShell Scripts:

- In the first screenshot below, you will see some variables which will have their values replaced

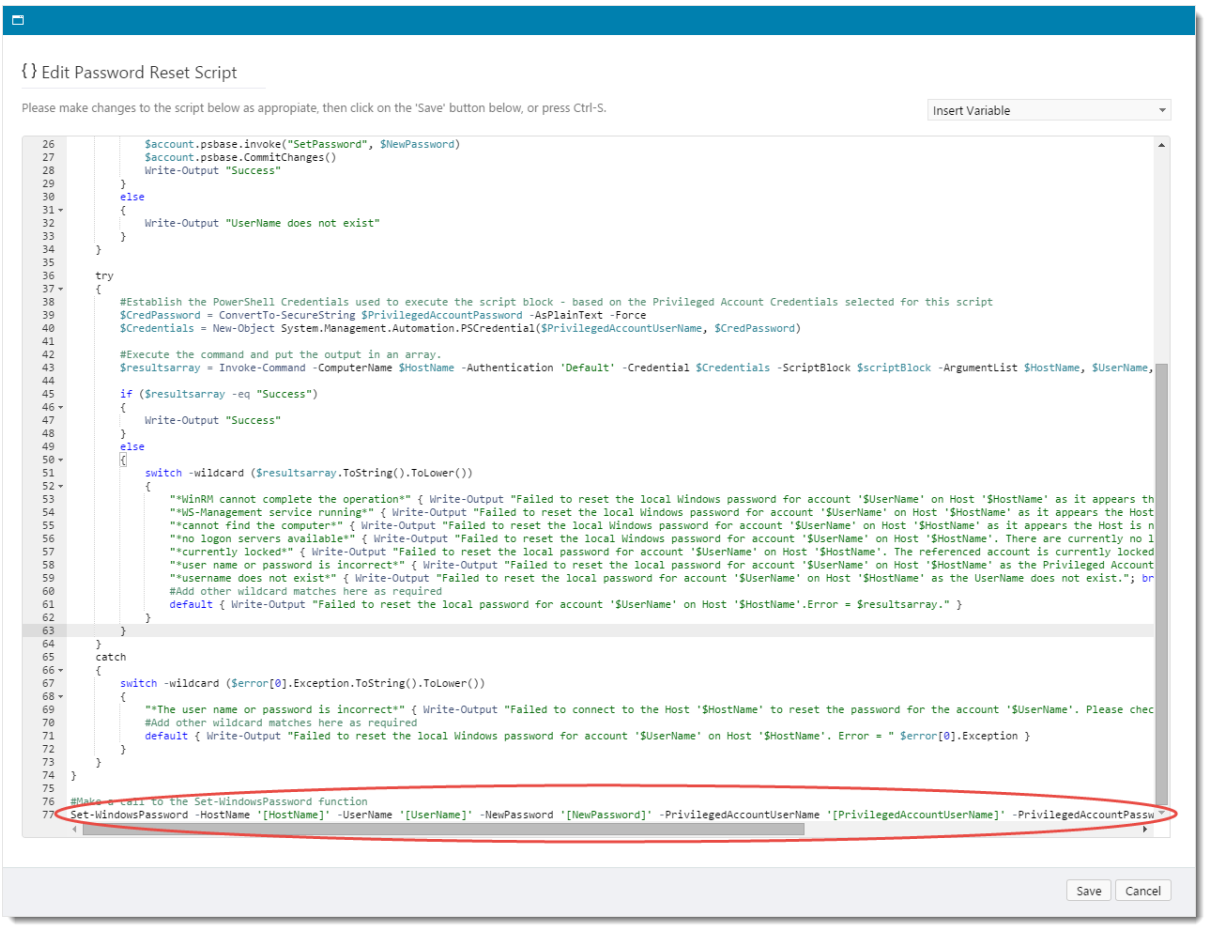
© 2017 Click Studios (SA) Pty Ltd

with that of details specific to the Host, Password Record, or Privileged Account Credentials. This replacement happens in real-time by the Passwordstate Windows Service when a Password Reset Script is being executed. As you can see in the second screenshot below, a few of these variables are used in the calling of the PowerShell function. Generally you would only need to place these variables here, but they can be used anywhere throughout the script

- You will also notice quite a bit of error checking/capturing in the default scripts provided. If there is some error event you're seeing when executing these scripts, but we've missed capturing the error gracefully, then any place you see the reference '#Add other wildcard matches here as required' you can add your own error exception capturing here

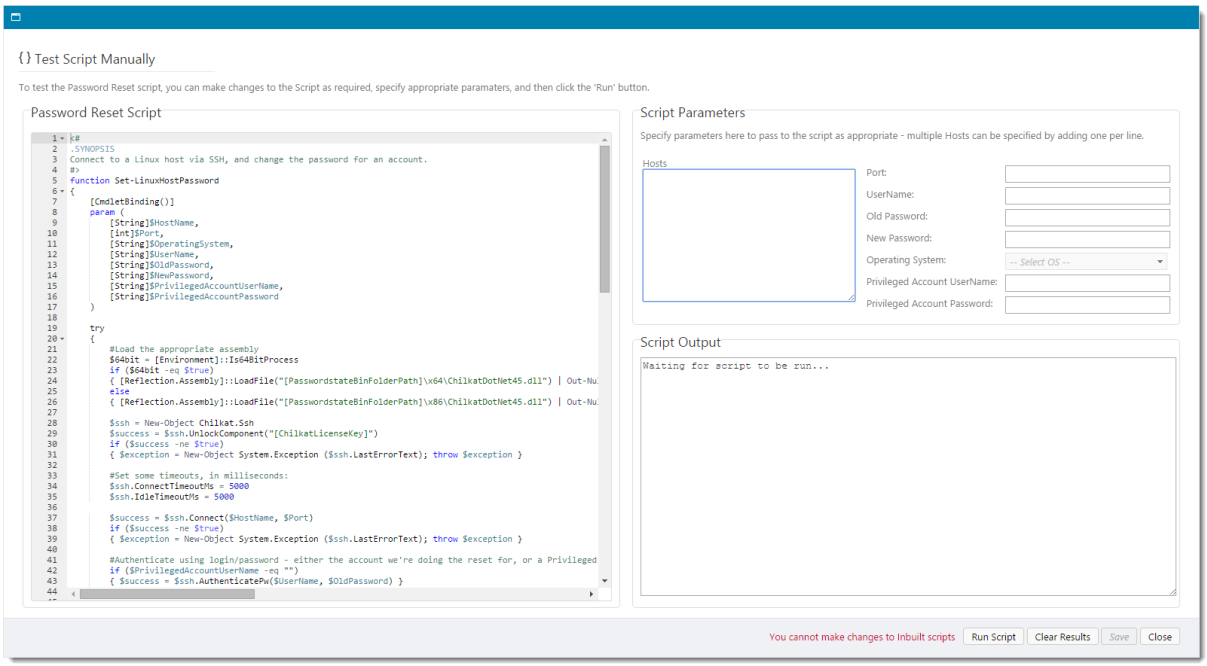


© 2017 Click Studios (SA) Pty Ltd



It's also possible to test scripts from within the Passwordstate user interface, buy selecting the 'Test Script Manually' actions menu item. When doing so, the parameters for each script will be different.

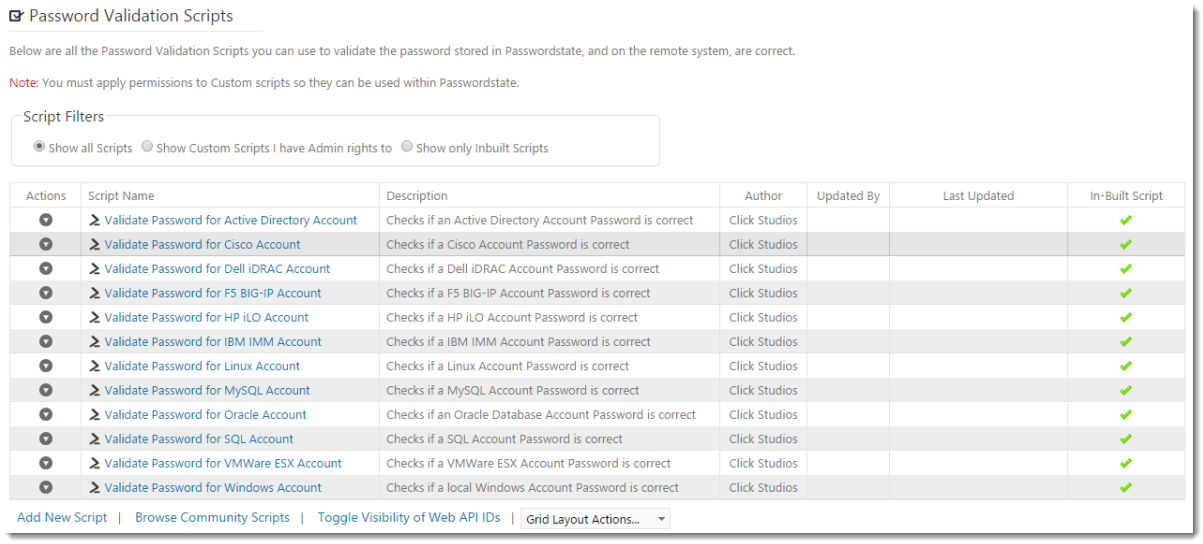
© 2017 Click Studios (SA) Pty Ltd



4.6 Scripts - Password Validation

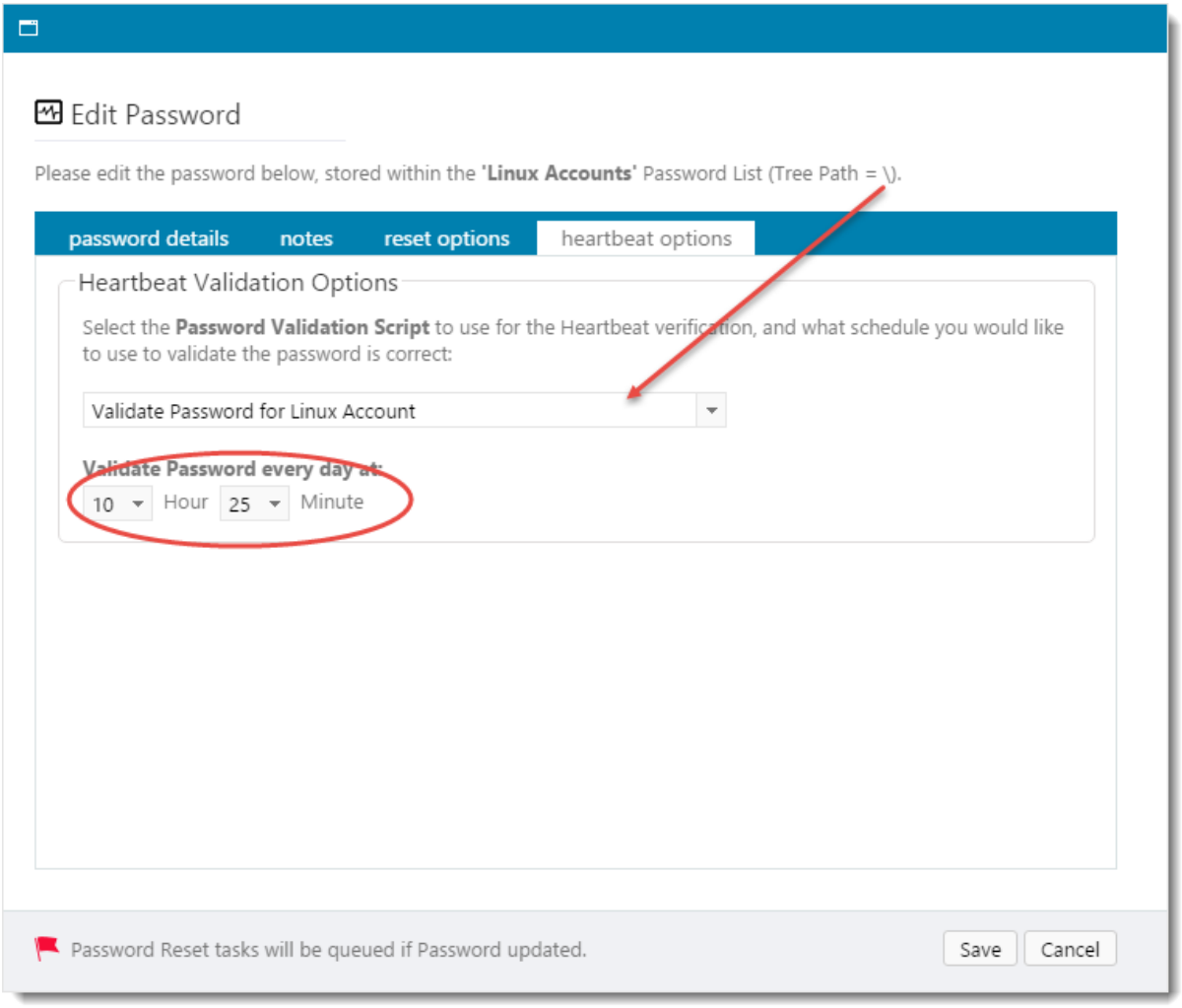
The Password Validation Scripts menu allows you to see the default scripts provided by Click Studios, or you can add your own.

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



These scripts can be associated with Password records which are configured for Password Resets, and are used as the basis for the Heartbeat Validation process. The second screenshot below shows where you can select the appropriate script, and at what time per day it should execute.

© 2017 Click Studios (SA) Pty Ltd



5 Reports Menu

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

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

5.1 Auditing

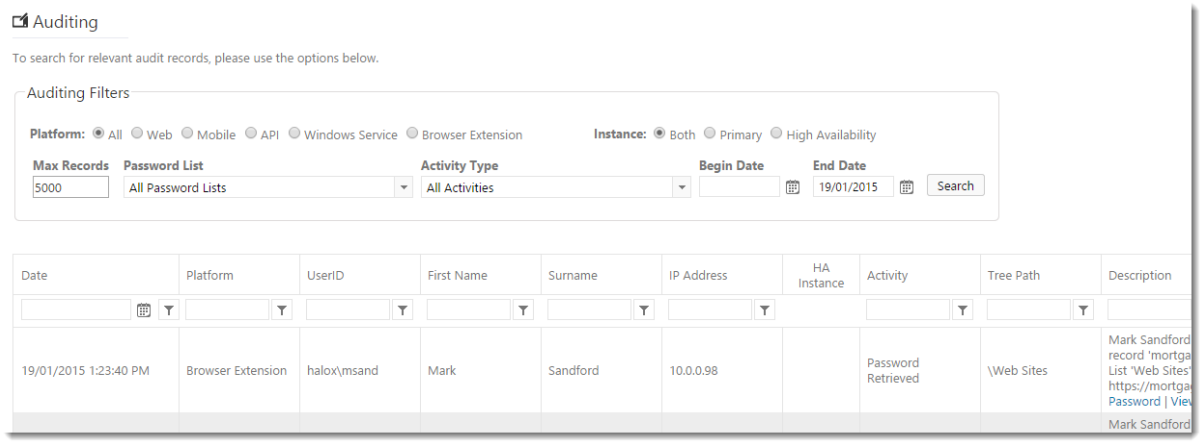
The Auditing menu allows you to view all the auditing data applicable to the Password Lists you have access to. It allows you to filter the data in multiple ways, as well as export the contents of

© 2017 Click Studios (SA) Pty Ltd

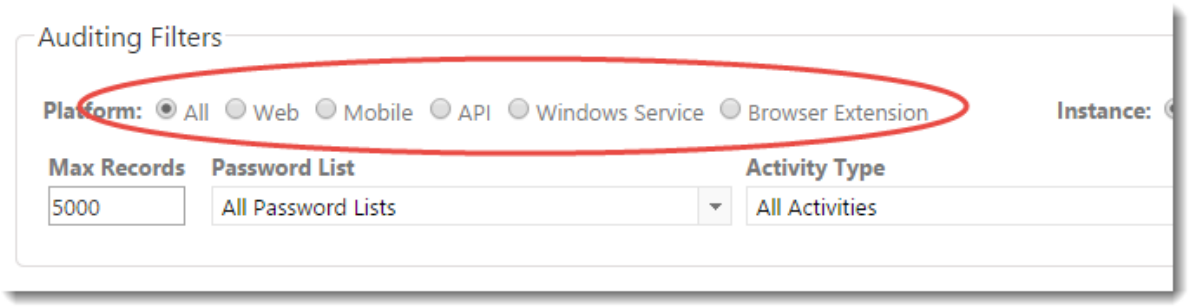
the search results to a csv file for further analysis if required.

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

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

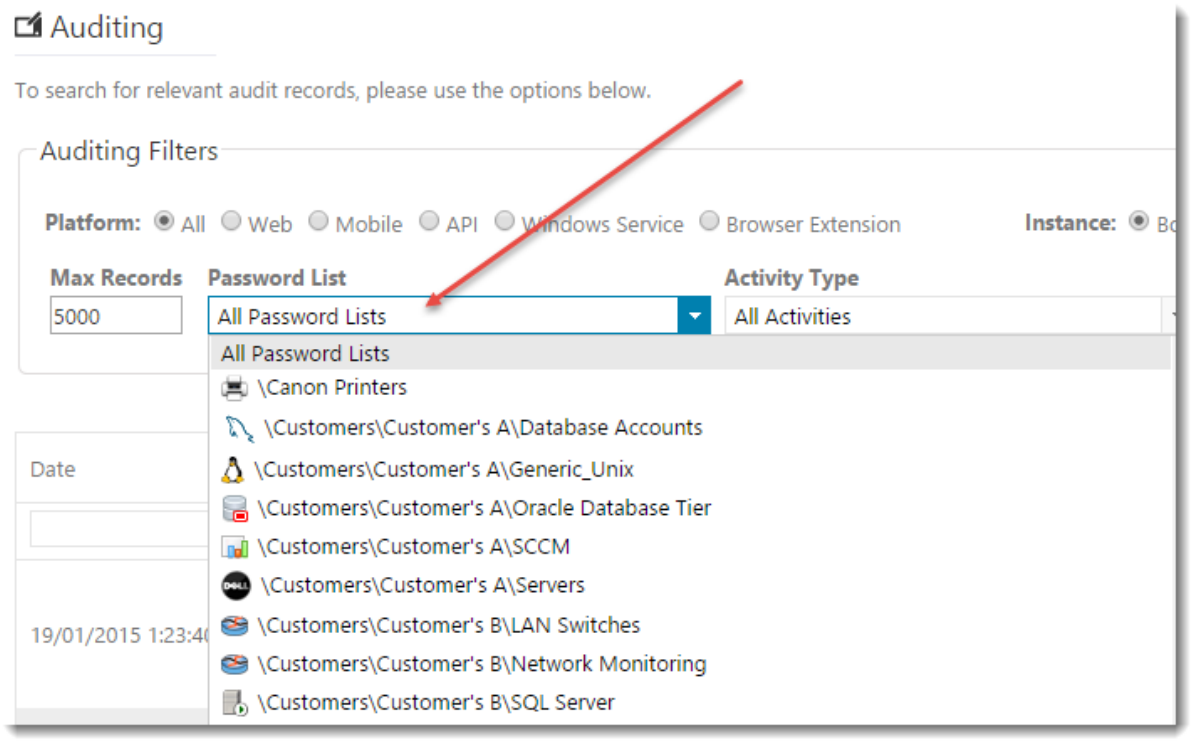


Filter by Platform

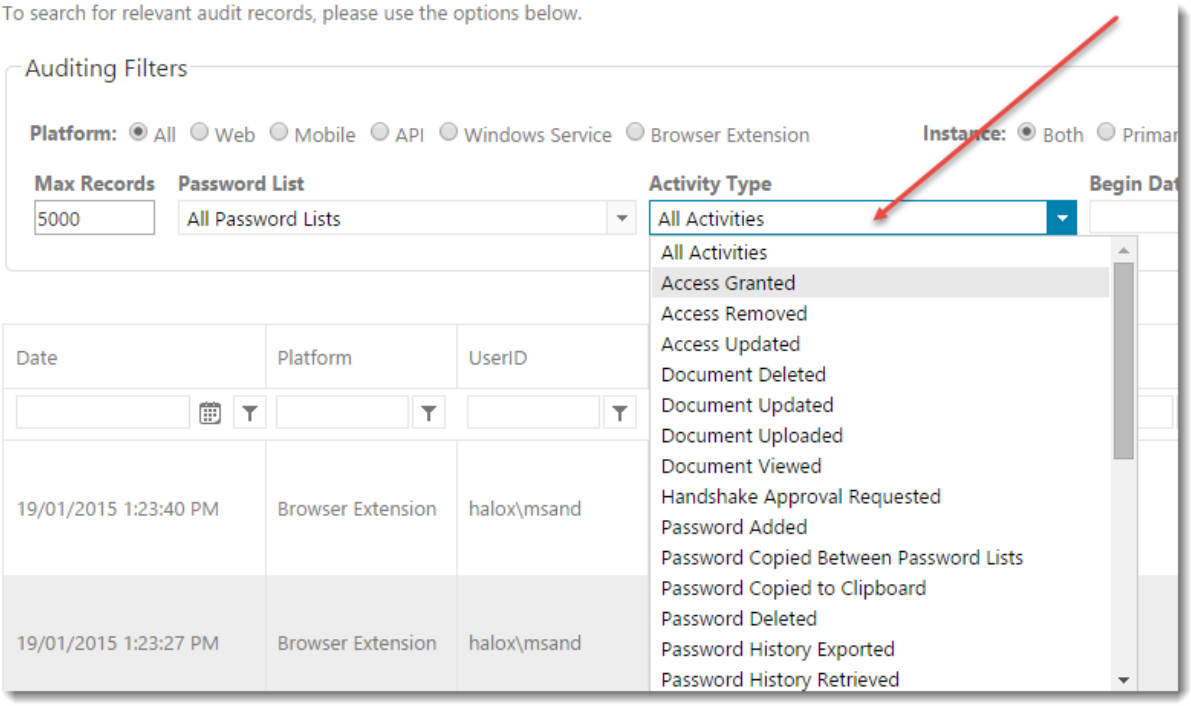


Filter by Specific Password Lists

© 2017 Click Studios (SA) Pty Ltd

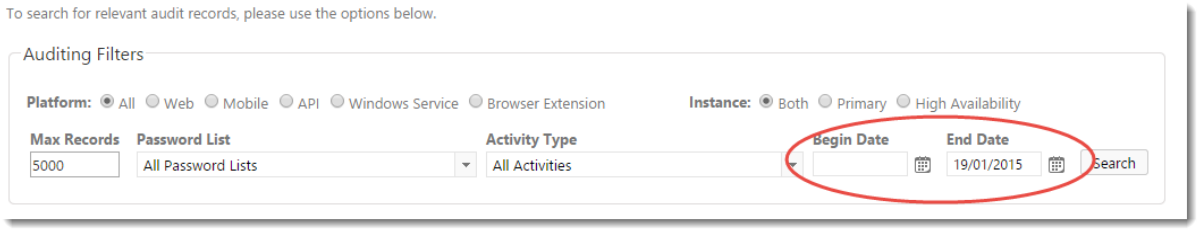


Filter by Specific Activity Type

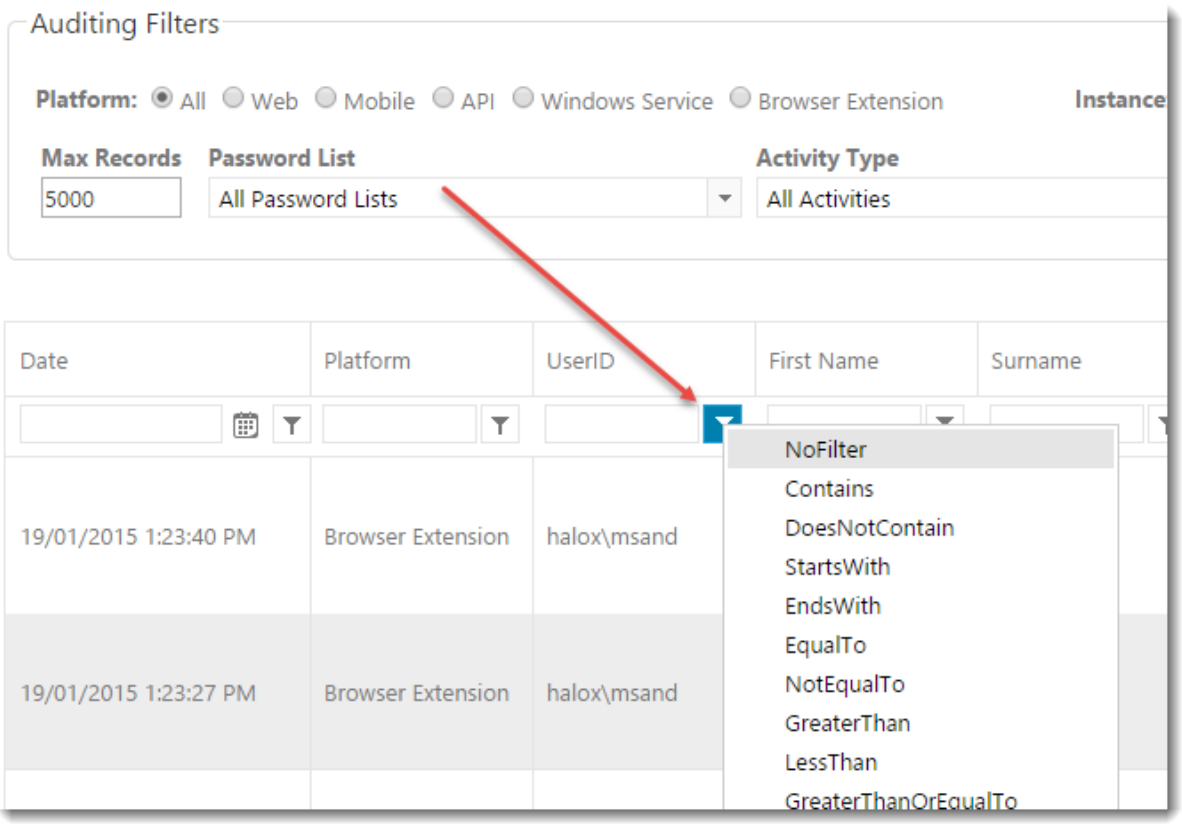


© 2017 Click Studios (SA) Pty Ltd

Filter between Specific Dates



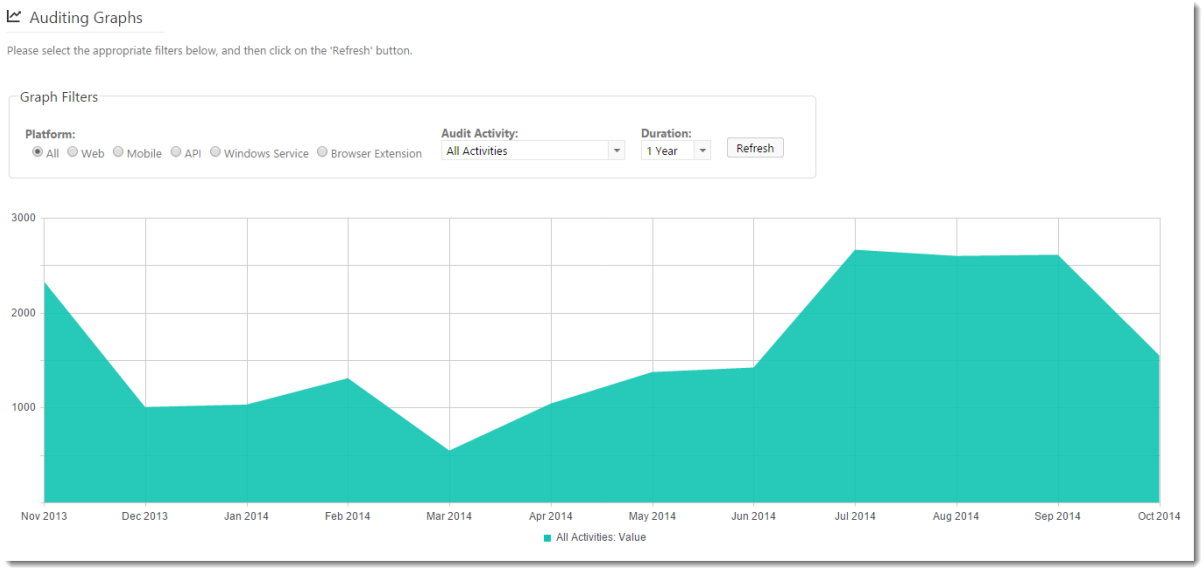
Further Filter by Search Results Contents



5.2 Auditing Graphs

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

© 2017 Click Studios (SA) Pty Ltd



5.3 Scheduled Reports

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

There are several different types of Reports you can schedule, and some may be disabled for you if you don't have the required Security Administrator's role. The reports are:

Choosing The Report Type

General Users Reports

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

Security Administrator Reports (Auditing Role Required)

- Custom Auditing Report - Allows you to specify a custom filter for reporting on audit activities

Security Administrator Reports (Reporting Role Required)

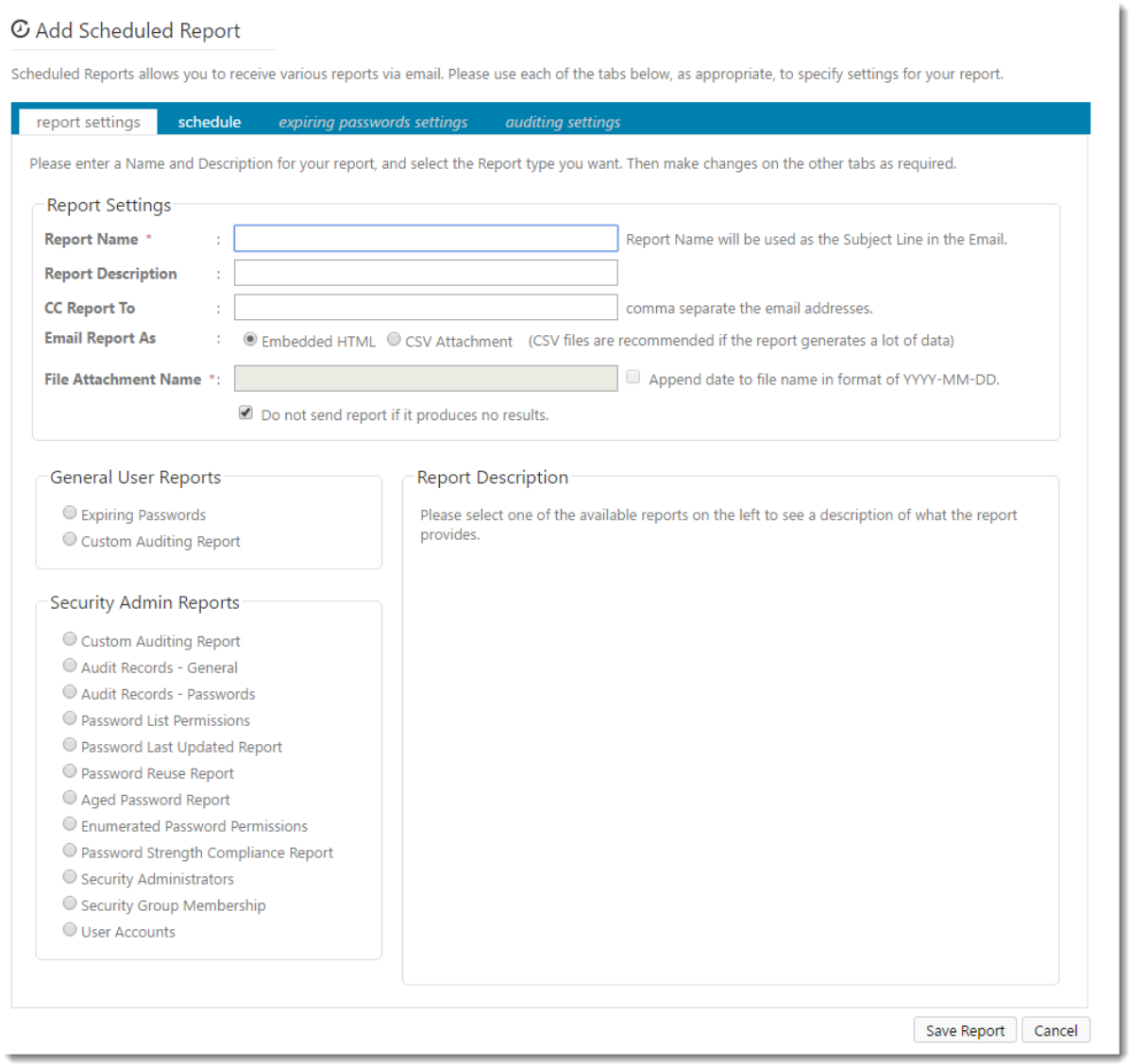
- Audit Records - General - produces a sorted list of all general audit records, not specific to Passwords or Password Lists. Please note this could be a large CSV file, depending on how many audit records there are
- Audit Records - Passwords - produces a sorted list of all audit records specific to Passwords and Password Lists. Please note this could be a large CSV file, depending on how many audit records there are
- Password List Permissions - produces a sorted list of permissions for all Password Lists, and any permissions applied to individual passwords
- Password Reuse Report - produces a list of records where the same password have been used more than once
- Aged Password Report - produces a list of each individual password record, showing the last

© 2017 Click Studios (SA) Pty Ltd

time any activity occurred for each record (excludes Private Password Lists)

- Enumerated Password Permissions - produces a sorted list of permissions for every individual password recorded in Passwordstate (excluding Private Password Lists)
- Password Strength Compliance Report - produces a sorted list of all Password Lists, the strength of each password, and whether or not the Password Strength is compliant or not
- Security Group Membership - produces a sorted list of Security Groups within Passwordstate, and their User Accounts membership
- User Accounts - produces a sorted list of User Accounts within Passwordstate

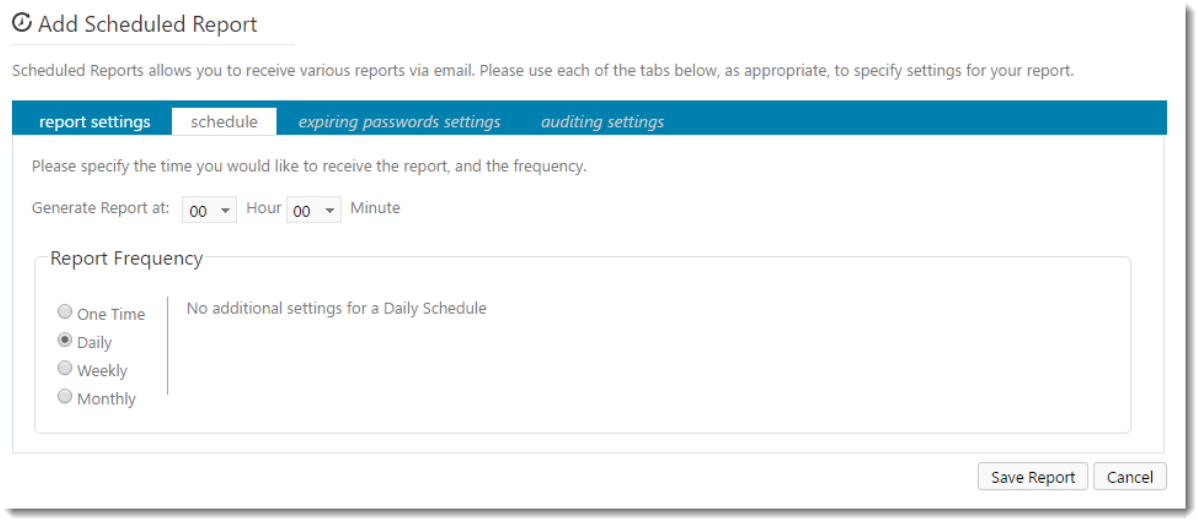
Once you've chosen the required type of report, you must specify a schedule for when the report is sent, and also any other additional settings for the Expiring Passwords report, or the Custom Auditing Reports



© 2017 Click Studios (SA) Pty Ltd

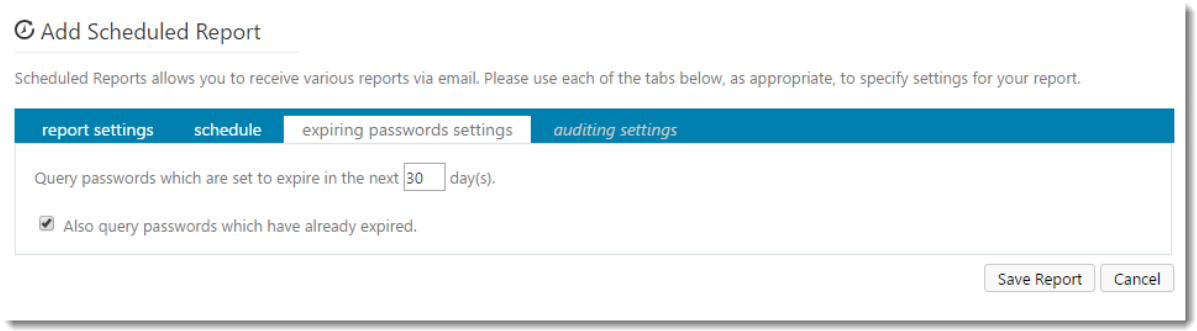
Setting The Schedule

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



Expiring Passwords Settings

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



Auditing Settings

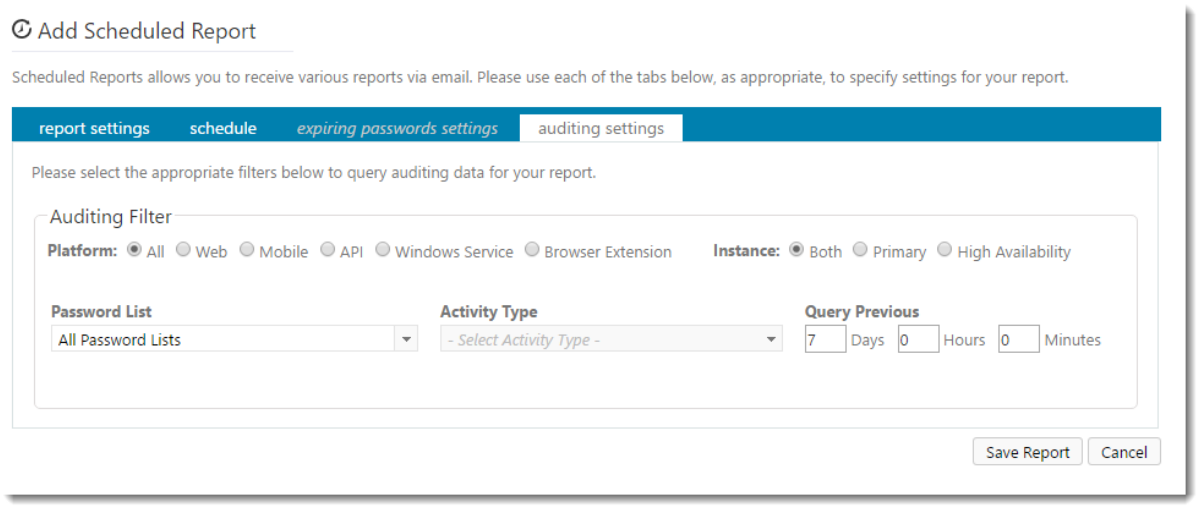
If you have chosen one of the 'Custom Auditing Reports', you can create your own filter for the auditing data, and specify how many days, hours and minutes into the past you wish to query the data.

Note 1: The list of Password Lists and Activity Types will be different here for the General Users report, and the Security Administrators report. Effectively the General Users report has the same data/options available as the Auditing Menu at the bottom of the screen, and the Security

© 2017 Click Studios (SA) Pty Ltd

Administrators Report has the same data/options available as the screen Administration -> Auditing.

Note 2: You can select one or more Audit Activities by checking the appropriate options in the 'Activity Type' dropdown list.



6 Preferences Menu

The Preferences Menu allows you to set various settings for your Passwordstate account, set various email notifications, and create Remote Session Credential queries if you wish to use the Remote Session launcher feature.

Preferences	Specify various settings for your Passwordstate account
Email Notifications	Select which Email Notifications you would like to receive, or block
Remote Session Credentials	Specify one or more Remote Session Credential queries for the Remote Session Launcher feature

6.1 Preferences

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

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

The Preferences screen has the following 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

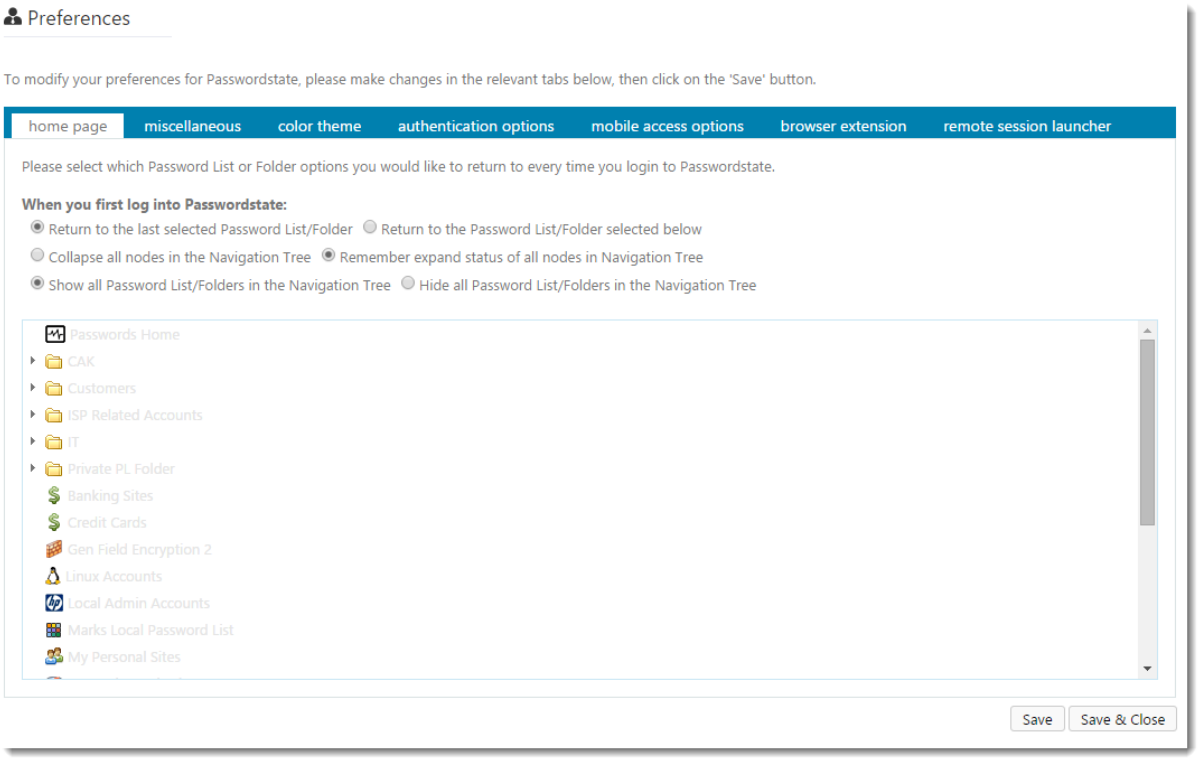
© 2017 Click Studios (SA) Pty Ltd

Miscellaneous Tab	A collection of different settings specific for your account
Color Theme Tab	Allows you to customize the colors for Passwordstate
Authentication Options Tab	Specify which authentication method you wish to use when first accessing the Passwordstate web site
Mobile Access Options Tab	Allows you to specify various settings for the Mobile Client version of Passwordstate, and also the Pin Number used for you to authenticate.
Browser Extension	The Browser Extension tab allows you to specify various settings for the Chrome Browser Extension, which is used to automatically form-fill web site logins
Remote Session Launcher	The Remote Session Launcher utility allows you to perform for RDP, SSH, Telnet or VNC remote sessions to Hosts

6.1.1 Home Page Tab

The Home Page Tab allows you to select the option to return to the last view Password List or Folder, or select a specific Password List or Folder you would like displayed when you first navigate to the Passwordstate web site.

You can also chose to collapse all nodes in the Navigation Tree when you first login, or leave them in the state they were when you last used Passwordstate.



© 2017 Click Studios (SA) Pty Ltd

6.1.2 Miscellaneous Tab

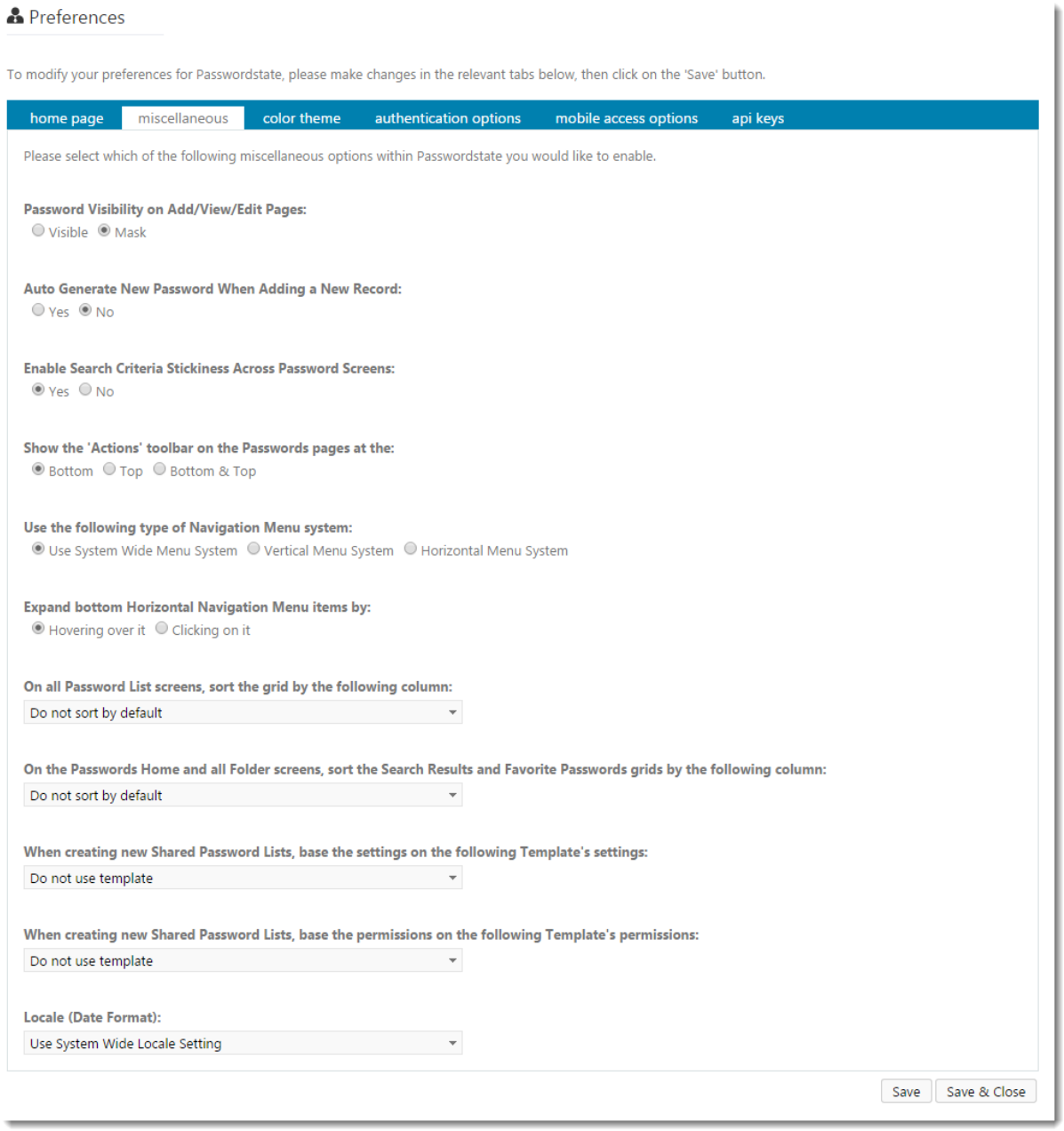
The Miscellaneous Tab has the following settings you can choose for your account:

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
Use the following type of Navigation Menu system	You can choose to use two types of main Navigation Menus - a Vertical one on the left-hand side of the screen, or a Horizontal one on the bottom of the screen
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
On all Password List screens, sort the grid by the following column	If you would like all Password grids to be sorted by default on a selected column, you can choose the column here. Note: this will override you manually sorting a column and then selecting the save the Grid layout
On the Passwords Home and all Folder screens, sort the Search Results and	Similar to the option above, but this sort order applies to the Search Results and Favorite Passwords

© 2017 Click Studios (SA) Pty Ltd

Favorite Passwords grids by the following column	grids on the Passwords Home page and and Folder pages
When creating new Shared Password Lists, base the settings on the following Template's settings	When creating new Shared Password Lists, you can choose to automatically specify all the settings based on the selected Template
When creating new Shared Password Lists, base the permissions on the following Template's permissions	When creating new Shared Password Lists, you can choose to automatically apply permissions based on the permissions set on the selected Template
Locale (Date Format)	Allows you to specify a date format for any date fields - you may need different format based on your region, compared to that of what Passwordstate is current set to use system wide

© 2017 Click Studios (SA) Pty Ltd



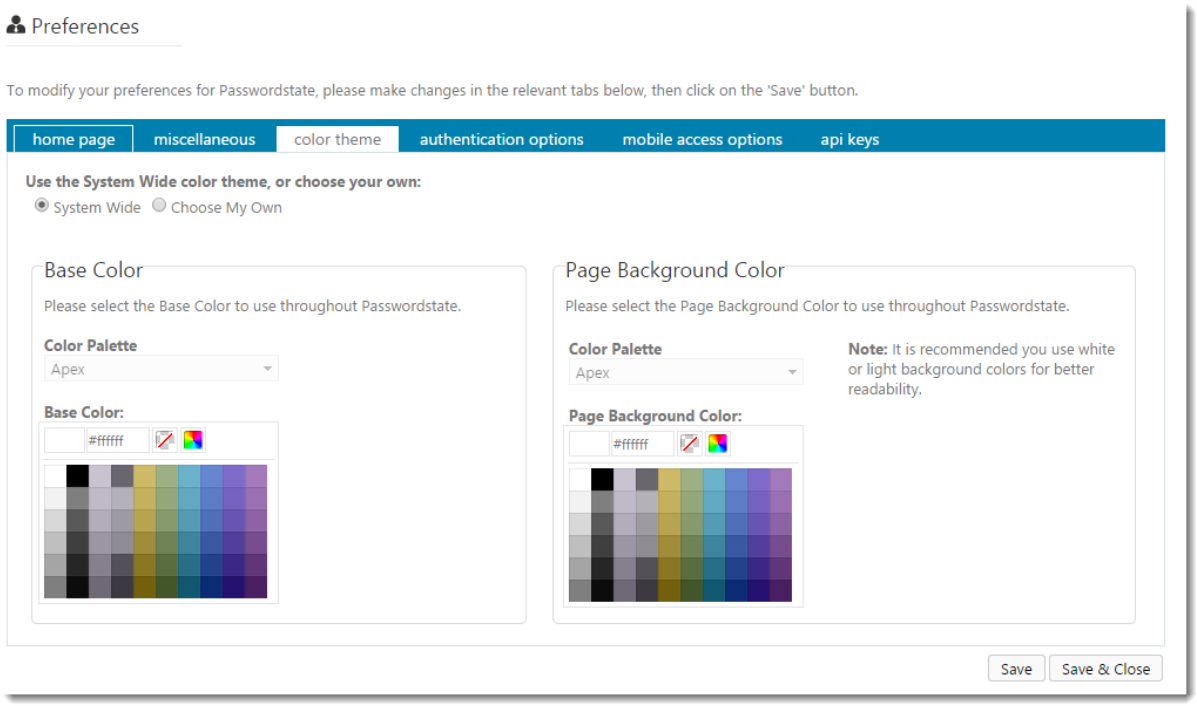
6.1.3 Color Theme Tab

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

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

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

© 2017 Click Studios (SA) Pty Ltd



6.1.4 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

© 2017 Click Studios (SA) Pty Ltd

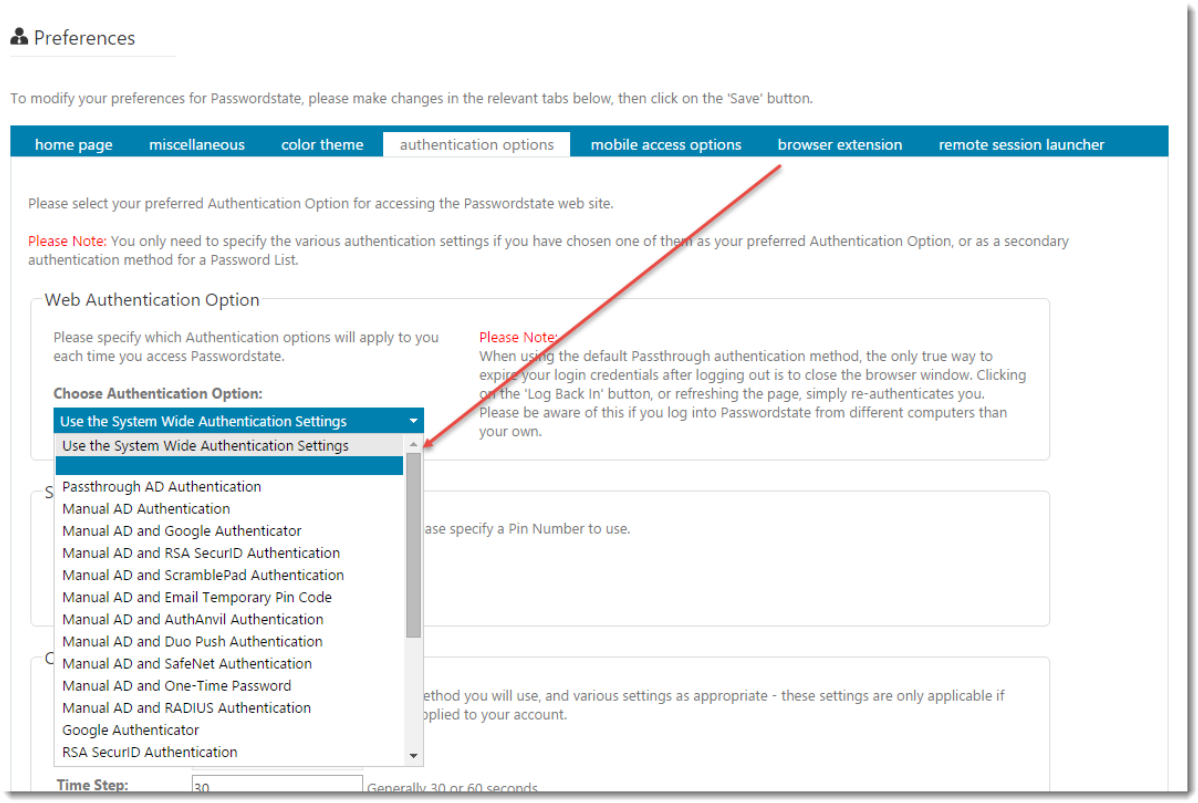
	domain credentials to the IIS web site, and the 'Windows Authentication' within IIS will validate your credentials against AD. If you are being prompted to enter your username and password, please ask your Security Administrators to investigate
Manual AD Authentication	This options will present you with 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, you 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, you 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
Manual AD and Email Temporary Pin Code	This authentication option will send you a temporary Pin Code to any email address you specify - which could also be an SMS Gateway if required. The temporary Pin Code expires after a set period, set by the Security Administrator(s) of Passwordstate, and cannot be reused after it expires. This authentication option requires you to validate both your Active Directory account credentials, plus the temporary Pin Code
Manual AD and AuthAnvil Authentication	In additional to manually specifying your AD username and Password, you must also specify your AuthAnvil Username and Passcode to authenticate. The Passcode is a combination of your Pin Code and the One-Time Password which is generated
Manual AD and Duo Push Authentication	In additional to manually specifying your AD username and Password, you must also specify your Duo Push Username so the Push Notification can be sent to you, then allowing the remainder of the authentication process

© 2017 Click Studios (SA) Pty Ltd

Manual AD and SafeNet Authentication	In additional to manually specifying your AD username and Password, you must also specify your SafeNet Username and Passcode to authenticate to Passwordstate
Manual AD and One-Time Password	In additional to manually specifying your AD username and Password, you can use a software or hardware based On-Time Password Authentication option, based on either the TOTP or HOTP algorithms
Manual AD and RADIUS Authenication	Authenticate your AD Account, as well as to a RADIUS server
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
Email Temporary Pin Code	This authentication option will send you a temporary Pin Code to any email address you specify - which could also be an SMS Gateway if required. The temporary Pin Code expires after a set period, set by the Security Administrator(s) of Passwordstate, and cannot be reused after it expires.
AuthAnvil Authentication	You must also specify your AuthAnvil Username and Passcode to authenticate. The Passcode is a combination of your Pin Code and the One-Time Password which is generated
Duo Push Authentication	You must specify your Duo Push Username so the Push Notification can be sent to you, then allowing the remainder of the authentication process
SafeNet Authentication	You must specify your SafeNet Username and Passcode to authenticate to Passwordstate
One-Time Password	You must specify your One-Time Password based on the use of either a software or hardware token, for either the TOTP or HOTP algorithms
Separate Password	A completely separate password, used in conjunction with Passthrough AD Authentication
SAML2 Authentication	Authenticate against a SAML 2.0 provider. Note: Your Passwordstate email address must match what's configured for your account on the SAML2 provider's web site
RADIUS Authentication	Authenticate against a RADIUS server

© 2017 Click Studios (SA) Pty Ltd

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

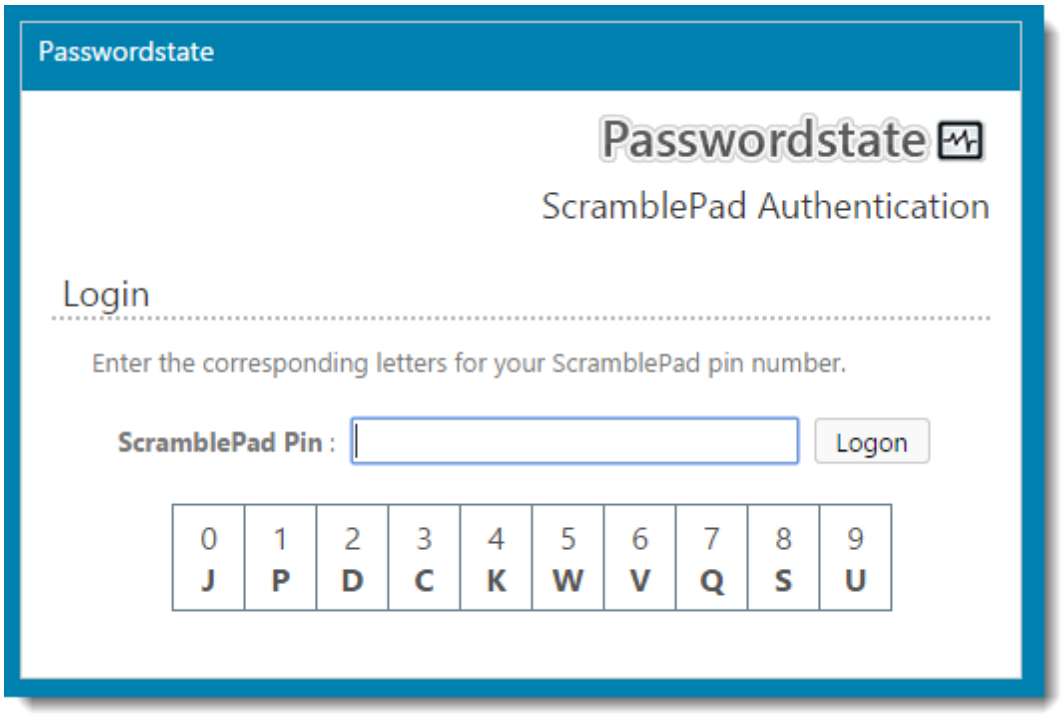


ScramblePad Pin Number

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.

© 2017 Click Studios (SA) Pty Ltd

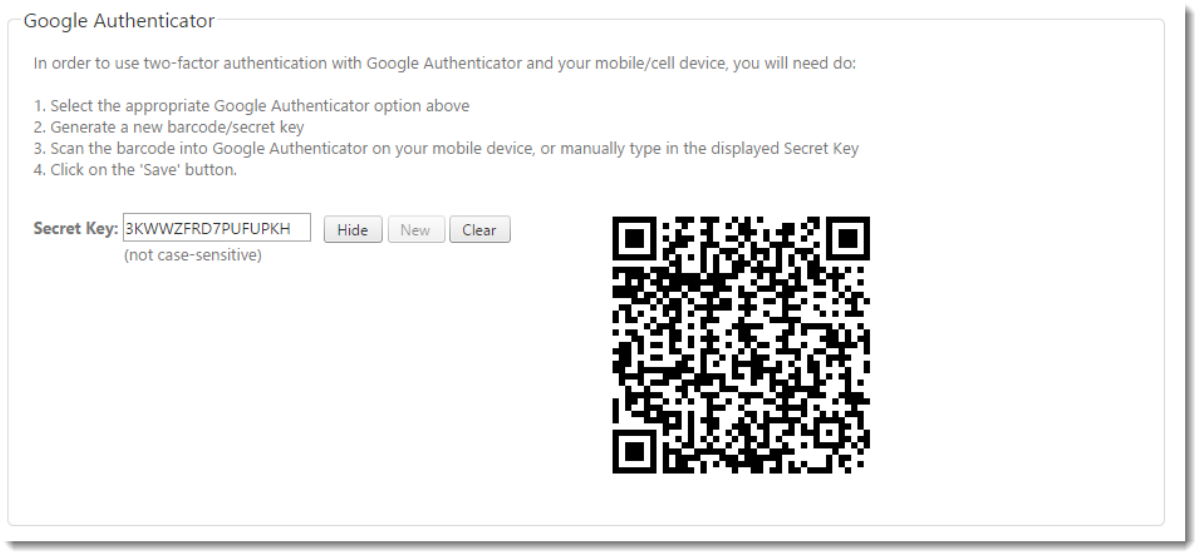


Google Authenticator

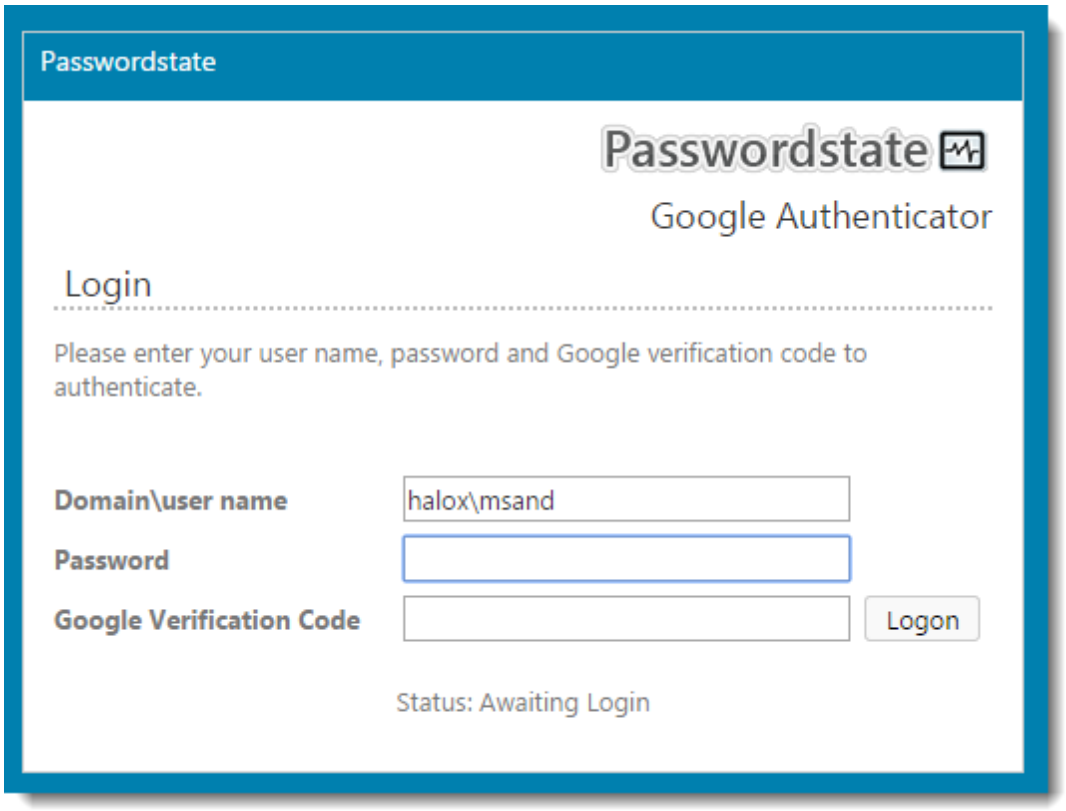
Prior to using Google Authenticator, you must first generate a new secret key for your account. To do so, you can follow these instructions:

- 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.

© 2017 Click Studios (SA) Pty Ltd

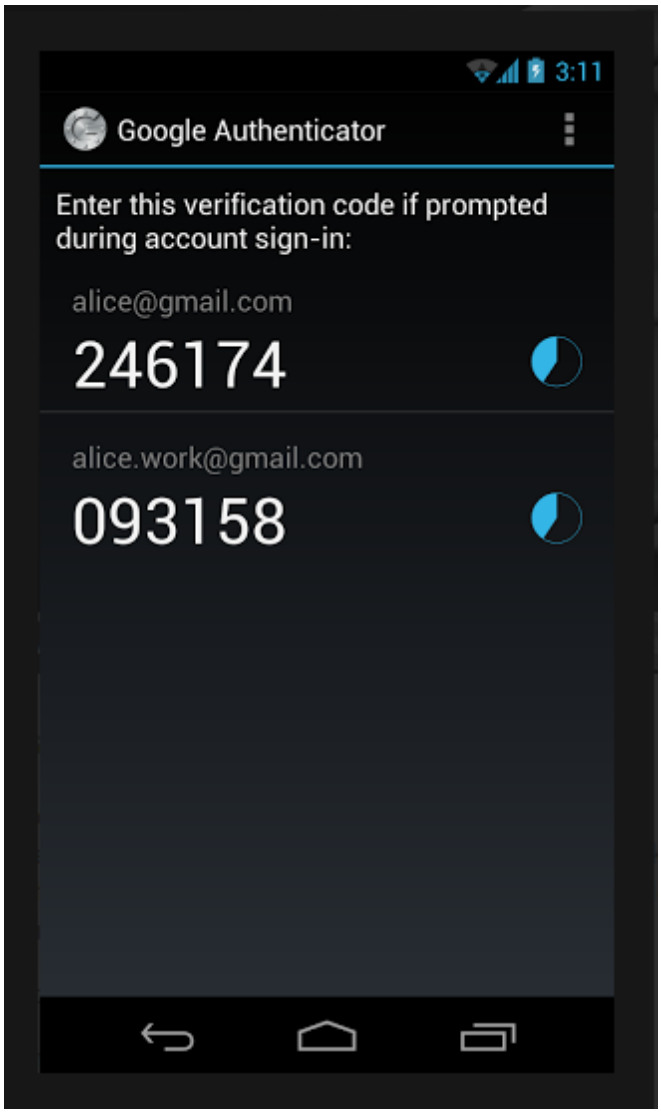


Once you have successfully enabled Google Authenticator with Passwordstate and on your mobile/cell device, then you will be presented with the following login screen next time you visit Passwordstate (this is the screen for 'Manual AD and Google Authenticator').



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.

© 2017 Click Studios (SA) Pty Ltd



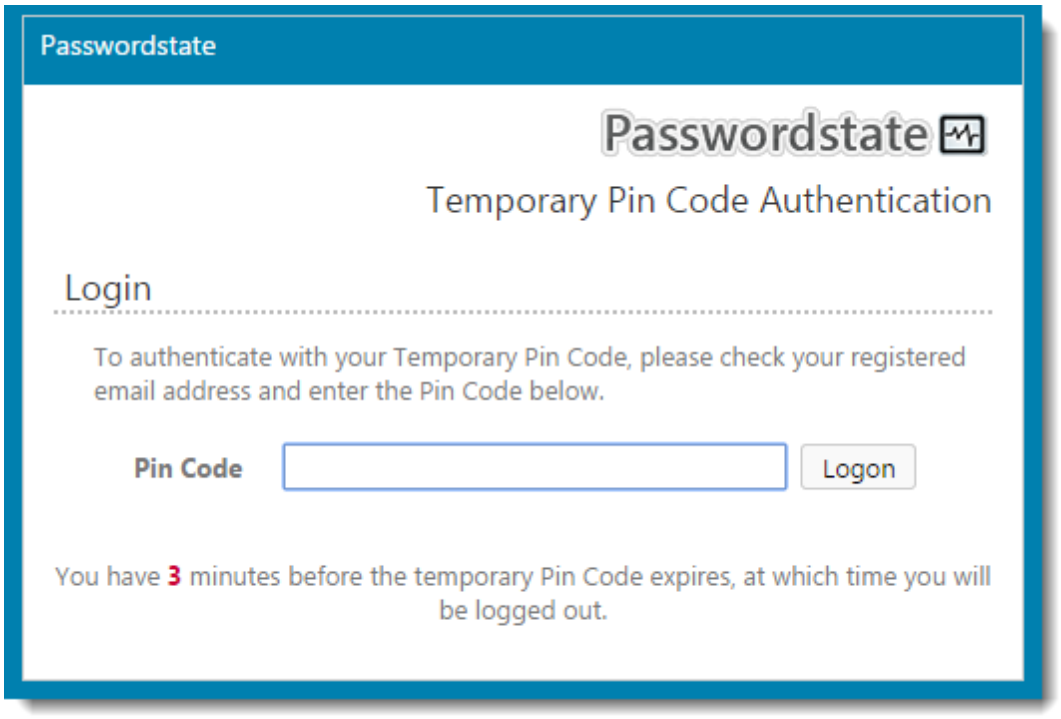
Email Temporary Pin Code

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

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

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

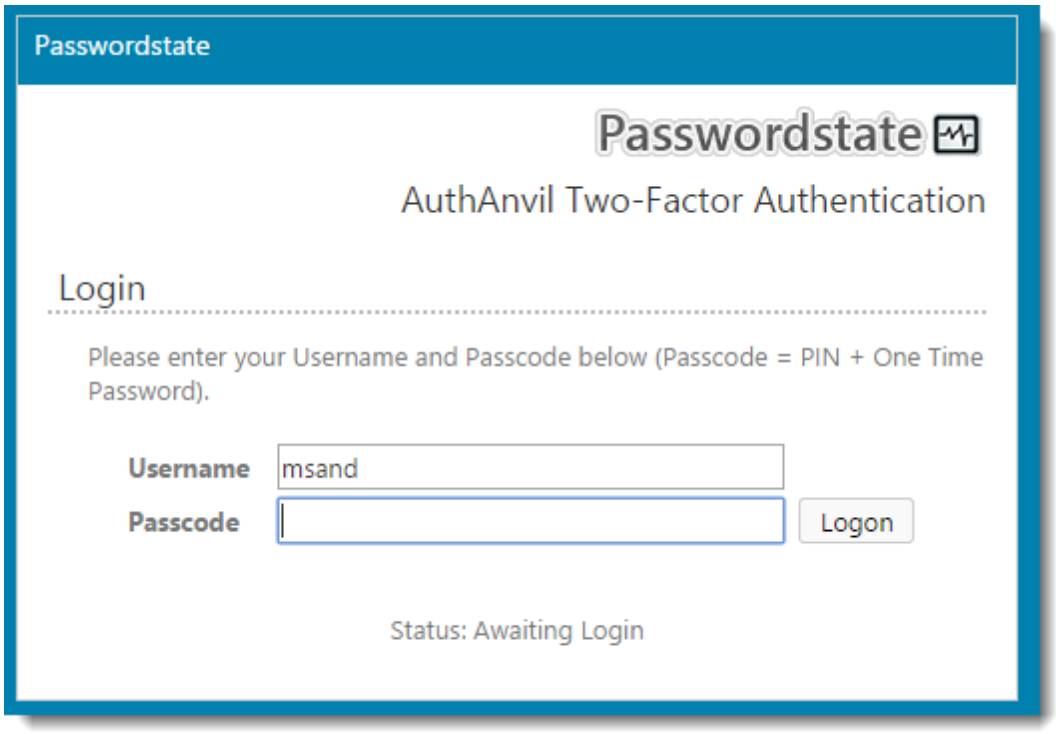
© 2017 Click Studios (SA) Pty Ltd



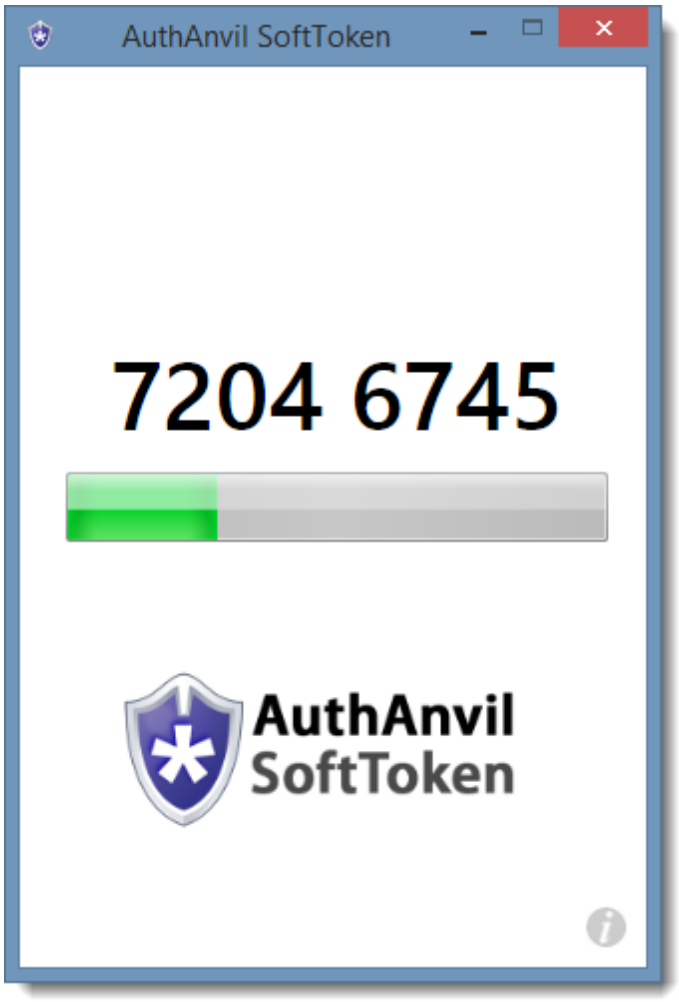
AuthAnvil Authentication

You must specify your AuthAnvil Username on this Preferences screen, and then you can begin to use this two-factor authentication method. You Passcode is a combination of your Pin, plus the One-Time Password. So in the example below, it would be something like 123472046745.

© 2017 Click Studios (SA) Pty Ltd



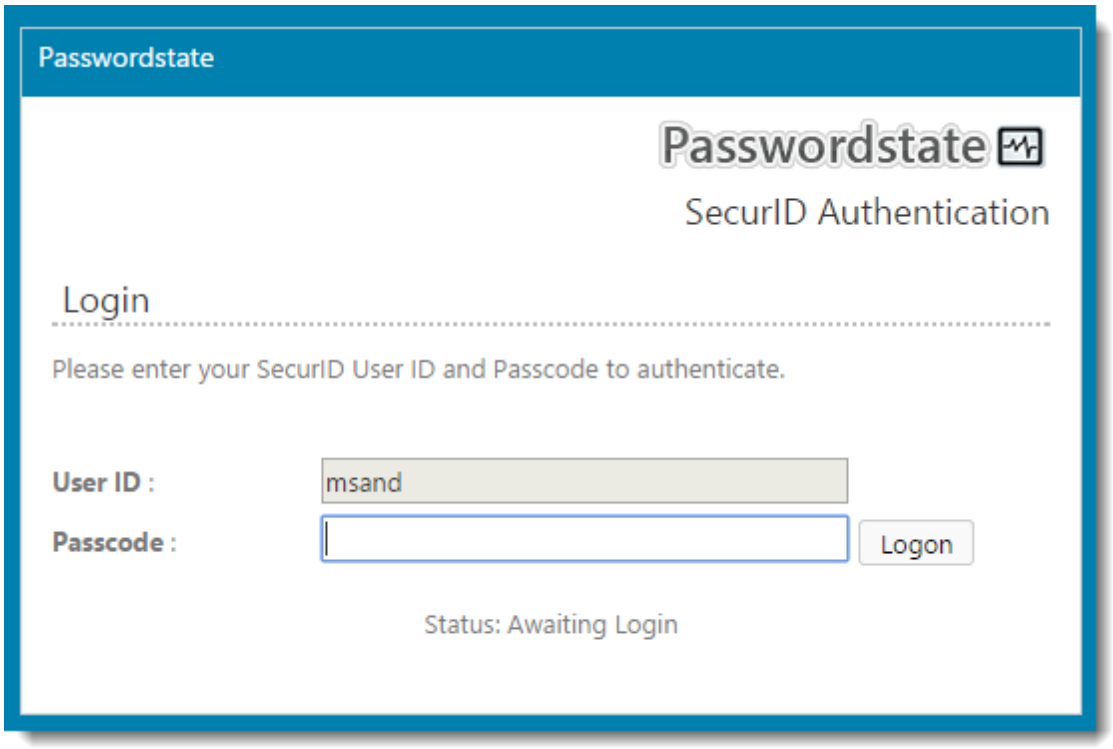
© 2017 Click Studios (SA) Pty Ltd



SecurID Authentication

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

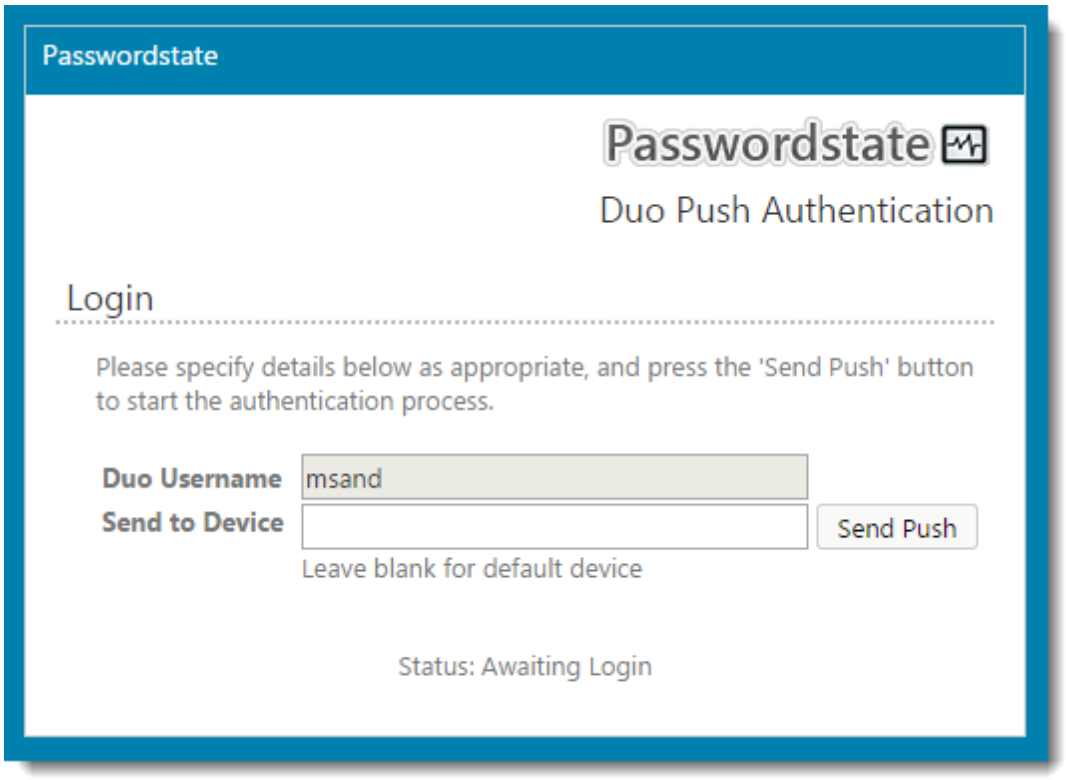
© 2017 Click Studios (SA) Pty Ltd



Duo Push Authentication

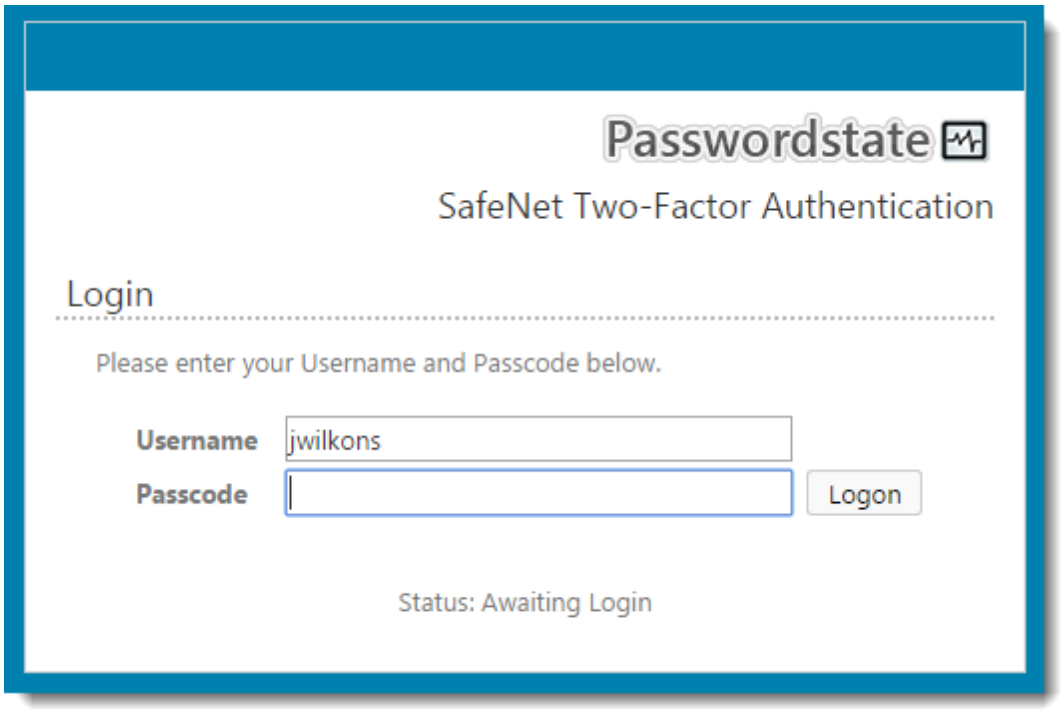
You must specify your Duo Username to send the Push notification to. You can also choose which device to send the Push Notification to.

© 2017 Click Studios (SA) Pty Ltd



SafeNet Authentication

You must specify your SafeNet UserName and Passcode to authenticate to Passwordstate



© 2017 Click Studios (SA) Pty Ltd

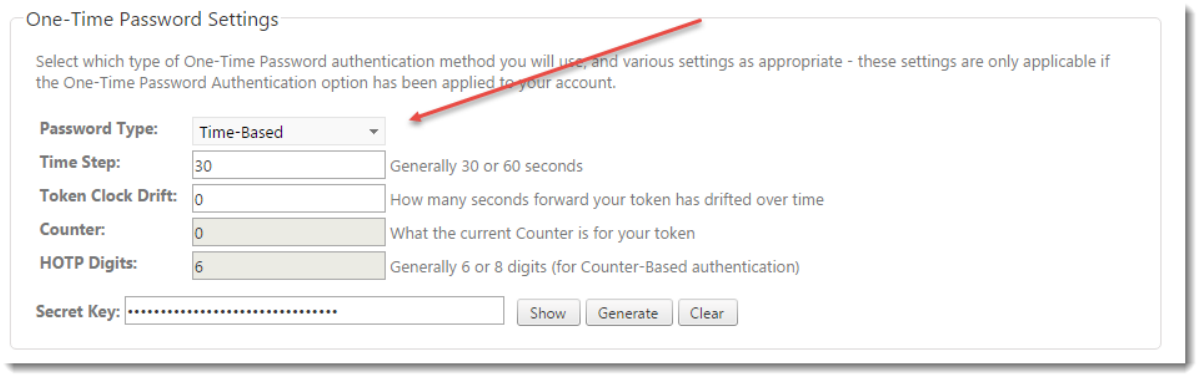
One-Time Password

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

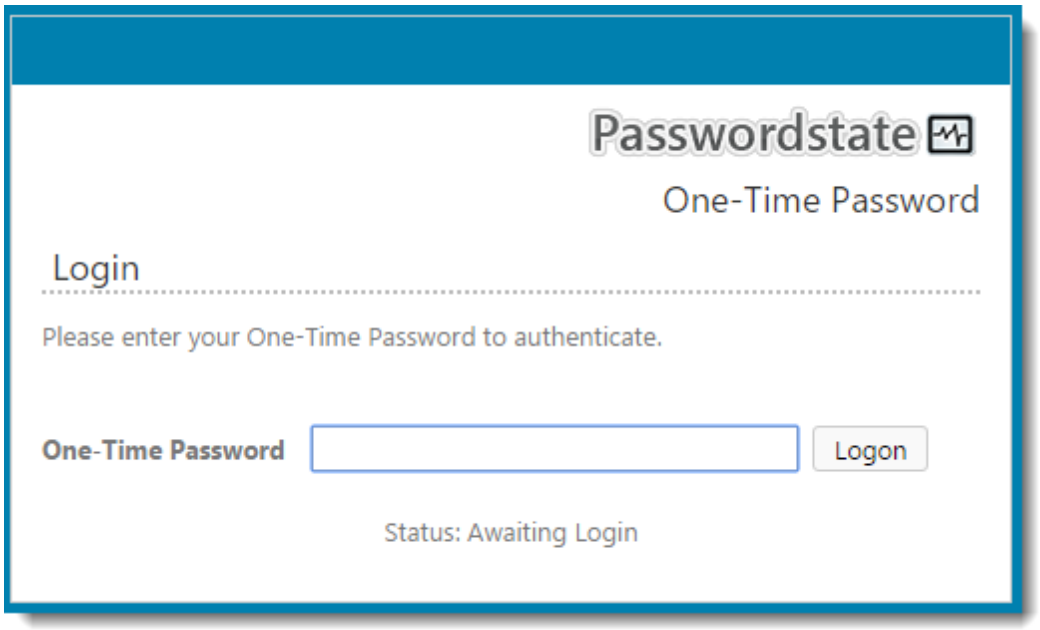
In order to use this authentication option, you must select the Password Type, and then select various settings for your token.

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

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

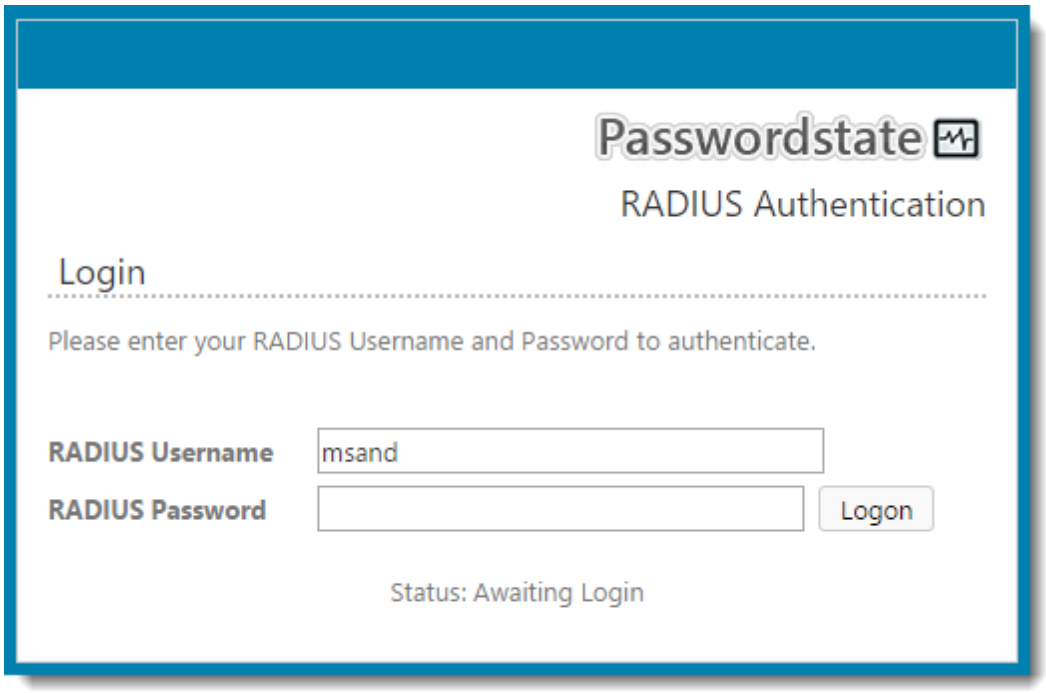


© 2017 Click Studios (SA) Pty Ltd



RADIUS Authentication

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



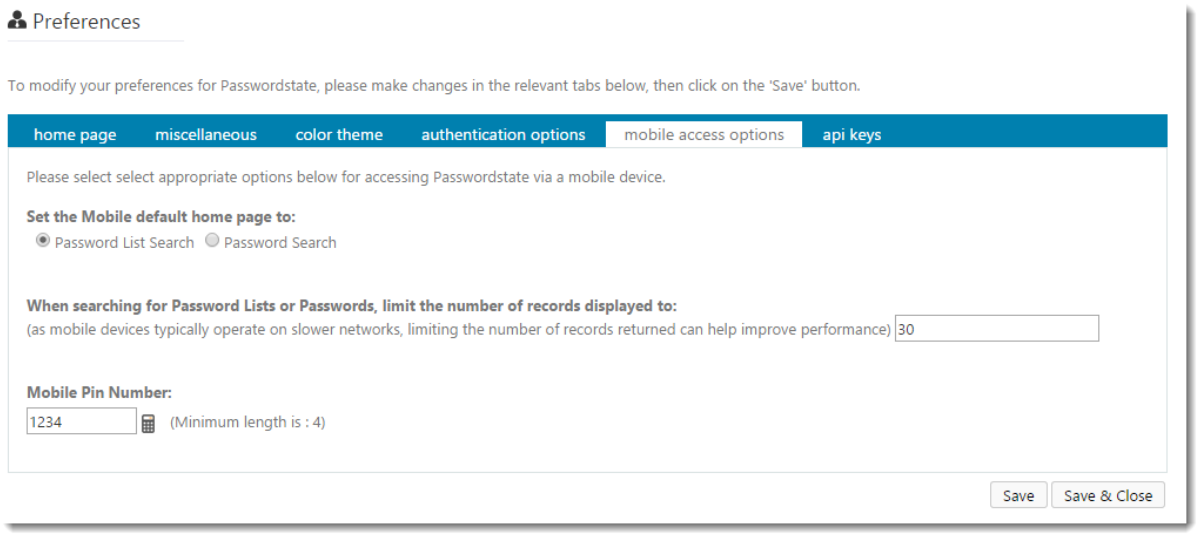
© 2017 Click Studios (SA) Pty Ltd

6.1.5 Mobile Access Options Tab

The Mobile Access Options tab allows you to specify various settings for the Mobile Client version of Passwordstate, and also the Pin Number used for you to authenticate. In particular you can specify:

Note: Your Passwordstate Security Administrator(s) may disable the use of the Mobile Client, in which case all option on this tab will be disabled. The length of the Pin Number is also controlled by your Security Administrator(s).

Default Home Page	You can either choose your default home page to browse/filter all the Password Lists you have access to, or go straight to a screen where you can search for the password record you require
Limit the Number of Records to	As cellular/mobile networks are typically slower than local networks, it's recommended you limit the number of records returned to help with performance.
Mobile Pin Number	The Pin Number you will use to authenticate with when using the Mobile Client - this is in conjunction with your UserID for Passwordstate

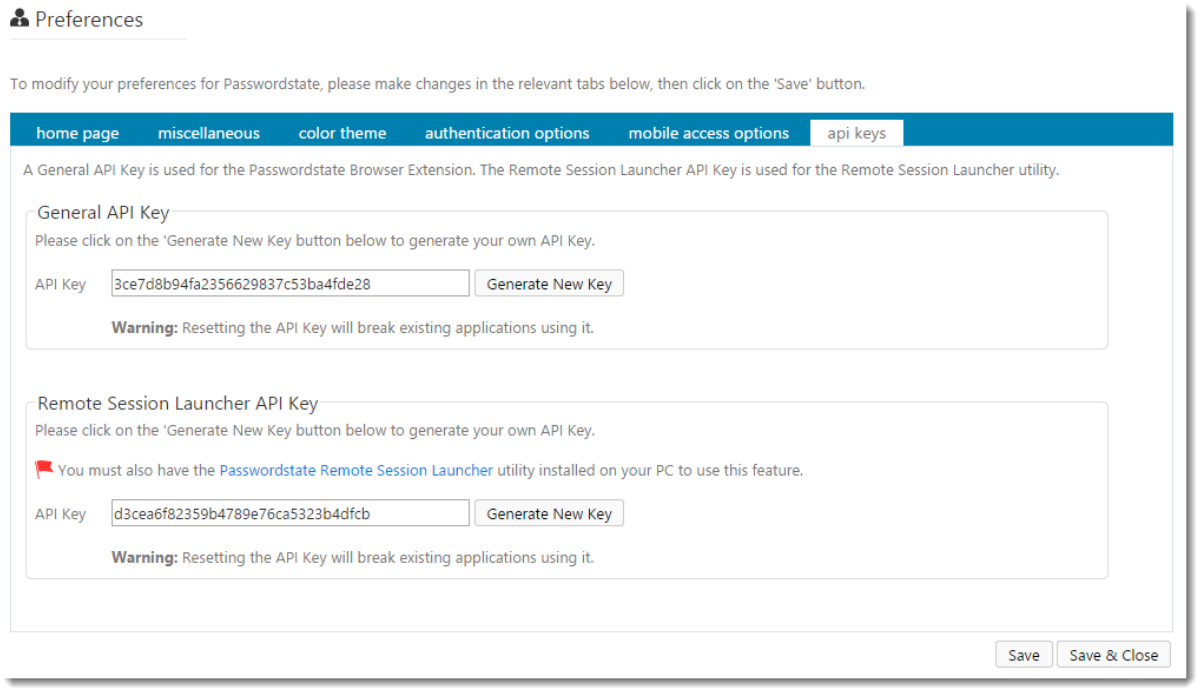


6.1.6 API Keys Tab

The API Keys Tab allows you to create API Keys for the Browser Extension and Remote Session Launcher features

Please refer to the Browser Extension Manual and 'Remote Session Launcher Installation Instructions.pdf' document for instructions on how to use these features

© 2017 Click Studios (SA) Pty Ltd



6.1.7 Browser Extension

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

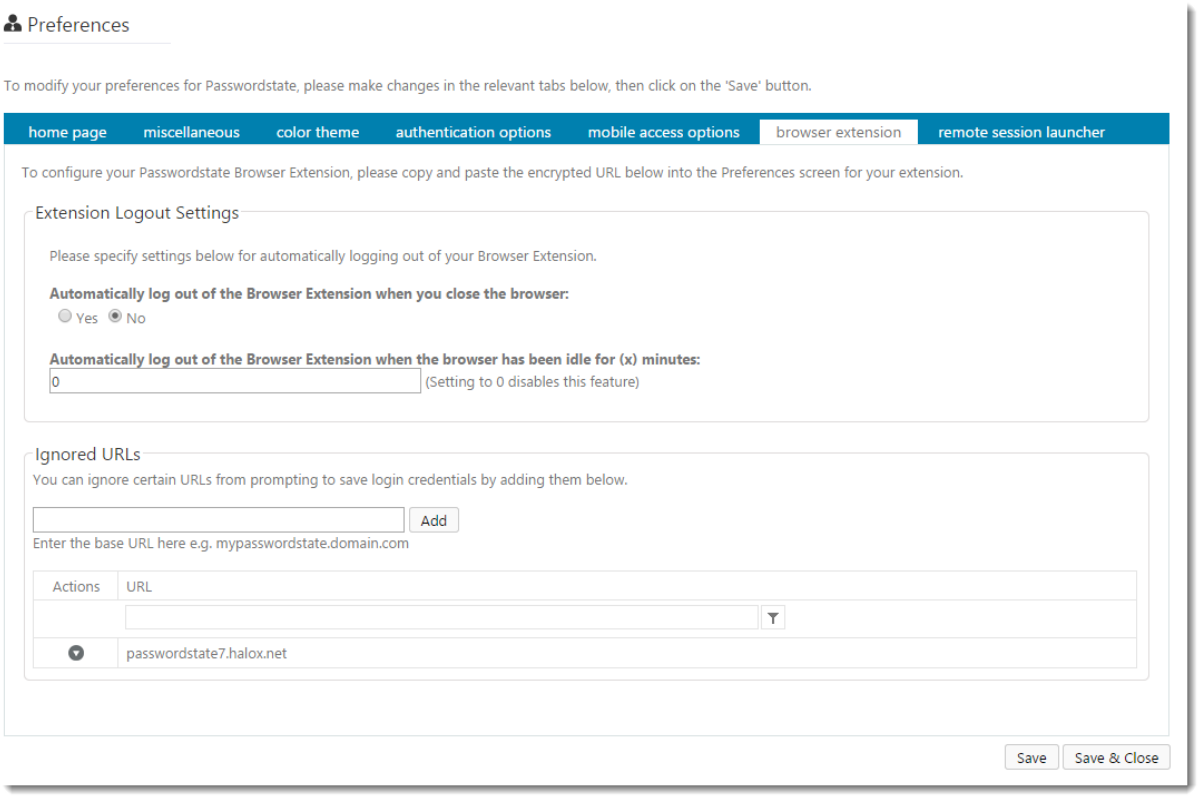
In particular you can:

- Specify various automatic logout settings, either when you close the browser, or if your browser has been idle for set period of time
- Specify which URLS will be ignored by the Browser Extension, so that it doesn't prompt you to save login credentials

Please refer to the Browser Extension Manual for instructions on how to use this feature.

Note: The Logout settings can be overridden by your Passwordstate Security Administrator(s), and they can also specify additional URLs to be ignored for all users

© 2017 Click Studios (SA) Pty Ltd



6.1.8 Remote Session Launcher

In order to use the Remote Session Launcher utility (for RDP, SSH, Telnet or VNC Sessions), you must first create an appropriate API Key for the utility, before you installed the local client for this feature.

Please refer to the 'Remote Session Launcher Installation Instructions.pdf' document for instructions on how to use this feature.

6.2 Email Notifications

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

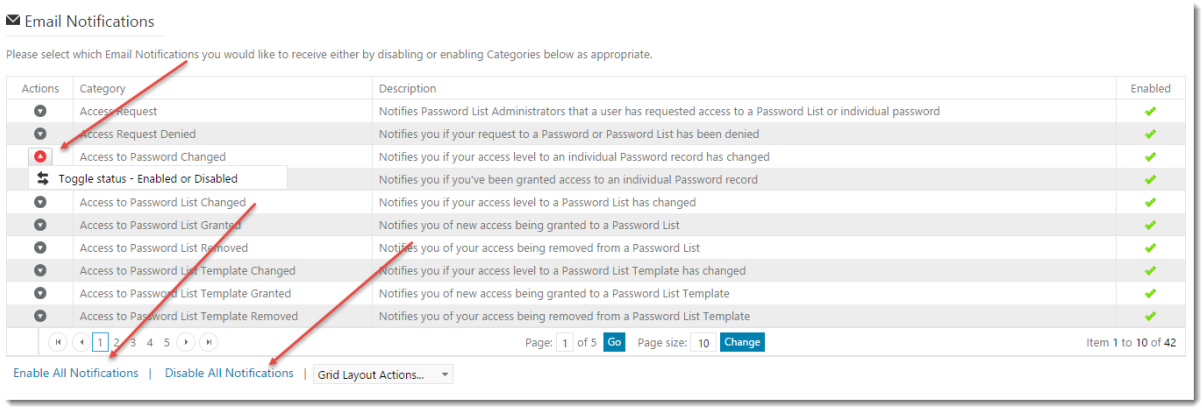
Note: There is a feature called 'Email Notification Groups' which your Security Administrators of Passwordstate can use, and using this feature for your account will cause the 'Choose Email Notifications' button below to be disabled

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

© 2017 Click Studios (SA) Pty Ltd

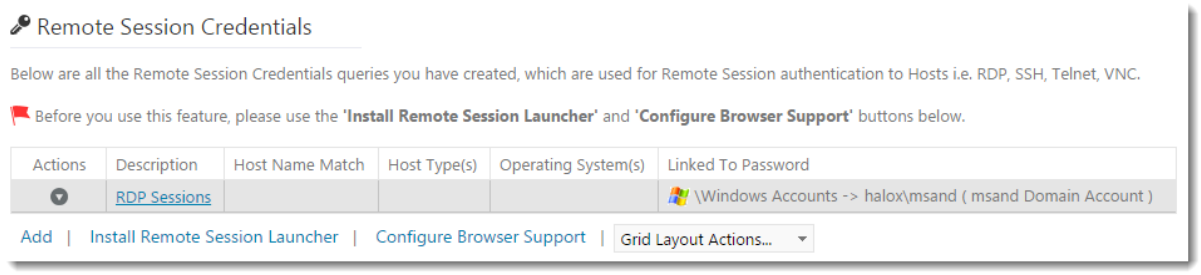
By Clicking on the 'Choose Email Notifications' button, you will be presented with a list of email categories, which can either be enabled or disabled. There is also an option to enable or disable all email notifications with the buttons at the bottom of the grid.



6.3 Remote Session Credentials

In order to use the Remote Session Launcher feature, you must create one or more Remote Session Credential queries which can be used as login credentials for the Remote Session. Prior to doing this you need to:

- Go to the screen Preferences -> API Keys Tab, and create an API Key for the Remote Session Launcher utility
- Install the Remote Session Launcher utility as per the document 'Remote_Session_Launcher_Installation_Instructions.pdf'. This file was included in the Passwordstate.zip file you downloaded, or can you find it here - http://www.clickstudios.com.au/documentation/default.html
- Click on the 'Configure Browser Support' button you see below to configure your browser
- Now create the Remote Session Credential query as appropriate - see further instructions below

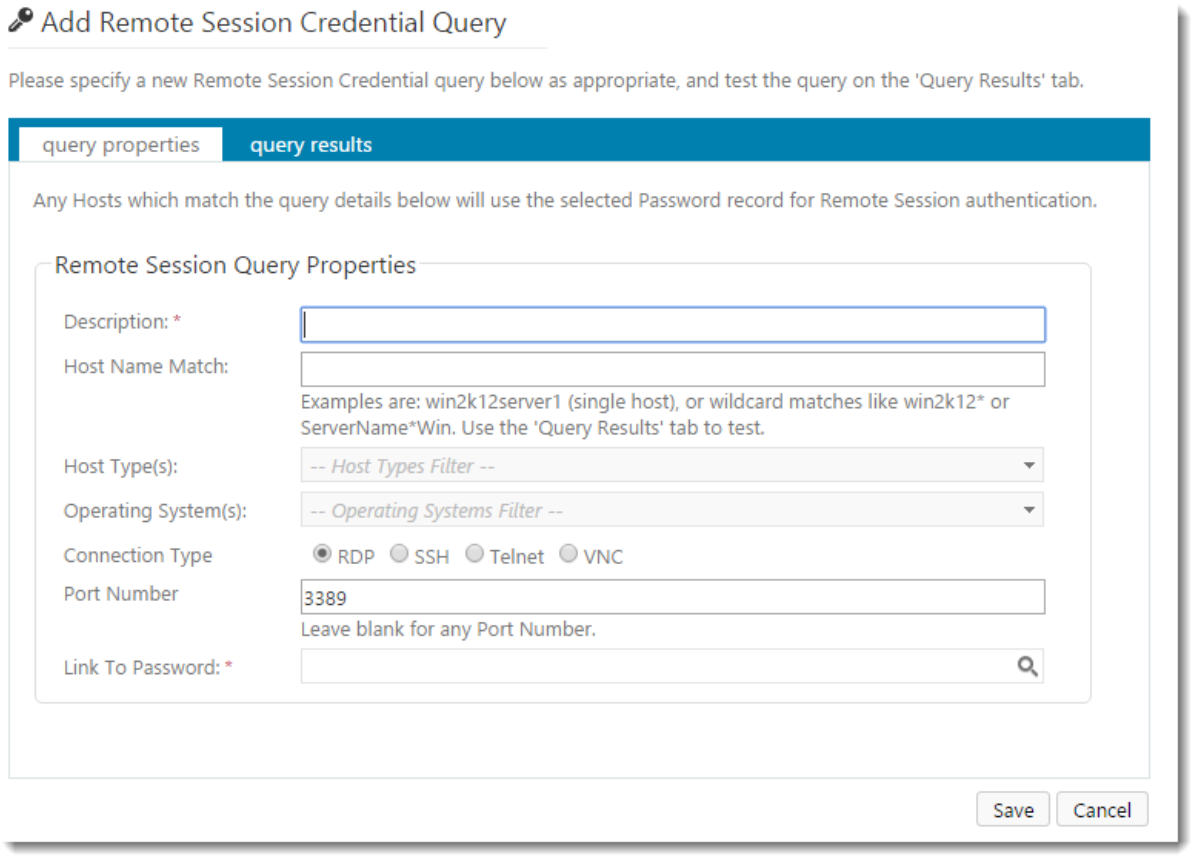


When creating a Remote Session Credential Query, you can perform certain filtering based on Host Name, Host Types, Operating Systems, Connection Types and Port Numbers. Once you've specified these parameters, you simply link the query to a password record in Passwordstate that you would like to authenticate with.

© 2017 Click Studios (SA) Pty Ltd

This query based approach allows you to supply different login credentials, based on whatever criteria you want i.e. if you had different domains, your could filter in the Host Name by the domain portion, and have different login credentials for each domain.

When using the Remote Session Launcher feature, if you click on a Host in Passwordstate and it detects more than one Remote Session Credential for the Host you are wanting to connect to, then it will present you with a popup screen asking you wish credential you would like to authenticate with.



Note: When you first create a Remote Session Credential, your account is given access to it. Then from the 'View Permissions' menu item under the 'Actions' menu, you can apply permissions for other users or security groups to also use these credentials. Even if the other users don't have access to the Linked password record in Passwordstate, they can still use the Remote Session Credential if you choose to allow them to.

7 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

© 2017 Click Studios (SA) Pty Ltd

Administrators Manual', available from the Help menu.

8 Help Menu

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

1. Browser Extension Manual - for form-filling web site logins
2. Guided Tour of Passwordstate - this will show a popup window guiding you through some of the basic functions
3. Mobile Client Manual - for using the Passwordstate Mobile client
4. Online Help - this links back to the Support page at Click Studio's web site
5. Remote Session Launcher (instructions for installing and using the Remote Session Launcher Utility)
6. Security Administrators Manual
7. User Manual (this help file you are referencing now)
8. Web API Documentation
9. What's New - this shows the change-log for Passwordstate

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

9 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.

Controlling Settings for Multiple User Accounts
Export All Passwords and Import into KeePass
How to Clone Folders and Password Lists
Moving Passwordstate to a New Database Server
Moving Passwordstate to a New Web Server
Multiple Options for Hiding Passwords
Specifying Your Own Custom Fields
Password Resets
Passwordstate Disaster Recovery

9.1 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.

© 2017 Click Studios (SA) Pty Ltd

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

Mobile Access Options

Set the Mobile default home page to
When searching for Password Lists or Passwords, limit the number of records displayed to

Password List Options

When creating new Shared Password Lists, base the settings on the following Template's settings
When creating new Shared Password Lists, base the permissions on the following Template's permissions
If copying settings from a Template to a Shared Password List, also link them
When creating new Private Password Lists, base the settings on the following Template's settings
If copying settings from a Template to a Private Password List, also link them

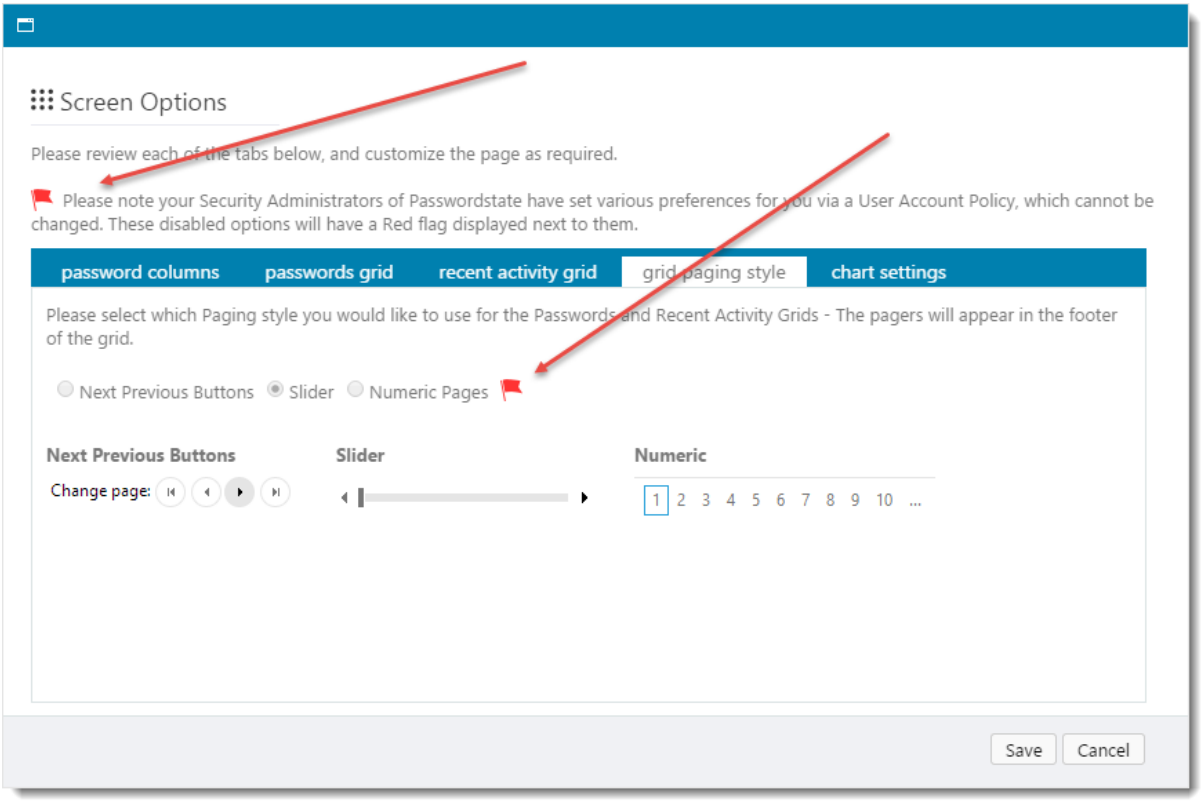
Note 1: When you first add a new User Account Policy, it is disabled by default. It is recommended that before you enable the policy, you apply the permissions required, then click on the 'Check for Conflicts' button. The Check for Conflicts process will ensure that there are no two settings with different values assigned to a user's account - this could cause confusion for the

© 2017 Click Studios (SA) Pty Ltd

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.



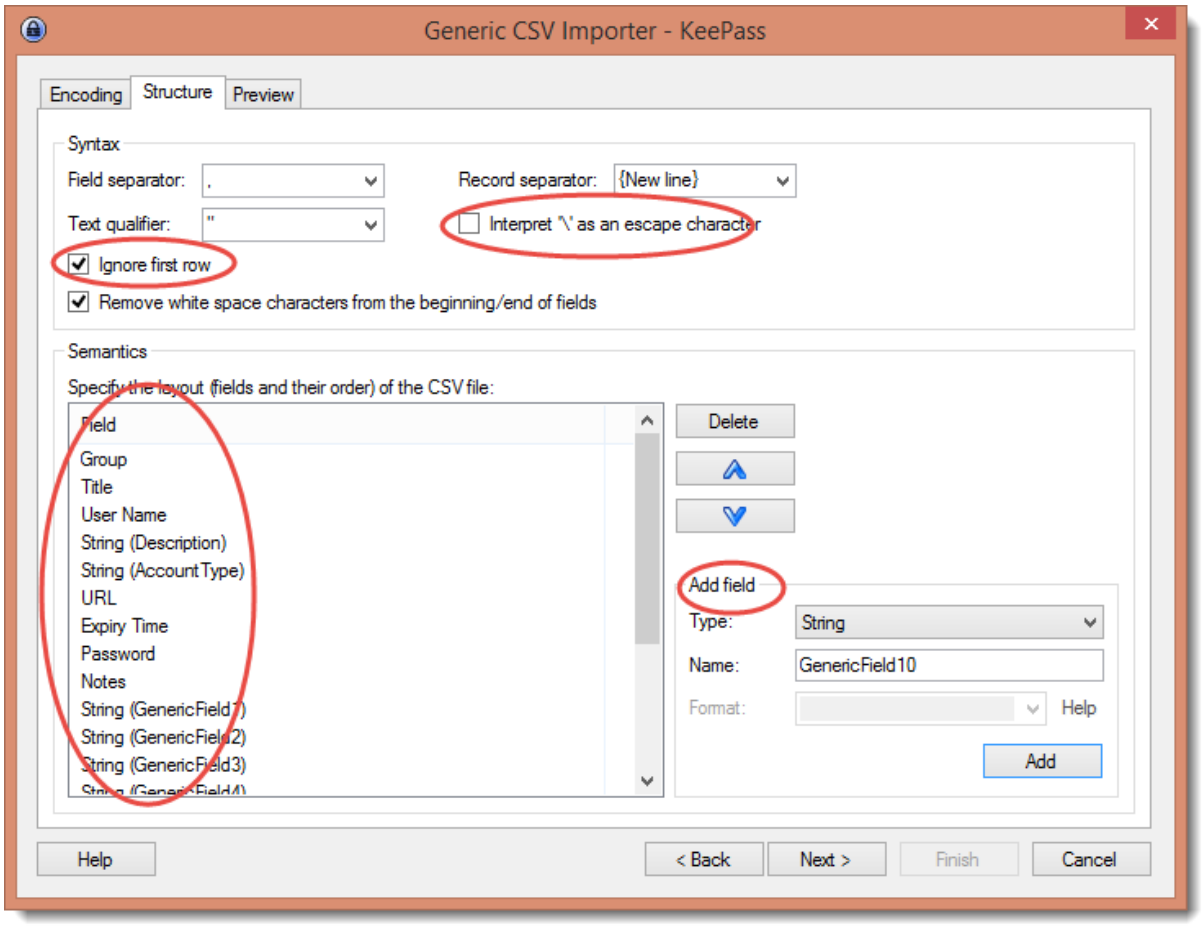
9.2 Export All Passwords and Import into KeePass

This KB article will explain how to export all Shared passwords from Passwordstate, and import them into KeePass. Note: KeePass 2.27 was used during documenting this process.

- Go to the page in Passwordstate Administration -> Export All Passwords
- Select the option 'KeePass Compatible CSV file', and check/uncheck the Auditing option as appropriate
- Save the exported csv file somewhere safe
- Open KeePass and create a new empty database
- From the 'File' menu, select 'Import'
- Select the 'Generic CSV Importer' option, browser to the saved csv file above, and click on the 'OK' button
- On the 'Structure' tab, select the 'Ignore First Row' option, deselect the option 'Interpret \ as an

© 2017 Click Studios (SA) Pty Ltd

escape character', and ensure the fields selected match the screenshot below (you will need to use the 'Add Field' feature on this screen to do this). Make sure you create the 10 Generic Fields as well



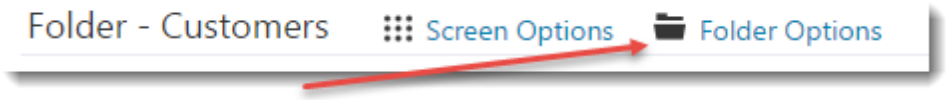
- Now click on the 'Next' button, and then the 'Finish' button

9.3 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:

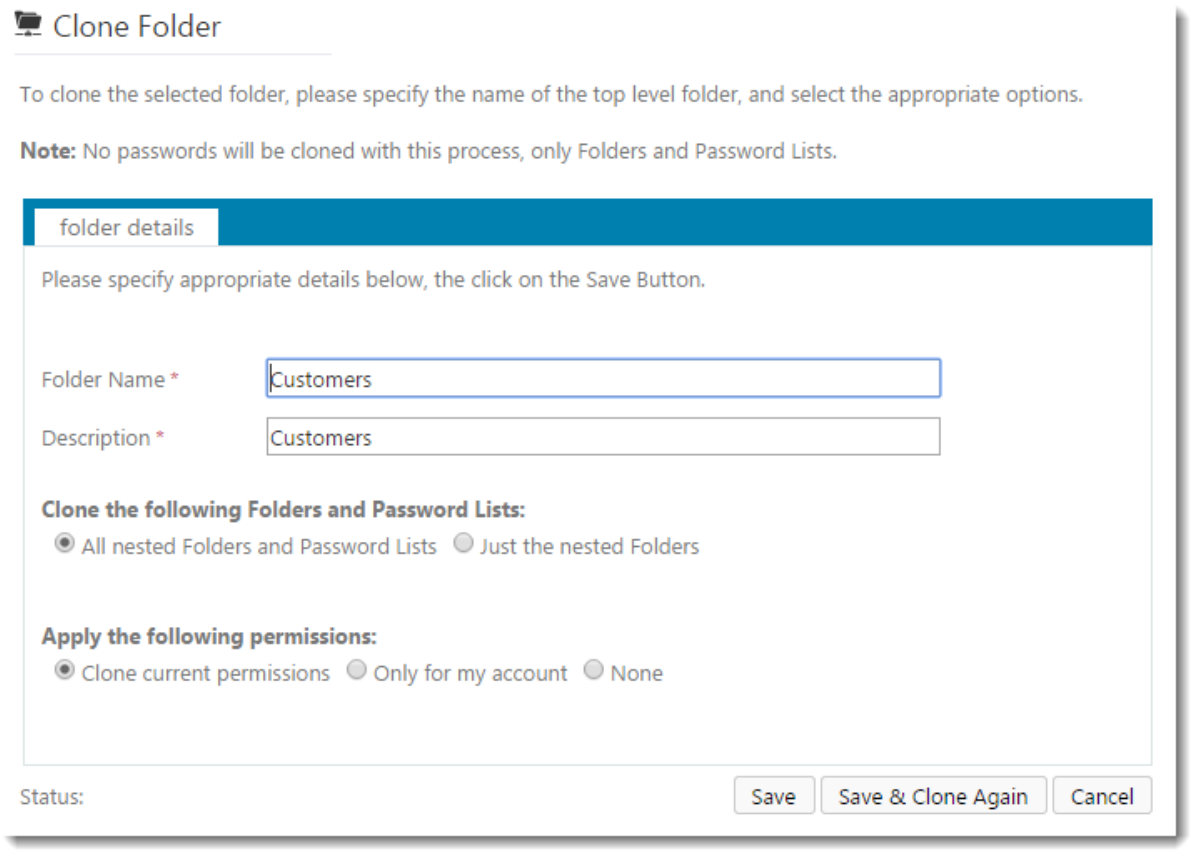


© 2017 Click Studios (SA) Pty Ltd

- 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.



9.4 Moving Passwordstate to a New Database Server

Please use the following instructions as a guide for moving an existing Passwordstate database to a new database server. Please note these instructions will assume you have some knowledge for using the Microsoft's SQL Server Studio Management Studios tool, and have appropriate

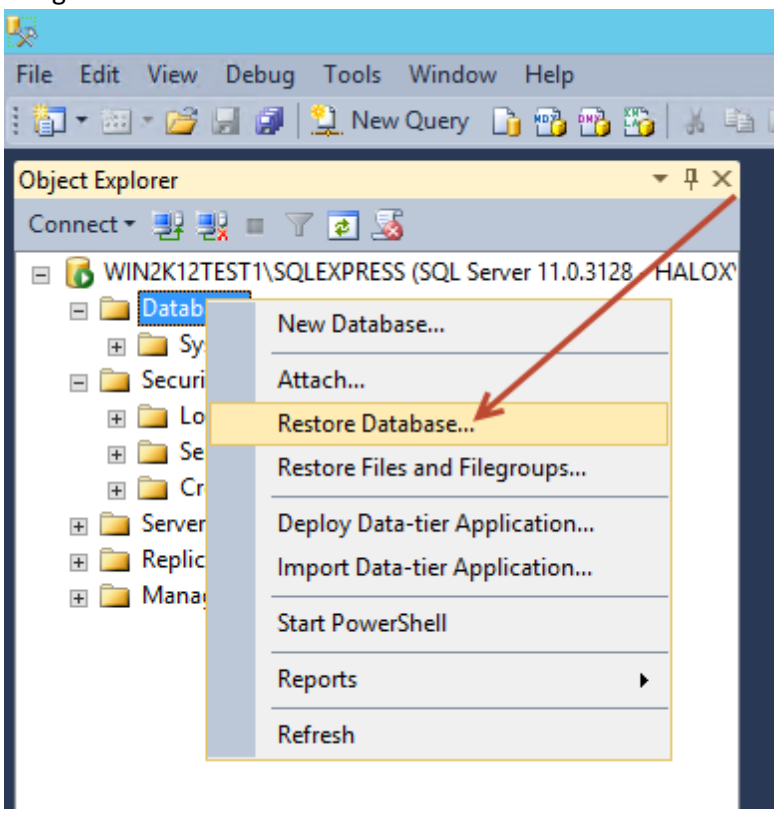
© 2017 Click Studios (SA) Pty Ltd

permissions to restore databases.

Note: These instructions are for Passwordstate version 6 and 7, using SQL Server Management Studio 2012 - some screens may look different to you for prior versions.

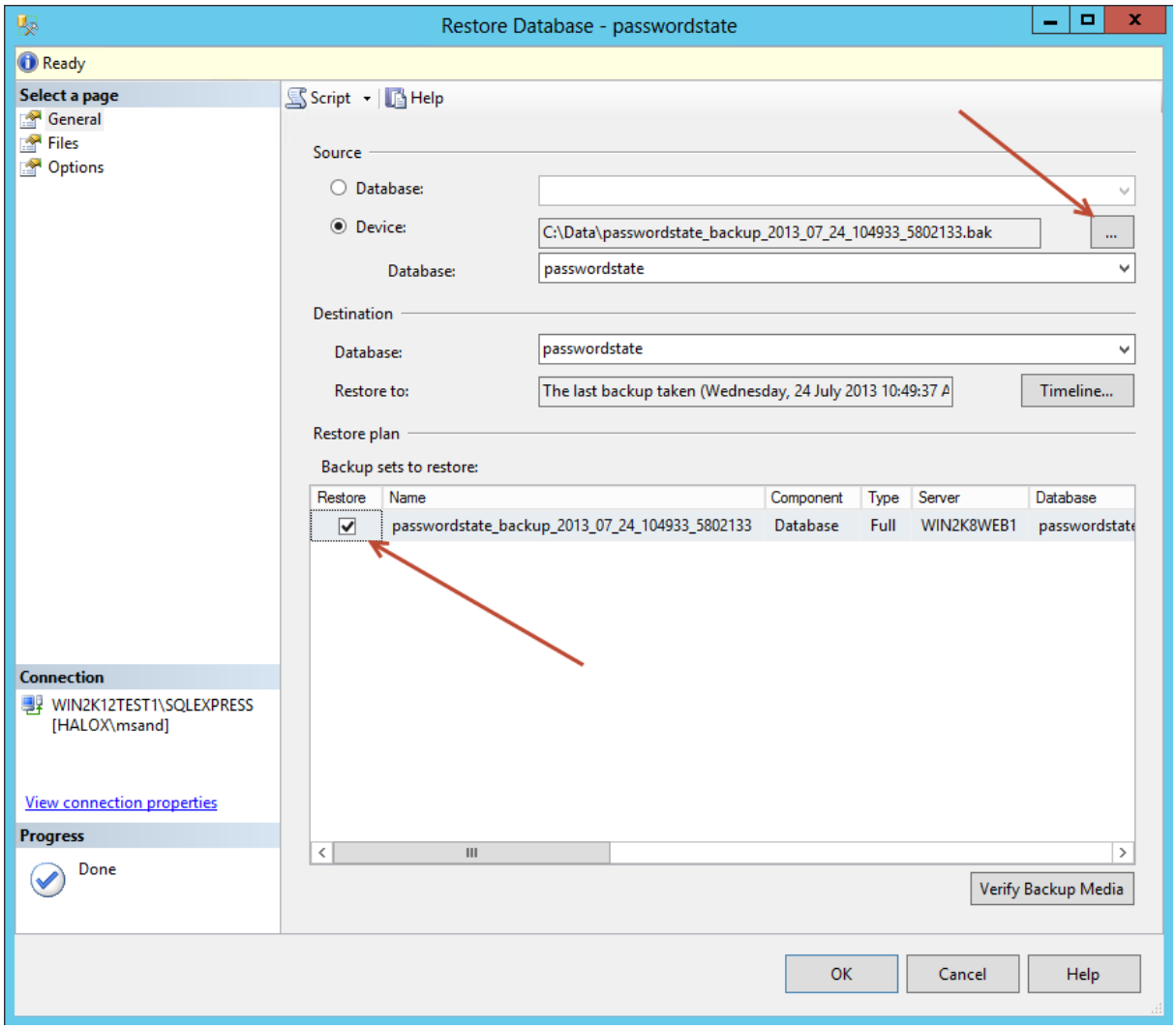
Restore your database:

- On your new database server, open Microsoft SQL Server Management Studio
- Right click on 'Databases' and select 'Restore Database'



- Click on the 'Device' eclipse and browse and select your saved database backup, and click the 'Restore' checkbox under the section 'Select the backup set to restore'

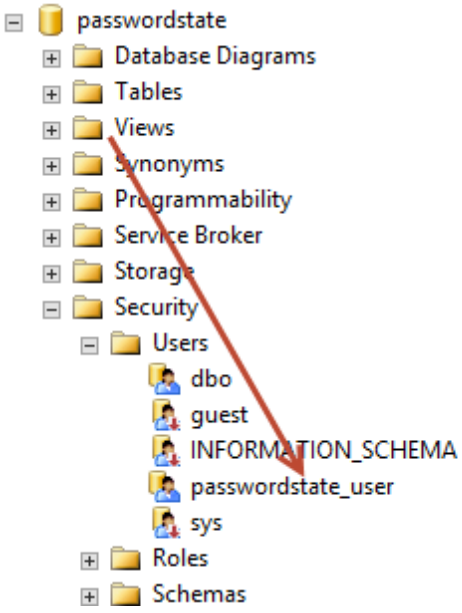
© 2017 Click Studios (SA) Pty Ltd



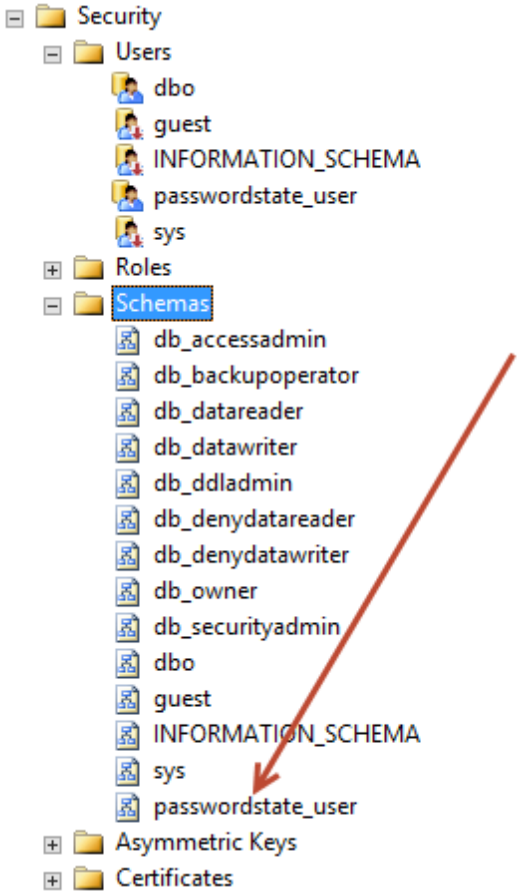
- Click the 'OK' button to restore, then right-click on 'Databases' again and click 'Refresh' so your restored database shows

Navigate to Databases -> passwordstate -> Security, and delete the account passwordstate_user

© 2017 Click Studios (SA) Pty Ltd

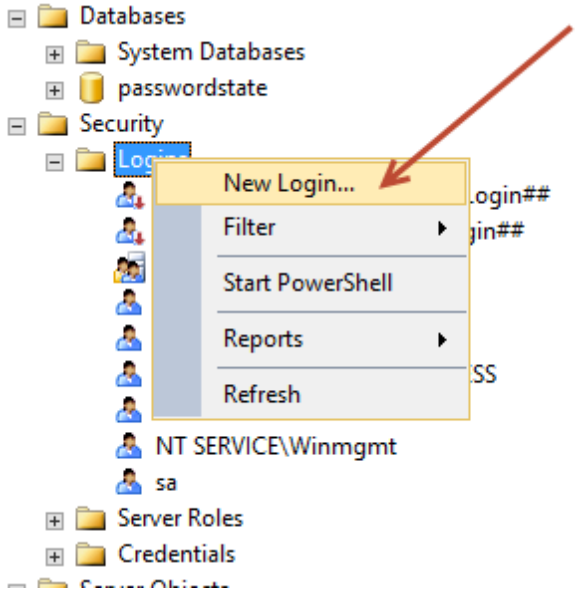


- If you receive an error message similar to 'The database principal owns a schema in the database, and cannot be dropped', then expand the 'Schemas' tree node and delete the 'passwordstate_user' schema



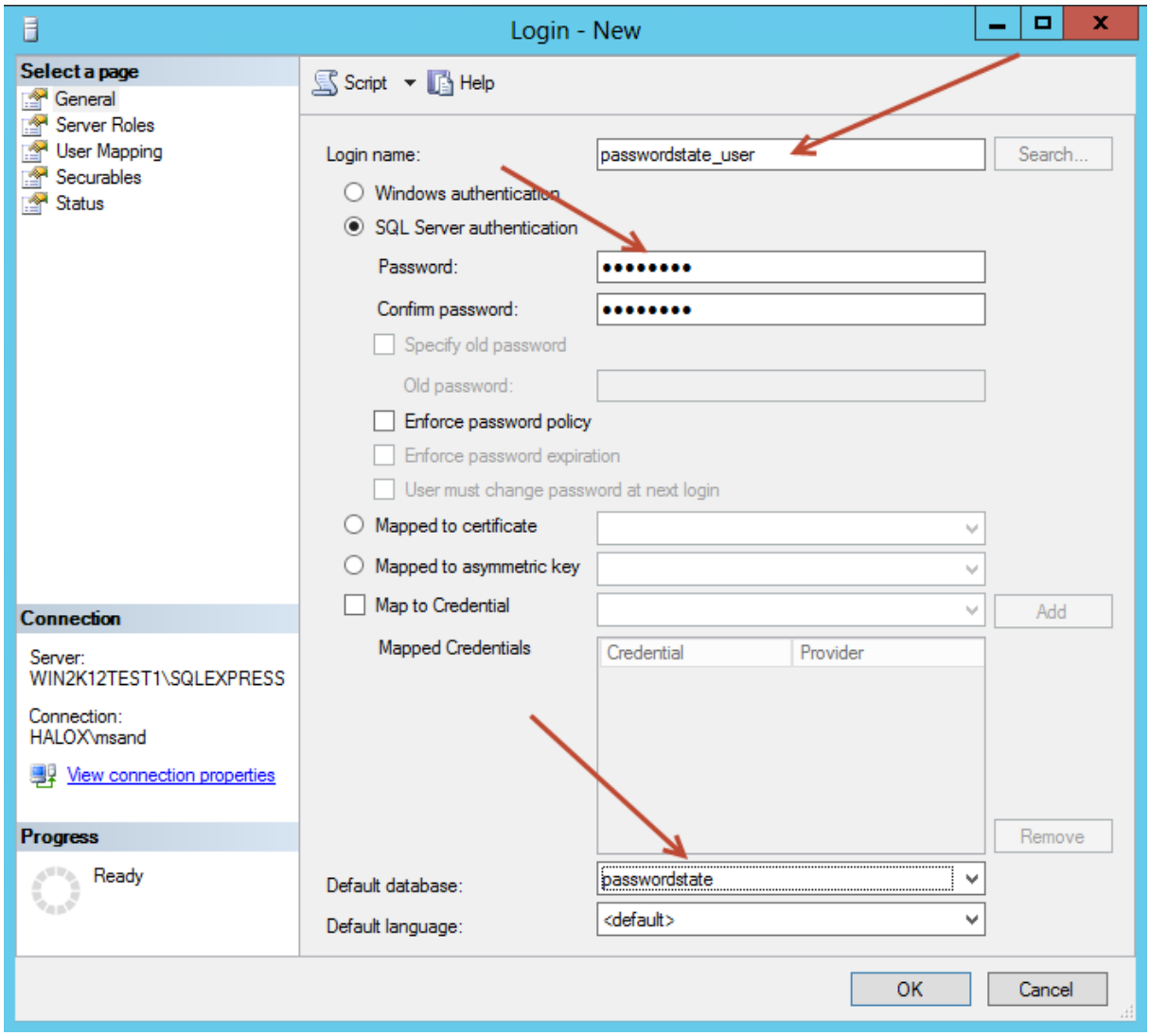
© 2017 Click Studios (SA) Pty Ltd

- Navigate to \Security -> Logins, right click and select New Login



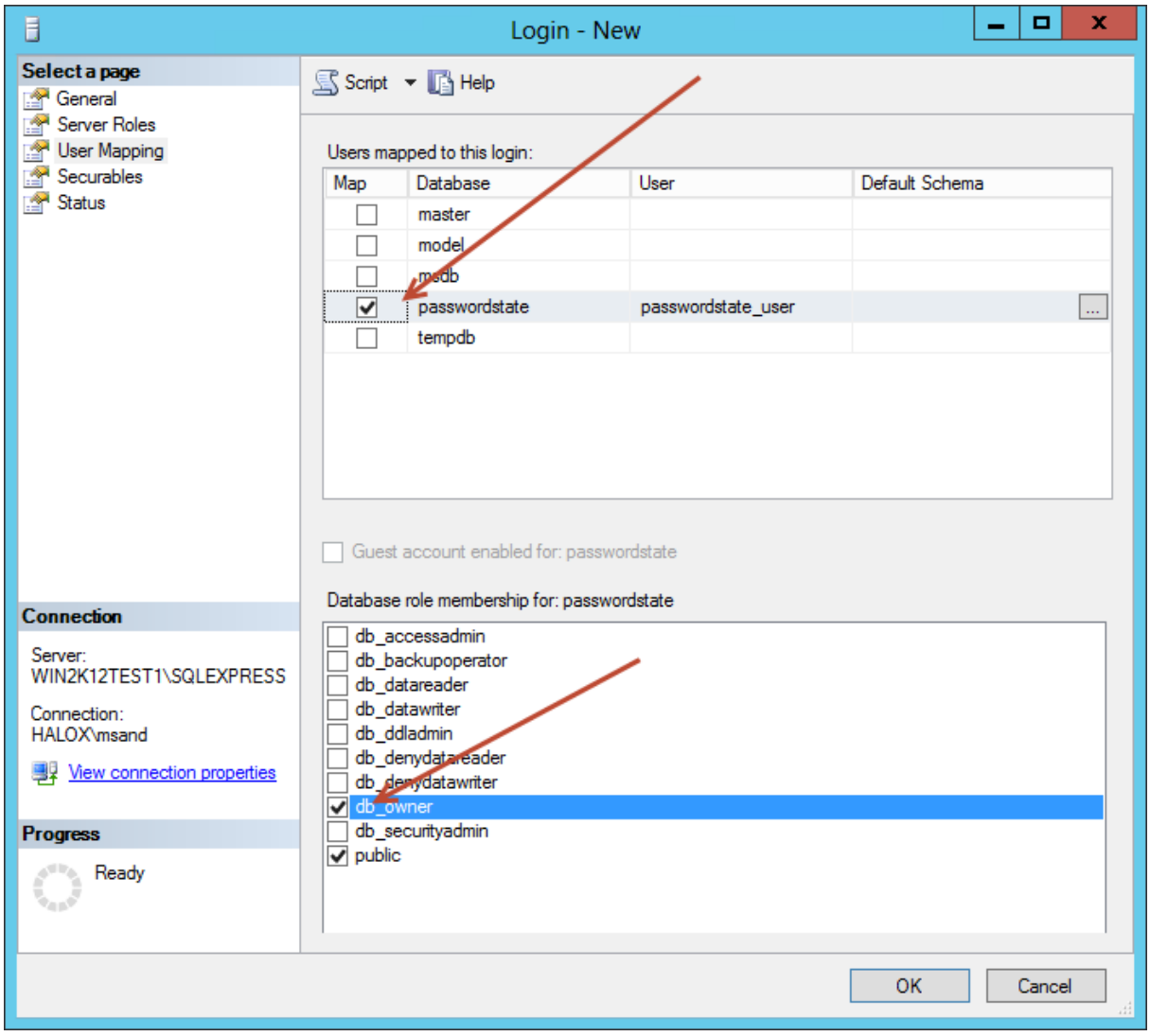
- Create a new SQL Account account called passwordstate_user, setting the password to the value in your database connection string in your web.config file (located in the root of the Passwordstate folder), set Default database to passwordstate

© 2017 Click Studios (SA) Pty Ltd



- Grant db_owner rights to the passwordstate database under the User Mapping page

© 2017 Click Studios (SA) Pty Ltd



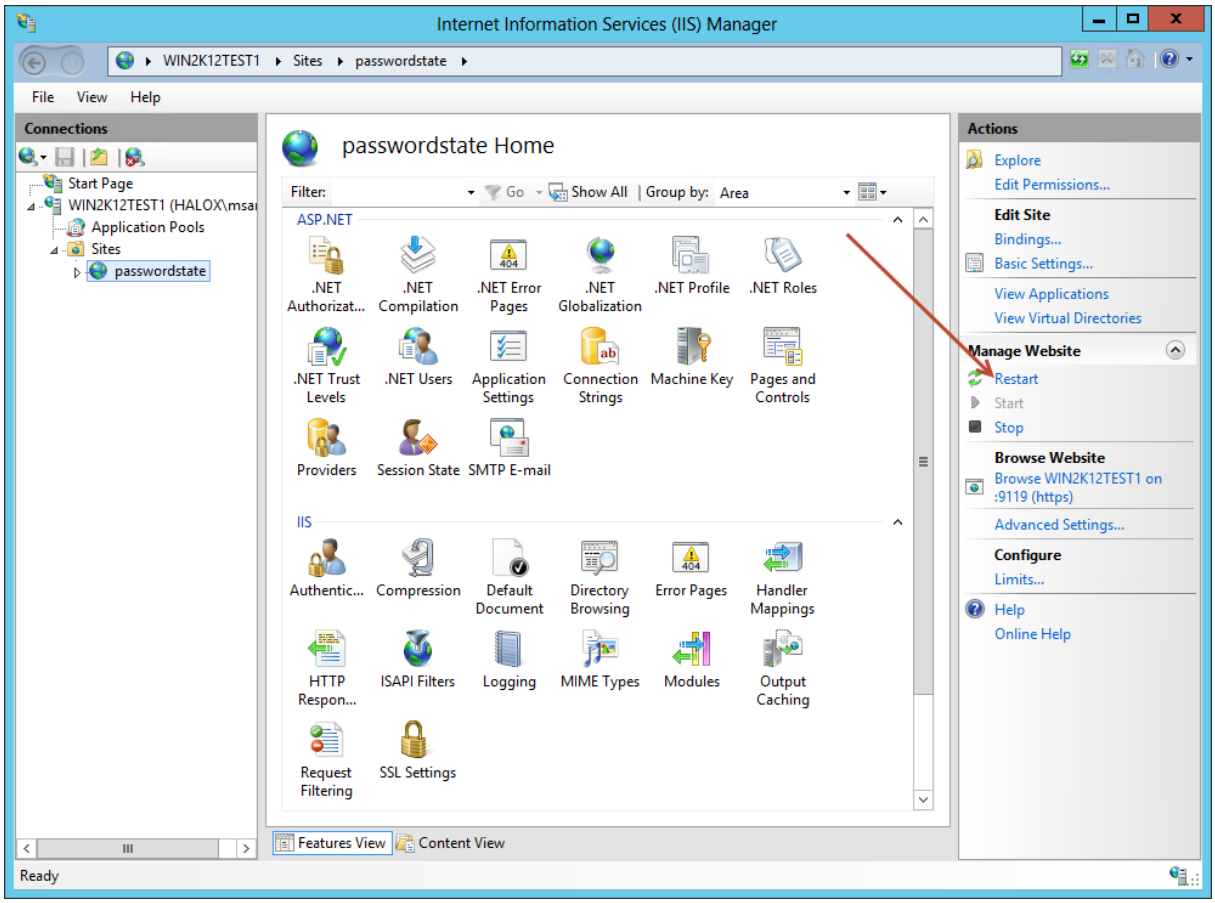
Final Changes to your Web Site:

- Now you need to edit the Data Source value in the web.config file for the PasswordstateConnectionString - this value needs to be the host name of your new database server. Note: if your SQL Server is installed with a named instance, then the formatting of the host name should be HostName\SQLInstance

```
<connectionStrings>
 <add name="PasswordstateConnectionString"
      connectionString="Data Source=win2k12test\sqlexpress;Initial Catalog=passwordstate;
      User ID=passwordstate_user;Password=MyPassword" providerName="System.Data.SqlClient"/>
</connectionStrings>
```

- Restart the Passwordstate Windows Service so it picks up the changes in the web.config file
- And restart your Passwordstate web site in IIS. You should now be able to point your browser to the Passwordstate web site, and successfully connect to your new database server

© 2017 Click Studios (SA) Pty Ltd



9.5 Moving Passwordstate to a New Web Server

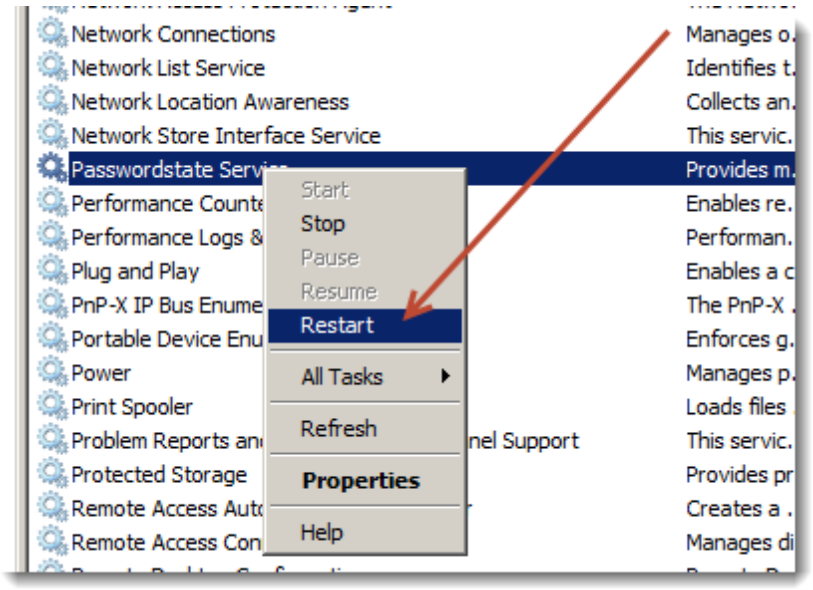
Please use the following instructions as a guide for moving an existing Passwordstate web installation to a new server. While it's not necessary, it's recommended you install the same version of Passwordstate on your new web server to rule out any upgrade issues during the migration. Previous builds can be downloaded from here - Download Archive

Installing Passwordstate:

- Prior to installing Passwordstate on your new web server, if the name of your new web server is changing, then must add the new web server's host name to the list of authorized web servers within Passwordstate. You can do this from the screen Administration -> Authorized Web Servers
- Download your correct build of Passwordstate from here - Passwordstate Build Archive
- Now you can follow the instructions in the document General Installation Instructions to install Passwordstate, stopping when you get to section 'Configuring Passwordstate for First Time Use'
- If you are using a CNAME DNS entry to resolve the URL binding for your web site, you will now need to edit the DNS entry and update the host name of your new web server (the DNS entry is used so you can type http://passwordstate into your browser)

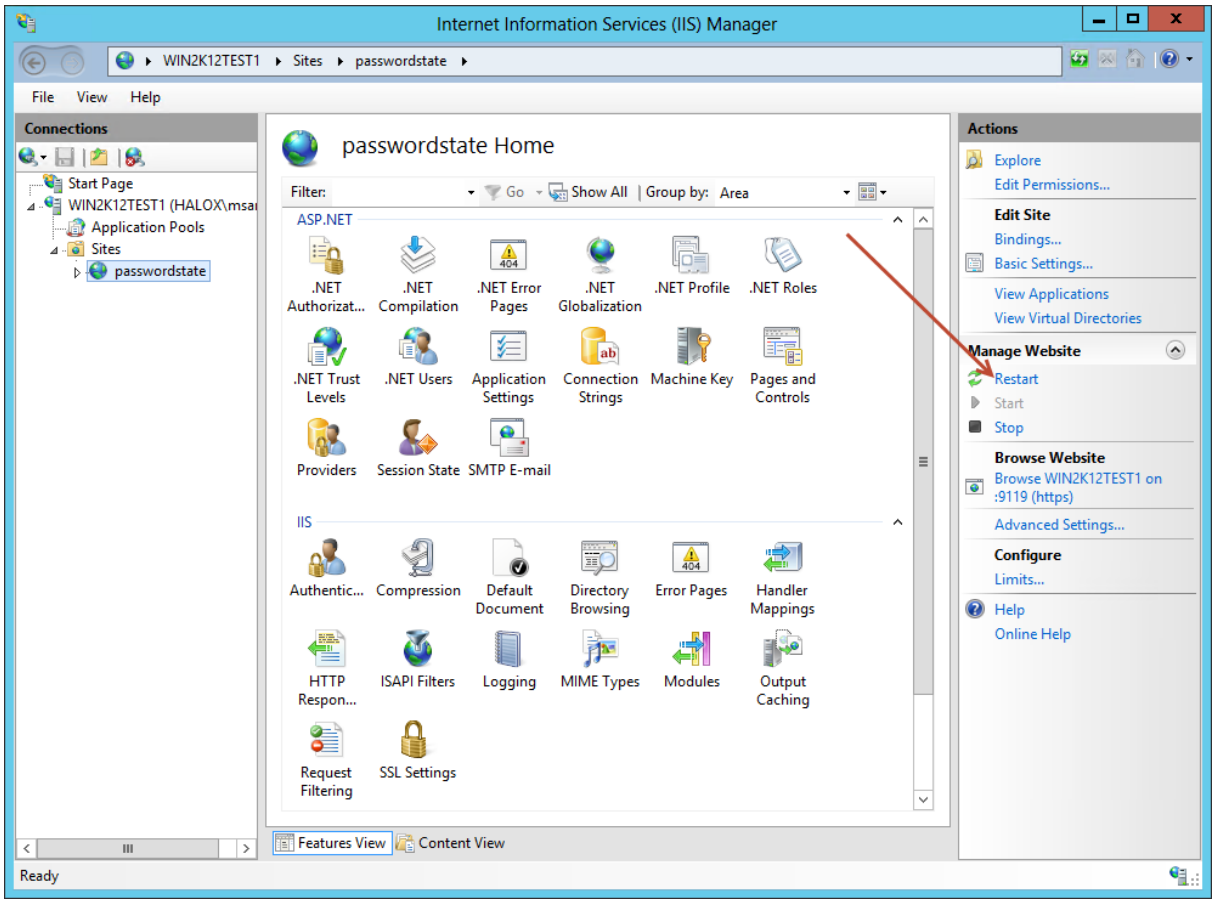
© 2017 Click Studios (SA) Pty Ltd

- If you are using an SSL Certificate with your existing installation of Passwordstate, then you will also need to configure this new installation to use a SSL Certificate as well
- Now you need to copy the web.config file from your existing installation (found in the root of the Passwordstate folder) to your new installation - this file includes settings for the database connection string, and split secrets which form part of the encryption keys. Note: If you have encrypted your database connection string, or AppSettings section of the web.config file, you will need to decrypt these prior to moving this file. Instructions for this can be found in the Installation Documentation - General Installation Instructions.
- If you are using RSA's SecurID two-factor authentication with Passwordstate, you will also need to copy across the file located in the /securid folder
- Restart the Passwordstate Windows Service on your new web server (after the Service has been restarted, it will recreate any custom Logos or images you have uploaded into Passwordstate - you may need to give it a minute or two to do this)



- Restart your Passwordstate web site in IIS

© 2017 Click Studios (SA) Pty Ltd

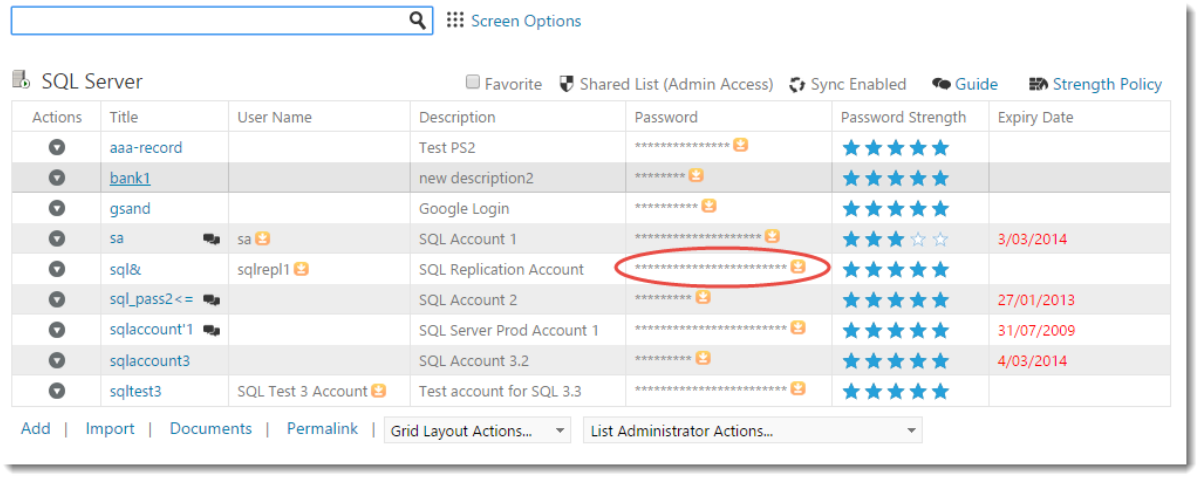


- If everything has been done correctly above, you should now be able to point your browser to the new Passwordstate web site.

9.6 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.

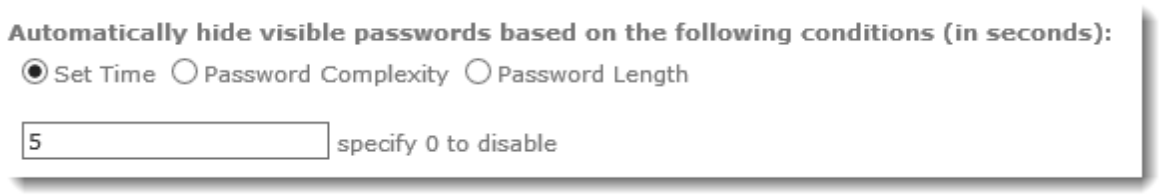
© 2017 Click Studios (SA) Pty Ltd



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:

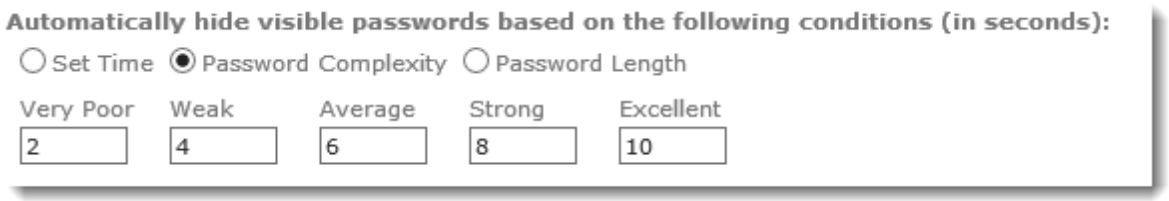
Option 1 – Hide Based on a Set Time

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

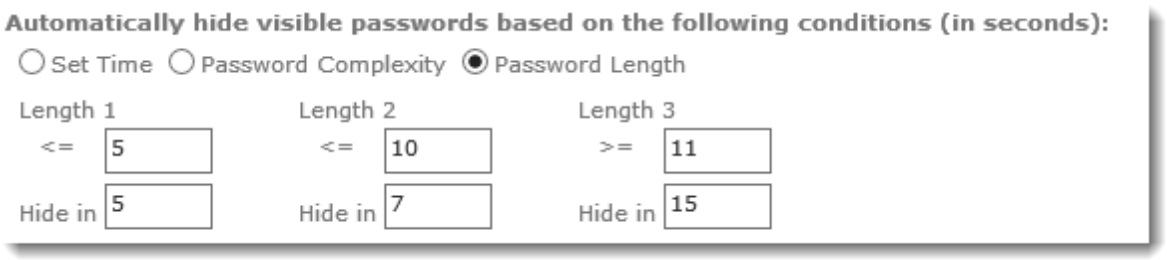
As you're aware, each Password is deemed to be of a certain 'Strength', and this strength can differ depending on which 'Password Strength Policy' is assigned to the Password List. You can set a specific time interval for each of the 5 different Password Strengths – Very Poor, Weak, Average, Strong & Excellent



© 2017 Click Studios (SA) Pty Ltd

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.



9.7 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

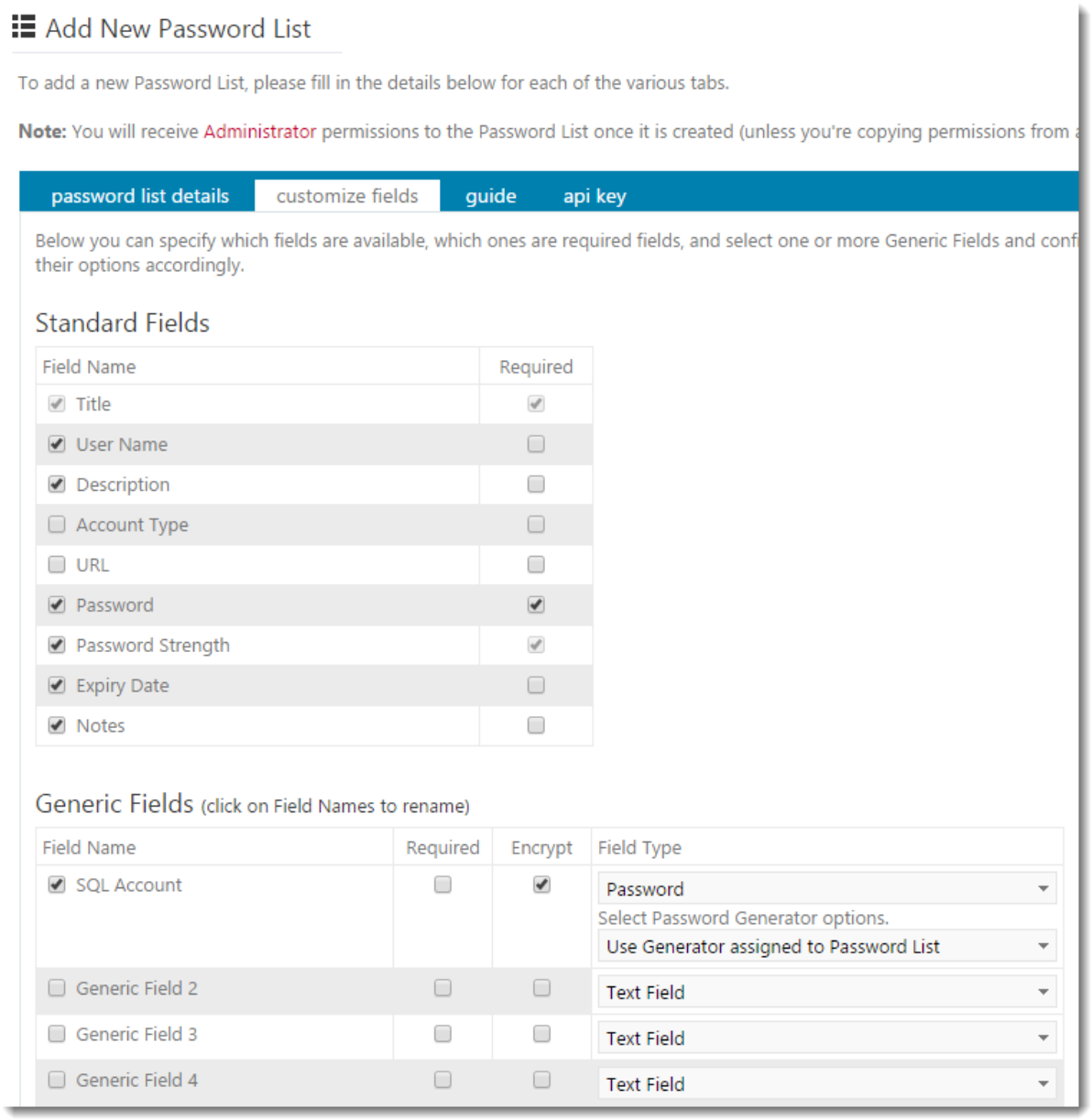
In addition to the Standard Fields, you can select up to 10 different custom fields, and the custom fields can be named to anything you want, and have the following data types:

- 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

© 2017 Click Studios (SA) Pty Ltd

- 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.



9.8 Password Resets

The following is a list of KB Articles relate to various Password Reset features in Passwordstate.

© 2017 Click Studios (SA) Pty Ltd

9.8.1 Password Reset Scripts and Requirements

In Passwordstate, it's possible to perform Password Resets on remote Hosts/Systems of the following type:

- Active Directory - see Resetting Active Directory Passwords
- Local Windows Accounts
- Windows Services
- IIS Application Pools
- Scheduled Tasks
- Cisco network equipment (routers, switches, etc)
- Linux/Unix Accounts
- Microsoft SQL Server, MySQL Server accounts and Oracle accounts
- Com+ Components
- VMWare ESX Accounts
- F5 BIG-IP Load Balancers
- HP iLO Out-Of-Band Management Cards
- IBM IMM Out-Of-Band Management Cards
- Dell iDRAC Out-Of-Band Management Cards
- Juniper ScreenOS firewalls
- Juniper Junos devices
- HP H3C switches and routers
- HP Procurve switches and routers
- And anything else you create your own PowerShell Password Reset scripts for

In order to use Password Reset and Validation features in Passwordstate, there are certain system requirements which must be met. A full list of requirements can be referenced in this document - http://www.clickstudios.com.au/downloads/version7/Password_Discovery_Reset_and_Validation_Requirements.pdf

The following content will describe additional high level details required for configuring Password Resets, and also specifics for each of the different Password Reset Scripts.

General Requirements

- Host records must be first added to Passwordstate, before you can associate Password records with them. You can either add Hosts manually, import via CSV, add via the API, or use a Host Discovery Job to query Active Directory - Hosts and Resource Discovery

© 2017 Click Studios (SA) Pty Ltd

- Some Password Reset Scripts require a Privileged Account Credential to be associated with them (table below details this). Privileged Accounts can initially be created on the screen Administration -> Privileged Account Credentials, and permissions applied to them on this screen as well
- The Password List your are storing password records in which you wish to perform resets for, must have the 'Enable Password Resets' option checked for the Password List, and the password record itself needs the 'Managed Account' option checked

Note: Resetting of Active Directory Accounts is the only account type which does not use PowerShell Scripts for performing resets - instead it uses native .NET Code for this. You simply need to ensure an appropriate Privileged Account Credential is selected on the Add/Edit Password screen, one which has appropriate permissions to reset accounts - generally Account Operators should be all that's required, although high privileges pay be required if you have made changes to default permissions on account and OUs.

Script Name	Script Description	Privileged Account Required	Notes
Reset Cisco Enable Secret	Reset the Enable Secret on Cisco Hosts	Yes	
Reset Cisco Host Password Priv 1	Reset the password on a Cisco switch or router of Privilege Level 1	Yes	• For Privilege Level 1 type accounts
Reset Cisco Host Password Priv 15	Reset the password on a Cisco switch or router of Privilege Level 15	Yes	• For Privilege Level 15 type accounts
Reset COM+ Component Password	Reset the password for a COM+ Component.	Yes	
Reset Dell iDRAC Account Password	Reset Dell iDRAC Account Password	No	
Reset F5 BIG-IP Account Password - AS	Reset F5 BIG-IP Account Password - Advanced Shell Terminal Access	Yes	• Accounts in BIG-IP appliances can be configured with Terminal Access of type 'Advanced Shell' or 'TMSH'. You need to select the appropriate BIG-IP reset script to use, depending on the Terminal Access type for the Privileged Account Credentials you have associated with the Password Reset Script
Reset F5 BIG-IP Account Password - TMSH	Reset F5 BIG-IP Account Password - TMSH Terminal Access	Yes	• Accounts in BIG-IP appliances can be configured with Terminal Access of type 'Advanced Shell' or 'TMSH'. You need to select the appropriate BIG-IP reset script to use, depending on the Terminal Access type for the Privileged Account Credentials you have associated with the Password Reset

© 2017 Click Studios (SA) Pty Ltd

			Script
Reset HP H3C Password	Reset HP H3C Account Password	Yes	
Reset HP iLO Password	Reset HP iLO Account Password	No	
Reset HP Procurve Password	Reset HP Procurve Account Password	Yes	• Can be used to reset both Manager and Operator accounts
Reset IBM IMM Account Password	Reset IBM IMM Account Password	No	• When resetting passwords on IBM IMM cards, you must know the LoginID of the account you wish to reset passwords for. In order to use this script, you must configure Generic Field 1 for the PasswordList with the name of 'LoginID' and this is where you can store the value for each account you wish to reset passwords for
Reset IIS Application Pool Password	Reset the password and then restart the Application Pool	Yes	
Reset Juniper Junos Password	Reset Juniper Junos Password	Yes	
Reset Juniper ScreenOS Password	Reset Juniper ScreenOS Password	Yes	• Can be used to reset the root account, and any other non-root accounts
Reset Linux Password	Reset the password for a Linux account	Yes or No	• If you do not associate a Privileged Account Credential with this script, you will SSH to the host using the account you wish to reset the password for • If you specify a Privileged Account Credential, you can SSH with this account, and then reset a password for a different account • If you want to reset the 'root' account password, then you need to specify a Privileged Account Credential to SSH with, and then the root account can be reset - generally most environments do not allow you to SSH in using the root account • When resetting passwords for Mac OS X, no Privileged Account Credential is required
Reset Linux Password using Public Key Auth	Reset the password for a Linux account using Public Key Authentication	Yes or No	• This script is intended to be used with Linux Operating Systems which require Public/ Private Key authentication to initially SSH to the host • After the initial SSH connection has been made, the SUSE Operating System does not

© 2017 Click Studios (SA) Pty Ltd

			require a Privileged Account Credential to reset the user's account, but other Operating Systems do
Reset MySQL Password	Reset the password for a MySQL account	Yes	
Reset Oracle Password	Reset the password for a Oracle Account	Yes or No	• You only need to use a Privileged Account Credential to connect to the database, if the account you're resetting the password for does not have enough permissions to perform a reset for itself
Reset Scheduled Task Password	Reset the password for a Scheduled Task	Yes	
Reset SQL Password	Reset Microsoft SQL Account Password	Yes or No	
Reset VMware ESX Password	Reset VMware ESX Account Password	Yes or No	
Reset Windows Password	Reset password for local account on Windows host	Yes	
Reset Windows Service Password	Reset the password for a Windows Service	Yes	

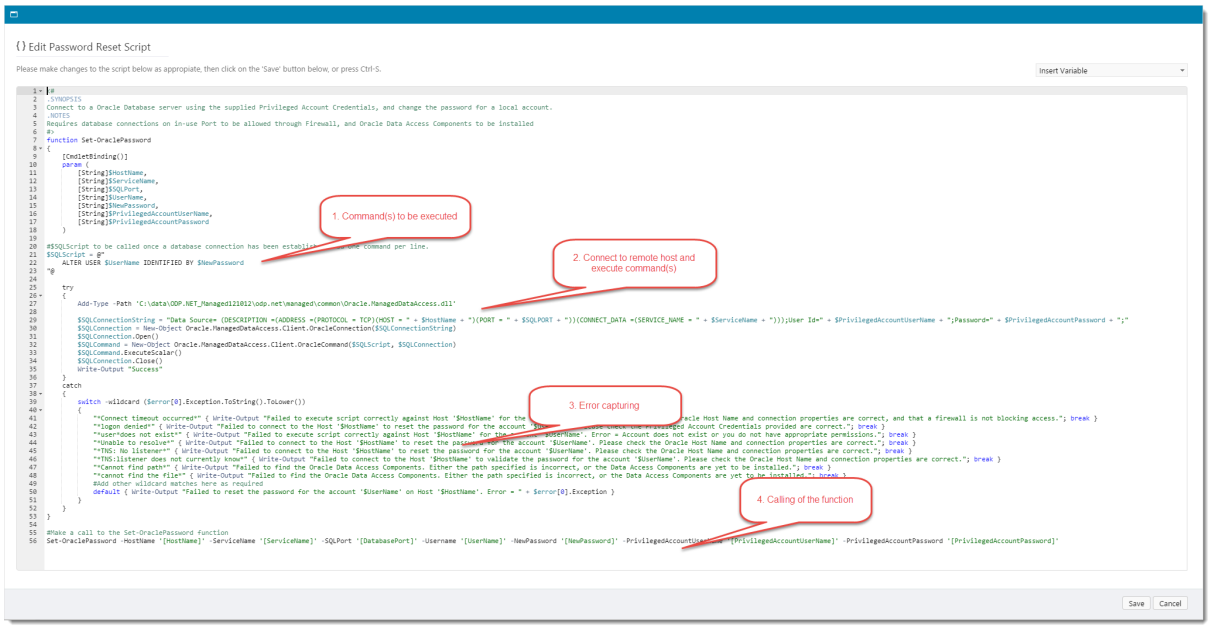
9.8.2 Structure of a Password Reset Script

When creating your own Password Reset Scripts, we recommend that you copy one of ours as a basis for your own. We recommend this so that the Passwordstate Windows Service understands when the script has been executed successfully, or has failed.

There are 4 key areas in all of our scripts, and there is a screenshot below which highlights these areas. They are:

1. Command(s) to be executed - this is the actual work done on the remote host to reset a password
2. Connect to remote host to execute command(s) - this connectivity method will vary on the host, but generally it is done via PowerShell Remoting, SSH connection, or a direct connection to a database server
3. Error Capturing - this is where we try and capture as many of the error scenarios as possible. The error messages here will be included in the email report you receive when a Password Reset attempt has failed for whatever reason
4. Calling the function - this is what initiates the call to all the 3 steps above it. The variables you see here, enclosed in square brackets [], are replaced in real-time by the Passwordstate Windows Service when the reset occurs - it queries relevant data from the password record, the host record, and possibly the privileged account record if required

© 2017 Click Studios (SA) Pty Ltd



9.8.3 Resetting Active Directory Passwords

It's possible to synchronize a password change in Passwordstate, with an Active Directory account. In order to perform this synchronization, there's a few permissions and settings which first need to be considered.

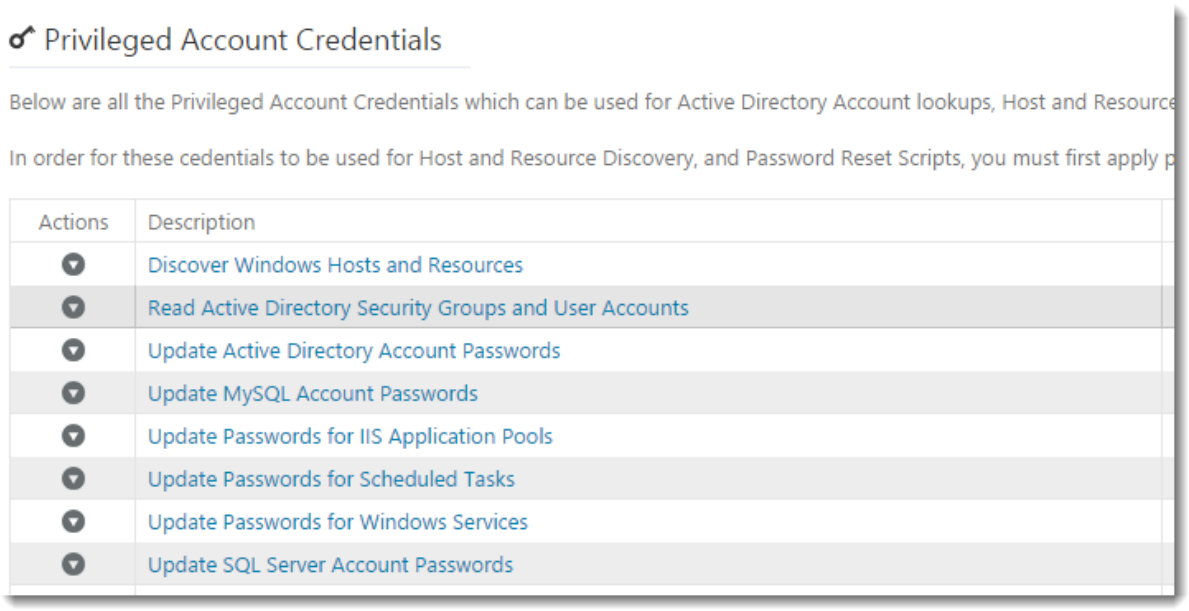
Privileged Account Credential

For Passwordstate to be able update passwords in Active Directory, it needs to use a domain account with elevated privileges to do so.

The first step is to go to the screen Administration -> Privileged Account Credentials, and either update the record 'Update Active Directory Account Passwords', or create your own

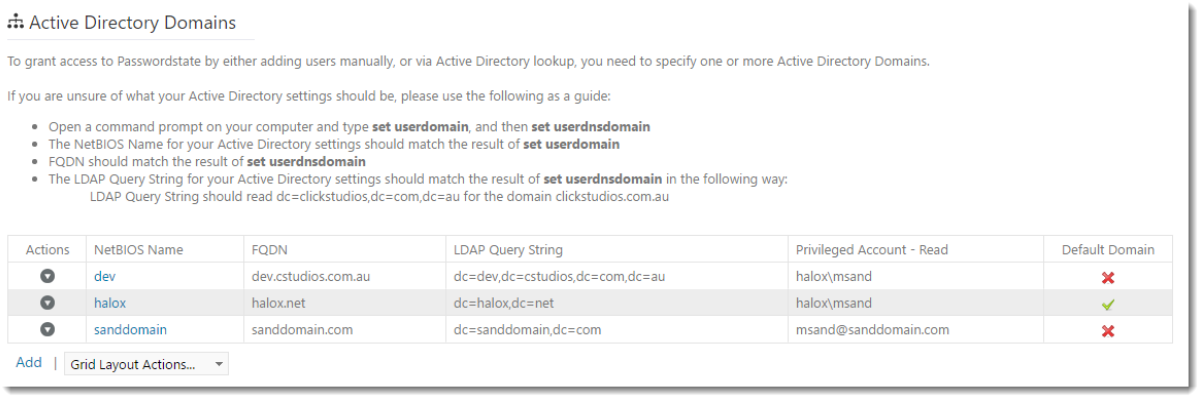
Note: This account must have Account Operator rights when changing passwords on the domain (if you need to change passwords for accounts which have Domain Admin rights, then the account you specify may also need Domain Admin rights, depending on how permissions on your domain have been restricted by your AD Administrators)

© 2017 Click Studios (SA) Pty Ltd



Add Appropriate Domains to the Active Directory Domains Screen

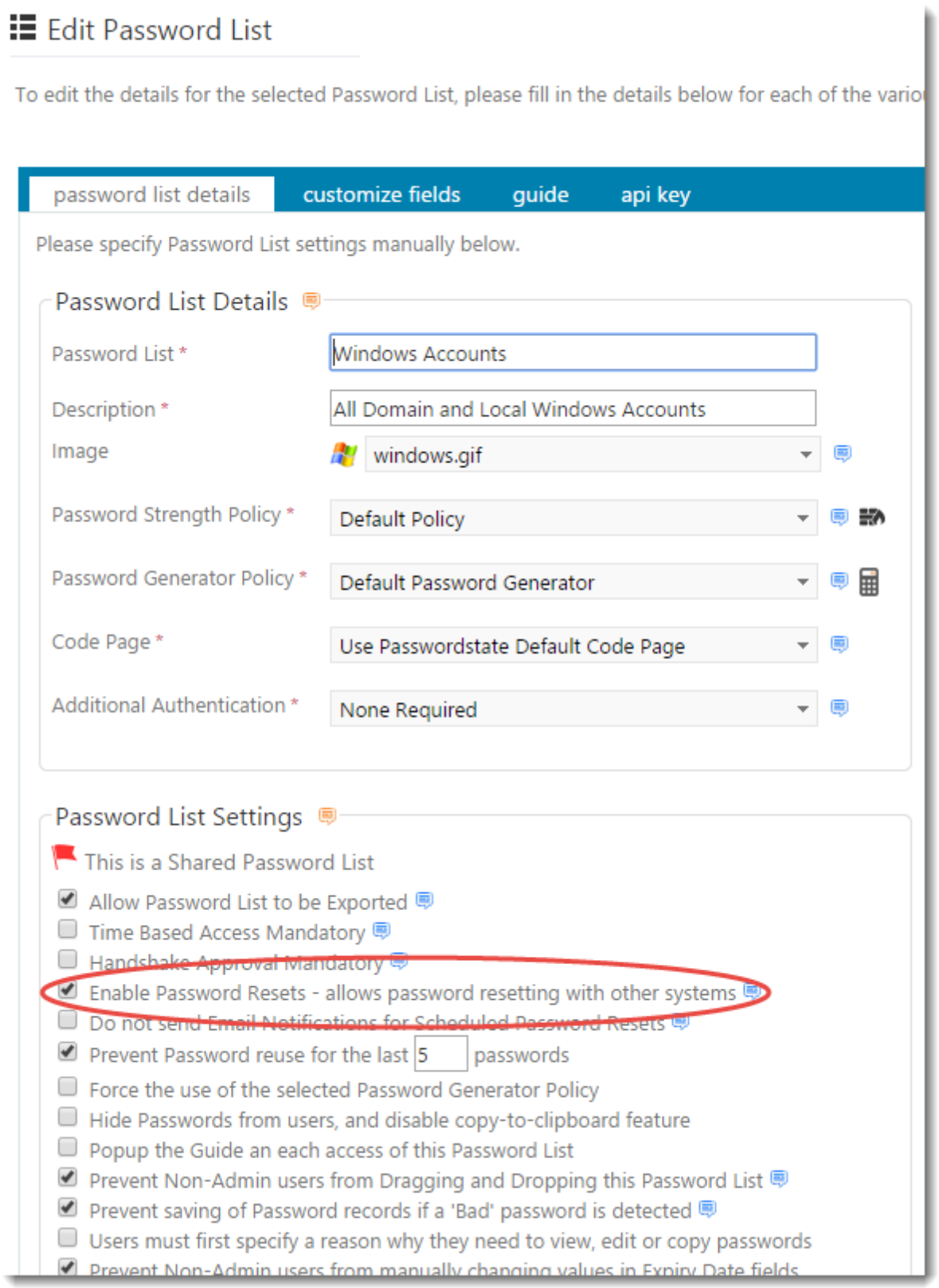
By default, you should already have one Active Directory Domain added to the screen Administration -> Active Directory Domains. If you want to synchronize password changes with other domains which aren't listed, then you must add them to this screen.



Configure a Password List for Password Resets

Now that all the permissions should be correct, we need to configure a Password List so that it is enabled for Password Resets. To do this you need to check the option 'Enable Password Resets'. Clicking this option will also select the 'UserName' and 'Account Type' fields on the 'Customize Fields' tab.

© 2017 Click Studios (SA) Pty Ltd



© 2017 Click Studios (SA) Pty Ltd

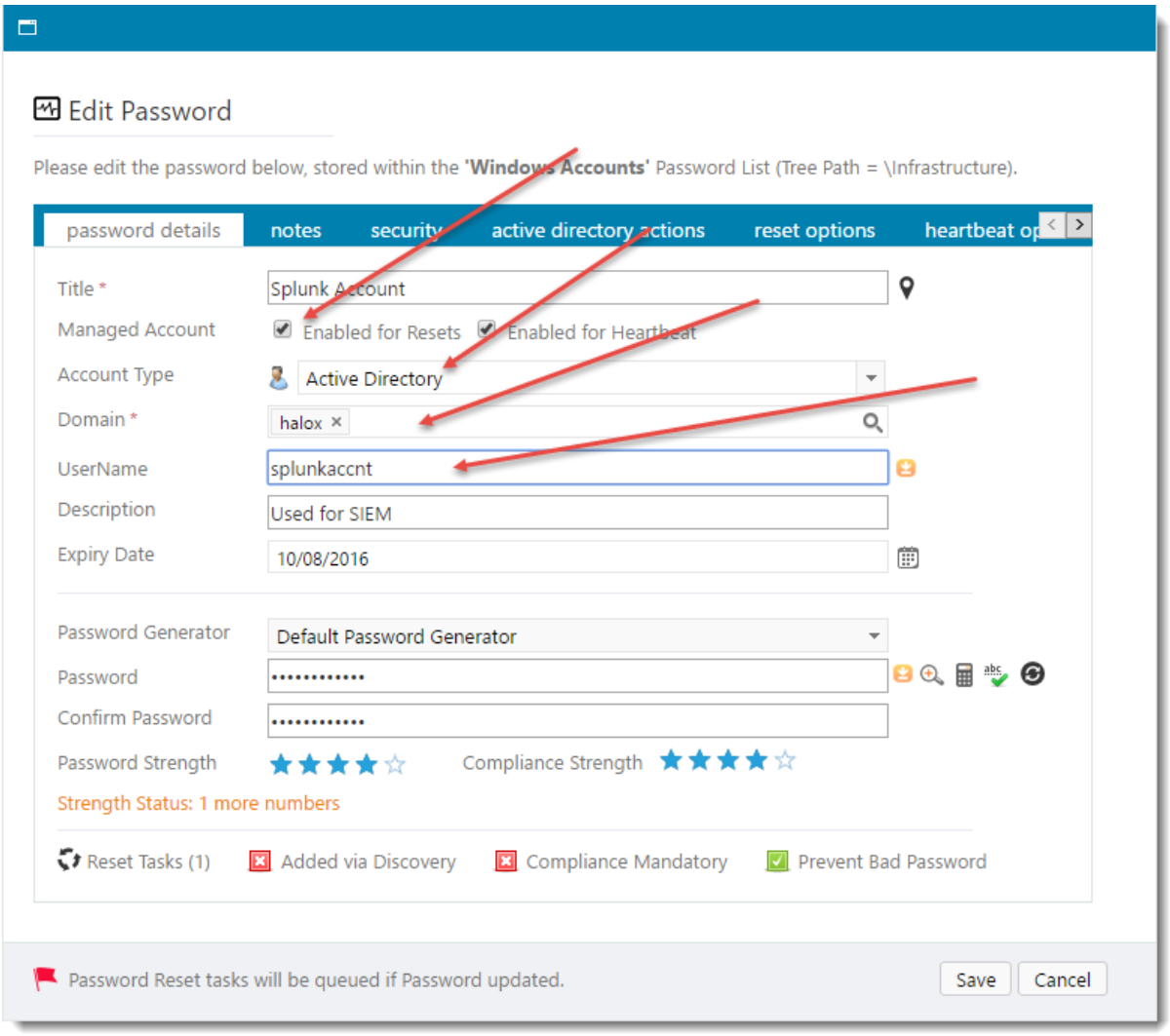
Configure a Password for Password Resets

The last thing required for configuring a password for Password Resets is:

- Enable the option to perform Password Resets
- Select the 'Active Directory' **Account Type**
- Select the appropriate Domain by searching for it
- Specify the **Username** of the account this can be specified in the Pre-Windows 2000 format of Username, or the UPN format of Username@Domain.com (pre-windows is preferred if possible)
- On the Reset Options tab, you must also select a Privileged Account Credential with sufficient permissions to reset the password for the AD Account.

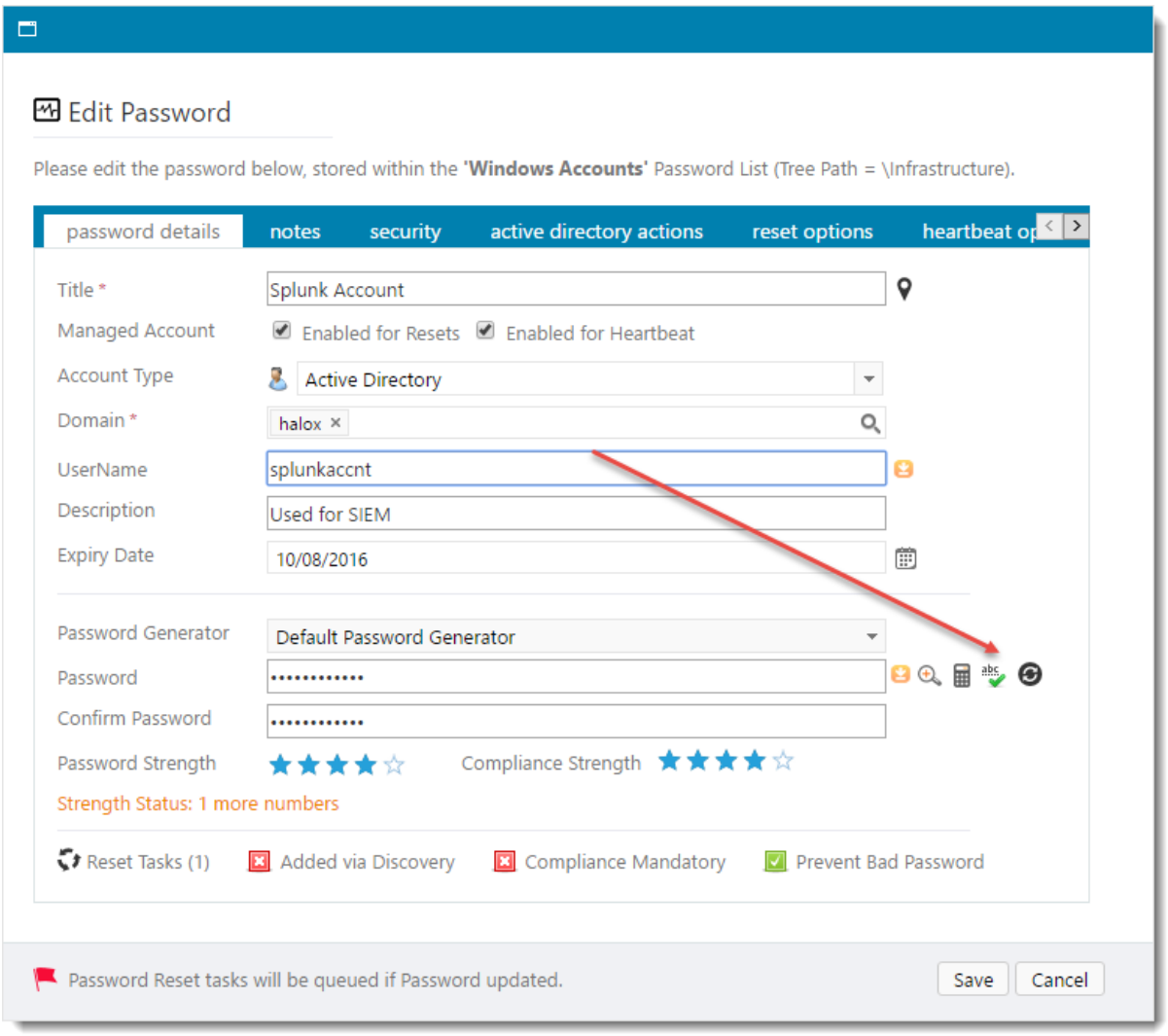
Note : If you edit a record such as this, but don't change the actual value of the password, then the account in Active Directory is not updated.

© 2017 Click Studios (SA) Pty Ltd



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.

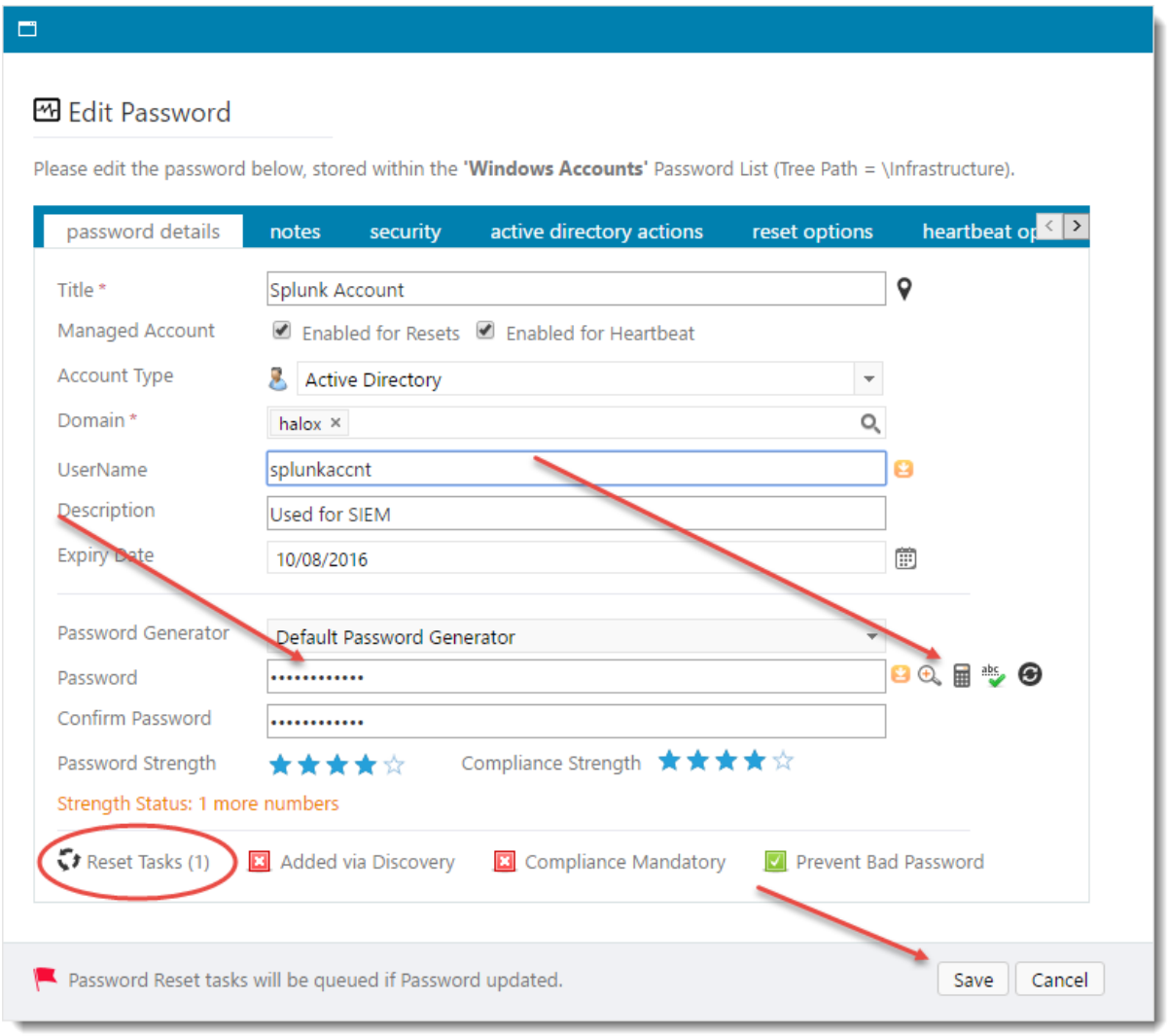
© 2017 Click Studios (SA) Pty Ltd



Manual Resets

It is possible to perform a manual reset for an Active Directory account, as well as scheduled resets. To perform a Manual Reset, you simply need to manually change the value of the password, or use the Password Generator, and then click the 'Save' button. This will update the password in Passwordstate, and AD, and will also trigger resets for any other related Password Reset Tasks i.e. Scheduled Tasks, Windows Services, etc. If there are other related reset tasks (dependencies), it is recommended you instead use a schedule to reset the passwords, as manual resets may interfere with other application/business systems while users are trying to use them.

© 2017 Click Studios (SA) Pty Ltd



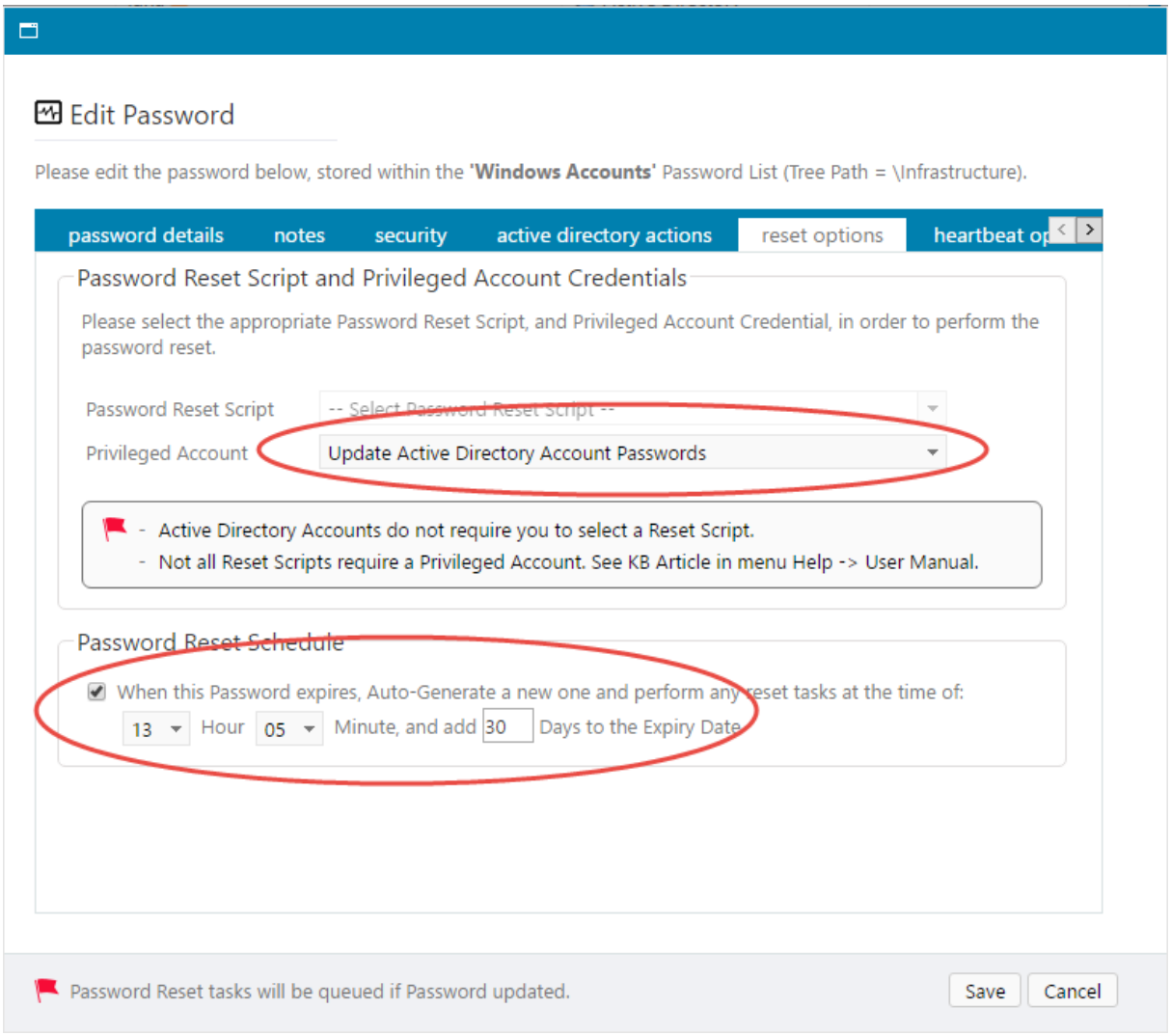
Scheduled Resets

In order to configure Scheduled Resets, two things are required - setting the day, and the time of the day the reset is to occur i.e.

- You must specify the 'Expiry Date' for the record (on the Password Details tab) - this is the day you wish the account to be reset
- On the 'Reset Options' tab for the password record, you must check the option to enable the Schedule, and specify what time of day the reset will occur

Note: If a Scheduled reset was to fail for any reason, no changes will be made to the password record, and the Expiry Date field will not be updated. By not updating the Expiry Date field, another attempted reset will occur at the same time the following day.

© 2017 Click Studios (SA) Pty Ltd



Password Reset Queuing System

When the value of the password is changed for an account, either manually or via a schedule, the account is added to a queuing system to perform the reset.

For information in the queuing system, please refer to this section of the manual - Password Reset Queuing System

9.8.4 Password Reset Example

The following documentation describes basic steps for configuring a Password record to perform resets. The example below is for resetting a Linux account, but the process is similar for all types of accounts.

© 2017 Click Studios (SA) Pty Ltd

Note: The process below is the manual method for configuring Password Resets, but there is also an automated method for certain Windows accounts using our Discovery feature. More information on Discovery can be found here - Hosts and Resource Discovery

Step 1 - Prerequisites

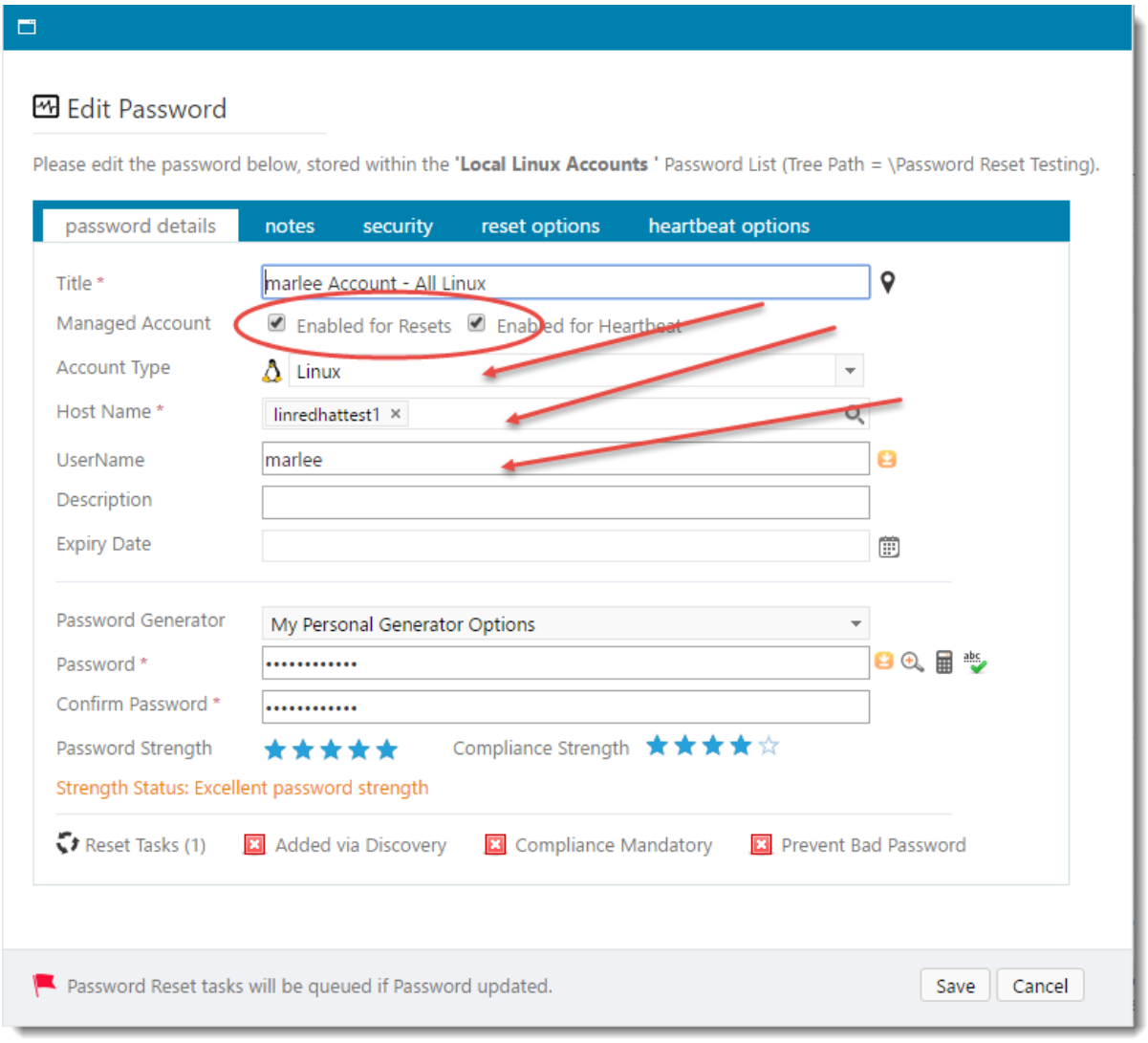
- Please refer to the following KB article as guidance for Password Reset requirements - Password Reset Scripts and Requirements

Step 2 - Password Details Tab

To configure an account for Password Resets, there are various options and fields on the Password Details tab which need to be selected/specified, and they are:

- Enable the option to perform Password Resets, and Account Heartbeat
- Select an appropriate Account Type - depending on which Account Type you select, a Password Validation Script will automatically be selected for you on the 'Heartbeat Options' tab
- Select the appropriate Host Name by searching for it
- Specify the Username for the account
- Specify an Expiry Date if you want scheduled resets
- And of course, the value of the password for the account

© 2017 Click Studios (SA) Pty Ltd

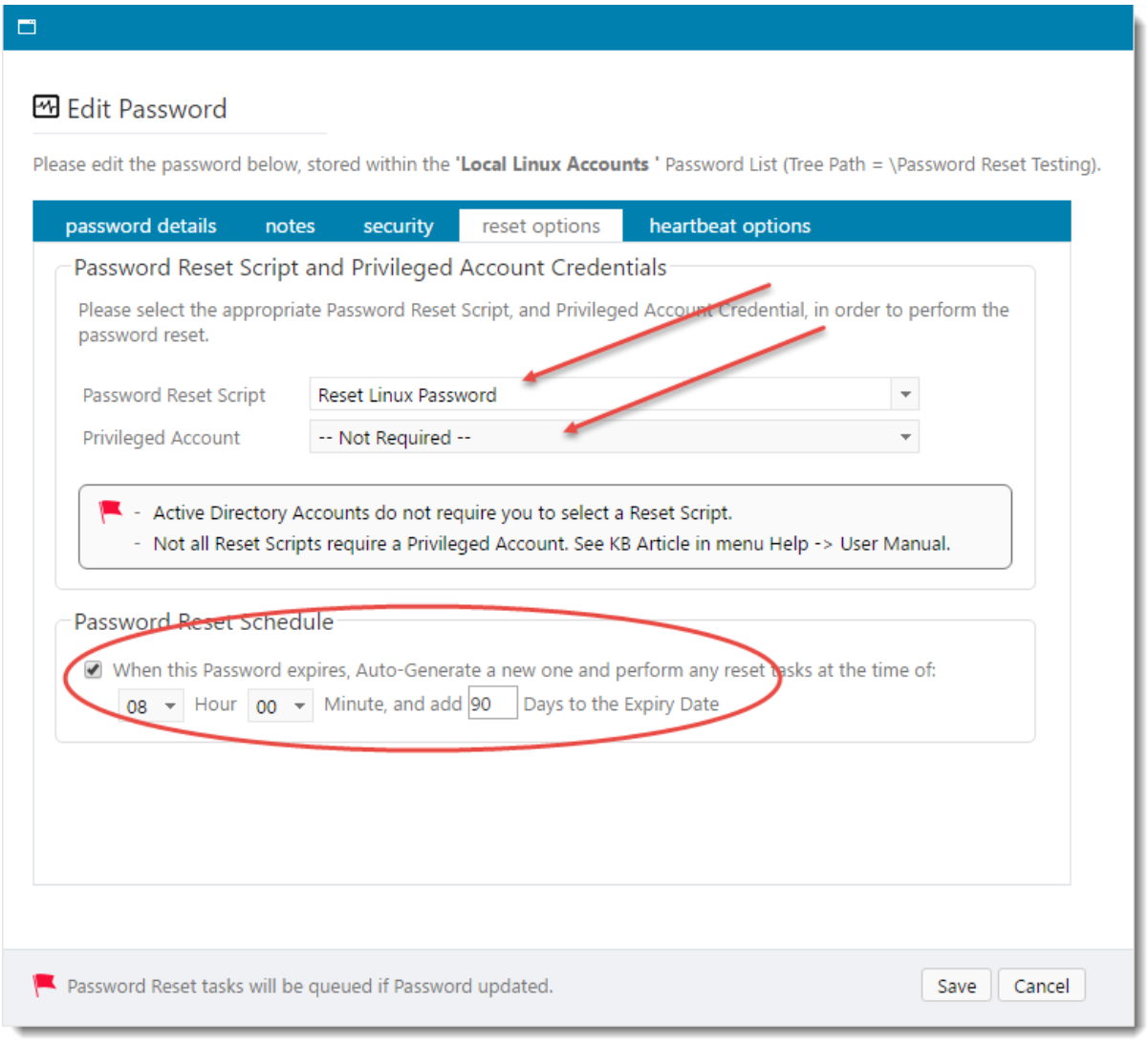


Step 3 - Reset Options Tab

In order to perform Password Resets for this account, you also need to select the appropriate Password Reset script, and possible an appropriate Privileged Account Credential to connect to the Host to perform the reset. Not all Password Resets require the use of a Privileged Account, and please refer to following page to determine if one is required or not - Password Reset Scripts and Requirements

If you want to enabled scheduled resets as well, you enable the option and set the time of day as appropriate. The schedule is based on this time, and also the date of the Expiry Date field.

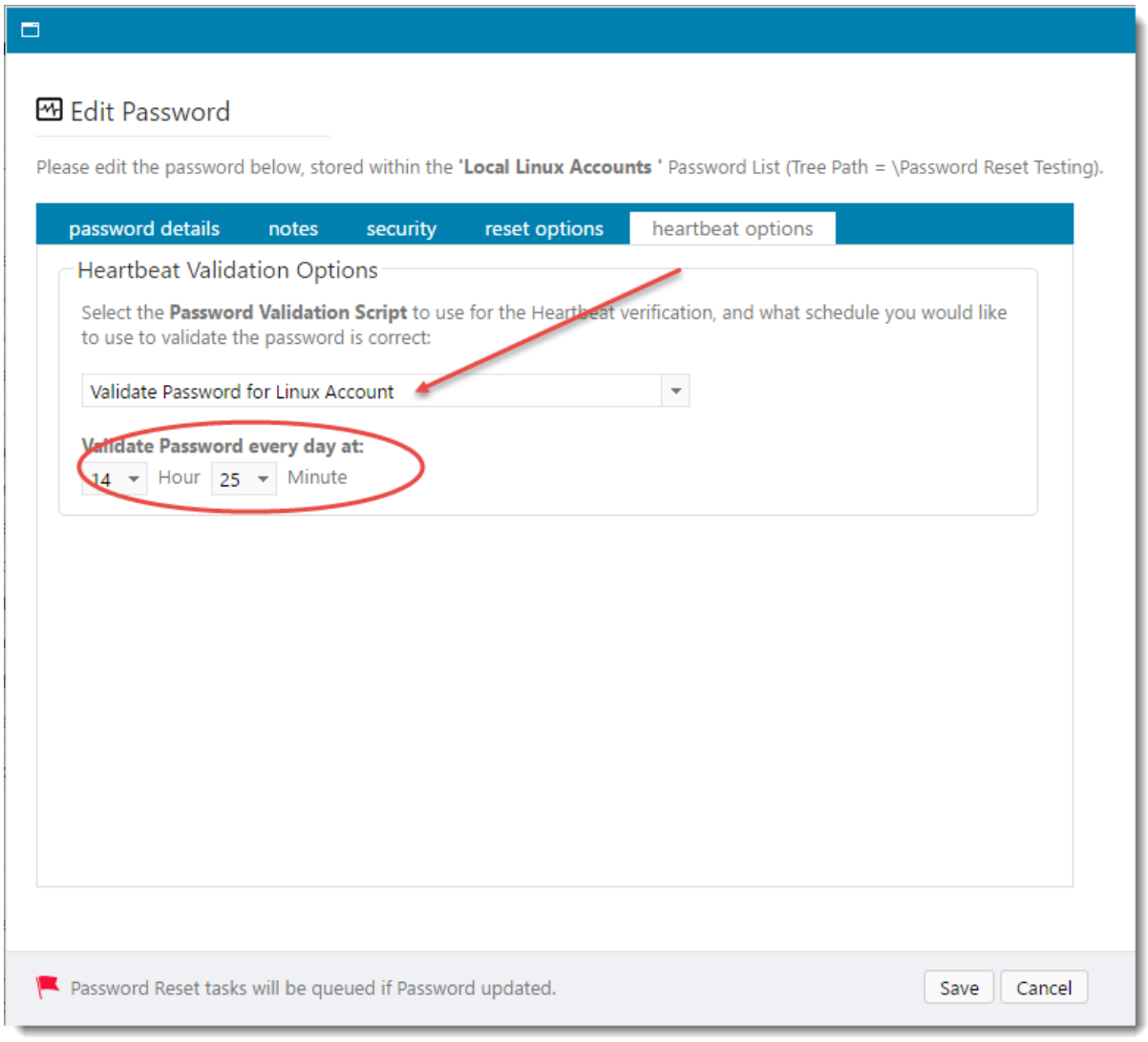
© 2017 Click Studios (SA) Pty Ltd



Step 4 - Heartbeat Options Tab

By Selecting a Password Validation script, and setting a schedule, Passwordstate can validate once a day if the passwords are in sync - this process is called Account Heartbeat

© 2017 Click Studios (SA) Pty Ltd



Step 5 - Password Reset Queuing System

When the value of the password is changed for an account, either manually or via a schedule, the account is added to a queuing system to perform the reset.

For information in the queuing system, please refer to this section of the manual - Password Reset Queuing System

9.8.5 Password Reset Queuing System

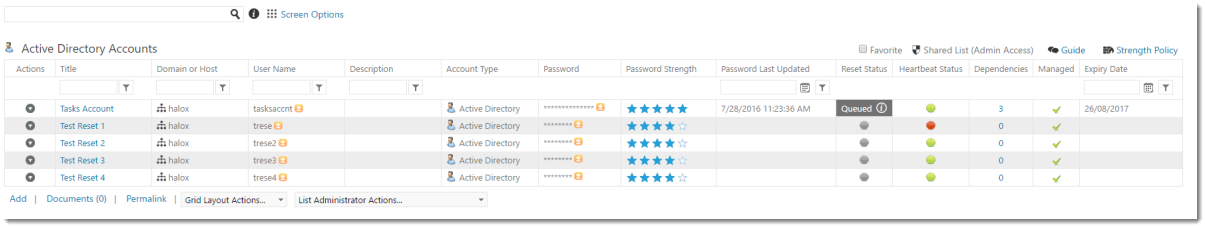
There are various conditions in which a password reset can be triggered, and they are:

1. Someone manually changes the value of the password on the Edit Password screen

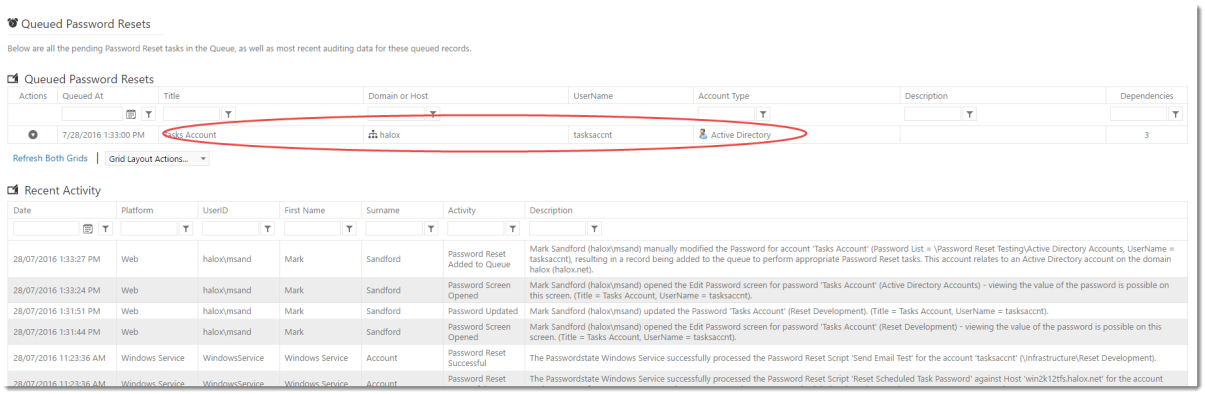
© 2017 Click Studios (SA) Pty Ltd

2. When someone manually updates the value of the password via the API
3. A Scheduled reset occurs
4. The 'Change Password On Check In' option is selected for a record, for the Check In/Check Out feature
5. When the option to reset a password is selected for Time Based Access permissions to individual password records

When any of the above events are triggered, the password record is added to a queue to perform the reset. No changes will be made to the password record itself, until the queued record has finished processing. In the Passwords grid, it will show the record is queued, and clicking on the white Information icon, will filtering the auditing records for you for this account.



If needed, you can also monitor the status of all queued records to all Password Lists you have access to on the screen Resets -> Queued Password Resets, as per the screenshot below. This will also show auditing data for all the queued records you see on his screen.



9.8.6 Password Reset Dependency Records

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

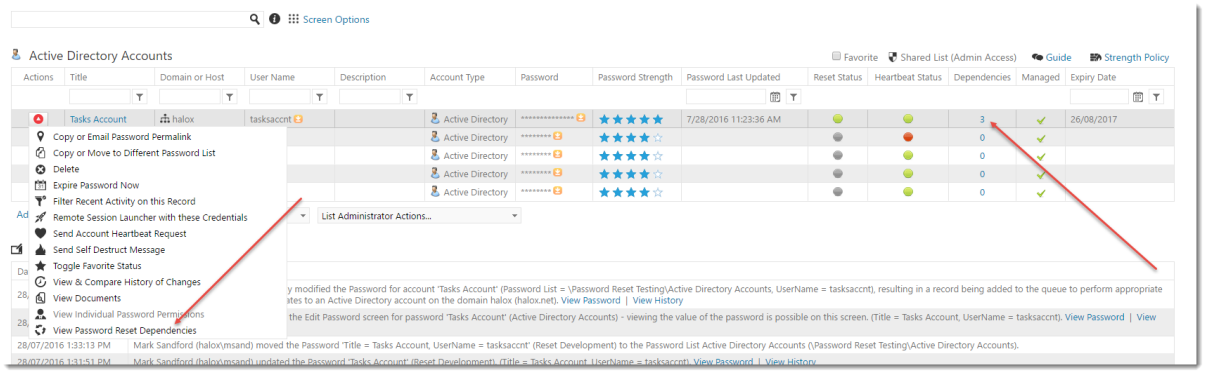
A typical example of this would be where the account is an Active Directory account, and it's being used as the "identity" for operations of Windows Services, Scheduled Tasks, IIS Application Pools or COM+ Components. It is also possible to automate account discovery, and these dependencies as well -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

It is also possible to execute any custom type of PowerShell script you want as well, and the script

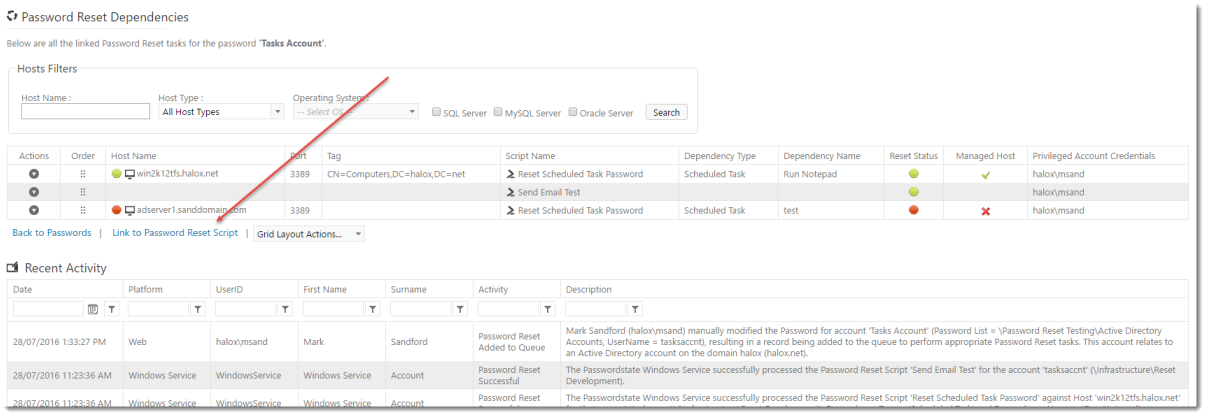
© 2017 Click Studios (SA) Pty Ltd

does not necessarily have to be associated with a Host record.

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



Then you click on the 'Link to Password Reset Script' button.



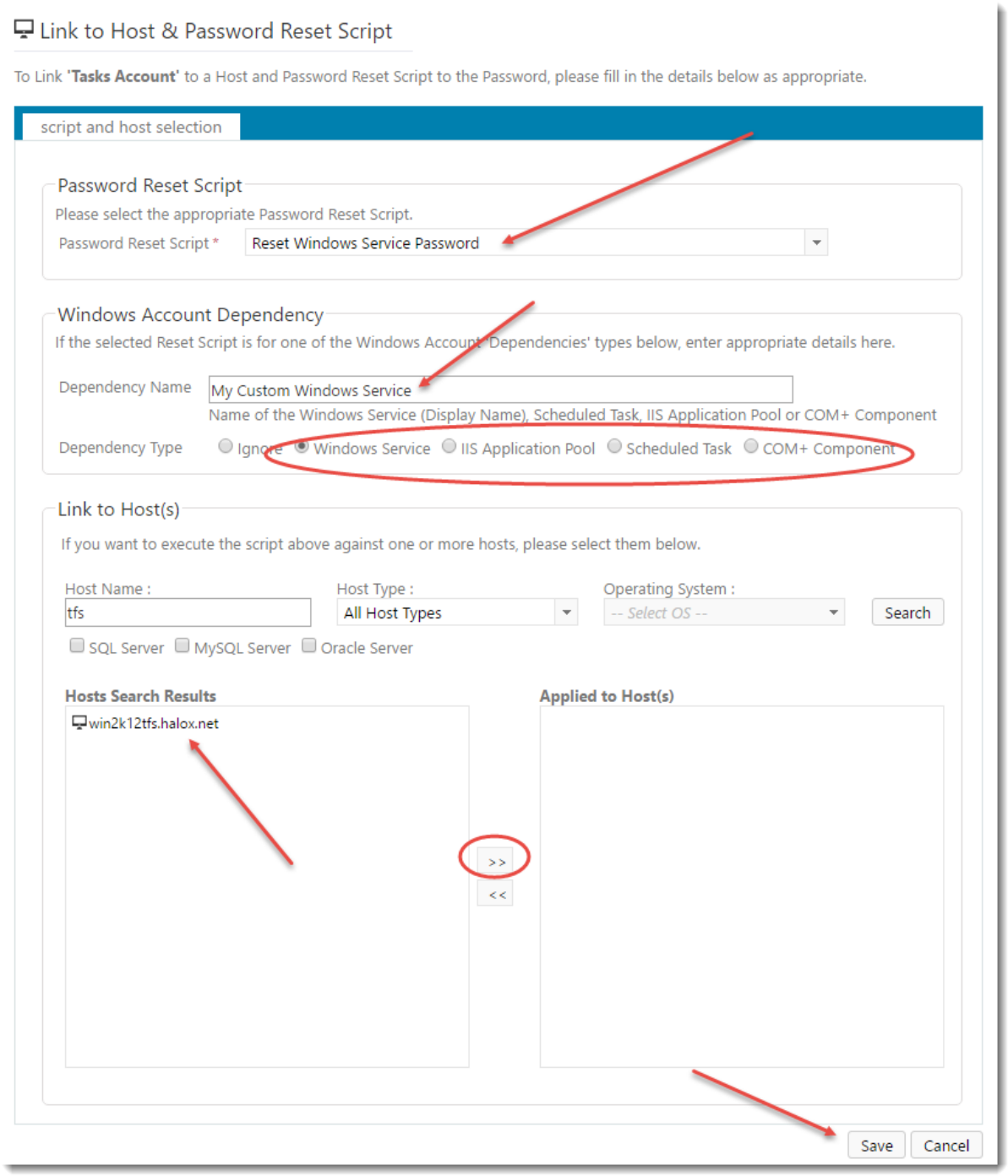
And then select the following options as appropriate:

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

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

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

© 2017 Click Studios (SA) Pty Ltd



9.8.7 Known Errors

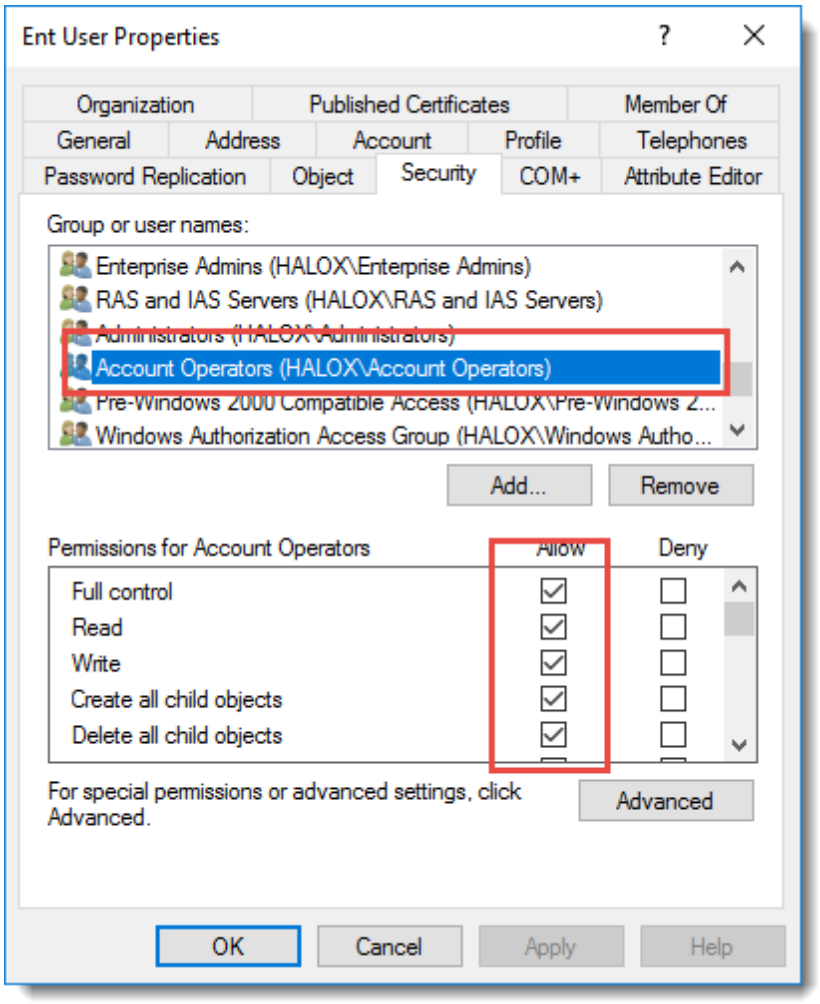
This KB Article provides feedback on certain error types which may be experienced during performing Password Resets.

Any failed resets should have sufficient auditing data to inform you of the issue, whereas this article will provider greater detail to assist with troubleshooting.

© 2017 Click Studios (SA) Pty Ltd

Active Directory Accounts

Error: "It appears the Privileged Account Credential being used for this reset does not have sufficient privileges to change the password"
Cause: This error indicates the account being reset may not have appropriate access rights for the Privileged Account on it's Security tab. As an example, if the Privileged Account is in the 'Account Operators' security group, you should also have the 'Account Operators' on the Security tab as per the screenshot below.



9.9 Passwordstate Disaster Recovery

The following topics in this KB Article describe how to restore your Passwordstate environment in the event of a disaster.

Disaster Recover Process	Description
Passwordstate Web Site Restore	Reinstall the Passwordstate Web Site
Passwordstate Database Restore	Restore a copy of your database
Rebuilding the Web.config File	Rebuild the settings in the web.config file if required

© 2017 Click Studios (SA) Pty Ltd

Resetting Password for Passwordstate_User SQL Account	Resetting the password for the SQL Account passwordstate_user
Recovery Emergency Access Password	Recover your Emergency Access Password, if needed, to resolve Unauthorized Web Server message

9.9.1 Passwordstate Web Site Restore

It is recommended during a Disaster event, you reinstall the same build of Passwordstate you are currently using prior to the disaster. This makes the restoration process a little simpler, as you do not need to be concerned with upgrading your database at the same time if installing a later build.

All previous builds of Passwordstate can be downloaded from the following URL - https://www.clickstudios.com.au/previous-builds.html

To re-install Passwordstate, you need to follow these steps:

- Unzip the Passwordstate.zip file from your download above
- Use the following document as a guide for reinstalling the software - https://www.clickstudios.com.au/downloads/version7/Installation_Instructions.pdf
- Before you open your browser and point it at the site for the first time, you need to restore a copy of your web.config file over the top of the existing file which exists in the folder c:\inetpub\passwordstate. If you do not have a backup of this file, then please follow these instructions for rebuilding this file with the correct configuration settings - Rebuilding the Web.config File. Note: if you are using the Backup feature in Passwordstate, the web.config file will be backed up and stored in your backup zip file
- If you also need to restore a copy of your database, then follow these instructions - Passwordstate Database Restore
- Now when you open your browser and navigate to the Passwordstate web site, you may see a screen which indicates that your new web server is "Not Authorised" to host the Passwordstate web site. This will occur if your server name has changed, or if you did not have a backup of your web.config file to use above. To fix this issue, you can simple enter your Emergency Access login password. If you have forgotten this password, please follow these instructions for contacted Click Studios so we can help you recovery it - Recovery Emergency Access Password

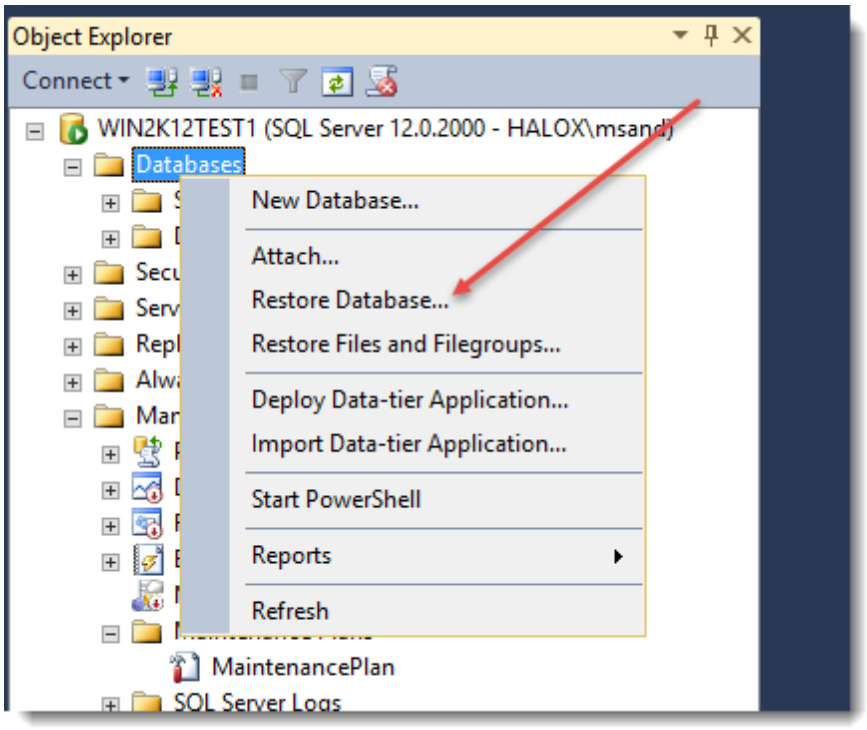
This should be all that is required to restore your Passwordstate environment.

9.9.2 Passwordstate Database Restore

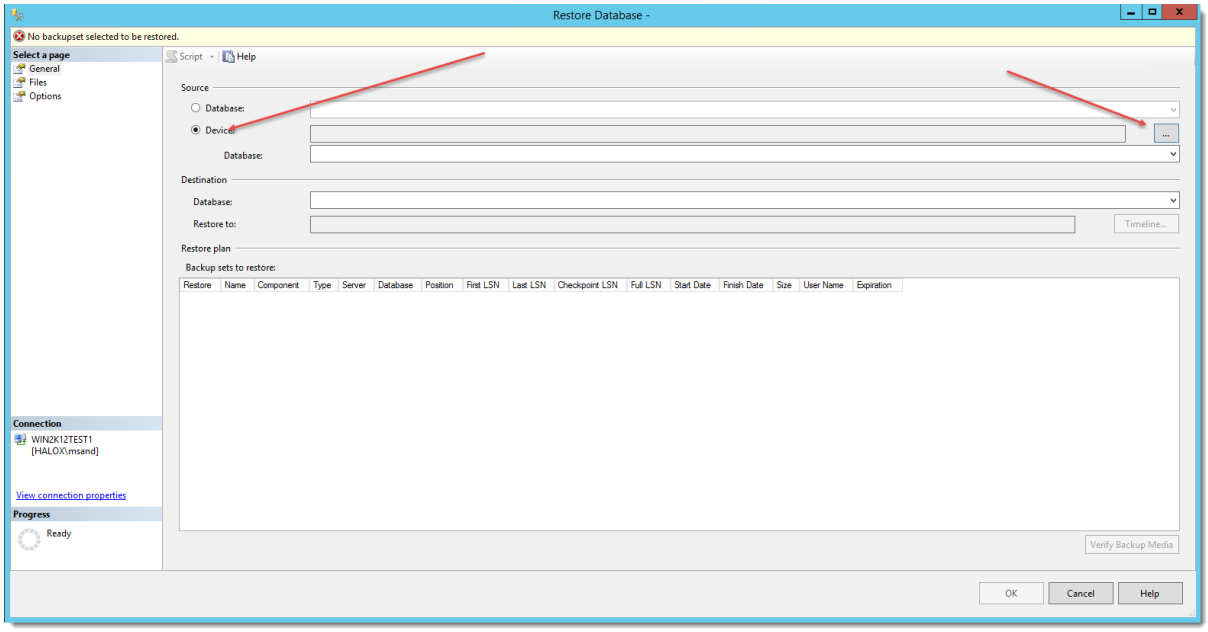
To restore a copy of your database, please follow these instructions:

- Start SQL Server Management Studio
- Right click on 'Databases' and select 'Restore Database...'

© 2017 Click Studios (SA) Pty Ltd

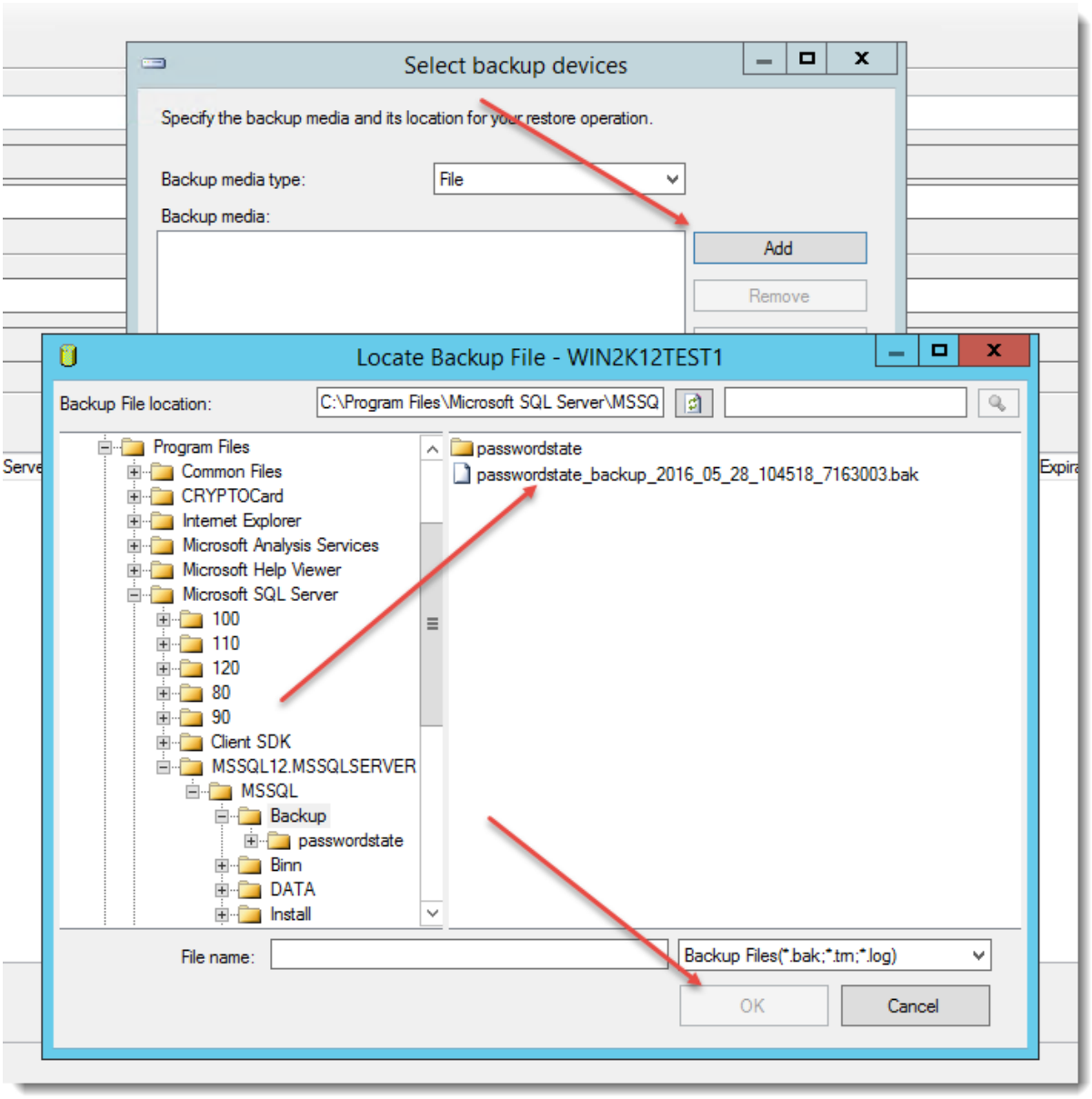


- Click on 'Device', and then on the Ellipsis button so you can select your database backup file



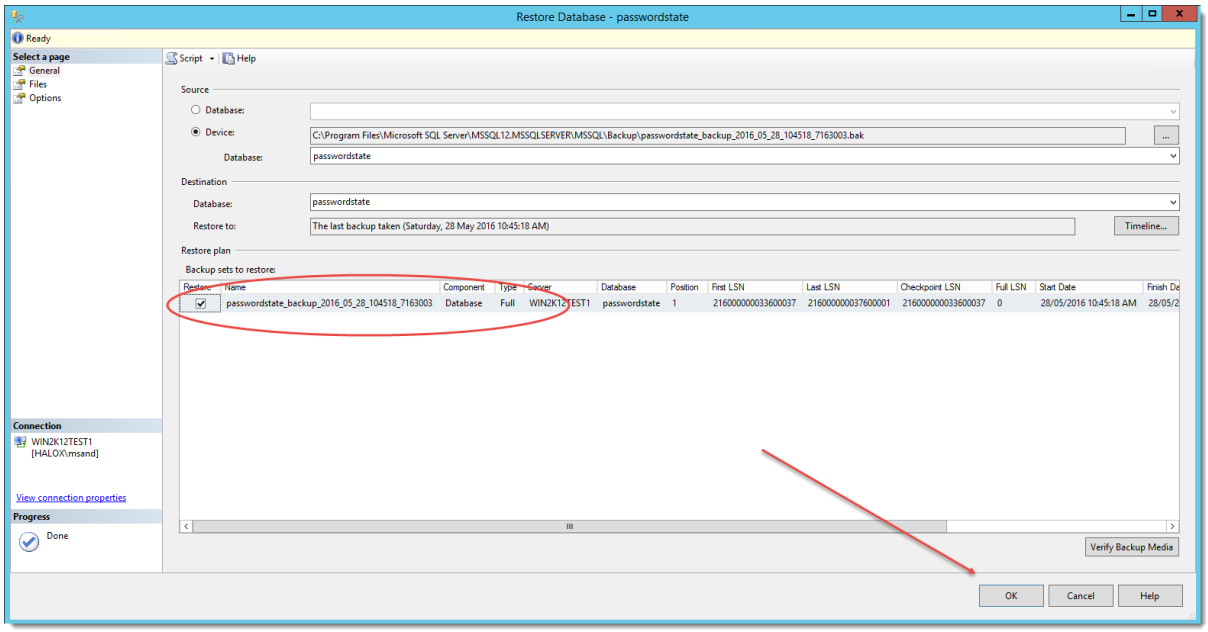
- Click on the 'Add' button and browse and select the location of your latest .bak file

© 2017 Click Studios (SA) Pty Ltd



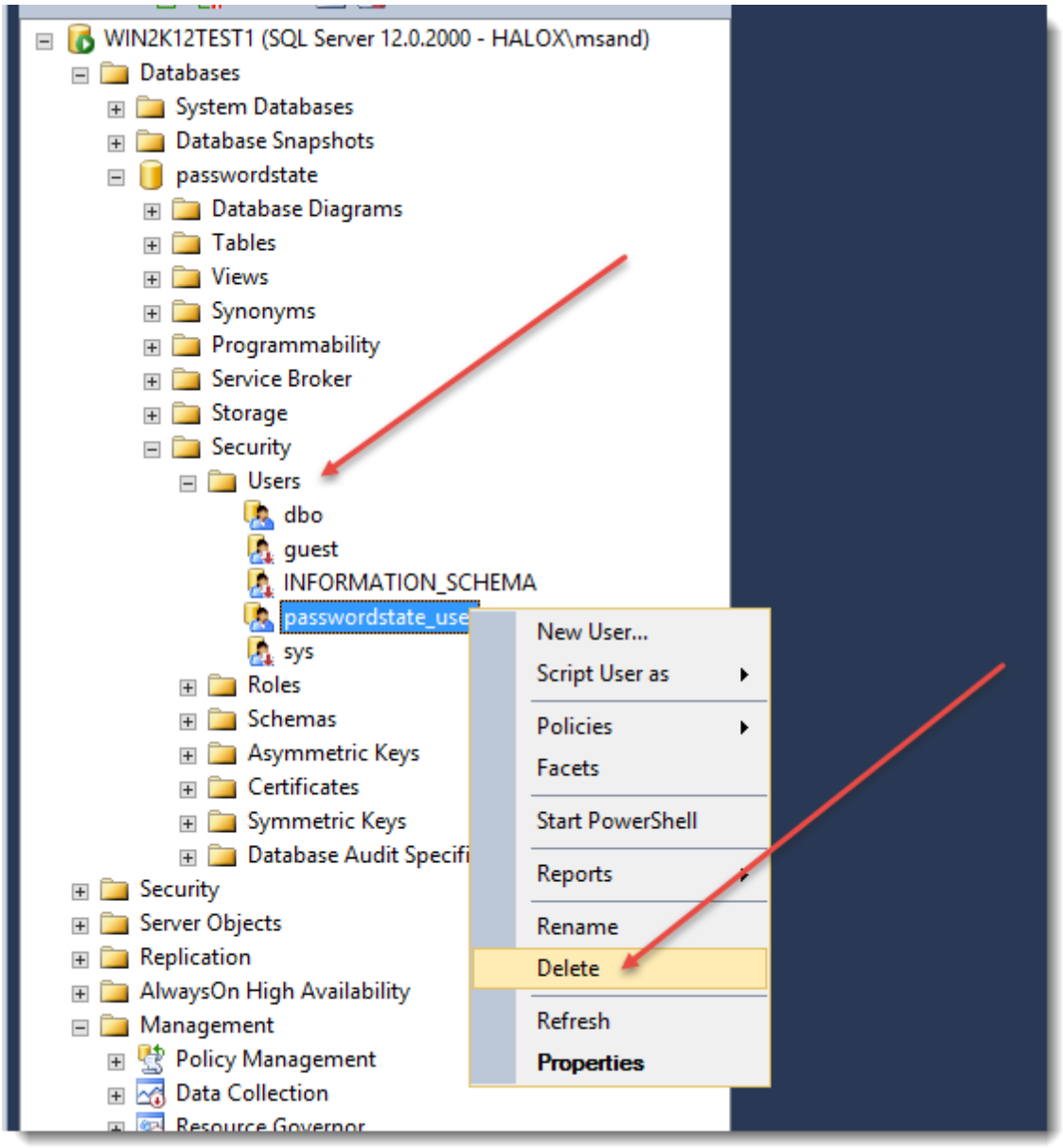
- Once the database is selected as per the screenshot below, click the 'OK' button to restore it

© 2017 Click Studios (SA) Pty Ltd



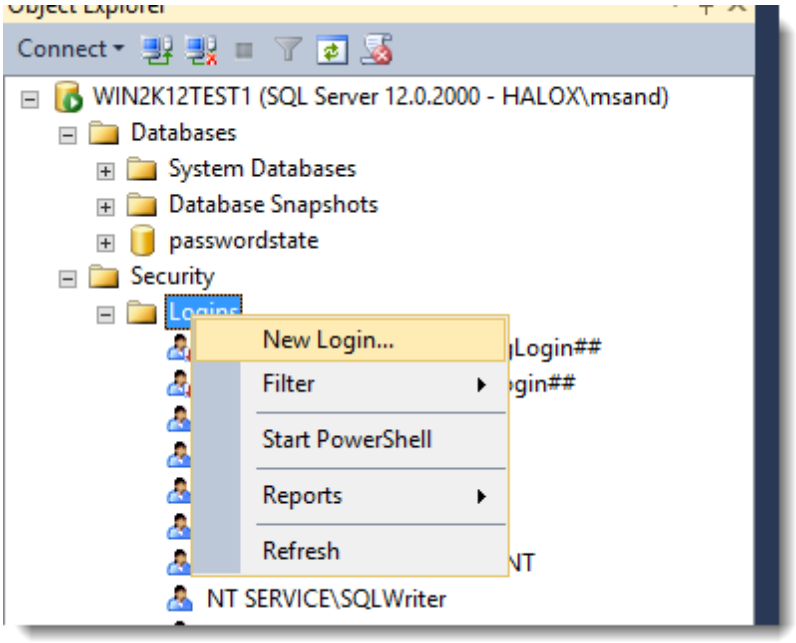
- Now expand the Security -> Users tree within the Passwordstate database, and delete the 'passwordstate_user' SQL Account

© 2017 Click Studios (SA) Pty Ltd

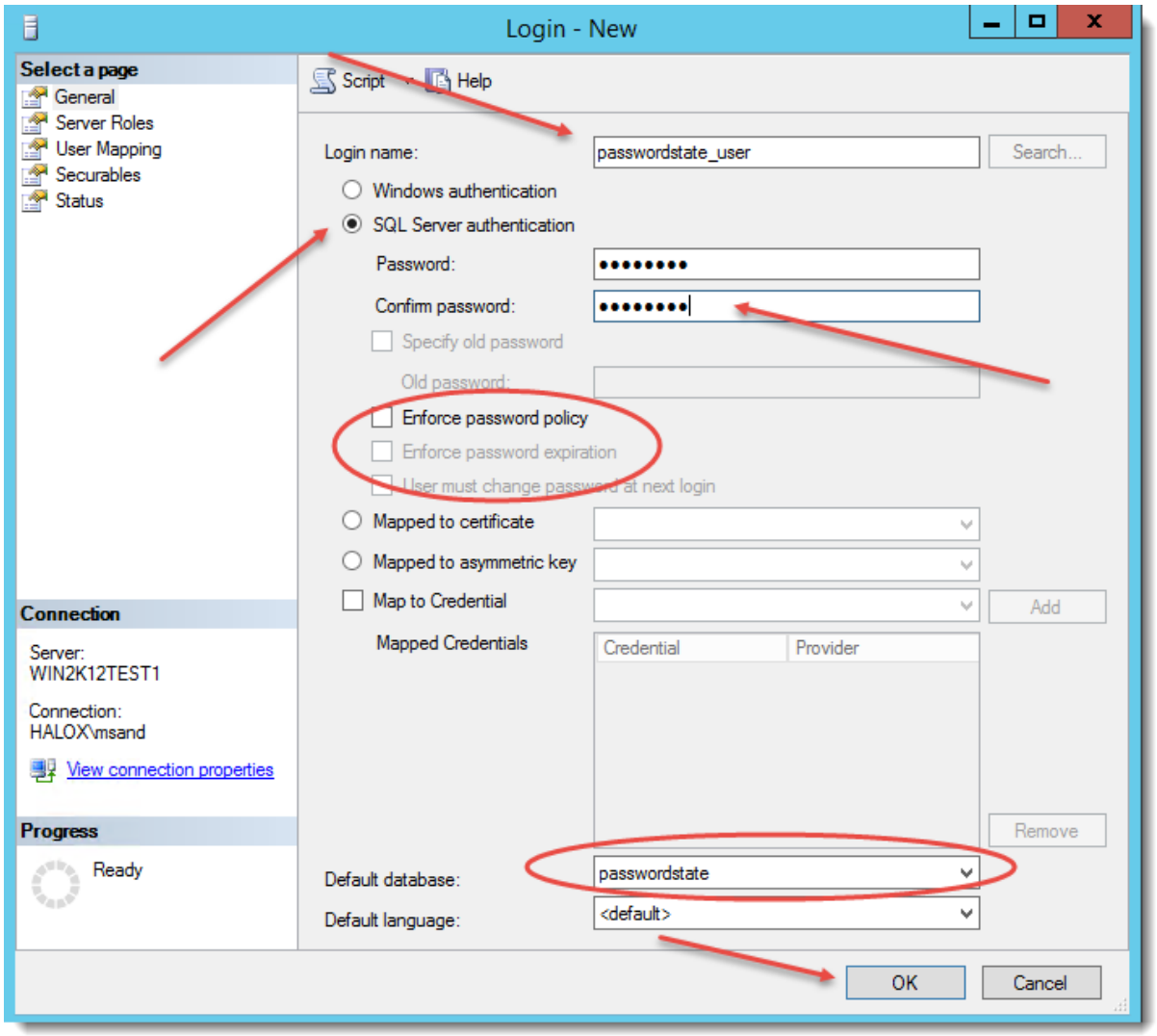


- Now expand the Security -> Logins tree. If you do not see the 'passwordstate_user' SQL Account, follow the next set of instructions for creating it. If it does exist, simply skip to the step below where we apply permissions for this account to the Passwordstate database

© 2017 Click Studios (SA) Pty Ltd

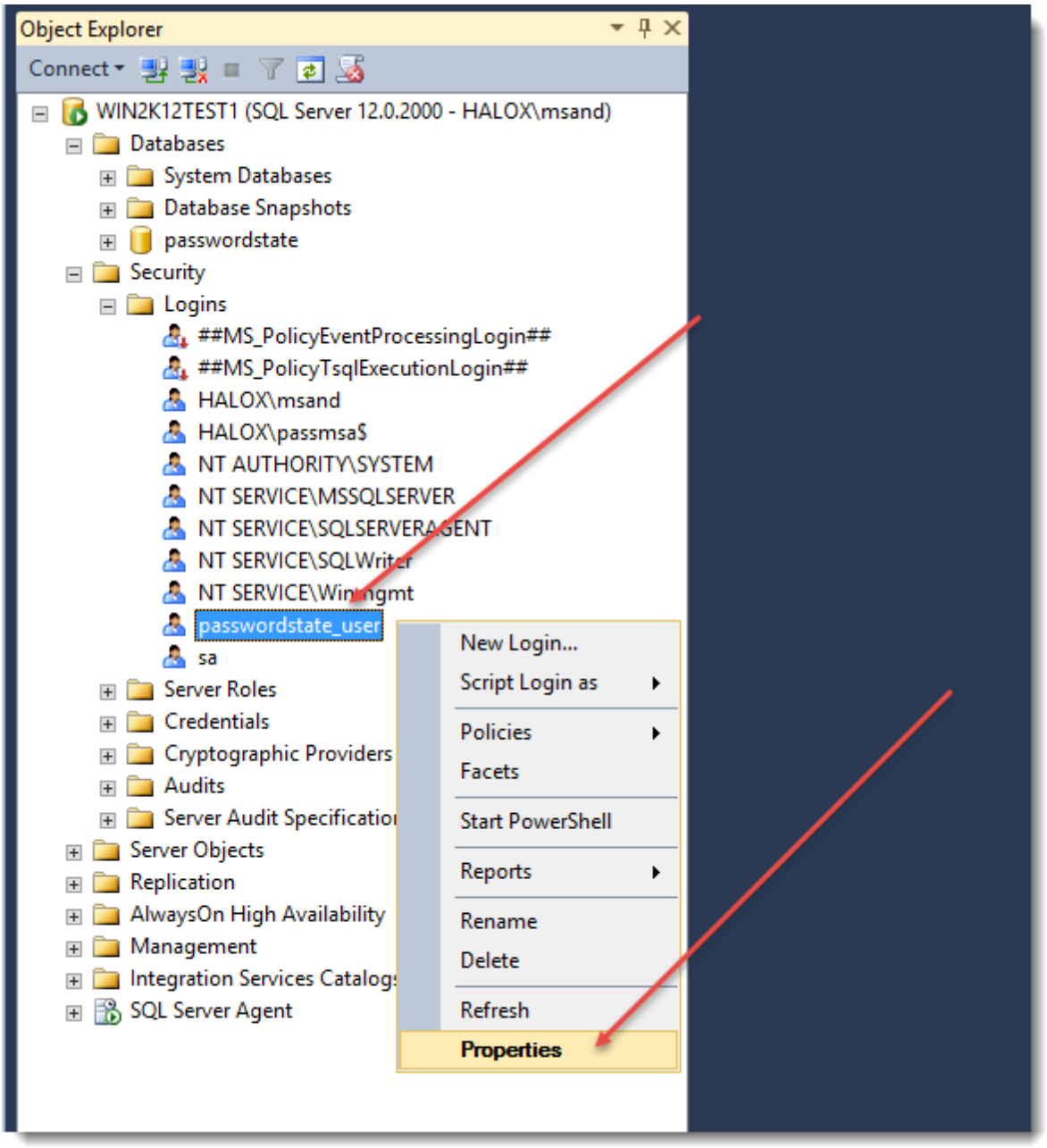


© 2017 Click Studios (SA) Pty Ltd



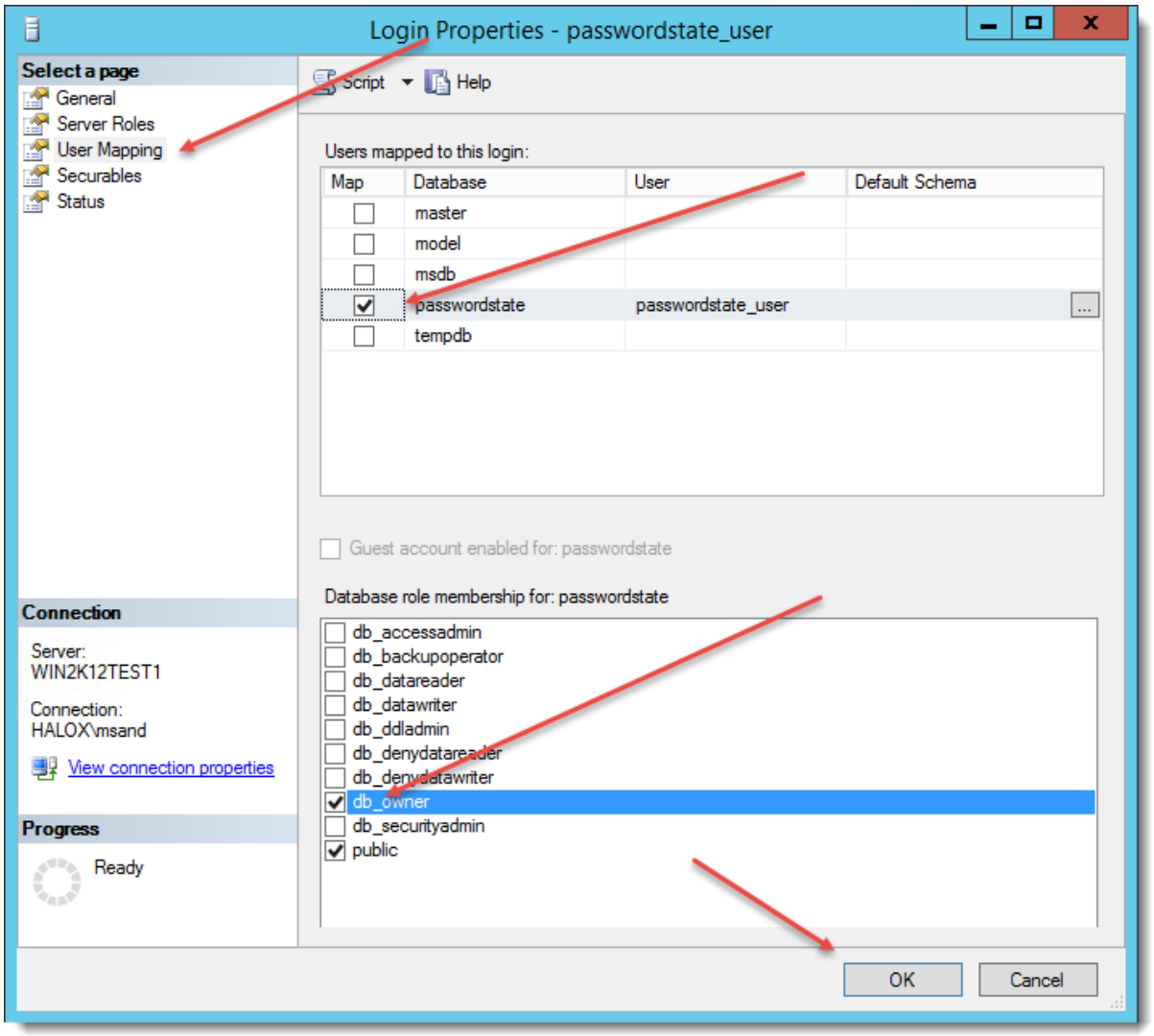
- Now select the 'Properties' menu option for the account

© 2017 Click Studios (SA) Pty Ltd



- And select db_owner rights to the Passwordstate database

© 2017 Click Studios (SA) Pty Ltd



- This is all that's required for restoring your database. As it's likely the password for the account passwordstate_user has changed, you may need to update the value of this password in the database connection string in the web.config file. To do this, simply edit the web.config file as an Administrator, and modify the 'Password' value you see in the screenshot below

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

9.9.3 Rebuilding the Web.config File

This topic will discuss how to take the default web.config file from a new Passwordstate installation, and configure it so the web site can communicate with your existing Passwordstate database. This document should only ever be needed if you have a server crash, and do not have a backup of your web.config file.

© 2017 Click Studios (SA) Pty Ltd

There are 3 areas in the web.config file which need to be modified, and they are:

- The database connection string
- The SetupStage key
- And the Secret1 and Secret2 keys (Note: these secrets are not relevant if you are using a build of Passwordstate prior to 7580 - see section below if you are not sure what build you're currently running)

```
</configSections>
<connectionStrings>
 <add name="PasswordstateConnectionString" connectionString="Data Source=[SERVERNAME];Initial Catalog=passwordstate;User ID=[SQLLOGINNAME];Password=[PASSWORD]" providerName="System.Data.SqlClient"/>
</connectionStrings>
<appSettings>
  <add key="SetupStage" value="Introduction" />
  <add key="PassiveNode" value="False" />
  <add key="Secret1" value="" />
  <add key="Secret2" value="" />
</appSettings>
<system.web>
```

Determine Current Passwordstate Build Number

Using SQL Server Management Studio, make a connection to your database server and execute the following query:

```
USE Passwordstate
SELECT BuildNo FROM [systemSettings]
```

It is in the next section you need to know your Build Number, so you know whether the Secret1 and Secret2 keys are required or not.

Modify Web.Config File

- The following settings need to be updated in the PasswordstateConnectionString
  - Data Source - this is the host name of your database server. If you have a specific Instance Name for you SQL install as well, this will need to be appended i.e. HostName\SQLExpress
  - User ID - this should be passwordstate_user
  - The password for the passwordstate_user SQL account (if you are not sure of what this password would be, there are instructions below on how to reset this)
- The SetupStage key needs to be set to "Setup Complete"
- If you are using Build 7580 or above, you will need to copy the Secret1 and Secret2 values across from the encryption keys which you would have been asked previously to export. Note: if you do not have these secrets, it is not possible to recover your system. If you are using a build earlier than 7580, you must delete these two Secrets from the web.config file if they exist.

Reset Password for Passwordstate_User SQL Account

As you have specified what is most likely a new password for the passwordstate_user SQL Account, you will need to reset this password on your SQL Server. To do this, please follow these instructions - Resetting Password for Passwordstate_User SQL Account

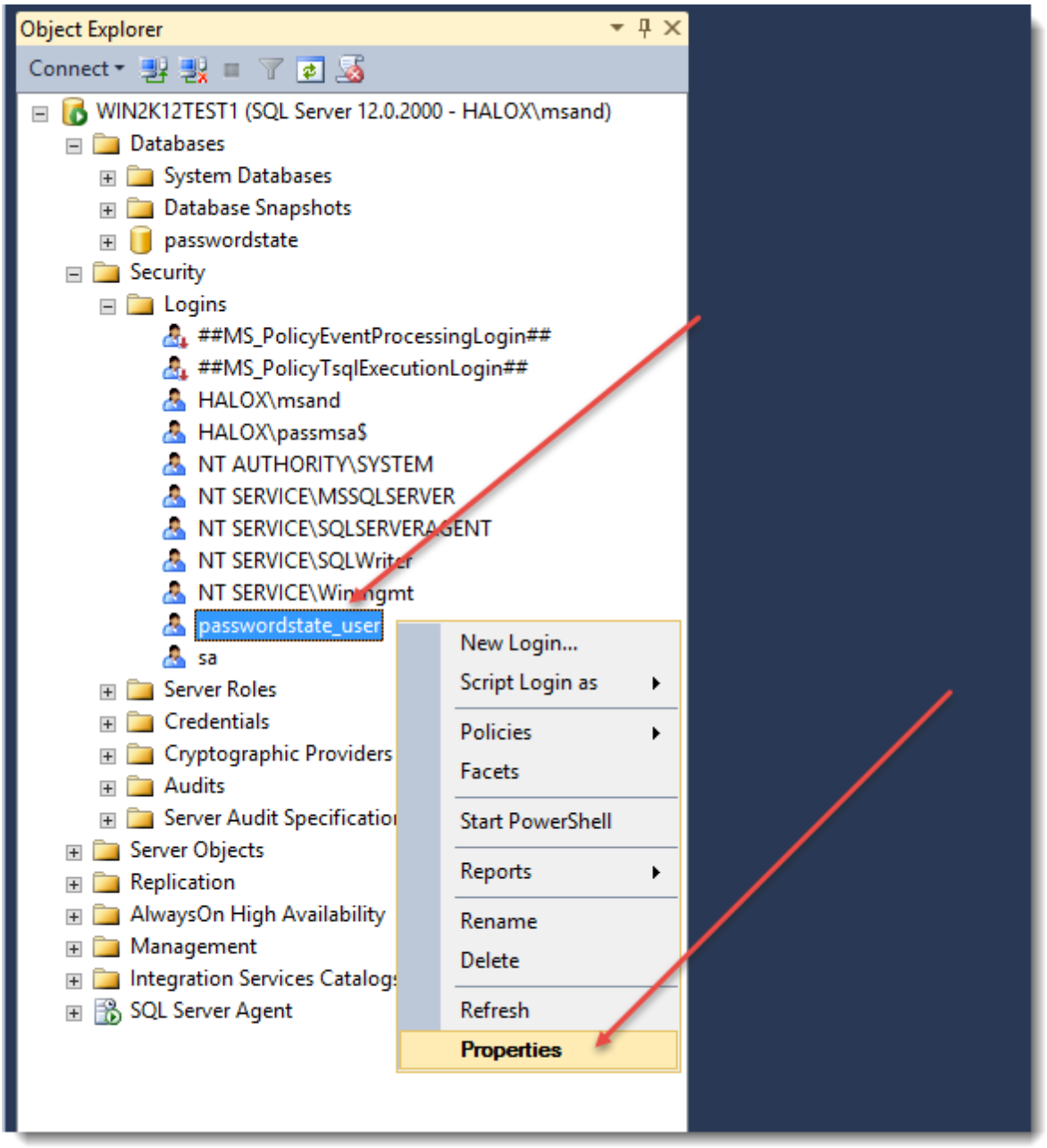
9.9.4 Resetting Password for Passwordstate_User SQL Account

To reset the password for the passwordstate_user SQL Account, please follow these instructions:

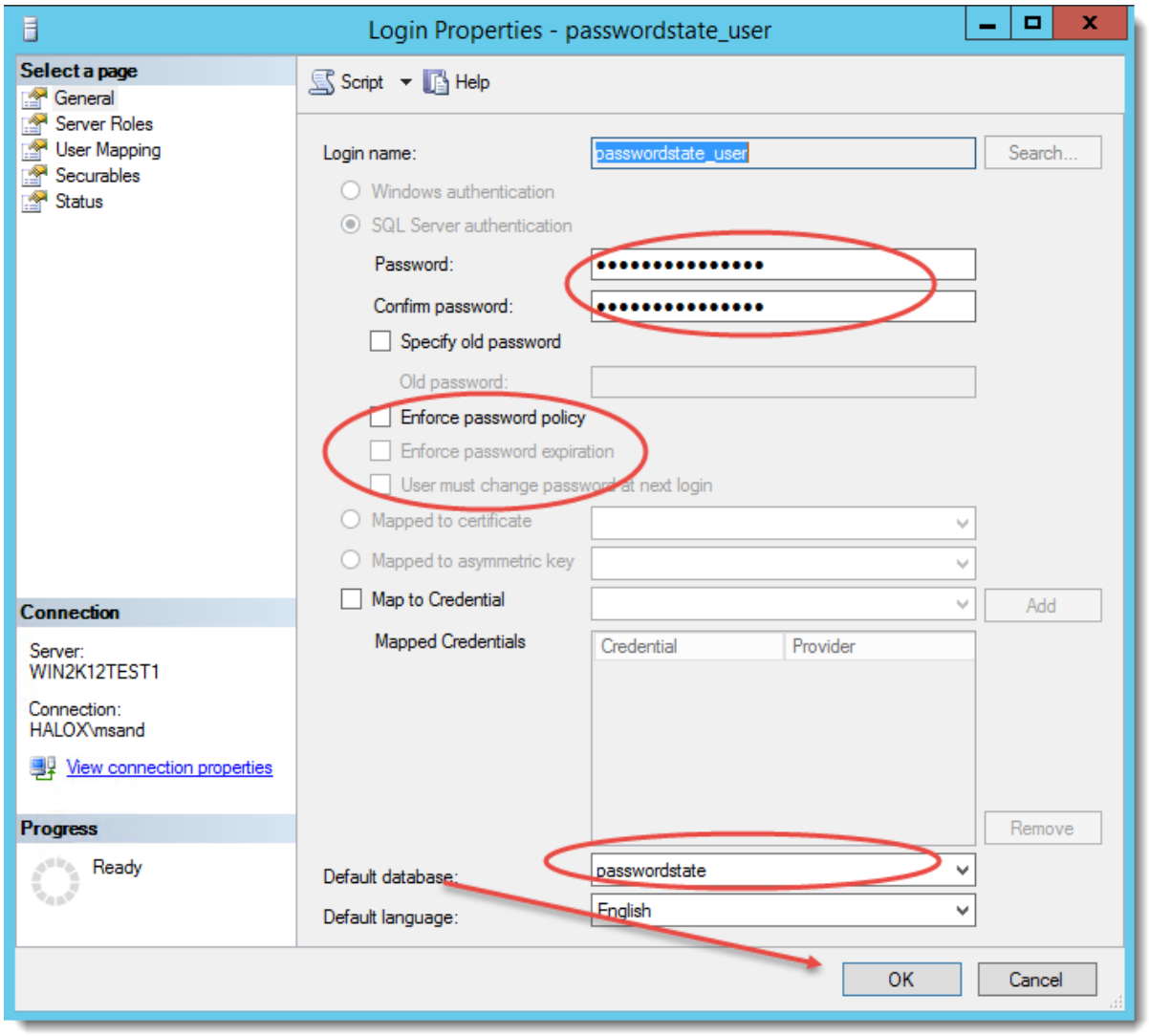
- Open SQL Management Studio and make a connection to your database server
- Browse to the Security -> Logins section, and double click on the passwordstate_user SQL Account

© 2017 Click Studios (SA) Pty Ltd

- Reset the password based on the following two screenshots



© 2017 Click Studios (SA) Pty Ltd



9.9.5 Recovery Emergency Access Password

If you need Click Studios' help in recovering your Emergency Access login password, please follow these instructions (if you are not sure of what build of Passwordstate you are using, please see the section 'Determine Current Passwordstate Build Number' below):

Using Build 7580 or Above

- Open SQL Server Management Studio, execute the following query:

```
Use Passwordstate
SELECT EA_Password, Secret3, Secret4 FROM SystemSettings
```

- Email us a copy of the results of the SQL Query above, and also a copy of your web.config file, which is generally located in the path of c:\inetpub\passwordstate (Note: If the appSettings section is encrypted in your web.config file, you will need to decrypt this before sending to us by following the instructions below)

© 2017 Click Studios (SA) Pty Ltd

Decrypt appSettings Section in Web.Config File

- On your Passwordstate web server, open the command prompt as Admin
- Type: CD C:\Windows\Microsoft.NET\Framework64\v4.0.30319
- Type: aspnet_regiis.exe -pdf "appSettings" "c:\inetpub\passwordstate" (your path may be different here)

Using a Build Prior to 7580

- Open SQL Server Management Studio, execute the following query, and email us the results:

```
Use Passwordstate
SELECT InitialisationVector, EA_Password FROM SystemSettings
```

Determine Current Passwordstate Build Number

- Using SQL Server Management Studio, make a connection to your database server and execute the following query:

```
USE Passwordstate
SELECT BuildNo FROM [systemSettings]
```

© 2017 Click Studios (SA) Pty Ltd