PasswordState Enterprise Password Management

Passwordstate User Manual

© 2023 Click Studios (SA) Pty Ltd

Table of Contents

	Foreword	0
Part I	Passwordstate User Manual	4
1	Glossary	
2	Quick Start Tutorials	
Part II	Passwords	13
1	Passwords Menu	15
	Passwords Home	
	Navigation Tree	
	Passw ords Home	
	Screen Options	
	Folders	
	Folder Properties	
	Clone a Folder	
	Passw ord Lists	
	Screen Options	
	Add Passw ord	
	Edit Passw ord	
	Upload Documents	
	Email Permalinks	
	Passw ord Actions	
	Check-In Passw ord	
	Copy or Email Passw ord Permalink	
	Copy or Move to Different Passw ord List	
	Filter Recent Activity on this Record	
	Link Account to Multiple Web Site URLs	
	Send Self Destruct Message	
	View & Compare History of Changes	
	View Individual Receiverd Dermissions	
	Cront New Permissions	
	View Possword Poset Dependencies	
	List Administrator Actions	
	Bulk I Indate Passwords	68
	Bulk Update Password Reset Ontions	71
	Edit Password List Properties	72
	Passw ord List Details Tab.	
	Customize Fields Tab	
	Guide Tab	
	API Key & Settings Tab	
	Save Passw ord List as Template	
	Toggle Visibility of Web API IDs	
	View Passw ord List Permissions	
	Grant New Permissions	
	View Recycle Bin	
	Add Folder	
	Add Private Password List	

	Add Shared Password List	
	Administer Bulk Permissions	
	Expiring Passwords Calendar	
	Password List Templates	
	Add New Template	
	Linked Passw ord Lists	
	Pending Access Requests	
	Request Access to Passwords	
	Toggle All Password List Visibility	
2	Tools Menu	108
	Account Discovery	
	Have I Been Pw ned Password Check	
	Import Passwords	
	Password Generator	
	Password Resets in Progress	
	Self Destruct Message	
3	Reports Menu	123
	Auditing	
	Auditing Graphs	
	Scheduled Reports	
4	Preferences Menu	
	Address Book	
	Preferences	
	Passw ords Tab	
	Hosts Tab	
	Miscellaneous Tab	
	Color Theme Tab	
	Authentication Options Tab	
	Mobile Access Options Tab	
	Brow ser Extension	
	API	
	Email Notifications	
Part III	Hosts	158
1	Hosts Home Screen	
	View All Host Records	
	View Host Discovery Jobs	
2	Remote Session Management	
Part IV	Administration	164
Part V	Help Menu	164

Part V Help Menu

3

1 Passwordstate User Manual



4

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 - <u>Glossary</u>.

Getting Started - New Users

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

1.1 Glossary

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

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

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

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' dropdown 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.

List Administrator Actions
List Administrator Actions
PASSWORD LIST ACTIONS
Bulk Delete Selected Passwords
🛉 🛉 Bulk Permissions for Individual Passwords
II ♣ Bulk Update Passwords
Bulk Update Password Reset Options
13 Convert to Shared Password List
Delete Password List
😫 Edit Password List Properties
Import Passwords
Save Password List as Template
I Toggle Visibility of Delete Checkboxes
I Toggle Visibility of Web API IDs
Niew Password List Permissions
Tiew Recycle Bin
EXPORT
All Password History Report
All Passwords Report
Enumerated Permissions Report
Have I Been Pwned Compromises
Password Strength Report
Standard Permissions Report

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'.

PASSWORDS	HOSTS	ADMINISTRATION
Search Lists or I	Folders	२ 🗟 🗘 🖈

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 ¹⁰ 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:
 - \circ View: Can only view the passwords
 - Modify: View access, plus edit and delete passwords
 - $\circ\,$ Administrator: Modify access, plus administer permissions and make changes to the Password List
- Individual Passwords:
 - \circ View: Can only view the password
 - \circ 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.

Q

Grid Layout Actions...

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

Screen Options

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.

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.

Grid Layout Actions... 💌

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 <u>Passwords Menu</u>, you can add new Folders and Password Lists, navigate back to Passwords Home, we well as various other features relating to this tabbed area of Passwordstate.



2.1 Passwords Menu

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

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

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

2.1.1 Passwords Home

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

≁	Passwordstate v9.0 (Build 9000)					
≣	PASSWORDS HOSTS ADMINISTRATION					
~	Search Lists or Folders 🭳 द 🗲 ★					
-	Passwords Home					
⊻	 Customers 					
-	Allsand					
.	Contoso					
2	Customer Template					
•	Halox					
	Sanddomain					
	4 🧰 Infrastructure					
	Active Directory Accounts					
	aD Discovery					
	a Amazon Logins					
	Cisco Network Devices					
	ESXi Accounts					
	Firewall Accounts					
	👌 Linux Accounts					
	Office 365/Azure AD Accounts					
	🕜 One-Time Passwords					
	🚥 Out of Band Management Cards					
	Routers and Switches					
	Switch Accounts					
	- Teamviewer Accounts					
	Web Sites					
	Workstation Accounts					
	Server Certificates					

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



2.1.1.1.1 Passwords Home

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

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

On this screen you can:

- Search for Passwords across all the Password Lists you have access to (from Passwords Home), or all passwords within the selected Folder. Note: To perform an exact match search, enclose your search term in double quotes i.e. "root_admin"
- View and access Passwords you've recently used i.e. viewed/editing/copied to clipboard, etc
- View your tagged Favorite Passwords
- View your tagged Favorite Password Lists
- View some basic auditing statistics statistics
- Customize the screen by clicking on the <u>Screen Options</u> 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 ² 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 <u>Password Actions</u> by selecting the appropriate menu option from the Actions drop-down menu

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



2.1.1.1.1.1 Screen Options

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

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

Dashboard Layout Tab

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

•		
Scroop Options		
Please review each of the tabs below, and customiz	e the page as required.	
dashboard layout password columns	number of records grid paging style	statistics
Drag and drop the position of each of the panels	below, and choose which panels to show or hide.	
Zone 1	Zone 2	
SEARCH PASSWORDS	FAVORITE PASSWORDS	
Show Search Passwords on this screen.	Show Favorite Passwords on this screen.	
Zone 3	Zone 4	
RECENT PASSWORDS	FAVORITE PASSWORD LISTS	
Show Recent Passwords on this screen.	Show Favorite Password Lists on this screen.	
		Sava Cancel
		Save Cancel

Password Columns Tab

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

Screen Options	abs below, and customiz	e the page as required.		
dashboard layout	password columns	number of records	grid paging style	statistics
Please specify which colu	ımns you would like disp	layed on this screen for al	'Password' grids.	
 Title Tree Path User Name Description Account Type URL Password Password Strength Expiry Date 	Pi th Lis	ease Note: It's possible to is page, but it's not possib st can have different Field	search for values in Ge le to display the columr Types for these column	neric Fields here on 1s as each Password 1s.
				Save Cancel

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.

Screen Options				
Please review each of the	tabs below, and customiz	e the page as required.		
dashboard layout	password columns	number of records	grid paging style	statistics
Please specify the numb	er of Records to display o	on the screen for the Searc	ch Results and Favorite P	asswords.
Number of records per page: 7 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 grids are set to display.

Screen Options				
ease review each of the	tabs below, and customiz	ze the page as required.		
dashboard layout	password columns	number of records	grid paging style	statistics
Please select which Pagi pagers will appear in the O Next Previous Butto	ing style you would like to e footer of the grid. Ins	o use for the Search Resul c Pages	lts and Favourite Passwoi	rds Grids - The
Next Previous Buttons	Slider		Numeric	
Change page: 🙀 ┥	• • •	•	1 2 3 4 5 6 7	8 9 10
				Save Cancel

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	tabs below and sustem	ize the page as required			
dashboard lavout	password columns	number of records	arid paging style	statistics	
You can choose to show 'stacked', and the color	w or hide the Passwords s theme.	Statistics Chart, as well as cl	hange the type of chart, w	whether the data is	
Show the Statistics	Chart				
Choose the Graph Typ	e: • Area O Line O E	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 Grap	hs' screen as well.		

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

Passwordstate van (Buid 2000)							Search Passwords or Hasts	۹ 🗄	2 Image Capture
BASSWORDS HOSTS ADMINISTRATION									
Alter of a large	Folder - Business Systems III SomerCycle Q. Sear Comparison of the Sear Part In some bund or you multi-artic prior and other Somer Comparison of the Sear Part of the Anton Document Name Add Document Toggle 0 Column Makelly	ns h Rasswords In Folder Decorption L Decorption Gel Laport Actions. *	Account Type	Modified By	Password File Size	Folder Properti St Losses: Paier D Paier D Paier Strain: Dourpool: Paintion Model Were Prevailable & External Links Add Link Joint Links	Ites Total State Annual State Annual State Marci (State Marci (State) Marci		

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	guide api key & settings
ease specify approp	priate details below for the Folder, then click on the Save Button.
Folder Proper	ties
Site Location *	Internal 💌
Folder ID *	6617
Folder Name *	Business Systems
Description	Business Systems Related Password Records
Permalink	https://passwordstate9.halox.net/fid=6617
	(you can modify the end of the Permalink URL to specify your own 'fid' value if required. The values must be unique and less than 100 characters in length.)
Descent New Adv	in users from December and December this Folder in the Nexistation Tree
Yes O No	in users from bragging and bropping this rolder in the Navigation free
5 1 1 5 ···	
Folder Permis	sion Model
Permission Mode	i la

Folder Properties Tab

On the Folder Properties tab you can:

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

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

Folder Permissions Model

There are two types of permission models available in Passwordstate:

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

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

2.1.1.1.2.2 Clone a Folder

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

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

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

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

토 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 appr	opriate details below, the click on the Save Button.
Site Location *	Internal All nested Folders & Password Lists will be marked as the selected Site above.
Folder Name *	Business Systems
Description	Business Systems Related Password Records
Clone the followin All nested Fold	ng Folders and Password Lists: lers and Password Lists O Just the nested Folders
Apply the followin	ng permissions: Dermissions O Only for my account O None
Status:	Save Save & Clone Again Cancel

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 <u>Screen Options</u> 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)

9 111 Screen Options

- You can copy a password to the clipboard by clicking on the ²³ 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 <u>Password Actions</u> 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 <u>List Administrator Actions</u> Actions drop-down list
- By clicking on one of the segments in the 'Password Strength Summary' pie chart, you can filter the results in the Passwords grid
- By clicking on one of the segments in the 'Most Active Users' pie chart, you can filter the results in the Recent Activity grid

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

2			User name	Description			Account Type	Password	Passwi	ord Strength Pas	sword Last Updated	Expiry Date			
	Andromeda			Andromeda Server			Report		**	*** 20/	01/2015 12:44:10 PM	20/01/2015		12%	/- 12%
	Centaurus	• 2		Centaurus Server1			VMware ESX	*********	**	** 20/	01/2015 12:44:21 PM	19/01/2015		1	
0	Circinus	-		Circinus Server 2				********	**	★★☆ 20/	01/2015 12:44:29 PM	21/01/2015			
2	Hercules			Hercules Server			Router	*******	**	★★☆ 2/0	5/2017 1:44:08 PM				
0	Lacerta			Lacerta Server Upda	ted BUD			*********	**	★★☆ 8/0	1/2015 12:51:50 PM				
0	Pegasus	0		Pegasus Server				*********	**	★ ☆ ☆ 29/	05/2013 11:12:10 AM	27/08/2013			
0	router1	0	router1 🔒					••••••	**	★★☆ 10/	02/2014 9:53:11 AM				
0	Serpens			Serpens Server			S Phone	***********	⊎ ★★	★★★ 26/	06/2013 2:29:07 PM	30/03/2013			
lecent	Activity ()		na Layout Accors	Ust Administrator Ad	uons										75%
te	Activity	V	UserID	First Name	Sumame	IP Address	Description						Ave	rage (12%) 🔳	Strong (75%) 🔳 Excel
11/2020	0:37:38 AM Access	s Granted	halox\images	Image	Capture	10.0.0.163	Image Capture (halox/images) g	granted Video Capture List /	Administrator Access to the Passw	ord List called 'Server Listing'.					
11/2020	020010 AM Access	s Granted	halox/images	Image	Capture	10.0.0.163	image Capture (halox)/mages) g	granted Video Capture List A	administrator Access to the Passw	ioro List called 'Server Listing'.			M	ost Active	Users (past 30 c
			٩	III Screen C	Options									• Ima	ge (2) E Lee (1)
Ctive I	Directory Acco	ounts (A	Q Ill Domain Accounts)	III Screen C	Options					🗆 Favorite 📲	ite Location (Inte	rnal) 👽 Shared Li	ist (Admin Acces	= ima	ge (2) = Lee (1)
tive l	Directory Accc	ounts (A	Q All Domain Accounts) Domain or Host	Screen C User Name	Pptions	Account Type	Password		Password Strength	Password Last Updated	ite Location (Inte Reset Status	rnal) 🐺 Shared Li Heartbeat Status	ist (Admin Acces Dependencies	• Imz (s) • Guid Managed	de Bo Streng
tive	Directory Acco Title	ounts (A	Q All Domain Accounts) Domain or Host	Screen C User Name	Dptions	Account Type	Password T		Password Strength	Favorite Int Password Last Updated	ite Location (Inte	rnal) 😨 Shared Li Heartbeat Status	ist (Admin Acces	• ima as) • Guidanaged	ge (2) = Lee (1) de Streng Expiry Date
ons	Directory Acco Title	ounts (A	Q Ill Domain Accounts) Domain or Host T thelox	User Name)ptions	Account Type	Password Y ctory		Password Strength	Favorite Favorite Password Last Updated To 1	ite Location (Inte Reset Status	rnal) 🐺 Shared Li Heartbeat Status	ist (Admin Access Dependencies 0	• ima (15) • Guidana Managed	ge (2) = Lee (1) de Streng Expiry Date
ons	Directory Accor Title T asclassdasd Check File Dists	ounts (A E T f	Q All Domain Accounts) Domain or Host T the halox	III Screen C User Name msand2 S msand S)ptions	Account Type	Password T ctory		Password Strength	Password Last Updated	ite Location (Inte Reset Status	rnal) 😨 Shared Li Heartbeat Status	ist (Admin Acces Dependencies 0 0	Imz imz is) Guid Managed X V	ge (2) = Lee (1) de Streng Expiry Date 5/10/2020
ions	Directory Accco Title T asdasdasd Check File Exists halox/aepoce	ounts (A	Q III Domain Accounts) Domain or Host T thalox thalox	III Screen C User Name msand 2 appropriate	Dptions	Account Type	Password T ctory		Password Strength	Password Last Updated \$708,2020 1482 PM \$708,2020 1482 PM \$709,2020 149255 AM	ite Location (Inte Reset Status	rnal) 😨 Shared Li Heartbeat Status	ist (Admin Acces Dependencies 0 0	• imz (s) • Gui d Managed	ge (2) = Lee (1) de Streng Expiry Date 5/10/2020 2/04/2018
Cive lions	Directory Accor Title Tasdasdasd Check File Exists halox/apppools balox/balox	ounts (A T T	Q UI Domain Accounts) Domain or Host T thalox thalox	User Name User Name msand 2 apppols 3 abbin 2)ptions	Account Type	Password T tdory tdory		Password Strength	Passwort Last Updated Sy08/2020 1/48:21 PM 31/10/2018 11:08:55 AM	Reset Status	rnal) 😨 Shared Li Heartbeat Status	ist (Admin Acces Dependencies 0 0 0	• ima is) • Guid Managed	ge (2) = Lee (1) de Bh Streng Expiry Date 5/10/2020 2/04/2018 31/08/2018
L) ctive l ions	Directory Acco Title T asdasdasd Check File Exists halox/apppools halox/apppools	ounts (A T T f	Q JII Domain Accounts) Somain or Host T thalox thalox thalox thalox	III Screen C User Name msand 2 apppools 2 bship 5	Dptions	Account Type	Password T totay totay totay totay		Password Strength ***** ***** ******	Password Last Updated Sylley2020 148:21 PM 31/10/2016 11:03:55 AM	ite Location (Inte Reset Status	rnai) 😨 Shared Li Heartbeat Status • •	ist (Admin Access Dependencies 0 0 0 0	■ ima (s) ● Guid Managed × ✓ ✓	ee (2) ■ Lee (1) Lepiny Date 5/10/2020 2/04/2018 31/08/2019
citive l	Directory Accc Title Tasdasdasd Check File Exists halox/sphpols halox/pshy.write	ounts (A T T f	Q All Domain Accounts) Domain or Host T thalox thalox thalox	User Name user Name msand 2 bhip 9 pws, write 0	Deptions	Account Type	Password T ctory ctory ctory ctory		Passoord Strength ***** ***** ***** ***** ***** ***** *****	Passorite III Passorita Lipdated Sy08/2020 148:21 PM 31/10/2018 11:03:55 AM 27/02/2020 9:51:03 AM	ite Location (Inte Reset Status	mai) ₹ Shared Li Heartbest Status	ist (Admin Access Dependencies 0 0 0 0 0 0	• Ima (s) • Guid Managed	ge (2) = Let (1) de B Streng Expiry Date 5/10/2020 2/04/2018 31/08/2019
ctive I	Directory Accor Title T adsadsasd Check File Exists halox/apppools halox/psr, with HALOXyschedtask	ounts (A T f f f f f f f f f f f f f f f f f f	Q III Domain Accounts) Domain or Host T thalox thalox thalox thalox thalox thalox	User Name User Name msand 2 apppols 3 bship 0 pvs, write 2 schedtasks 3	Pptions	Account Type Active Dire Active Dire Active Dire Active Dire Active Dire Active Dire Active Dire	Password Y ctory cto		Password Strength ***** ****** *********************	Password Last Updated Sylay 2020 1:48:21 PM 31/10/2018 11:38:55 AM 25/05/2019 851:58 AM	ite Location (Inte Reset Status	mai) 😵 Shared Li Heartbeat Status	Ist (Admin Acces Dependencies 0 0 0 0 0 0 1	 Ima S) Could Guide Guide Managed X <li< td=""><td>ge (2) ■ Lee (1) de Br Streng Expiry Date 5/10/2020 2/04/2018 31/08/2019</td></li<>	ge (2) ■ Lee (1) de Br Streng Expiry Date 5/10/2020 2/04/2018 31/08/2019
Citive I ions	Directory Accc Title T asdasdaid Check File Exists halox/brinp halox/brinp halox/brinp halox/brinp halox/brinp	ounts (A T T S S S S	Q II Domain Accounts) Somain or Hest T th halox th halox th halox th halox th halox	User Name User Name msand 2 apppols 3 bship 3 pss, write 3 schedtaks 2 statex 8	Diptions T	Account Type Active Dire Active Dire Acti	Password T today today today today today Requires Chec		Passional Strength ***** ******* ********************	Password Last Updated 5/08/2020 1:48:21 PM 3/10/2016 11:03:55 AM 25/05/2019 85:156 AM 25/05/2019 85:156 AM	ite Location (inte Reset Status	rnal) ♥ Shared Li Heartbeat Status ● ● ● ● ● ● ● ●	ist (Admin Access Dependencies 0 0 0 0 0 0 1 1	Imz	ge (2) = Lee (1) de Expiry Date 5/10/2020 2/04/2016 31/08/2019
Ctive I dions	Directory Acccr Title T asdasdasd Check File Exists halox/psrip halox/psrip halox/psrip halox/psrip mares Farthing	ounts (A T T S S T T S S S T T S S S S S S S S	Q Ul Domain Accounts) Domain or Host T The second secon	User Name User Name msand 2 msand 3 appools 3 bship 6 pss, write 4 statex 3 farja 6	Deptions	Account Type Active Dire Active Dire Acti	Password T tory tory tory tory tory tory Requires Chec tory tory		Password Strength ***** ****** ****** ******	Password Last Updated Password Last Updated Syn8/2020 1:48:21 PM 31/10/2016 11:03:55 AM 27/02/2020 951:03 AM 25/02/2020 951:03 AM 21/06/2020 11:57:20 AM	ite Location (Inte Reset Status	mai) ₹ Shared Li Heartbat Status ● ● ● ● ●	ist (Admin Acces Dependencies 0 0 0 0 0 1 1 1 1 0	 Ima Ima Guida Managed X X	de Bh Streng Expiry Date 5/10/2020 2/04/2016 31/08/2019
Ctive I tions	Directory Accc Title Title Check File Exists halox,pappod halox,pay, write Halox,park Halox,taktes James Farthing James Farthing	ounts φ τ τ ε ε ε ε ε ε ε ε ε ε ε ε ε ε ε ε ε	Q UI Domain Accounts) Domain or Host T T A halox A halox A halox A halox A halox A halox A halox A halox	III Screen C User Name msand 2 msand 2 babip 3 pos, write 3 schedtasis statex 9 faja	Pptions	Account Type	Password T ctory cto	kout	Password Strength ***** ****** *********************	Password Last Updated 5/08/2020 148-21 PM 31/10/2018 10-55 AM 27/02/2020 9-51:03 AM 25/05/2020 15:03 AM 25/05/2020 15:03 AM 25/05/2020 15:03 AM	ite Location (Inter Reset Status	rnal) V Shared Li Heartbeat Status • • • • • • • • • • • • • • • • • • •	Ist (Admin Acces Dependencies 0 0 0 0 0 0 1 1 1 0 0	 Ima Solution Managed X <l< td=""><td>ge (2) = Lee (1) de Bh Streng Expiry Date 5/10/2020 2/04/2018 31/08/2019 13/12/2018</td></l<>	ge (2) = Lee (1) de Bh Streng Expiry Date 5/10/2020 2/04/2018 31/08/2019 13/12/2018

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 **\F**, 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.

Screen Options					
ease review each of the t	abs below, and custor	nize the page as required.			
password columns	passwords grid	recent activity grid	grid paging style	chart settings	
Visible Columns		Apply to the following Pas	ssword Lists (Show All) (Select All)	
Title					
🗹 User Name					
Description					
Account Type					
 Password Strength 					
Expiry Date					
					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 or 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 b display on the screen.	elow, please select wh	ich attributes you would I	ike to show or hide, and	how many records you would like to
🗆 Filters 🗹 Header				
Number of records per p	age:			
Note: specifying 0 will di	isplay all records, but c	an slow down page rende	ering significantly if you l	nave 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 Hease 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. If Visible Header Number of records per page: 5 Note: specifying 0 will display all records, but can slow down page rendering significantly if you have many records to display.					
 A screen Options Idease 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: 5 Note: specifying 0 will display all records, but can slow down page rendering significantly if you have many records to display. 	Scroon Ontions				
lease 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. Image: Comparison of the screen of the	Screen Options				
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. Image: Constraint of the screen of	lease review each of the ta	abs below, and custom	ize the page as required.		
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: S Note: specifying 0 will display all records, but can slow down page rendering significantly if you have many records to display.	password columns	passwords grid	recent activity grid	grid paging style	chart settings
	Visible Header Number of records per p 5 Note: specifying 0 will di	age: splay all records, but c	an slow down page rende	ering significantly if you	have many records to display.

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.

password columns	passwords grid	recent activity grid	grid paging style	chart settings
Please select which Pagin of the grid.	ig style you would like	to use for the Passwords	and Recent Activity Grids	- The pagers will appear in the footer
Next Previous Buttor	ns OSlider ONume	ric Pages		
Next Previous Buttons	Slider		Numeric	
Change page: 🔟 🔹 🕨	н н	•	1 2 3 4 5 6 7	8 9 10

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.

ease review each of the t	tabs below, and custom	lize the page as required.			
password columns	passwords grid	recent activity grid	grid paging style	chart settings	
You can choose to show	or hide the Pie Charts,	as well as select a color th	heme for them.		
✓ Visible					
Choose Color Theme :	Blue Opal	-			

2.1.1.2.2 Add Passw ord

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

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

Password Details Tab

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

A few things to note on this tab is:

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

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

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

-	
password details	notes security
Title *	
UserName	
Description	
Expiry Date	Ê
Password Generator	Default Password Generator
Password *	M 😫 🔍 🖩 🛬 😭
Confirm Password *	
Password Strength	$\bigstar \dot{x} \dot{x} \dot{x} \dot{x} \dot{x}$ Compliance Strength $\bigstar \bigstar \bigstar \dot{x} \dot{x}$
Strength Status:	
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 Z Enabled for Heartbeat
Account Type	- Select Account Type -
Domain or Host	٥,
UserName	8
Description	
Expiry Date	
Password Generator	Default Password Generator
Password *	
Descriver d Strength	
Strength Status:	
	Compliance Mandatory Vervent 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.

☑ Add New Password Add new password to 'Servers' Password List (Tree Path = \Customers \ Customer's A). password details notes I ★ FB @ B I U = E E E E A + Ø + Font Name • Real... • ♥ I ★ FB @ B I & U = E E E E E E SE A + Ø + Font Name • Real... • ♥ Save Save & Add Another Cancel

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.

-	
password details not	les security reset options heartbeat options
Password Security Se	tungs ta
Password Requires Check	: Out
Change Password On Che	eck In
Check In Automatically A	fter 01 Hour(s) 00 Minute(s) Setting to 00:00 will disable automatic check-in.
Password Export	Allow this Password to be Exported

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 <u>Bulk Update Password Reset</u> <u>Options</u> feature

	ra ae	tails	note	s sec	urity	reset	option	S	heartb	eat optio	ns			
assw	ord	Reset	Script	and Priv	ileged A	ccoui	nt Cree	dentia	als					
lease asswo	select ord re	t the ap set.	propriat	e Passwo	rd Reset S	cript, a	nd Privi	leged	Account	t Credenti	al, in ord	ler to pe	rform th	ne
Passw	ord R	eset Scr	ipt	Select	Password	Reset	Script -	-				*		
Privile	ged A	ccount		Select	if Require	ed						*		
assw	ord	Reset	Schedu	ıle										
VI	hen th	nis Pass	word ex	pires, Auto	o-Generat	e a nev	v one a	nd per	form an	y reset ta:	sks at the	e time of	f:	
0	6 -	Hour	00 -	Minute,	and add	90	Day(s)	-	to the	Expiry Dat	te.			

ation Options rd Validation Script to			
rd Validation Script to			
he password is correct:	use for the Heartbeat ve	erification, and what sche	dule you would like
n Script		-	
d every day at: Minute			
e ti	on Script eged Account Credential tion (only used for Linux a r d every day at: 8 v Minute	eged Account Credential selected on the 'Reset (tion (only used for Linux accounts if required): rd every day at:	eged Account Credential selected on the 'Reset Options' tab to perform the tion (only used for Linux accounts if required): rd every day at:

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

Edit Passwo	rd	
password detai		e Path = \Customers\Halox).
Heartbeat Va Select the Pase to use to valida	lidation Options word Validation Script to use for the Heartbeat verification, and what s te the password is correct:	chedule you would like
Validate Pass Use the Pr for this vali	vileged Account Credential selected on the 'Reset Options' tab to perfor lation (only used for Linux accounts if required):	m the authentication
15 • Hour	36 Vinute	

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.

📒 Windo	ws Admin Accounts			
Actions	Title	Domain or Host	User Name	Description
0	appserver01\admin1	☐ appserver01.sanddomain.com	admin1 😫	Local Administrator Acc on appserver01.sanddoma
0	appserver01\Administrator	p appserver01.sanddomain.com	Administrator 😫	Local Administrator Acc on appserver01.sanddoma
• (appserver01\marlee	p appserver01.sanddomain.com	marlee 😫	Local Administrator Acc on appserver01.sanddoma
0	desktop10\marlee	Q desktop10.sanddomain.com	marlee 😫	Local Administrator Acc on desktop10.sanddomain
0	desktop10\TestUser1	₽ desktop10.sanddomain.com	TestUser1 😫	Local Administrator Acc on desktop10.sanddomain
0	desktop10\TestUser2	Ç desktop 10. sanddomain.com	TestUser2 😫	Local Administrator Acc on desktop10.sanddomain

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.

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

ase eart the password	below, stored within the Active inection		ratii – (initastructure).
password details	notes security reset option	is heartbeat options	
Title *	James Furthing		♀
Managed Account	Enabled for Resets Enabled for	or Heartbeat	
Account Type	2 Active Directory		
Domain	halox ×	Q	
UserName	farja		9
Description]
Expiry Date	13/12/2018		
Password Generator	SQL Password Generator	<u>~</u> -	
Password *		*	😫 🔍 🖩 🖖 🔚 🤎
Confirm Password *	•••••]
Password Strength	\star \star \star \star \star \star \star Compliance Str	ength \star ★ ★ ★	
Strength Status: 1 more	e characters		
🗘 Reset Tasks (1)	🗵 Added via Discovery 🛛 🗵 Complia	ance Mandatory 🗵 Prevent Ba	d Password

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).

litle *	Test Password	0
] *]
UserName	msand	J <mark>8</mark>
Description]
Expiry Date		Ê
Deceword Concreter		
Password Generator	Default Password Generator	
Password *	····· ··· ··· ··· ··· ··· ··· ··· ···	😢 🔍 🖩 🖖 🔚
Confirm Password *]
Password Strength	\star \star \star \star \star Compliance Strength \star \star \star \star	
Strength Status: Excelle	ent password strength	
Reset Tasks (0)	🛛 Added via Discovery 🛛 🔣 Compliance Mandatory 📝 Prevent Ba	d Password

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.

쩐 Edit Password	
Please edit the password below, stored within the 'Windows Accounts' Password List (Tree Path = \Infrastructure).	
password details notes security active directory actions reset options heartbeat 🄇 🕨	
 You can perform any one of the following Active Directory Actions when you click on the 'Save' button. These actions will occur regardless of whether you change the password for this account or not. Unlock this account if locked User must change password at next logon Disable this account Enable this account 	
Password Reset tasks will be queued if Password updated. Save 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 Privileged Account Credential to associate with the record so a Password Reset can occurnot 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 <u>Bulk Update Password Reset</u> <u>Options</u> feature

M Edit Decoverd
Please edit the password below, stored within the 'Active Directory Accounts' Password List (Tree Path = \Infrastructure).
password details notes security reset options heartbeat options
Password Reset Script and Privileged Account Credentials
Please select the appropriate Password Reset ocript, and Privileged Account Credential, in order to perform the password reset.
Password Reset Script Reset Active Directory Password
Privileged Account Update Active Directory Account Passwords
 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: 00 - Hour 00 - Minute, and add 45 Day(s) - to the Expiry Date.
Password Reset tasks will be queued if Password updated. Save Cancel

🔁 Edit Password

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

sword details	notes	security	active directory actions	reset options	heartbeat options	< >
Heartbeat	Validatio	n Options –				
Select the P to use to va	assword Va	alidation Scrip assword is con	it to use for the Heartbeat ve rect:	rification, and what so	chedule you would like	
Validate Pa	assword for	Active Director	ry Account			
Use the for this y	Privileged validation (c	Account Crede only used for Li	ntial selected on the 'Reset (inux root accounts if required	Options' tab to perform i):	m the authentication	
09 - Ho	our 40 -	Minute				
Password Res	set tasks wil	l 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.

Actions	Document Name	Description	Modified	Modified By	File Size
0	Installation_Instructions.pdf	Passwordstate Installation Instructions	20/06/2013	Mark Sandford	1.1 MB
0	Preinstallation_Checklist.pdf	Passwordstate Preinstallation Checklist	20/06/2013	Mark Sandford	381 KB
0	Upgrade_Instructions.docx	Upgrade Instructions	20/06/2013	Mark Sandford	39 KB

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 * Search for people... Password Permalink Subject Permalink https://passwordstate9.halox.net/pid=67918 | 💥 🛍 👜 B I U | 🚍 🚍 🚍 | 🔄 🗄 🛱 🛱 | 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 Send Email Close

2.1.1.2.6 Passw ord Actions

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

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

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

2.1.1.2.6.1 Check-In Password

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

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

```	reen Options			
counts				
tle	User Name	Description	Password	Passwo
T	Т	T		
dministrator on Hyperv1	administrator 😫		***********	**
arlee on CentOS 🛛 🖈 🔗	marlee 😫		******	**
arlee on Marks-Imac	marlee 😫		******	**
ot	root 😫	Root account for all machines	Requires Checkout	**
ot on LinRedhatTest1	root 😫	Updated today.	***	**
st1	test1 😫	test1 on linredhattest1	******* 😢	**
stHistory	TestHistory 😫		*******	**
and	tsand 😫	tsand Local Account	****	**
ti a a c c s s a	e ministrator on Hyperv1 rlee on CentOS ★ d rlee on Marks-Imac it to n LinRedhatTest1 t1 tHistory nd	e User Name ▼ ▼ ministrator on Hyperv1 administrator a rlee on CentOS ★ oP marke B marke C it root B it on LinRedhatTest1 root C it1 test I itHistory TestHistory B ind tsand B	Sounts e User Name Description T T T ministrator on Hyperv1 administrator 9 T administrator 9 administrator 9 T rifee on CentOS * 0* marke 9 att root 9 Root account for all machines att root 9 Updated today. t1 test 9 test 1 on linredhattest1 tHistory TestHistory 9 tsand 9 nd tsand 9 tsand Local Account	Perform User Name Description Password ▼ ▼ ▼ ▼ Iministrator on Hyperv1 administrator 9 Iministrator 9 Iministrator 9 administrator on Hyperv1 administrator 9 Iministrator 9 Iministrator 9 rife on CentOS ★ P marke 9 Iministrator 9 rife on Marks-Imac marke 9 Iministrator 9 Iministrator 9 rife on Marks-Imac marke 9 Iministrator 9 Iministrator 9 rife on Marks-Imac marke 9 Iministrator 9 Iministrator 9 rife on CentOS ★ P marke 9 Iministrator 9 Iministrator 9 rife on Marks-Imac more 9 Iministrator 9

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

☑ Check Out Required	
This password record must be checked out in order to give you exclusive ac Would you like to check out this record?	cess to it.
	Yes No

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.

ctions	Title	User Name	Description	Password
	T	T	T	
0	Administrator on Hyperv1	administrator 😫		*****
0	marlee on CentOS 🗶 🔗	marlee 😫		*****
0	marlee on Marks-Imac	marlee 😫		*****
0	root	root 😫	Root account for all machines	Checked Out (i)
0	root on LinRedhatTest1	root 😫	Updated today.	****
0	test1	test1 😫	test1 on linredhattest1	*****
0	TestHistory	TestHistory 😫		******
0	tsand	tsand 😫	tsand Local Account	*******

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 Passw ord 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.

Copy or Email Pas	sword Permalink	
To email another user the Pa	ssword Link details below, please select the user from the dro	p-down list below.
Select Email Address *	Search for people)
Subject	Password Permalink	
Permalink	https://passwordstate9.halox.net/pid=67918	
🗙 🛍 🖨 B Z 🗵	🚍 🚍 🗮]፰ 🗄 🚝 🗱 A ▪ ♠ ▪ Verdana	12px ■ abc abc
цi		
Image Capture is sending	g you the following Password Permalink.	
Password: Games Card		
Password List: Credit C Permalink: https://pass	ards wordstate9.halox.net/pid=67918	
Decoverdatata 0.0. Coc	in Decourd Management	
https://passwordstate9.h	nalox.net	
🖊 Design 🔍 Preview		.::
		Send Email Close

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
A Passwords Home
4 🛅 Business Systems
Credit Cards
🖳 Database Accounts
🖳 Microsoft SQL Local Accounts
Oracle ERP Accounts
Shared Team Passwords
SharePoint Accounts
SSL Certificates
Fest 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 Farthin g. UserNimme = Fagia. Were Password 'Une Visitory'
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 g. UserNimme = faight. View Password (View Vistory)
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 validated the password for the Active Directory account halon(farja (Infrastructure)Active Directory Accounts). Error = Failed to validate the Active Directory pas sword for account halon(farja 'UserName or Password's incorrect, or account is locked/disabled. View Password 'UserWindory
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 validated the password for the Active Directory account halon(farja (Infrastructure)Active Directory Accounts). Error = Failed to validate the Active Directory pas sword for account halon(farja (Unfrastructure)Active Directory Accounts). Error = Failed to validate the Active Directory pas "Wer Assword (Verwintory)"
18/11/2020 12:00:11 PM	Password Validation Failed	WindowsService	Windows Service	Account	10.0.0.91	A scheduled Account Hearbeat check failed to validated the password for the Active Directory account halon(farja (Infrastructure)Active Directory Accounts). Error = Failed to validate the Active Directory pas sword for account halon(farja'). UserName or Password is incorrect, or account is locked/disabled. View Password UserWrithory
Change page: H	4 b N					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 Ac	count to Multiple Web Site URLs			
By listing add	itional URLs below, you can be logging into multiple URLs using t	he same Username and Password value from the	parent record with the Browser Extensions for F	Passwordstate - for Chrome and Firefox.
Linked URL		Add		
Actions	URL	UserName Field ID	Password Field ID	
0	http://win2k19apps1:8090	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:

- Specify the message, how long the message will be active for, and how many times the message can be viewed
- 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 <u>Address Book</u> 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.

Aessage Content	Email to Recipient	Passphrase Protection	
nter the contents of the Self Dest	truct message you want the recipient to read.		
💥 🛍 🛱 B / 🗓 📥	ॾ ॾ ॾ ऺॗ E ≇ ≇ A · ♠ ·	"Segoe UI", T 🔻 13px 🔹	
HostName: Username: atsadmin Description: SonicWALL Account	it on 12.28.229.178		
AccountType: SonicWALL Password: [Updated When Mes: Expiry Date: 19/08/2018	sage Sent - Do Not Alter]		
AccountType: SonicWALL Password: [Updated When Mes: Expiry Date: 19/08/2018 Preview Preview	sage Sent - Do Not Alter]		.:
AccountType: SonicWALL Password: [Updated When Mess Expiry Date: 19/08/2018 Preview Automatically self-destruct this me	sage Sent - Do Not Alter] essage if not viewed in: 3 days		.:i
AccountType: SonicWALL Password: [Updated When Mess Expiry Date: 19/08/2018 Design Q Preview Automatically self-destruct this me sllow the self-destruct message to	essage if not viewed in: 3 days		.::

you want Passwordst	tate to send the Self Destruct Message Email and URL, please select the Recipient below. Otherwise	e, please click the
CRE DIREON.		
Select Recipient	Click Studios (support@clickstudios.com.au)	-
Subject	Passwordstate - Self Destruct Message	
X ≞ ĝ B <i>I</i>	$T \ \underline{U} \mid \equiv \equiv \equiv \equiv \stackrel{1}{\underline{\exists}} \equiv \equiv \ddagger \blacksquare \stackrel{1}{\underline{\exists}} \equiv \equiv \ddagger \blacksquare \mathbf{A} \cdot \boldsymbol{\Diamond} \cdot \text{Verdana} \cdot 12px \cdot \stackrel{abc}{\underline{\bullet}} $	
OIL DEIOW.		
URL: <u>https://passw</u> This message will e: Passwordstate 9.0 - https://passwordsta	vordstate9appserver.halox.net/selfdestruct/?id=902af4360fc64bb1b43f9b6fb9968e44 expire [ExpirePeriod] from the time of this email being sent. - Secure Password Management. ate9.halox.net	
URL: <u>https://passw</u> This message will e: Passwordstate 9.0 - https://passwordstate	vordstate9appserver.halox.net/selfdestruct/?id=902af4360fc64bb1b43f9b6fb9968e44 expire [ExpirePeriod] from the time of this email being sent. - Secure Password Management. ate9.halox.net	.:i
URL: https://passw This message will e: Passwordstate 9.0 - https://passwordstate Cancel	vordstate9appserver.halox.net/selfdestruct/?id=902af4360fc64bb1b43f9b6fb9968e44 expire [ExpirePeriod] from the time of this email being sent. - Secure Password Management. :ate9.halox.net eview	.:: 5 Next
URL: https://passw This message will e: Passwordstate 9.0 - https://passwordsta Design	wordstate9appserver.halox.net/selfdestruct/?id=902af4360fc64bb1b43f9b6fb9968e44 expire [ExpirePeriod] from the time of this email being sent. - Secure Password Management. :ate9.halox.net eview eview uct Message lessage to another person, please specify details as appropriate for each stage of the Wizard below.	s Next

2.1.1.2.6.7 View & Compare History of Changes

Cancel

Passphrase Protection:

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

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.

.....

€,

Send

Previous

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.

ase use the navigation	buttons below to cycle through the history records	s. All cha	nges are highlighted in Dark Grey .
	29/10/2018 12:03:10 AM		31/08/2018 11:39:32 AM
Changed By	Windows Service Account (WindowsService)		Windows Service Account (WindowsService)
Title	James Farthing		James Farthing
UserName	farja		farja
Description			
Account Type	2 Active Directory		2 Active Directory
Password	GapYuWybtNLVyd6	茶	Zm9tWRra82dSQiH
Expiry Date	13/12/2018	쁥	15/10/2018
Notes			

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.

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

2.1.1.2.6.9 View Individual Password Permissions

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

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

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

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

ant additio	nal access simply click on the 'Grant Permissions' b	utton, or to modify existing perm	issions click on th	ne appropriate 'A	Actions' drop-do	own menu.
es Farth	ing (Active Directory Accounts)	🚨 User Ad	ccount 🐣 Local S	Security Group	. Active Direct	ory Security G
Actions	User or Security Group	Site Location	View	Modify	Expires	One-Time Access
0	🚨 Adam Finley	Internal		×		
0	. Zachary Edkins	Internal		~		

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

	Pa	ssw	orc	Permissions			
To g dov	grant vn m	t addi enu.	ition	al access simply click on th	ne 'Gra	nt Permission	is' button, or to mod
He	rcu	les	(Se	rvers)			🚨 User Acc
	Actions			User or Security Group			
		0		🚨 Fiona Case			
		٤٦	Cha	ange Access to 'View'			
Re	eturr	11 ()	Cha Mo Up	ange Access to 'Modify' dify Expiry Time date Access Notes		missions	Grid Layout Actions
		٢	Rer	nove Access			

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 <u>Grant New Permissions</u> 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 us	er or security group (use *	to search for all).		
Site Location : Internal			-	
Search : *			2	
Search For : 🖲 User	Security Group			
Search Results	View Perm	lissions	Reason for Access	
	>>			
	<<			
	Modify Pe	rmissions		
	>>			
	<<			
	Administr	ator Permissions		
	>>			
	<<			
				1
atus:				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: 0 Hours: 0 Minutes: 0	
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:	Save Cancel

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 - <u>Account Discovery</u>

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.

	Active	Directory Accounts (All Domain Ac	counts)						🗆 Favorite 🛛 📲 S	ite Location (Inte	ernal) 🛡 Shared Li	st (Admin Acces	s) 🏾 🌤 Guid	le 🛛 🗃 Strength Policy
A	ctions	Title	Domain or H	lost Us	er Name	Account	t Type	Password	Password Strength	Password Last Updated	Reset Status	Heartbeat Status	Dependencies	Managed	Expiry Date
	0	asdasdasd	rth halox	ms	sand2 😢	activ	ve Directory	**********************************	****			•	0	×	
	0	Check File Exists		ms	sand 😫			******************	****	5/08/2020 1:48:21 PM	Queued ①		0	×	5/10/2020
	0	halox\apppools	rt halox	ар	ppools 😫	activ	ve Directory	*******	***	31/10/2018 11:03:55 AM	•	•	0	×	2/04/2018
	0	halox\bship	the halox	bs	hip 😫	activ	ve Directory	*******	****		•	•	0	×	31/08/2019
	0	halox\pws_write	th halox	pw	vs_write 😣	activ	ve Directory	******	****	27/02/2020 9:51:03 AM		•	0	× .	
	0	HALOX\schedtasks	thalox	sch	hedtasks 😣	Activ	ve Directory	******** 😫	*****	25/05/2019 8:51:58 AM		•	1	×	
	♀ Co	py or Email Password Perma	link	sta	itex 😫 💋	activ	ve Directory	Requires Checkout	****	21/06/2020 11:07:20 AM			1	×	
	12 Co	py or Move to Different Pass	sword List	far	ja 😫 💋	activ	ve Directory	•••••••••	****	29/10/2018 12:03:10 AM		•	0	~	13/12/2018
	O De	lete		jtw	vilson:cg 🔁	activ	ve Directory	••••••	****		•		0		
	Exp	pire Password Now		Isa	nd	activ	ve Directory	******** 😫	★★★ ☆☆				0		
	V HI	ter Recent Activity on this Re nd Account Heartbeat Reque	est											Page	2, items 1 to 10 of 16.
Ad	📥 Se	nd Self Destruct Message		ctions	* List Admin	istrator Act	ions	*							
	* To	ggle Favorite Status													
Ľ	⊘ Vie ඬ Vie	ew & Compare History of Ch ew Documents	anges	/											
Da	🙎 Vie	ew Individual Password Perm	issions	D	First Name	Surname	IP Address	Description							
1/1	Vie 2/2020	ew Password Reset Depender 138334 PM Opened	ncies 🔎	naiox\images	Image	Capture	10.0.0.108	Image Capture (halox\images) opened the E ccount, UserName = splunkaccnt, Descriptio	dit Password screen for passwor on = Used for SIEM).	d 'Splunk Account' (Active Directo	ry Accounts) - vie	wing the value of th	e password is po	ssible on thi	s screen. (Title = Splum, A

Then you click on the 'Add Dependency' button.

Password Reset	Password Reset Dependencies													
Below are all the linked I	Password Reset	isks, or P	ost Reset tasks, for the	password 'HALOX\sc	redtasks'.									
Hosts Filters														
Host Name :	Hoof Name : Hoof Type ; Operating System ; Dutabase Server Type All Hoot Types * - Select Control or Type - * Select Donotore Type - * Select													
Actions Order	Host Name		UserName		Script Name					Dependency Type	Dependency Name	Reset Status	Managed Host	Privileged Account Credentials
0	😑 🖵 10.0.0.5	/	halox\sched	tasks	Reset Windows Si	heduled Task Pass	word			O Scheduled Task	TestFolder\Run Notepad	•	×	r.
Back to Passwords	Add Depend	ncy	Grid Layout Actions	*										
Date	Platform		UserID	First Name	Surname	Activity	De	scription						
Ē	T	т	т	т	т		т		т					
25/05/2019 8:50:33 AM	4 Windows	ervice	WindowsService	Windows Service	Account	Password Reset Successful	Th	e Passwords counts). Dep	state Windows Service suo pendency Type = 'Schedul	essfully processed the Password Reset Scri ed Task' and Dependency Name = 'TestFold	pt 'Reset Windows Scheduled Task Password' against ler\Run Notepad'.	Host 'win2k12w	eb1.halox.net' for th	e account 'schedtasks' (\Infrastruc
25/05/2019 8:50:33 AM	4 Windows	iervice	WindowsService	Windows Service	Account	Password Reset Removed from Oueue	Th Pr	e Passwords ocess Reset 1	state Windows Service rem Task is now complete. This	oved the account "HALOX\schedtasks' (Pas account relates to an Active Directory account	sword List = \Infrastructure\Active Directory Accounts sunt on the domain halox (halox.net)	, UserName = s	chedtasks, Descriptio	on = Active Directory Domain Acc

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.

P Add Dependency

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

ript and nost select	tion	
Decoverd Poset (or Past Passt Script	
Password Reset C	or Post Reset Script	
Please select the app	propriate Password Reset Script.	
Password Reset Scrip	pt * Reset Windows Service Password	
Note: If you wish to e can execute any cust	execute a script Post Reset, you do not need to select a dependency, or How record below to link it to - yo tom script you like. The order in which scripts are executed can also be changed on the previous screen).	bu
Windows Assourt	Int Dependency	
Windows Accour	nt Dependency	
IT the selected Reset :	. script is for one of the windows Account "Uppendencies" types below, enter appropriate details nere.	
Dependency Name	My Custom Windows Service	
	Name of the Windows Service (Display Name), Scheduled Task, IIS Application Pool or COM+ Componer	nt
Dependency Type	Quanore Windows Service QUS Application Pool QScheduled Task QCOM+ Component	
L L O		
Web2 Database Server Tvn	All Host Types	1
Web2 Database Server Typ	All Host Types	1
web2 Database Server Typ Select Database	Pe Type	
WeD2 Database Server Typ Select Database Hosts Search Resul	All Host Types Image: Constraint of the second se	1
Web2 Database Server Typ Select Database Hosts Search Resul	All Host Types	1
Web2 Database Server Typ Select Database Hosts Search Resul	All Host Types	1
Web2 Database Server Typ Select Database Hosts Search Resul Win2k12web2.hale	All Host Types	1
Web2 Database Server Typ Select Database Hosts Search Resu Win2k12web2.hal	All Host Types Search All Host Types Search Se	1
Web2 Database Server Typ Select Database Hosts Search Resu Win2k12web2.hal	All Host Types	
Web2 Database Server Typ Select Database Hosts Search Resu win2k12web2.hal	All Host Types	
Web2 Database Server Typ Select Database Hosts Search Resu win2k12web2.hal	All Host Types	1
web2 Database Server Typ Select Database Hosts Search Resu Win2k12web2.hal	All Host Types	1
Web2 Database Server Typ Select Database Hosts Search Resu Win2k12web2.hal	All Host Types	1
web2 Database Server Typ Select Database Hosts Search Resu I win2k12web2.hal	All Host Types	1
web2 Database Server Typ Select Database Hosts Search Resu I win2k12web2.hal	All Host Types Search	1
web2 Database Server Typ Select Database Hosts Search Resu win2k12web2.hal	All Host Types	1
web2 Database Server Typ Select Database Hosts Search Resu win2k12web2.hal	All Host Types	

2.1.1.2.7 List Administrator Actions

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

A summary of the features are:

Bulk Delete Selected Passwords	Use in conjunction with the 'Toggle Visibility of 'Delete Checkboxes', it is possible to delete more than one password record at a time
Bulk Permissions for Individual Passwords	Allows you to apply permissions for a User's Account, or a Security Group, to multiple individual passwords records at once
Bulk Update Passwords	Instead of editing data/fields for a single Password record, 'Bulk Update Passwords' allows you to use a CSV file to update many records at once
Bulk Update Password Reset Options	When you have a Password List enabled to perform Password Resets, you can use this feature to change multiple "reset" options for one or more password records i.e. schedules, Privileged Account Credentials, etc
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. F Note: There is no Recycle Bin for a Password List, so please use this feature with caution
Edit Password List Details	Allows you to modify existing settings for the Password List, change which fields you would like to use, and create an API key so records in the Password List can be queried or manipulated via the Passwordstate API
Save Password List as Template	Allows you to save all the settings and chosen fields as a Template, which can then be used for the creation or management of other Password Lists
Toggle Visibility of 'Delete Checkboxes	When you select this menu item, checkboxes will appear next to the 'Title' field in the grid. You can then select any number of records, and then use the 'Bulk Delete Selected Passwords' menu item to delete more than one record at a time
Toggle Visibility of Web API IDs	Allows you to see various ID fields required for the Passwordstate API
View Password List Permissions	Allows you to view existing permissions applied to this Password List, modify existing permissions and add new ones
View Recycle Bin	Allows you to see what Password records have been deleted, and gives you the option to restore from the Recycle Bin or permanently delete
Export All Password History	The report will export all history relating to each Password record, including the date data was changed, and who it was changed by. F 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. Key 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 Si	ites						
Actions	Title		User Name		Description	URL	
0	AA - Host Rec	ord					
0	аааа						
0	adaptiveinsigh	nts 🙆					
0	arubainstanto	n					
0	asdasdasd						
0	auth.services.a	dobe.com					
0	bancsabadell						
0	business.apple	com					
0	central.aruban	etworks					
0	crowdstrike	-					
Chan	ige page: 🕡 🖣	I P H					
🖆 Recent	t Activity 🕖			List Administrate List Administrate PASSWORD LIST	or Actions Actions ACTIONS	c	
Date		Activity		Bulk Permiss	ions for Individual	Passwords	Surname
21/12/2021	2:55:53 PM	Document Viewed		📭 Bulk Update	Passwords		Sandford
21/12/2021	2:06:41 PM	Password Restored	I	II Bulk Update 13 Convert to S	Password Reset O hared Password Li:	ptions st	Sandford
21/12/2021	2:06:26 PM	Password Deleted		🙁 Delete Passv	vord List		Sandford
21/12/2021	2:06:12 PM	Password Restored	I	Edit Passwor	d List Properties rd List as Template	2	Sandford
21/12/2021	2:04:55 PM	Password Deleted		 Toggle Visib Toggle Visib 	ility of Delete Cheo ility of Web API ID:	s s	Sandford
21/12/2021	11:37:36 AM	Password Screen O	pened	View Passwo View Recycle	ord List Permissions Bin (2)	5	Sandford
21/12/2021	11:37:35 AM	Password Updated		EXPORT			Sandford
21/12/2021	11:37:27 AM	Password Screen O	pened	Export All Pa	ssword History sswords		Sandford
21/12/2021	11:26:33 AM	Password Viewed		Enumerated	Permissions Repo Pwned Compromi	rt ses	Sandford
21/12/2021	11:26:31 AM	Password Screen O	pened	Password Str	rength Report		Sandford
Chan	ige page: 🕡 🖣	I) I) III		an standard Per	missions 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'.

🖻 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	
To bulk update one or more passwords for this Password List, you must first export all the passwords to a CSV file. To do so, please click on the 'Export Passwords' button below.	
Once you have your exported list of Passwords, please continue by clicking on the 'Step 2 - Update Data' tab.	
F If your import data includes Unicode characters, please save your CSV file with Unicode encoding before importing - please refer to Excel or other application documentation for how to do this.	
Export Passwords	
Can	cel

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 s	tep 2 - update data step	3 - import data		
When updating data in the CSV file	, there are a few rules to consid	er:		
. Consider the Column requirement. Do not modify the PasswordID v	nts below alues in any way			
Vhen ready, please click on the ' St	æp 3 - Import Data' tab.			
Column Name	Field Type	Size (Max)	Required	Please note: As this Password List
Title	String	255	×	the possible values you can enter for
UserName	String	255	×	it are displayed in this Listbox.
Description	String	255	×	- Available Account Types -
AccountType	String	NA	×	- Available Account Types -
Notos	String	NA	×	
Notes				
URL	String	1000	×	
URL Password	String Password	1000 NA	× ~	
URL Password ExpiryDate	String Password Date	1000 NA NA	× ~ ×	
URL Password ExpiryDate WebUser_ID	String Password Date String	1000 NA NA 200	× ~ × ×	

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 dat	ta
Now you are rea Passwords' butt	dy to import your upd	ated csv file. To do s	so, please select your C	SV file by clicking the 'Select' button, then click on the 'Import
Please Note: 1. Please ensure 2. CSV file must	your data does not co be under 100MB in siz	ntain any commas e.		
Email all users v	who have access to th	is Password List in	forming them of the u	updated records:
0 123 0 110				
	Select	Test Update	Update Passwords	

2.1.1.2.7.2 Bulk Update Passw ord Reset Options

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

With this feature you can:

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

					,			
search/filter for passwords	fields to update	reset options	heartbeat options	1				
earch/Filter for password reco	ords you wish to change P	assword Reset Setti	ngs for.					
Search Criteria								
Password Record Search	Account Type - Select Account	Type - 💌	Expiry Date From	Expiry Date To	Privileged Ac	count	▼ Search	Clear
Password Record Search	Account Type - Select Account bled for Resets)	Type - 🔻	Expiry Date From	Expiry Date To	Privileged Ac	count	* Search	Clear
Password Record Search	Account Type - Select Account bled for Resets)	Type -	Expiry Date From	Expiry Date To	Privileged Ac	count	▼ Search	Clear
Password Record Search	Account Type - Select Account bled for Resets) User Name	Type - 💌	Expiry Date From	Expiry Date To	Privileged Ac	Description	 Search Expiry 	Clear
Password Record Search	Account Type - Select Account bled for Resets) User Name	Type - 🔻	Expiry Date From	Expiry Date To	Privileged Ac	Description	Search Expiry 26/03/	Clear Date /2017
Password Record Search Managed Account (Ena Title Domain Splunk Account	Account Type - Select Account bled for Resets) User Name splunkaccnt@h	Type - ▼	Expiry Date From	Expiry Date To	Privileged Ac	Description Used for SIEM	Search Search Expiry 26/03/ 15/07/	Clear Date /2017 /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 passw	ords fields to update	reset options	heartbeat options	
Select which of the follow	ring fields below you would li	ke to change for the	selected password record	s.
Fields To Update				
Account Type	- Select Account Type -		•	
Expiry Date				Ē
Managed Account	Enable Password Reset	s option for these acc	count(s)	
Account Heartbeat	Enable Account Hearth	eat option for these	account(s)	

HBulk 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 passwor	rds fields to update reset options heartbeat options
elect which Password Reset	t Options below you would like to change for the selected password records.
- 🔲 Change Password	d Reset Script and Privileged Account Credentials
Please select the appropr password reset.	riate Password Reset Script, and Privileged Account Credential, in order to perform the
Password Reset Script	Make No Changes to Selected Password Reset Scripts 💌
Privileged Account	Make No Changes to Selected Privileged Account Credentials
Change Password When this Password OO + Hour OO	d Reset Schedule expires, Auto-Generate a new one and perform any reset tasks at the time of: v Minute, and add and and bays to the Expiry Date
	Save

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.

2.1.1.2.7.3 Edit Passw ord List Properties

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

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

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

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

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

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

Password List Details Section

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

Site Location	A Site Location of "Internal" will be used if the Password List is being created in the root of Passwords Home, or it will inherit the location of its parent Folder. Adding different Site Locations requires an active subscription for the Remote Site Locations module
Password List	The Title for your Password List, as it would be displayed on the Navigation Tree
Description	A brief description outlining the purpose of the Password List
Image	An image you would like displayed for the Password List in the Navigation Tree
Password Strength Policy	The Password Strength Policy you would like applied to the Password List. Clicking on the Pas
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 yethey can access the Password List, you can choose authentication methods in this drop-down list	our users befo any one of th
Password List Details 🦷)	
Site Location	Internal	
Password List *	Active Directory Accounts]
Description	All Domain Accounts]
Image	windows.png	۲
Password Strength Policy *	Default Policy 🔻	■ #2
Password Generator Policy *	SQL Password Generator 👻	
Code Page *	Western European (Windows)	
Additional Authentication *	None Required	ņ

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 <u>Navigation Tree</u>
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	Provides you with another Tab on the Edit Password screen which allows:
Directory Accounts	Unlock this account if locked
	 User must change password at next logon
	 Disable this account
	Enable this account

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 Prevent Password reuse for the last Disable Email Notifications for this Password List Force the use of the selected Password Generator Policy Hide Passwords from users with the following permissions 	
 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 	

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 🔍	ך
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 - <u>Bulk Update Password Reset Options</u>

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 Password Reset Schedule for the account, and schedule the reset at a random time between the two time slots below:	
Start Time Finish Time	
02 • Hour 00 • Minute 03 • Hour 45 • Minute	
And when the account expires, add 2 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 Poilcy
Expiry Date	All passwords should be reset after a certain period of time. The Expiry Date field can be used to indicate when this time is, and can be used for reporting purposes, or for Automatic Password resetting
Notes	Allows you to specify longer HTML formatted text for any general notes you need to maintain for the record
Generic Fields (1 to 10)	Generic Fields can be configured for any purpose you like, and also named any way you like. The following Field Types are available for Generic Fields:
	 Text Field A single line text field Free Text Field Multiple line text field Password An encrypted password field Select List A vertical drop-down list of predefined values Radio Buttons A horizontal checklist of predefined values Date Picker A popup calendar style control for picking date values URL Field Allows you to click on the URL in the Grid view and launch the web site

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

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

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

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

password details	notes security	
Title *	Test Password	Q
UserName	msand	8
Description		
Expiry Date		Ê
Password Generator	Default Password Generator	•
Password *	••••••	📔 🔍 🖩 🖖 🔚
Confirm Password *	•••••	
Password Strength	\bigstar	
Strength Status: Excelle	ent password strength	

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.

password list details customize fields guide api key	
😸 階 🗐 B / 坦 🛵 三 三 三 三 三 三 三 洋 洋 A · Ø · Font Name - Real • 💖	
This list is used for recording all Oracle E-Business related passwords.	
Please record passwords for both the application tier, and database tier in the list, and ensure they are reviewed on a monthly basis.	
The Oracle Team.	
✓ Design ♦> HTML ♥ Preview	
	Save & Close Cancel

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.

Favorite	Shared List (Admin	Access) 🕨 🥶 Guide	👪 Strength Policy

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



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

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

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

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

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

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

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

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

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

Save Save & Close Cancel

Ö E	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.

issword 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 b2a57c34fe96d8f36a89c25eb47d4b6c Generate New Key

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

_ API	Sett	ings
-------	------	------

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 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 us 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 Require	۶d
--	----

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 return 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 ca	an 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 retu	rned 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 A	dministration -> System Settings -> Allowed IP Ranges tab

2.1.1.2.7.4 Save Passw ord 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 (<u>Linked Password Lists</u>).

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 - <u>Password List Templates</u>.

	ustomize fields guide	
lease specify Password List se	ttings manually below.	
Password List Details		Default Password Reset Schedule
Description		 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.
Image	- Select Image - 💌 👼	Enable the the Password Reset Schedule for the account, and schedule
Password Strength Policy *	Default Policy 👻 🖲 🗱	reset at a random time between the two time slots below:
Password Generator Policy *	Default Password Generator 💌 🖲 🖬	Start Time Finish Time
Code Page *	Use Passwordstate Default Code Page 💌 🖲	
Additional Authentication *	None Required 💌 🔍	And when the account expires, add 90 Day(s) To the Expiry Date
Enable One-Time Passwo Allow Password List to be Time Pased Access Mand	andws password resetting with other systems 🗢 rd Generation 🖷 2 Exported 🖷	
Enable One-Time Passwo Allow Password List to be Time Based Access Mand Disable Inheritance of of Multiple Approvers Manc Prevent Password reuse f Disable Email Notification Force the use of the selee Hide Passwords from use Popup the Guide on each Prevent Non-Admin user Prevent Non-Admin user Prevent Saving of Passwo Users must first specify a Prevent Non-Admin user Set the Expiry Date to Cu	alows password resetting with other systems and the systems are dependent on the systems are required for the systems and upper level folder permission propagation datory • a total of 1 • approver(s) are required for this List for the last 5 = passwords are started password List ted Password List ted Password Generator Policy rs with the following permissions • access to this Password List a from Dragging and Dropping this Password List are for a "Bassword" is detected are reason why they need to view, edit or copy passwords a from manually changing values in Expiry Date fields rrent Date + 0 Days when adding new passwords are started passwords are started passwords are started by the password is detected are started by the passwords by the passwo	

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.

Actions	PasswordID	Title	Domain or Host	User Name	Account Type	Password	Password Strength
0	70301	asdasdasd	nalox	msand2 😫	2 Active Directory	********	****
0	69866	Check File Exists		msand 😫		*********	****
0	67200	halox\apppools	r halox	apppools 😫	active Directory	*****	***
0	69274	halox\bship	nalox	bship 😫	2 Active Directory	****	****
0	69312	halox\pws_write	n halox	pws_write 😫	2 Active Directory	*********	****
0	69270	HALOX\schedtasks	n halox	schedtasks 😫	2 Active Directory	******** 😫	****
0	67187	halox\statex	r halox	statex 😫	active Directory	Requires Checkout	****
0	62147	James Farthing 🛛 🔺	nhalox	farja 😫	2 Active Directory	*****	*****
0	67949	jtwilsonxxx	📩 halox	jtwilsonxxx 😫	active Directory	*****	****
0	69304		nalox	2	active Directory	*******	****
Cha	nge page: 🙀	<u>.</u> • р. я.					
Cha	inge page.						

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 <u>List Administrator Actions</u> dropdown 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

gr	ant additior	nal access simply click on the 'Grant Permissions' button, or to moo	lify existing permissions click on	the appropriate	'Actions' drop-	down menu.			
) (Dut of Ba	and Management Cards			🚨 User Accour	nt 🐣 Local Sec	curity Group	E Active Directory S	ecurity Grou
	Actions	User or Security Group	Site Location	Guest	View	Modify	Admin	Mobile Access	Expires
,	0	E Department - Shared Services (Information Technology)	Internal			×		×	
	0	Lee Sandford	Internal				×	×	
	0	S Mark Sandford	Internal				 Image: A set of the set of the	 Image: A set of the set of the	

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

🚨 Pa	ssword List Permissions								
To grant	t additional access simply click on the 'Grant	Permissions' button, or to modi	fy existing permissions click on t	he appropriate 'A	ctions' drop-	down menu.			
🕶 Ou	t of Band Management Cards			3	User Accour	nt 👋 Local Sec	urity Group	Active Directory S	ecurity Group
А	ctions User or Security Group		Site Location	Guest	View	Modify	Admin	Mobile Access	Expires
>	Department - Shared Services (Information Technology)	Internal			×		×	
	🔷 🍧 🤱 Lee Sandford		Internal				<	×	
	Change Access to 'View'		Internal				×	×	
t1 Change Access to 'View' t2 Change Access to 'Modify' t3 Change Access to 'Modify' t4 Change Access to 'Admin' I2 Change Access to 'Admin' I2 Enable/Disable Mobile Access I2 Modify Expiry Time I2 Dydate Access Notes I2 Remove Access		×							

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 <u>Grant New Permissions</u> 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

Td 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 bas	sed access	
Search for an appropriate user or sec	urity group (use * to search for al	1).
Site Location : Internal		•
Search : *		<u>م</u>
Search For : OUser OSecuri	ty Group	
Search Results	View Permissions	Mobile Access
 Desktop Team		Enabled Mobile Access for these permissions:
A Human Resources	>>	🖲 Yes 🔍 No
🗏 IS Department	<<	Reason for Access
🌯 My Group 2		
🌯 Nested Group 1		
🌯 Network Team	Modify Permissions	
Passwordstate-Auditing Security Gro	>>	
A Passwordstate-Export-All-Password	Se	
A Radius Users		
SecurityGroup 1		
& Svdnev-TestGroup	Administrator Permissio	ns
4 Test		
	>>	
	<<	
•	•	
tatus:		Save

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	
apply time based acco	ss to the selected Password List, please use the appropriate opt	ions below.
Access Expires : ອ		
Never		
O In: Days: 0	Hours: 0 Minutes: 0	
O At: Date:	📺 Time: 🕒	
us:		Save Cancel

2.1.1.2.7.7 View Recycle Bin

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

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

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

Recycle	Bin - Oracle Da	tabase	e Tier 💷					
Actions	Title	User Name	Description	Local Password	Commission Date	Password	Password Strength	Expiry Date
0	ddfg			******		********	****	29/12/2013
0	regex_delete_test			******		****** 😢	*****	29/12/2013
Return to	Passwords Em	pty Recy	/cle Bin G	rid Layout Actions	Ŧ			

Recycle	Bin - Oracle Da	tabase	Tier 🛡					
Actions	Title	bser Name	Description	Local Password	Commission Date	Password	Password Strength	Expiry Date
0	ddfa			*********		***************************************	★★★★ ☆	29/12/2013
٥	regex_delete_test			******		*****	*****	29/12/2013
Re' 🕑 🙁	View & Compare Hist Delete Restore	tory of Ch	nanges	Layout Actions	Ŧ			

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 <u>Navigation Tree</u>
Description	A description of the folder describing it's purpose
Prevent Non-Admin users from Dragging and Dropping this Password Folder in the Navigation Tree	You can prevent users with Non-Admin rights to the Folder from dragging-and-dropping the position of the folder in the <u>Navigation Tree</u>
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 appr	ppriate details below, then click on the Save Button.
Folder Settir	gs
Site Location *	Internal 🔻
Folder Name *	
Description	
Yes O No Folder Perm Permission Max	ssion Model
Standard - Ir	herit permissions from nested Password Lists OAdvanced - Propagate permissions down from top level folder
Permissions on F	olders and Password Lists can be managed in one of two ways:
 Standard Disabling Advance Lists, unle 	Permission Model - Permissions on the folder are inheritted from any nested Password Lists beneath it. No of inheritance is at Folder or Password List level is possible. Permission Model - Permissions are generally propagate down from the Folder to nested Folders and Password is Disabling of inheritance is selected on any nested items.
	Save Save & Add Another Cancel

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.

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
	□ Link this Password List to the selected Template. □ Disable future use of this Wizard
Cancel	Next

🖌 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.

lease confirm	he details below are correct, then click the 'Finish' button.	
Site Location:	Internal	
Password List:	V Private Password Vault	
Description :	Log in Passwords for Various sites	
Template:	Standard Password List	
Permissions:	Image Capture (Admin)	

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

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

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

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 <u>Navigation Tree</u> just below the selected node (Password List or Folder). You can then drag-and-drop the Password List to any position in the <u>Navigation Tree</u> 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

ease specify Password List se	ttings manually below.	Or copy settings/permissions from existing Templates or Password Lists.
Password List Details 🏾)	Copy Details & Settings From 🤍
Site Location	Internal	Copying a Template or another Password List's settings will populate all
Password List *		fields/settings on this screen, except for any API Keys.
Description		- Copy Settings From Template -
mage	- Select Image - 💌 🖲	Search and Copy Settings from Password List
Password Strength Policy *	Default Policy 💌 🛡 🗰	□ Link this Password List to the selected Template.
assword Generator Policy *	Build Policy	Copy Permissions From 🔋
Additional Authentication *	None Required	If you would like to copy permissions from an existing Template or Password List, please select the appropriate option below.
		- Copy Permissions from Template -
Paseword List Settings This will be a Private Pa	ssword List	- Copy Permissions from Template - Search and Copy Settings from Password List
Paseword List Settings This will be a Private Par Broble Password Resets Enable One-Time Passwo	ssword List allows presented resetting with other systems rd Generation	- Copy Permissions from Template - Search and Copy Settings from Password List Password List Permission Settings
Paseword List Settings This will be a Private Par Enable Password Resets Enable One-Time Password Allow Password List to be Time Based Access Mand Multiple Approvers Mand	ssword List allows presented resetting with other systems rd Generation Exported latory latory latory total of T approver(s) are required for this List	- Copy Permissions from Template - Search and Copy Settings from Password List Password List Permission Settings If using the Advanced Permission Model, you can prevent permission propagation to this Password List with the setting below.
Paseword List Settings This will be a Private Pas Brable Password Resets Carbon Password Allow Password List to be Time Based Access Mand Multiple Approvers Mand Prevent Password reuse f Carbon Password reuse f	ssword List allows passmord resetting with other systems af Generation at Generation at Same approver(s) are required for this List for the last Same approver(s) at	- Copy Permissions from Template - - Search and Copy Settings from Password List 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
Assword List Settings This will be a Private Pa: Enable Password Resets Enable One-Time Password Allow Password List to be Time Based Access Mand Multiple Approvers Mand Prevent Password reuse f Disable Email Notification Force the use of the sele: Hide Passwords from use	ssword List allows preserved resetting with other systems rd Generation tatory batory - a total of r approver(s) are required for this List or the last passwords ns for this Password List ted Password Generator Policy rrs with the following permissions	- Copy Permissions from Template - Search and Copy Settings from Password List 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
Assevord List Settings This will be a Private Pa: Enable Password Resets - Enable One-Time Password Allow Password List to be Time Based Access Mand Multiple Approvers Mand Multiple Approvers Mand Prevent Password reuse f Disable Email Notification Force the use of the select Hide Passwords from use Popup the Guide on eact Prevent Non-Admin user	ssword List allows preserved resetting with other systems rd Generation Exported latory latory = total of or the last passwords is for this Password List ted Password Generator Policy rs with the following permissions r access to this Password List from Dranging and Proposing this Password List Base of the password List s from Dranging and Proposing this Password List s from Pranging and Proposing this Password Pranging the Prang	Copy Permissions from Template - - Search and Copy Settings from Password List 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 Only applicable if this Password List is enabled for Resets.
Paseworld List Settings This will be a Private Par Enable Password Resets Enable One-Time Password Allow Password List to be Time Based Access Mand Multiple Approvers Mand Prevent Password reuse f Disable Email Notification Force the use of the sele Hide Passwords from use Popup the Guide on ead Prevent Non-Admin user Prevent saving of Password Users must first previse	ssword List • allows presented resetting with other systems ird Generation • Exported • Exported • Latory • atory - a total of • approver(s) are required for this List • for this Password List cted Password Generator Policy • a socess to this Password List • access to this Password List • are order the following permissions • arecess to this Password List	Copy Permissions from Template - Copy Permissions from Template - Search and Copy Settings from Password List 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 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.
Aseword List Settings This will be a Private Pa: Enable One-Time Password Enable One-Time Password List to be Time Based Access Mand Multiple Approvers Mano Prevent Password reuse f Disable Email Notification Force the use of the select Hide Passwords from use Popup the Guide on eacd Prevent Non-Admin user Prevent saving of Password Users must first specify a Prevent Non-Admin user Set the Expiry Date to CU	■ ssword List allows preserved resetting with other systems ■ rd Generation ■ ≥ Exported ■ latory ■ jatory ■ jatory ■ for the last 5 passwords ns for this Password List cted Password Generator Policy rrs with the following permissions r access to this Password List s from Dragging and Dropping this Password List ■ reason why they need to view, edit or copy passwords s from manually changing values in Expiry Date fields rrent Date + 0 Days when adding new passwords ■	Copy Permissions from Template - - Search and Copy Settings from Password List 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 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:
Aseword List Settings This will be a Private Pa: Enable One-Time Password Enable One-Time Password Allow Password List to be Time Based Access Mand Multiple Approvers Mand Prevent Password reuse f Disable Email Notification Force the use of the select Hide Password from use Popup the Guide on each Prevent Non-Admin user Prevent Saving of Password Users must first specify a Prevent Non-Admin user Set the Expiry Date to Curr Additional Authentication	■ allows preserved resetting with other systems ■ rd Generation ■ Exported ■ latory ■ jatory = jatory = istory ■ jatory = static jatory = jatory = ist	Copy Permissions from Template - - Search and Copy Settings from Password List 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 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 Finish Time
Paseworld List Settings This will be a Private Pa: Enable One-Time Passworl Enable One-Time Passworl Allow Password List to be Time Based Access Mand Multiple Approvers Mand Prevent Password reuse f Disable Email Notification Force the use of the selet Hide Passwords from user Popup the Guide on each Prevent Non-Admin user Prevent Non-Admin user Prevent Non-Admin user Set the Expiry Date to Cur Set the Expiry Date to Cur Additional Authentication Show 'Active Directory Active Dire	Image: source of the setting with other systems allows preserved resetting with other systems ind constraint allows preserved altory actions altory altory altory altory altory altory action the last 5 password Generator Policy res with the following permissions a access to this Password List s from Dragging and Dropping this Password List reacon why they need to view, edit or copy passwords s from manually changing values in Expiry Date fields rrent Date + [0] Days when adding new passwords ent Date + [0] Days when manually updating Passwords en only required once per session (*) ctions' options for Active Directory accounts	Copy Permissions from Template - Search and Copy Settings from Password List 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 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 Reset Schedule for the account, and schedule the reset at a random time between the two time slots below: Start Time OO Hour OO Minute

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.

assword List Details	Permissions	Confirmation		
Site Location:	Internal			
Password List: *	Shared Password Vault			
Description :	Used to share various credentials for Adm	in team]	
Template:	Standard Password List	Ψ		
Image:	🐓 protect.png	Ŧ		
Template Description:	Standard selection of settings, and basic U	Isername and Password fields		
		Disable future use of	this Wizard	
Cancel			Next	
Cancel			Next	

🌢 Add Shared Password List Wizard

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

Site Location : Internal Search : * Search For : © User ® Security Group	
Search Results Core Distribution EmptyGroup Finance Department S IS Department Cocal SG My Group 2 Network Team Passwordstate-Auditing Security Group Test Test Test Users SG	View Permissions >> << Modify Permissions
Status: Cancel	Previous Next

🐐 Add Shared Password List Wizard

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

Site Location:				
Site Location.	Internal			
Password List: 📲	Shared Passwo	rd Vault		
Description : U	sed to share vari	ous credentials for Adm	nin team	
Template: St	tandard Passwor	d List		
Permissions: Co	oreAdmins (Mod	lify), Mark Sandford (Ad	lmin)	

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

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

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

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 <u>Navigation Tree</u> just below the selected node (Password List or Folder). You can then drag-and-drop the Password List to any position in the <u>Navigation Tree</u> 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).

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

, , , , , , , , , , , , , , , , , , , ,	tings manually below.		Or copy settings/permissions from existing Templates or Password Lists.
assword List Details 🏾 🖲			Copy Details & Settings From 👼
e Location	Internal		Copying a Template or another Password List's settings will populate all
ssword List *			fields/settings on this screen, except for any API Keys.
scription			- Copy Settings From Template -
age	- Select Image -	-	Search and Copy Settings from Password List
ssword Strength Policy *	Default Policy	, I I I I I I I I I I I I I I I I I I I	Link this Password List to the selected Template.
ssword Generator Policy * de Page *	Build Policy Use Passwordstate Default Code Page	- -	Copy Permissions From 🔋
ditional Authentication *	None Required	•	If you would like to copy permissions from an existing Template or Password List, please select the appropriate option below.
			- Copy Permissions from Template -
This will be a Shared Pas Enable Possword Bocot Enable One-Time Password Allow Password List to be Time Based Access Mand Multiple Approvers Manc Prevent Password reuse fi Disable Email Notification	ssword List allows password resetting with other systems Exported tatory = atory = atory = atory = atory = approver(s) are required or the last 5 passwords is for this Password List	for this List	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
 Force the use of the select Hide Passwords from use Popup the Guide on each Prevent Non-Admin user Prevent saving of Passwo Users must first specify a Prevent Non-Admin user: Set the Expiry Date to Curr Aeditional Authentication 	ted Password Generator Policy rs with the following permissions access to this Password List from Dragging and Dropping this Password List rd records if a 'Bad' password is detected reason why they need to view, edit or copy pass from manually changing values in Expiry Date fi rrent Date + 0 Days when adding new pass ent Date + 0 Days when manually updating o noly required once per session tions' options for Active Directory accounts	vords ields vords ® Passwords	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 Finish Time 00 + Hour 00 + Minute 00 + Hour 00 + Minute
Show 'Active Directory Ac			

2.1.5 Administer Bulk Permissions

The standard method of apply permissions to a Password List is via the <u>Grant New Permissions</u> 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.

H Administer Bulk Permissions for Password Lists

Adrivistering 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.

ccess permissions			
arch for an appropriate user or secu	urity group (use * to search for all).		
te Location : Internal	•		
earch : *		Q	
search For : OUser OSecurit	y Group	-	
earch Results	Available Password Lists	View Permissions	Mobile Access
CoreAdmins	Filter 😣	🖳 \Business Systems \Microsoft SQL Local Accounts	Enabled Mobile Access for these permissions:
Desktop Team	Business Systems\Credit Cards	>>	● Yes ○ No
8 Human & Resources	Business Systems (Creat edits)		Reason for Access
IS Department	Rusiness Systems (Database Accounts		
Local Domain Group	Business Systems (Oracle EKP Accounts		
My Group 2	business systems (lest Password List	Modify Permissions	
Nested Group 1	Customers Alisand Workstation Accounts		
8 Network Team	Vustomers\Contoso\DBAs\Database Credential:	>>	
Passwordstate-Auditing Security Gro	Customers\Contoso\Infratructure\Active Directo	<<	
Passwordstate-Export-All-Password S	Customers\Contoso\Infratructure\Domain Passv		
Radius Users	Customers\Contoso\Infratructure\ISP Details		
SecurityGroup1	Customers\Contoso\Infratructure\Network Devi	Administrator Permissions	
8 SecurityGroup2	Customers\Contoso\Infratructure\Office 365 Acc	Business Systems\SharePoint Accounts	
Sydney-TestGroup	Customers\Contoso\Infratructure\Server Listing	>>	
- Jost	🗟 \Customers\Contoso\Infratructure\Service Accour 🖕	<<	
" Iest			

2.1.6 Expiring Passwords Calendar

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

On this calendar you can:

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

 ✓ today * dec, 2020 						DAY WEEK MONTH
Sun	Mon	Tue	Wed	Thu	Fri	Sat
29	30	1 Dec	2	3	4	5 ^
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
			Splunk Account			
27	28	29	30	31	1 Jan	2
			Tasks Account	PWS Backup		

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 (<u>Password List Details Tab</u>)
- 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 <u>Edit Password List Details</u>
- You can also apply permissions to a Template, and these permissions can be used for:
 - $\,\circ\,$ Allow other users to see the Templates via the 'Password List Templates' menu option
 - $\,\circ\,$ 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 (<u>Password List Details Tab</u>)

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 <u>Add New Template</u> button on this screen, or via the <u>Save Password List as Template</u> option for an existing Password List.

88]Pass	sword	List Templates						
Listed be	elow are	all the Password List Templates stored within Passwor	dstate.					
Ac	ctions	Password List	Description	Linked Password Lists	Deny Export	Time Based Access	Prevent Password Reuse	In-Built Template
		Т	T					Т
	0	🔇 Alarm/Door Codes	Store building alarms codes, or door pin tumbler combinations	0			×	×
	0	Credit Cards	Securely store credit card information	0			×	×
	0	🐨 Enabled for Password Resets 🧠	Perform password resets on a scheduled, or on demand, for many different types of accounts	0			×	 ✓
	0	One-Time Password Authenticator	Generate One-Time Passwords based off scanned QR Codes	0			×	×
	0	Software Licenses	Store various metadata related to software licensing	0			×	~
	0	SSH Account (Key Storage Only)	Store SSH Keys with Passphrase recorded in Password field - Used for SSH Sessions	0			×	×
	0	SSH Account (Passphrase + Key Storage)	Store SSH Keys with Passphrase and optional Password field	0			×	×
	0	SSL Certificates	Store SSL certificates and receive reminders of when they need to be renewed	0			×	×
>	0	Standard Password List	Standard selection of settings, and basic Username and Password fields	1			×	×
	0	Standard Password List (Hide Passwords)	Standard Password List where the values of passwords are hidden from non-administrators	0			 ✓ 	 ✓
H	1 2	Э	Page: 1 of 2 Go Page size: 10 Change					Item 1 to 10 of 13
Add No	ew Tem	plate Toggle ID Column Visibility Grid Layo	ut 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 - <u>Password List Details Tab</u>, <u>Customize Fields Tab</u> & <u>Guide</u>.

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

Password List Template Actions

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

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

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

l below are	e all the Password List Temp	plates stored within Passwoi	rdstate.		
Actions	Password List		Description		
	Т		T		
0	🔇 Marm/Door Codes		Store building alarms codes, or door pin tumbler com		
0	Credit Cards		Securely store credit card information		
M	Enabled for Password	d Resets 📭	Perform password resets on a scheduled, or on den		
X v	iew Permissions	thenticator	Generate One-Time Passwords based off scanned QR		
& Li	nked Password Lists		Store various metadata related to software licensing		
U D	elete Template	orage Only)	Store SSH Keys with Passphrase recorded in Password		
0	SSH Account (Passph	nrase + Key Storage)	Store SSH Keys with Passphrase and optional Passwor		
0	SSL Certificates		Store SSL certificates and receive reminders of when t		
0	Standard Password Li	st	Standard selection of settings, and basic Username an		
0	Standard Password List (Hide Passwords)		Standard Password List where the values of password		
1 2	())				

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 - <u>Password List</u> <u>Details Tab</u>, <u>Customize Fields Tab</u> & <u>Guide Tab</u>. One exception to this is the API Key tab, as each Password List's API Key details must be unique.

Rote: 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 🦷]		Default Password Reset Schedule
Assword List Details Assword List Details Assword List * Assword List * Assword Strength Policy * Assword Generator Policy * Assword Generator Policy * Additional Authentication * Additional Authentication * Anable Password Resets - Enable One-Time Password Allow Password List to be Enable One-Time Password Allow Password List to be Anable Access Mand Multiple Approvers Manc Prevent Password reuse f Disable Email Notification Force the use of the selet Prevent Non-Admin user Prevent Non-Admin user Prevent Non-Admin user Set the Expiry Date to Cur Reset Expiry Date to Cur			Perault 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 Finish Time OO * Hour OO * Minute OO * Hour OO * Minute And when the account expires, add 90 Day(s) * to the Expiry Date.

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 <u>API</u> <u>Key Tab</u>.

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 Pas 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 t

Available Password List(s)			Linked Password List(s)		
Filter	ω		Filter	•	Э
🔎 \Abigail Brown's Passwords			Versonal Password Lists\Test Private List		
શ \Active Directory Accounts					
➢\Browser Testing					
Business Systems\Credit Cards					
🖳 \Business Systems\Database Accounts					
🖳 \Business Systems\Microsoft SQL Local Accounts					
Business Systems\Oracle ERP Accounts		>>			
🖳 \Business Systems\Shared Team Passwords		<<			
Husiness Systems\SharePoint Accounts					
Business Systems\SSL Certificates					
➢\Business Systems\Test Password List					
Customers\Allsand\Workstation Accounts					
🖳 \Customers\Contoso\DBAs\Database Credentials					
	bu				
Customers\Contoso\Infratructure\Domain Passwords	-				
Countri 01			Count: 1		

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

Pending Access Required Pen	Jests											
3elow is a list of Pending Access	Requests that you are either ne fields are blank, then the	r responsible for processing, o user is requesting access to tl	or they're your a	access request it, and not an i	ts waiting for approval. individual record within	it.						
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 b	riefly	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 m	nedia advertising.	Admin	1	0		2019-02-28 12:00:00 AM
🌲 My Pending Access Rec	luests											
Actions Date	Password List	Title	Use	rName	Descript	lion	Reason	Permissio	ns No. of Approve	rs Approval Co	ount 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.

access request se	ttings
User :	
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.

request a	cess to a Folder, Password List or individual Pase	word record, please perform your search and select the	appropriate menu from the 'Actions' drop-down menu, then foll	low the on-screen instructions.	
Search I	ilter				
Tree Pat	h P	assword List Password Record			
	<i>•</i>		Search Clear		
Actions	Tree Path	Password List	Title	Domain or Host	Account Type
	T	Т	Т	T	Т
0	\Passwords Home	No Access	sdfsdf		
0	\Passwords Home	Optus Dialup	OD1		
0	\Passwords Home	Optus Dialup	testdelete		Facebook
0	\Passwords Home	🖤 Optus Dialup	Yes1		
🖾 Re	quest Access to Password List	🦁 Optus Dialup	Yes2		
Re Re	quest Access to Password Record	🖤 Optus Dialup	Yes3		
0	\Passwords Home	🦁 Optus Dialup	Yes4		
0	\Passwords Home	🜍 OTP Test Shared List	Test Password 4		
0	\Passwords Home	Tumbler Door Codes	blankpassword		Calendar
0	\Passwords Home	Tumbler Door Codes	blankpassword2		
(H)	+ 1 2 3 4 5 6 7 8 9 10 _ • · ·		Page: 1 of 65 Go Page size	: 10 Change	item 1 to 10 of 6-

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

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

Request Access To request access to the why and click on the 'Sul	to Password List Password List 'Optus Dialup' with the details below, please specify a reason bmit' 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 <u>Navigation Tree</u>.

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.



© 2023 Clic

2.2 Tools Menu

108

There are three options available under the Tools menu.

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

2.2.1 Account Discovery

The Account Discovery Menu allows you to perform various account discoveries on your network, based on Host records which have been added under the <u>Hosts</u> 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

R Account Discovery

Below are all	the Account Discovery jobs added to Passw	vordstate.								
Actions	Job Name	Description	Job Type	SiteL ocation	Run Discovery At	Schedule Type	In Progress	Last Discovery Took	Simulation Mode	Enabled
	Т	Т	T	Т	T	Т	T	т	T	Ψ
0	All Local Admins On Servers	All Local Admins On Servers	Windows Local Admin Accounts	Internal	11:00 PM	Weekly - Sunday				×
0	Linux Discovery Halox External - No Key	Linux Discovery Halox External	Linux And Mac Accounts	Halox	01:20 PM	Daily		00:00:02		×
0	Local Windows Admins on Halox	Local Windows Admins on Halox	Windows Local Admin Accounts	Halox	03:54 PM	Daily		00:00:10		×
0	Windows Dependencies on Halox	Windows Dependencies on Halox	Dependencies	Halox	02:40 PM	Daily		00:00:05		×
Select Disco	very Job Type to Add * Grid Layo	ut 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 <u>Bulk Update Password Reset Options</u> 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 (<u>Password List Details Tab</u>) 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 <u>Bulk Update Password Reset Options</u> feature for each Password List which allows you to change these values for more than one password record at a time.

liscovery job settings	schedule ł	hosts to be queried		
iscovery Job Name * escription *	:	1		
te Location *	: Internal			
mulation Mode	: 🗆 Simu	ulation Mode will ema	il you the resul	Its without adding/updating any data in the database
eport on the following:	: 💿 Only	y newly Discovered Ac	counts O All	Discovered Accounts - New or Existing
Diagonal Carach C				
Discovery Search Cr	iteria			
Please specify filtering o	ptions for which Ho	osts you wish to query	for new accou	unts, as well as any filtering options for the names of accounts.
Host Types:				Operating Systems:
Select Host Type				Select OS
Include Hosts based o	n Host Name mate	ch:		Include Hosts based on Tag Field match:
Exclude Hosts based o	n Host Name mate	ch:		Exclude Hosts based on Tag Field match:
	leannan matala			Exclude Accounts based on Username match:
Discover Accounts by	Jsername match:			
Discover Accounts by Query the following L- Administrators	ocal Administrator	r Group Name(s):		
Discover Accounts by Query the following L Administrators Each of the fields abo	ocal Administrator	r Group Name(s):	separating the	em with semicolon characters.
Discover Accounts by Query the following L Administrators Each of the fields abo Discovery Actions	ve can have multip	r Group Name(s): Ie values specified, by	separating the	em with semicolon characters.

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 (<u>Password List Details Tab</u>) 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 <u>Bulk Update Password Reset Options</u> feature for each Password List which allows you to change these values for more than one password record at a time.

discovery job settings s	schedule hosts to be queried	
Please select appropriate option Discovery Job Name * Description * Site Location *	is for the Discovery Job below, and set the set of the	e scheduie as required.
Active Directory Domain * Simulation Mode Report on the following:	Simulation Mode will email yo Only newly Discovered Depen	 Only accounts from this selected domain will be discovered u the results without adding/updating any data in the database dencies All Discovered Dependencies - New Existing or No Dependencies
Discover the following Dep	pendencies configured to use an Active	Discovery Job.
Discover the following Dep Windows Services IIS	pendencies configured to use an Active S Application Pools Scheduled Tasks I Hosts with the following Operating Sy	e Directory account: ystems: Select OS
Discover the following Deg Windows Services IIIS Discover Dependencies on Include Hosts based on Ho	pendencies configured to use an Active S Application Pools Scheduled Tasks Hosts with the following Operating Sy ost Name match:	e Directory account: ystems: Select OS Include Hosts based on Tag Field match:
Discover the following Dep Windows Services IIIS Discover Dependencies on Include Hosts based on Ho Exclude Hosts based on Ho	pendencies configured to use an Active S Application Pools Scheduled Tasks Hosts with the following Operating Sy ost Name match:	e Directory account: ystems: Select OS Include Hosts based on Tag Field match: Exclude Hosts based on Tag Field match:
Discover the following Dep Windows Services IIIS Discover Dependencies on Include Hosts based on Ho Exclude Hosts based on Ho Exclude Hosts based on Ho	pendencies configured to use an Active S Application Pools Scheduled Tasks Hosts with the following Operating Sy ost Name match: can have multiple values specified, by sep	Piscovery 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 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 T. 0 All MariaDB Accounts 0 Dependencies on Domain Controllers 0 Discover all PostgreSQL Accounts 0 Discover All SonicWALL Accounts 0 Discover Server Admin Accounts 0 Windows Local Admin Accounts Oelete Sele Actions... 🕑 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 (<u>https://haveibeenpwned.com</u>) tracks and provides an API to check if passwords have been exposed in prior breaches.

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

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

SHave 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

Please spec	fy a password below to check if it has been known to be compromised in any public data breaches.
Please note and comple	that a 'Pass' here does not necessarily mean the password is strong in nature - you should use long x passwords where possible.
Password:	Check Password Clear
Status: Waitin	g 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. Bitwarden
- 4. KeePass
- 5. LastPass
- 6. Delinea Secret Server
- 7. Password Manager Pro

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

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

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

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

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.

lect Import	Type Instructions	Import Data	Results	
ease select w	hat type of Import you would like to p	perform below, and then follow further o	n screen instructions for your imp	port.
nport Type:	Choose Import Type	,	r	
	Choose Import Type			
	CSV file into Single Password List			
	CSV file into Multiple Password Lists			
	Bitwarden			
	KeePass			
	LastPass			
	Delinea Secret Server			
	Password Manager Pro			Nort

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.

			Q	 Screen 	n Options		
9 Web S	ites (Passv	vordListID = 20259) (Al	PI Key = N	ot Set)			
Actions	PasswordID	Title		User Name		Description	URL
0	70457	AA - Host Record					
0	70461	aaaa					ł
0	70336	adaptiveinsights	ත		•		
0	70337	arubainstanton					h
0	70338	auth.services.adobe.co	m		3		ł
0	70339	bancsabadell					v
0	70340	business.apple.com					5
0	70341	central.arubanetworks					h
0	70342	crowdstrike	-		•		ŀ
0	7034	directsourcing		-			ŀ
Add Di	ocuments (0)) Permalink Grid	l Layout Ac	tions V Lis Lis PA	st Administrator Action st Administrator Action ASSWORD LIST ACTION	15 5 NS	•
Add D	ocuments (0) t/Activity () Permalink Grid	l Layout Ac	tions V Lis	st Administrator Action st Administrator Action ASSWORD LIST ACTION	15 5 NS	•
Add D Add D Add	ocuments (0) t/Activity) Permalink Grid	l Layout Ac	tions V Lis	st Administrator Action st Administrator Action ASSWORD LIST ACTION Bulk Delete Selected	ns s NS Passwords	•
Add D Add D Recent Date 8/12/2021 S	ocuments (0) t/Activity	Permalink Grid Activity Password List Update	l Layout Ac	tions V Lis Lis PA	st Administrator Action st Administrator Action ASSWORD LIST ACTION Bulk Delete Selected Bulk Permissions for	15 5 VS Passwords Individual Passwords	
Add D Add D Add	ocuments (0) t Activity 9:41:06 AM 2:32:39 PM	Permalink Grid Activity Password List Update Password List Update	l Layout Ac	tions VLis Lis PA	st Administrator Action st Administrator Action. ASSWORD LIST ACTION Bulk Delete Selected Bulk Permissions for Bulk Update Passwor	ns s NS Passwords Individual Passwords rds	
Add D Add D D Add D D D D D D D D D	ocuments (0) t Activity 9:41:06 AM 2:32:39 PM 2:19:55 PM		l Layout Ac	tions V Lis Lis PA	st Administrator Action st Administrator Action ASSWORD LIST ACTION Bulk Delete Selected Bulk Permissions for Bulk Update Passwor Bulk Update Passwor	15 5 VS Passwords Individual Passwords rds rd Reset Options	
Add D Add D Add D Add Add D Add Add Add Add Add Add Add Add Add Ad	ocuments (0) t Activity 2:41:06 AM 2:32:39 PM 2:19:55 PM 2:19:55 PM 2:18:06 PM	Permalink Grid Activity Password List Update Password List Vpdate Password List Vpdate Password List Vpdate Password List Vpdate Pas	l Layout Ac	tions V Lis PA	st Administrator Action st Administrator Action ASSWORD LIST ACTION Bulk Delete Selected Bulk Permissions for Bulk Update Passwor Bulk Update Passwor Convert to Shared Password List	ns s NS Passwords Individual Passwords rds rd Reset Options assword List	
Add D Add D Add	ocuments (0) t Activity 9:41:06 AM 2:32:39 PM 2:19:55 PM 2:18:06 PM 1:10:22 PM	Permalink Grid Activity Password List Update Password List Vpdate Password List Vpdate Password List Vpdate Password List Vpdate Pas	ed ed ed ed ed ed	tions Vis Lis PA S I I I I I I I I I I I I I I I I I I	st Administrator Action st Administrator Action ASSWORD LIST ACTION Bulk Delete Selected Bulk Permissions for Bulk Update Passwor Bulk Update Passwor Convert to Shared Pa Delete Password List Edit Password List Pr	ns s NS Passwords Individual Passwords rds rd Reset Options assword List	
Add D Add D Add D Add Recent 8/12/2021 2 1/12/2021 2 1/12/2021 2 1/12/2021 2 1/12/2021 2	ocuments (0) t Activity 2:41:06 AM 2:32:39 PM 2:19:55 PM 2:19:55 PM 2:19:55 PM 1:10:22 PM 1:00:00 PM	Permalink Grid Activity Password List Update Password List Update Password List Update Password List Update Password List Update Password List Update	Layout Ac	tions V Lis PA	st Administrator Action at Administrator Action ASSWORD LIST ACTION Bulk Delete Selected Bulk Permissions for Bulk Update Passwor Bulk Update Passwor Convert to Shared Pas Delete Password List Edit Password List Pr	ns s NS Passwords Individual Passwords rds rd Reset Options assword List coperties s Template	
Add Date 8/12/2021 2 1/12/2021 2 1/12/2021 2 1/12/2021 2 1/12/2021 2 1/12/2021 2 1/12/2021 2 26/11/2021	ocuments (0) t Activity 9:41:06 AM 2:32:39 PM 2:19:55 PM 2:19:55 PM 2:18:06 PM 1:10:22 PM 1:09:00 PM 9:06:41 AM	Permalink Grid Activity Activity Password List Update Password List Update	ed ed ed ed ed ed ed ed ed ed ed ed ed e	tions V Lis Lis P4 4 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Administrator Action at Administrator Action ASSWORD LIST ACTION Bulk Delete Selected Bulk Permissions for Bulk Update Passwor Bulk Update Passwor Convert to Shared Pas Delete Password List Edit Password List Pr Save Password List at Toggle Visibility of D	ns s NS I Passwords Individual Passwords rds rd Reset Options assword List coperties s Template velete Checkboxes	
Add D Add D Add	ocuments (0) t Activity 2:41:06 AM 2:32:39 PM 2:19:55 PM 2:18:06 PM 1:10:22 PM 1:09:00 PM 9:06:41 AM	Permalink Grid Activity Password List Update Password List Update Password List Update Password List Update Password List Update Password List Update Self Destruct Messag	ed ed ed ed ed ed ed ed ed ed ed ed ed e		st Administrator Action at Administrator Action ASSWORD LIST ACTION Bulk Delete Selected Bulk Permissions for Bulk Update Passwor Bulk Update Passwor Convert to Shared Pa Delete Password List Edit Password List Pr Save Password List at Toggle Visibility of D Toggle Visibility of W	IS S NS I Passwords Individual Passwords rds rds rd Reset Options assword List coperties s Template velete Checkboxes Veb API IDs	
Add Date Date 8/12/2021 2 1/12/2021 2 1/12/2021 2 1/12/2021 2 1/12/2021 2 1/12/2021 2 26/11/2021 25/11/2021	ocuments (0) t Activity 9:41:06 AM 2:32:39 PM 2:19:55 PM 2:19:55 PM 1:10:22 PM 1:09:00 PM 9:06:41 AM 1:59:43 PM	Permalink Grid Activity Activity Password List Update Password List Update Password List Update Self Destruct Messag Password Updated Password Updated	ed ed ed ed ed ed ed ed ed ed ed ed	tions Lis	st Administrator Action st Administrator Action (SSWORD LIST ACTION Bulk Delete Selected Bulk Permissions for Bulk Update Passwor Bulk Update Passwor Convert to Shared Pas Delete Password List Edit Password List Pr Save Password List Pr Save Password List at Toggle Visibility of D Toggle Visibility of W	IS S NS I Passwords Individual Passwords rds rd Reset Options assword List coperties s Template velete Checkboxes Veb API IDs Permissions	
Add D Add D Add	ocuments (0) t Activity (2:41:06 AM 2:32:39 PM 2:19:55 PM 2:19:55 PM 2:19:55 PM 1:10:22 PM 1:09:00 PM 9:06:41 AM 1:59:43 PM 1:59:38 PM	Permalink Grid Activity Password List Update Password List Update Password List Update Password List Update Password List Update Password List Update Self Destruct Messag Password Updated Password Screen Ope	l Layout Ac		st Administrator Action at Administrator Action ASSWORD LIST ACTION Bulk Delete Selected Bulk Permissions for Bulk Update Passwor Bulk Update Passwor Convert to Shared Pas Delete Password List Edit Password List Pr Save Password List an Toggle Visibility of D Toggle Visibility of W View Password List P	IS s NS I Passwords Individual Passwords rds rd Reset Options assword List coperties s Template velete Checkboxes Veb API IDs Permissions	
Add D Add D Add	ocuments (0) t Activity 2:41:06 AM 2:32:39 PM 2:19:55 PM 2:19:55 PM 2:19:55 PM 2:19:55 PM 2:19:55 PM 2:19:55 PM 2:19:55 PM 1:09:00 PM 9:06:41 AM 1:59:43 PM 1:59:38 PM 1:59:38 PM	Permalink Grid Activity Password List Update Password List Update Password List Update Password Screen Ope Password Screen Ope Password History Exp Password History Exp	d Layout Ac		st Administrator Action st Administrator Action SSWORD LIST ACTION Bulk Delete Selected Bulk Permissions for Bulk Update Passwor Bulk Update Passwor Convert to Shared Pa Delete Password List Pr Save Password List Pr Save Password List Pr Save Password List Pr Coggle Visibility of D Toggle Visibility of W View Password List P View Recycle Bin (2) CONT	NS s NS I Passwords Individual Passwords rds rd Reset Options assword List coperties s Template velete Checkboxes Veb API IDs Permissions	
Add D Add D Add	ocuments (0) t Activity (2:41:06 AM 2:32:39 PM 2:19:55 PM 2:19:55 PM 2:19:55 PM 1:10:22 PM 1:09:00 PM 9:06:41 AM 1:59:43 PM 1:59:38 PM 12:58:02 PM 12:58:02 PM	Permalink Grid Activity Password List Update Password List Update Password List Update Password List Update Password List Update Password List Update Self Destruct Messag Password Updated Password Screen Ope Password History Exp	l Layout Ac		st Administrator Action at Administrator Action ASSWORD LIST ACTION Bulk Delete Selected Bulk Permissions for Bulk Update Password Bulk Update Password Convert to Shared Pas Delete Password List Edit Password List Pr Save Password List Pr Save Password List Pr Save Password List Pr Congle Visibility of D Toggle Visibility of W View Password List P View Recycle Bin (2) (PORT	IS s NS I Passwords Individual Passwords rds rd Reset Options assword List coperties s Template velete Checkboxes Veb API IDs Permissions History	
Add Date Date 8/12/2021 2 1/12/2021 2 1/12/2021 2 1/12/2021 2 1/12/2021 2 1/12/2021 2 25/11/2021 25/11/2021 25/11/2021 25/11/2021 Char	ocuments (0) t Activity 2:41:06 AM 2:32:39 PM 2:19:55 PM 2:19:55 PM 2:19:55 PM 2:19:55 PM 2:19:55 PM 2:19:55 PM 1:09:00 PM 1:09:00 PM 1:09:00 PM 1:59:38 PM 1:59:38 PM 12:58:02 PM 12:58:02 PM	Permalink Grid Activity Password List Update Self Destruct Messag Password Updated Password Screen Ope Password History Exp	l Layout Ac	tions V Lis Lis PA U U U U U U U U U U U U U U U U U U	st Administrator Action st Administrator Action SSWORD LIST ACTION Bulk Delete Selected Bulk Permissions for Bulk Update Passwor Bulk Update Passwor Bulk Update Password Convert to Shared Pass Convert to Shared Pass Convert to Shared Password Convert to Shared Password	NS s NS I Passwords Individual Passwords rds rd Reset Options assword List coperties s Template velete Checkboxes Veb API IDs Permissions History constant	
Add D Add D Add	ocuments (0) t Activity (2:41:06 AM 2:32:39 PM 2:19:55 PM 2:19:55 PM 2:18:06 PM 1:09:00 PM 9:06:41 AM 1:59:43 PM 1:59:43 PM 12:58:02 PM 12:58:02 PM 12:58:02 PM 12:58:02 PM	Permalink Grid Activity Password List Update Password List Update Password List Update Password List Update Password List Update Password List Update Self Destruct Messag Password Updated Password Screen Ope Password Screen Ope Password History Exp	l Layout Ac		st Administrator Action at Administrator Action ASSWORD LIST ACTION Bulk Delete Selected Bulk Permissions for Bulk Update Password Bulk Update Password Convert to Shared Pass Convert to Shar	IS s NS I Passwords Individual Passwords rds rd Reset Options assword List coperties s Template velete Checkboxes Veb API IDs Permissions History compromises	
Add D Add D Add	ocuments (0) t Activity (9:41:06 AM 2:32:39 PM 2:19:55 PM 2:19:55 PM 2:19:55 PM 2:19:55 PM 2:19:55 PM 2:19:55 PM 1:09:00 PM 1:09:00 PM 1:09:00 PM 1:59:43 PM 1:59:38 PM 12:58:02 PM 12:58:02 PM 12:58:02 PM	Permalink Grid Activity Password List Update Self Destruct Messag Password Updated Password Screen Ope Password Screen Ope Password History Exp	l Layout Ac		st Administrator Action st Administrator Action ASSWORD LIST ACTION Bulk Delete Selected Bulk Permissions for Bulk Update Password Bulk Update Password Bulk Update Password Convert to Shared Pass Convert to Shared Pass Convert to Shared Pass Convert to Shared Password List Edit Password List Pr Save Password List Pr Save Password List Pr Save Password List Pr Coggle Visibility of D Toggle Visibility of D Toggle Visibility of W View Password List P View Recycle Bin (2) (PORT Export All Password Stendth P Have I Been Pwned C Password Stendth P	NS s NS I Passwords Individual Passwords rds rd Reset Options assword List roperties s Template relete Checkboxes Veb API IDs Permissions History ions Report Compromises renort	



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.

enerate passwords	hanumerics & special characters	word phrases
■ include Alphanumencs & Sp		
Password Length		
Length : 8 Min 12	Max	
Alphanumerics		
🗹 Lower-case 🛛 Upper-	case 🖉 Numbers	
Include higher ratio of al	phanumerics vs special characters	
Include ambiguous alpha	numerics (I, I, o, 0 and 1)	
Table is falled in a descel		
abcdABCD	ers and numerics	
Special Characters		
Include the following spe	cial characters	
!@#\$%^&*+/=		
Include the following bra	ckets	
[](){}<>		
Generate Using a Patte	m	
Generate based on a patt	ern of upper and lowercase letters, an	d numbers
uulliinnnniiinnnn	and a feature base is a 100 million	
I for Lowercase, u for upperca	ase, and n for numbers i.e. ulllinnnnlilli	nnnn
		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		
lease use the various tabs below to specify options for your Personal Pa	assword Generator o	options.
generate passwords alphanumerics & special characters	word phrases	
☑ Include Word Phrases		
Quantity & Length		
Number of Words :1Maximum Word Length :4		
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		
		Save Options

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	alphanumerics & special characters	word phrases
Use settings from: My Number of Passwords	Personal Generator Options 15 Generate Generate & Spell	Select All
cot-Jy6Hz3MpFS5R emit-Q6SZE5TjrRfq rice-2MxkgG8SPVN jots-3MpsHTLfr net-Q6SZE5TjrRfq lees-gXixsTVqY3u5 tear-sWtLxRHPz7w wags-U6gzrWPGHFx dry-89XQLizn glad-XWx623ptES next-Xn5ZhtzPKJYf flee-pzyeJ4i3 twig-z4tJqeRpSiY rib-LvNKgepTQ ease-Nv97T4sJz		
		Save Options

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.

elow are oublesho	all the pending Pa ot any issues as to	ssword R why the	eset tasks in y are not mo	the Queu wing thro	e at the n ugh the c	nomer Jueue.	t, as well	as most r	ecent auditin	g data fo	r these queu	ed record	ds. You can us	e this screen to watch	resets progress throu	gh the queue, or to
1 Pass	word Reset Q	lueue														
Actions	Queued At		Title		Domain	or Ho	st U	serName		Accoun	it Type	Descrip	otion	Site Location	Dependencies	
		t T		Ŧ			T		T		T		T	T	T	
0	13/06/2017 12:5	9:00 PM	Splunk Acc	ount	🚓 halo:	x	s	olunkaccn	t@halox.net	& Acti Directo	ve ry	Used fo	or SIEM	Internal	0	
Date		Platforr	n -	UserID		F	irst Name		Surname	-	Activity	-	Description			
	iii T		T			T		T		T		Ť		Ť		
13/06/20	17 12:58:56 PM	Web				ţ					Password F Added to 0	leset Jueue	'Splunk Act UserName a record be tasks. This (halox.net).	ma count' (Password List = = splunkaccnt@halox.i ing added to the queu account relates to an A	nually modified the P \Infrastructure\Active net, Description = Use le to perform appropi active Directory accou	assword for account 2 Directory Account 2d for SIEM), resulti riate Password Rese nt on the domain h
13/06/20	17 12:58:51 PM	Web									Password S Opened	creen	'Splunk Aco password i splunkaccn	ope count' (Active Directory s possible on this scree t@halox.net, Descriptio	ened the Edit Passwor / Accounts) - viewing en. (Title = Splunk Acc on = Used for SIEM).	d screen for passwo the value of the count, UserName =
13/06/20	17 11:40:46 AM	Web									Password S Opened	creen	password i splunkacen	ope count: (Active Directory s possible on this scree t@halox.net, Descriptio	ened the Edit Passwor / Accounts) - viewing m. (Title = Splunk Acc on = Used for SIEM).	d screen for passw the value of the count, UserName =
											Deserved		A sub-sub-ta-		la e els este e e e e e e e e e e e e e e e e e	design of all the second second

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
- 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
- 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 <u>Address Book</u> 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.

essage Content	Email to Recipient	Passphrase Protection	
ter the contents of the Self De	struct message you want the recipient to read.		
💥 🛍 🖨 B Z 🗓 🛔	≣ ≣ ≣ 1 ⊟ ≣ ⊯ ⊯ A • Ø •	"Segoe UI", T 🔻 13px 🔹	
li John,			
he password for <u>HostXYZ</u> is <u>N</u>	lyStrongPassword123		
legards			
ohn			
Design Review			.::
tomatically self-destruct this r	nessage if not viewed in: 3 days 🔹		
	to be viewed 60 times.		
ow the self-destruct message	once		

you want Passwordsta ext button.	te to send the Self Destruct Message Email and URL, please sel	ect the Recipient below. Otherwise, please click th
elect Recipient	Click Studios (support@clickstudios.com.au)	•
ubject	Passwordstate - Self Destruct Message	
🐰 🛍 🛱 B 🖊	<u> 빈</u> 돌 돌 ≡ ¹ / ₅ Ξ 등 章 章 A · Ø · Verdana	12px ▼ abc
ні		
You've been sent a S URL below. URL: <u>https://passwol</u>	elf Destruct Message from Passwordstate, and you can view rdstate9appserver.halox.net/selfdestruct/?id=902af4360fc6	w the detail of the message by clicking the 64bb1b43f9b6fb9968e44
You've been sent a S URL below. URL: <u>https://passwo</u> r This message will exp	elf Destruct Message from Passwordstate, and you can view rdstate9appserver.halox.net/selfdestruct/?id=902af4360fc6 pire [ExpirePeriod] from the time of this email being sent.	w the detail of the message by clicking the 54bb1b43f9b6fb9968e44
You've been sent a S URL below. URL: <u>https://passwor</u> This message will exp Passwordstate 9.0 - <u>S</u> https://passwordstat	elf Destruct Message from Passwordstate, and you can view rdstate9appserver.halox.net/selfdestruct/?id=902af4360fc6 pire [ExpirePeriod] from the time of this email being sent. Secure Password Management. e9.halox.net	w the detail of the message by clicking the 64bb1b43f9b6fb9968e44
You've been sent a S URL below. URL: <u>https://passwor</u> This message will exp Passwordstate 9.0 - S https://passwordstat	elf Destruct Message from Passwordstate, and you can view rdstate9appserver.halox.net/selfdestruct/?id=902af4360fc6 pire [ExpirePeriod] from the time of this email being sent. Secure Password Management. e9.halox.net	w the detail of the message by clicking the 54bb1b43f9b6fb9968e44 .::

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

lessage Content	Email to Recipient	Passphrase Protection
o protect access to your S	ielf Destruct message with the user of a Passphr.	ase, please specify this below - you must inform your
ecipient the value of this I	Passphrase before they can read the message.	
assphrase Protection:	•••••	Q,
Cancel		Previous Send
		Trevious oction

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.

124 Passwordstate User Manual

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

2.3.1 Auditing

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

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

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

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

ゴ Auditing													1
To search for releva	nt audit recor	rds, please use the opt	ions below.										
Auditing Filter	rs												
Platform: 🔘 All	I O Web O	Mobile Oapi Ow	indows Service OBro	wser Extension	Instance: 💿 🛛	oth (⊖ Primary ⊖ HA	(Passive Nod	e)	Archived Data:	No	O Yes	
Max Records	Password Li All Password	st d Lists	All Ac	y Type tivities	¥	Site	Location Activity Il Site Locations -	Begin	Date	End Date # 4/12/202	0	E Search	
Date		Platform	UserID	First Name	Surname		IP Address	HA In	stance	Activity		Tree Path	Descr
	T	T	T	T		T		Ŧ			Ŧ	T	
4/12/2020 11:39:14	4 AM	Web	halox\images	Image	Capture		10.0.0.108			Login Attempt Succeeded			Succe
4/12/2020 11:32:3	6 AM	Windows Service	WindowsService	Windows Service	Account		10.0.0.125			Password Validation Successful		\Infrastructure\AD Discovery	A sch View I
4/12/2020 11:32:3	6 AM	Windows Service	WindowsService	Windows Service	Account		10.0.0.125			Password Validation Successful		\Infrastructure\AD Discovery	A sche View I

Filter by Platform

uditing Filte	ars		
	I Oweb Owebie Owe	lindows Sonvice O Prowser Extension	Instanc
Plattorm: 🖲 A	II 🔍 Web 🔍 Mobile 🔍 API 🔍 W	Vindows service Browser Extension	matane
Max Records	Password List	Activity Type	mstane

Filter by Specific Password Lists

Auditing Filte	ers					
Auditing Filte	ers NI Oweb Omobile Oapi Owind					
Platform: 🔘 🖉	All Oweb Omobile OAPI Owind					
		and Somico O Proweor Extension Insta	ance: Roth O Brimany O HA (B	accive Node)	Archived Data:	O Vor
Marco De consta	Description	A sticks True	Cite Leasting A	abile Beele	Deter Fiel De	
FOOD	Password List	Activity Type	Site Location A	tivity Begin	Date End Da	.te 2020 📾 Sear
5000	All Password Lists	Air Acuvities	All Site Locat	ons	10/12/3	2020 [[] 300
	Business Systems\Credit Cards					
	🖳 \Business Systems\Database Acc	ounts				
ate	🖳 \Business Systems\Microsoft SQL	Local Accounts	IP Address	HA Instance	Activity	Tree Path
	\Business Systems\Oracle ERP Ac	counts	T		Т	Т
	🖶 \Business Systems\SharePoint Ac	counts				
	🚫 \Business Systems\SSL Certificate	15			Password	\Infrastructure\AD
)/12/2020 9:07:	³⁰ Business Systems\Test Password	List	10.0.0.91		Validation Failed	Discovery
	\Customers\Allsand\Workstation	Accounts				
	\Customers\Contoso\DBAs\Data	base Credentials				
		a) Activo Directory Accounts			Password	\Infrastructure\AD
0/12/2020 9·07·	3(Customers\Contoso\Infratructur	evacuive Directory Accounts	10.0.0.91			

Filter by Specific Activity Type

🖬 Auditing

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

Auditing Filte	rs						
Platform: 🖲 A	ll 🔍 Web 🔍	Mobile 🔍 API 🔍 W	indows Service		Browser Extension	1 O P	Primary 🔘 H
Max Records	Password Lis	t			Activity Type	Site	Location
5000	All Password	Lists		•	All Activities	A	ll Site Locati
					All Activities	-	
					Access Granted	- 1	
					Access Removed	- 1	
Date		Platform	UserID		Access to Password Approved		ess
	T	T		•	Access to Password Denied		т
13/06/2017 12:58	8:56 PM	Web	halox\msand		Access to Password Requested Access to Password List Approved Access to Password List Denied		9
13/06/2017 12:58	8:51 PM	Web	halox\msand		Access to Password List Requested Access Updated		9
13/06/2017 12:56	5:33 PM	Windows Service	WindowsServi	ice	Discovery Job Added Discovery Job Completed Discovery Job Deleted		9
13/06/2017 12:52	2:04 PM	Web	halox\msand		Discovery Job Updated	-	9

Filter between Specific Dates

Auditing Filters			
Platform: All O Web O Mobile O API O Windows Service	e O Browser Extension	Instance: Both O Primary O HA (Passive Node)	Archived Data: No O Yes
Max Records Password List 5000 All Password Lists	Activity Type All Activities	Site Location Activity Begin Date 	End Date # 4/12/2020 # Search

Further Filter by Search Results Contents

/

Auditing Filters Platform: All Web Max Records Password All Password All Password	O Mobile O API O) Windows Servic	e O	Browser Extension Activity Type	Instance
All Passo			Ť	All Activities	
Date	Platform	UserID		First Name	Surname
111 T	T			NoFilter	
19/01/2015 1:23:40 PM	Browser Extension	halox\msand		Contains DoesNotContain StartsWith EndsWith	
19/01/2015 1:23:27 PM	Browser Extension	halox\msand		EqualTo NotEqualTo GreaterThan LessThan	
				GreaterThanOrEq	ualTo

2.3.2 Auditing Graphs

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



2.3.3 Scheduled Reports

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

Choosing The Report Type

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

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

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

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

User Reports

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

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

Passwords Reports

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

Permissions Reports

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

Audit Activity Reports

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

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

☑ 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	schedu	ıle expirin	g passwords settings	auditing settings	security admin report options	
Please enter a Nam	e and Desc	ription for you	r report, and select the Re	eport type you want.	Then make changes on the other tabs as required.	
Report Settin	gs					
Report Name *	:				Report Name will be used as the Subject Line in the Email.	
Report Descript	ion :					
CC Report To					comma separate the email addresses	
Email Report As		Embadda		ent (CSV files are re	acommanded if the report constants a lot of data)	
Linui report / a		© Embedde		ient (CSV nies are re	econimended in the report generates a lot of data)	
File Attachment	Name *:				Append date to file name in format of YYYY-MM-DD.	
		🗹 Do not se	nd report if it produces n	o results.		
Select Report	t Туре		Report	escription & Crit	teria	
Please choose t	he appropr	riate report belo	ow. Report N	ame: Please select or	ne of the available reports on the left to see a description of what the report provi	des.
			Report D	escription:		
Choose Report	t		~			
Choose Report						
Custom Auditi	ng Report				Save	anort Cancal
USER REPORTS	5				Saven	cancer
What passwor	ds can a us	er see?				
What passwor	ds does a u	iser still know?				
What has a use	er been doi	ing lately?				
What Failed lo	gin attemp	ts have there b	een?			
Who hasn't log	gged in rec	ently?				
Who has one o	or more Sec	curity Administr	rator roles?			
What user acc	Sessions na	is a user been o urrontly disable	Joing lately:			
What user acco	ounts are s	et to evoire?	545 C			
Which users ha	ave logged	in using the En	nergency Access account	?		
What user acc	ount imper	sonation has be	een occurring?			
PASSWORD R						
What passwor	ds have fail	ed Heartbeat?				
What passwor	ds have fail	ed Reset?		-		
-						

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.

DAdd Schedule	ed Report			
cheduled Reports allo	ows you to rece	ive various reports via email. Please	use each of the tabs b	elow, as appropriate, to specify settings for your report.
report settings	schedule	expiring passwords settings	auditing settings	security admin report options
Please specify the ti	me you would	like to receive the report, and the fi	equency.	
Generate Report at:	00 - Hou	r 00 🔻 Minute		
Report Freque	ency			
One Time	No additiona	al settings for a Daily Schedule		
Daily				
Weekly				
Monthly				

Save Report Cancel

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.

	·	'			
report settings	schedule	expiring passwords settings	auditing settings	security admin report options	
Password List(s)		Passwords ex	piring in the next		
All Password Lists		▼ 30 day(s).	Also query passwor	ds 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.

port settings schedule	expiring passwords settings	auditing settings security	v admin report options	
ase select the appropriate filters b	elow to query auditing data for y	vour report.		
Auditing Filter				
latform: I All Web Mob	oile O API O Windows Service	Browser Extension Instan	ice: Both Primary High	Availability
Password List	Activity Ty	pe	Site Location	Query Previous
All Password Lists	▼ - Select Ac	tivity Type -	▼ All Site Locations ▼	7 Days 0 Hours 0 Minutes
	Filter on co	ontent in Description Field		
Filter By User Account				
Filter By User Account				

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 Schedule	ed Report									
Scheduled Reports allo	ows you to recei	ve various reports via email. Please	use each of the tabs be	elow, as	appropriate, to s	pecify settin	gs for your repor	rt.		
report settings	schedule	expiring passwords settings	auditing settings	secu	rity admin repor	t options				
Depending on the t	ype of report se	ected, certain controls below may	disabled - certain repo	rts allov	v you to further fi	ter on speci	fic users.			
Passwordstate Use	er Account	Site Loca	tion		Duration					
		All Sit	e Locations	*	Past 30 Days	v				
									Save Report	Cancel

2.4 Preferences Menu

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

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

2.4.1 Address Book

The address book is used primarily for two features:

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

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

ted below	are all your personal contacts, as well as any global cont	acts. The Address Book can be used f	or storing a	any personal contacts, a	nd can also be used	in conjuction with the S	elf Destruct Message feature.	
ow only :	Personal Contacts Global Contacts							
Actions	Full Name	Email Address		Company	Business Phone	Personal Phone	Global Contact	Passphrase Set
		T	т	T			T	T
0	Michael Reznor	mreznor@outlook.com						×
0	Felicity Carter	f.carter@mail.com						
				and the second second				

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.

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

The Preferences screen has the following 8 tabs:

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 O 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 O 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: O Client Based Launcher								
Use Load On Demand Feature for faster loading and expanding of Nodes in the Passwords Navigation Tree: O 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 numbers of enders this will be a limit an angles in the start of Descured Lience only.								
3. Only the root no 4. Expanding the no 5. Searching for Pas	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.							
						Save Save & Close		

2.4.2.2 Hosts Tab

The Hosts Tab allows you to select various options for the Hosts Navigation Tree under the <u>Hosts</u> 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

nosts tab	miscellaneous	color theme	admentication options	mobile access options	browser extension	opi	
ase specify settings for featur	es under the Hosts ta	b as appropriate.					
osts Options							
mit the number of displaye	d Nodes (Folders an etting to 0 will show a	d Host records) in the	e Navigation Tree to: a the number of displayed No	des use the 'Search Hosts' fe	ature)		
(5	stang to o will show a	in Nodes, and in initially	g the number of displayed in	des, use the Search hosts le	aurea		
se Load On Demand Featur ⊃Yes ●No	e for faster loading a	and expanding of No	des in the Hosts Navigation	Tree:			
ad On Demand is used for p If limiting the number of no Only the root nodes will be Expanding the nodes will ret Searching for Folders/Hosts	erformance reasons w des, this will be a limit visible, and collapsed, trieve the nested node will behave as per no	when you have thousar on nodes in the root of when first navigating f so live from the databa rmal.	nds of nodes in the Navigatio of Hosts Home only to the tree ise	n Tree. When enabled, the foll	owing will occur:		
rowser Based Remote S	Session Settinas						
	g-						
r RDP Sessions, use the fo	lowing performance	settings:					
items checked		•					
you would like to use a dif	ferent Keyboard law	out for RDP sessions	nlease select it here:				
- Select Keyboard Layout		.					
			-to-to				
or 55H Sessions, select the	ont size you would i	The to use in the term	ninai:				
3							
or SSH Sessions, please sele	ect the Background a	nd Font colors that y	ou would like to use:				
- demonstration Deletter	Freed Colo	Deletter					
Apex	 Apex 	r Palette	Ŧ				
ackground Color:	Font Cold	or:					

2.4.2.3 Miscellaneous Tab

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

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

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

Preferences

modify your prefere	ences for Passwo	ordstate, please make	e changes in the re	levant tabs below, then click o	n the 'Save' button.	
passwords tab	hosts tab	miscellaneous	color theme	authentication options	mobile access options	browser extension
Please select which	of the following	miscellaneous optic	ons within Password	dstate you would like to enable	à	
Password Visibility	y on Add/View/ k	/Edit Pages:				
Auto Generate Ner	w Password Wł	hen Adding a New F	Record:			
Enable Search Crit	eria Stickiness /	Across Password Sc	reens:			
Show the 'Actions' Bottom O Top	toolbar on the	e Passwords pages a Top	it the:			
On all Password Li Do not sort by def	st screens, sort ault	the grid by the foll	owing column: •			
On the Passwords Do not sort by def	Home screen, s ault	sort the Search Resu	Ilts and Favorite P	Passwords grids by the follow	ing column:	
When creating new	w Shared Passw	vord Lists, base the	settings on the fo	llowing Template's settings:		
Do not use templa	ite		*			
When creating new	w Shared Passw	vord Lists, base the	permissions on th	e following Template's perm	issions:	
Do not use templa	ite		-			
Locale (Date Form	at):					
Use System Wide I	Locale Setting		•			
If you would like t Select Keyboard	o use a differer l Layout	nt Keyboard layout	for RDP sessions v	when using the Browser Base	d Launcher, please select it l	here.
						Save Save & Close

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 W System Wide	ide color them ○ Choose My C	e, or choose your ow Jwn	/n:				
Base Color Please select the Color Palette ADex	Base Color to u	use throughout Passwo	ordstate.				
Base Color:							
						S	ave 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.

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

The following table describes each of the Authentication Options:

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

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

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

or as a secondary authentication
or as a secondary authentication
cable if

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.

Login Enter the corresponding letters for your ScramblePad pin number. ScramblePad Pin : Logon 0 1 2 3 4 5 6 7 8 9	Ogin Enter the corresponding letters for your ScramblePad pin number. ScramblePad Pin : Logon 0 1 2 3 4 5 6 7 8 9 H E B R L X W C U Y							≁ Scra	Pa	SSV ePad	vor Aut	ds t	tate ication
ScramblePad Pin : Logon 0 1 2 3 4 5 6 7 8 9	ScramblePad Pin : Logon 0 1 2 3 4 5 6 7 8 9 H E B R L X W C U Y	Login Enter th	ne corr	respon	iding le	etters f	for you	ır Scra	mblePa	ad pin	numb	er.	
0 1 2 3 4 5 6 7 8 9	0 1 2 3 4 5 6 7 8 9 H E B R L X W C U Y	Scra	mbleP	ad Pir	1:							Log	on
			0 H	1 F	2 B	3 R	4	5 X	6 W	7	8 U	9 V	

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 <u>Android</u>, <u>iOS</u> & <u>Windows Phone</u>
- 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:
 Select the appropriate Google Authenticator option above Generate a new barcode/secret key Scan the barcode into Google Authenticator on your mobile pevice, or manually type in the displayed Secret Key Click on the 'Save' button.
Secret Key: HMJTAJHGKVAM45ZI New Clear

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').

	Coogle Authenticator
Login	
Please enter your us authenticate.	er name, password and Google verification code to
Username	halox\ *
Password	
Verification Code	Logon
	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).
Temporary Pin Code Authentication
Login
To authenticate with your Temporary Pin Code, please check your registered email address and enter the Pin Code below.
Pin Code Logon
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 (couner-based algorithm which does not require internet connectivity)
- OATH TOTP (time-based algorithm which does not require internet connectivity)

By default, new YubiKey's are configured for Yubico OTP, but the configuration can be changed using Yubico tools. Below are instructions for configuring your YubiKey for each of the authentication options above. The following tools will need to be downloaded and installed on your desktop:

- To configure for Yubico OTP or HOTP, you need this tool -<u>https://www.yubico.com/products/services-software/download/yubikey-personalization-tools/</u>
- To configure and authenticate using TOTP, you need this tool <u>https://www.yubico.com/products/services-software/download/yubico-authenticator/</u>

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.

146 Passwordstate User Manual

YubiKey Person	alization Tool					
Yubico OTP	ОАТН-НОТР	Static Password	Challenge-Response	Settings	Tools	Abo
2						
		Program in Yu	bico OTP mode			
	_					
Ouick	-					
Quickly progra	im a YubiKey for us	e with Yubico Validation	Server			
Advance	d					
Allows you to p	program one or mo	ore YubiKeys with greater	r control over the configuration	n values		
	-		-			
						_
🕖 YubiKey Persor	nalization Tool					
Yubico OTP	ОАТН-НОТР	Static Password	Challenge-Response	Settings	Tools	A
Yubico OTP	ОАТН-НОТР	Static Password	Challenge-Response	Settings	Tools	A
Yubico OTP	оатн-нотр	Static Password gram in Yubic	Challenge-Response	Settings	Tools	A
Yubico OTP	оатн-нотр	Static Password gram in Yubic	Challenge-Response	Settings	Tools	A
Yubico OTP Configuration	OATH-HOTP	Static Password	Challenge-Response	Settings ick	Tools	A
Yubico OTP Configuration Select the confi	OATH-HOTP Pro	Static Password gram in Yubic	Challenge-Response	Settings	Tools	A
Yubico OTP Configuration Select the confi O Configuratio	OATH-HOTP Pro	Static Password gram in Yubic programmed O Configuration S	Challenge-Response	Settings	Tools	
Yubico OTP Configuration Select the confi Configuratio Yubico OTP Pa	OATH-HOTP Pro Slot iguration slot to be on Slot 1	Static Password gram in Yubic programmed () Configuration S generated)	Challenge-Response	Settings	Tools	
Yubico OTP Configuration Select the confi Configuratio Yubico OTP Pa Public Identity (OATH-HOTP Pro Slot iguration slot to be in Slot 1 arameters (auto (6 bytes Modhex)	Static Password gram in Yubic programmed O Configuration S generated) vv ct lt hi bg ri	Challenge-Response	Settings	Tools	
Yubico OTP Configuration Select the confi © Configuratio Yubico OTP Pa Public Identity (Public Identity (OATH-HOTP Pro Slot iguration slot to be in Slot 1 arameters (auto (6 bytes Modhex)	Static Password gram in Yubic programmed O Configuration S generated) vv ct It hi bg ri	Challenge-Response	Settings	Tools	
Yubico OTP Configuration Select the confi © Configuratio Yubico OTP Pa Public Identity (Mide values Private Identity	OATH-HOTP Pro Slot guration slot to be in Slot 1 arameters (auto (6 bytes Modhex)	Static Password gram in Yubic programmed O Configuration S generated) vv ct It hi bg ri	Challenge-Response	Settings	Tools	
Yubico OTP Configuration Select the confi Configuratio Yubico OTP Pa Public Identity (Hide values Private Identity Secret Key (16	OATH-HOTP Pro Slot iguration slot to be in Slot 1 arameters (auto (6 bytes Modhex) (6 bytes Hex) bytes Hex)	Static Password gram in Yubic programmed () Configuration S generated) vv ct lt hi bg ri	Challenge-Response	Settings	Tools	
Yubico OTP Configuration Select the confi © Configuratio Yubico OTP Pa Public Identity (Mide values Private Identity Secret Key (16 Actions	OATH-HOTP Pro Slot iguration slot to be on Slot 1 arameters (auto (6 bytes Modhex) (6 bytes Hex) bytes Hex)	Static Password gram in Yubic programmed () Configuration S generated) vv ct It hi bg ri	Challenge-Response	Settings	Tools	
Yubico OTP Configuration Select the confi Configuratio Yubico OTP Pa Public Identity (Hide values Private Identity Secret Key (16 Actions Press Write Cor	OATH-HOTP Pro Slot guration slot to be in Slot 1 arameters (auto (6 bytes Modhex) (6 bytes Hex) bytes Hex)	Static Password gram in Yubic programmed O Configuration S generated) vv ct lt hi bg ri vv ct lt hi bg ri	Challenge-Response o OTP mode - Qu Slot 2	Settings ick	Tools	
Yubico OTP Configuration Select the confi © Configuratio Yubico OTP Pa Public Identity (Mide values Private Identity Secret Key (16 Actions Press Write Con Write Con	OATH-HOTP Pro Slot iguration slot to be in Slot 1 arameters (auto (6 bytes Modhex) (6 bytes Hex) bytes Hex) nfiguration button to figuration	Static Password gram in Yubic programmed () Configuration S generated) vv ct It hi bg ri vv ct It hi bg ri o program your YubiKey Upload to Yubico	Challenge-Response	Settings ick	Tools	

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.

Select which type of Yu	Select which type of YubiKey authentication method to use, and follow instructions below as appropriate:			
2. TOTP - Generate a QI 3. HOTP - Using the Xul	R Code and use the Yubico Pico Personalization tool, c	a press the button on your Yubiker Authenticator App to scap the QR Code in opy and paste the HOTP Secret Key from the tool into the field below		
Authentication Type:	Yubico OTP	-		
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 6 digits (for Counter-Based authentication)		
Secret Key: <u>6c737629c</u>	6ec17999076eb1298c73cf	4 Generate Clear		

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.

W YubiKey Person	alization Tool			
Yubico OTP	ОАТН-НОТР	Static Password	Challenge-Response	Settings
\searrow				
	1	Program in OA	TH-HOTP mode	
Quick Quickly progra	ım a YubiKey in OA	TH-HOTP mode		
Advance	d			
Allows you to p	program one or mo	re YubiKeys in OATH-HO	TP mode with greater control of	over the configu

🦻 YubiKey Personalization Tool				
Yubico OTP	ОАТН-НОТР	Static Password	Challenge-Response	Settings Tools Al
5	Progra	m in OATH-HO	TP mode - Adva	nced
Colort the config	Slot			
Configuration	n Slot 1	 Configuration Sl 	ot 2	
Program Mu	Iltiple YubiKeys		Configuration Protectio	on (6 bytes Hex)
Automatically	/ prograph YubiKeys	when inserted	YubiKey(s) unprotected -	Keep it that way
Parameter Gene	eration Scheme	0	Current Access Code	
Increment Ider	itities; Randomize S	ecret 🔻	New Access Code	×
ОАТН-НОТР Ра	arameters		Use Senai Number	
OATH Token	Identifier (6 bytes)	All numeric		
OMP (1) + TT (1	.) + MUI (4)	00 00 00 00 0	0 00 00 Generate	MUI
HOTP Length		6 Digits 0 8	Digits	
Moving Factor S	eed	Fixed zero	▼ 0	
Secret Key (20	bytes Hex)	d0 fb d6 e0 be 0e	27 44 60 1c 6a 98 c4 e2 32 92	2 ba e7 5 Generate
Actions Press Write Con	figuration button to	program your YubiKey's	selected configuration slot	
Write Conf	figuration	Stop Res	et Back	
Results	H Takan Identifiar	Status Timostama		
# 0A1	n token idenuner	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.

Select which type of Yub	piKey authentication metho	d to use, and follow instructions below as appropriate:
1. Yubico OTE - give the	Secret Key field focus, and	press the batton 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 YUD	ico Personalization tool, co	py and paste the HOLP 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 bas drifted over time
Counter:	0	What the current Counter is for your token
HOTP Digits:	6	Generally 6 or 8 argits (for Counter-Based authentication)

Configure YubiKey for OATH - TOTP Support

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

In Passwordstate, on your Preferences screen, you need to select 'OATH - TOTP', and click then Generate button so the QR Code is displayed.

-YubiKey Authenticati	on Settings				
Select Which type of Yub	Select which type of YubiKey authentication method to use, and follow instructions below as appropriate:				
1. Yubico OTP - give the 2. TOTP - Generate a QR 3. HOTP - Using the Yub	Secret Key field focus, and Code and use the Yubico A ico Personalization tool, cop	press the button on your YubiKey uthenticator App to scan the QR Code in by and paste the HOTP Secret Key from the tool into the field below			
Authentication Type:	ОАТН – ТОТР 🦊				
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:	б	Generally 6 or 8 digits (for Counter-Based authentication)			
Secret Key: NL6J5XW4F	QRYBM3HGU3EPZVDTK7A	ESCK Generate Clear			

Then in the Yubico Authenticator Application, select Settings from the File menu, and select which Slot you want to store the config in

💿 Yubico Authenticator [Slot mode]		×
File Edit Help		
Settings	×	
Authenticator Mode YubiKey Slots	~	
Read from Slot 1 Digits 6	\sim	
Read from Slot 2 Digits 6	~	
Show in system tray		
Hide on launch	_	
Cancel Save Sett	ings	
	\checkmark	

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.

Yubico Authenticator	[Slot mode]	_	×
File Edit Help	New credential Secret key DW64JRBKVZ3MLNCPFQ YubiKey Slot Slot 2 Require touch Cancel Save credential		

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. You Passcode is a combination of your Pin, plus the Tokencode.

	Passwordstate SecurID Authentication
Login	
Please enter you	r SecurID Passcode to authenticate.
Passcode :	Logon
	Status: Awaiting Login

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.

	Passwordstate Duo Authentication
Login	
Please specify your (button.	Duo Account details below, and click on the appropriate authentication
Duo Username	images
Passcode	
	Passcode Login Send Push Send SMS Call Phone
	Status: Awaiting Login

One-Time Password

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

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

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

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

One-Time Passwo	rd Settings	tication mathed you will use and various sattings as appropriate - these sattings are only applicable if
the One-Time Passw	ord Authentication option h	as been applied to your account.
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
Counter:	5	What the current Counter is for your token
HOTP Digits:	6	Generally 6 or 8 digits (for Counter-Based authentication)
Secret Key: BW4SC	KT7ZEGR56DXJVNPHFQ3M	Generate Clear

	Passwordstate One-Time Password
Login	
Please enter your One-Time Pa	ssword to authenticate.
One-Time Password	Logon
S	Status: Awaiting Login

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.

✤ Passwordstate								
	RADIUS Authentication							
Login								
Please enter your RA	Please enter your RADIUS Username and Password to authenticate.							
RADIUS Username	awils							
RADIUS Password	Logon							
	Status: Awaiting Login							

2.4.2.6 Mobile Access Options Tab

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

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

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

sswords tab	hosts tab	miscellaneous	color theme	authentication options	mobile access options	browser extension	api
ise select select	t appropriate op	tions below for acces	sing Passwordstate	via a mobile device.			
1obile App	Settings						
Please specify	your Master Pas	sword for using the N	Nobile App, and sca	an the QR Code below into the	Passwordstate Mobile App o	n you phone.	
Mobile App S	erver QR Code		Mobile	App Username:			
			迴				
		1.21.21	Mobile	App Master Password:			
138			28 -				
		の思想を	96				
			1947 1947				
R (2							
2.53			85				
na sa sa	20 A	6.191					
	1 06 -0-14/75	SPECKOR	NRC .				

2.4.2.7 Browser Extension

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

In particular you can:

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

Please refer to the Browser Extension Manual for further instructions.

🎝 Preferences

asswords ta	b hosts tab	miscellaneous	color theme	authentication options	mobile access options	browser extension	api
ase specify I auto-confi	settings as approp gure itself.	riate below for the Pass	wordstate Browse	r extensions. Once your extens	ion is installed, all you need to	o do is login to Passwordstate	e, and the extension
rowser	Extension Ma	ster Password					
Please spe	tify your Master Pa	ssword for using the B	rowser Extensions	feature. The password must be	e used to authenticate your ex	tension, before it can be use	d.
Browser Master Pa	Extension Master ssword saved to d	Password: atabase Clear					
ear Clipt	oard Settings						
Please spe	cify settings below	for automatically clear	ing the clipboard	via the Browser Extensions.			
When trig seconds a	gering a 'Copy to fter the event: (Yo	Clipboard' event in I ou must have one of the	asswordstate or Passwordstate bi	the Browser Extension, allow rowser extensions installed for	r the Browser Extension to an this functionality)	utomatically clear the clipb	oard after (x)
10			(Setting to	0 disables this feature)			
	21 -						
ith lanored	URLs. this will pre	vent prompting to save	e login credentials	for a web site, automatically for	orm-filling the site, and display	ing the icon overlay on field:	s on the site.
	, ,		Add		5 . 15	5	
ter the bas	e URL here e.g. m	passwordstate.domain	.com				
Actions	URL						
					Т		
0	stresstest.clickse	c.net					
Clear All Ig	nored URLs						

2.4.2.8 API

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

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

& 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	
Windows Inte	egrated API C	one-Time Passwor	d					
In order to use	One-Time Pass	word Two-Factor auth	entication with the	e Windows Integrated API, you	will need do:			
1. Generate a n 2. Scan the bar 3. Click on the	ew barcode/sec code into your 2 'Save' button.	rret key 2FA App on your mob	ile device, or man	ually type in the displayed Seci	ret Key			
Secret Key: (no	ot case-sensitive	New (Clear					
							Save	Save & Close

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.

lease select	which Email Notifications you would like to receive ei	ther by disabling or enabling Categories below as appropriate.	
Actions	Category	Description	Enabled
0	Access Request	Notifies Password List Administrators that a user has requested access to a Password List or individual password	×
0	Access Request Denied	Notifies you if your request to a Password or Password List has been denied	A
0	Access to Password Changed	Notifies you if your access level to an individual Password record has changed	×
\$ То	ggle status - Enabled or Disabled	Notifies you if you've been granted access to an individual Password record	A
0	Access to Password List Changed	Notifies you if your access level to a Password List has changed	4
0	Access to Password List Grantso	Notifies you of new access being granted to a Password List	A
0	Access to Password List Removed	Notifies you of your access being removed from a Password List	×
0	Access to Password List Template Changed	Notifies you if your access level to a Password List Template has changed	A
0	Access to Password List Template Granted	Notifies you of new access being granted to a Password List Template	×
0	Access to Password List Template Removed	Notifies you of your access being removed from a Password List Template	A
н	 1 2 3 4 5 	Page: 1 of 5 Go Page size: 10 Change	Item 1 to 10 of 42
Enable All	Notifications Disable All Notifications Grid	lavout Actions 💌	

3 Hosts

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

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

Browser Based

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

Client Based

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

Note 1: By default, all users have access to all features under this Hosts tab. It is recommended a Security Administrator of Passwordstate visit the page Administration -> Passwordstate Administration -> Feature Access -> Hosts tab and Remote Sessions tab, and review each of the varying levels of access, and modify permissions as appropriate.

Note 2: Microsoft have removed the ability to pass a SQL Server account password value to SQL Server Management Studio via the command line, in Management Studio 2018. Authenticating with Active Directory accounts works with Management Studio 2018, but if you wish to use SQL Accounts you will instead need to use Management Studio 2017.

3.1 Hosts Home Screen

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

From this screen you can:

- Click on <u>View All Host Records</u> to see all Host records, and manage them
- Click on <u>View Host Discovery Jobs</u> 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.

Passwordstate valo (stuid accos)						Search Passward	's ar Hosts	र 🗄 🖓	🙎 image Capture 🛛 👌
PASSWORDS HOSTS ADMINISTRATION									
Search Hosts Q	Hosts Home								
Hosts Home	Host Statistics		& Remo	te Session Credenti	als				
🖉 🔺 🛅 Customers	Total Hosts : 206	Out-Of-Band Hosts: 2	Actions	Description	Host Name Match	Site Location	Connection Type	Linked To Password	
Alisand	Unmanaged Hosts : 12	Router Hosts : 2		T	Ϋ́	T	т	Υ	
Contoso	Windows Hosts : 165	Switch Hosts : 0	0	Cisco Devices		Internal	SSH		
V Halow	Linux Hosts : 24	Unix Hosts: 0	0	Linux Sessions	Linediate indexest	Internal	SSH	A Unit in the I	
> Firewalls	Entered Massword Nectors : 157	Host Decomants : 1	0	RDP		Internal	RDP	The second second	
Internal infrastructure			0	SQL		Internal	50.	SA Account	
 Client Based RSL 	Add Host View All Host Records View Host Discov	ery Jobs	0	SSH Key test	Q	Internal	SSH	<u>A</u> 1	U
 Linux Servers 			0	VNC		Internal	VNC		
Windows Servers			Add Cred	ential I deid avout activ	105 T				
MySQL Servers									
* switches									

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 <u>Discovery Job</u> to import them from Active Directory

sts Filters										
st Name : Show all Ma	naged Hosts O Show Hosts wi	Host Type : All Host Types v ich are Unmanaged	Operating System : Select OS *	Site Location All Site Locations *	Database Server Type Select Database Type Search					
ions 🗆	Host Name	Site Location	Port	Title	Tag	Host Type	Operating System	Database Server Type	Heartbeat Daily Schedule	Last Successful Heartbeat
	т	т	т	т	Т	т	т	τ	ĒΤ	Ē
	🔴 🖵 10.0.0.27	Internal	22			Firewall	pfSense		05:47 PM	
	😐 📮 10.0.0.5 🖜	Internal	3389			Windows	Windows Server 2019	SQL Server	02:15 AM	29/10/2018 2:15:26
	😐 🖵 10.0.0.74	Internal	22	Unifi AP1		Linux	Mint		09:52 AM	4/12/2020 9:52:35
	😑 🖵 12.28.229.178	Internal	63122	SonicWALL	SoniciP	Firewall	SonicWALL		04:07 AM	4/12/2020 4:07:28
	34.77.52.22	Internal	22	Google Cloud		Linux	RedHat Enterprise Linux		11:12 PM	
	😑 🖵 81.140.26.149	Internal	22			Switch	Cisco IOS		06:16 AM	4/12/2020 6:16:32
	🔴 🖵 AAA_Test2	Internal	22			Firewall	Fortigate		08:32 AM	
	😑 🖵 AAA_TestHost	Internal	22			Firewall	Fortigate		03:29 AM	
	• 🖓	Internal	3389		CN=Computers,DC=halox,DC=netxyz	Windows	Windows 10		04:17 PM	12/04/2020 4:17:39
	•	Internal	3389		CN=Computers,DC=halox,DC=net	Windows	Windows 10		05:25 PM	

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.

ase specify details for the H	lost as appropriate.	
Conoral Host Proportis		
Seneral Host Propertie	25	
Host Name: *		
	Fully Qualified Domain Name (FQDN) provides greater flexibility and performance, or NetBio	DS
Title:	name can be used in needed.	
	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	Internal	-
Host Type: *	Windows	*
Operating System: *	Windows 10	-
Internal IP:		
External IP:		
MAC Address:		
Session Recording: *	● Yes ● No (record all remote sessions for this Host)	
Virtual Machine: *	○ Yes ● No	
Virtual Machine Type:	O Amazon O Azure O HyperV O VirtualBox O VMware O Xen	
Database Server Type:	Select 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:	10 - Hour 01 - Minute (time each day a Heartbeat is executed)	
Remote Connection Pr	operties	
By specifying appropiate se	ettings below, this will allow a remote connection to the host directly from within Passwordstate	2.
Connection Type *	RDP 🔍 SSH 🔍 Teamviewer 🔍 Telnet 🔍 VNC	
Port Number * 338	9	
Additional Parameters		
The parameters below will you're using for Remote Se	be passed to the Passwordstate Remote Session Launcher, in an encrypted format. If the client ssions 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 (iscovery Jobs									
Below are a	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
	т	Т	Т	т	T	Т	T	т	T	T
0	Import Server Hosts	Import Server Hosts	Hosts	Internal	01:00 PM	Daily		00:00:01		×
0	Test Import	Test Import	Hosts	Internal	11:00 PM	Weekly - Sunday		00:00:01		×
Return to	Hosts Home Add Discovery Job Grid La	yout 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 a	ctive directory ous schedule
Discovery Job Name *	: Import Server Hosts
Description *	: Import Server Hosts
Site Location *	· Internal
Active Directory Domain *	
Active Directory Domain	Please specify at least one QLI on the 'Active Directory QLIs' tab.
Simulation Mode	: Simulation Mode will email you the results without adding/updating any data in the database
-Discovery Search Criteri Please select which search o	ia ptions you would like to define for the Discovery Job.
Discover hosts with the fol	llowing Operating Systems: Windows Server 2019 👻
Only discover Hosts where	the last loaded on date is greater than or equal to
only discover hosts where	the Last Logged on date is greater than of equal to .
Populate the Host's Tag fie Yes ONO When a new Host is found RDP OSSH OTelnet If an existing Host in Passw Do Nothing O Set it to	eld with the Organizational Unit (OU) it belongs to: , set its Remote Connection Properties to : O VNC Port Number: 3389 wordstate is no longer found in any of the OUs specified, perform the following action for the Host record in Passwordstate: Unmanaged O Delete it, but only when there are no associated password records O Delete it and all associated password records
Privileged Account Crea	dentials
Please select which Privilege	d Account Credential will be used to execute this Discovery Job.
Update Active Directory Ac	count Passwords 🔹
	Save Cance

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.

Real Host Discovery Jobs

Below are all the Host Discovery jobs added to Passwordstate, for querying Active Directory for host records.

А	ctions	Job Name	Description
		Т	T
	٥	Import Server Hosts	Import Server Hosts
Ret	• • • •	Delete Run Discovery Job Now Toggle Status - Enabled or Disabled View Discovery Job History View Permissions	ns *

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 <u>Passwordstate_Remote_Session_Management_Manual.pdf</u>

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)