



## **Passwordstate User Manual**

# Table of Contents

Foreword	0
<b>Part I Passwordstate User Manual</b>	<b>4</b>
1 Glossary.....	4
2 Quick Start Tutorials.....	5
<b>Part II Passwords</b>	<b>13</b>
1 Passwords Menu.....	15
<b>Passwords Home</b> .....	<b>16</b>
Navigation Tree.....	18
Password Home.....	21
Screen Options .....	22
Folders .....	26
Folder Properties.....	27
Clone a Folder .....	28
Password Lists.....	29
Screen Options .....	30
Add Password .....	35
Edit Password .....	42
Upload Documents.....	48
Email Permalinks.....	49
Password Actions.....	50
Check-In Password.....	51
Copy or Email Password Permalink.....	53
Copy or Move to Different Password List.....	54
Filter Recent Activity on this Record.....	55
Link Account to Multiple Web Site URLs.....	56
Send Self Destruct Message.....	56
View & Compare History of Changes.....	58
View Documents.....	59
View Individual Password Permissions.....	60
Grant New Permissions.....	61
View Password Reset Dependencies.....	63
List Administrator Actions.....	65
Bulk Update Passwords.....	68
Bulk Update Password Reset Options.....	71
Edit Password List Properties.....	72
Password List Details Tab.....	73
Customize Fields Tab.....	79
Guide Tab .....	80
API Key & Settings Tab.....	81
Save Password List as Template.....	83
Toggle Visibility of Web API IDs.....	84
View Password List Permissions.....	85
Grant New Permissions.....	86
View Recycle Bin.....	88
<b>Add Folder</b> .....	<b>89</b>
<b>Add Private Password List</b> .....	<b>90</b>

Add Shared Password List .....	93
Administer Bulk Permissions .....	97
Expiring Passwords Calendar .....	98
Password List Templates .....	99
Add New Template.....	101
Linked Password Lists.....	102
Pending Access Requests .....	103
Request Access to Passwords .....	104
Toggle All Password List Visibility .....	106
<b>2 Tools Menu.....</b>	<b>108</b>
Account Discovery .....	108
Have I Been Pwned Password Check .....	112
Import Passwords .....	113
Password Generator .....	117
Password Resets in Progress .....	120
Self Destruct Message .....	121
<b>3 Reports Menu.....</b>	<b>123</b>
Auditing .....	124
Auditing Graphs .....	127
Scheduled Reports .....	128
<b>4 Preferences Menu.....</b>	<b>132</b>
Address Book .....	132
Preferences .....	132
Passwords Tab.....	133
Hosts Tab.....	134
Miscellaneous Tab.....	135
Color Theme Tab.....	137
Authentication Options Tab.....	138
Mobile Access Options Tab.....	155
Browser Extension.....	155
API .....	156
Email Notifications .....	157
<b>Part III Hosts</b>	<b>158</b>
<b>1 Hosts Home Screen.....</b>	<b>158</b>
View All Host Records .....	159
View Host Discovery Jobs .....	162
<b>2 Remote Session Management.....</b>	<b>164</b>
<b>Part IV Administration</b>	<b>164</b>
<b>Part V Help Menu</b>	<b>164</b>

# 1 Passwordstate User Manual



Welcome to the Passwordstate User Manual.

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

## Getting Started - Glossary

---

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

## Getting Started - New Users

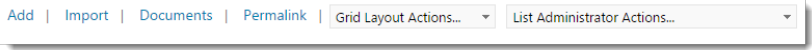
---

If you are new to Passwordstate, please study the [Quick Start Tutorials](#) to familiarize yourself with the basics.

### 1.1 Glossary

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

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

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

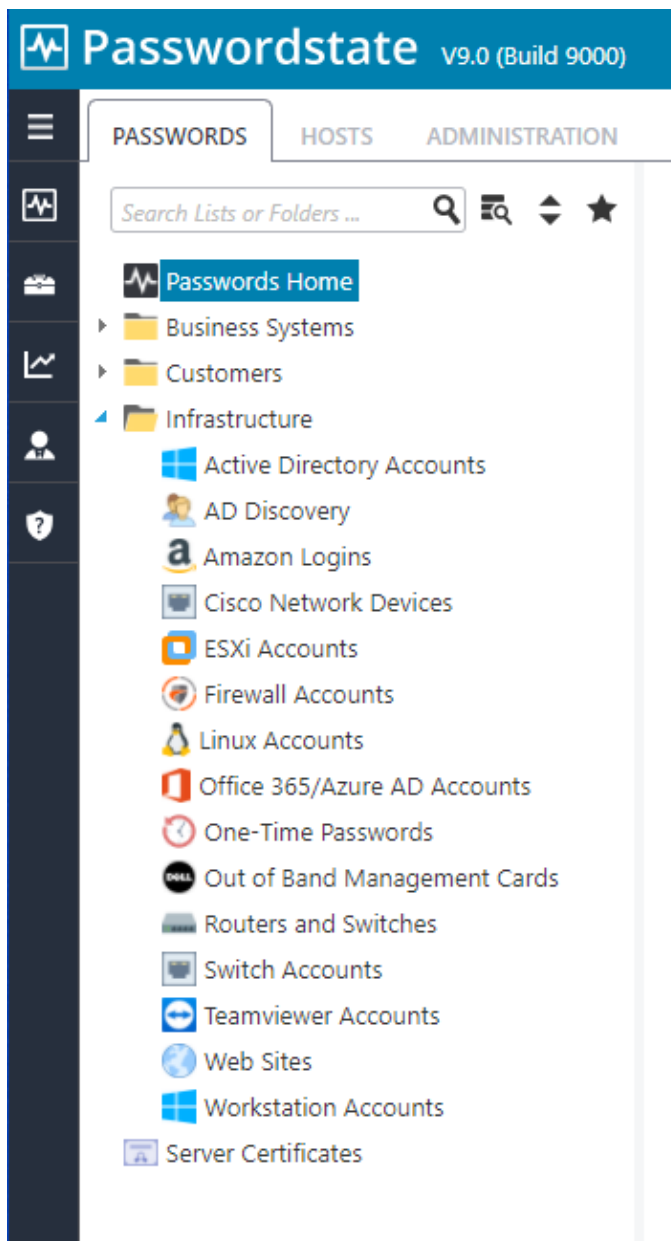
## 1.2 Quick Start Tutorials

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

### Organizing Password Lists Navigation Tree

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

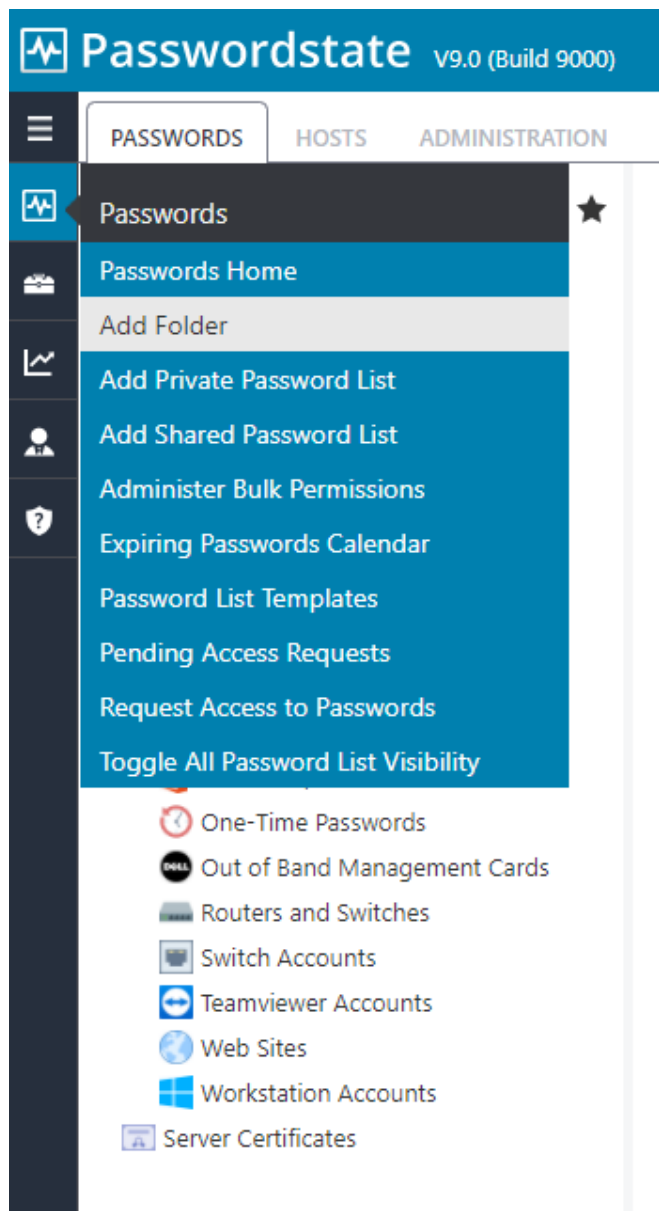
If you want a tree node to be displayed at the root of the navigation tree, simple drag and drop onto the highlighted 'Passwords Home' node you see in this picture.



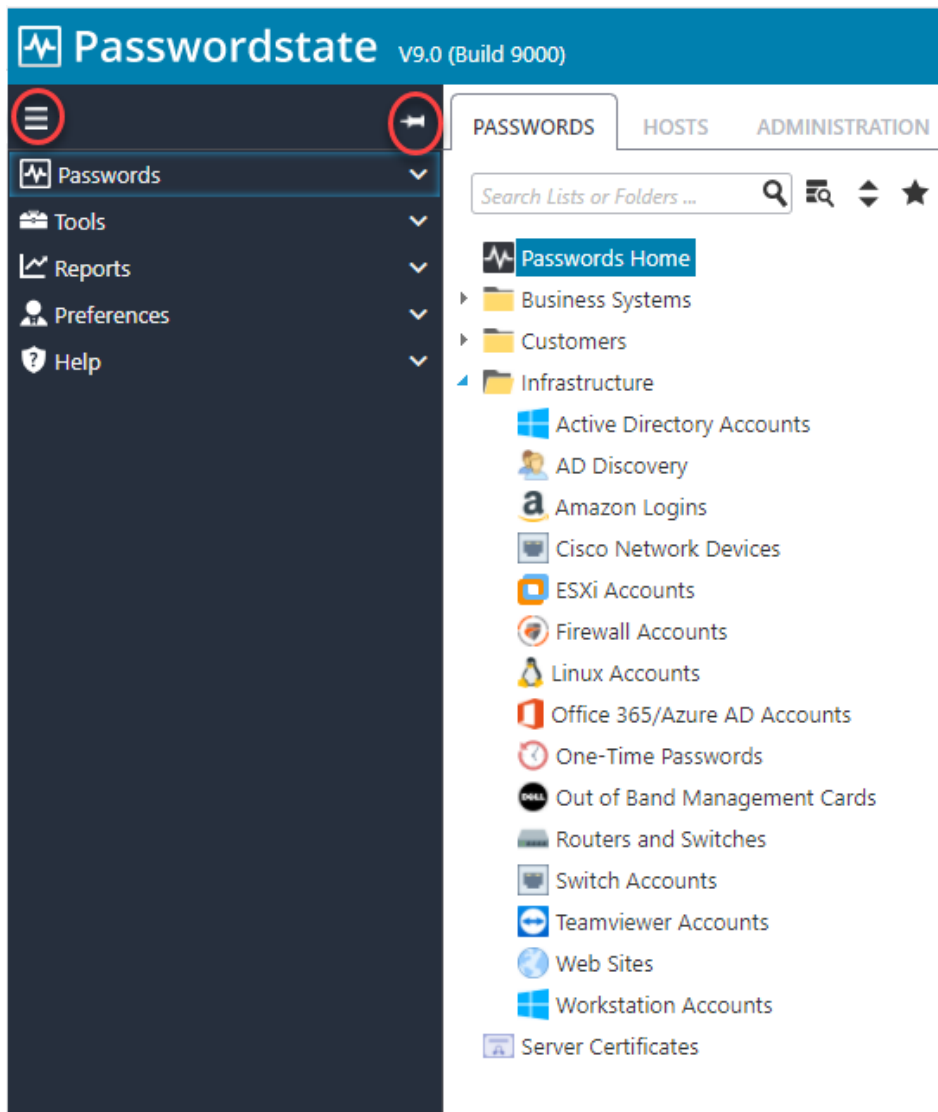
## Navigation Menu

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

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



You can also expand and pin the Vertical Menu.

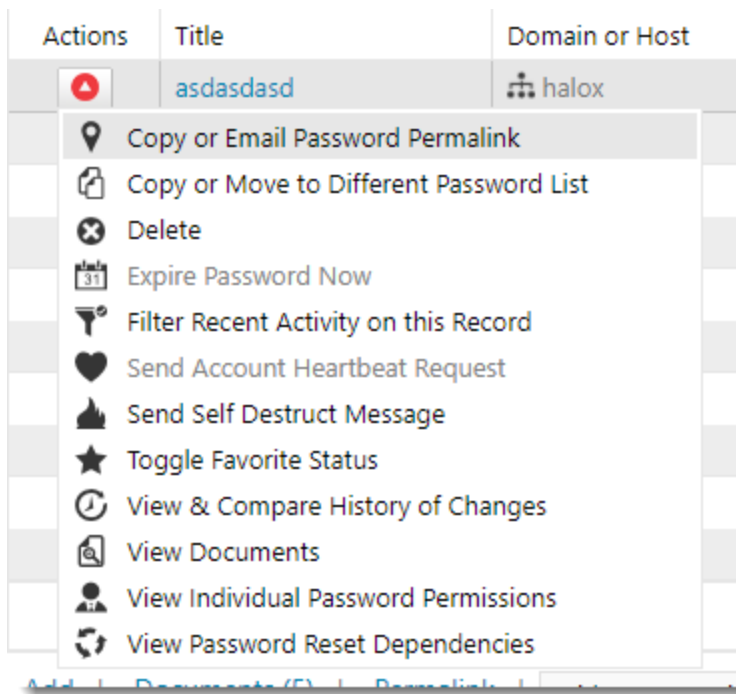


## Grid Actions Drop-down Menus

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

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

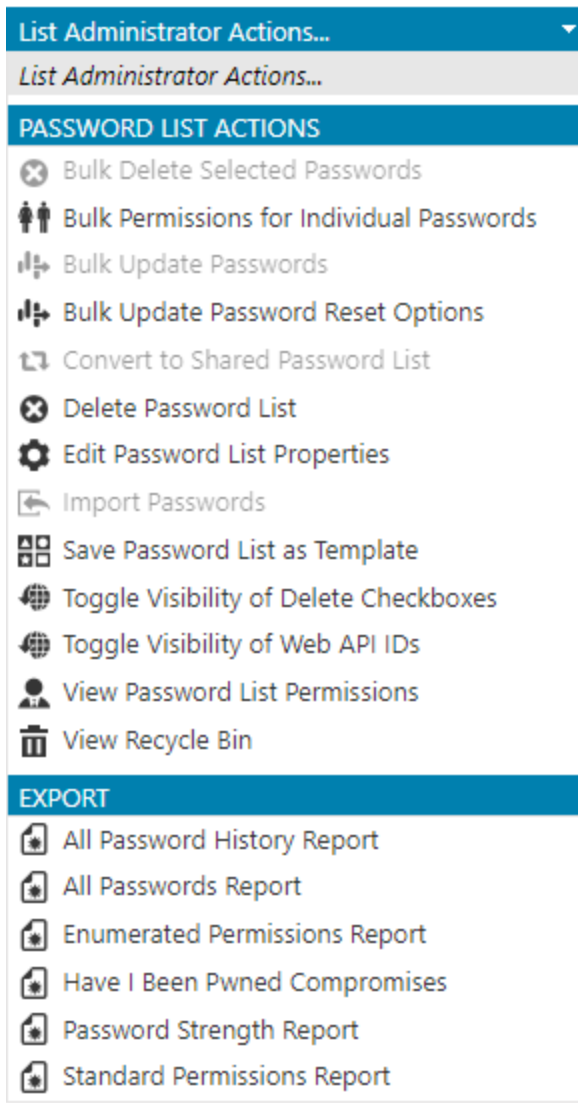




## Password List Administrator Actions

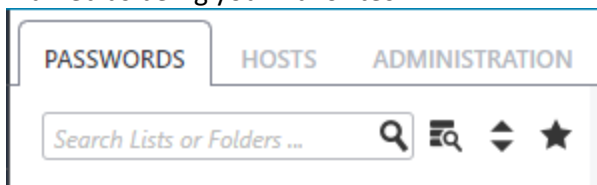
At the bottom of each of the Passwords grids, you may see a 'List Administrator Actions' drop-down list as per the image to the left. From this drop-down you are able to administer permissions and edit details for the Password List, as well as various types of reporting.

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



## Searching for Password Lists and Folders in the Navigation Tree

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



## Resizing the Navigation Tree Pane


---

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

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

## View or Copy Password to Clipboard

---

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

Both of these actions will add an audit event record.

## Password and Password List Permissions

---

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

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

## Searching for Passwords

---

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

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

## Resetting Number of Rows in Grids

---

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

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

A button with a grid icon and the text "Screen Options".

## 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.

A button with a grid icon and the text "Screen Options".

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

## Reordering and Resizing Grid Columns

---


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

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

---

## Generate a Random Password

---

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

## Preferences

---

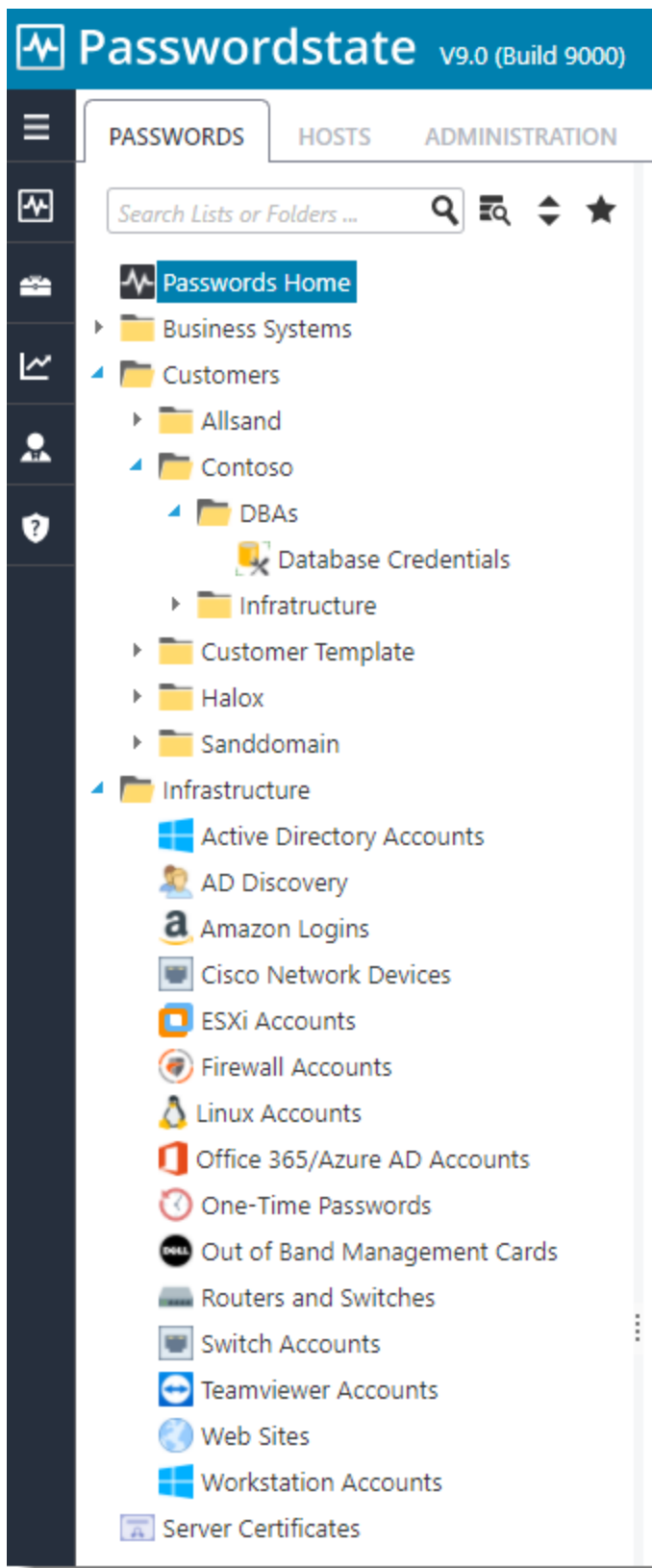
By clicking on the main 'Preferences' Menu Item, you can specify multiple settings which are specific to your account. In particular:

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

## 2 Passwords

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

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



## 2.1 Passwords Menu

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

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

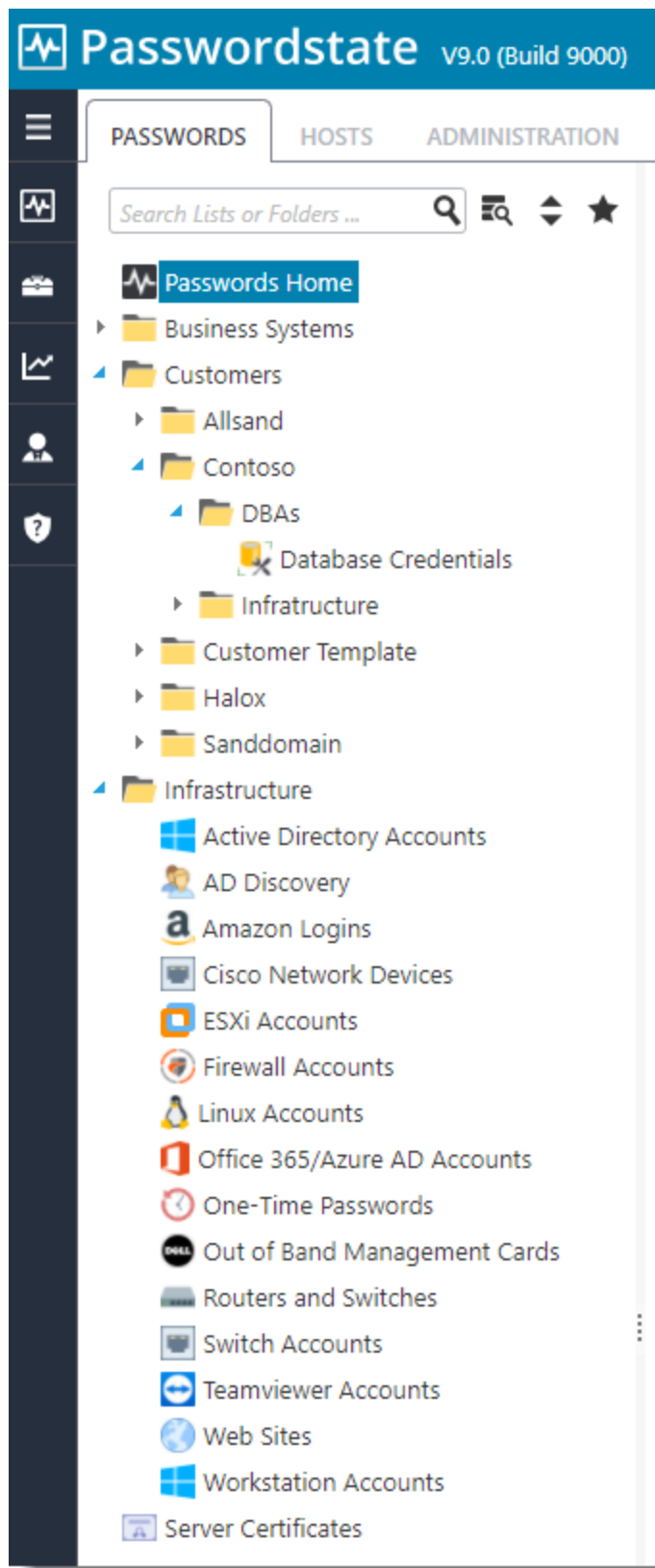
Menu Item	Description
<a href="#">Passwords Home</a>	Clicking on Passwords Home will display whatever Password List, or Folder, you have selected as being your default Home Page in the <a href="#">Preferences</a> area
<a href="#">Add Folder</a>	Allows you to add a new Folder, for organizing a group of related Password Lists
<a href="#">Add Private Password List</a>	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
<a href="#">Add Shared Password List</a>	Allows you to create a new Shared Password List, which can be shared with other users in Passwordstate
<a href="#">Administer Bulk Permissions</a>	Allows you to assign permissions to multiple Password Lists at once, for either user accounts in Passwordstate, or security groups
<a href="#">Expiring Passwords Calendar</a>	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
<a href="#">Password List Templates</a>	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
<a href="#">Pending Access Requests</a>	Allows you view/process any access requests you are responsible for, or view our own status of access requests
<a href="#">Request Access to Passwords</a>	Allows you to search for Password Lists or Password Records, and request access to them
<a href="#">Toggle All Password List Visibility</a>	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 <b>Red</b> if you do not have access, and clicking on them will allow you to request access

### 2.1.1 Passwords Home

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

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



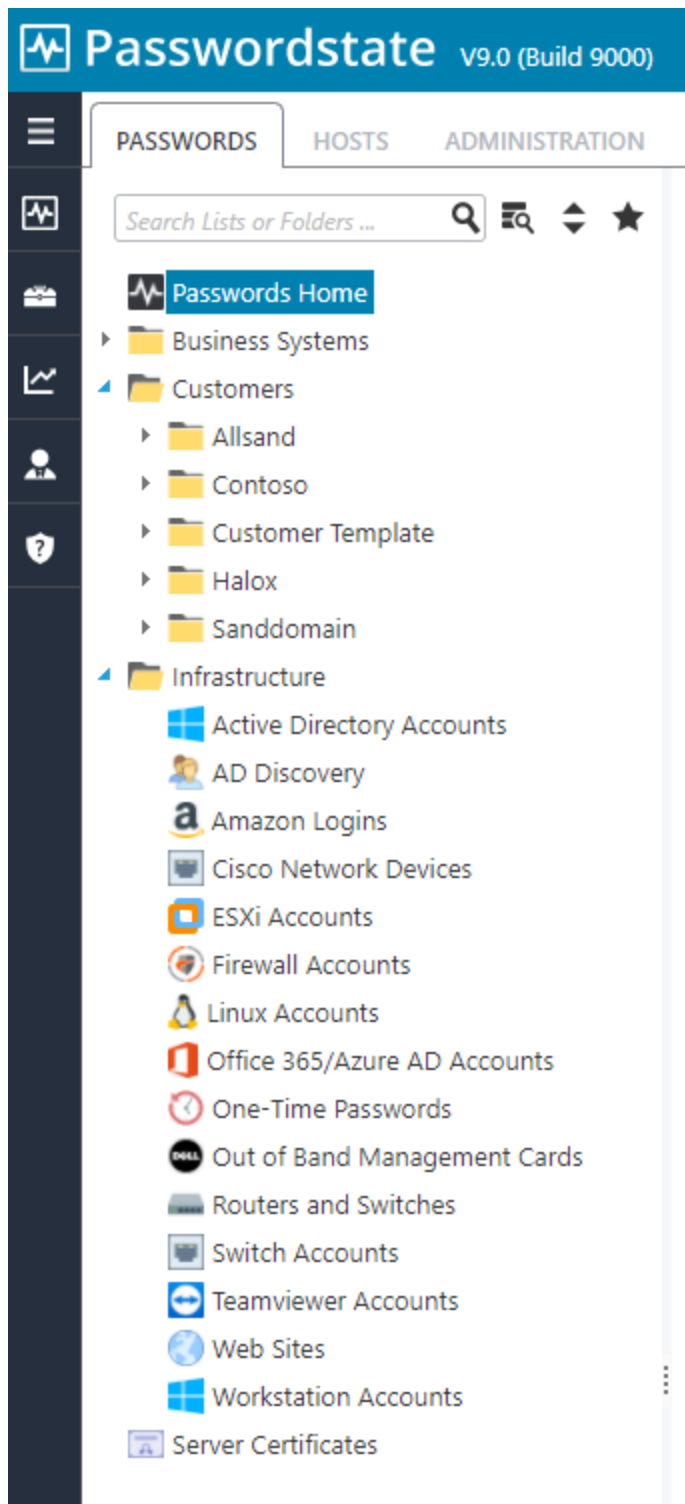


### 2.1.1.1 Navigation Tree

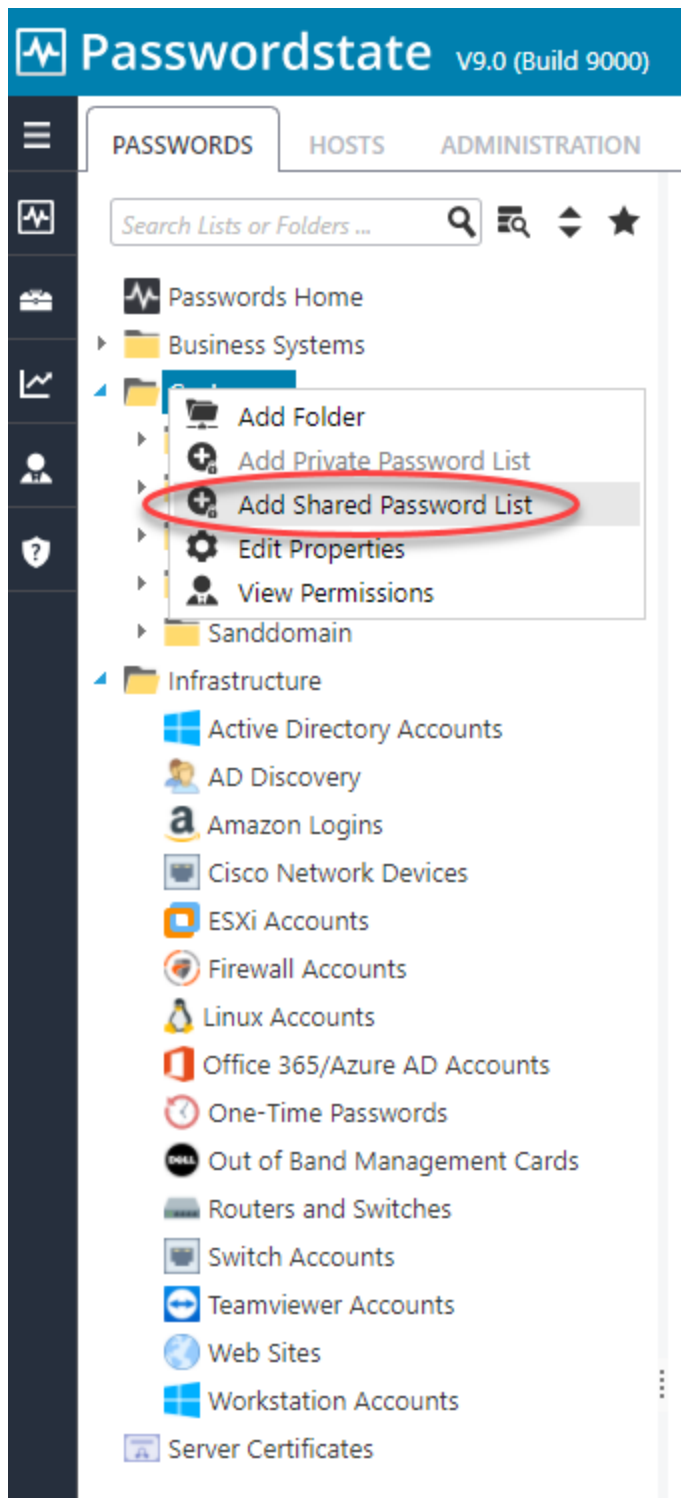
The Passwords **Navigation Tree** is used to access all of the Password List you have been given access to, and it is used to logically group related Password Lists and Folders. The only Folders and Password Lists visible in this panel are the ones you have been given access to.

Some of the features of the Navigation Tree are:

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



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





2.1.1.1.1 Passwords Home

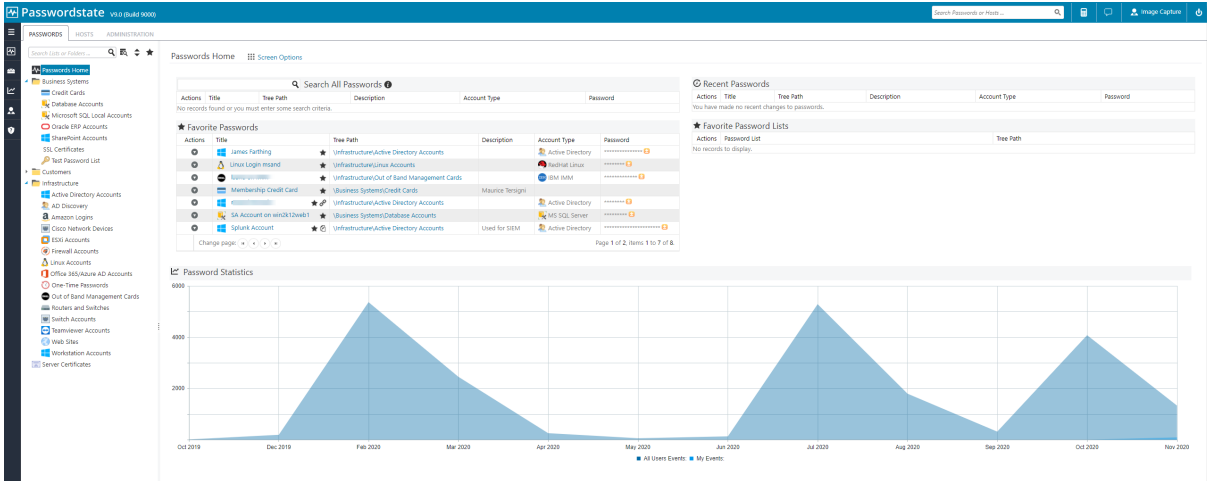
Clicking on the **Passwords Home** icon will display the screen below. This screen will be a **filtered view** of all Password Lists you have access to (.

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

On this screen you can:

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

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




The screenshot displays the Passwordstate application interface. At the top, there is a search bar and navigation tabs for 'PASSWORDS', 'HOSTS', and 'ADMINISTRATION'. The main content area is divided into several sections:

- Search All Passwords:** A table with columns for Actions, Title, Tree Path, Description, Account Type, and Password. It lists various password entries such as 'James Farthing', 'Unit Login misad', and 'Membership Credit Card'.
- Recent Passwords:** A section indicating 'No records found or you must enter some search criteria.'
- Favorite Password Lists:** A table listing favorite password lists with columns for Actions, Password List, and Tree Path.
- Password Statistics:** A line chart showing password usage over time from Dec 2019 to Nov 2020. The chart shows two distinct peaks in activity, one in early 2020 and another in mid-2020.

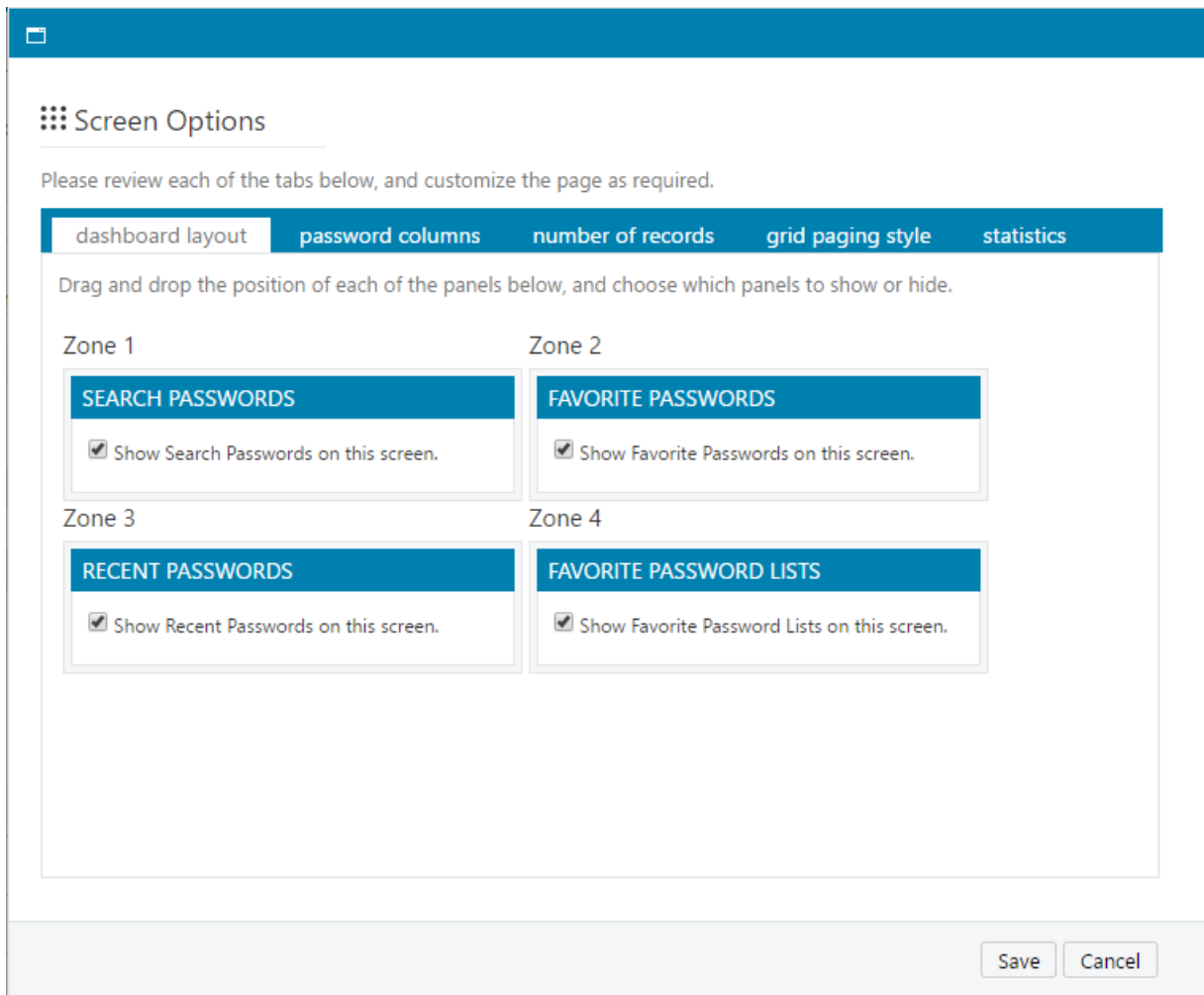
## 2.1.1.1.1.1 Screen Options

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

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

## Dashboard Layout Tab

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



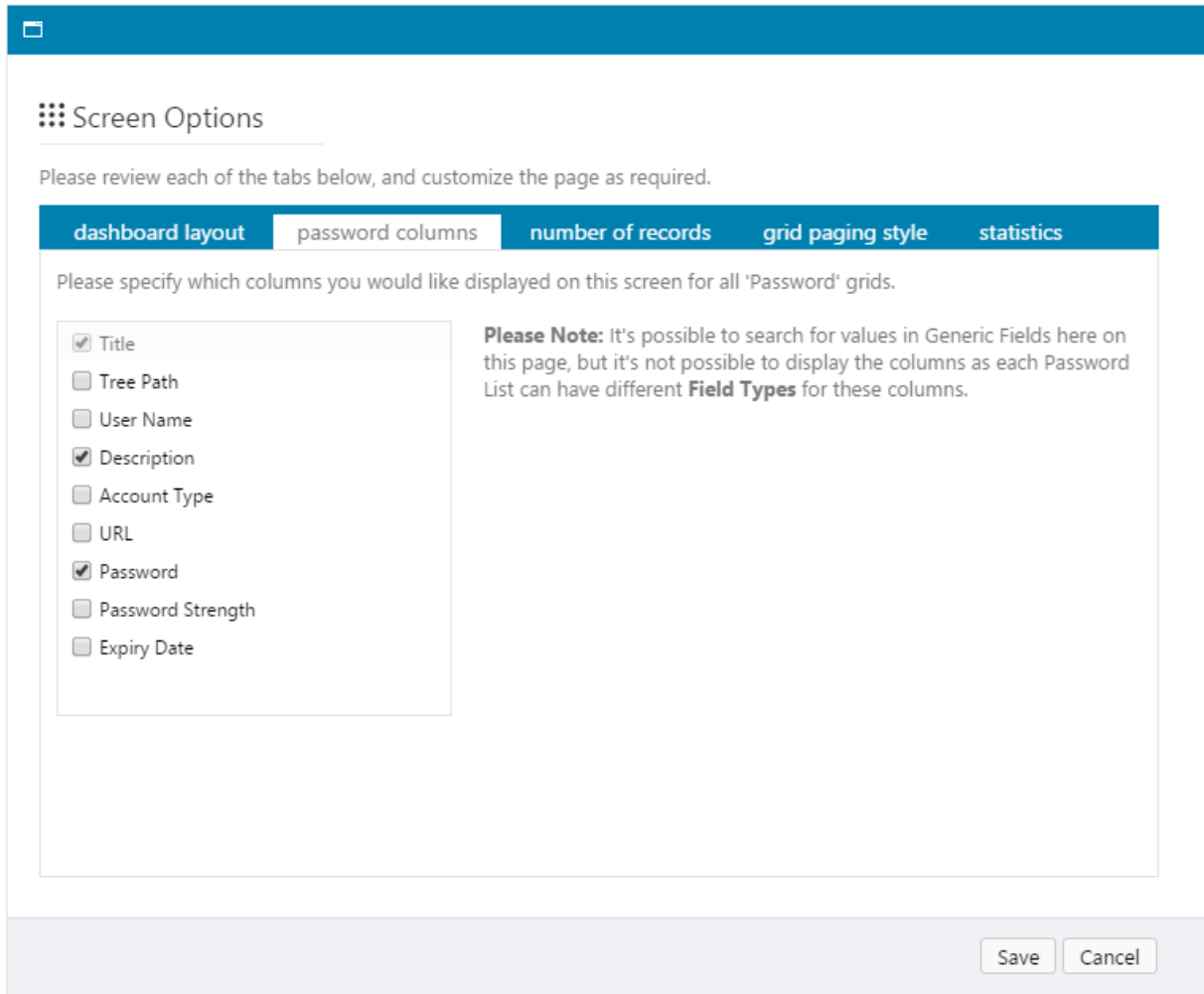
The screenshot shows the 'Screen Options' configuration page. At the top, there is a navigation bar with five tabs: 'dashboard layout' (selected), 'password columns', 'number of records', 'grid paging style', and 'statistics'. Below the tabs, a message reads: 'Please review each of the tabs below, and customize the page as required.' Underneath, a instruction says: 'Drag and drop the position of each of the panels below, and choose which panels to show or hide.' The main area is divided into four zones:

- Zone 1:** Contains a panel titled 'SEARCH PASSWORDS' with a checkbox labeled 'Show Search Passwords on this screen.' which is checked.
- Zone 2:** Contains a panel titled 'FAVORITE PASSWORDS' with a checkbox labeled 'Show Favorite Passwords on this screen.' which is checked.
- Zone 3:** Contains a panel titled 'RECENT PASSWORDS' with a checkbox labeled 'Show Recent Passwords on this screen.' which is checked.
- Zone 4:** Contains a panel titled 'FAVORITE PASSWORD LISTS' with a checkbox labeled 'Show Favorite Password Lists on this screen.' which is checked.

At the bottom right of the configuration area, there are two buttons: 'Save' and 'Cancel'.

## Password Columns Tab

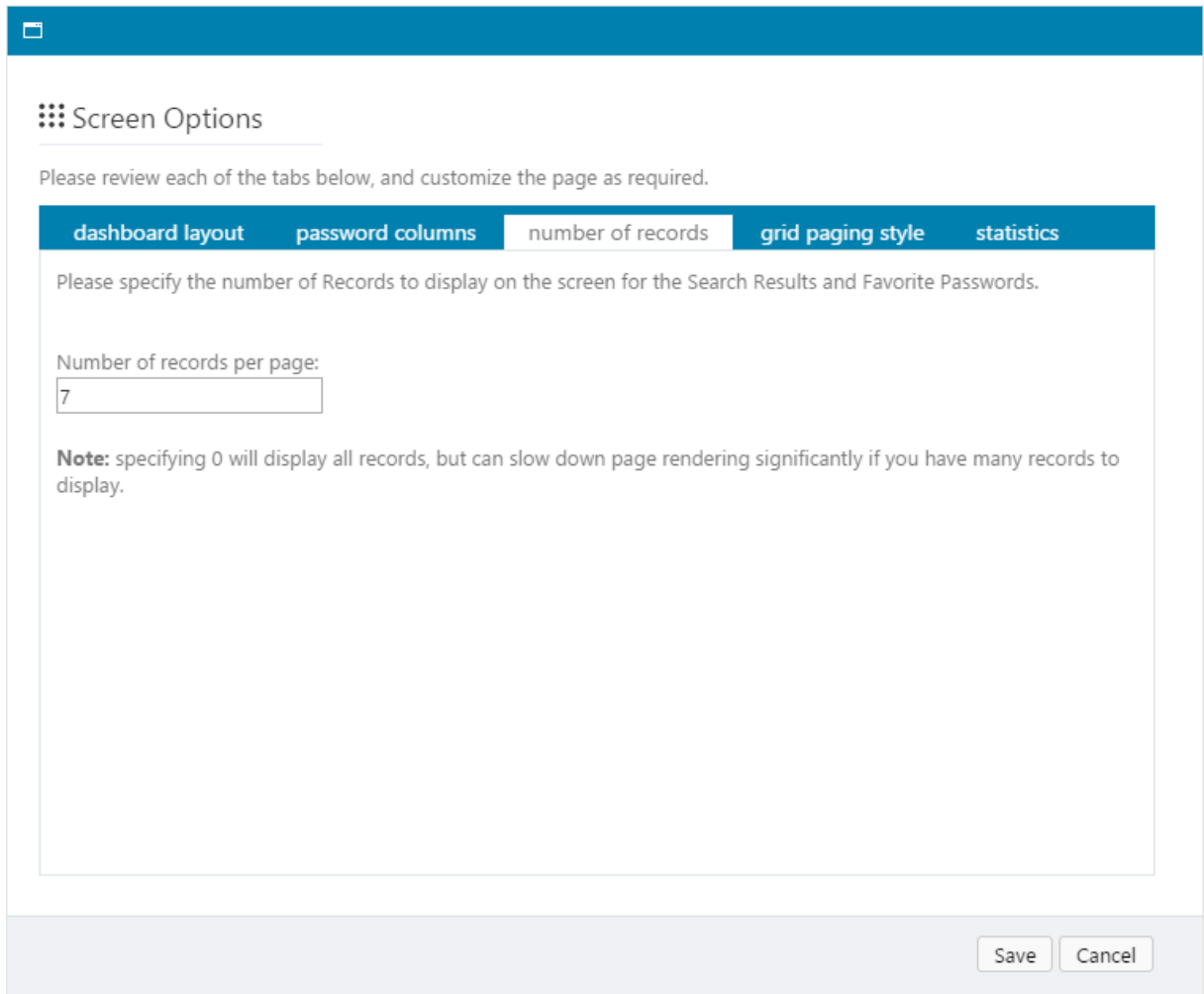
The Password Columns tab allows you to select which columns you want displayed for each of the Passwords Grids.



The screenshot shows a web interface for configuring screen options. At the top, there's a blue header with a square icon. Below it, the title 'Screen Options' is displayed with a grid icon. A sub-header reads 'Please review each of the tabs below, and customize the page as required.' There are five tabs: 'dashboard layout', 'password columns', 'number of records', 'grid paging style', and 'statistics'. The 'password columns' tab is active. Below the tabs, a text prompt says 'Please specify which columns you would like displayed on this screen for all 'Password' grids.' To the left is a list of checkboxes: Title (checked), Tree Path, User Name, Description (checked), Account Type, URL, Password (checked), Password Strength, and Expiry Date. To the right is a 'Please Note' section: 'Please Note: It's possible to search for values in Generic Fields here on this page, but it's not possible to display the columns as each Password List can have different Field Types for these columns.' At the bottom right, there are 'Save' and 'Cancel' buttons.

## 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.



The screenshot shows a 'Screen Options' dialog box with a blue header bar. Below the header, there is a title 'Screen Options' and a sub-header 'Please review each of the tabs below, and customize the page as required.' A horizontal tab bar contains five tabs: 'dashboard layout', 'password columns', 'number of records', 'grid paging style', and 'statistics'. The 'number of records' tab is currently selected. Below the tabs, there is a text prompt: 'Please specify the number of Records to display on the screen for the Search Results and Favorite Passwords.' This is followed by a label 'Number of records per page:' and a text input field containing the number '7'. A note below the input field states: 'Note: specifying 0 will display all records, but can slow down page rendering significantly if you have many records to display.' At the bottom right of the dialog, there are two buttons: 'Save' and 'Cancel'.

## 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.



☐

### Screen Options

Please review each of the tabs below, and customize the page as required.

dashboard layout
password columns
number of records
grid paging style
statistics

Please select which Paging style you would like to use for the Search Results and Favourite Passwords Grids - The pagers will appear in the footer of the grid.

Next Previous Buttons
  Slider
  Numeric Pages

**Next Previous Buttons**

Change page: ⏪ ⏩ ⏴ ⏵

**Slider**

⏪  ⏵

**Numeric**

1 2 3 4 5 6 7 8 9 10 ...

## 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.

**Screen Options**

Please review each of the tabs below, and customize the page as required.

dashboard layout password columns number of records grid paging style **statistics**

You can choose to show or hide the Passwords Statistics Chart, as well as change the type of chart, whether the data is 'stacked', and the color theme.

Show the Statistics Chart

**Choose the Graph Type:**  Area  Line  Bar

**Stack the data points on top of each other:**  Yes  No

**Choose Color Theme :** Flat

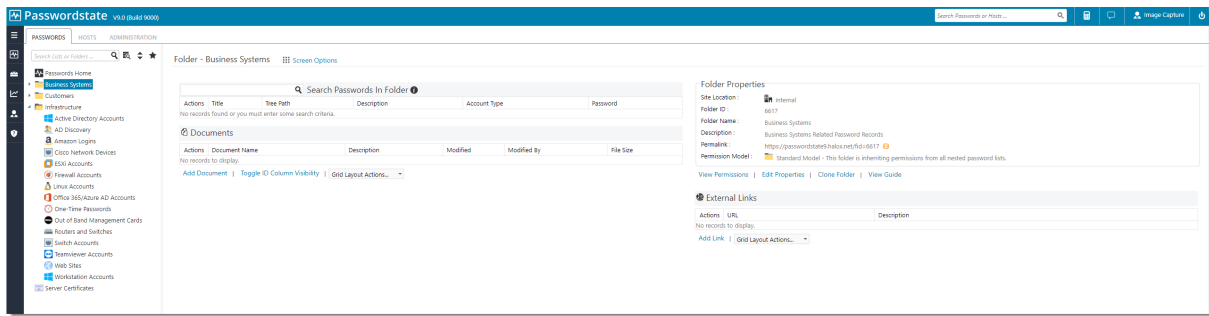
**Note:** The color theme you select here will also apply to the 'Auditing Graphs' screen as well.

Save Cancel

#### 2.1.1.1.2 Folders

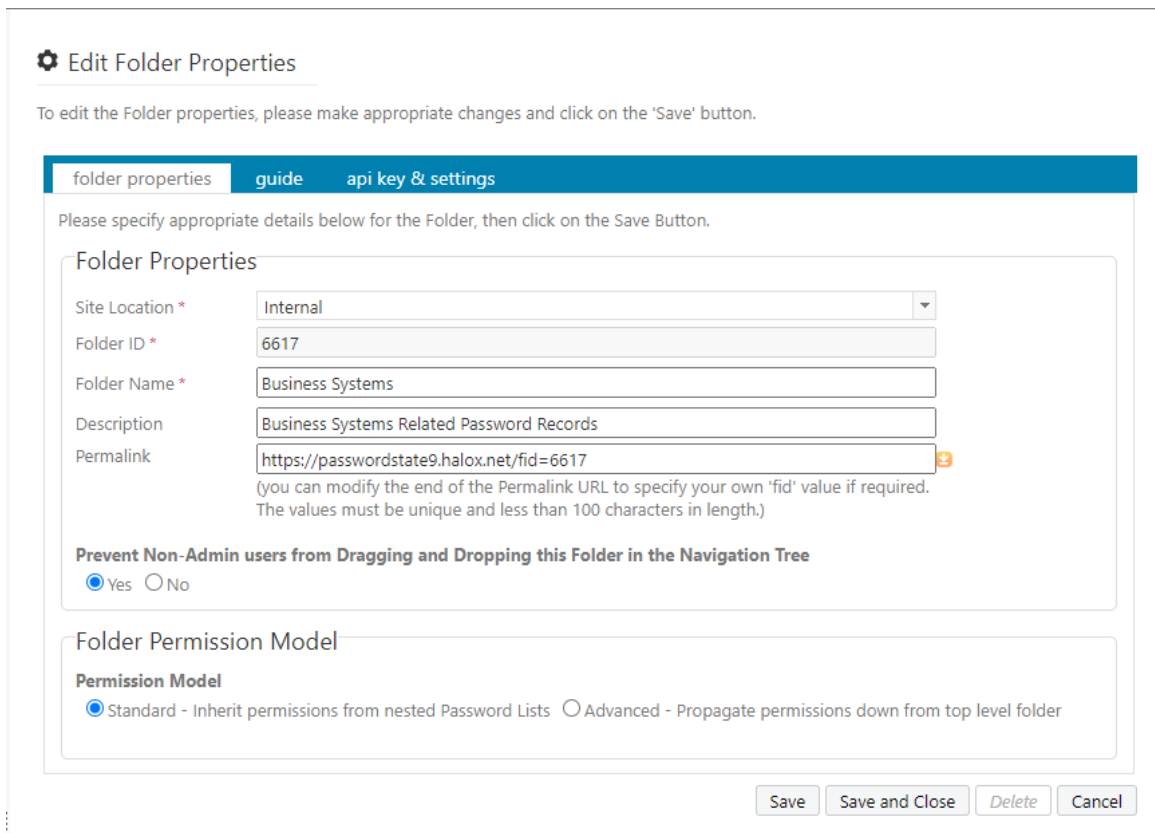
Clicking on a **Folder** will display a screen similar to below. This screen will show the following details for the Folder:

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



### 2.1.1.1.2.1 Folder Properties

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



## Folder Properties Tab

On the Folder Properties tab you can:

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

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

## Folder Permissions Model

---

There are two types of permission models available in Passwordstate:

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

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

### 2.1.1.1.2.2 Clone a Folder

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

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

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

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

**Clone Folder**

To clone the selected folder, please specify the name of the top level folder, and select the appropriate options.

**Note:** No passwords will be cloned with this process, only Folders and Password Lists.

**folder details**

Please specify appropriate details below, the click on the Save Button.

Site Location \*  All nested Folders & Password Lists will be marked as the selected Site above.

Folder Name \*

Description

**Clone the following Folders and Password Lists:**

All nested Folders and Password Lists  Just the nested Folders


**Apply the following permissions:**

Clone current permissions  Only for my account  None

Status:



### 2.1.1.2 Password Lists

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

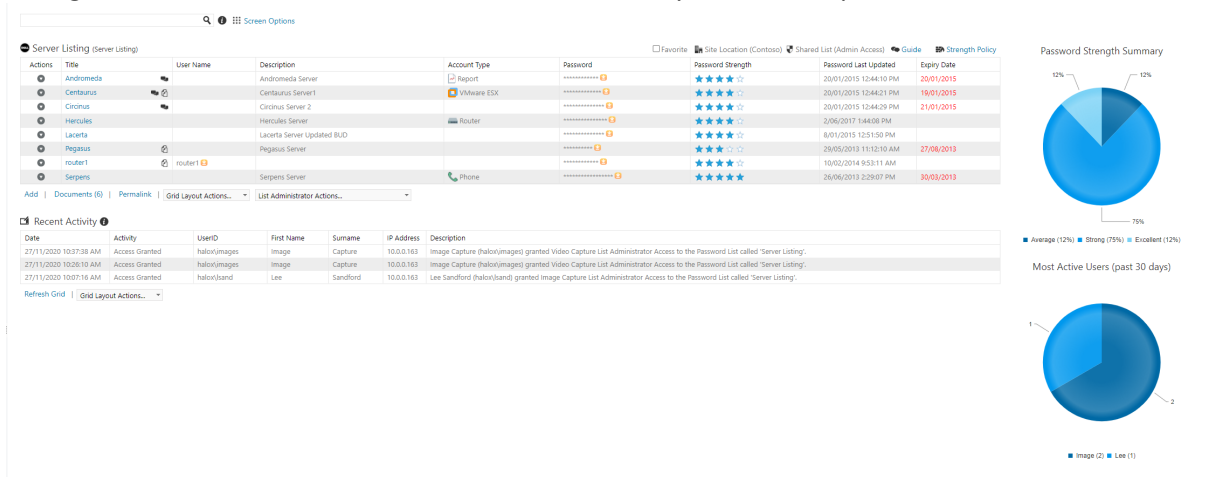
 **Note:** Some of these features detailed below may be hidden or disabled for you, depending on your access rights, and what settings have been applied to the selected Password List.

On this screen you can:

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

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

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

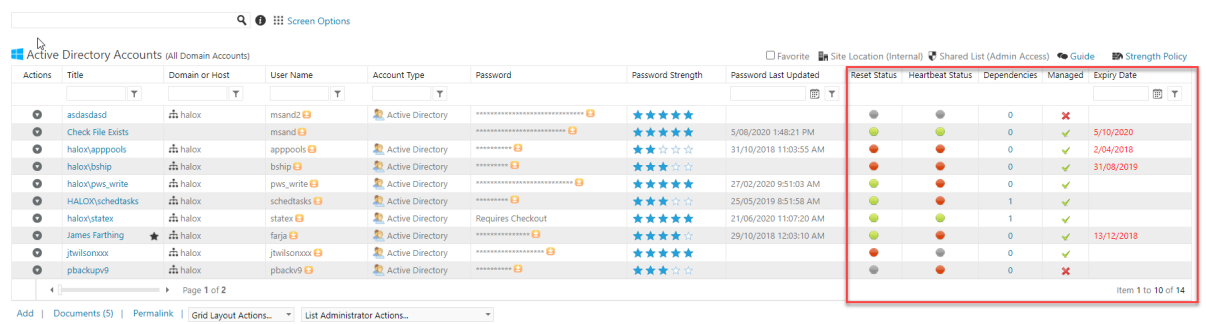


The screenshot displays the Passwordstate interface. The main table is titled 'Server Listing (Server Listing)' and contains the following data:

Actions	Title	User Name	Description	Account Type	Password	Password Strength	Password Last Updated	Expiry Date
	Andromeda		Andromeda Server	Report	*****	★★★★☆	20/01/2015 12:44:10 PM	20/01/2015
	Cerberus		Cerberus Server1	VMware ESX	*****	★★★★☆	20/07/2015 12:44:21 PM	19/07/2015
	Cirrus		Cirrus Server 2		*****	★★★★☆	20/01/2015 12:44:20 PM	21/01/2015
	Hercules		Hercules Server	Router	*****	★★★★☆	2/06/2017 1:44:08 PM	
	Lacerta		Lacerta Server Updated RUD		*****	★★★★☆	8/01/2015 12:51:50 PM	
	Pegasus		Pegasus Server		*****	★★★★☆	29/05/2013 11:12:10 AM	27/08/2013
	router1	router1			*****	★★★★☆	10/02/2014 9:53:11 AM	
	Serpens		Serpens Server	Phone	*****	★★★★☆	26/06/2013 2:29:07 PM	30/03/2013

Below the grid are two pie charts:

- Password Strength Summary:** A pie chart showing the distribution of password strengths. The legend indicates: Average (12%), Strong (75%), and Excellent (12%).
- Most Active Users (past 30 days):** A pie chart showing the distribution of most active users. The legend indicates: Image (2) and Lee (1).




The screenshot displays the Passwordstate interface for Active Directory Accounts. The main table is titled 'Active Directory Accounts (all Domain Accounts)' and contains the following data:

Actions	Title	Domain or Host	User Name	Account Type	Password	Password Strength	Password Last Updated	Reset Status	Heartbeat Status	Dependencies	Managed	Expiry Date
	asdasd	halox	msand2	Active Directory	*****	★★★★★				0	✗	
	Check File Exists	halox	msand	Active Directory	*****	★★★★★	5/08/2020 1:48:21 PM			0	✓	5/10/2020
	halox/appools	halox	appools	Active Directory	*****	★★★★☆	31/10/2018 11:03:55 AM			0	✓	2/04/2018
	halox/bshp	halox	bshp	Active Directory	*****	★★★★☆				0	✓	31/08/2019
	halox/pws_write	halox	pws_write	Active Directory	*****	★★★★★	27/02/2020 9:51:03 AM			0	✓	
	HALOX/schedtasks	halox	schedtasks	Active Directory	*****	★★★★☆	25/05/2019 8:51:58 AM			1	✓	
	halox/statex	halox	statex	Active Directory	Requires Checkout	★★★★★	21/06/2020 11:07:20 AM			1	✓	
	James Farthing	halox	farja	Active Directory	*****	★★★★☆	29/10/2018 12:03:10 AM			0	✓	13/12/2018
	jwilsonxxx	halox	jwilsonxxx	Active Directory	*****	★★★★★				0	✓	
	pbackupv9	halox	pbackv9	Active Directory	*****	★★★★☆				0	✗	

### 2.1.1.2.1 Screen Options

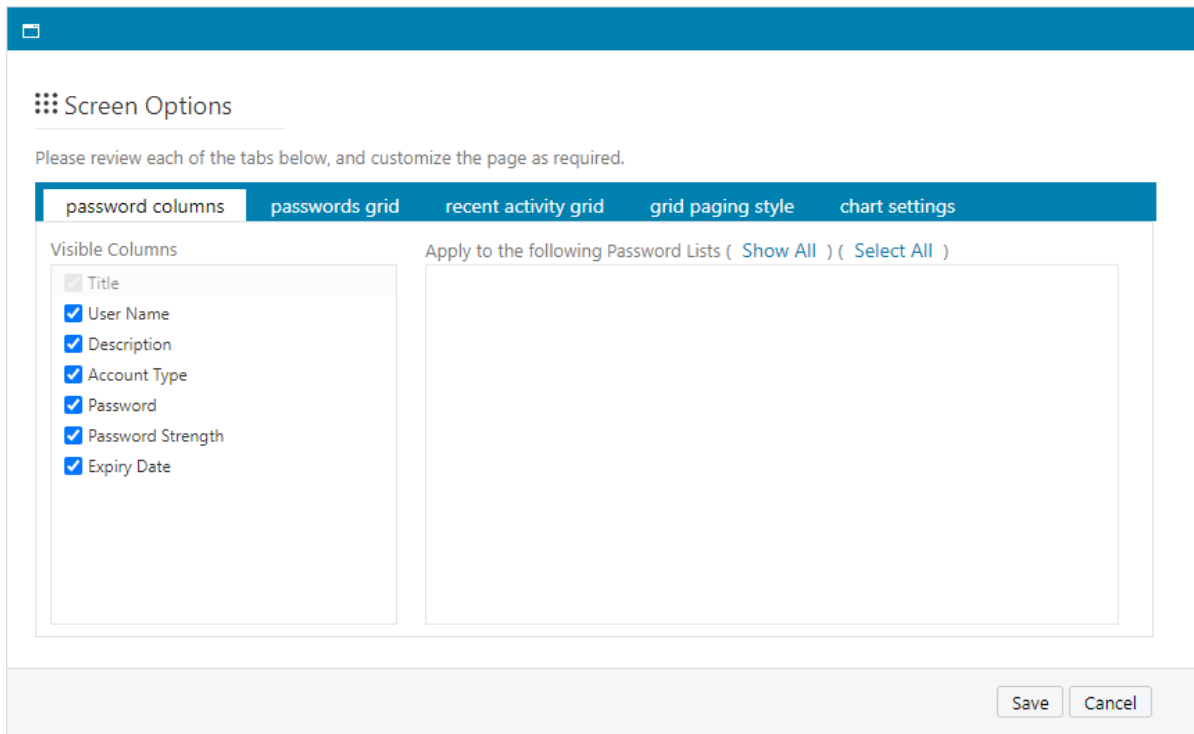
Screen Options allows you to specify various settings for how you would like to see the grids and charts displayed on the screen.

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

## Password Columns Tab

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

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



The screenshot shows the 'Screen Options' dialog box with the 'password columns' tab selected. The dialog contains a list of columns to be displayed in the Passwords grid. The columns are: Title (unchecked), User Name (checked), Description (checked), Account Type (checked), Password (checked), Password Strength (checked), and Expiry Date (checked). There are also buttons for 'Save' and 'Cancel' at the bottom right.

Screen Options

Please review each of the tabs below, and customize the page as required.

password columns passwords grid recent activity grid grid paging style chart settings

Visible Columns

- Title
- User Name
- Description
- Account Type
- Password
- Password Strength
- Expiry Date

Apply to the following Password Lists ( Show All ) ( Select All )

Save Cancel

## 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 of records to display in the grid.

Screen Options

Please review each of the tabs below, and customize the page as required.

password columns passwords grid recent activity grid grid paging style chart settings

For the Passwords Grid below, please select which attributes you would like to show or hide, and how many records you would like to display on the screen.

Filters  Header

Number of records per page:

**Note:** specifying 0 will display all records, but can slow down page rendering significantly if you have many records to display.

Save Cancel

## 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.



Screen Options

Please review each of the tabs below, and customize the page as required.

password columns passwords grid recent activity grid grid paging style chart settings

For the Recent Activity Grid below, please select which attributes you would like to show or hide, and how many records you would like to display on the screen.

Visible  Header

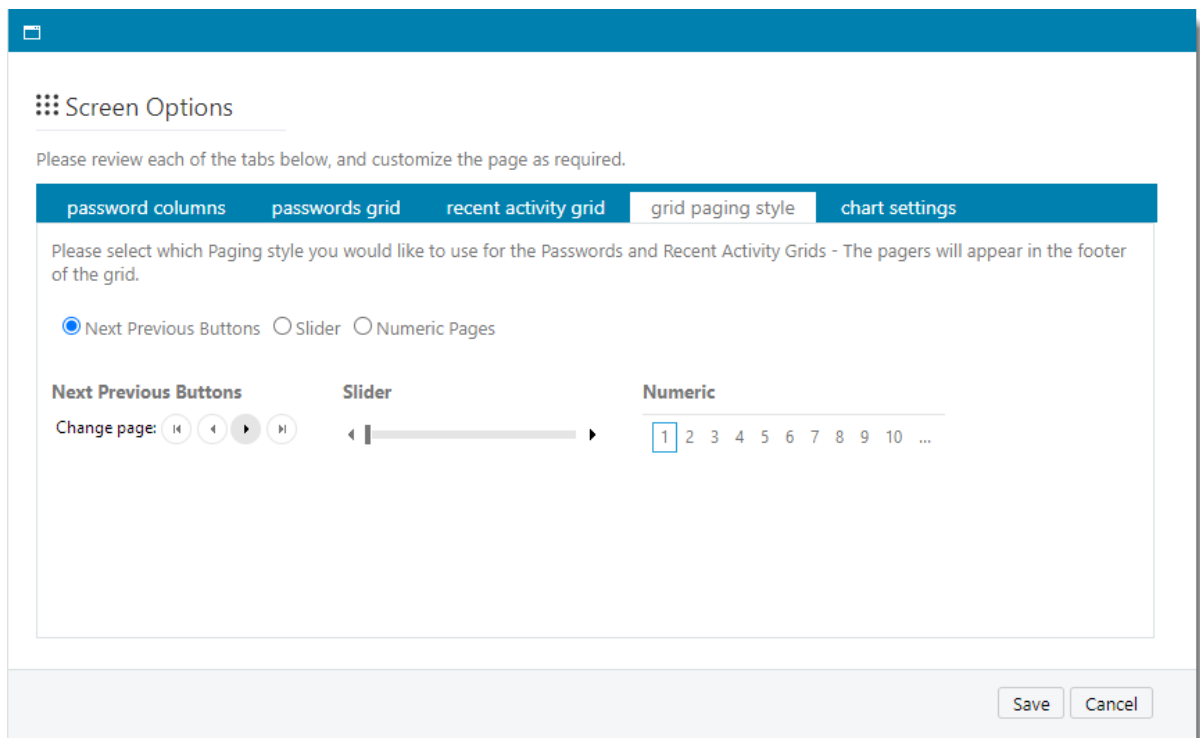
Number of records per page:

**Note:** specifying 0 will display all records, but can slow down page rendering significantly if you have many records to display.

Save Cancel

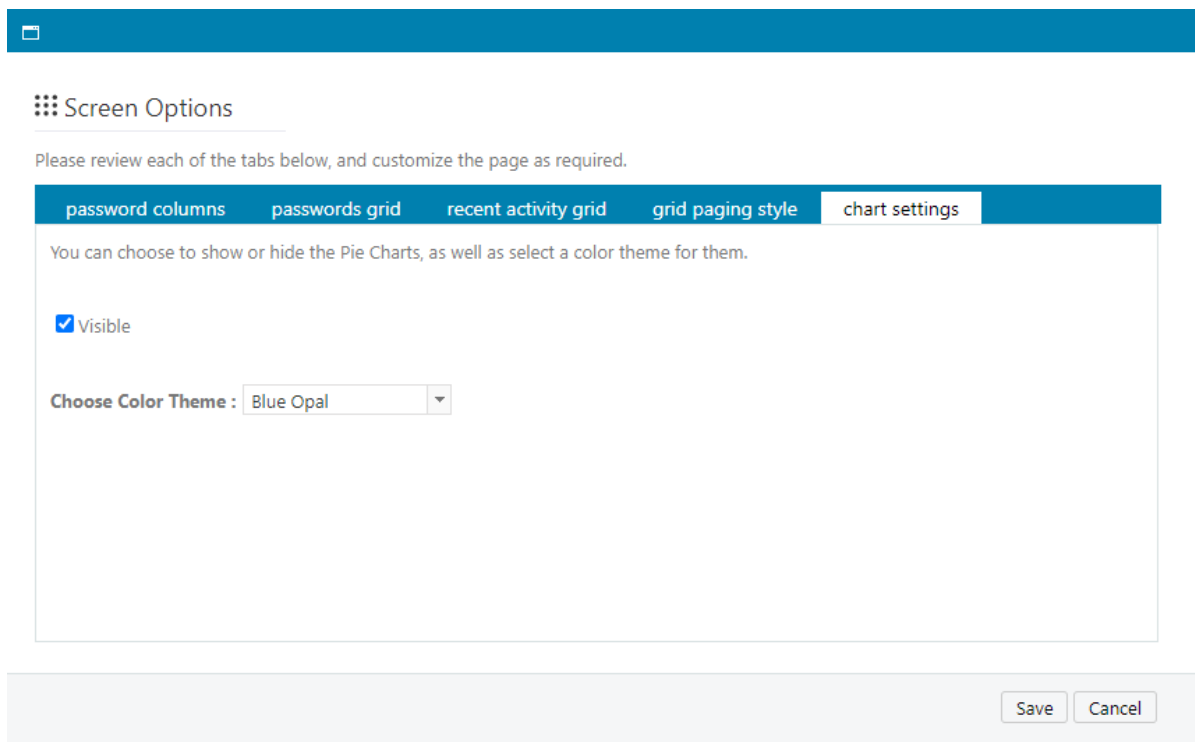
## Grid Paging Style Tab

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



## Chart Settings Tab

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



#### 2.1.1.2.2 Add Password

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


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

### Password Details Tab

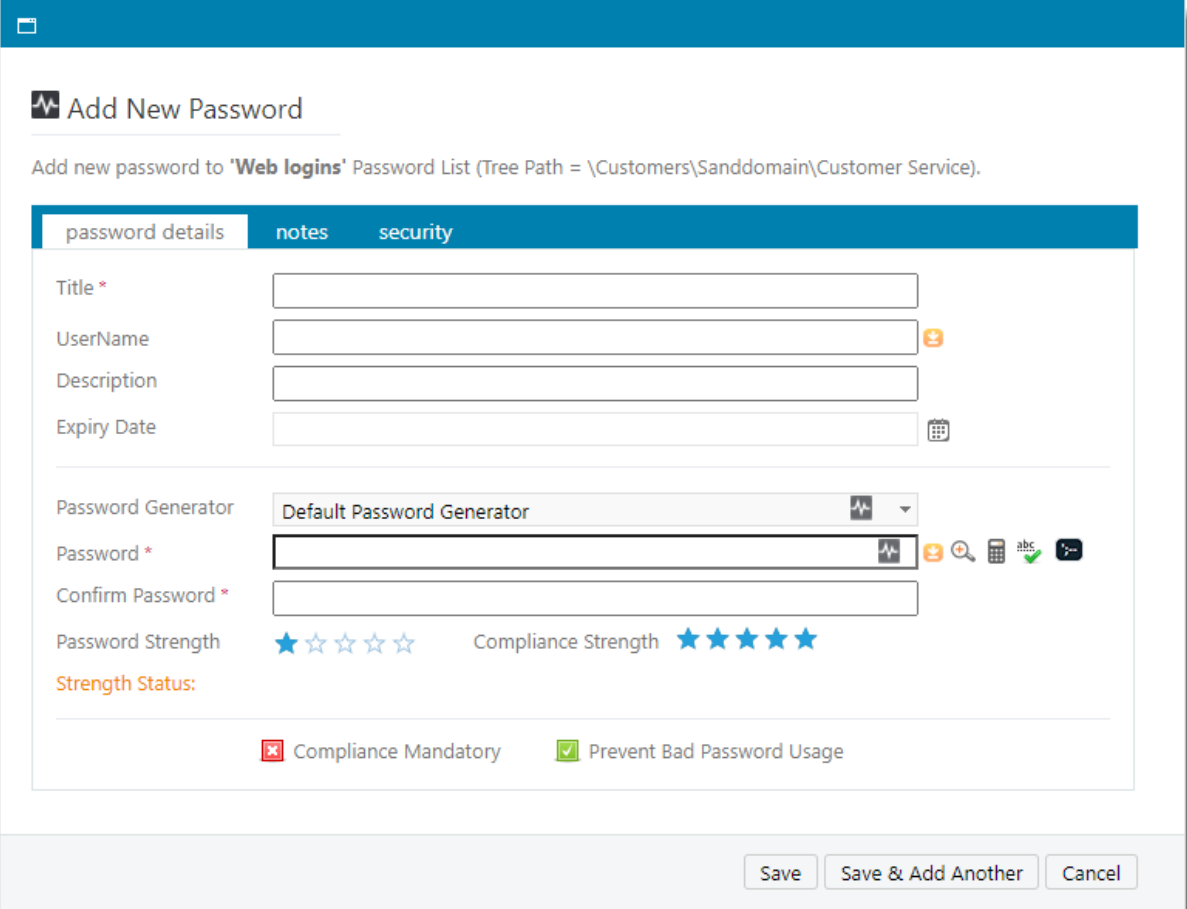
The Password Details tab is where you specify the values for the majority of fields associated with the selected Password List, and each field can be configured of different types i.e. URL, Text, Date, Radio Buttons, etc.

A few things to note on this tab is:

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

- The policy set for the selected Password List may also place certain restrictions to the Password record, like a certain Password Strength must be 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.




**Add New Password**


Add new password to 'Web logins' Password List (Tree Path = \Customers\Sanddomain\Customer Service).


password details notes security






Title \*

UserName  



Description

Expiry Date  

Password Generator  

Password \*      

Confirm Password \*

Password Strength  Compliance Strength 

Strength Status:

Compliance Mandatory  Prevent Bad Password Usage

Save Save & Add Another Cancel

☰

### Add New Password

Add new password to 'Active Directory Accounts' Password List (Tree Path = \Customers\Contoso\Infratructure).

password details
notes
security
reset options
heartbeat options

Title \*

Managed Account  Enabled for Resets  Enabled for Heartbeat

Account Type - Select Account Type -

Domain or Host

UserName

Description

Expiry Date

---

Password Generator Default Password Generator

Password \*

Confirm Password \*

Password Strength ★☆☆☆☆ Compliance Strength ★★★★★

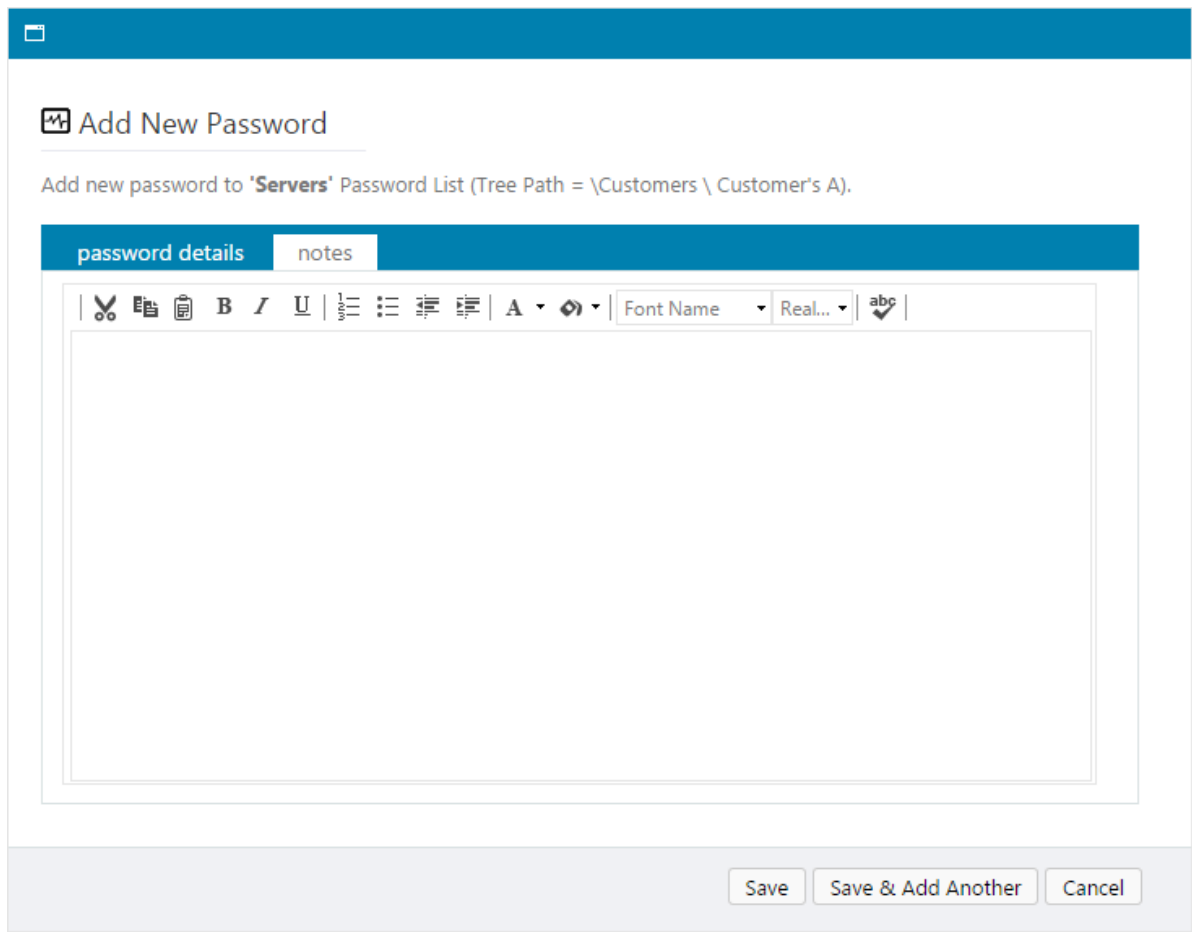
Strength Status:

❌ Compliance Mandatory
✅ Prevent Bad Password Usage

Save
Save & Add Another
Cancel

## Notes Tab

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



## Security Tab

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

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

The screenshot shows a web-based interface for adding a new password. The title is "Add New Password" with a sub-header "Add new password to 'Windows Admin Accounts' Password List (Tree Path = \Customers\Sanddomain)". The interface has five tabs: "password details", "notes", "security", "reset options", and "heartbeat options". The "security" tab is active, showing "Password Security Settings" with the following options:

- Password Requires Check Out:
- Change Password On Check In:
- Check In Automatically After: 01 Hour(s) 00 Minute(s). Below this, it says "Setting to 00:00 will disable automatic check-in."
- Password Export:  Allow this Password to be Exported

At the bottom right, there are three buttons: "Save", "Save & Add Another", and "Cancel".

## Reset Options and Heartbeat Options Tabs

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

Options available are:

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

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

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

**Add New Password**

Add new password to '**Windows Admin Accounts**' Password List (Tree Path = \Customers\Sanddomain).

password details   notes   security   **reset options**   heartbeat options

**Password Reset Script and Privileged Account Credentials**

Please select the appropriate Password Reset Script, and Privileged Account Credential, in order to perform the password reset.

Password Reset Script   -- Select Password Reset Script --

Privileged Account   -- Select if Required --

- Not all Reset Scripts require a Privileged Account. See KB Article in menu Help -> User Manual.  
- Active Directory Accounts do not require you to select a Reset Script.

**Password Reset Schedule**

When this Password expires, Auto-Generate a new one and perform any reset tasks at the time of:  
06 Hour 00 Minute, and add 90 Day(s) to the Expiry Date.

Save   Save & Add Another   Cancel



The screenshot shows a web-based interface for adding a new password. The main heading is "Add New Password" with a sub-heading "Add new password to 'Windows Admin Accounts' Password List (Tree Path = \Customers\Sanddomain)". Below this is a tabbed interface with five tabs: "password details", "notes", "security", "reset options", and "heartbeat options". The "heartbeat options" tab is active and contains the following content:

**Heartbeat Validation Options**

Select the **Password Validation Script** to use for the Heartbeat verification, and what schedule you would like to use to validate the password is correct:

-- Select Validation Script --

Use the Privileged Account Credential selected on the 'Reset Options' tab to perform the authentication for this validation (only used for Linux accounts if required):

**Validate Password every day at:**

12 Hour 18 Minute

At the bottom of the dialog are three buttons: "Save", "Save & Add Another", and "Cancel".

## Validating Linux Root Account Passwords

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

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

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

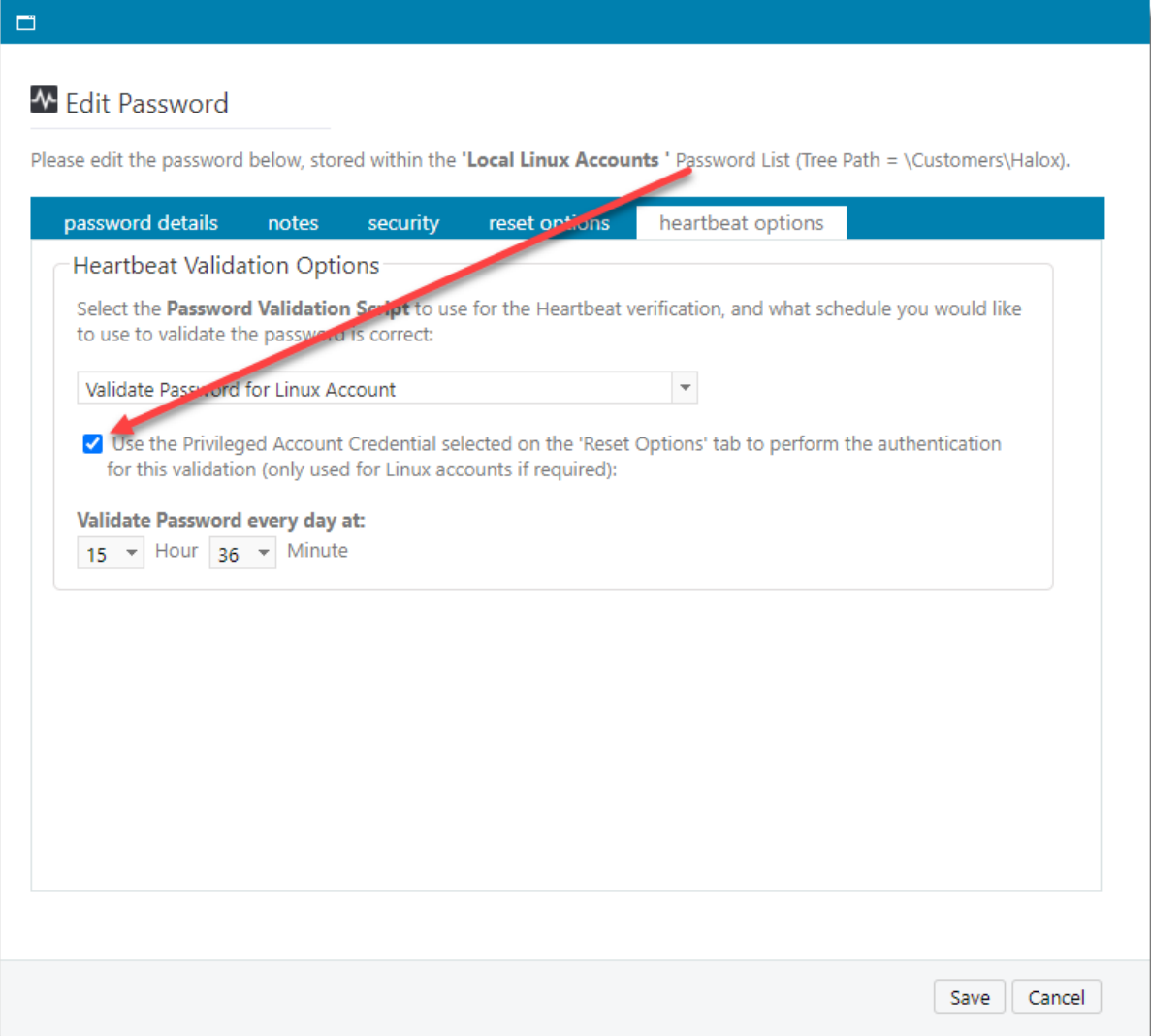
- Open the Sudoers file with visudo using the following command:

**Sudo visudo -f /etc/sudoers**

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

```
## Enable sudo rootpw for Passwordstate Privileged Account
```

```
Defaults:<username> rootpw
```



The screenshot shows the 'Edit Password' interface in Passwordstate. The page title is 'Edit Password'. Below the title, it says 'Please edit the password below, stored within the 'Local Linux Accounts' Password List (Tree Path = \Customers\Halox)'. There are five tabs: 'password details', 'notes', 'security', 'reset options', and 'heartbeat options'. The 'heartbeat options' tab is active. Under this tab, there is a section titled 'Heartbeat Validation Options'. It contains a dropdown menu with 'Validate Password for Linux Account' selected. Below the dropdown is a checked checkbox with the text 'Use the Privileged Account Credential selected on the 'Reset Options' tab to perform the authentication for this validation (only used for Linux accounts if required):'. At the bottom of this section, it says 'Validate Password every day at:' followed by two dropdown menus: '15' for 'Hour' and '36' for 'Minute'. At the bottom right of the interface are 'Save' and 'Cancel' buttons. A red arrow points from the top right towards the dropdown menu.

#### 2.1.1.2.3 Edit Password

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


Windows Admin Accounts

Actions	Title	Domain or Host	User Name	Description
▼	appserver01\admin1	appserver01.sanddomain.com	admin1	Local Administrator Account on appserver01.sanddomain.com
▼	appserver01\Administrator	appserver01.sanddomain.com	Administrator	Local Administrator Account on appserver01.sanddomain.com
▼	appserver01\marlee	appserver01.sanddomain.com	marlee	Local Administrator Account on appserver01.sanddomain.com
▼	desktop10\marlee	desktop10.sanddomain.com	marlee	Local Administrator Account on desktop10.sanddomain.com
▼	desktop10\TestUser1	desktop10.sanddomain.com	TestUser1	Local Administrator Account on desktop10.sanddomain.com
▼	desktop10\TestUser2	desktop10.sanddomain.com	TestUser2	Local Administrator Account on desktop10.sanddomain.com

Once the Edit Password screen is open, each of the fields and options on the Tabs is similar to the [Add Password](#) screen.

### Password Details tab

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

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

**Edit Password**

Please edit the password below, stored within the **'Active Directory Accounts'** Password List (Tree Path = \Infrastructure).

password details | notes | security | **reset options** | heartbeat options

Title \* James Farthing

Managed Account  Enabled for Resets  Enabled for Heartbeat

Account Type Active Directory

Domain halox

UserName farja

Description

Expiry Date 13/12/2018

Password Generator SQL Password Generator

Password \* .....

Confirm Password \* .....

Password Strength ★★★★★ Compliance Strength ★★★★★

Strength Status: 1 more characters

Reset Tasks (1)  Added via Discovery  Compliance Mandatory  Prevent Bad Password

Password Reset tasks will be queued if Password updated.

Save Cancel

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

☰

### 🔑 Edit Password

Please edit the password below, stored within the **'Test Password List'** Password List (Tree Path = \Business Systems).

password details
notes
security

Title \*

Test Password

📍

UserName

msand

👤

Description

Expiry Date

📅

---

Password Generator

Default Password Generator

⚙️

Password \*

.....

🔑

👤

🔍

📱

abc

✅

Confirm Password \*

.....

Password Strength

★★★★★

Compliance Strength

★★★★★

Strength Status: Excellent password strength

---

🔄
Reset Tasks (0)

❌
Added via Discovery

❌
Compliance Mandatory

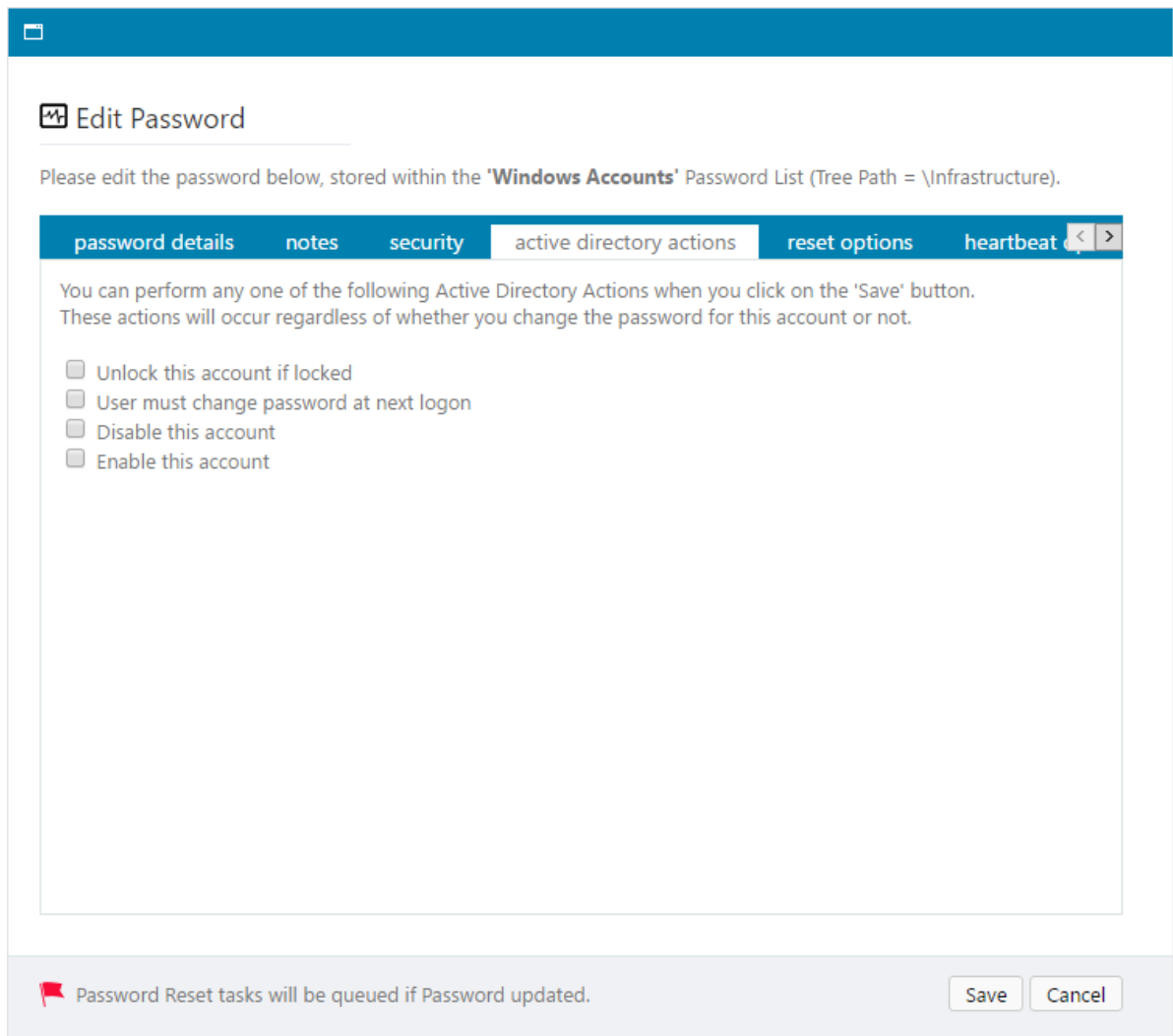
✅
Prevent Bad Password

Save

Cancel

## Active Directory Actions tab

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



## Reset Options and Heartbeat Options Tabs

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

Options available are:

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

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

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

The screenshot shows the 'Edit Password' interface with the following elements:

- Header:** 'Edit Password' with a warning icon.
- Instruction:** 'Please edit the password below, stored within the **Active Directory Accounts** Password List (Tree Path = \Infrastructure).'
- Navigation Tabs:** 'password details', 'notes', 'security', 'reset options', 'heartbeat options'. The 'reset options' tab is active.
- Section: Password Reset Script and Privileged Account Credentials**
  - Text: 'Please select the appropriate Password Reset Script, and Privileged Account Credential, in order to perform the password reset.'
  - Field: 'Password Reset Script' with a dropdown menu set to 'Reset Active Directory Password'.
  - Field: 'Privileged Account' with a dropdown menu set to 'Update Active Directory Account Passwords'.
  - Warning box: '- Not all Reset Scripts require a Privileged Account. See KB Article in menu Help -> User Manual. - Active Directory Accounts do not require you to select a Reset Script.'
- Section: Password Reset Schedule**
  - Checked checkbox: 'When this Password expires, Auto-Generate a new one and perform any reset tasks at the time of:'
  - Fields: '00' Hour, '00' Minute, and add '45' Day(s) to the Expiry Date.
- Footer:** A warning message 'Password Reset tasks will be queued if Password updated.' and 'Save' and 'Cancel' buttons.

**Edit Password**

Please edit the password below, stored within the **'Active Directory Accounts'** Password List (Tree Path = \Infrastructure).

password details notes security active directory actions reset options **heartbeat options**

**Heartbeat Validation Options**

Select the **Password Validation Script** to use for the Heartbeat verification, and what schedule you would like to use to validate the password is correct.

Validate Password for Active Directory Account

Use the Privileged Account Credential selected on the 'Reset Options' tab to perform the authentication for this validation (only used for Linux root accounts if required):

**Validate Password every day at:**

09 Hour 40 Minute

Password Reset tasks will be queued if Password updated. Save Cancel

#### 2.1.1.2.4 Upload Documents

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

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

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



Documents for Password List 'Servers'

Actions	Document Name	Description	Modified	Modified By	File Size
▼	<a href="#">Installation_Instructions.pdf</a>	Passwordstate Installation Instructions	20/06/2013	Mark Sandford	1.1 MB
▼	<a href="#">Preinstallation_Checklist.pdf</a>	Passwordstate Preinstallation Checklist	20/06/2013	Mark Sandford	381 KB
▼	<a href="#">Upgrade_Instructions.docx</a>	Upgrade Instructions	20/06/2013	Mark Sandford	39 KB

[Return to Passwords](#) | 
 [Add Document](#) | 
 [Toggle ID Column Visibility](#) | 
 Grid Layout Actions...

2.1.1.2.5 Email Permalinks

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

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

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

☐

**✉ Copy or Email Password Permalink**

To email another user the Password Link details below, please select the user from the drop-down list below.

**Select Email Address \***

**Subject**

**Permalink**

✂ 📄 📋 **B** *I* U |
 ☰ ☰ ☰ ☰ |
 1/3 ☰ ☰ ☰ |
 **A** 🔍 | Verdana | 12px | abc

Hi,

Image Capture is sending you the following Password Permalink.

**Password:** Games Card  
**Password List:** Credit Cards  
**Permalink:** <https://passwordstate9.halox.net/pid=67918>

Passwordstate 9.0 - Secure Password Management.  
<https://passwordstate9.halox.net>

🎨 Design 🔍 Preview

## 2.1.1.2.6 Password Actions

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

<a href="#">Check-In Password</a>	Allows a user to check a record back in, after they have checked it out for exclusive use
<a href="#">Copy or Email Password Permalink</a>	Similar to Permalinks for Password Lists, you can also copy or email Permalinks for individual Password records
<a href="#">Copy or Move to Different Password List</a>	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
<a href="#">Filter Recent Activity on this Record</a>	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
<a href="#">Link Account to Multiple Web Site URLs</a>	If using our Chrome or Browser extensions, and you use the same account to login to multiple different web sites (normally internal sites), then you can use this feature to achieve that.
Remote Session Launcher with these Credentials	This menu will be available if the record is a local account for a Host record, and you have been give access to use the Remote Session Launcher feature
Send Account Heartbeat Request	If the password record has the option enabled to perform account Heartbeats, to validate the password is correct against the remote Host or Active Directory, then you can use this menu option to perform the validation real-time.
<a href="#">Send Self Destruct Message</a>	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
<a href="#">View &amp; Compare History of Changes</a>	Every change made to a Password record retains a history of the change. By clicking on 'View & Compare History of Changes' you can visually compare what has changed, at what time, and by who.
<a href="#">View Documents</a>	You can upload one or more documents/attachments and associate them with individual Password records
<a href="#">View Individual Password Permissions</a>	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 browses 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
<a href="#">View Password Reset Dependencies</a>	Shows any password reset dependencies which are linked to the selected Password record. Typically these would be Windows Services, IIS Application Pools and Scheduled Tasks.
Unlink & Delete Password	Allows you to unlink and delete a linked password record - it will be moved to the recycle bin
Unlink Password	Allows you to unlink a linked password record

2.1.1.2.6.1 Check-In Password

When a password is configured 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.

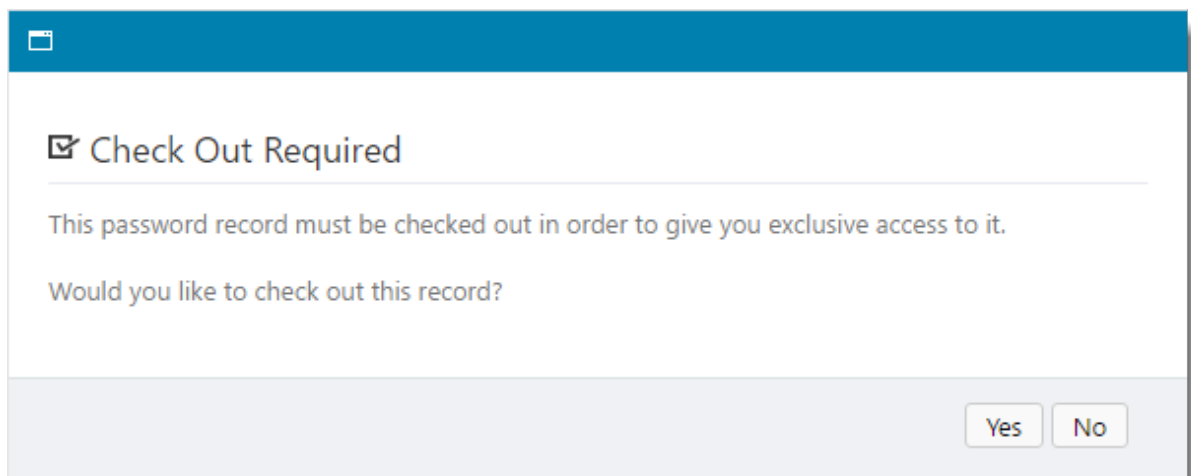
Search Screen Options

### Linux Accounts

Actions	Title	User Name	Description	Password	Passwo
	Administrator on Hyperv1	administrator		*****	☆☆
	marlee on CentOS	marlee		*****	☆☆
	marlee on Marks-lmac	marlee		*****	☆☆
	root	root	Root account for all machines	***** Requires Checkout	☆☆
	root on LinRedhatTest1	root	Updated today.	*****	☆☆
	test1	test1	test1 on linredhatest1	*****	☆☆
	TestHistory	TestHistory		*****	☆☆
	tsand	tsand	tsand Local Account	*****	☆☆

Add | Import | Documents (1) | Permalink | Grid Layout Actions... | List Administrator Actions...

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



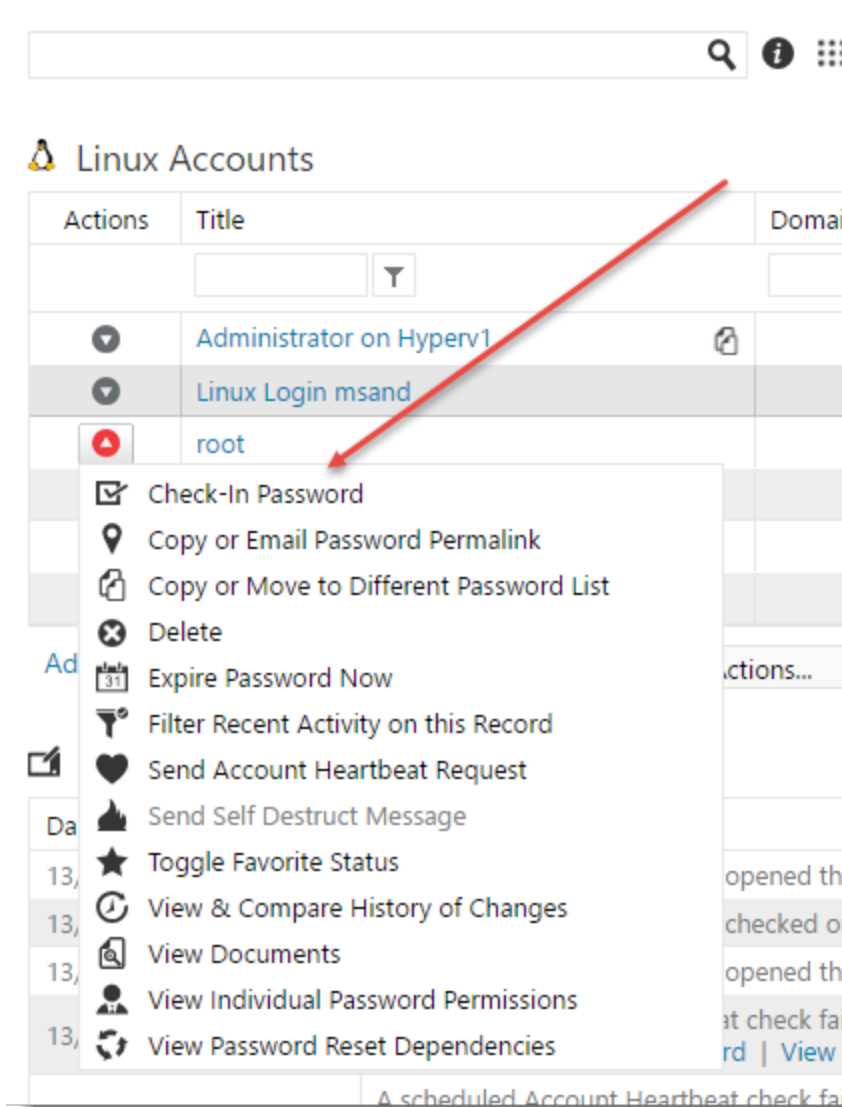
When checked out, it also indicates this in the password grid, and no other users can access the password until it is checked back in.

### Linux Accounts

Actions	Title	User Name	Description	Password	Passwo
	Administrator on Hyperv1	administrator		*****	☆☆
	marlee on CentOS	marlee		*****	☆☆
	marlee on Marks-lmac	marlee		*****	☆☆
	root	root	Root account for all machines	***** Checked Out	☆☆
	root on LinRedhatTest1	root	Updated today.	*****	☆☆
	test1	test1	test1 on linredhatest1	*****	☆☆
	TestHistory	TestHistory		*****	☆☆
	tsand	tsand	tsand Local Account	*****	☆☆

Add | Import | Documents (1) | Permalink | Grid Layout Actions... | List Administrator Actions...

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



### Security Administrator Checking Back in Password record

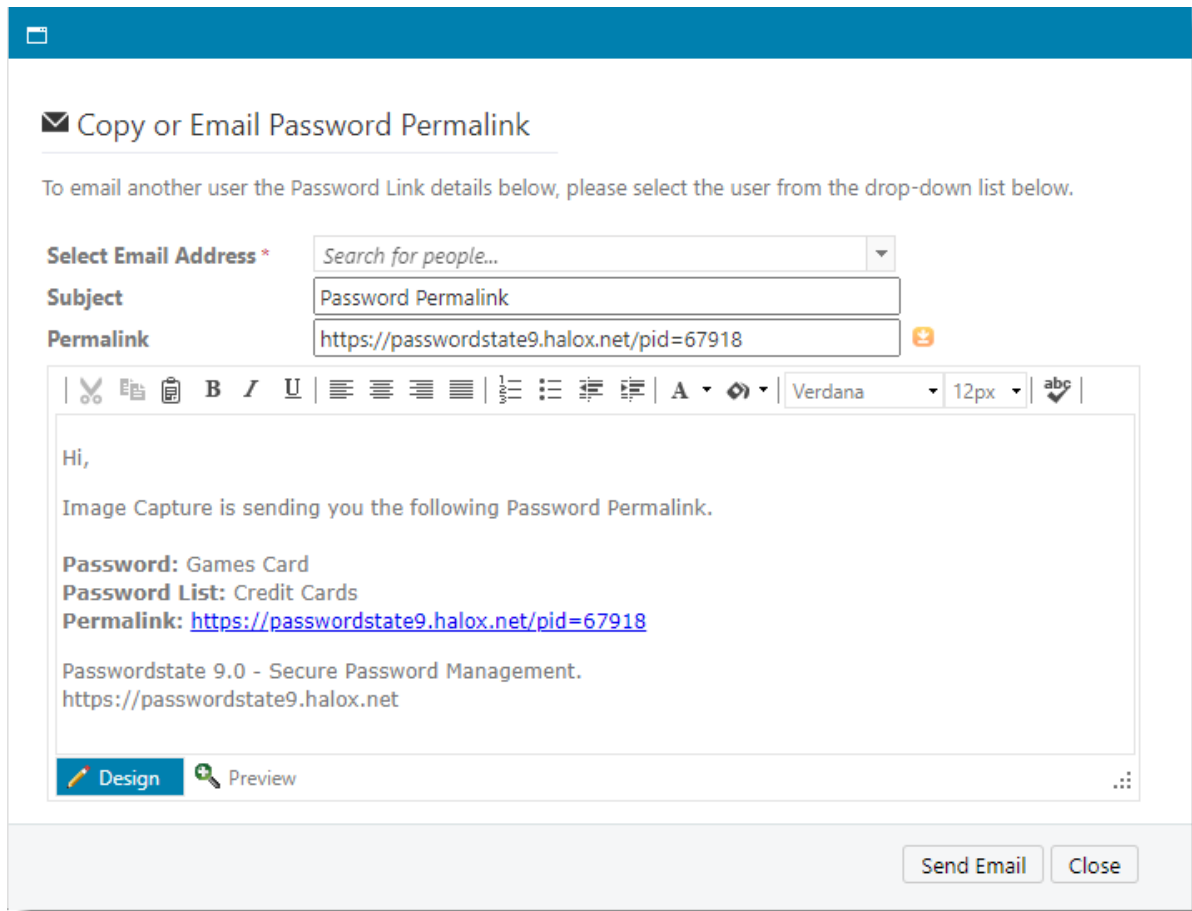
If the user who checked a record out is unavailable to check a record back in, Security Administrators can also check the record back in for the user.

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

#### 2.1.1.2.6.2 Copy or Email Password Permalink

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

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



#### 2.1.1.2.6.3 Copy or Move to Different Password List


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

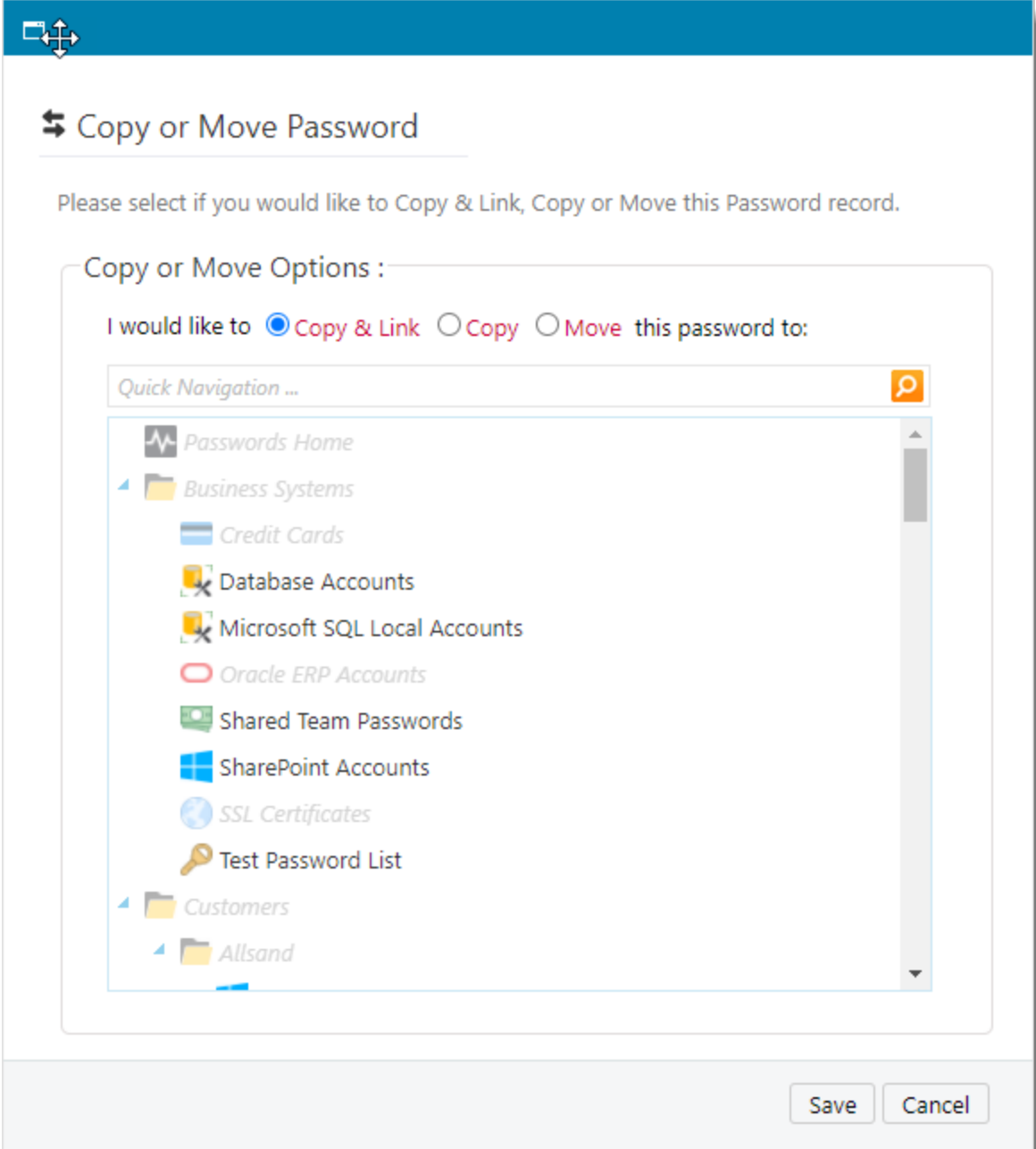
- You need at least Modify rights to the Destination Password List
- The Destination Password List must have the same selected fields as the Source Password List
- For security reasons, you also cannot move a password in a Shared Password List, into a Private Password List
- And you cannot copy records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

If a Password List is grayed out and disabled on the pop-up windows below, then one of the three restrictions above would be the cause. Hovering over the disabled item, should provide you a Tooltip with the specific reason why

Copy & Link will create a duplicate record in the Destination Password List, and all linked records will be kept in sync when any changes are made to either of the records. When a Password record is linked, you will see a linked chain icon next to the Title, similar to this image



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



**Copy or Move Password**

Please select if you would like to Copy & Link, Copy or Move this Password record.

**Copy or Move Options :**

I would like to  Copy & Link  Copy  Move this password to:

Quick Navigation ...

- Passwords Home
- Business Systems
  - Credit Cards
  - Database Accounts
  - Microsoft SQL Local Accounts
  - Oracle ERP Accounts
  - Shared Team Passwords
  - SharePoint Accounts
  - SSL Certificates
  - Test Password List
- Customers
  - Allsand

Save Cancel

#### 2.1.1.2.6.4 Filter Recent Activity on this Record

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

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

Recent Activity Clear Filter


Date	Activity	UserID	First Name	Surname	IP Address	Description
1/12/2020 12:58:44 PM	Password Screen Opened	halox\images	Image	Capture	10.0.0.108	Image Capture (halox\images) opened the Edit Password screen for password 'James Farthing' (Active Directory Accounts) - viewing the value of the password is possible on this screen. (Title = James Farthing, Username = farja). <a href="#">View Password</a>   <a href="#">View History</a>
1/12/2020 12:53:38 PM	Password Screen Opened	halox\images	Image	Capture	10.0.0.108	Image Capture (halox\images) opened the Edit Password screen for password 'James Farthing' (Active Directory Accounts) - viewing the value of the password is possible on this screen. (Title = James Farthing, Username = farja). <a href="#">View Password</a>   <a href="#">View History</a>
1/12/2020 12:00:31 PM	Password Validation Failed	WindowsService	Windows Service	Account	10.0.0.125	A scheduled Account Heartbeat check failed to validate the password for the Active Directory account halox\farja (Infrastructure\Active Directory Accounts). Error = Failed to validate the Active Directory password for account 'halox\farja' - Username or Password is incorrect, or account is locked/disabled. <a href="#">View Password</a>   <a href="#">View History</a>
19/11/2020 12:00:30 PM	Password Validation Failed	WindowsService	Windows Service	Account	10.0.0.91	A scheduled Account Heartbeat check failed to validate the password for the Active Directory account halox\farja (Infrastructure\Active Directory Accounts). Error = Failed to validate the Active Directory password for account 'halox\farja' - Username or Password is incorrect, or account is locked/disabled. <a href="#">View Password</a>   <a href="#">View History</a>
18/11/2020 12:00:11 PM	Password Validation Failed	WindowsService	Windows Service	Account	10.0.0.91	A scheduled Account Heartbeat check failed to validate the password for the Active Directory account halox\farja (Infrastructure\Active Directory Accounts). Error = Failed to validate the Active Directory password for account 'halox\farja' - Username or Password is incorrect, or account is locked/disabled. <a href="#">View Password</a>   <a href="#">View History</a>

Change page: ◀ ▶ ⏪ ⏩ Page 1 of 2, Items 1 to 5 of 10

#### 2.1.1.2.6.5 Link Account to Multiple Web Site URLs


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

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

 Link Account to Multiple Web Site URLs

By listing additional URLs below, you can be logging into multiple URLs using the same Username and Password value from the parent record with the Browser Extensions for Passwordstate - for Chrome and Firefox.

Linked URL

Actions	URL	Username Field ID	Password Field ID
	<a href="http://win2k19apps1:8090">http://win2k19apps1:8090</a>	os_username	os_password

Grid Layout Actions... ▼

#### 2.1.1.2.6.6 Send Self Destruct Message

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

Creating a Self Destruct message is a three step process:

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

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



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

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

### Send Self Destruct Message

To send a Self Destruct Message to another person, please specify details as appropriate for each stage of the Wizard below.

Message Content | Email to Recipient | Passphrase Protection

Enter the contents of the Self Destruct message you want the recipient to read.

**PASSWORD DETAILS**  
Title: 12.28.229.178\atsadmin  
HostName:  
Username: atsadmin  
Description: SonicWALL Account on 12.28.229.178  
AccountType: SonicWALL  
Password: [Updated When Message Sent - Do Not Alter]  
Expiry Date: 19/08/2018

Automatically self-destruct this message if not viewed in: 3 days

Allow the self-destruct message to be viewed (x) times: Once

Cancel | Next

Message Content **Email to Recipient** Passphrase Protection

If you want Passwordstate to send the Self Destruct Message Email and URL, please select the Recipient below. Otherwise, please click the Next button.

Select Recipient: Click Studios (support@clickstudios.com.au)

Subject: Passwordstate - Self Destruct Message

Hi,

You've been sent a Self Destruct Message from Passwordstate, and you can view the detail of the message by clicking the URL below.

URL: <https://passwordstate9appserver.halox.net/selfdestruct/?id=902af4360fc64bb1b43f9b6fb9968e44>

This message will expire [ExpirePeriod] from the time of this email being sent.

Passwordstate 9.0 - Secure Password Management.  
<https://passwordstate9.halox.net>

Design Preview

Cancel Previous Next

### Send Self Destruct Message

To send a Self Destruct Message to another person, please specify details as appropriate for each stage of the Wizard below.

Message Content Email to Recipient **Passphrase Protection**

To protect access to your Self Destruct message with the user of a Passphrase, please specify this below - you must inform your recipient the value of this Passphrase before they can read the message.

Passphrase Protection: .....


Cancel Previous Send

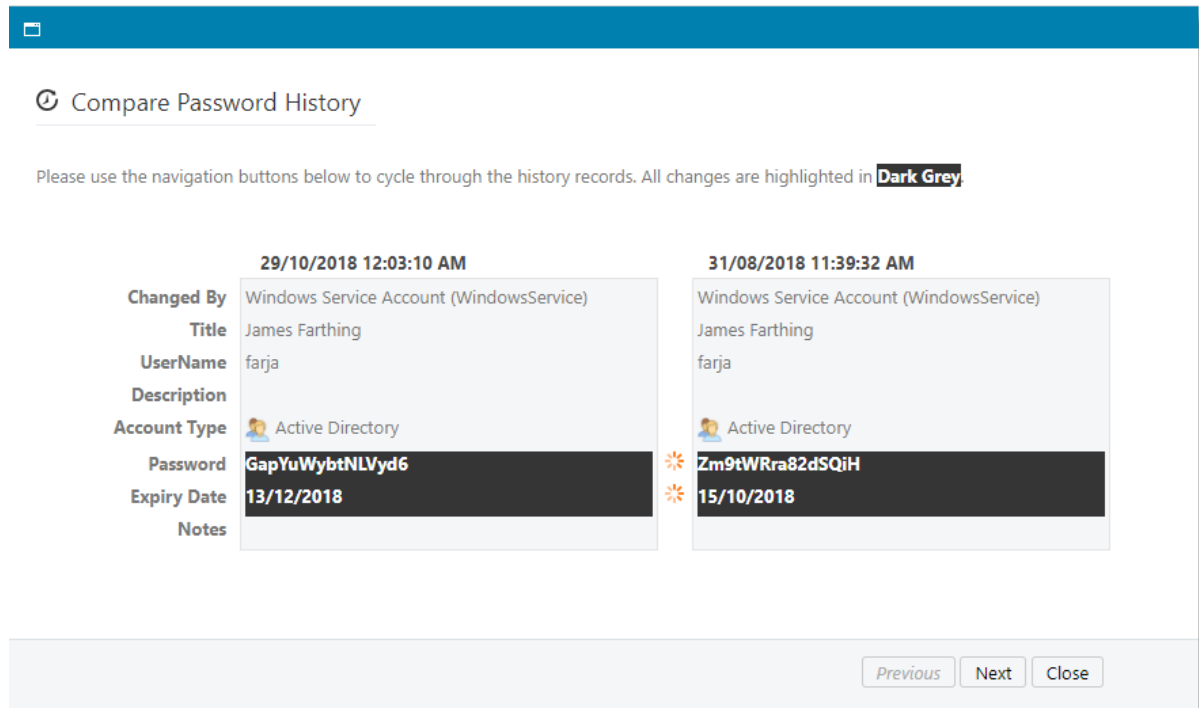
#### 2.1.1.2.6.7 View & Compare History of Changes

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

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

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

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



2.1.1.2.6.8 View Documents

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

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

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

## Documents for Password 'Splunk Account'

Actions	Document Name	Description	Modified	Modified By	File Size
	passwordstate.key	Test Key 2	28/06/2018 9:51:00 AM		90
	pwdstateaes.key	Encryption Key	28/06/2018 8:18:00 AM		296
	QueryADGroup.txt.txt		28/06/2018 8:20:00 AM		4 KB

Return to Passwords | Add Document | Toggle ID Column Visibility | Grid Layout Actions...

## 2.1.1.2.6.9 View Individual Password Permissions

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

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

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

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

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

## Password Permissions

To grant additional access simply click on the 'Grant Permissions' button, or to modify existing permissions click on the appropriate 'Actions' drop-down menu.

## James Farthing (Active Directory Accounts)

User Account Local Security Group Active Directory Security Group

Actions	User or Security Group	Site Location	View	Modify	Expires	One-Time Access
	Adam Finley	Internal				
	Zachary Edkins	Internal				

Return to Passwords Page | Grant New Permissions | Grid Layout Actions...

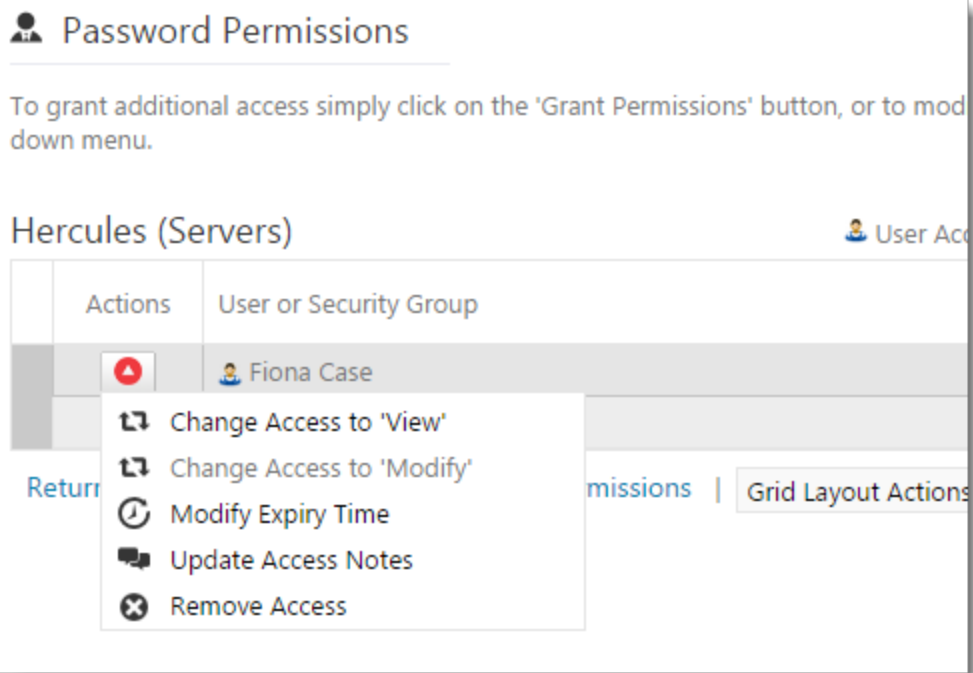
From the 'View Individual Password Permissions' screen, you have the following features available:

## Password Permission Actions

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

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

- Or remove the access altogether



## Grant New Permissions

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

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

## Access Permissions

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

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


## Grant New Permissions

To grant additional permissions to the '**Administrator on Hyperv1 (Linux Accounts)**' Password, simply click on the three **Tabs** below to specify appropriate permissions and/or settings.

access permissions
time based access

Search for an appropriate user or security group (use \* to search for all).

Site Location :

Search :  

Search For :  User  Security Group

**Search Results**

**View Permissions**

>>  
<<

**Modify Permissions**

>>  
<<

**Administrator Permissions**

>>  
<<

**Reason for Access**

Status: Save Cancel

## 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.

## Grant New Permissions

To grant additional permissions to the **'Administrator on Hyperv1 (Linux Accounts)'** Password, simply click on the three **Tabs** below to specify appropriate permissions and/or settings.



**access permissions** | **time based access**

To apply time based access to the selected Password, please use the appropriate options below.


**Access Expires :** 

Never

In: Days:  Hours:  Minutes:


At: Date:   Time:  

Automatically generate new Password when this access expires (uses the Password List's Password Generator options, and will execute any associated Password Reset Tasks if there are any)

**Access Expires when Password Changes :** 

If you would like to have the access removed on next Password change, please select this checkbox.

Remove Access on Next Password Change

**One-Time Access :** 

If you only require the user or security group members to access this password once, please check the option below.

Provide One-Time Access to this Password

Status:

### 2.1.1.2.6.10 View Password Reset Dependencies

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

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

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

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

The screenshot shows the 'Active Directory Accounts' grid. The columns include Actions, Title, Domain or Host, User Name, Account Type, Password, Password Strength, Password Last Updated, Reset Status, Heartbeat Status, Dependencies, Managed, and Expiry Date. The 'HALOX/schedtasks' account is highlighted, showing 1 dependency. The left sidebar contains various actions, with 'View Password Reset Dependencies' selected.

Then you click on the 'Add Dependency' button.

The screenshot shows the 'Password Reset Dependencies' dialog. Below the dialog is a table with the following data:

Actions	Order	Host Name	Username	Script Name	Dependency Type	Dependency Name	Reset Status	Managed Host	Privileged Account Credentials
		10.0.0.3	halox/schedtasks	Reset Windows Scheduled Task Password	Scheduled Task	TestFolder/Run Notepad	Green	Green	

Below the table is a 'Recent Activity' section with a table showing password reset events.

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.



### Add Dependency

To link the password 'HALOX\schedtasks' to a Host and Password Reset Script, please fill in the details below as appropriate.

script and host selection

#### Password Reset or Post Reset Script

Please select the appropriate Password Reset Script.

Password Reset Script \* Reset Windows Service Password

**Note:** If you wish to execute a script Post Reset, you do not need to select a dependency, or Host record below to link it to - you can execute any custom script you like. The order in which scripts are executed can also be changed on the previous screen).

#### Windows Account Dependency

If the selected Reset Script is for one of the Windows Account 'Dependencies' types below, enter appropriate details here.

Dependency Name My Custom Windows Service  
Name of the Windows Service (Display Name), Scheduled Task, IIS Application Pool or COM+ Component

Dependency Type 
 Ignore
  Windows Service
  IIS Application Pool
  Scheduled Task
  COM+ Component

#### Link to Host(s)

If you want to execute the script above against one or more hosts, please select them below.

Host Name : web2    Host Type : All Host Types    Operating System : -- Select OS --    Search

Database Server Type -- Select Database Type --

#### Hosts Search Results

🖥 win2k12web2.halox.net

#### Applied to Host(s)



>>  
 <<


Save
Cancel

#### 2.1.1.2.7 List Administrator Actions

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

A summary of the features are:

Bulk Delete Selected Passwords	Use in conjunction with the 'Toggle Visibility of 'Delete Checkboxes'', it is possible to delete more than one password record at a time
Bulk Permissions for Individual Passwords	Allows you to apply permissions for a User's Account, or a Security Group, to multiple individual passwords records at once
<a href="#">Bulk Update Passwords</a>	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
<a href="#">Bulk Update Password Reset Options</a>	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
<a href="#">Edit Password List Details</a>	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
<a href="#">Save Password List as Template</a>	Allows you to save all the settings and chosen fields as a Template, which can then be used for the creation or management of other Password Lists
Toggle Visibility of 'Delete Checkboxes	When you select this menu item, checkboxes will appear next to the 'Title' field in the grid. You can then select any number of records, and then use the 'Bulk Delete Selected Passwords' menu item to delete more than one record at a time
<a href="#">Toggle Visibility of Web API IDs</a>	Allows you to see various ID fields required for the Passwordstate API
<a href="#">View Password List Permissions</a>	Allows you to view existing permissions applied to this Password List, modify existing permissions and add new ones
<a href="#">View Recycle Bin</a>	Allows you to see what Password records have been deleted, and gives you the option to restore from the Recycle Bin or permanently delete
Export All Password History	The report will export all history relating to each Password record, including the date data was changed, and who it was changed by.  Note: The password field values will be exported in clear text with this report

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

Web Sites

Actions	Title	User Name	Description	URL
▼	AA - Host Record			
▼	aaaa			
▼	adaptiveinsights			
▼	arubainstanton			
▼	asdasdasd			
▼	auth.services.adobe.com			
▼	bancsabadell			
▼	business.apple.com			
▼	central.arubanetworks			
▼	crowdstrike			

Change page: ⏪ ⏩ ⏴ ⏵

Add | Documents (0) | Permalink | Grid Layout Actions...

Recent Activity ⓘ

Date	Activity	Surname
21/12/2021 2:55:53 PM	Document Viewed	Sandford
21/12/2021 2:06:41 PM	Password Restored	Sandford
21/12/2021 2:06:26 PM	Password Deleted	Sandford
21/12/2021 2:06:12 PM	Password Restored	Sandford
21/12/2021 2:04:55 PM	Password Deleted	Sandford
21/12/2021 11:37:36 AM	Password Screen Opened	Sandford
21/12/2021 11:37:35 AM	Password Updated	Sandford
21/12/2021 11:37:27 AM	Password Screen Opened	Sandford
21/12/2021 11:26:33 AM	Password Viewed	Sandford
21/12/2021 11:26:31 AM	Password Screen Opened	Sandford

Change page: ⏪ ⏩ ⏴ ⏵

List Administrator Actions...

PASSWORD LIST ACTIONS

- Bulk Delete Selected Passwords
- Bulk Permissions for Individual Passwords
- Bulk Update Passwords
- Bulk Update Password Reset Options
- Convert to Shared Password List
- Delete Password List
- Edit Password List Properties
- Save Password List as Template
- Toggle Visibility of Delete Checkboxes
- Toggle Visibility of Web API IDs
- View Password List Permissions
- View Recycle Bin (2)

EXPORT

- Export All Password History
- Export All Passwords
- Enumerated Permissions Report
- Have I Been Pwned Compromises
- Password Strength Report
- Standard Permissions Report

#### 2.1.1.2.7.1 Bulk Update Passwords

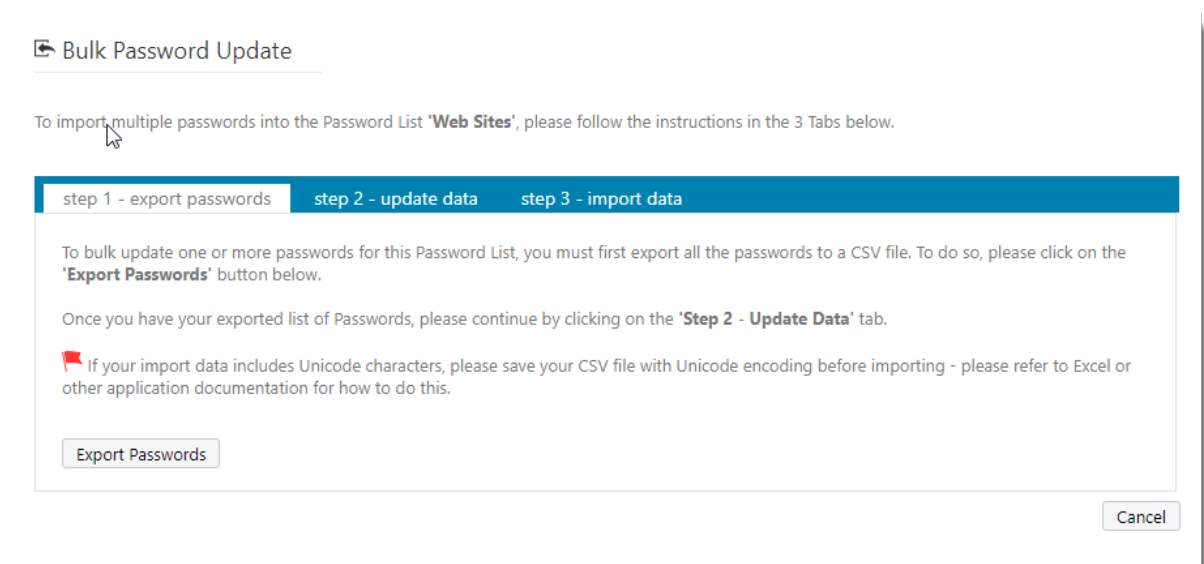
If you have a requirement to update more than one Password record at a time, then you can use the 'Bulk Update Passwords' feature.

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.

- 🚩 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

## Bulk Password Update

To import multiple passwords into the Password List '**Web Sites**', please follow the instructions in the 3 Tabs below.

step 1 - export passwords
step 2 - update data
step 3 - import data

When updating data in the CSV file, there are a few rules to consider:

1. Consider the Column requirements below
2. Do not modify the PasswordID values in any way

When ready, please click on the '**Step 3 - Import Data**' tab.


Column Name	Field Type	Size (Max)	Required
Title	String	255	✓
UserName	String	255	✗
Description	String	255	✗
AccountType	String	NA	✗
Notes	String	NA	✗
URL	String	1000	✗
Password	Password	NA	✓
ExpiryDate	Date	NA	✗
WebUser_ID	String	200	✗
WebPassword_ID	String	200	✗


**Please note:** As this Password List has a column called 'AccountType', the possible values you can enter for it are displayed in this Listbox.

- Available Account Types -

## 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.

### Bulk Password Update

To import multiple passwords into the Password List 'Servers', please follow the instructions in the 3 Tabs below.

step 1 - export passwords
step 2 - update data
step 3 - import data

Now you are ready to import your updated csv file. To do so, please select your CSV file by clicking the 'Select' button, then click on the 'Import Passwords' button.

**Please Note:**

1. Please ensure your data does not contain any commas
2. CSV file must be under 100MB in size.

**Email all users who have access to this Password List informing them of the updated records:**

Yes  No

#### 2.1.1.2.7.2 Bulk Update Password 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

### Bulk Update Password Reset Options

To change Password Reset Options for one or more password records, please search/filter for the passwords to be changed, and then select options on each of the tabs as appropriate.

search/filter for passwords
fields to update
reset options
heartbeat options

Search/Filter for password records you wish to change Password Reset Settings for.

**Search Criteria**

Password Record Search	Account Type	Expiry Date From	Expiry Date To	Privileged Account	
<input type="text"/>	<input type="text" value="- Select Account Type -"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="Search"/> <input type="button" value="Clear"/>

Managed Account (Enabled for Resets)

Title	User Name	Account Type	Description	Expiry Date
Domain		Active Directory		26/03/2017
Splunk Account	splunkacctn@halox.net	Active Directory	Used for SIEM	15/07/2017
Tasks Account	tasksacctn	Active Directory		21/09/2017

### Bulk Update Password Reset Options

To change Password Reset Options for one or more password records, please search/filter for the passwords to be changed, and then select options on each of the tabs as appropriate.

search/filter for passwords
fields to update
reset options
heartbeat options

Select which of the following fields below you would like to change for the selected password records.

**Fields To Update**

Account Type ▼  
 Expiry Date 🗑️  
 Managed Account  Enable Password Resets option for these account(s)  
 Account Heartbeat  Enable Account Heartbeat option for these account(s)

### Bulk Update Password Reset Options

To change Password Reset Options for one or more password records, please search/filter for the passwords to be changed, and then select options on each of the tabs as appropriate.

search/filter for passwords
fields to update
reset options
heartbeat options

Select which Password Reset Options below you would like to change for the selected password records.

**Change Password Reset Script and Privileged Account Credentials**

Please select the appropriate Password Reset Script, and Privileged Account Credential, in order to perform the password reset.

Password Reset Script ▼  
 Privileged Account ▼

**Change Password Reset Schedule**

When this Password expires, Auto-Generate a new one and perform any reset tasks at the time of:  
00 Hour 00 Minute, and add 90 Days to the Expiry Date

### Bulk Update Password Reset Options

To change Password Reset Options for one or more password records, please search/filter for the passwords to be changed, and then select options on each of the tabs as appropriate.

search/filter for passwords
fields to update
reset options
heartbeat options

Select which Account Heartbeat Options below you would like to change for the selected password records.

**Change Heartbeat Validation Options**


Select the **Password Validation Script** to use for the Heartbeat verification, and what schedule you would like to use to validate the password is correct:

- Select Validation Script - ▼

**Validate Password every day at:**  
00 Hour 00 Minute

#### 2.1.1.2.7.3 Edit Password List Properties

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


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

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



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



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

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

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


## Password List Details Section

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

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



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



### Password List Details



Site Location  Internal


Password List \*


Description

Image   

Password Strength Policy \*   

Password Generator Policy \*   

Code Page \*  

Additional Authentication \*  

## Password List Settings Section


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









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

Disable Email Notifications for this Password List	Disable email notifications for this specific Password List i.e. Password Added, Updated, Deleted, Copied to Clipboard, etc
Force the use of the selected Password Generator Policy	With this option set, users cannot enter their own passwords manually - they must use the Password Generator button to generate new passwords
Hide Passwords from users with the following permissions	You can hide passwords, and disable copy to clipboard, based on permissions the user has to the Password List i.e. View, Modify or Admin
Popup the Guide on each access to this Password List	If you would like the 'Guide' to be displayed every time a user accesses this Password List, you can select this option
Prevent Non-Admin users from Dragging and Dropping	You can select this option to minimize who can drag and drop the Password List around in the <a href="#">Navigation Tree</a>
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: <ul style="list-style-type: none"> <li>• Unlock this account if locked</li> <li>• User must change password at next logon</li> <li>• Disable this account</li> <li>• Enable this account</li> </ul>
---	---


### Password List Settings

 This is a Shared Password List

- Enable Password Resets - allows password resetting with other systems 
- Enable One-Time Password Generation 
- Allow Password List to be Exported 
- Time Based Access Mandatory 
- Multiple Approvers Mandatory - a total of  approver(s) are required for this List
- Prevent Password reuse for the last  passwords
- Disable Email Notifications for this Password List
- Force the use of the selected Password Generator Policy
- Hide Passwords from users with the following permissions
- Popup the Guide on each access to this Password List
- Prevent Non-Admin users from Dragging and Dropping this Password List 
- Prevent saving of Password records if a 'Bad' password is detected 
- Users must first specify a reason why they need to view, edit or copy passwords
- Prevent Non-Admin users from manually changing values in Expiry Date fields
- Set the Expiry Date to Current Date +  Days when adding new passwords 
- Reset Expiry Date to Current Date +  Days when manually updating passwords
- Additional Authentication only required once per session 
- Show 'Active Directory Actions' options for Active Directory accounts

## Copy Details & Settings from Section

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

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

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

### Copy Details & Settings From

Copying a Template or another Password List's settings will populate all fields/settings on this screen, except for any API Keys.

- Copy Settings From Template -

-- Search and Copy Settings from Password List --

Link this Password List to the selected Template.

**Note:** If copying settings from a Password List or Template causes the Field Type to change for any Generic Fields (on the Customize Fields tab), then these values will be cleared in the database when you click on the 'Save' button.

## 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.

### Copy Permissions From


If you would like to copy permissions from an existing Template or Password List, please select the appropriate option below.

- Copy Permissions from Template -

-- Search and Copy Settings from Password List --

## Password List Permission Settings

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

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

#### Password List Permission Settings


If using the Advanced Permission Model, you can prevent permission propagation to this Password List with the setting below.


Disable Inheritance of any upper level folder permission propagation

## Default Password Reset Schedule

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

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

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

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

#### Default Password Reset Schedule

Please specify the default settings for 'Reset Options' when new records are added to this Password List.

Enable the the Password Reset Schedule for the account, and schedule the reset at a random time between the two time slots below:

**Start Time**

02 ▾ Hour 00 ▾ Minute

**Finish Time**


03 ▾ Hour 45 ▾ Minute

And when the account expires, add  **Month(s)** ▾ to the Expiry Date.


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


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

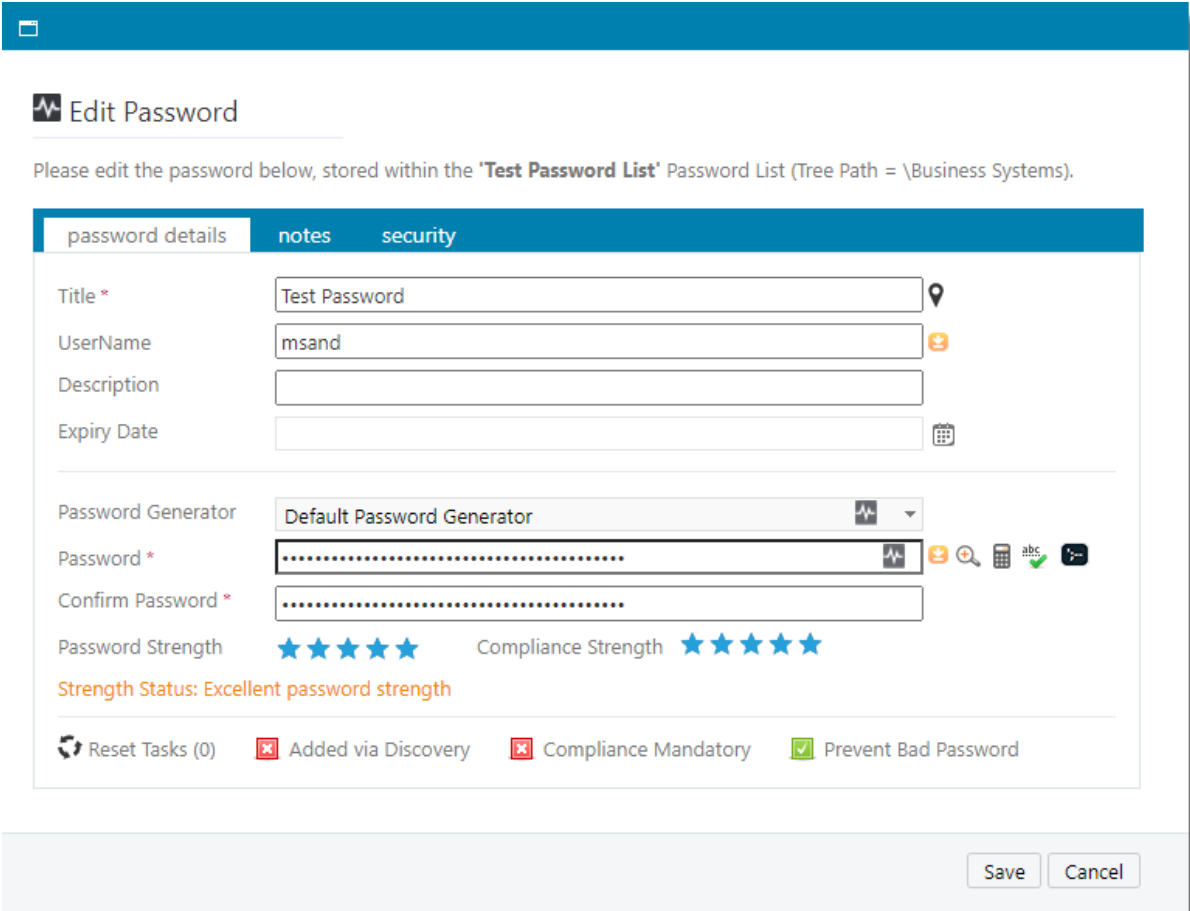
Title	This is the one mandatory field you must specify, and it's intended as a brief description as to what the Password record relates to
Username	If you must specify a username to authenticate against the end resource, this is the field you would use i.e. Username and Password to authentication to a web site, or network switch, etc
Description	A longer description as to what the Password record relates to
Account Type	Account Type can be used to visually show the type of account the record belongs to i.e. a switch, a firewall, and web login, etc.
URL	If you would like to associate as web sites URL with the Password record, then you can use this field. You can launch the URL by clicking on it when shown in the Passwords grid
Password	The actual password itself
Password Strength	You cannot enter any data for the Password Strength field - it's a graphical representation of how strong the password is, based on the selected Password Strength Policy
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)	<p>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:</p> <ul style="list-style-type: none"> <li>• Text Field      A single line text field</li> <li>• Free Text Field   Multiple line text field</li> <li>• Password      An encrypted password field</li> <li>• Select List      A vertical drop-down list of predefined values</li> <li>• Radio Buttons    A horizontal checklist of predefined values</li> <li>• Date Picker      A popup calendar style control for picking date values</li> <li>• URL Field      Allows you to click on the URL in the Grid view and launch the web site</li> </ul>

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

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

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


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




**Edit Password**


Please edit the password below, stored within the **'Test Password List'** Password List (Tree Path = \Business Systems).


password details | notes | security








Title \*  

UserName  



Description

Expiry Date  





Password Generator  

Password \*        

Confirm Password \*

Password Strength  Compliance Strength 

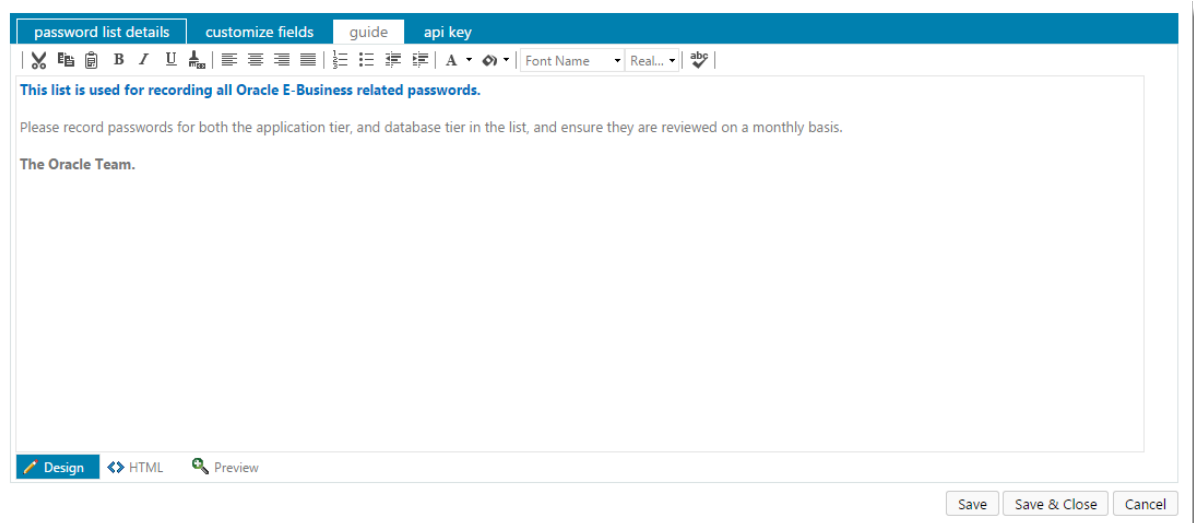
Strength Status: Excellent password strength

 Reset Tasks (0)  Added via Discovery  Compliance Mandatory  Prevent Bad Password

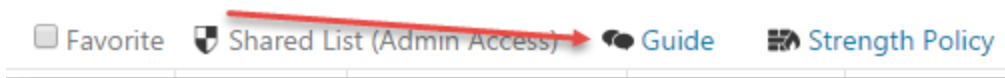
Save Cancel

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

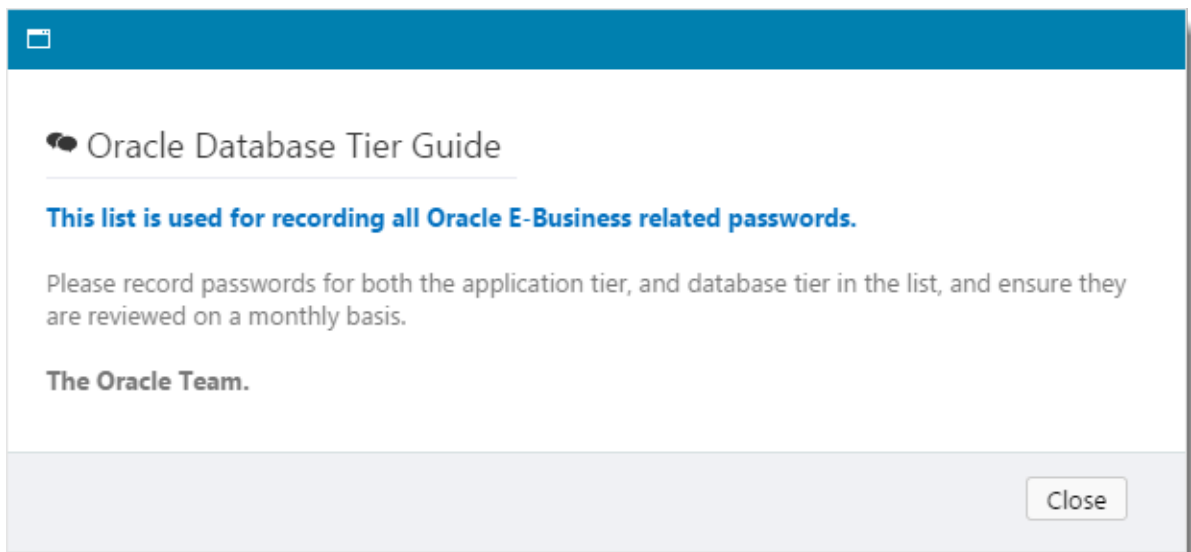




Once you have specified the required detail in the Guide tab, your users can view the guide by clicking on the 'View Guide' button at the top right-hand side of the Password Grid.



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



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


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


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

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

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

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

 **Caution:** It is imperative that you take great precautions in ensuring the API Key is not exposed to any users who should not have access. Doing so means they have unrestricted access to all the API function calls relevant to the Password List.

 **Note:** If an API Key is set to restrict retrieving of passwords, then any API Calls which retrieve passwords from more than one Password List at a time will simply ignore Password Lists which have this setting - as opposed to returning a HTTP Status code of '403 Forbidden'

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

⚙️ Edit Password List Properties

To edit the details for the selected Password List, please fill in the details below for each of the various tabs.

password list details
customize fields
guide
api key & settings

If you would like to expose this Password List's data via the Passwordstate API, please generate an API Key and choose the settings as appropriate.

**Please Note:** There is also a Windows Integrated API available as well which does not require the use of API Keys.

**API Key**

Click on the **Generate New Key** button below to create a new API Key for this Password List - this key will give 3rd party programs full access to the contents of this Password List.

API Key  Generate New Key

**Warning:** Resetting the API Key will break existing applications using it.

**API Settings**

Please select which options the API is authorized to perform for this Password List.

- API is authorized to retrieve Passwords
- API is authorized to update Passwords
- API is authorized to add new Passwords
- API is authorized to retrieve Password History
- Return blank Password value instead of actual Password
- Return blank Password value for Generic Fields of Type Password
- Mandatory Hash - Passwords must be returned as a Hash, using the HashType parameter (retrieving and updating passwords)
- Mandatory Reason - A 'Reason' must be specified as to why the API Call is being made, using the Reason Header attribute (retrieving, updating and deleting passwords)

If an API call is made for an 'unauthorized' feature, a HTTP Status code of '403 Forbidden' will be returned.

**API Allowed IP Ranges - Restrict Access if Required**

By default, all IP Addresses are allowed to make calls to the API. If you want to restrict which IP Addresses can make calls to this Password List, you can specify the Allowed IP Ranges below - a HTTP Status Code 403 (Forbidden) will be returned if outside of these IP Range(s).

**Note 1:** You can specify ranges in the format of 192.168.1.\*, 192.168.\*, 192.\*.\*, 192.168.1.1-192.168.2.254, or you can specify individual IP Addresses such as 192.168.1.50

**Note 2:** Specify one IP Address or range per line

**Note 3:** If making a call which retrieves data from multiple Password Lists (System Wide API Key), no data will be returned for this Password List if the IP Address is invalid

**Note 4:** You can also set Allowed IP Ranges for all Password Lists from the screen Administration -> Passwordstate Administration -> System Settings -> Allowed IP Ranges tab

Save
Save & Close
Cancel

2.1.1.2.7.4 Save Password List as Template

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

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

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

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

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

#### Add New Password List Template

To add a new Password List Template, please fill in the details below for each of the 3 tabs.

password list details
customize fields
guide

Please specify Password List settings manually below.

**Password List Details**

Password List \*

Description

Image - Select Image -

Password Strength Policy \* Default Policy

Password Generator Policy \* Default Password Generator

Code Page \* Use Passwordstate Default Code Page

Additional Authentication \* None Required

**Password List Settings**

Enable Password Resets - allows password resetting with other systems

Enable One-Time Password Generation

Allow Password List to be Exported

Time Based Access Mandatory

Disable Inheritance of any upper level folder permission propagation

Multiple Approvers Mandatory - a total of 1 approver(s) are required for this List

Prevent Password reuse for the last 5 passwords

Disable Email Notifications for this Password List

Force the use of the selected Password Generator Policy

Hide Passwords from users with the following permissions

Popup the Guide on each access to this Password List

Prevent Non-Admin users from Dragging and Dropping this Password List

Prevent saving of Password records if a 'Bad' password is detected

Users must first specify a reason why they need to view, edit or copy passwords

Prevent Non-Admin users from manually changing values in Expiry Date fields

Set the Expiry Date to Current Date + 0 Days when adding new passwords

Reset Expiry Date to Current Date + 0 Days when manually updating passwords

Additional Authentication only required once per session

Show 'Active Directory Actions' options for Active Directory accounts

**Default Password Reset Schedule**

! Only applicable if this Password List is enabled for Resets.

Please specify the default settings for 'Reset Options' when new records are added to this Password List.

Enable the the Password Reset Schedule for the account, and schedule the reset at a random time between the two time slots below:

**Start Time** 00 Hour 00 Minute

**Finish Time** 00 Hour 00 Minute

And when the account expires, add 90 Day(s) to the Expiry Date.

Save Cancel

#### 2.1.1.2.7.5 Toggle Visibility of Web API IDs

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

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

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

Active Directory Accounts (PasswordListID = 183) (API Key = b2a57c34fe96d8f36a89c25eb47d4b6c)

Actions	PasswordID	Title	Domain or Host	User Name	Account Type	Password	Password Strength
	70301	asdasdasd	halox	msand2	Active Directory	*****	★★★★★★
	69866	Check File Exists	halox	msand	Active Directory	*****	★★★★★★
	67200	halox\appools	halox	appools	Active Directory	*****	★★★★☆☆
	69274	halox\bship	halox	bship	Active Directory	*****	★★★★☆☆
	69312	halox\pws_write	halox	pws_write	Active Directory	*****	★★★★★★
	69270	HALOX\schedtasks	halox	schedtasks	Active Directory	*****	★★★★☆☆
	67187	halox\statex	halox	statex	Active Directory	Requires Checkout	★★★★★★
	62147	James Farthing	halox	farja	Active Directory	*****	★★★★☆☆
	67949	jtWilsonxxx	halox	jtWilsonxxx	Active Directory	*****	★★★★★★
	69304		halox		Active Directory	*****	★★★★☆☆

Change page: [Navigation icons]

Add | Documents (5) | Permalink | Grid Layout Actions... | List Administrator Actions...

### 2.1.1.2.7.6 View Password List Permissions

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

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

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

👤 Password List Permissions

To grant additional access simply click on the 'Grant Permissions' button, or to modify existing permissions click on the appropriate 'Actions' drop-down menu.

📄 Out of Band Management Cards 👤 User Account 📁 Local Security Group 🏢 Active Directory Security Group

Actions	User or Security Group	Site Location	Guest	View	Modify	Admin	Mobile Access	Expires
>	🏢 Department - Shared Services (Information Technology)	Internal			✓		✓	
	👤 Lee Sandford	Internal				✓	✓	
	👤 Mark Sandford	Internal				✓	✓	

[Return to Passwords Page](#) | [Grant New Permissions](#) | Grid Layout Actions...

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

## Password List Permission Actions

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

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

👤 Password List Permissions

To grant additional access simply click on the 'Grant Permissions' button, or to modify existing permissions click on the appropriate 'Actions' drop-down menu.

🔍 Out of Band Management Cards

User Account Local Security Group Active Directory Security Group

Actions	User or Security Group	Site Location	Guest	View	Modify	Admin	Mobile Access	Expires
	Department - Shared Services (Information Technology)	Internal			✓		✓	
	Lee Sandford	Internal				✓	✓	
	Internal	Internal				✓	✓	

Return

Change Access to 'View'

Change Access to 'Modify'

Change Access to 'Admin'

Enable/Disable Mobile Access

Modify Expiry Time

Update Access Notes

Remove Access

Grid Layout Actions...

## Grant New Permissions

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

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

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

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

## Access Permissions

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


### Grant New Permissions

To grant additional permissions to the 'Linux Accounts' Password List, simply click on the three **Tabs** below to specify appropriate permissions and/or settings.

access permissions
**time based access**

Search for an appropriate user or security group (use \* to search for all).














Site Location :

Search :  


Search For :  User  Security Group

---

**Search Results**

-  Desktop Team >>
-  Human Resources <<
-  IS Department <<
-  My Group 2
-  Nested Group 1
-  Network Team
-  Passwordstate-Auditing Security Group >>
-  Passwordstate-Export-All-Password S <<
-  Radius Users <<
-  SecurityGroup1
-  SecurityGroup2
-  Sydney-TestGroup
-  Test >>

**View Permissions**

-  CoreAdmins

**Mobile Access**

Enabled Mobile Access for these permissions:

Yes  No

**Reason for Access**

**Modify Permissions**

**Administrator Permissions**

Status:

## 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.

### Grant New Permissions

To grant additional permissions to the 'Linux Accounts' Password List, simply click on the three **Tabs** below to specify appropriate permissions and/or settings.



access permissions
time based access

To apply time based access to the selected Password List, please use the appropriate options below.

Access Expires : 

Never


In: Days:  Hours:  Minutes:


At: Date:   Time:  

Status:







#### 2.1.1.2.7.7 View Recycle Bin

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

 **Note:** Clicking on 'Empty Recycle Bin, or 'Delete' from the Actions drop-down menu will permanently delete the record(s), along with other related data.

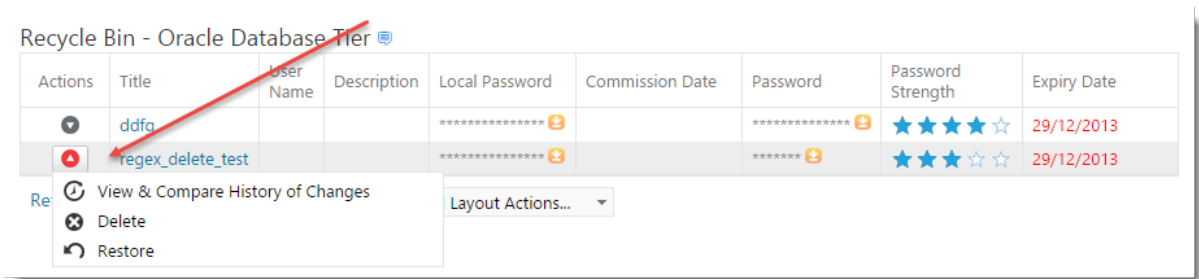
 **Note:** There is an option Security Administrators can set on the page Administration -> System Settings -> Password Options Tab which can also permanently delete linked Password records as well if required - by default, this is disabled

#### Recycle Bin - Oracle Database Tier

Actions	Title	User Name	Description	Local Password	Commission Date	Password	Password Strength	Expiry Date
	ddfg			***** 		***** 	★★★★★☆☆	29/12/2013
	regex_delete_test			***** 		***** 	★★★★☆☆☆	29/12/2013

[Return to Passwords](#) | [Empty Recycle Bin](#) | [Grid Layout Actions...](#)





### 2.1.2 Add Folder

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

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

Site Location	By default, the "Internal" site location will be the most common, unless you have purchased a subscription for the Remote Site Locations module
Folder Name	The name of the Folder as it will be displayed in the <a href="#">Navigation Tree</a>
Description	A description of the folder describing its 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 <a href="#">Navigation Tree</a>
Folder Permission Model	Select from one of the two permission models available

### Folder Permissions Model

There are two types of permission models available in Passwordstate:

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

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

## Add New Folder

To add a new folder, allowing you to organize your Password Lists in a structured way, please fill in the details below.

folder details guide api key & settings

Please specify appropriate details below, then click on the Save Button.

### Folder Settings

Site Location \*

Folder Name \*

Description

**Prevent Non-Admin users from Dragging and Dropping this Folder in the Navigation Tree**

Yes  No

### Folder Permission Model

**Permission Model**

Standard - Inherit permissions from nested Password Lists  Advanced - Propagate permissions down from top level folder

Permissions on Folders and Password Lists can be managed in one of two ways:

- **Standard Permission Model** - Permissions on the folder are inherited from any nested Password Lists beneath it. No Disabling of inheritance is at Folder or Password List level is possible.
- **Advanced Permission Model** - Permissions are generally propagate down from the Folder to nested Folders and Password Lists, unless Disabling of inheritance is selected on any nested items.

### 2.1.3 Add Private Password List

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

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

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

### 🔑 Add Private Password List Wizard

To create your Private Password List, please specify details below and select the type of Password List you would like based off the available Templates.

The screenshot shows a wizard window with a progress bar at the top. The first step, 'Password List Details', is highlighted in blue. Below the progress bar, the following fields are visible:

- Site Location: Internal
- Password List: \* My Private Password Vault
- Description: Log in Passwords for Various sites
- Template: Standard Password List
- Image: protect.png
- Template Description: Standard selection of settings, and basic Username and Password fields

At the bottom, there are two checkboxes:  Link this Password List to the selected Template. and  Disable future use of this Wizard. The 'Next' button is highlighted in blue, while 'Cancel' is a standard grey button.

**Note:** Additional settings can be changed after the Password List has been created.

### 🔑 Add Private Password List Wizard

To create your Private Password List, please specify details below and select the type of Password List you would like based off the available Templates.

The screenshot shows the second step of the wizard, 'Confirmation'. The progress bar now highlights the 'Confirmation' step. The text reads: 'Please confirm the details below are correct, then click the 'Finish' button.' The details listed are:

- Site Location: Internal
- Password List: My Private Password Vault
- Description: Log in Passwords for Various sites
- Template: Standard Password List
- Permissions: Image Capture (Admin)


At the bottom, there are three buttons: 'Cancel', 'Previous', and 'Finish'. The 'Finish' button is highlighted in blue.


**Note:** Additional settings can be changed after the Password List has been created.


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

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

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

 Note 1: Be careful if you choose the 'Use Separate Password' Additional Authentication option for your Private Password Lists. If you forget this Password, Security Administrators of Passwordstate are not able to reset it, meaning you will have lost access to the Password List.

 Note 2: When you add a new Private Password List, your account will be granted Admin rights to the Password List, and it will be positioned in the [Navigation Tree](#) just below the selected node (Password List or Folder). You can then drag-and-drop the Password List to any position in the [Navigation Tree](#) that you like.

 Note 3: The Site Location for Password Lists will always be 'Internal' if created in the root of Passwords Home, otherwise if nested beneath a Folder, it will use the same Site Location the Folder is set at.

### Add New Password List

To add a new Password List, please fill in the details below for each of the various tabs.

**Note:** You will receive **Administrator** permissions to the Password List once it is created (unless you're copying permissions from another Password List).

Use the Add Password List Wizard page in future for creating Password Lists

## 2.1.4 Add Shared Password List

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


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

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

## Add Shared Password List Wizard

To create a Shared Password List, please specify appropriate details below, and select the permissions you would like applied.


Progress bar: Password List Details (active), Permissions, Confirmation

Site Location:  Internal

Password List: \*

Description:

Template:

Image: 

Template Description: Standard selection of settings, and basic Username and Password fields

Disable future use of this Wizard

**Note:** Additional settings/permissions can be changed after the Password List has been created.

## 👉 Add Shared Password List Wizard

To create a Shared Password List, please specify appropriate details below, and select the permissions you would like applied.

Password List Details   **Permissions**   Confirmation

---

Search for Users or Security Groups below, and apply appropriate permissions.

Site Location :  ▾

Search :  🔍

Search For :  User  Security Group

---

### Search Results

- Core Distribution
- EmptyGroup
- Finance Department
- IS Department
- Local SG
- My Group 2
- Network Team
- Passwordstate-Auditing Security Group
- Test
- Test Users SG

### View Permissions

>>

<<

### Modify Permissions

- CoreAdmins

>>

<<

### Administrator Permissions

- Mark Sandford

>>

<<

Status:

---

**Note:** Additional settings/permissions can be changed after the Password List has been created.

## 🔑 Add Shared Password List Wizard

To create a Shared Password List, please specify appropriate details below, and select the permissions you would like applied.

Please confirm the details below are correct, then click the 'Finish' button.

Site Location: 🏠 Internal

Password List: 🗝️ Shared Password Vault

Description : Used to share various credentials for Admin team

Template: Standard Password List

Permissions: CoreAdmins (Modify), Mark Sandford (Admin)

Cancel Previous Finish

**Note:** Additional settings/permissions can be changed after the Password List has been created.

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

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

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

🚩 **Note 1:** When you add a new Shared Password List, by default your account will be granted Admin rights to the Password List (Security Administrators of Passwordstate can change this setting though), and it will be positioned in the [Navigation Tree](#) just below the selected node (Password List or Folder). You can then drag-and-drop the Password List to any position in the [Navigation Tree](#) that you like.

🚩 **Note 2:** The Site Location for Password Lists will always be 'Internal' if created in the root of Passwords Home, otherwise if nested beneath a Folder, it will use the same Site Location the Folder is set at.



### Add New Password List

To add a new Password List, please fill in the details below for each of the various tabs.

**Note:** You will receive **Administrator** permissions to the Password List once it is created (unless you're copying permissions from another Password List).

Use the Add Password List Wizard page in future for creating Password Lists

## 2.1.5 Administer Bulk Permissions

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

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

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

#### 👤 Administer Bulk Permissions for Password Lists

Administering Bulk Permissions is a three step process - 1. Search for a User or Security Group, 2. Apply new or modify existing permissions, and 3. Save the changes.

**Note 1:** You cannot administer bulk permissions for Password Lists which have mandatory options set for Time Based Access.

**Note 2:** Only Password Lists you are an Administrator of will be available on this screen.

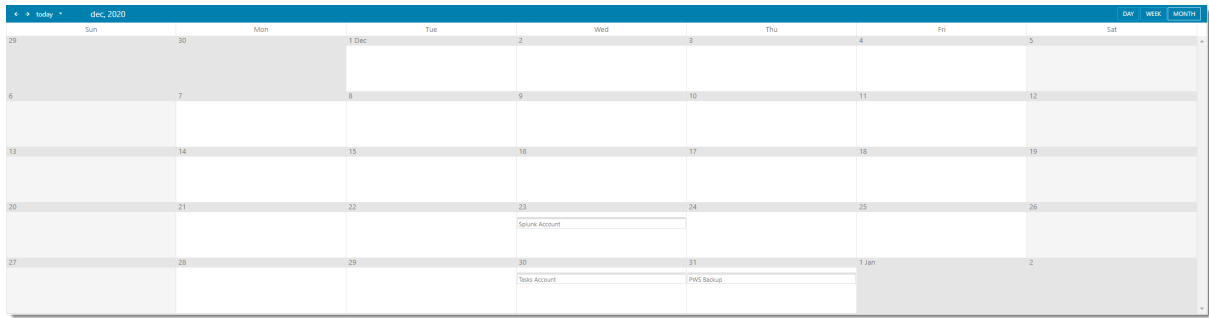
**Note 3:** Password Lists nested underneath folders using the Advanced Permission Model cannot have their permissions changed here - unless Disable Inheritance is enabled.

## 2.1.6 Expiring Passwords Calendar

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

On this calendar you can:

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



### 2.1.7 Password List Templates

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

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

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

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

**Password List Templates**

Listed below are all the Password List Templates stored within Passwordstate.


Actions	Password List	Description	Linked Password Lists	Deny Export	Time Based Access	Prevent Password Reuse	In-Built Template
	Alarm/Door Codes	Store building alarms codes, or door pin tumbler combinations	0				
	Credit Cards	Securely store credit card information	0				
	Enabled for Password Resets	Perform password resets on a scheduled, or on demand, for many different types of accounts	0				
	One-Time Password Authenticator	Generate One-Time Passwords based off scanned QR Codes	0				
	Software Licenses	Store various metadata related to software licensing	0				
	SSH Account (Key Storage Only)	Store SSH Keys with Passphrase recorded in Password field - Used for SSH Sessions	0				
	SSH Account (Passphrase + Key Storage)	Store SSH Keys with Passphrase and optional Password field	0				
	SSL Certificates	Store SSL certificates and receive reminders of when they need to be renewed	0				
	Standard Password List	Standard selection of settings, and basic Username and Password fields	1				
	Standard Password List (Hide Passwords)	Standard Password List where the values of passwords are hidden from non-administrators	0				

Page: 1 of 2 | [Go](#) | Page size: 10 | [Change](#) | Item 1 to 10 of 13

[Add New Template](#) | [Toggle ID Column Visibility](#) | [Grid Layout Actions...](#)

## 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 be 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.

## Password List Templates

Listed below are all the Password List Templates stored within Passwordstate.

Actions	Password List	Description
	<input type="text"/> <input type="button" value="Y"/>	<input type="text"/> <input type="button" value="Y"/>
	Alarm/Door Codes	Store building alarms codes, or door pin tumbler combinat
	Credit Cards	Securely store credit card information
	Enabled for Password Resets	Perform password resets on a scheduled, or on demand, fo
	Authenticator	Generate One-Time Passwords based off scanned QR Code
	Linked Password Lists	Store various metadata related to software licensing
	Delete Template	
	SSH Account (Key Storage Only)	Store SSH Keys with Passphrase recorded in Password field
	SSH Account (Passphrase + Key Storage)	Store SSH Keys with Passphrase and optional Password field
	SSL Certificates	Store SSL certificates and receive reminders of when they n
	Standard Password List	Standard selection of settings, and basic Username and Pas
	Standard Password List (Hide Passwords)	Standard Password List where the values of passwords are l

Page: \_\_\_\_\_

[Add New Template](#) | [Toggle ID Column Visibility](#) | [Grid Layout Actions...](#)

### 2.1.7.1 Add New Template

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

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

### Add New Password List Template

To add a new Password List Template, please fill in the details below for each of the 3 tabs.

password list details
customize fields
guide

Please specify Password List settings manually below.

**Password List Details**

Password List \*

Description

Image - Select Image -

Password Strength Policy \* Default Policy

Password Generator Policy \* Build Policy

Code Page \* Use Passwordstate Default Code Page

Additional Authentication \* None Required

**Password List Settings**

Enable Password Resets - allows password resetting with other systems

Enable One-Time Password Generation

Allow Password List to be Exported

Time Based Access Mandatory

Multiple Approvers Mandatory - a total of 1 approver(s) are required for this List

Prevent Password reuse for the last 5 passwords

Disable Email Notifications for this Password List

Force the use of the selected Password Generator Policy

Hide Passwords from users with the following permissions

Popup the Guide on each access to this Password List

Prevent Non-Admin users from Dragging and Dropping this Password List

Prevent saving of Password records if a 'Bad' password is detected

Users must first specify a reason why they need to view, edit or copy passwords

Prevent Non-Admin users from manually changing values in Expiry Date fields

Set the Expiry Date to Current Date + 0 Days when adding new passwords

Reset Expiry Date to Current Date + 0 Days when manually updating passwords

Additional Authentication only required once per session

Show 'Active Directory Actions' options for Active Directory accounts

**Default Password Reset Schedule**

⚠ Only applicable if this Password List is enabled for Resets.

Please specify the default settings for 'Reset Options' when new records are added to this Password List.

Enable the the Password Reset Schedule for the account, and schedule the reset at a random time between the two time slots below:

**Start Time**  
00 Hour 00 Minute

**Finish Time**  
00 Hour 00 Minute

And when the account expires, add 90 Day(s) to the Expiry Date.

Save Cancel

#### 2.1.7.2 Linked Password Lists

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

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

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

## Linked Password Lists

Below are a list of Password Lists which can be, or are already linked, to the Template 'Standard Password List'.

**Note 1:** A Password List can only be linked to one Template at a time. If already linked to another Template, it will be disabled in the 'Available Password Lists'.

**Note 2:** If you link a Password List to this Template, and the Template has different Generic Field field types compared to the Password List, then the Password List will be disabled.

## 2.1.8 Pending Access Requests

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

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

**Access Requests For Me To Approve**

Date	User Requesting Access	Password List	Title	UserName	Description	Reason	Permissions	No. of Approvers	Approval Count	Commences At	Expires At
2019-02-22 11:44:00 AM		No Access				Only need access briefly	Modify	1	0		
2019-02-22 11:45:00 AM		Optus Dialup	testdelete			Need to testdialup for customer	Modify	1	0		2019-02-28 12:00:00 AM
2019-02-24 9:48:00 AM		Infrastructure\Web Sites			Book Depository Sign In	Needed for social media advertising.	Admin	1	0		2019-02-28 12:00:00 AM

**My Pending Access Requests**

Actions	Date	Password List	Title	UserName	Description	Reason	Permissions	No. of Approvers	Approval Count	Commences At	Expires At
No records to display.											


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

### ✉ Process Access Request



Below are the user's access request details. Please modify, approve or deny as appropriate.



**access request settings**

**User :** [Redacted]

**Password List :**  \Infrastructure\Web Sites Book Depository Sign In

**Access Type :**  View  Modify  Administrator

**Start Date :** [ ]   (Leave blank for no specific start)


**Expiration Date :** 2019-02-28 12:00 AM   **(Mandatory for this Password List)**

**Reason : \***  
[ Needed for social media advertising. ]

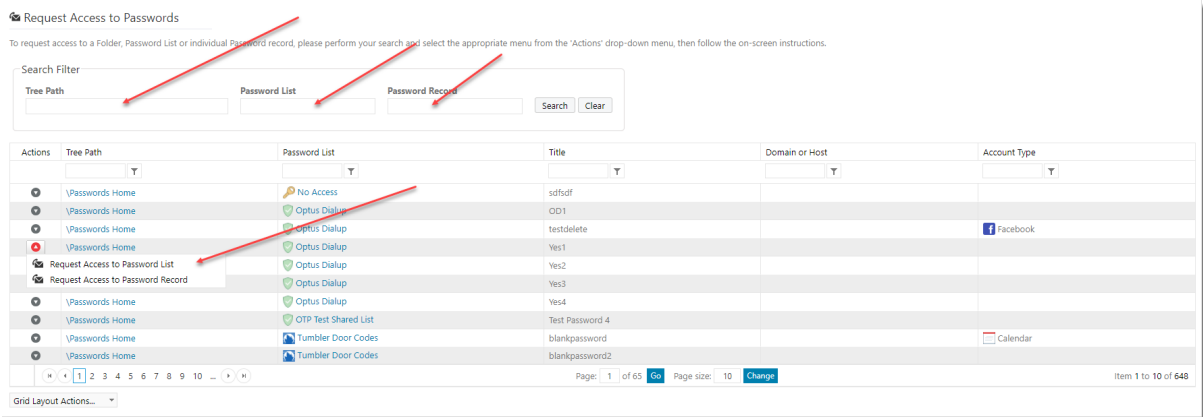
## 2.1.9 Request Access to Passwords

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

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

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





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

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

**Request Access to Password List**

To request access to the Password List 'Optus Dialup' with the details below, please specify a reason why and click on the 'Submit' button.

**Request Details :**

**Password List :**  Optus Dialup

**Access Type :**  View  Modify  Administrator

**Start Date :**  (Leave blank for no specific start)

**Expiration Date :**  **(Mandatory for this Password List)**

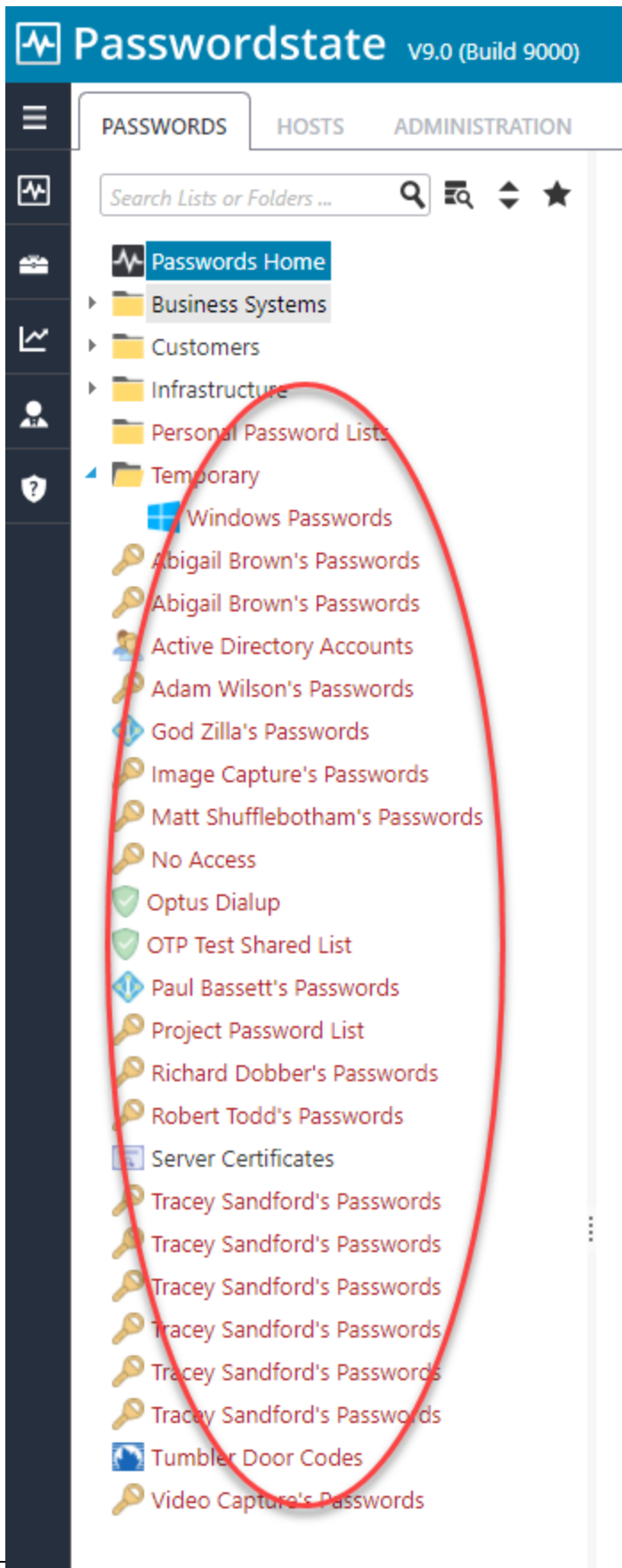
**Reason : \***

### 2.1.10 Toggle All Password List Visibility

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

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

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



## 2.2 Tools Menu

There are three options available under the Tools menu.


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


### 2.2.1 Account Discovery


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


The following Account Discovery jobs are available:


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


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

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

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

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

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

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

Account Discovery

Below are all the Account Discovery jobs added to Passwordstate.


Actions	Job Name	Description	Job Type	Site Location	Run Discovery At	Schedule Type	In Progress	Last Discovery Took	Simulation Mode	Enabled
	All Local Admins On Servers	All Local Admins On Servers	Windows Local Admin Accounts	Internal	11:00 PM	Weekly - Sunday				
	Linux Discovery Halox External - No Key	Linux Discovery Halox External	Linux And Mac Accounts	Halox	01:20 PM	Daily		00:00:02		
	Local Windows Admins on Halox	Local Windows Admins on Halox	Windows Local Admin Accounts	Halox	03:54 PM	Daily		00:00:10		
	Windows Dependencies on Halox	Windows Dependencies on Halox	Dependencies	Halox	02:40 PM	Daily		00:00:05		

Select Discovery Job Type to Add... Grid Layout Actions...

## Discover Accounts

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

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

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

the Password List, that way each record will have its 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.

**Add Windows Local Admin Accounts Discovery Job**

To add a new Discovery Job to find Accounts on your network, please select the appropriate options on each of the tabs below and click on the 'Save' button.

discovery job settings | **schedule** | hosts to be queried

Discovery Job Name \* :

Description \* :

Site Location \* :

Simulation Mode :  Simulation Mode will email you the results without adding/updating any data in the database

Report on the following: :  Only newly Discovered Accounts  All Discovered Accounts - New or Existing

**Discovery Search Criteria**

Please specify filtering options for which Hosts you wish to query for new accounts, as well as any filtering options for the names of accounts.

Host Types:  Operating Systems:

Include Hosts based on Host Name match:  Include Hosts based on Tag Field match:

Exclude Hosts based on Host Name match:  Exclude Hosts based on Tag Field match:

Discover Accounts by Username match:  Exclude Accounts based on Username match:

Query the following Local Administrator Group Name(s):

Each of the fields above can have multiple values specified, by separating them with semicolon characters.

**Discovery Actions**

Please select appropriate options below when new Accounts are discovered.

Set the 'Managed Account' settings for newly discovered accounts: (these settings can be changed after the record has been created if needed)

Enabled for Resets  Enabled for Heartbeat

## Discover Windows Dependencies

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

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

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

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

**Add Windows Dependency Discovery Job**

To add a new Discovery job to find "Dependencies" on your Windows Hosts, please select the appropriate options on each of the tabs below and click on the 'Save' button.

discovery job settings   **schedule**   hosts to be queried

Please select appropriate options for the Discovery Job below, and set the schedule as required.

**Discovery Job Name \*** :

**Description \*** :

**Site Location \*** :

**Active Directory Domain \*** :  Only accounts from this selected domain will be discovered

**Simulation Mode** :  Simulation Mode will email you the results without adding/updating any data in the database

**Report on the following:** :  Only newly Discovered Dependencies    All Discovered Dependencies - New, Existing or No Dependencies

---

**Discovery Search Criteria**

Please specify which search options you would like to define for the Discovery Job.

**Discover the following Dependencies configured to use an Active Directory account:**

Windows Services    IIS Application Pools    Scheduled Tasks

**Discover Dependencies on Hosts with the following Operating Systems:**

**Include Hosts based on Host Name match:**

**Include Hosts based on Tag Field match:**

**Exclude Hosts based on Host Name match:**

**Exclude Hosts based on Tag Field match:**

Each of the fields above can have multiple values specified, by separating them with semicolon characters.

---

**Discovery Actions**

**When a newly discovered Active Directory Account (being used by a Dependency) is found, check the 'Managed Account' option for the account to enable automatic scheduled resets:** (If you select No, you can enable this option for one or more records at a later time - from within the appropriate Password List)

Yes    No

## Discovery Job History

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

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

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

Account Discovery

Below are all the Account Discovery jobs added to Passwordstate.

Actions	Job Name
	<input type="text"/> <input type="button" value="Y"/>
▼	All MariaDB Accounts
▼	Dependencies on Domain Controllers
▼	Discover all PostgreSQL Accounts
▼	Discover All SonicWALL Accounts
▼	Discover Server Admin Accounts
▲	Windows Local Admin Accounts

Select Actions...

- Delete
- Run Discovery Job Now
- Toggle Status - Enabled or Disabled
- View Discovery Job History
- View Permissions

### 2.2.2 Have I Been Pwned Password Check

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

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

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



### Have I Been Pwned Password Check

Millions of passwords have been exposed on the internet in various data breaches, and the 'Have I been Pwned' web site (<https://haveibeenpwned.com/>)

have i been pwned check

Please specify a password below to check if it has been known to be compromised in any public data breaches.

Please note that a 'Pass' here does not necessarily mean the password is strong in nature - you should use long and complex passwords where possible.

Password:


Status: Waiting for check


## 2.2.3 Import Passwords


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

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

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

 **Note 1:** For the CSV imports, you must have created the Password Lists already to import into. And when importing into Multiple Password Lists, you must know the PasswordListID values for each Password List, as you need to specify these in the import CSV file. Please see instructions below of 'Determining PasswordListID's for CSV Imports' for how to determine these ID's

 **Note 2:** When using the 'CSV file into Multiple Password Lists', you must be a Security Administrator of Passwordstate, which has the Password Lists Security Administrator role. This restriction is in place to prevent standard user accounts from importing data into Password Lists which they have not been given access to.

 **Note 3:** For importing from the 4 different products listed above, the Base URL of your Passwordstate web site must be recorded correctly in Passwordstate, so the API can be used to perform this import

## 🖱 Import Passwords

To import passwords via csv files, or from other systems, please select the appropriate option below, and then follow the on screen instructions.

Please select what type of Import you would like to perform below, and then follow further on screen instructions for your import.

Import Type: Choose Import Type

- Choose Import Type
- CSV file into Single Password List
- CSV file into Multiple Password Lists
- KeePass
- LastPass
- Thycotic Secret Server
- Password Manager Pro

Cancel Next

## Determining PasswordListID's for CSV Imports

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

Search [ ] [i] [Screen Options]

Web Sites (PasswordListID = 20259) (API Key = Not Set)

Actions	PasswordID	Title	User Name	Description	URL
▼	70457	AA - Host Record			
▼	70461	aaaa			h
▼	70336	adaptiveinsights			"
▼	70337	arubainstanton			h
▼	70338	auth.services.adobe.com			h
▼	70339	hancsabadell			v
▼	70340	business.apple.com			'
▼	70341	central.arubanetworks			h
▼	70342	crowdstrike			h
▼	70343	directsourcing			h

Change page: [ ] [ ] [ ] [ ]

Add | Documents (0) | Permalink | Grid Layout Actions... ▼

Recent Activity [i]

Date	Activity
8/12/2021 9:41:06 AM	Password List Updated
1/12/2021 2:32:39 PM	Password List Updated
1/12/2021 2:19:55 PM	Password List Updated
1/12/2021 2:18:06 PM	Password List Updated
1/12/2021 1:10:22 PM	Password List Updated
1/12/2021 1:09:00 PM	Password List Updated
26/11/2021 9:06:41 AM	Self Destruct Message Sent
25/11/2021 1:59:43 PM	Password Updated
25/11/2021 1:59:38 PM	Password Screen Opened
25/11/2021 12:58:02 PM	Password History Exported

Change page: [ ] [ ] [ ] [ ]

Refresh Grid | Grid Layout Actions... ▼

- List Administrator Actions...
  - List Administrator Actions...
  - PASSWORD LIST ACTIONS**
  - Bulk Delete Selected Passwords
  - Bulk Permissions for Individual Passwords
  - Bulk Update Passwords
  - Bulk Update Password Reset Options
  - Convert to Shared Password List
  - Delete Password List
  - Edit Password List Properties
  - Save Password List as Template
  - Toggle Visibility of Delete Checkboxes
  - Toggle Visibility of Web API IDs
  - View Password List Permissions
  - View Recycle Bin (2)
  - EXPORT**
  - Export All Password History
  - Export All Passwords
  - Enumerated Permissions Report
  - Have I Been Pwned Compromises
  - Password Strength Report
  - Standard Permissions Report

Passwordstate V9.3 (Build 9381)

PASSWORDS HOSTS ADMINISTRATION

Administration

- Account and Host Discovery
- Active Directory Domains
- Auditing
- Auditing Graphs
- Authorized Web Servers
- Backups and Upgrades
- Bad Passwords
- Browser Extension Settings
- Brute Force Blocked IPs
- Email Notification Groups
- Email Templates
- Emergency Access
- Encryption Keys
- Error Console
- Export All Passwords
- Feature Access
- Host Types & Operating Systems
- Images and Account Types
- License Information
- Password Folders
- Password Generator Policies
- Password Lists**
- Password List Templates
- Password Strength Policies
- Privileged Account Credentials

Password Lists

Listed below are all the Password Lists within Passwordstate.

Show only :  Shared Password Lists  Private Password Lists

Clicking on a Shared Password List allows you to **Administer Permissions and Edit Passwords**

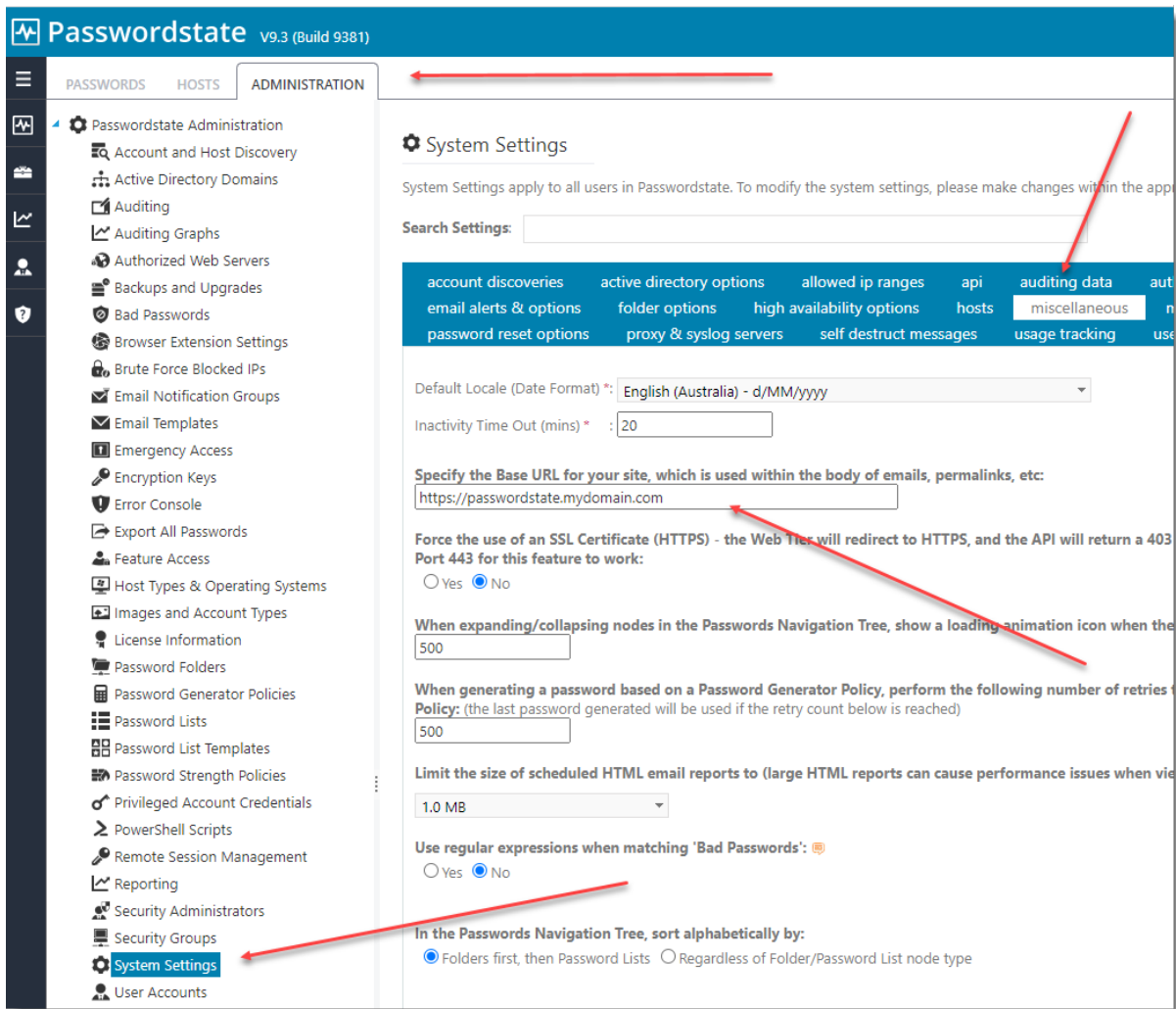
Actions	PasswordListID	Password List
▼	20257	\Browser Testing
▼	6507	\Business Systems\Credit Cards
▼	7	\Business Systems\Database Accounts
▼	19961	\Business Systems\Microsoft SQL Local Accounts
▼	6618	\Business Systems\Oracle ERP Accounts
▼	6619	\Business Systems\SharePoint Accounts
▼	5300	\Business Systems\SSL Certificates
▼	10133	\Customers\Allsand\Workstation Accounts
▼	4174	\Customers\Contoso\DBAs\Database Credentials
▼	9744	\Customers\Contoso\Infrastructure\Active Directory Accounts

Export Password List Information | Toggle ID Column Visibility | Perform Bulk Process

## Determining PasswordListID's for CSV Imports

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

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



## 2.2.4 Password Generator

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

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

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

### Alphanumeric & Special Characters

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

## Password Generator

Please use the various tabs below to specify options for your Personal Password Generator options.

generate passwords alphanumerics & special characters word phrases

Include Alphanumerics & Special Characters

Password Length

Length :  Min  Max

Alphanumerics

Lower-case    Upper-case    Numbers

Include higher ratio of alphanumerics vs special characters

Include ambiguous alphanumerics (l, I, o, 0 and 1)

Exclude the following characters and numerics

Special Characters

Include the following special characters

Include the following brackets

Generate Using a Pattern

Generate based on a pattern of upper and lowercase letters, and numbers

l for Lowercase, u for uppercase, and n for numbers i.e. uullllnnnnllllnnnn

[Save Options](#)

## 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.

### Password Generator

Please use the various tabs below to specify options for your Personal Password Generator options.

generate passwords
alphanumerics & special characters
word phrases

Include Word Phrases

**Quantity & Length**

Number of Words :

Maximum Word Length :

**Positioning**

Prefix Words to Alphanumerics & Special Characters

Append Words to Alphanumerics & Special Characters

Insert Randomly into Alphanumerics & Special Characters

**Separation**

Separate Words with Dashes


Separate Words with Spaces


No Separation

## 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

## 📄 Password Generator

Please use the various tabs below to specify options for your Personal Password Generator options.

generate passwords | alphanumeric & special characters | word phrases

Use settings from:


Number of Passwords :

```
cot-Jy6Hz3MpFS5R
emit-Q6SZE5TjrRfq
rice-2MxkgG8SPVN
jots-3MpsHTLfr
net-Q6SZE5TjrRfq
lees-gXixsTVqY3u5
tear-sWtLxRHPz7w
wags-U6gZrWPGHFx
dry-89XQLzn
glad-XWx623ptES
next-Xn5ZhtzPKJYf
flee-pzyeJ4i3
twig-z4tUqeRpSiY
rib-LvNKgepTQ
ease-Nv97T4sJz
```

### 2.2.5 Password Resets in Progress

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

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

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



Password Resets In Progress

Below are all the pending Password Reset tasks in the Queue at the moment, as well as most recent auditing data for these queued records. You can use this screen to watch resets progress through the queue, or to troubleshoot any issues as to why they are not moving through the queue.

Password Reset Queue

Actions	Queued At	Title	Domain or Host	UserName	Account Type	Description	Site Location	Dependencies
	13/06/2017 12:59:00 PM	Splunk Account	halox	splunkacct@halox.net	Active Directory	Used for SIEM	Internal	0

Refresh Both Grids | Grid Layout Actions...

Recent Activity

Date	Platform	UserID	First Name	Surname	Activity	Description
13/06/2017 12:58:56 PM	Web				Password Reset Added to Queue	manually modified the Password for account 'Splunk Account' (Password List = \Infrastructure\Active Directory Accounts, UserName = splunkacct@halox.net, Description = Used for SIEM), resulting in a record being added to the queue to perform appropriate Password Reset tasks. This account relates to an Active Directory account on the domain halox (halox.net).
13/06/2017 12:58:51 PM	Web				Password Screen Opened	opened the Edit Password screen for password 'Splunk Account' (Active Directory Accounts) - viewing the value of the password is possible on this screen. (Title = Splunk Account, UserName = splunkacct@halox.net, Description = Used for SIEM).
13/06/2017 11:40:46 AM	Web				Password Screen Opened	opened the Edit Password screen for password 'Splunk Account' (Active Directory Accounts) - viewing the value of the password is possible on this screen. (Title = Splunk Account, UserName = splunkacct@halox.net, Description = Used for SIEM).
					Password	A scheduled Account Heartbeat check successfully validated the password for

## 2.2.6 Self Destruct Message

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

Creating a Self Destruct message is a three step process:

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

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

## Send Self Destruct Message

To send a Self Destruct Message to another person, please specify details as appropriate for each stage of the Wizard below.

Message Content    Email to Recipient    Passphrase Protection

---

Enter the contents of the Self Destruct message you want the recipient to read.

Hi John,

The password for HostXYZ is MyStrongPassword123

Regards  
John

Design    Preview

Automatically self-destruct this message if not viewed in:

Allow the self-destruct message to be viewed (x) times:

Cancel    Next

Message Content **Email to Recipient** Passphrase Protection

---

If you want Passwordstate to send the Self Destruct Message Email and URL, please select the Recipient below. Otherwise, please click the Next button.

**Select Recipient**

**Subject**

Hi,

You've been sent a Self Destruct Message from Passwordstate, and you can view the detail of the message by clicking the URL below.

URL: <https://passwordstate9appserver.halox.net/selfdestruct/?id=902af4360fc64bb1b43f9b6fb9968e44>

This message will expire [ExpirePeriod] from the time of this email being sent.

Passwordstate 9.0 - Secure Password Management.  
<https://passwordstate9.halox.net>

Design Preview

### Send Self Destruct Message

To send a Self Destruct Message to another person, please specify details as appropriate for each stage of the Wizard below.

Message Content **Email to Recipient** **Passphrase Protection**

---

To protect access to your Self Destruct message with the user of a Passphrase, please specify this below - you must inform your recipient the value of this Passphrase before they can read the message.

Passphrase Protection:

## 2.3 Reports Menu


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


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

## 2.3.1 Auditing

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

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

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

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

### Auditing

To search for relevant audit records, please use the options below.

**Auditing Filters**

Platform:  All  Web  Mobile  API  Windows Service  Browser Extension Instance:  Both  Primary  HA (Passive Node) Archived Data:  No  Yes

Max Records:  Password List:  Activity Type:  Site Location Activity:  Begin Date:  End Date:

Date	Platform	UserID	First Name	Surname	IP Address	HA Instance	Activity	Tree Path	Descr
4/12/2020 11:39:14 AM	Web	halox\images	Image	Capture	10.0.0.108		Login Attempt Succeeded		Succe
4/12/2020 11:32:36 AM	Windows Service	WindowsService	Windows Service	Account	10.0.0.125		Password Validation Successful	\Infrastructure\AD Discovery	A sch View
4/12/2020 11:32:36 AM	Windows Service	WindowsService	Windows Service	Account	10.0.0.125		Password Validation Successful	\Infrastructure\AD Discovery	A sch View

## Filter by Platform

**Auditing Filters**

**Platform:**  All  Web  Mobile  API  Windows Service  Browser Extension **Instance:**  Both  Primary  HA (Passive Node)

**Max Records:**  **Password List:**  **Activity Type:**

## Filter by Specific Password Lists

**Auditing**

To search for relevant audit records, please use the options below.

**Auditing Filters**

**Platform:**  All  Web  Mobile  API  Windows Service  Browser Extension **Instance:**  Both  Primary  HA (Passive Node) **Archived Data:**  No  Yes

**Max Records:**  **Password List:**  **Activity Type:**  **Site Location Activity:**  **Begin Date:**  **End Date:**

Date	IP Address	HA Instance	Activity	Tree Path
10/12/2020 9:07:31	10.0.0.91		Password Validation Failed	\Infrastructure\AD Discovery
10/12/2020 9:07:31	10.0.0.91		Password Validation Failed	\Infrastructure\AD Discovery

## Filter by Specific Activity Type

## Auditing

To search for relevant audit records, please use the options below.

**Auditing Filters**

Platform:  All  Web  Mobile  API  Windows Service  Browser Extension Instance:  Both  Primary  HA (Passive Node)

Max Records:  Password List:  Activity Type:  Site Location:

Date	Platform	UserID	Activity Type	Site Location
13/06/2017 12:58:56 PM	Web	halox\msand	Access Granted	9
13/06/2017 12:58:51 PM	Web	halox\msand	Access Removed	9
13/06/2017 12:56:33 PM	Windows Service	WindowsService	Access to Password Approved	9
13/06/2017 12:52:04 PM	Web	halox\msand	Access to Password Denied	9

## Filter between Specific Dates

**Auditing Filters**

Platform:  All  Web  Mobile  API  Windows Service  Browser Extension Instance:  Both  Primary  HA (Passive Node) Archived Data:  No  Yes

Max Records:  Password List:  Activity Type:  Site Location Activity:  Begin Date:  End Date:  Search

## Further Filter by Search Results Contents

**Auditing Filters**

**Platform:**  All  Web  Mobile  API  Windows Service  Browser Extension **Instance**

**Max Records:**  **Password List:**  **Activity Type:**

Date	Platform	UserID	First Name	Surname
<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>
19/01/2015 1:23:40 PM	Browser Extension	halox\msand		
19/01/2015 1:23:27 PM	Browser Extension	halox\msand		

- NoFilter
- Contains
- DoesNotContain
- StartsWith
- EndsWith
- EqualTo
- NotEqualTo
- GreaterThan
- LessThan
- GreaterThanOrEqualTo

### 2.3.2 Auditing Graphs

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

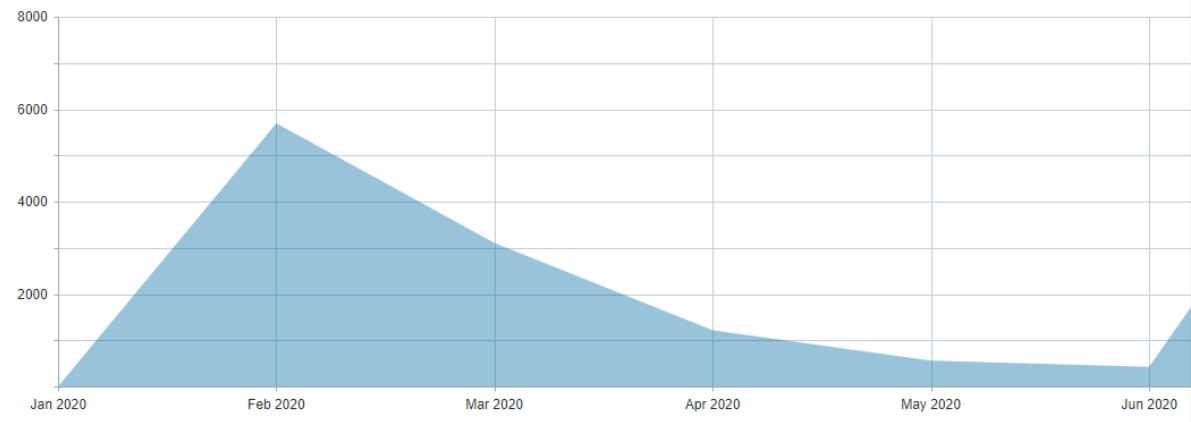
### Auditing Graphs

Please select the appropriate filters below, and then click on the 'Refresh' button.

Graph Filters

Platform:  All  Web  Mobile  API  Windows Service  Browser Extension Archived Data:  No  Yes

Audit Activity:  Site Location Activity:  Duration:  Refresh



### 2.3.3 Scheduled Reports

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

#### Choosing The Report Type

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

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

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

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

#### User Reports

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



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

### **Passwords Reports**

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

### **Permissions Reports**

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

### **Audit Activity Reports**

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

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

### 🕒 Add Scheduled Report

Scheduled Reports allows you to receive various reports via email. Please use each of the tabs below, as appropriate, to specify settings for your report.

report settings
schedule
expiring passwords settings
auditing settings
security admin report options

Please enter a Name and Description for your report, and select the Report type you want. Then make changes on the other tabs as required.

**Report Settings**

**Report Name \*** :  Report Name will be used as the Subject Line in the Email.

**Report Description** :

**CC Report To** :  comma separate the email addresses.

**Email Report As** :  Embedded HTML  CSV Attachment (CSV files are recommended if the report generates a lot of data)

**File Attachment Name \*** :   Append date to file name in format of YYYY-MM-DD.

Do not send report if it produces no results.

**Select Report Type**

Please choose the appropriate report below.

Choose Report...

Choose Report...

**AUDITING REPORTS**

Custom Auditing Report

**USER REPORTS**

What passwords can a user see?

What passwords does a user still know?

What has a user been doing lately?

What Failed login attempts have there been?

Who hasn't logged in recently?

Who has one or more Security Administrator roles?

What Remote Sessions has a user been doing lately?

What user accounts are currently disabled?

What user accounts are set to expire?

Which users have logged in using the Emergency Access account?

What user account impersonation has been occurring?

**PASSWORD REPORTS**

What passwords have failed Heartbeat?

What passwords have failed Reset?

**Report Description & Criteria**

**Report Name:** Please select one of the available reports on the left to see a description of what the report provides.

**Report Description:**

## 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.

### 🕒 Add Scheduled Report

Scheduled Reports allows you to receive various reports via email. Please use each of the tabs below, as appropriate, to specify settings for your report.

report settings
schedule
expiring passwords settings
auditing settings
security admin report options

Please specify the time you would like to receive the report, and the frequency.

Generate Report at:  Hour  Minute

**Report Frequency**

One Time | No additional settings for a Daily Schedule

Daily

Weekly

Monthly

## 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.

🔗 Add Scheduled Report

Scheduled Reports allows you to receive various reports via email. Please use each of the tabs below, as appropriate, to specify settings for your report.


report settings
schedule
expiring passwords settings
auditing settings
security admin report options

**Password List(s)**

**Passwords expiring in the next**  
 day(s).  Also query passwords which have already expired.

## Auditing Settings

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

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

🔗 Add Scheduled Report

Scheduled Reports allows you to receive various reports via email. Please use each of the tabs below, as appropriate, to specify settings for your report.

report settings
schedule
expiring passwords settings
auditing settings
security admin report options

Please select the appropriate filters below to query auditing data for your report.

**Auditing Filter**

**Platform:**  All  Web  Mobile  API  Windows Service  Browser Extension **Instance:**  Both  Primary  High Availability

**Password List**  **Activity Type**  **Site Location**  **Query Previous**  Days  Hours  Minutes

**Filter By User Account**  **Filter on content in Description Field**

## Security Admin Report Options

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

[Add Scheduled Report](#)

Scheduled Reports allows you to receive various reports via email. Please use each of the tabs below, as appropriate, to specify settings for your report.

report settings   schedule   *expiring passwords settings*   auditing settings   security admin report options

Depending on the type of report selected, certain controls below may be disabled - certain reports allow you to further filter on specific users.

Passwordstate User Account:   
 Site Location: -- All Site Locations --  
 Duration: Past 30 Days

Save Report   Cancel

## 2.4 Preferences Menu

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

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

### 2.4.1 Address Book

The address book is used primarily for two features:

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

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

[Address Book](#)

Listed below are all your personal contacts, as well as any global contacts. The Address Book can be used for storing any personal contacts, and can also be used in conjunction with the Self Destruct Message feature.


Show only:  Personal Contacts    Global Contacts

Actions	Full Name	Email Address	Company	Business Phone	Personal Phone	Global Contact	Passphrase Set
	<input type="text"/>	<input type="text"/>	<input type="text"/>			<input type="text"/>	<input type="text"/>
<input checked="" type="radio"/>	Michael Reznor	mreznor@outlook.com					<input checked="" type="checkbox"/>
<input checked="" type="radio"/>	Felicity Carter	f.carter@mail.com					<input checked="" type="checkbox"/>
<input checked="" type="radio"/>	John Williams	jwilliams@gmail.com	Ignite Industries	+61 88140 0341			<input checked="" type="checkbox"/>

[Add Contact](#) | [Import Contacts](#) | [Grid Layout Actions...](#)

### 2.4.2 Preferences

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

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

The Preferences screen has the following 8 tabs:


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

#### 2.4.2.1 Passwords Tab

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

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

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

 Preferences

To modify your preferences for Passwordstate, please make changes in the relevant tabs below, then click on the 'Save' button.

passwords tab **hosts tab** miscellaneous color theme authentication options mobile access options browser extension

Please select which Password List or Folder options you would like to return when you navigate to the Passwords Tab.

**Passwords Navigation Tree Defaults**

Collapse all nodes in the Navigation Tree  Remember expand status of all nodes in Navigation Tree  
 Show all Password List/Folders in the Navigation Tree  Hide all Password List/Folders in the Navigation Tree

**Limit the number of displayed Nodes (Password Lists and Folders) in the Navigation Tree to:**  
 (setting to 0 will show all Nodes, and if limiting the number of displayed Nodes, use the 'Search Password Lists' feature.)

**If launching a Remote Session to a Host from within the Passwords tab, and you have access to both the Browser and Client Based versions of the Remote Session Launcher, which launcher would you like to use:**

Client Based Launcher  Browser Based Launcher

**Use Load On Demand Feature for faster loading and expanding of Nodes in the Passwords Navigation Tree:**

Yes  No

Load On Demand is used for performance reasons when you have thousands of nodes in the Navigation Tree. When enabled, the following will occur:

1. Some options above will be disabled
2. If limiting the number of nodes, this will be a limit on nodes in the root of Passwords Home only
3. Only the root nodes will be visible, and collapsed, when first navigating to the tree
4. Expanding the nodes will retrieve the nested nodes live from the database
5. Searching for Password Lists/Folders will behave as per normal.

#### 2.4.2.2 Hosts Tab

The Hosts Tab allows you to select various options for the Hosts Navigation Tree under the [Hosts](#) tab.

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

**Preferences**

To modify your preferences for Passwordstate, please make changes in the relevant tabs below, then click on the 'Save' button.

passwords tab hosts tab miscellaneous color theme authentication options mobile access options browser extension api

Please specify settings for features under the Hosts tab as appropriate.

**Hosts Options**

**Limit the number of displayed Nodes (Folders and Host records) in the Navigation Tree to:**  
 (setting to 0 will show all Nodes, and if limiting the number of displayed Nodes, use the 'Search Hosts' feature.)

**Use Load On Demand Feature for faster loading and expanding of Nodes in the Hosts Navigation Tree:**  
 Yes  No

Load On Demand is used for performance reasons when you have thousands of nodes in the Navigation Tree. When enabled, the following will occur:  
 1. If limiting the number of nodes, this will be a limit on nodes in the root of Hosts Home only  
 2. Only the root nodes will be visible, and collapsed, when first navigating to the tree  
 3. Expanding the nodes will retrieve the nested nodes live from the database  
 4. Searching for Folders/Hosts will behave as per normal.

**Browser Based Remote Session Settings**

**For RDP Sessions, use the following performance settings:**

If you would like to use a different Keyboard layout for RDP sessions, please select it here:

**For SSH Sessions, select the font size you would like to use in the terminal:**

**For SSH Sessions, please select the Background and Font colors that you would like to use:**

**Background Color Palette**

**Background Color:**


**Font Color Palette**

**Font Color:**


**2.4.2.3 Miscellaneous Tab**

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

<p><b>Password Visibility on Add/View/Edit Pages</b></p>	<p>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</p>
<p><b>Auto Generate New Password When Adding a New Record</b></p>	<p>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</p>

<p>Enable Search Criteria Stickiness Across Password Screens</p>	<p>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 <a href="#">Navigation Tree</a>, 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</p>
<p>Show the 'Actions' toolbar on the Passwords pages at the</p>	<p>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</p>
<p>On all Password List screens, sort the grid by the following column</p>	<p>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</p>
<p>On the Passwords Home screen, sort the Search Results and Favorite Passwords grids by the following column</p>	<p>Similar to the option above, but this sort order applies to the Search Results and Favorite Passwords grids on the Passwords Home page</p>
<p>When creating new Shared Password Lists, base the settings on the following Template's settings</p>	<p>When creating new Shared Password Lists, you can choose to automatically specify all the settings based on the selected Template</p>
<p>When creating new Shared Password Lists, base the permissions on the following Template's permissions</p>	<p>When creating new Shared Password Lists, you can choose to automatically apply permissions based on the permissions set on the selected Template</p>
<p>Locale (Date Format)</p>	<p>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</p>
<p>RDP Keyboard Layout</p>	<p>When using the Browser Based Remote Session Launcher, the default keyboard used is United States (English). This default can be change for all users on the screen Administration -&gt; Feature Access -&gt; Remote Sessions tab, or individual users can change it here on their Preferences screen</p>



 Preferences

To modify your preferences for Passwordstate, please make changes in the relevant tabs below, then click on the 'Save' button.

passwords tab   hosts tab   **miscellaneous**   color theme   authentication options   mobile access options   browser extension

Please select which of the following miscellaneous options within Passwordstate you would like to enable.

**Password Visibility on Add/View/Edit Pages:**  
 Visible  Mask

**Auto Generate New Password When Adding a New Record:**  
 Yes  No

**Enable Search Criteria Stickiness Across Password Screens:**  
 Yes  No

**Show the 'Actions' toolbar on the Passwords pages at the:**  
 Bottom  Top  Bottom & Top

**On all Password List screens, sort the grid by the following column:**  
 Do not sort by default

**On the Passwords Home screen, sort the Search Results and Favorite Passwords grids by the following column:**  
 Do not sort by default

**When creating new Shared Password Lists, base the settings on the following Template's settings:**  
 Do not use template

**When creating new Shared Password Lists, base the permissions on the following Template's permissions:**  
 Do not use template


**Locale (Date Format):**  
 Use System Wide Locale Setting


If you would like to use a different Keyboard layout for RDP sessions when using the Browser Based Launcher, please select it here.  
 -- Select Keyboard Layout --

#### 2.4.2.4 Color Theme Tab

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

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

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

 Preferences



To modify your preferences for Passwordstate, please make changes in the relevant tabs below, then click on the 'Save' button.

passwords tab   hosts tab   miscellaneous   **color theme**   authentication options   mobile access options   browser extension

Use the System Wide color theme, or choose your own:  
 System Wide    Choose My Own

Base Color  
 Please select the Base Color to use throughout Passwordstate.


Color Palette  
 Apex

Base Color:  
  

Save   Save & Close

#### 2.4.2.5 Authentication Options Tab

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

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

## Authentication Option


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

The following table describes each of the Authentication Options:

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

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

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

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

Preferences

To modify your preferences for Passwordstate, please make changes in the relevant tabs below, then click on the 'Save' button.

passwords tab   hosts tab   miscellaneous   color theme   authentication options   mobile access options   browser extension   api

Please select your preferred Authentication Option for accessing the Passwordstate web site.

**Please Note:** You only need to specify the various authentication settings if you have chosen one of them as your preferred Authentication Option, or as a secondary authentication method for a Password List.

Web Authentication Option

Please specify which Authentication options will apply to you each time you access Passwordstate.

Choose Authentication Option:

- Use the System Wide Authentication Settings
- Use the System Wide Authentication Settings
- SAML2 Authentication
- Manual Login Authentication
- Manual Login and RSA SecurID Authentication
- Manual Login and ScramblePad Authentication
- Manual Login and Email Temporary Pin Code
- Manual Login and Duo Authentication
- Manual Login and One-Time Password
- C AD Single Sign-On
- AD Single Sign-On and RSA SecurID Authentication
- AD Single Sign-On and ScramblePad Authentication
- AD Single Sign-On and Email Temporary Pin Code
- AD Single Sign-On and Duo Authentication

token type: Time-Based

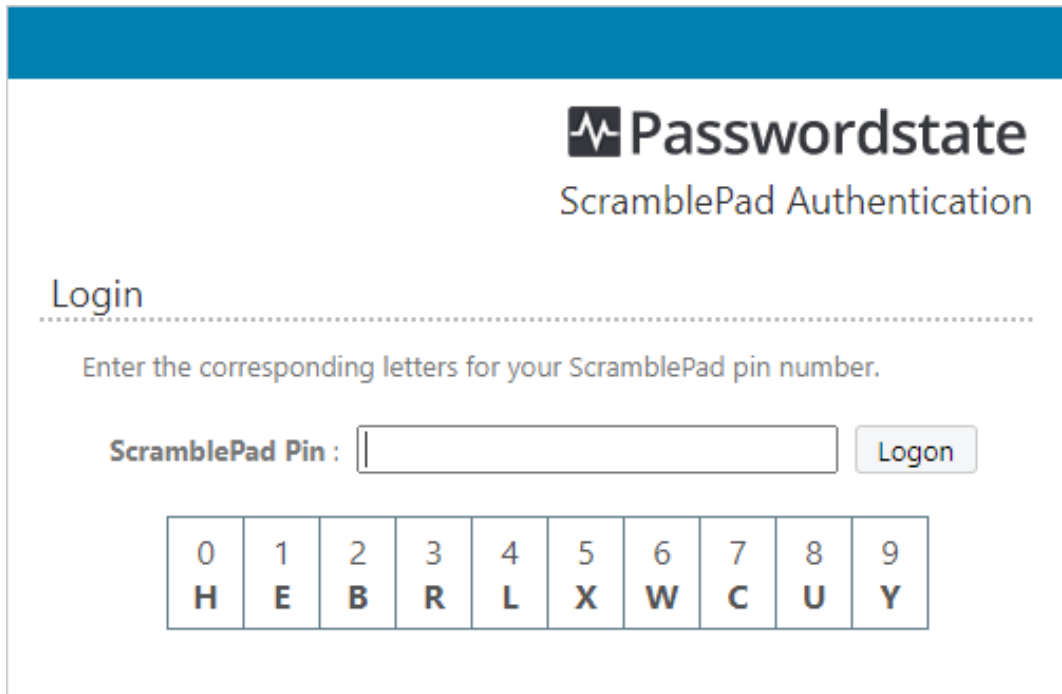
Time Step: 30 Generally 30 or 60 seconds

Token Clock Drift: 0 How many seconds your token has drifted over time

## 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.



The screenshot shows the Passwordstate ScramblePad Authentication login interface. At the top right, the Passwordstate logo is displayed above the text "ScramblePad Authentication". Below this, the word "Login" is centered. A dotted line separates the title from the instructions: "Enter the corresponding letters for your ScramblePad pin number." Below the instructions is a text input field labeled "ScramblePad Pin :". To the right of the input field is a "Logon" button. Below the input field is a grid of ten boxes, each containing a number and a corresponding letter: 0 H, 1 E, 2 B, 3 R, 4 L, 5 X, 6 W, 7 C, 8 U, 9 Y.

wylu

## Google Authenticator

---

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


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

Google Authenticator

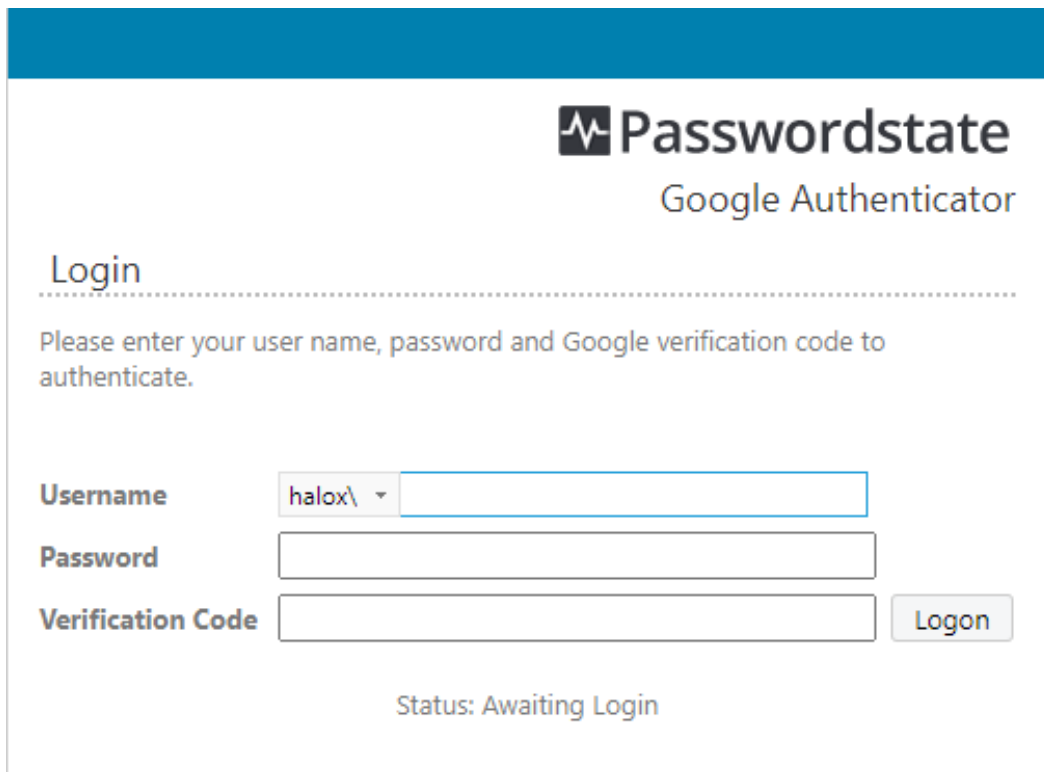
In order to use two-factor authentication with Google Authenticator and your mobile/cell device, you will need do:

1. Select the appropriate Google Authenticator option above
2. Generate a new barcode/secret key
3. Scan the barcode into Google Authenticator on your mobile device, or manually type in the displayed Secret Key
4. Click on the 'Save' button.

Secret Key:     
(not case-sensitive)



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').



Passwordstate  
Google Authenticator

Login

Please enter your user name, password and Google verification code to authenticate.

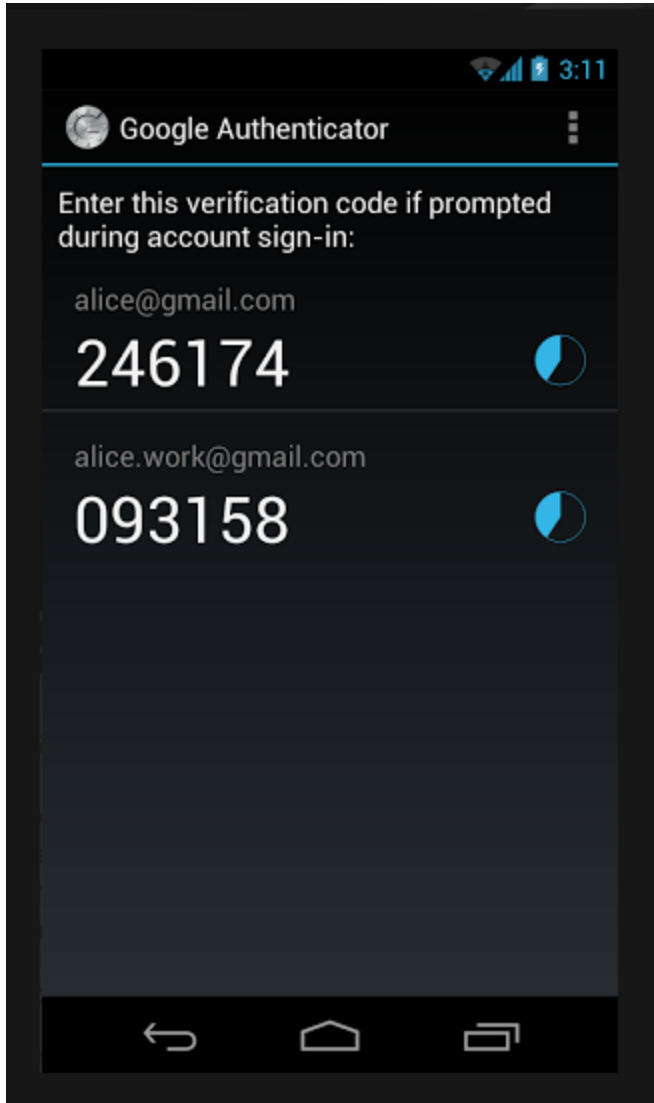
Username

Password

Verification Code

Status: Awaiting Login

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




## Email Temporary Pin Code

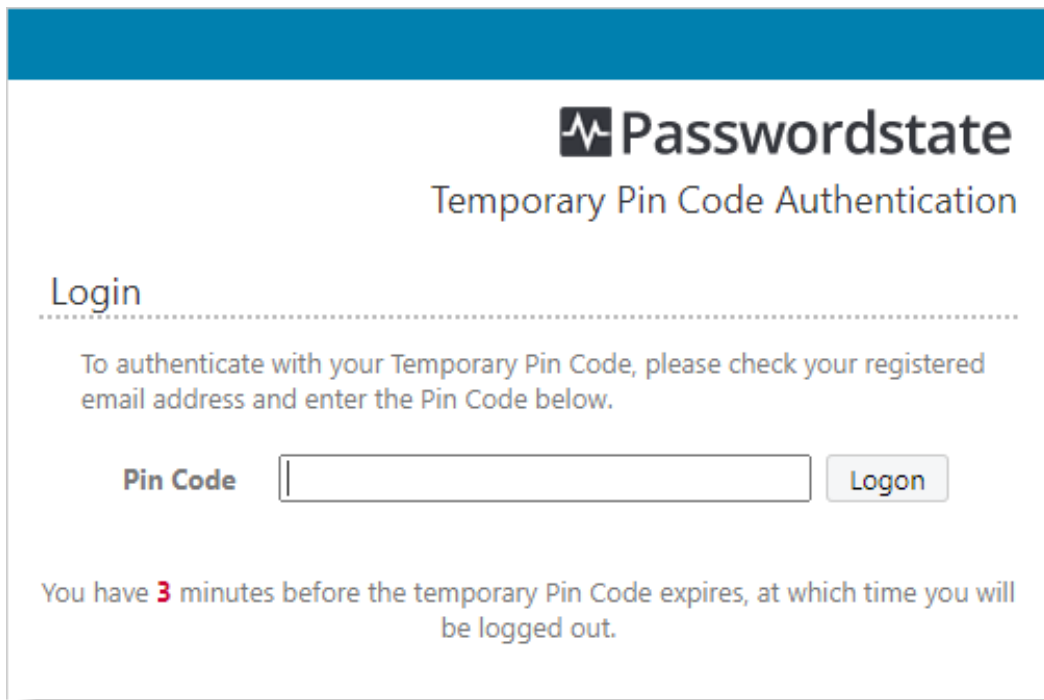
---

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

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

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





The screenshot shows a web interface for Passwordstate. At the top, there is a blue header with the Passwordstate logo and the text "Temporary Pin Code Authentication". Below this, the word "Login" is displayed. A message instructs the user to check their registered email address and enter a pin code. There is a text input field labeled "Pin Code" and a "Logon" button. A warning message at the bottom states: "You have 3 minutes before the temporary Pin Code expires, at which time you will be logged out."

## YubiKey Authentication

Passwordstate can support the following YubiKey authentication methods:

- Yubico OTP (this queries Yubico's API on the internet)
- OATH - HOTP (counter-based algorithm which does not require internet connectivity)
- OATH - TOTP (time-based algorithm which does not require internet connectivity)

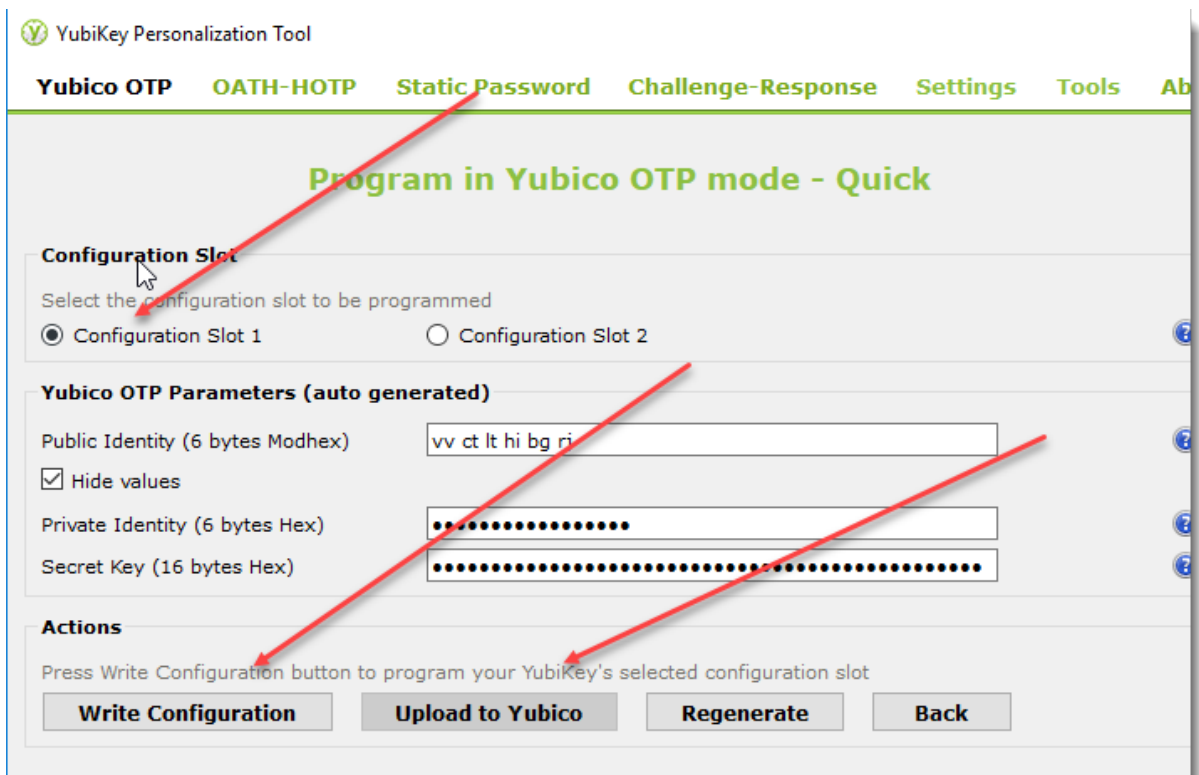
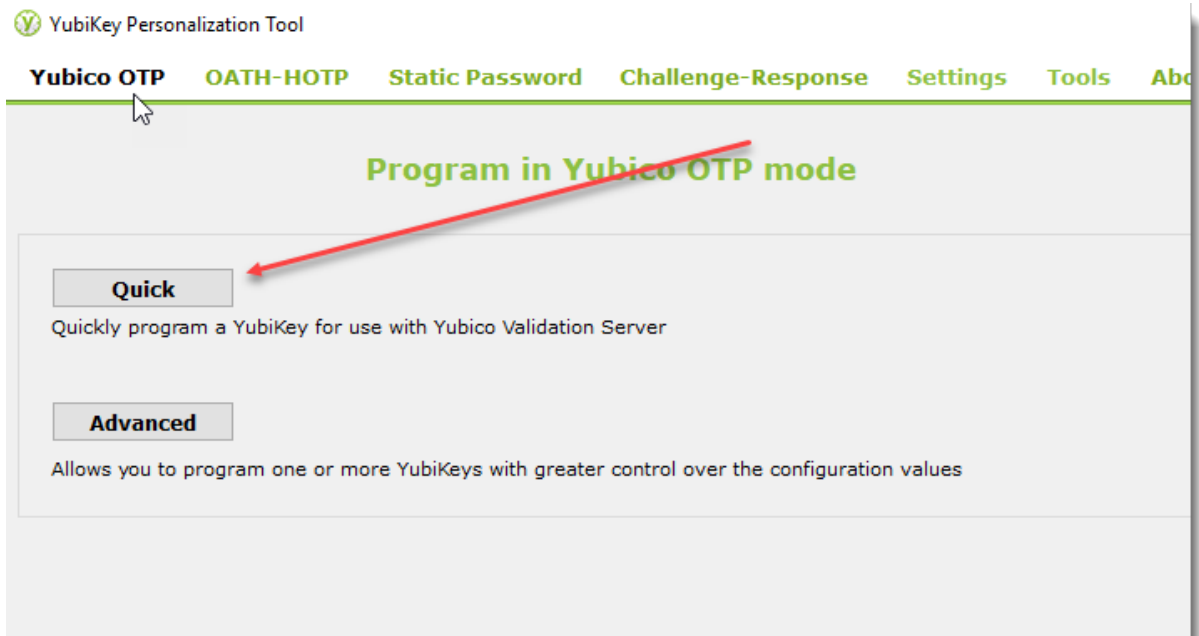
By default, new YubiKey's are configured for Yubico OTP, but the configuration can be changed using Yubico tools. Below are instructions for configuring your YubiKey for each of the authentication options above. The following tools will need to be downloaded and installed on your desktop:

- To configure for Yubico OTP or HOTP, you need this tool - <https://www.yubico.com/products/services-software/download/yubikey-personalization-tools/>
- To configure and authenticate using TOTP, you need this tool - <https://www.yubico.com/products/services-software/download/yubico-authenticator/>

### Configure YubiKey for Yubico OTP Support

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

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



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

YubiKey Authentication Settings

Select which type of YubiKey authentication method to use, and follow instructions below as appropriate:

1. Yubico OTP - give the Secret Key field focus, and press the button on your YubiKey
2. TOTP - Generate a QR Code and use the Yubico Authenticator App to scan the QR Code in
3. HOTP - Using the Yubico Personalization tool, copy and paste the HOTP Secret Key from the tool into the field below

Authentication Type:

Time Step:  Generally 30 or 60 seconds

Token Clock Drift:  How many seconds your token has drifted over time

Counter:  What the current Counter is for your token

HOTP Digits:  Generally 6 or 8 digits (for Counter-Based authentication)

Secret Key:

### Configure YubiKey for OATH - HOTP Support

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

YubiKey Personalization Tool

**Yubico OTP** OATH-HOTP Static Password Challenge-Response Settings

## Program in OATH-HOTP mode

**Quick**  
Quickly program a YubiKey in OATH-HOTP mode

**Advanced**  
Allows you to program one or more YubiKeys in OATH-HOTP mode with greater control over the configuration

YubiKey Personalization Tool

Yubico OTP OATH-HOTP Static Password Challenge-Response Settings Tools

## Program in OATH-HOTP mode - Advanced

**Configuration Slot**  
Select the configuration slot to be programmed

Configuration Slot 1  Configuration Slot 2

**Program Multiple YubiKeys**

Automatically program YubiKeys when inserted

Parameter Generation Scheme ?  
Increment Identities; Randomize Secret

**Configuration Protection (6 bytes Hex)**

YubiKey(s) unprotected - Keep it that way

Current Access Code

Use Serial Number

New Access Code

Use Serial Number

**OATH-HOTP Parameters**

OATH Token Identifier (6 bytes)

OMP (1) + TT (1) + MUI (4)

HOTP Length  6 Digits  8 Digits

Moving Factor Seed

Secret Key (20 bytes Hex)

**Actions**

Press Write Configuration button to program your YubiKey's selected configuration slot

**Results**

#	OATH Token Identifier	Status	Timestamp
---	-----------------------	--------	-----------

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

**YubiKey Authentication Settings**

Select which type of YubiKey authentication method to use, and follow instructions below as appropriate:

1. Yubico OTP - give the Secret Key field focus, and press the button on your YubiKey
2. TOTP - Generate a QR Code and use the Yubico Authenticator App to scan the QR Code in
3. HOTP - Using the Yubico Personalization tool, copy and paste the HOTP Secret Key from the tool into the field below

**Authentication Type:** OATH - HOTP  
**Time Step:** 30 Generally 30 or 60 seconds  
**Token Clock Drift:** 0 How many seconds your token has drifted over time  
**Counter:** 0 What the current Counter is for your token  
**HOTP Digits:** 6 Generally 6 or 8 digits (for Counter-Based authentication)

**Secret Key:**

### Configure YubiKey for OATH - TOTP Support

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

In Passwordstate, on your Preferences screen, you need to select 'OATH - TOTP', and click the Generate button so the QR Code is displayed.


**YubiKey Authentication Settings**

Select which type of YubiKey authentication method to use, and follow instructions below as appropriate:

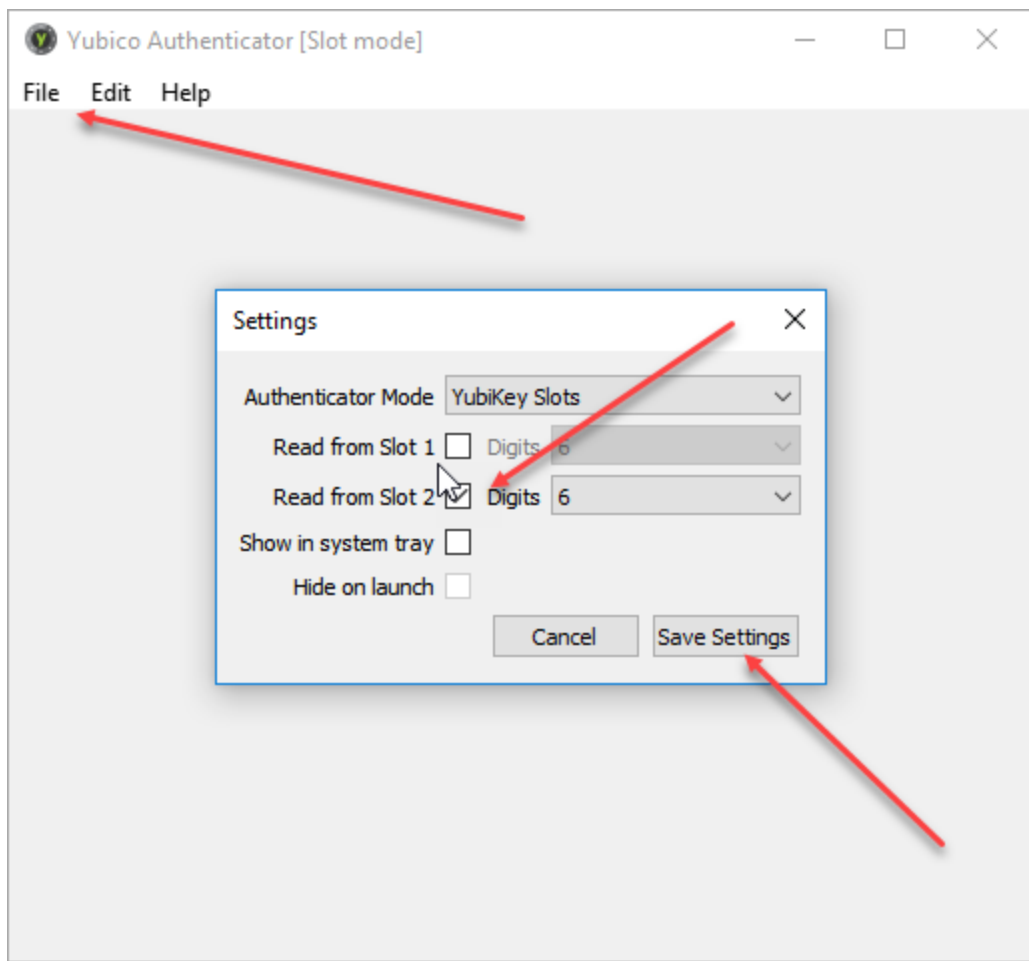
1. Yubico OTP - give the Secret Key field focus, and press the button on your YubiKey
2. TOTP - Generate a QR Code and use the Yubico Authenticator App to scan the QR Code in
3. HOTP - Using the Yubico Personalization tool, copy and paste the HOTP Secret Key from the tool into the field below

**Authentication Type:** OATH - TOTP  
**Time Step:** 30 Generally 30 or 60 seconds  
**Token Clock Drift:** 0 How many seconds your token has drifted over time  
**Counter:** 0 What the current Counter is for your token  
**HOTP Digits:** 6 Generally 6 or 8 digits (for Counter-Based authentication)

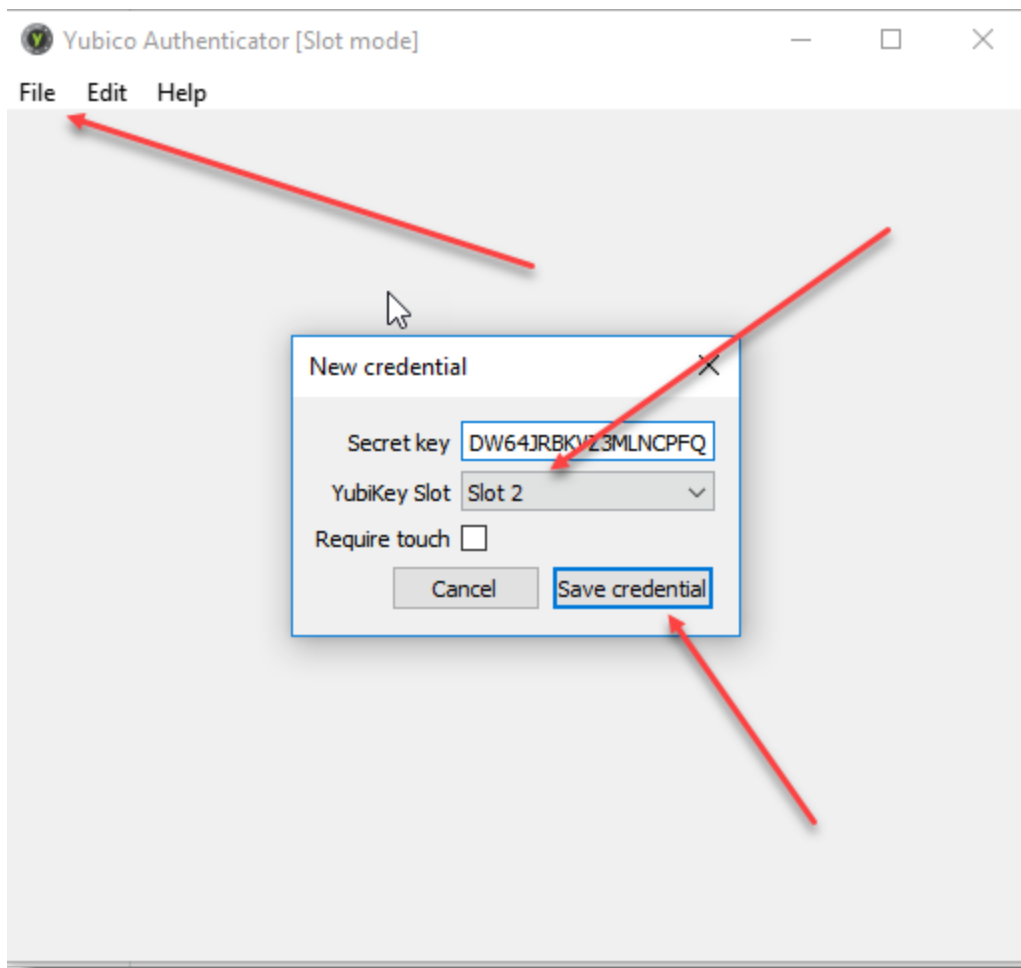
**Secret Key:**



Then in the Yubico Authenticator Application, select Settings from the File menu, and select which Slot you want to store the config in



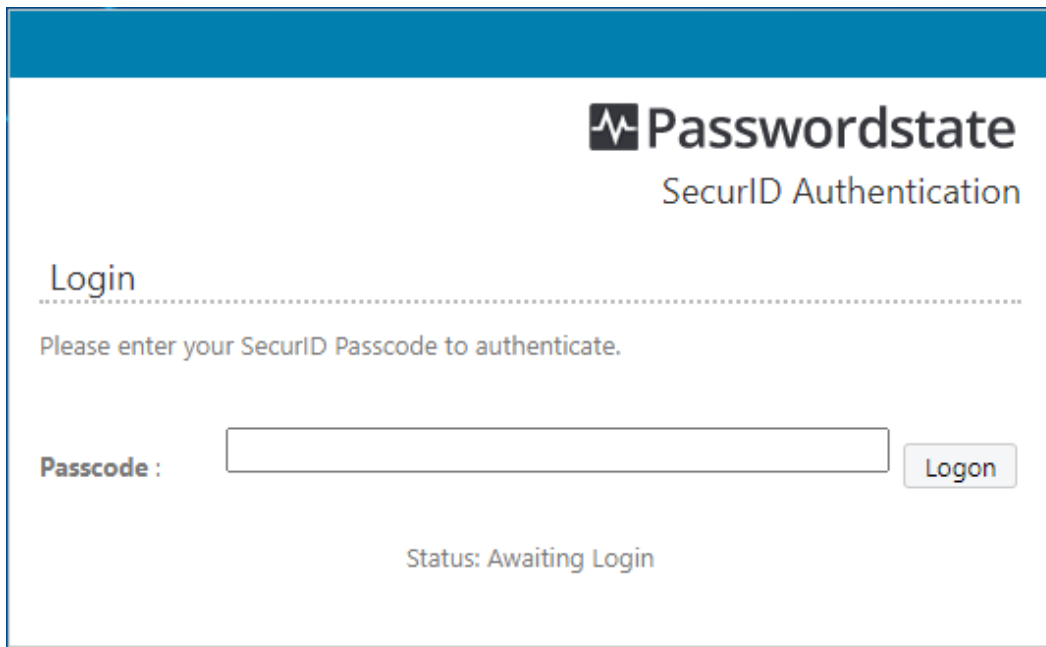
The again from the File menu, select 'Scan QR Code', and scan the code from your screen in Passwordstate, and select the Slot you want to save it into.



And then back in Passwordstate, remember to click the 'Save' button to save your Preferences.

## SecurID Authentication

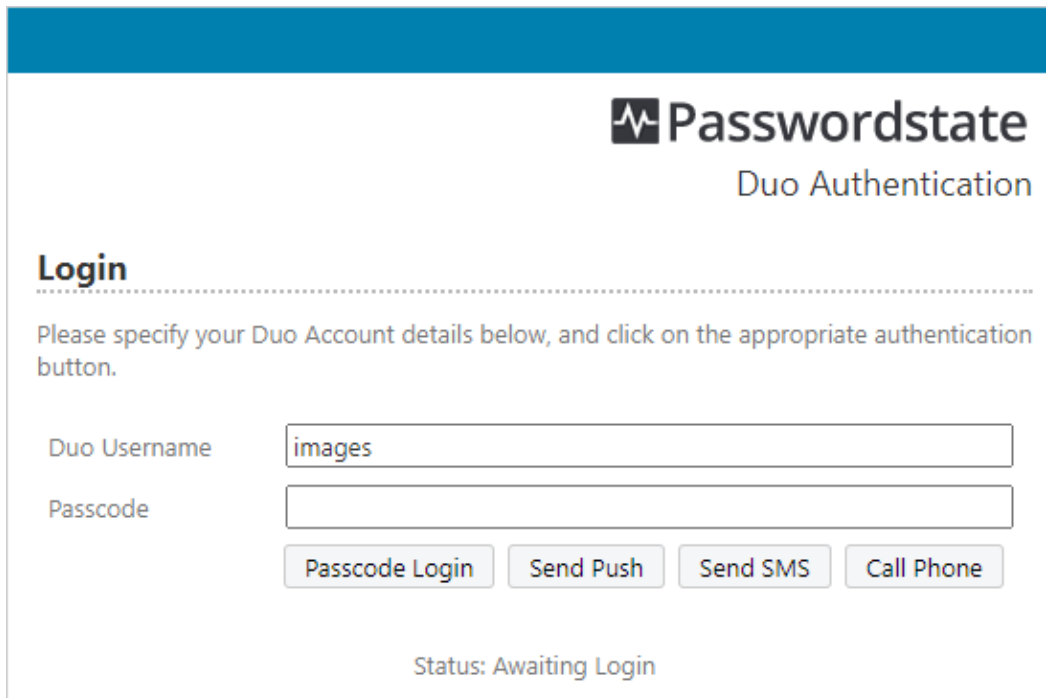
You must specify your SecurID User ID on this Preferences screen, and then you can begin to use this two-factor authentication method. Your Passcode is a combination of your Pin, plus the Tokencode.



The screenshot shows the Passwordstate SecurID Authentication login page. At the top right, there is a logo consisting of a square with a white pulse line, followed by the text "Passwordstate" in a large, bold font, and "SecurID Authentication" in a smaller font below it. Underneath the logo, the word "Login" is displayed in a large font, followed by a horizontal dotted line. Below the dotted line, the text "Please enter your SecurID Passcode to authenticate." is centered. There is a label "Passcode :" on the left, followed by a text input field. To the right of the input field is a button labeled "Logon". At the bottom center of the page, the text "Status: Awaiting Login" is displayed.

## Duo Authentication

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



The screenshot shows the Passwordstate Duo Authentication login page. At the top right, there is a logo consisting of a square with a white pulse line, followed by the text "Passwordstate" in a large, bold font, and "Duo Authentication" in a smaller font below it. Underneath the logo, the word "Login" is displayed in a large font, followed by a horizontal dotted line. Below the dotted line, the text "Please specify your Duo Account details below, and click on the appropriate authentication button." is centered. There are two labels on the left: "Duo Username" and "Passcode". The "Duo Username" label is followed by a text input field containing the text "images". The "Passcode" label is followed by an empty text input field. Below the input fields, there are four buttons: "Passcode Login", "Send Push", "Send SMS", and "Call Phone". At the bottom center of the page, the text "Status: Awaiting Login" is displayed.



## 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 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.

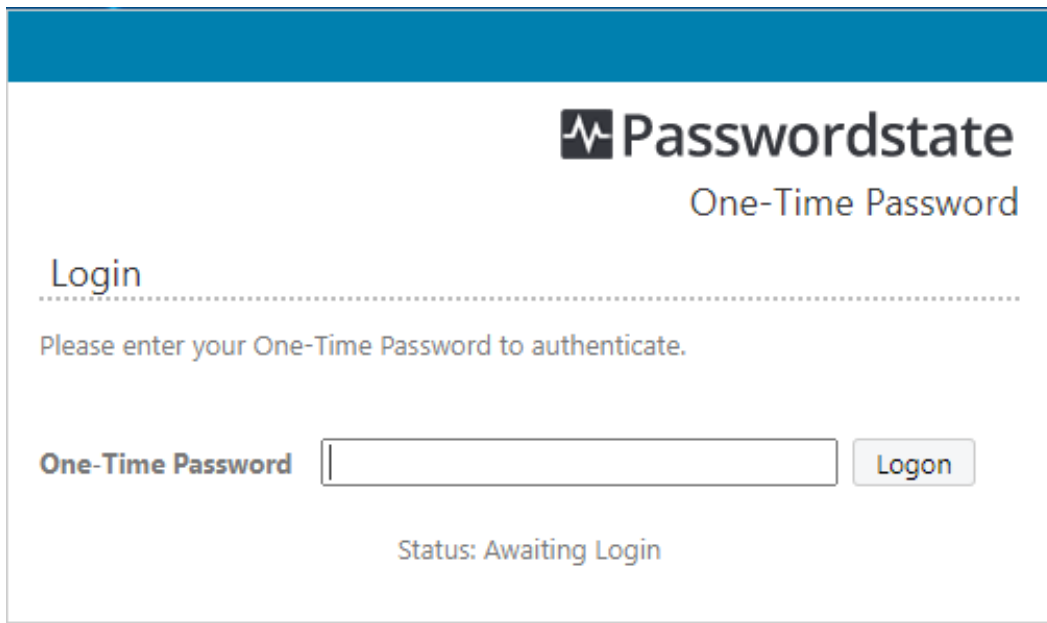
One-Time Password Settings

Select which type of One-Time Password authentication method you will use, and various settings as appropriate - these settings are only applicable if the One-Time Password Authentication option has been applied to your account.

Token Type:	<input type="text" value="Time-Based"/>	
Time Step:	<input type="text" value="30"/>	Generally 30 or 60 seconds
Token Clock Drift:	<input type="text" value="0"/>	How many seconds your token has drifted over time
Counter:	<input type="text" value="5"/>	What the current Counter is for your token
HOTP Digits:	<input type="text" value="6"/>	Generally 6 or 8 digits (for Counter-Based authentication)

Secret Key:



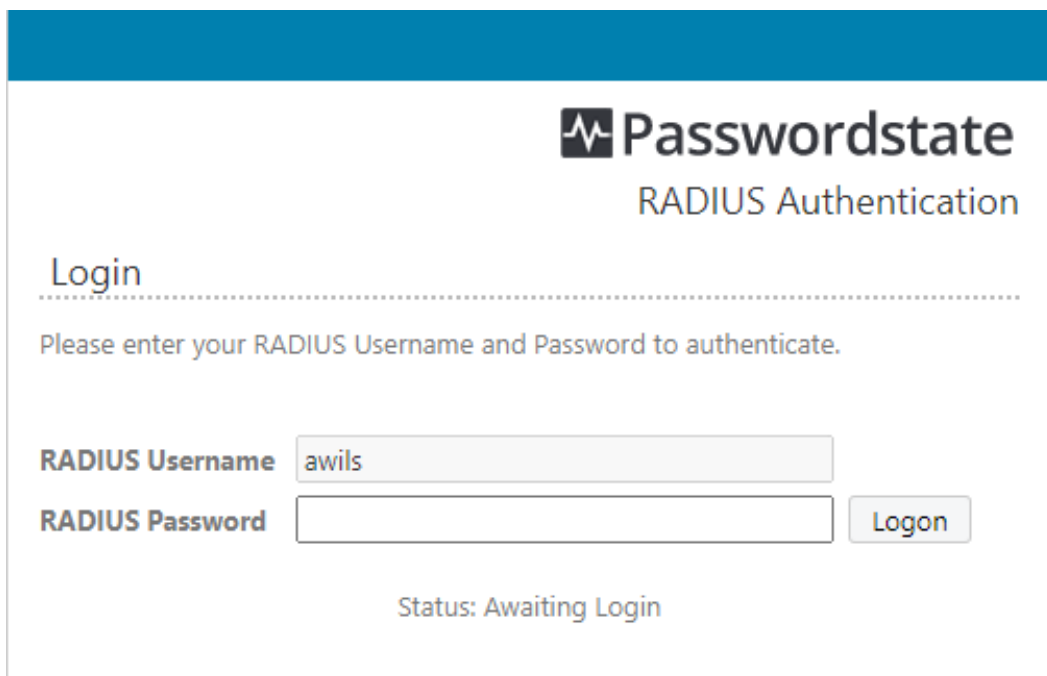


The screenshot shows the Passwordstate One-Time Password login interface. At the top right, the Passwordstate logo is displayed above the text "One-Time Password". Below this, the word "Login" is followed by a horizontal dotted line. A message reads: "Please enter your One-Time Password to authenticate." There is a text input field labeled "One-Time Password" and a "Logon" button to its right. At the bottom center, the status "Status: Awaiting Login" is shown.

## 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.



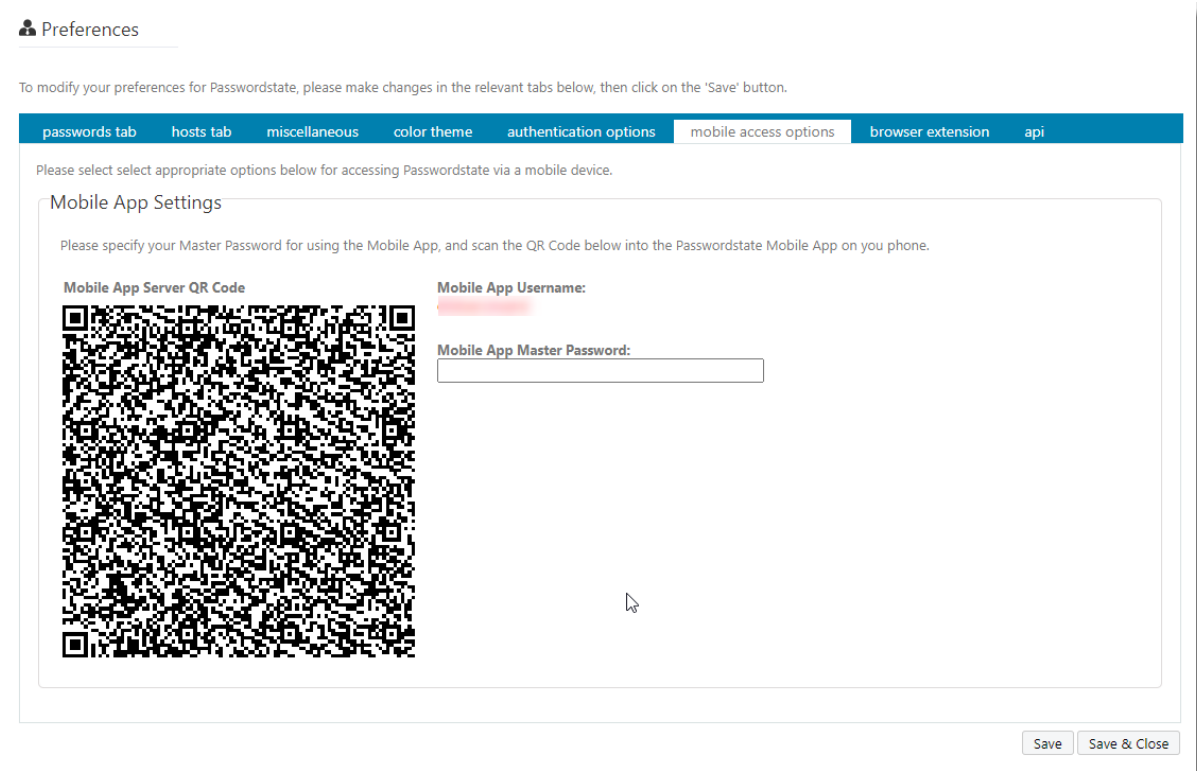
The screenshot shows the Passwordstate RADIUS Authentication login interface. At the top right, the Passwordstate logo is displayed above the text "RADIUS Authentication". Below this, the word "Login" is followed by a horizontal dotted line. A message reads: "Please enter your RADIUS Username and Password to authenticate." There are two text input fields: "RADIUS Username" containing the text "awils" and "RADIUS Password". A "Logon" button is positioned to the right of the password field. At the bottom center, the status "Status: Awaiting Login" is shown.

### 2.4.2.6 Mobile Access Options Tab

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

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

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




### 2.4.2.7 Browser Extension


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

In particular you can:

- Specify 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, form-fill the sites, or show the icon overlay
- The browser extension can also be used to automatically clear any contents in your clipboard at a set interval.

Please refer to the Browser Extension Manual for further instructions.

 **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

 Preferences

To modify your preferences for Passwordstate, please make changes in the relevant tabs below, then click on the 'Save' button.

passwords tab   hosts tab   miscellaneous   color theme   authentication options   mobile access options   browser extension   **api**

Please specify settings as appropriate below for the Passwordstate Browser extensions. Once your extension is installed, all you need to do is login to Passwordstate, and the extension will auto-configure itself.

**Extension Logout Settings**

Please specify settings below for automatically logging out of your Browser Extension.

**Automatically log out of the Browser Extension when you close the browser:**  
 Yes  No

**Automatically log out of the Browser Extension when your computer has been idle for (x) minutes:**  
 (Setting to 0 disables this feature)

**When triggering a 'Copy to Clipboard' event in Passwordstate or the Browser Extension, allow the Browser Extension to automatically clear the clipboard after (x) seconds after the event:** (You must have one of the Passwordstate browser extensions installed for this functionality)  
 (Setting to 0 disables this feature)

**Ignored URLs**

With Ignored URLs, this will prevent prompting to save login credentials for a web site, automatically form-filling the site, and displaying the icon overlay on fields on the site.

Enter the base URL here e.g. mypasswordstate.domain.com

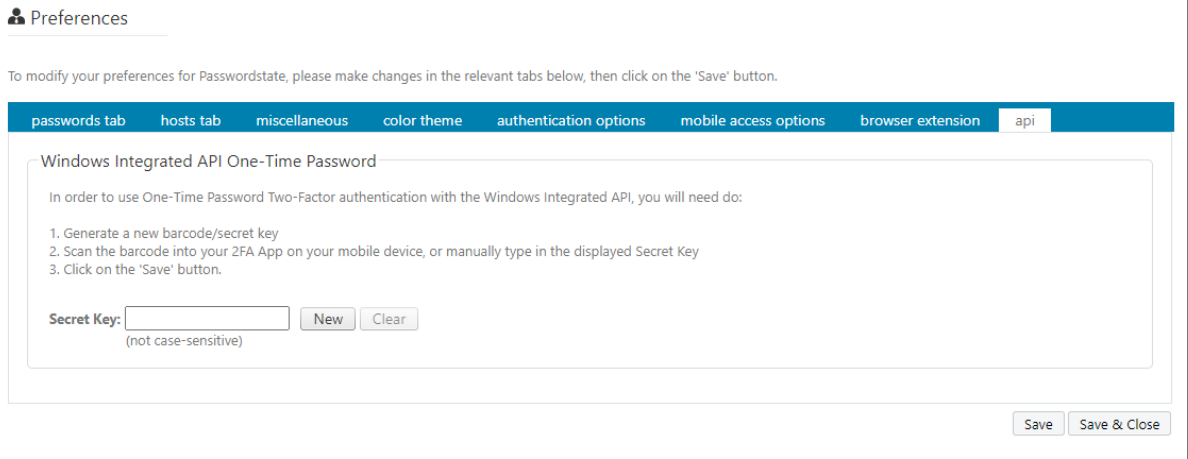
Actions	URL
	<input type="text"/>

No records to display.

#### 2.4.2.8 API

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

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



### 2.4.3 Email Notifications

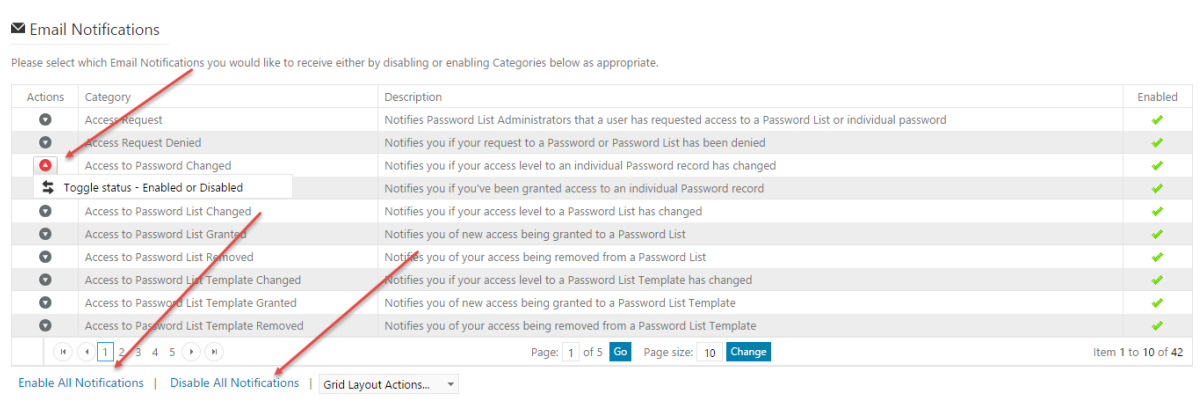
The Email Notifications screen allows you to enabled/disabled one or more of the many different email notifications Passwordstate can send you.

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

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

### Choose Email Notifications

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



## 3 Hosts

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


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


### Browser Based

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

### Client Based

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

 Note 1: By default, all users have access to all features under this Hosts tab. It is recommended a Security Administrator of Passwordstate visit the page Administration -> Passwordstate Administration -> Feature Access -> Hosts tab and Remote Sessions tab, and review each of the varying levels of access, and modify permissions as appropriate.

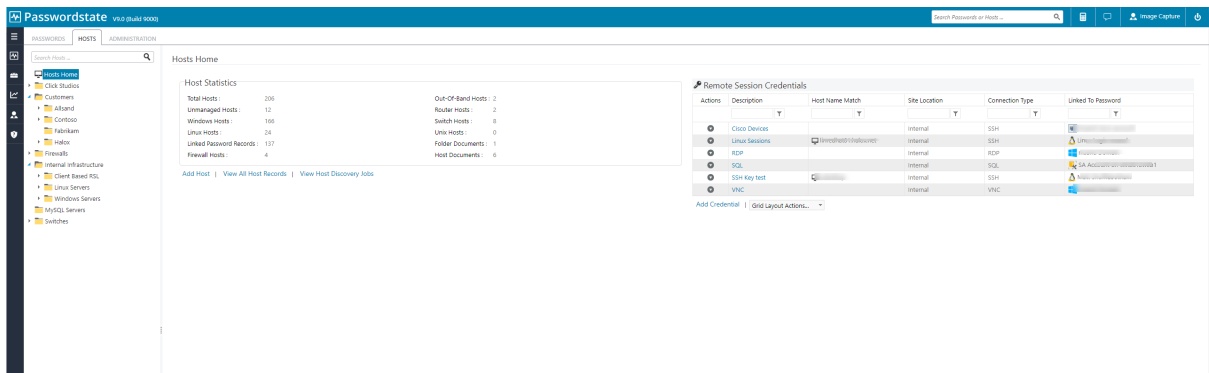
 Note 2: Microsoft have removed the ability to pass a SQL Server account password value to SQL Server Management Studio via the command line, in Management Studio 2018. Authenticating with Active Directory accounts works with Management Studio 2018, but if you wish to use SQL Accounts you will instead need to use Management Studio 2017.

### 3.1 Hosts Home Screen

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

From this screen you can:

- Click on [View All Host Records](#) to see all Host records, and manage them
- Click on [View Host Discovery Jobs](#) to manage Discovery Jobs for querying Active Directory for Host records - and import them into Passwordstate
- And manage Remote Session Credentials which can be used with the Remote Session Launcher Utility.



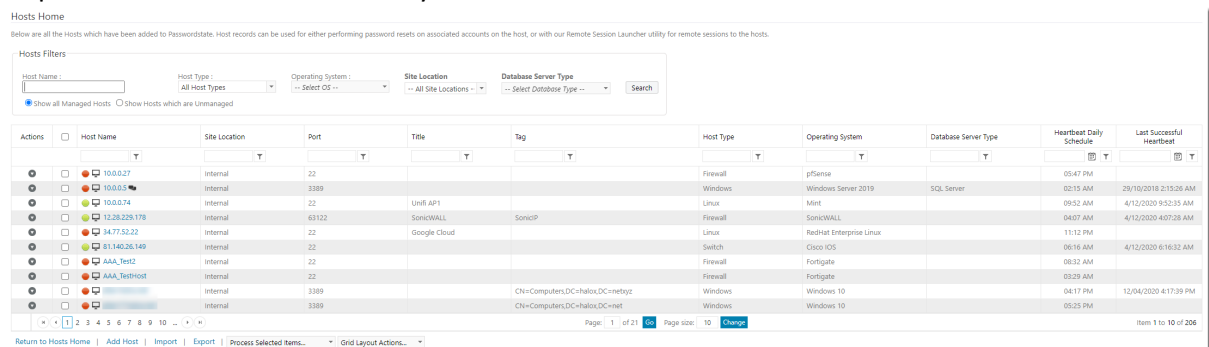
### 3.1.1 View All Host Records

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

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

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


**Note:** It is also possible to import Hosts via the Passwordstate API, or use a [Discovery Job](#) to import them from Active Directory



## Adding New Hosts Manually

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

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

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



## Add New Host

To add a new Host, please fill in the details below.

host details
notes

Please specify details for the Host as appropriate.

### General Host Properties

Host Name: \*

Fully Qualified Domain Name (FQDN) provides greater flexibility and performance, or NetBIOS name can be used if needed.

Title:

If the Title field has a value, this will be displayed in the Hosts Navigation Tree instead.

Tag:

Can be any descriptive Tag you want, which is also included in Host search results.

Site Location:

Host Type: \*

Operating System: \*

Internal IP:

External IP:

MAC Address:

Session Recording: \*  Yes  No (record all remote sessions for this Host)

Virtual Machine: \*  Yes  No

Virtual Machine Type:  Amazon  Azure  HyperV  VirtualBox  VMware  Xen

Database Server Type:

Database Instance:

This is for an SQL Server Instance, or Oracle Service Name if required.

Database Port Number:

If using default ports, blank values will generally work here.

Host Heartbeat:  Hour  Minute (time each day a Heartbeat is executed)

### Remote Connection Properties

By specifying appropriate settings below, this will allow a remote connection to the host directly from within Passwordstate.

Connection Type \*  RDP  SSH  Teamviewer  Telnet  VNC

Port Number \*

Additional Parameters

The parameters below will be passed to the Passwordstate Remote Session Launcher, in an encrypted format. If the client you're using for Remote Sessions requires additional command line parameters to function, you can specify them above.

**Parameters Passed** : Host Name, Port Number, UserName and Password

### 3.1.2 View Host Discovery Jobs

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

Host Discovery Jobs

Below are all the Host Discovery jobs added to Passwordstate, for querying Active Directory for host records.

Actions	Job Name	Description	Job Type	Site Location	Run Discovery At	Schedule Type	In Progress	Last Discovery Took	Simulation Mode	Enabled
	Import Server Hosts	Import Server Hosts	Hosts	Internal	01:00 PM	Daily	<input type="checkbox"/>	00:00:01	<input type="checkbox"/>	<input checked="" type="checkbox"/>
	Test Import	Test Import	Hosts	Internal	11:00 PM	Weekly - Sunday	<input type="checkbox"/>	00:00:01	<input type="checkbox"/>	<input checked="" type="checkbox"/>

[Return to Hosts Home](#) | [Add Discovery Job](#) | [Grid Layout Actions...](#)

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

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

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

## Edit Hosts Discovery Job

To edit settings for the Discovery job below, please make changes as appropriate and then click on the 'Save' button.

discovery job settings
active directory ous
schedule

**Discovery Job Name \*** :

**Description \*** :

**Site Location \*** :

**Active Directory Domain \*** :

**Active Directory OUs** : Please specify at least one OU on the 'Active Directory OUs' tab.

**Simulation Mode** :  Simulation Mode will email you the results without adding/updating any data in the database

**Discovery Search Criteria**

Please select which search options you would like to define for the Discovery Job.

**Discover hosts with the following Operating Systems:**

**Only discover Hosts where the Last Logged on date is greater than or equal to :**

**Discovery Actions**

**Populate the Host's Tag field with the Organizational Unit (OU) it belongs to:**

Yes  No

**When a new Host is found, set its Remote Connection Properties to :**

RDP  SSH  Telnet  VNC    Port Number:

**If an existing Host in Passwordstate is no longer found in any of the OUs specified, perform the following action for the Host record in Passwordstate:**

Do Nothing  Set it to Unmanaged  Delete it, but only when there are no associated password records  Delete it and all associated password records

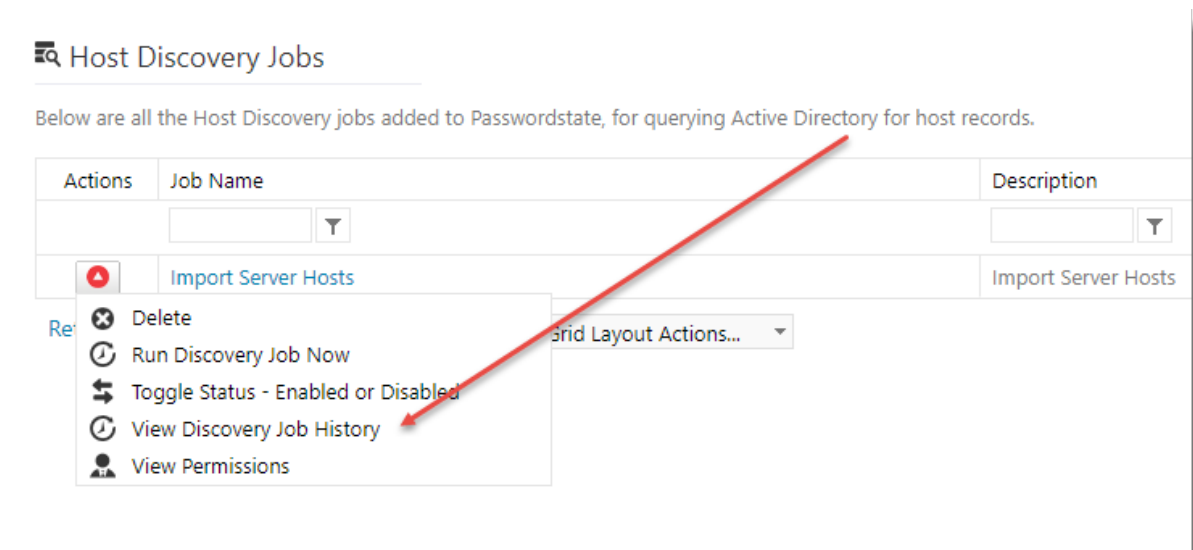
**Privileged Account Credentials**

Please select which Privileged Account Credential will be used to execute this Discovery Job.

## Discovery Job History

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

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



## 3.2 Remote Session Management

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

## 4 Administration

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


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

## 5 Help Menu

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

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

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

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