Passwordstate Enterprise Password Management

Passwordstate Security Administrators Manual

© 2025 Click Studios (SA) Pty Ltd

Table of Contents

2

	Foreword	0
Part I	Security Administrators Manual	5
Part II	Passwordstate Administration	5
1	Account and Host Discovery	. 7
2	Active Directory Domains	. 8
3	Auditing	21
4	Auditing Graphs	22
5	Authorized Web Servers	23
6	Backups	24
7	Bad Passwords	25
8	Browser Extension Settings	27
9	Brute Force Blocked IPs	30
10	Email Notification Groups	30
11	Email Templates	32
12	Emergency Access	35
13	Encryption Keys	37
14	Error Console	40
15	Export All Passwords	40
16	Feature Access	41
17	Host Types & Operating Systems	46
18	Images and Account Types	48
19	License Information	50
20	Password Folders	50
21	Password Generator Policies	53
22	Password Lists	59
23	Password List Templates	66
24	Password Strength Policies	69
25	Privileged Account Credentials	73
26	PowerShell Scripts	76
27	Remote Session Management	79
28	Reporting	80
29	Security Administrators	81
30	Security Groups	82
31	System Settings	89
	Account Discoveries	90
	Active Directory Options Tax	30

@ 2025 Click Studios (SA) Pty Ltd $% \mathcal{A}$

3

	Allowed IP Ranges Tab	
	API 180	
	Authentication Ontions Tab	95
	Duo Auth API Configuration	
	SAML2 Provider Examples	
	Branding Tab	
	Check for Updates Tab	127
	Email Alerts & Options Tab	
	Folder Options	
	High Availability Options Tab	
	Hosts Tab	
	Miscellaneous Tab	
	Password List Ontions Tab	136
	Password Options Tab	
	Password Reset Options	
	Email, Proxy & Syslog Servers Tab	
	Self Destruct Messages	
	Usage Tracking Tab	
	User Acceptance Policy Tab	
32	User Accounts	
33	User Account Policies	167
Part III	Remote Site Administration	169
1	Remote Site Locations	170
Part IV	Password Reset Portal Administration	172
Part IV	Password Reset Portal Administration	172
Part IV 1 2	Password Reset Portal Administration Active Directory Domains	172
Part IV 1 2 3	Password Reset Portal Administration Active Directory Domains Auditing	172 172 174 175
Part IV 1 2 3	Password Reset Portal Administration Active Directory Domains Auditing Auditing Graphs	172
Part IV 1 2 3 4	Password Reset Portal Administration Active Directory Domains Auditing Auditing Graphs Bad Passwords	172
Part IV 1 2 3 4 5	Password Reset Portal Administration Active Directory Domains. Auditing. Auditing Graphs. Bad Passwords. Password Policies.	172 172 174 174 175 175 175
Part IV 1 2 3 4 5 6	Password Reset Portal Administration Active Directory Domains. Auditing. Auditing Graphs. Bad Passwords. Password Policies. Privileged Account Credentials.	172 172 174 174 175 175 175 177 178
Part IV 1 2 3 4 5 6 7	Password Reset Portal Administration Active Directory Domains	172 172 174 174 175 175 177 177 178 180
Part IV 1 2 3 4 5 6 7 8	Password Reset Portal Administration Active Directory Domains. Auditing. Auditing Graphs. Bad Passwords. Password Policies. Privileged Account Credentials. Reporting. Security Groups.	172 172 174 174 175 175 175 177 178 180 182
Part IV 1 2 3 4 5 6 7 8 9	Password Reset Portal Administration Active Directory Domains. Auditing. Auditing Graphs. Bad Passwords. Password Policies. Privileged Account Credentials. Reporting. Security Groups. System Settings.	172 172 174 174 175 175 175 177 178 180 182 182
Part IV 1 2 3 4 5 6 7 8 9 10	Password Reset Portal Administration Active Directory Domains. Auditing. Auditing Graphs. Bad Passwords. Password Policies. Privileged Account Credentials. Reporting. Security Groups. System Settings. User Account Management.	172
Part IV 1 2 3 4 5 6 7 8 9 10 11	Password Reset Portal Administration Active Directory Domains. Auditing. Auditing Graphs. Bad Passwords. Password Policies. Privileged Account Credentials. Reporting. Security Groups. System Settings. User Account Management. Verification Policies.	172
Part IV 1 2 3 4 5 6 7 8 9 10 11	Password Reset Portal Administration Active Directory Domains. Auditing Auditing Graphs. Bad Passwords. Password Policies. Privileged Account Credentials. Reporting. Security Groups. System Settings. User Account Management. Verification Policies. Duo Authentication	172
Part IV 1 2 3 4 5 6 7 8 9 10 11	Password Reset Portal Administration Active Directory Domains. Auditing. Auditing Graphs. Bad Passwords. Password Policies. Privileged Account Credentials. Reporting. Security Groups. System Settings. User Account Management. Verification Policies. Duo Authentication Email Temporary PIN Code	172 172 174 175 175 175 177 178 180 182 182 182 182 182 189 192 195
Part IV 1 2 3 4 5 6 7 8 9 10 11	Password Reset Portal Administration Active Directory Domains. Auditing Auditing Graphs. Bad Passwords. Password Policies. Privileged Account Credentials. Reporting. Security Groups. System Settings. User Account Management. Verification Policies. Duo Authentication Email Temporary PIN Code Google Authenticator	172 172 174 175 175 175 177 178 180 182 182 182 182 182 182 189 192 195 196
Part IV 1 2 3 4 5 6 7 8 9 10 11	Password Reset Portal Administration Active Directory Domains	172 172 174 174 175 175 175 177 178 180 182 182 182 182 182 182 182 182 182 195 196 196
Part IV 1 2 3 4 5 6 7 8 9 10 11	Password Reset Portal Administration Active Directory Domains	172 172 174 174 175 175 175 177 178 180 182 182 182 182 182 182 189 192 195 196 196
Part IV 1 2 3 4 5 6 7 8 9 10 11	Password Reset Portal Administration Active Directory Domains. Auditing. Auditing Graphs. Bad Passwords. Password Policies. Privileged Account Credentials. Reporting. Security Groups. System Settings. User Account Management. Verification Policies. Duo Authentication Email Temporary PIN Code Google Authenticator One-Time Passwords (TOTP or HOTP) PIN Number Questions and Answers PADILIS Authontication	172 172 174 175 175 175 175 177 178 180 182 182 182 182 182 189 192 195 196 196 197 198
Part IV 1 2 3 4 5 6 7 8 9 10 11	Password Reset Portal Administration Active Directory Domains. Auditing Auditing Graphs. Bad Passwords Password Policies. Privileged Account Credentials. Reporting. Security Groups. System Settings. User Account Management. Verification Policies. Duo Authentication Email Temporary PIN Code Google Authenticator One-Time Passwords (TOTP or HOTP) PIN Number Questions and Answers RADIUS Authentication RSA Securit D Authentication	172 172 174 175 175 175 177 178 180 182 182 182 182 182 182 189 192 195 196 196 197 198 199 200 201
Part IV 1 2 3 4 5 6 7 8 9 10 11	Password Reset Portal Administration Active Directory Domains. Auditing Auditing Graphs. Bad Passwords Password Policies. Privileged Account Credentials. Reporting. Security Groups. System Settings. User Account Management. Verification Policies. Duo Authentication Email Temporary PIN Code Google Authenticator One-Time Passwords (TOTP or HOTP) PIN Number Questions and Answers RADIUS Authentication RSA SecurID Authentication	172 172 174 175 175 175 175 177 178 180 182 182 182 182 182 182 182 182

Part V KB Articles

1	Passwordstate Disaster Recovery	204
	Passwordstate Web Site Restore	
	Passwordstate Database Restore	205
	Rebuilding the Web.config File	213
	Resetting Password for Passwordstate_User SQL Account	
	Recovery Emergency Access Password	216
2	Controlling Settings for Multiple User Accounts	217
3	Encrypt Settings in Configuration Files	219
4	Export & Purging Auditing Data	220
5	Export All Passwords and Import into KeePass	223
6	Multiple Options for Hiding Passwords	224
7	Security Response Headers in Web.config Files	226

4

1 Security Administrators Manual



Welcome to the Passwordstate Security Administrators Manual.

This manual is organized into three key areas, relating to the back-end administration of Passwordstate:

- <u>Passwordstate Administration</u> Administration of the core of the product, relating to Privileged Account Management (PAM)
- <u>Remote Site Administration</u> Creating and monitoring the status of any Remote Site Agent deployments
- <u>Password Reset Portal Administration</u> Administration for the Password Reset Portal, for users to reset or unlock their own Active Directory accounts (A Self Service Password Reset Portal)
- KB Articles Various article for system administration of Passwordstate

2 Passwordstate Administration

The Passwordstate Administration area is where you configure user accounts, system wide settings, and various other features for the core functionality of the software.

The following table describes each of the different sections available within the Passwordstate Administration area.

Active Directory Domains	Specify which Active Directory Domains can be queried from within Passwordstate, either for User Accounts or Security Groups
Auditing	Provides the ability to query all auditing data within the system, with multiple filtering options, and the ability to export data as well if required
Auditing Graphs	Simply a graphical representation of all the auditing data, with similar filtering features
Authorized Web Servers	Authorized Web Servers is used to specify which web server host names are authorized to run the Passwordstate web site - used as a mechanism to prevent theft of the database an hosting in a different environment
<u>Backups</u>	Allows you to specify settings and a schedule for perform backups of all web files and the database.
Bad Passwords	A list of password values which are deemed to be 'bad' and can educate your users not to use these values

Browser Extension Settings	Allows you to specify various settings for how the Browser Extension feature is used
Brute Force Blocked IPs	A list of IP Addresses which have been blocked due to brute force login detection
Email Notification Groups	Can be used to manage email notification settings for a group of individual users accounts, or members of security groups
Email Templates	Allows you to customize the emails sent from Passwordstate, or to enable/disable notifications
Emergency Access	A separate 'Security Administrator' role login which can be used in the event other accounts are locked out, or inaccessible for any reason
Encryption Keys	This menu allows you to export your encryption keys to a password protected zip file, and also to perform key rotation of your encryption keys
<u>Error Console</u>	Any errors experienced within Passwordstate will be logged on this screen, which can be reported to Click Studios for troubleshooting purposes
Export All Passwords	Allows you to export all Password records from the system to a CSV file
Feature Access	Feature Access allows you to grant or deny access to various Features and Menus, for either User's Accounts or Security Groups.
Host Types & Operating Systems	Allows you to add additional Host Type and Operating System records which can be associated with Host records in Passwordstate
Images and Account Types	Custom Images are used in two locations in Passwordstate - icons for the Password List themselves, and also for the 'Account Type' field for Password records
License Information	Allows you to enter your license keys for Passwordstate - either Client Access Licenses, Annual Support or High Availability
Password Folders	Shows all Password Folders created in Passwordstate
Password Generator Policies	Create, edit or delete Password Generator Policies. Policies can be associated with one or more Password Lists, and are used as a basis for generating random passwords - of varying complexity
Password Lists	Shows all the Shared Password Lists in Passwordstate, and provides various features for administering permissions, moving passwords around, or importing passwords in bulk
Password List Templates	Shows all the Password List Templates stored in Passwordstate, which can be used to apply a common set of settings to one or more Password Lists
Password Strength Policies	Password Strength Policies are used as a set of rules for determining the strength of a Password. Once a policy is created, it can be applied to one or more Password Lists
Privileged Account Credentials	Various features in Passwordstate require Active Directory Accounts to perform certain tasks i.e. Resetting Passwords,

7

	querying active directory, etc. This screen allows you to add those accounts to be used
PowerShell Scripts	Each of the various default PowerShell scripts for Account Discovery, Password Resets and Account Heartbeat are available on this screen.
<u>Remote Session Management</u>	Manage permissions and settings for Remote Session Credentials, play back recorded remote sessions, and make changes to the Gateway for the browser based version of the Remote Session Launcher
<u>Reporting</u>	Various reports which can be exported to CSV files
Security Administrators	Allows you to specify which users are 'Security Administrators' within Passwordstate, and select which roles they can have.
Security Groups	Allows you to manage either local security groups created within Passwordstate, or Active Directory security groups. These groups can then be used for applying permissions to Password Lists, or to give/deny access to various features
<u>System Settings</u>	System Settings is used to manage the majority of system wide settings for Passwordstate
<u>User Accounts</u>	Allows you to specify the user accounts which are able to access the Passwordstate web site
User Account Policies	User Account Policies are used to apply a specify set of settings, to any number of user accounts or security group members

2.1 Account and Host Discovery

The Account and Host Discovery screen allows Security Administrators to access all Account and Host Discovery Jobs added to Passwordstate. This may be required if permissions are accidentally removed from a Discovery Job.

From this screen you can:

- Edit details for any Discovery Job
- Delete jobs
- Run the Discovery Job now
- Enable or disable a Discovery Job
- And manage permissions for jobs

selow are all	the Account and Host Discovery jobs added	d to Passwordstate.								
Actions	Job Name	Description	Job Type	SiteL ocation	Run Discovery At	Schedule Type	In Progress	Last Discovery Took	Simulation Mode	Enabled
	T	T	T	т	Т	Т	T	Т	T	T
0	All Local Admins On Servers	All Local Admins On Servers	Windows Local Admin Accounts	Internal	11:00 PM	Weekly - Sunday				×
0	Import Server 2016 Hosts	Import Server 2016 Hosts	Hosts	Halox	10:16 AM	Daily		00:00:01		×
0	Import Servers from Sanddomain	Import Servers from Sanddomain	Hosts	Sanddomain	11:39 AM	Daily		00:00:01	×	×
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		×
GI O De GI RU ST TO VIII	Hete In Discovery Job Now ggle Status - Enabled or Disabled ew Permissions									

2.2 Active Directory Domains

The Active Directory Domains screen is used primarily for two purposes:

- Adding domains which will be used to authenticate to access the Passwordstate web site
- Adding domains which will be used to perform password resets for accounts on those domains

A few things to note about Active Directory Domains:

- If you are wanting to authenticate where non-trusted domains are being used, then you need to ensure Anonymous Authentication for the site in enabled in Internet Information Services (IIS)
- You must specify a domain account which has Read access to the domain, and this account can be setup on the <u>Privileged Account Credentials</u> screen. By default it is recommended this account is a member of the 'Account Operators' security group, but higher privileges may also be required if your System Administrators have applied permission restrictions to accounts or OUs.
- The 'Used for Authentication' option is for Authentication screens in Passwordstate, as you see from the second screenshot below. if you do not want a domain to show in this dropdown list for authentication, the deselect this option
- You can also use LDAPS (LDAP over SSL) for connectivity as well if required. When using LDAPS, if you are wanting to communicate to non-trusted domains, please see the section below title 'LDAPS and Non-Trusted Domains'. Please note that LDAP communicates over Port 389 (UDP), and LDAPS over 636 (TCP) these ports must be open to your domain controllers.
- You can also choose to use Kerberos when authenticating to Active Directory, which requires ports 88 and 464 UDP/TCP to be open to your domain controllers
- Please note all authentication options require UDP Port 389 to be open, in order to find the nearest domain controller

Note: If you are unsure of what NetBIOS Name and LDAP Query String settings to specify, please speak with your Active Directory Administrators for assistance.

🚓 Active	Directory Domair	ıs					
To grant acce	ess to Passwordstate by	either adding users man	ually, or via Active Directory lo	okup, you need to specif	y one or more Active Directory Domain	ns.	
If you are un	sure of what your Active	Directory settings shoul	d be, please use the following	as a guide:			
The N FQDN The L	letBIOS Name for your A I should match the resul DAP Query String for yo	t of set userdnsdomain ur Active Directory setting	hould match the result of set gs should match the result of a	userdomain set userdnsdomain. e.g. Site Location	dc=clickstudios,dc=com,dc=au for the	e domain clickstudios.com.au Used For Authentication	Default Domain
, and the	T	T	T	T	T	T	T
0				Internal		✓	~
0	sanddomain	sanddomain.com	dc=sanddomain,dc=com	SandDomain	sanddomain\svc_passwordstate	✓	×
Add G	rid Layout Actions 🔻						

8

9



LDAPS and Non-Trusted Domains

If you also want Passwordstate to communicate to non-trusted domains with LDAPS, i.e. other domains your web server is not a member of, then you will need to export the CA certificate from these domains, and import them onto your Passwordstate web server. If you have Passwordstate installed on a server in a Workgroup environment, then this is also needed for all domains you wish to communicate with. Below are some instructions for how this can be done:

Export the Domain CA Certificate

- On your server that has the CA installed, Click Start > Control Panel -> System and Security -> Administrative Tools > Certificate Authority to open the CA Microsoft Management Console (MMC) GUI
- Right-click the CA server and select Properties

🚋 certsrv - [Certification Authority	(Local)]		_	×
File Action View Help				
(⇔ ⇔) 🔒 🛛 🖓 🕨 🔳				
Certification Authority (Local)	Name	Description		
	All Tasks > K16AD-C	A Certification Authority		
	Refresh			
*	Properties			
	Help			
Opens the properties dialog box for t	he current selection.			

• From the General Menu, click View Certificate

ollment Agents	Storage		Certificate M	lanager	8
and the state of t	Auditina	Recover	v Agents	Sec	- uritv
General	Policy Mod	dule	Exit	Module	
ertification authority (CA)				
ame:	Fabrikam-WIN	2K16AD-C/	A		
A certificates:					
ertificate #0					
		\searrow			
			View Ce	ertificate	;
			View Ce	ertificate	;
yptographic settings			View Ce	ertificate	;
yptographic settings ovider:	Microsoft Softv	ware Key St	View Ce orage Provid	ertificate der	;
yptographic settings ovider: ash algorithm:	Microsoft Softv SHA256	ware Key St	View Ce orage Provid	ertificate Jer	•
yptographic settings ovider: ash algorithm:	Microsoft Softv SHA256	ware Key St	View Ce orage Provid	ertificate der	;
yptographic settings ovider: ash algorithm:	Microsoft Softv SHA256	ware Key St	View Ce orage Provid	ertificate der	2
yptographic settings ovider: ash algorithm:	Microsoft Softv SHA256	ware Key St	View Ce orage Provid	ertificate der	;
yptographic settings ovider: ash algorithm:	Microsoft Softv SHA256	ware Key St	View Ce orage Provid	ertificate Jer	*
yptographic settings	Microsoft Soft	vare Key St	View Ce	ertificate	

• On the Details tab, click Copy to File



• Click Next

🔶 😺 Certificate Export Wizard	×
Welcome to the Certificate Export Wizard	
This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.	
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.	
To continue, click Next.	
Next Cancel	

• Choose Base-64 encoded X.509(.CER) and click Next

Ex	port File Format Certificates can be exported in a variety of file formats	
	certificates can be exported in a variety of the formats.	
	Select the format you want to use:	
	O DER encoded binary X.509 (.CER)	
	Base-64 encoded X.509 (.CER)	
	Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)	
	 Personal Information Exchange - PKCS #12 (.PFX) Include all certificates in the certification path if possible 	
	Delete the private key if the export is successful	
	Export all extended properties	
	Enable certificate privacy	
	 Microsoft Serialized Certificate Store (.SST) 	

• Save the certificate to your desktop, or somewhere local and click Next

		\times
← 🍠	Certificate Export Wizard	
F	ile to Export Specify the name of the file you want to export	
	rile name: C:\Users\sand\Desktop\DomainCertificate.cer	
	Next Cance	el l

• Click Finish



• Copy the certificate to your Passwordstate web server and close all windows.

Importing the Certificate into your Passwordstate web server

- On your Passwordstate web server, open Certificate Manager for Local computer by typing certIm.msc into your Run command bar
- Expand Trusted Root Certificate Authorities -> Certificates
- Right Click Certificates and select All Tasks -> Import

🖀 certIm - [Certificates - Local Computer\Trusted Root Certification Authoriti 🗕 🗖 🗙							
File Action View Help							
🗢 🔿 🙍 🗊 📋 🙆 🛃 👔							
🗊 Certificates - Local Computer	Issued To	Issued By	<u> </u>				
Personal	🔄 AddTrust External CA Root	AddTrust External CA Root					
Trusted Root Certification Au	🛱 alien	allen					
	Root	Baltimore CyberTrust Root	≡				
▶ Ent All Tasks	Certificat	Class 3 Public Primary Certificatio					
View	Copyright (c) 1997 Microsoft C	Copyright (c) 1997 Microsoft Corp.					
Refresh	DigiCert Assured ID Root CA	DigiCert Assured ID Root CA					
N Thi Export List	DigiCert Global Root CA	DigiCert Global Root CA					
	DigiCert High Assurance EV Ro	DigiCert High Assurance EV Root					
help	DST Root CA X3	DST Root CA X3					
Remote Desktop	Entrust Root Certification Auth	Entrust Root Certification Authority					
Certificate Enrollment Reques	Equifax Secure Certificate Auth	Equifax Secure Certificate Authority					
Smart Card Trusted Roots	GeoTrust Global CA	GeoTrust Global CA					
Trusted Devices	GeoTrust Primary Certification	GeoTrust Primary Certification Au					
Web Hosting	GlobalSign	GlobalSign					
GlobalSign Root CA GlobalSign Root CA							
< III >	Control Class 2 Certification	Go Daddy Class 2 Certification Au					
Contains actions that can be performed on the item.							

• Click Next

🍥 🍠 Certificate Import Wizard	X
Welcome to the Certificate	Import Wizard
This wizard helps you copy certificates, ce lists from your disk to a certificate store.	rtificate trust lists, and certificate revocation
A certificate, which is issued by a certificat and contains information used to protect o connections. A certificate store is the syst	tion authority, is a confirmation of your identity lata or to establish secure network em area where certificates are kept.
Store Location	
 Current User Local Machine 	
To continue, click Next.	
	Next Cancel

• Browse to the certificate and click Next

×
📀 🍠 Certificate Import Wizard
File to Import Specify the file you want to import.
File name: C:\Users\sand\Desktop\DomainCertificate.cer Browse
Note: More than one certificate can be stored in a single file in the following formats: Personal Information Exchange- PKCS #12 (.PFX,.P12)
Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)
Microsoft Serialized Certificate Store (.SST)
Next Cancel

• Click Next

	×
🗧 🛃 Certificate Import Wizard	
Certificate Store	
Certificate stores are system areas where certificates are kept.	
Windows can automatically select a certificate store, or you can specify a location the certificate.	for
Automatically select the certificate store based on the type of certificate	
Place all certificates in the following store	
Certificate store:	
Trusted Root Certification Authorities Browse	
Next	Cancel

• Click Finish and then OK

) Ertificate Import Wizard	×					
Completing the Certif	icate Import Wizard					
The certificate will be imported afte	er you dick Finish.					
You have specified the following se	ettings:					
Certificate Store Selected by Use	r Trusted Root Certification Authorities					
Content	Certificate					
File Name	C: \Users \sand \Desktop \DomainCertificate.cer					
L						
	Finish Cancel					

• This ends the import process, and your domains should now be able to securely communicate using LDAP over SSL

2.3 Auditing

The Auditing screen allows you do report/filter on all auditing data within Passwordstate. Filtering can be done by:

- Platform events generated through the web site, the Mobile App, the API, Windows Service or Browser Extension
- Password List filter on events specific to a selected Password List

- Activity Type not all audit events relate to passwords i.e. there's audit events for sending emails, failed authentication attempts, etc. To see a complete list of 'Activity Types' ensure the 'Password List' drop-down list has 'All Password Lists' selected
- Beginning and end date by default, date filtering is not enabled
- There are also some rules which can be configured for moving Auditing data to the Auditing Archive table, and the purpose of this is to help with performance of the UI. This setting can be found on the screen <u>Auditing Data</u>

In addition to reporting on auditing data on the screen, you can export the data for further analysis to a CSV file if required.

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

🖬 Auditing									
To search for relevant audit reco	rds, please use the opti	ons below.							
Auditing Filters									
Platform: All Web	Mobile 🔍 API 🔍 W	indows Service 🔘 Bro	owser Extension	Instance: Bo	oth 🔍 Primary 🔍 HA (Pas	sive Node) 🛛 🖌	Archived Data: No	• Ves	
Max Records Password L	st	Activit	у Туре	S	Site Location Activity	Begin Date	End Date		
5000 D All Passwor	d Lists	▼ All Ac	tivities	•	All Site Locations 🔻		24/08/2018	Search Search	
Date	Platform	UserID	First Name	Surname	IP Address	HA Instance	Activity	Tree Path	Des
1 T	Ť	T	Ť		T		T	T	
24/08/2018 10:26:13 AM	Windows Service	WindowsService	Windows Service	Account	10.0.0.9		Email Sent		An e

2.4 Auditing Graphs

The Auditing Graphs screen is simply a graphical representation of the auditing data, with similar filtering options. Instead of filtering between dates, you just select a specified period i.e. 1 year, 2 years, etc.

✓ Auditing Graphs

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



2.5 Authorized Web Servers

The Authorized Web Servers screen is where you can specify the host names of the web servers which are authorized to host the Passwordstate web site, or Passwordstate App Server.

The intention of this feature is to prevent the theft of a copy of the database, and hosting it and the web site in an untrusted environment.

Note 1: If you plan on moving your Passwordstate web installation to a new web server, you must first register the host name of the new web server on this screen

Note 2: If you also purchased the High Availability module, you must register the host name of your High Availability instance web server, and select the appropriate role for the HA server i.e. either Passive or Active

Note 3: The host names are not case sensitive

Functional Roles

In addition to specifying the server role, you can also specify what "functional roles" are allowed to be used.

Add New Authorized Web Server

To add a new Authorized Web Server, please fill in the details below and click Save.

Web Server Host Name: *		
Server Role: *	Primary Server	-
High Availability Mode: *	Active (Read/Write to Database)	Ŧ
Functional Roles: *	Standard API	
	✓ Windows Integrated API	
	Mobile App	
	Browser Extensions	
	Remote Site Locations Agent	
	Password Reset Portal	
	Self Destruct Messages	
The Mobile App functio	nal role is only relevant to the Passwords	tate A

Keep Alive Monitoring Functionality

If you wish to use monitoring software to determine the availability of your Passwordstate web site and database, you can make calls to the URL of https://<YourURL>/keepalive or https://<YourURL>/keepalive/default.aspx

A HTTP 200 Response will be returned if both the web and database tier are available.

2.6 Backups

The Backups screen allows you to specify the settings required to perform automatic backups, as well execute manual backups and view the status of any backups.

The following instructions will provide some guidance for configuring the backup settings, and other permissions required to backup all the web tier and database files.

Overview

Passwordstate is a physically installed application that communicates to, and stores all or your data in a Microsoft SQL Database. In the event of a disaster, you may need to restore your database and Passwordstate installation files, which will require you to have them backed up.

Passwordstate has a built-in automatic backup feature which can be configured to suit your requirements. For example, you may already have another solution for your Microsoft SQL database backups, so you can set Passwordstate to not backup up your database, but maybe just the install files.

Not only is the Microsoft SQL database critical to have a backup of, but there are also encryption keys which are located in your web.config file. These too are also critical to have a copy of in the event of a disaster, so setting up the Passwordstate automated Backup feature will ensure you have everything you need to restore your environment, in the event of a disaster.

Backup Instructions

We have two manuals to choose from to configure your backups screen. The first manual is if you intend on using a domain account with a network share. The second should be followed if you wish to use a Local Windows account with a literal path to a folder on your Passwordstate web server. Domain accounts are most commonly used for performing backups.

Automatic Backups using **Domain** account and **Network Share**: <u>https://www.clickstudios.com.au/downloads/version9/Passwordstate_Automatic_Backups_Dom</u> <u>ain_Account.pdf</u>

Automatic Backups using a **Local Windows** account and **Static Folder** path: <u>https://www.clickstudios.com.au/downloads/version9/Passwordstate_Automatic_Backups_local_Account.pdf</u>

Remote Session Recordings and Backups

If you are using the Browser Based version of the Remote Session Launcher with Session Recordings, Session Recordings will not be included in the standard Passwordstate backup functionality, due to the potential size of the files. If you have left the recording folder in the default path, then you need to organize your own backups of these files if required.

2.7 Bad Passwords

On the Bad Passwords screen, there are three options available to prevent users from using certain passwords which are deemed to be 'Bad'.

You can either user the built in Custom Bad Passwords database, or you can use the online 'Have I been Pwned' database from this site - <u>https://haveibeenpwned.com/</u>, or you can use both. 'Have I been Pwned' is a list of known password from various security breaches across the globe. If using this feature, your web server hosting the Passwordstate Reset Portal must be able to make calls to the internet.

Note 1: If you use the 'Have I been Pwned' database, this is only available on the Add and Edit Passwords screens. The Passwordstate API, scheduled resets, and importing in bulk, will instead use the Custom Bad Passwords database

Note 2: If you use the 'Have I been Pwned' database, your Passwordstate web server must have access to the internet to query this API online, and it can slow down performance of saving records on the Add/Edit screens, as it first needs to reach out to the Internet to perform the check
 Note 3: The 'Have I been Pwned' integration is both client and server based, depending on the feature used i.e. reports execute from the server, and UI buttons for checking are client based. This means access to the 'Have I been Pwned' API must be allowed from the Passwordstate web server, and from user's desktops

There are options on the screen Administration -> <u>System Settings</u> -> <u>Miscellaneous Tab</u>, and <u>Password Options Tab</u> for notifying your users when bad passwords are detected.

If required, you can also import multiple 'Bad Passwords' for the Custom Bad Passwords database, via the use of a csv file.

🛛 Bad Pa	Bad Passwords					
Please select	which type of Bad Passwords database yed would like to use to prevent users from using specific passwords.					
Bad Pass	swords Database					
Note 1: The Note 2: Som	'Have I Been Pwned API' database is only used on the Add and Edit Password screens. The Passwordstate API, scheduled resets, and importing in bulk, will instead use the custom database below. se of the default Bad Passwords in the Custom database below may be of an offensive nature, but have proven to be the most common passwords used. These can be deleted if required.					
Actions	Password					
	T					
0	1111					
0	112233					
0	1212					
0	121212					
0	123123					
0	1234					
0	123456					
0	12345678					
0	1313					
0	131313					
н	 (1) 2 3 4 5 6 7 8 9 10 () (H) 					
Add Ir	nport Export Grid Layout Actions *					

2.8 Browser Extension Settings

The Browser Extension Settings area allows you to specify various settings, for all users, for how the Browser Extension feature is used. In Particular:

- Browser Extension Settings various settings for session timeout, logging out of the extension, form-filling behaviour, etc. Please see examples of how Session Timeouts work below the screenshot below.
- Ignored URLs if you don't want users to save login credentials for certain web sites, you can add them as 'Ignored URLs' this will also prevent automatic form-filling, and the icon overlay on fields
- Allowed to Use the Extension IF you don't want to allow certain users, or members of a security group, to use the Browser Extension feature, then you can specify them on this tab
- Prevent Users From Saving Logins if you only want certain users to use the Browser Extension to form-fill web site logins, and not allow them to save any new records, you can do so on this tab

Browser Extension Settings

Use each of the appropriate Tabs below to indicate various Settings, which URLs are ignored by the Browser Extension, which users are allowed to use the Extension, or which users are not allowed to save new logins.

browser extension settings	ignored urls	allowed to use the extension	prevent users from saving logins				
Browser Extension Set	tings						
Please specify general settings	Please specify general settings below for the behavior of the Browser Extension.						
Browser Extension Session Timeout: When the browser extension session expires, the user will be required to login to Passwordstate, and into the browser extension using their Master Password.							
Session expiry is based on sliding tokens and the setting below, and sessions will only expire after the browser is closed (i.e. the extension isn't interacting with the Passwordstate API).							
F If the session is still active,	restarting the brow	ser will only require users to unlo	ck the extension using their Master Password.				
1 Hour							
Auto Unlock Browser Extens	ion upon Browser	Startup:					
Note: Organizations should co setting this option to 'Yes'. By device. If using this option and controls.	Note: Organizations should consider their usage / operational requirements and perform an internal risk assessment prior to setting this option to 'Yes'. By selecting 'Yes' the users browser extension encryption key will be stored within the browser on their device. If using this option an organization needs to consider how devices are protected and any applicable compensating controls.						
Setting this option to 'Yes' wou is still active.	ıld result in users n	ot needing to enter their Master	Password into the extension, when their session				
If you need your browser ext please specify it here: (in the communicating with, otherwis	ensions to comm format of https://n e encryption/decry	unicate to a different URL comp nypasswordstate.com). This must ption will not work with different	pared to your main Passwordstate URL, also be the same database you're encryption keys.				
		Sa	ve				
Various menus in the Browser Extension navigate users back to your Passwordstate Web Site. Please select below which URL you would like to use for this purpose: O Alternative URL Specified Above Base URL Specified on the System Settings page							
Enable Form-Filling of OTP c	Enable Form-Filling of OTP codes:						
	U YES ♥ NO						
Prevent Password Lists with "Additional Authentication" option set from being used with the Browser Extensions: (if set to No, there is no Additional Authentication functionality within the browser extensions)							
♥Yes ♥No							
Select the Password Strength Policy the user's Master Password for Authentication must adhere to (It is strongly recommended you select a policy which enforces complex passwords, with the Mandatory Compliance option checked):							
Default Policy							

Browser Extension Settings

There are multiple settings which can be selected, to change the behaviour of how authenticated sessions in browser extensions operate.

To start using the Browser Extensions, users must login to Passwordstate, create a Master Password on the screen Preferences -> Browser Extension, and then they can login to the extension using this Master Password.

Browser Extension Session Timeout

Session Timeout is based on sliding authentication tokens, and how long the users browser has been closed for. By default, if the user leaves their browser open throughout the day, then the extensions will not "lock", requiring their Master Password to unlock them.

If their browser has been closed longer that the Session Timeout setting, then the users will need to log both into Passwordstate, and then the browser extension with their Master Password, in order to use the extensions again. Below are a few examples of how the session timeout setting could work:

- Timeout set to 1 hour, and browser closed for 30 minutes. User re-opens their browser, and only needs to enter their Master Password to "unlock" the extension
- Timeout set to 1 hour, and browser closed for 2 hours. User re-opens their browser, and will need to log both into Passwordstate, and then the browser extension with their Master Password
- Timeout set to 4 hours, and user closes browser at 5pm at the end of the work day. The following morning at 8am, the user re-opens their browser, and will need to log both into Passwordstate, and then the browser extension with their Master Password
- Timeout set to 18 hours, and user closes browser at 5pm at the end of the work day. The following morning at 8am, the user re-opens their browser, and only needs to enter their Master Password to "unlock" the extension
- Timeout set to 3 days, and user closes browser at 5pm, on a Friday, at the end of the work day. The following Monday morning at 8am, the user re-opens their browser, and only needs to enter their Master Password to "unlock" the extension

These timings above are based on the last time authentication tokens were refreshed, which can be at different intervals when the browser is open, based on browser activity.

Auto Unlock Browser Extension upon Browser Startup

Note: Organizations should consider their usage / operational requirements and perform an internal risk assessment prior to setting this option to 'Yes'. By selecting 'Yes' the users browser extension encryption key will be stored within the browser on their device. If using this option an organization needs to consider how devices are protected and any applicable compensating controls.

With this option set to Yes, any time the user opens their browser and would normally be required to enter their Master Password to "unlock" then extension, then the Master Password would not be required - it would simply automatically unlock.

In the examples given above for Session Timeout, if the user is required to log both into Passwordstate, and the browser extension, then this option will not change that behaviour.

Clearing Browser Extension Access Tokens

There are two ways to clear Access Tokens used for Browser Extensions.

On this screen you can clear all tokens for all user accounts. Or, if you only want to clear an access token for a single user, you can do this from the screen Administration -> User Accounts, and then from the appropriate 'Actions' menu for the user.

Clearing tokens would result in users browser extension automatically logging out, next time the browser extension tries to communicate with the Passwordstate API - which would happen by simply browsing different web sites, or on the default 1 hour automatic synchronization process.

2.9 Brute Force Blocked IPs

The core Passwordstate product, Passwordstate App server for mobile apps, and Password Reset Portal module, each have brute force login detection.

If the number of specified failed logins are reached, the authenticating user will be permanently blocked from the relevant module, until their IP Address is removed from this screen.

💼 Brute	e Force Blocked IPs	
Listed belo	ow are all the IP Addresses, and	respective platforms, where users were blocked access due to too many failed login attempts
Actions	Blocked Date	IP Address
	T	T
No record	s to display.	
Grid Layo	ut Actions 👻	

2.10 Email Notification Groups

The Email Notification Groups screen is used to manage email notification settings for a group of individual users accounts, or members of security groups.

Using Email Notification Groups, you can specify which email notifications certain users receive, or don't receive i.e. you may wish to have certain notifications enabled for Security Administrators, but disabled for 'normal' user accounts in Passwordstate.

Note 1: Any system wide <u>Email Templates</u> which are disabled will cause any settings here to be ignored

Note 2: If a user has specified their own Email Notification Settings as part of their Preferences, any permissions you apply here for the user will override their personal settings

Note 3: If you have more than one Notification Group created for a user, any disabled email categories will over-ride any enabled ones (be careful applying duplicates for a user)

Email Notification Groups

Email Notification Groups can be used to enable or disable real-time email notifications for multiple users at once.

Note 1: Any system wide 'Email Templates' which are disabled will cause any settings here to be ignored. **Note 2:** If a user has specified their own Email Notification Settings as part of their Preferences, any permissions you apply here for the user will override their personal settings.

Note 3: If you have more than one Notification Group created for a user, any disabled email categories will over-ride any enabled ones (be careful applying duplicates for a user).

	Actions	Notification Group	Description	
	No Access Requests		No Access Requests	
Add Grid Layout Actions 👻				

Once you have created a Notification Group, you can then assign permissions for who is affected by the settings, and which emails are either enabled or disabled. You do this by clicking on the appropriate menu item in the 'Actions' drop-down menu.



Email Notifications

Please select which Email Notifications you would like set for the notification group 'No Access Requests' by selecting the appropriate option from the 'Actions' drop-down menus below.

Actions	Category	Description	Enabled	
0	Access Request	Notifies the user if their request to access a Password or Password List has been denied	*	
0	Access Request Denied	Notifies the user if their request to access a Password or Password List has be denied	A. 1	
0	Access to Password Changed	Notifies user if their access level to an individual Password record has changed	1 de 1	
0	Access to Password Granted	Notifies user if they have been granted access to an individual Password record	1	
0	Access to Password List Changed	Notifies user if their access level to a Password List has changed		
0	Access to Password List Granted	Notifies user if they have been granted access to a Password List	1	
0	Access to Password List Removed	Notifies user if their access to a Password List has been removed	1	
0	Access to Password List Template Changed	Notifies user if their access level to a Password List Template has changed		
0	Access to Password List Template Granted	Notifies user if they have been granted access to a Password List Template	1	
0	Access to Password List Template Removed	Notifies user if their access to a Password List Template has been removed		
Image: Image:<				
Return to Notification Groups Enable All Notifications Disable All Notifications Grid Layout Actions 🔻				

2.11 Email Templates

The Email Templates screen allows you to customize the emails sent from Passwordstate, or to enable/disable notifications as required.

Enabling/Disabling Email Notifications

You can enable/disable email notifications in one of either two ways:

1. Individually by the appropriate 'Actions' drop-down menu

Actions	Category	Description
0	Access Request	Notifies the use
0	Access Request Denied	Notifies the use
Toggle status - Enabled or Disabled Not Restore Default Template Not		Notifies user if t
		Notifies user if t
0	Access to Password List Changed	Notifies user if t

2. Enabling/disabling all email notifications at once by clicking on the appropriate 'Enable All' or 'Disable All' buttons at the bottom of the grid

U	Access to Password List Template Granted	Notifies user if they have been granted a
0	Access to Password List Template Removed	Notifies user if their access to a Password
Η	 1 2 3 4 5 → N 	Page: 1 of 5 Go
Enable All I	Email Templates Disable All Email Temp	olates Grid Layout Actions 🔻

Editing Email Template Content

By clicking on the 'Category' hyperlink in the grid, you can edit the content of the email template - specifying your own words, and formatting options.

At the top right-hand side of the Editor you will notice the 'Variables' tab/ribbon bar. From this drop-down list, you can insert the following variables into your email templates:

- ToFirstName the First Name of the user who is receiving the email
- ToUserID the UserID of the user who is receiving the email
- SiteURL the URL of your Passwordstate web site
- PermissionType the permission being applied to a Password List or Password record for the user
- PasswordList the name of the Password List
- Password the title of the Password record
- Version the Version number of your Passwordstate install
- UserName A combination of the Firstname and Username of the user
- ExpiresAt the date at which a users permissions to a Password List or Password will be removed
- AdditionalBodyText reserved by Click Studios for various custom text messages
- AuthenticationMethod which Authentication method was used for authenticated to the Passwordstate web site, or to a Password List

Note: In addition to the emails being sent to the relevant intended users, you can also send each email category to a different email address as well, as per the highlighted textbox in the screenshot below. This is useful if you want to send specific email types to a shared mailbox, or SMS alerting service.

Edit Email Template

To edit the selected Email Template, please fill in the details below.

ubject : *					
Inc. Court Encoder To	ubject : * Passwordstate - Password Updated				
Also Send Emails To :					
	Emails can	also be sent to generi	ic email addresses	by specify	ing them here, separated by semicolons,
				- , - , - , - , - , - , - , - , - , - ,	
Home					
verdana, "san 🗸 🖪	I <u>U</u> A•	日 結 師 師 师	Apply CSS CI	5-	Insert Variable 👻
13рх - аве	_{ε χ² Χ₂ (λ) -}	≣ ≣ ≣ ⊠	Normal -	C'-	
Aa aA 🛛 🔊	f-			23	
Font		Paragraph	Styles	Editing	Variables
[SiteURL]					
🥕 Design 🛛 🔍 Pre	eview				

If while editing the contents or formatting of an Email Template you decide you don't like the changes you've made, you can restore back to the original content as supplied by Click Studios by selecting 'Restore Default Template' from the appropriate Actions drop-down menu.

Actions	Category	Description
0	Access Request	Notifies the user if their req
•	Access Request Denied	Notifies the user if their req
Toggle status - Enabled or Disabled		Notifies user if their access
C Re	estore Default Template	Notifies user if they have be
0	Access to Password List Changed	Notifies user if their access
0	Access to Password List Granted	Notifies user if they have be

Testing and Troubleshooting Emails being Sent

When editing a Password List template, there is a button called 'Test Email'. This button will test sending the email template to your own email account. This testing is different however to how emails are normally sent from Passwordstate - normally records are added to the database, and the Passwordstate Windows Service checks and send emails every minute. This 'Test Email' button sends directly from the web site, and does not use the Passwordstate Windows Service.

If emails are queuing up and not being sent as expected, the following suggestions may help to troubleshoot why:

- Check you have correctly specified your email server's settings on the screen Administration -> <u>System Settings</u> -> <u>Email Alerts & Options Tab</u>
- 2. Ensure the Passwordstate Windows Service is started
- 3. Check the event log on your web server to see if any errors are being reported as to why emails aren't being sent look for the Source of 'Passwordstate Service'
- Check there aren't any Email Templates disabled, either on the screen <u>Email Templates</u>, or <u>Email Notification Groups</u>, or possibly the user has disabled an email notification in their Preferences area

2.12 Emergency Access

The Emergency Access screen allows you to specify a password for a separate 'Security Administrator' role login which can be used in the event other accounts are locked out, or inaccessible for any reason.

A couple of scenarios where this would be applicable is:

- You have issues with authenticating on your domain, and can no longer authenticate to Passwordstate using your normal domain account
- Someone has accidentally deleted or disabled all Security Administrator accounts, and no-one is able to administer all the settings for Passwordstate

The Emergency Access URL is HTTPS://<Your Passwordstate URL>/Emergency

Note 1: Simply browsing to the Emergency Access URL will generate audit records, and notify Security Administrators via email

Note 2: You must specify a reason why you need to access the Emergency Access Login, and this reason is added to the auditing data

Note 3: Once you've logged in with this account, you will have access to the Administration area of Passwordstate

Note 4: An option is also provided to enable Two-Factor Authentication for the Emergency Access login account as well - see screenshot 2 below.

	Passwordstate Emergency Access Authentication	
Login		
To login with the Emergency Access account, please specify the password and reason for access below.		
Accessing this page, plus any authentication attempts, are both audited events which also cause email alerts.		
Password :		
Reason :	Logon	
	Status: Awaiting Logon	
Emergency Access

The 'Emergency Access' account is only used to gain Administrative Access to Passwordstate in the event all other user accounts are unable to log in.

The intention is for you to click on the 'Print Emergency Access Details' button, print and securely store the page which is presented to you.

Please Note: The following events will generate an audit event as well as sending all Security Administrators an email:

1. Simply browsing to the Emergency Access Login page 2. Successful or failed login attempts

Please specify a password for the Emergency Access account.	
Paceword *	
Confirm Password *	
2FA with Google Authenticator	
In order to use two-factor authentication with Google Authenticator and your mobile/cell device, you will need do:	
2. Scan the barcode into Google Authenticator op your mobile device, or manually type in the displayed	
Secret Key	
s. click on the save button.	
Secret Key: FMU22Q57WGL7SQSG New Clear	
(not case-sensitive)	
「「「「「「「」」」を発見ていた。	
Print Emergency Access Details Save	

2.13 Encryption Keys

From the Encryption Keys screen, you can do the following:

- Set the reminder period for how often you should be generating new encryption keys, and reencrypting all data in the database. User's who have access to this Encryption Keys screen, will receive a notification in the Notification centre
- Export your Encryption Keys to a password protected zip file
- Generate new encryption keys, and re-encrypt all data

Encryption Keys

From this screen you can export your Encryption Keys to a password protected zip file, and you're also able to re-encrypt all your data with new encryption keys.

Encryption Key Rotation	
NIST the National Institute of Standa an organization's risk factors.	ards and Technology, recommends that Symmetric Data Encryption Keys be changed every 2 years, or earlier based on
Encryption Keys Updated On: Encryption Key Update Reminder:	Sunday, 19 September 2021 O 6 Months O 12 Months O 18 Months I 24 Months
Please click on one of the appropriate t	outtons below for more information about these two features.
🛱 Export Keys 🕼 Key Rotation	

Export Keys

You can export your encryption keys, in the format of split secrets, to a password protected zip file.

In order to restore your Passwordstate environment after a disaster, the minimum you need is a copy of the web.config file, and a copy of the database - the encryption keys are split between these two locations. For safe keeping, you can also export your encryption keys and store them away safely.

Note: If you were to lose the split secrets in the web.config file, you would not be able to restore your environment in the event of a disaster - it is very important you have a copy of this file, or export the keys using this feature.

Key Rotation

With this feature, you can update your Encryption Keys used in Passwordstate, and then reencrypt all your data with these new encryption keys. When performing key rotation, it's very important your follow the on screen instructions so that the re-encryption process is not interfered with in any way.

Conception Key Rotation

In order to perform encryption key rotation, it is recommended you take the following steps to mitigate against any issues with re-encrypting your data:

 Ensure you have a backup of your web.config file and database before starting
 Conce you start the key rotation process, do not navigate away from the screen by clicking elsewhere
 Place Passwordstate in Maintenance Mode, and ensure there are no other users currently using Passwordstate
 Place Passwordstate in Maintenance Mode, and ensure there are no other users currently using Passwordstate
 Place Passwordstate Windows Service
 Place Rosswordstate Windows Service
 Export your new encryption below
 Once the key rotation is complete, restart the Passwordstate Windows Service
 Export your new encryption keys again for safe offline storage
 If using the High Availability module, copy the new Secret1 and Secret2 values from your primary site's web.config file, to your HA site's web.config file
 And perform another backup of your web.config file - highly recommende
 And perform another backup of your wish to swap between AES 256-bit or FIPS encryption, you will need updated License Keys from Click Studios prior to performing this task.

 Please Note: During the re-encryption process, if you wish to swap between AES 256-bit or FIPS encryption, you will need updated License Keys from Click Studios prior to performing this task.

 Explore Maintenance Mode
 Place Maintenance Mode

When generating new encryption keys, and re-encrypting all your data, it is also possible to swap between the two types of encryption Passwordstate supports ie. AES 256-bit and FIPS 140-2.

Rote: If you do wish to change encryption methods, you first need to contact Click Studios and request updated License Keys for your software - as they will need to be updated on the screen, during this re-encryption process.

Caracteria Contraction

In order to perform encryption key rotation, it is recommended you take the following steps to mitigate against any issues with re-encrypting your data:

- Ensure you have a backup of your web.config file and database before starting
 Once you start the key rotation process, do not navigate away from the screen by clicking elsewhere
 The start the NUTE Demissions for the NETWORK SERVICE account
- Please ensure your web.config file has Modify NTFS Permissions for the NETWORK SERVICE account
 Place Passwordstate in Maintenance Mode, and ensure there are no other users currently using Passwordstate
- Ensure the AppSettings section in your web.config file is not encrypted (currently it is not encrypted)
- Stop the Passwordstate Windows Service
- Peform the Key Rotation by clicking on the button below
- Once the key rotation is complete, restart the Passwordstate Windows Service
- Export your new encryption keys again for safe offline storage
- If using the High Availability module, copy the new Secret1 and Secret2 values from your primary site's web.config file, to your HA site's web.config file
 Re-encrypt the AppSettings section in your web.config file highly recommended
- · And perform another backup of your database

Please Note: During the re-encryption process, if you wish to swap between AES 256-bit or FIPS encryption, you will need updated License Keys from Click Studios prior to performing this task.

During the re-encryption process, migrate from standard AES 256-bit Encryption, to FIPS 140-2 Encryption

I have read the Notifications above and understand some action is required of me before and after the key rotation

Begin Key Rotation

© 2025 Click Studios (SA) Pty Ltd

SP Encryption Key Rotation

To begin the process of re-encrypting all relevant data, please click on the 'Re-Encrypt Data' button at the bottom of the page.

Table Name	Record Count	Status
BackupSettings	1 record to process	Ø
DiscoveryJobs	8 records to process	Ø
DiscoveryJobsACL	15 records to process	Q
DiscoveryScripts	2 records to process	Ø
HandshakeRequests	0 records to process	Q
HostsACL	109 records to process	(C)
PasswordHistory	5492 records to process	Q
PasswordLists	73 records to process	(C)
PasswordListsACL	230 records to process	Q
PasswordListTemplates	15 records to process	(C)
Passwords	4448 records to process	Q
PasswordsACL	5 records to process	Ø
PrivilegedAccounts	14 records to process	Q
PrivilegedAccountsACL	13 records to process	(C)
RemoteSessionCredentialsACL	8 records to process	Q
	Pag	je 1 of 2, items 1 to 15 of 2
tatus:		Re-Encrypt Dat

2.14 Error Console

Any errors experienced within Passwordstate will be logged on this screen, which can be reported to Click Studios for troubleshooting purposes.

U Error Cor	nsole					
Below is any err	or debugging i	nformation which you can e	port and provide to Click Studios to help	p troubleshoot any technical issues you may be having (support@clickstudios.com.au).		
General Erro	ors					
Date		Category	Error Information	Event Type		
	۳	T	T	T		
No records to display.						
Export Pu	urge Error Data	3				

2.15 Export All Passwords

The Export All Passwords screen allows you to export all Password records from the system to a CSV file.

There are two types of exports available - 1. a CSV file heading information per Password List, and 2. a CSV file which is formatted for importing into KeePass. Please refer to the KB Article in the User Manual titled 'Export All Passwords and Import into KeePass' for how to import into KeePass.

Note : If you choose to export all passwords to a csv file, they must be stored away somewhere securely as the passwords appear as plain-text in the csv file

Export All Passwords

To export all passwords from Passwordstate into a CSV file, please choose one of the options below, then click on the 'Export' button.

Please Note: Due to the sensitive nature of exporting all the passwords, please consider the following:

1. One audit record will be added indicating you have run the report

2. Select 'Save' instead of 'Open' to avoid sensitive information being cached to your temporary internet files.

Export Options	Description
 Fomatted CSV file with Unique Headings KeePass Compatible CSV file 	Please select one of the available export options on the left, and click the 'Export' button.
Add one 'Password Viewed' audit record for every password exported.	
	Export

2.16 Feature Access

The Feature Access screen allows you to grant or deny access to various Features and Menus, for either User's Accounts or Security Groups. Below are the 6 main areas where control of features can be managed.

API

On the API Tab, you can specify the following:

- Restrict which Administrator's of Password Lists are allowed to create API Keys for the Password Lists, and selection which API Methods are allowed to be used
- Which users are allowed to make calls to the Windows Intergrated API
- Which users are allowed to make changes on the 'API Keys and Settings' tab on the Password List settings screen this can further restrict access from Administrators of the Password Lists

Folder Options

- On the Folder Options tab, you can set permissions for which users are allows to create Folders in the root of the Navigation Tree (Password Home)
- Specify which users, who have Administrator rights on Folders, to be able to convert between the different permission models

F Important: For the converting of Permission Model setting above, if you allow users to convert the Permissions Model from Standard to Advanced, then you are giving them adequate rights to

manage permissions on all nested Folders and Password Lists. It is possible they may not have previously had access to some nested Password Lists, prior to converting the permissions model

Hosts

On the Hosts tab, you can specify which users are allowed to have access to various features under the Hosts navigation tab. The features are:

- Which users have access to the Hosts navigation tab itself
- Which users are responsible for managing Host records add/edit/delete records, and Host Discovery Jobs
- Which users are allowed to manage Folders in the Hosts navigation tab
- Which users are allowed to see the buttons under the 'Host Statistics' area for the 'Hosts Home' screen
- Which users are allowed to manage Documents and External Links within the Hosts tab

Menu Access

The Menu Access tab allows you to specify which users or security groups are allowed to access the various main navigational menus in Passwordstate

By clicking on the appropriate 'Set Permissions' button, you can allow all users to have access, or just the ones you specify.

You can choose to either Disable the menu for users who do not have access, or hide it from them completely.



Miscellaneous

The Miscellaneous tab allows you to specify which users are allowed to manage 'Global' contacts for the Address book feature

Mobile

The Mobile tab allows you to specify which users are allowed to use the native iOS and Android Apps for Passwordstate

Password List Options

On the Password Lists options tab, you can specify which users are allowed to have access to various Password List features. The features are:

- Which users are allowed to create Shared Password Lists in the root of the Passwords Navigation Tree
- Which users are allowed to create Private Password Lists in the root of the Passwords Navigation Tree
- Which users are allowed to Drag-n-Drop around Password Lists and Folders in the Passwords Navigation Tree. By default, any user who has Admin rights to the Password List or Folder can do this, but using this feature you can further restrict this ability
- Specify which users are to use the Add Password List Wizard: (this is not applicable if a User Account Policy is forcing the use of Password List settings)
- If users are using the 'Add Password List Wizard', do you want to allow them to disable the use of the Wizard
- Specify additional 'Approvers' of Access Requests for Password Lists and Password records in addition to Administrators of the Password Lists
- With the additional approvers setting above, you can specify if you want them included in all Access Requests, or only when there are no Administrators configured on the Password List(s)

Password Reset Options

On the Password Reset Options tab, you can specify which users are allowed to see either Password Lists or Password List Templates which have the 'Enabled Password Resets' option enabled, when they are creating new Password Lists.

Remote Sessions

Passwordstate has two types of Remote Session Launchers - one is client based, and requires an install on your Windows PC, and one is browser based which can be used from any operating system.

The Remote Sessions tab allows you to specify various levels of access and features for our Remote Session Launchers, in particular:

- Which users are allowed to use the Client based version of the Remote Session Launcher
- Which users are allowed to use the Browser based version of the Remote Session Launcher
- If using the browser based version, do you want to record the user's sessions for later playback

- Do you want to hide any buttons and configuration screens for one of the Remote Session Launcher types that the user may not have access to
- Do you want to display a Session Recording warning to users so they know their remote sessions are being recorded
- For the Browser Based Remote Session Launcher, you can modify the default Keyboard layout for RDP sessions United States (English) is the default
- Which users are allowed to add/edit/delete Remote Session Credentials from within the Hosts Navigation Tab
- Which users are allowed to manage permissions on any Remote Session Credentials they have access to
- Specify which users are allowed to authenticate remote sessions using local accounts they have access to under the Passwords tab
- Specify which users are allowed to see the 'Manual Launch' buttons for the hosts

Note 1: If you are using the High Availability module for Passwordstate, it is recommended you save recorded sessions to a network share so both Passwordstate web servers are able to replay those session recordings.

Note 2: If you are using an active/passive configuration for Passwordstate with the High Availability module, then session recording is not possible on the Passive Node of Passwordstate, as you cannot write to the database with this read-only instance - and DB access is require for session recording.

Restricted Features

On the Restricted Features tab, there are certain settings which can only be changed by working in conjunction with Click Studios. The screenshot below describes which features can be changed, and the process for changing them:

- Remove the requirement for users to create and enter a Master Password for browser extension authentication
- Allow Security Administrators to export shared passwords from within the Administration area
- Allow Security Administrators to see and print the Emergency Access login password
- Allow the Emergency Access login to make changes in the Security Administrators menu
- Prevent Security Administrators from adding or modifying any PowerShell scripts

Note : Making any changes here adds an auditing record under the Activity Type of 'Restricted Feature Changes'.

hange access to va	arious features and menus in Pa	sswordstate, please review and	modify permissions on e	ach of the tabs bel	ow as appropriate.		
ch Settings:							
ipi folder op	otions hosts menu a	ccess miscellaneous	mobile password	list options p	assword reset options re	mote sessions	restricted features
nstructions							
With the Restricted	d Features on this screen, pleas	e follow the instructions below	to unlock/change certain	features.			
 Click on the Please note Once Click 	e appropriate 'Generate Reques e Click Studios' also requires em Studios provides you the Unloc	t Code' button, and then on the ail approval from your Manage k Code, enter it at the bottom (e 'Email Click Studios' but r for any features below v of the screen and click the	ton when it appear which have the 📕 e 'Unlock' button	s con next to it		
Restricted Fea	atures						
Remove the reque Note: Organization Incryption key will	irement for users to create ar ns should consider their usage , I be stored within the browser o	nd enter a Master Password for / operational requirements and on their device. If using this opt	pr browser extension aut perform an internal risk a ion an organization needs	thentication: assessment prior to s to consider how o	setting this option to 'Yes'. By s levices are protected and any a	electing 'Yes' the us oplicable compensa	sers browser extension uting controls.
etting this option	to 'Yes' would result in users n	ot needing to enter their Maste	r Password into the exter	nsion. Changing thi	s option will end all existing exte	ension sessions.	
🔍 Yes 🔍 No	Generate Request Code		•	E.			
Allow Security Ac	dministrators to export share Generate Request Code	d passwords from within the	Administration area:				
U.S. C. S. Market A.		Ale - European - Access In 199					
Yes ONO	Generate Request Code	the Emergency Access login	password.				
Allow the Emerge	ency Access login to make cha	anges in the Security Adminis	trators menu:				
Yes ONO	Generate Request Code						
havent Caswity	Administrators from adding	ar madifying any DawayShall	eninte and using the Te	et Carint Manuall	. fantuur		
Ves No	Generate Request Code		scripts, and using the re	est script manuali	reature.		
f needed, you can	clear any Request Codes above	e by clicking the following butt	On: Clear Request Code	es			
Jnlock Featu	re						
Once Click Studios	provides you with the appropr	riate Unlock Code, enter it belo	w and click the Unlock bu	itton.			

2.17 Host Types & Operating Systems

The Host Types & Operating Systems screen allows you to add additional Host Type and Operating System records which can be associated with Host records in Passwordstate.

Simply add or delete Host Types and Operating System types as appropriate.

Hosts & Operating Systems

Below are all the Host Types and Operating Systems which can be used when adding or importing Hosts on the screen Resets -> Hosts.

	Actions	Host Type
>	0	Firewall
>	0	Linux
>	0	Out-Of-Band Management
>	0	Router
>	0	Switch
>	0	Unix
>	0	Windows
Ad	ld Host Type	e View Operating Systems Grid Layout Actions •

Host Types & Operating Systems

Hosts & Operating Systems

Below are all the Operating Systems which can be used when adding or importing Hosts on the screen Resets -> Hosts.

Operating	Systems
-----------	---------

Actions	Operating System	Host Type	AD Attribute	Heartbeat Start Hour	Heartbeat End Hour
0	Arch Linux	Linux	Arch Linux	0	0
0	CentOS	Linux	CentOS	0	0
0	Cisco ASA	Firewall	Cisco ASA	0	0
0	Cisco CatOS	Switch	Cisco CatOS	0	0
0	Cisco IOS	Router	Cisco IOS	0	0
0	Cisco IOS	Switch	Cisco IOS	0	0
0	Cisco PIX	Firewall	Cisco PIX	0	0
0	Debian	Linux	Debian	0	0
0	Dell iDRAC	Out-Of-Band Management	Dell iDRAC	0	0
0	Fedora	Linux	Fedora	0	0
Change page: (II) (II) (II) Pa					5, items 1 to 10 of 52.

When using the Account Heartbeat validation feature for Password records, you may only want the Heartbeat poll to occur during certain times for different Operating Systems. By editing each of the Operating System records, you can change this poll time e.g. You only want to validate local administrator accounts for Windows 7 workstations during business hours.

Edit Operating System

Please make changes to the Operating System record below as appropriate.

Host Type *	Windows 👻
Operating System *	Windows 7
AD Attribute *	Windows 7 The AD Attribute field is used when 'Discovering' Hosts within your AD environment
Heartbeat Hours *	12:00 AM O 12:00 AM O Heartbeat checks the Host is online between the hours selected above.
	Save Cancel

2.18 Images and Account Types

The 'Images and Account Types' screen allows you to upload images which can be used as icons for the Password List themselves, and also for the 'Account Type' field for Password records.

Note 1: All images exist on the web server file system in the path <Passwordstate Folder>\images\LookupImages, and are also stored within the Passwordstate database as well. Deleting them from the file system will caused them to be recreated by the Passwordstate Windows Service.

Note 2: It is recommended you keep these images relatively small, inline with the size of the supplied images, otherwise it can distort the view of Password Lists in the Navigation Tree, and anywhere Account Type images are displayed

Note 3: If using the Passwordstate API, you may need to know the AccountTypeID for some of the images you see on this screen. To do this, simply click on the 'Toggle ID Column Visibility'

Images and Account Types

Listed below are all the Images which can be assigned to Password Lists in the navigation tree, or assigned to the Account Type field within Password records.

Actions	Account Type	Image File Name	Managed
0	& Active Directory	activedirectory.png	✓
0	iți Android	android.png	
0	🔹 Apple	apple.png	
0	Application Account	stats.png	
0	23 Calendar	calendar.png	
0	4월 CentOS	centos.png	×
0	🧑 Chrome	chrome.png	
0	😂 Cisco IOS	switches.gif	×
0	i Cloud	cloud.png	
0	🔊 Code	code.png	
М	 1 2 3 4 5 6 7 8 9 	Page: 1 of 9 Go Page size: 10 Change	Item 1 to 10 of 82
dd To	oggle ID Column Visibility Grid Layout Actions		

Managed Account Types

When adding your own Account Types, you can set the option 'Managed' to Yes, as per the screenshot below.

Having this option set to Yes means you can select these account types for password records which are stored in Password Lists that are configured for Resets - and then you can also select your own custom Reset and Validation PowerShell scripts if you have written some.

🖸 Add	New	Account	Type
-------	-----	---------	------

To add a new Account Type and Image, please specify a name, upload an image by clicking on the 'Select' button, then click on the 'Save' button.

PI	eas	e N	ote:
	-		~ ~ ~ ~

1. Images must be of	png, gif or jpg format
----------------------	------------------------

- 2. Images must be 18x18 pixles in size, or less
- 3. The file names of the images must be unique.

4. Managed means the Account Type can be selected for Password Lists which have the Password Reset option enabled.

2.19 License Information

50

The License Information screen simply allows you to update your license registration keys for Passwordstate.

Note 1: When you purchase your renewal for Annual Support + Upgrades, it's import you update your 'Annual Support' registration key on this screen, otherwise you will be prevented from upgrading to new builds of Passwordstate.

Note 2: If you were to purchase a subscription for the Password Reset Portal, or Remote Site Locations modules, Click Studios will always ensure your Passwordstate Maintenance and Subscription dates are always properly co-terminated

Licenses Information

To update details for one of the License Types below, please click on the appropriate License Type link.

Send Email Reminders for expiring Maintenance or License Subscription:

		\frown	
()	Voc	()	NLo
\mathbf{v}	162	\sim	INU

License Type	Registration Name	License Count	Expires	Registration Key	
Client Access Licenses	Click Studios	Enterprise		EACB-0525-E80A-3	
Annual Support	Click Studios	Enterprise	2021-08-21	B7DD-C024-3B20-4	
High Availability	Click Studios	Enterprise		79AF-BBC7-E986-5	
Password Reset Portal	Click Studios	Enterprise	2021-04-16	92E6-FAF8-9793-D	
Remote Site Locations	Click Studios	Enterprise	2021-04-16	156B-8F87-4DF0-3	
Request a Quote Grid Layout Actions 🔻					

2.20 Password Folders

The Password Folders screen show you all the Password Folders which have been created in Passwordstate. From this screen you can:

Edit Password Folder Details & Delete the Folder

By clicking on the 'Password Folder' hyperlink you see in the grid, you will be taken to a screen where you can perform the following actions on the Folder:

- Edit name, description and settings
- Modify permission model, and Disable Inheritance settings if applicable
- Delete the folder deleting a folder will not delete any nested Folders or Password Lists

Celebrater Content Con

To edit the Folder properties, please make appropriate changes and click on the 'Save' button.

folder properties	guide api key & settings
Please specify appropri	ate details below for the Folder, then click on the Save Button.
Folder Properti	es
Site Location *	Internal 🔻
Folder ID *	85
Folder Name *	Customers
Description	Customers
Permalink	https:// t/fid=85 (you can modify the end of the Permalink URL to specify your own 'fid' value if required.
Prevent Non-Admin ● Yes ○ No	n users from Dragging and Dropping this Folder in the Navigation Tree
Folder Permissi	on Model
Permission Model	
O Standard - Inheri	it permissions from nested Password Lists . I Advanced - Propagate permissions down from top level folder
	Save Save and Close Delete Cancel

View Nested Password Lists

By selecting the option 'View Nested Password Lists' from the appropriate Actions drop-down menu, a popup screen will appear showing all Folders and Password Lists nested beneath the one you've chosen.



Deleting Folders

Also in the 'Actions' menu are two options for deleting a folder:

- Delete Folder will delete just the folder, and nothing else. The Navigation Menu will look different to your users once you've done this, as it will need to rearrange any nested Password Lists/Folders (you can only delete a single Folder if there are no Password Lists nested beneath it)
- Delete Folder and all Nested Items Please use with caution, as this will deleted all nested Password Lists/Folders, including all associated passwords

Actions	Password Folder
	Т
0	Business Systems
😣 Del	ete Folder
😣 Del	ete Folder and all Nested Items
🖙 Exp	ort All Passwords In Folder
💂 Viev	w Folder Permissions
Viev	w Nested Password Lists
0	Customers\Sanddomain 🗣
0	Customers\Contoso\DBAs 🗣
0	🚬 \Customers\Contoso\Infratructure 🗣 🗙
0	💳 \Customers\Sanddomain\Customer Service 🖶 🗙
H	 1 2 → H
Toggle ID C	olumn Visibility Grid Layout Actions 🔻

2.21 Password Generator Policies

The Password Generator Policies screen allows you to create and manage multiple settings for the Password Generator, which can then be applied to one or more Password Lists.

Note: The Default Password Generator policy cannot be deleted - it can be renamed and its settings modified, but it cannot be deleted.

When adding or editing a Password Generator Policy, you have the following options available to you:

Password Generator Details

Edit the name and description for the Policy.

Edit Password Generator Policy

Please use the various tabs below to specify options for the Password Generator Policy 'Default Password Generator'.

passwords generator details	generate passwords	alphanumerics & special characters	word phrases
Please specify naming details for t	he Password Generator Poli	cy Below.	
Policy Name *: Default Password	Generator		
Description : Default Password	Generator with medium co	mplexity of alphanumeric characters.	
			Save Cance

Alphanumerics & 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.

passwords generator details	generate passwords	alphanumerics & special characters	word phrases
✓ Include Alphanumerics & Spec	ial Characters		
Password Length			
· · · · · · · · · · · · · · · · · · ·			
Min Length : 10 Max Le	ngtn: 15		
Alphanumerics			
	a 🗸 Numbers		
✓ Include higher ratio of alpha	numerics vs special charact	ers	
Include ambiguous alphanu	merics (I, I, o, 0 and 1)		
Evolute the following characters	and numerics		
	and numerics		
Special Characters Include the following specia (@#\$%^&*+/=	l characters		
Include the following bracke	ets		
-Generate Using a Pattern-			
Generate based on a pattern	of upper and lowercase let	ters, and numbers	
		· · · · · · · · · · · · · · · · · · ·	
i for Lowercase, u for uppercase,	n for numbers and s for sp	ecial characters I.e. Ulliinnnnssss	
Word Phrases can be included b	y inserting the letter w, or V	V if you want the first letter in the word Cap	italize.
Any other characters you insert	into your Pattern above, will	be inserted into the random password liter	rally.
			Save Cancel

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.

passwords generator details	generate passwords	alphanumerics & special characters	word phrases
Include Word Phrases			
Quantity & Length Number of Words : 1 Maximum Word Length : 7			
Positioning			
Prefix Words to Alphanumer	ics & Special Characters		
Append Words to Alphanum	erics & Special Characters		
Insert Randomly into Alphar	umerics & Special Characte	ers	
Separation			
Separate Words with Dashes			
Separate Words with Spaces			
No Separation			
			Save Cancel

Generate Passwords

The Generate Passwords tab allows you to test the settings you have specified on the other tabs, and also generate any number of random passwords based on your settings. Click on the 'Generate' button just gives you the random passwords.

Number of Passwords : 15 dims-xSMuQGZ unblown-LMwt-6 copying-c9Dzfyy	Generate Generate	e & Spell Select All	
dims-xSMuQGZ unblown-LMwt-6 copying-c9Dzfyy			
grains-#Cs+TW5 trash-&UDcy/W under-BUr%C+ hunched-VJf@u saucers-NKzVzs set-JsXW7E left-BENESi exotic-sGA\$RKm bearers-Aad83 praying-eNGu/ leaker-khZ%B frame-WjQaG			

Clicking on the 'Generate & Spell' button, gives you the random passwords, and spells them out for you as well.

passwords generator details	generate passwords	alphanumerics & special charact	ers word phrases	
Number of Passwords : 15	Generate Generate	e & Spell Select All		
burnish-h/kCJ bravo uniform ror jewels-LeHCjR juliet echo whiske grouper-kc73Br golf romeo osca recount-W4fMKYm romeo echo exempts-uK8%a echo xray echo devised-n#4J\$^B delta echo vic punters-eEPyS4 papa uniform n craning-hcH&Wd charlie romeo gapes-D&&nAut golf alpha papa discard-VeSJLun delta india sier noticed-PywfY november oscar enraged-d#=8Sk2 echo novemt azaleas-TVzin alpha zulu alpha I gasser-jUw^t golf alpha sierra s gall-u3DbxqE golf alpha lima lin	neo november india sierra h y echo lima sierra hyphen l ir uniform papa echo rome charlie oscar uniform nove mike papa tango sierra hyphen icor india sierra echo delta h ovember tango echo romec alpha november india nove echo sierra hyphen DELTA tango india charlie echo de er romeo alpha golf echo de erra echo romeo hyphen ju na hyphen uniform three DE	notel hyphen hotel forward-slash kilo co JMA echo HOTEL CHARLE juliet ROMI to hyphen kilo charlie seven three BRAV mber tango hyphen WHISKEY four too ohen uniform KILO eight percent alpha sierra hyphen echo ECHO PAPA yank ember golf hyphen hotel charlie HOTEL ampersand eight november APLHA ur hyphen VICTOR echo SIERRA JULIET L ta hyphen PAPA yankee whiskey foxtrr lelta hyphen delta hash equals eight SI en TANGO VICTOR zulu india novembel liet UNIFORM whiskey caret tango SLTA bravo xray quebec ECHO	harlie JULIET EO 'O romeo rot MIKE KILO YANKEE mike ar caret BRAVO ee SIERRA four . ampersand WHISKEY delta iiform tango JIMA uniform november t YANKEE ERRA kilo two r	
				Save Cancel

Once a Password Generator Policy has been created, it can be assigned to a Password List or Password List Template, by editing the appropriate settings, as per this screenshot below. When

your users now click on the 🖩 icon, the random password generated will be based on the selected Password Generator Policy.

Edit Password List

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

password list details c	ustomize fields	guide	api key		
Please specify Password List se	ttings manually be	low.			Or copy settings
Password List Details 🦷)				Copy Detail
Password List *	Servers				Copying a Ten
Description *	Servers				fields/settings
Image	🚭 dell.png			-	- Copy Settin
Password Strength Policy *	Default Policy			- 🖲 🖬	- Copy Settin
Password Generator Policy *	Default Passwor	d Generator			Link this P
Code Page *	User's Personal Default Passwor	Options rd Generator			Note: If copyin Type to chang
Additional Authentication *	Exclude Y & Zs Just Numbers				these values w button.
	Network Device	Passwords			Comu Dorma
Password List Settings	🛒 Pattern Match				Copy Permi
This is a Shared Passwo	SQL Password G rc Weak Generato	Generator r Policy			If you would li
Allow Password List to be	el Windows (20-25	5 char.)			List, please sei
Time Based Access Mano	latory 🔍				- Copy Permi
Handshake Approval Ma	ndatory 🔍				

Toggle Visibility of Web API IDs

When using the Passwordstate Web API, there are certain API calls which can also automatically generate passwords. In order to specify which policy to use when making these API calls, you need to know the PasswordGeneratorID value - a unique identifier for each policy. By clicking on the 'View Visibility of Web API IDs' button, you will see the PasswordGeneratorID values as per this screenshot:



2.22 Password Lists

The Password Lists screen shows all **Password Lists** created in Passwordstate, regardless of whether your account has Administrative rights to the Password Lists or not.

Note 1: You can view which Private Password Lists have been created, and who created them, but you cannot manage any permissions or settings for them

Note 2: For the Shared Password Lists, you cannot grant yourself access to any Shared Password Lists you do not already have access to

Note 3: When clicking on a Shared Password List, all passwords will be hidden and some features will be disabled for you

From this screen, the following features are available:

Actions Menu - Edit Password List Details

By clicking on the 'Edit Password List Details' menu option in the 'Actions' drop-down menu, you will be able to edit settings for the selected Password List.

Note: Please refer to the Passwordstate User Manual for detailed instructions on settings which can be applied to a Password List or Template.

Actions Menu - View Password List Permissions

By clicking on the 'View Password List Permissions' Action menu, you can view all permissions which are applied to the Password List. From here you can make any number of changes to permissions as required.

Actions Menu - Bulk Permissions for Individual Passwords

By clicking on the 'Bulk Permissions for Individual Passwords' menu option in the 'Actions' dropdown menu, you will be able to apply permissions for a user account or security group to multiple individual password records at once.

s screen allows you to apply permis	sions to more than one individ	ual passwo	rd record at a time for a User or Sec	curity Group. This does not aff	ect permissions for any Password
ministering Bulk Permissions is a thr	ee step process - 1. Search for	a User or S	ecurity Group, 2. Apply new or mod	dify existing permissions, and 3	3. Save the changes.
access permissions time ba	sed access				
Search for an appropriate user or se	curity group, and apply the rec	quired perm	issions for passwords in the Passwo	ord List 'Test Password List' (u	ise * to search for all).
Site Location : Internal			T		
Search : *					
			2		
Search For · OUser OSecur	ity Group				
earch Results	Available Passwords		View Permissions	Reason for Access	
💂 CoreAdmins	OracleTest123		/P passees1		
💂 Desktop Team	Share Admin Card 3	>>			
🏝 Human & Resources	PTest a chareschter	<<			
IS Department	Prest Password				
E Local Domain Group			Modify Permissions		
Nested Group 1					
A Network Team		>>			
Passwordstate-Auditing Security G					
Passwordstate-Export-All-Passwor		~~			
🕾 Radius Users				-	
SecurityGroup1			Administrator Permissions		
SecurityGroup2					
Sydney-TestGroup		>>			
4e Test		< <			

Actions Menu - Convert to Private Password List

Under certain circumstances, you may want to change a Shared Password List into a Private one.

Warning: Please use this feature with caution, as it is an irreversible process once complete you will need to restore a copy of your database if you wish to undo any changes with this feature. In order to use this feature, you must first apply permissions to only the intended recipient of the Private Password List - meaning you must remove all Security Group permissions, and any other 'user account' based permissions which are not appropriate for a Private Password List. Once you have done this and select this feature, the following processes will occur:

- Delete any 'permission' records applied at the individual password record level
- Delete any 'Favorite' password records for the list
- Delete any linkages to Password List Templates
- If any users have the Password List set as their Default Home Page, then it will be changed to the 'Passwords Home' node in the Navigation Tree
- And finally it will marked the Password List as private

Actions Menu - Delete Password List

By selecting the 'Delete Password List' menu option in the 'Actions' drop-down menu, you will be given the opportunity to delete the selected Password List.

Export

The Export button simply allows you to export the list of Password Lists to a csv file - no Passwords are exported, just basic information about the Password Lists themselves.

Toggle ID Column Visibility

The Toggle ID Column Visibility button will either show or hide the PasswordListID value for each of the Password Lists. These PasswordListID values may be required if you are using the Passwordstate API, or the Bulk Password Import feature below.



Clicking on a Shared Password List allows you to Administer Permissions and Edit Password List Details only - all other functions are disabled. Passw

Perform Bulk Processing - Administer Bulk Permissions

Administer Bulk Permissions allows you to apply new permissions, or remove permissions, for a user account or security group to multiple Password Lists at once.

After you have searched for a user account or security group, and then clicked on it, the 'Available Password Lists' listbox shows which Password Lists the user/security group does not have access to, and the 'View/Modify/Administrator Permissions' listbox shows what Password Lists the user/security group already has access to.

To apply new permissions, or remove existing permissions, simply move the Password Lists between the different listboxes using the various arrow buttons, then click on the Save button.

Note: You cannot manage permissions here for Password Lists which have mandatory options set for Time-Based Access.

†† Administer Bulk Permissions for Password Lists

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

Note 1: We cannot administer bulk permissions for Passwords Lists which have mandatory options set for Time Based Access. Note 2: Only Password Lists you are an Administrator of will be available on this screen. Note 3: Password Lists nested underneath folders using the Advanced Permission Model cannot have their permissions changed here - unless Disable Inheritance is enabled.

earch for an appropriate user or s ite Location : Internal iearch : * iearch For : OUser @ Sect	ecurity group (use * to search for all).	*	P	
earch Results	Available Password Lists	3	View Permissions	Mobile Access Enabled Mobile Access for these permissions:
E Corestantais E Desktop Team Human & Resources I IS Department	VAbigail Brown's Passwords Active Directory Accounts Ususiness Systems/Credit Cards	>> <<		Yes ONo Reason for Access
Local Domain Group My Group 2 Nested Group 1 Network Team Passwordstate-Auditing Security 0	Kusiness Systems/Database Accounts Kusiness Systems/Microsoft SQL Local Accounts Business Systems/Shared Team Passwords Nusiness Systems/SSL Certificates August Systems/SSL Certificates	>>	Modify Permissions Image: Systems Oracle ERP Accounts	
8 Passwordstate-Export-All-Passwor 8 <i>Radius Users</i> 8 SecurityGroup1 8 <i>SecurityGroup2</i> 8 Sydney-TestGroup	Vousiness Systemister's essence dat Vousiness Systemister's essence dat Vousioners\Contoso\DBa\Database Credential Vousioners\Contoso\Infatructure\Active Directo Vousioners\Contoso\Infatructure\Domain Passo Customers\Contoso\Infatructure\Domain Passo Customers\Contoso\Infatructure\DPB Details	>>	Administrator Permissions	
lest	<	•		

Perform Bulk Processing - Bulk Copy/Move Passwords

The Bulk Copy/Move Passwords feature allows you to Copy, Move or Copy & Link multiple passwords from multiple Password Lists to a different Password List at once - instead of doing one record at a time as users can do through the standard interface. This feature is useful if you are reorganizing your Password Lists, and need to move records around in mass.

Note: You can only copy/move records between Password Lists which have similar fields configured. If the fields are not compatible, then the destination Password List will be disabled, preventing you from copying/moving records to it.

Bulk Copy/Move Passwords

To copy/move multiple Passwords from one Password List to another is a 3 step process:

1. Select the Source Password List(s)

2. Select all the Source Passwords you want to move

3. Select the Destination Password List, and click the 'Copy/Move' button

Note: Any Password Lists which have incompatible Generic Field settings will be disabled.

ource Password List(s)	Source Password(s) (Select All)	Destination Password List
ilter 😢	Hare Admin 1	Filter
Abigail Brown's Passwords	Share Admin 2	Abigail Brown's Passwords
Active Directory Accounts	🔚 Share Admin Card 3	X \Active Directory Accounts
\Business Systems\Credit Cards	ESharePoint Reporting Account	Business Systems\Credit Cards
Kusiness Systems\Database Accounts		🖳 \Business Systems \Database Accounts
Kusiness Systems\Microsoft SQL Local Accounts		➡\Business Systems\Microsoft SQL Local Accounts
Business Systems\Oracle ERP Accounts		\Business Systems\Oracle ERP Accounts
Business Systems\Shared Team Passwords		Business Systems\Shared Team Passwords
Business Systems\SharePoint Accounts		Business Systems\SharePoint Accounts
\Business Systems\SSL Certificates		()\Business Systems\SSL Certificates
Susiness Systems\Test Password List		Business Systems\Test Password List
\Customers\Allsand\Workstation Accounts		Customers\Allsand\Workstation Accounts
Customers\Contoso\DBAs\Database Credentials		🖳 \Customers\Contoso\DBAs\Database Credentials
\Customers\Contoso\Infratructure\Active Directory Accou		Customers\Contoso\Infratructure\Active Directory Accou
Customers\Contoso\Infratructure\Domain Passwords		Customers\Contoso\Infratructure\Domain Passwords
10		^\^

Perform Bulk Processing - Bulk Password Resets

The Bulk Password Resets features allows you to view all records which are configured for Password Resets (Managed), and perform resets in bulk if required.

This feature is useful if you have an employ leave, and you can filter on password records the user has access to, as well as ones which are recommended to be reset based on the user's previous activity i.e. have they seen the value of the password since it was last reset.

ear	다 Filter								Reset	Schedule								
Pass	wordstate User A	ccount		Si	te Location				Schee	dule At			Selected Recor	rds: 0	Total Records: 510			
				-	- All Site Locati	ons	Ψ	Search	14/1	2/2020 1:04 PI	M m	O Now	Add Selected	Records to Queue	Add All Records to Queu	e		
® R ● S	ecommended rese how records enable	ts base ed for I	d on historical user activ Reset O Show records	vity () which	All passwords are not enable	the user	has access to et		Interr	nal Sites will s	tart processi	ng within a	minute, and Remo	te Sites during the ne	ext agent poll.			
Sea	arch Results																	
	PasswordID	Tit	le	D	omain or Host	Us	er Name	Account Typ	e	Description		TreePath		SiteLocation	Password Last Updated	Reset Stat	us Heartbeat Statu	is Dependencie
	T	·	т			T	T		T		т		Т	Т	· @	Т		
	67314	12	28.229.178\localuser2	Ę	12.28.229.178	lo	aluser2	SonicW/	ALL	SonicWALL 12.28.229.1	Account on 78	\Infrastru Accounts	cture\Firewall	Internal	5/21/2018 4:51:48 PM	•	•	0
	67316	12	.28.229.178\localuser2x	x 🗣	12.28.229.178	lo	caluser2xxx	SonicW4	ALL	SonicWALL 12.28.229.1	Account on 78	\Infrastru Accounts	cture\Firewall	Internal	5/21/2018 5:52:34 PM	•		0
	67124	ad	min on win2k12tfs	W	in2k12tfs.halox	net ad	min	Hindow 🗧	IS			\Infrastru Admin Ad	cture\Server Local counts	Internal		•	۰	0
	67133	ad	min10 on win2k12tfs	W	in2k12tfs.halox	net ad	min10	🚼 Window	IS			\Infrastru Admin Ad	cture\Server Local counts	Internal				0
	67125	ad	min2 on win2k12tfs	W	in2k12tfs.halox	net ad	min2	🚼 Window	rs			\Infrastru Admin Ad	cture\Server Local counts	Internal				0
	67127	ad	min4 on win2k12tfs	W	in2k12tfs.halox	net ad	min4	🚼 Window	IS			\Infrastru Admin Ad	cture\Server Local counts	Internal				0
2	67128	ad	min5 on win2k12tfs	W	in2k12tfs.halox	net ad	min5	🚼 Window	IS			\Infrastru Admin Ad	cture\Server Local counts	Internal				0
c	67129	ad	min6 on win2k12tfs	W	in2k12tfs.halox	net ad	min6	Hindow 🗧	s			\Infrastru Admin Ac	cture\Server Local counts	Internal				0
2	67130	ad	min7 on win2k12tfs	W	in2k12tfs.halox	net ad	min7	🚼 Window	IS			\Infrastru Admin Ad	cture\Server Local counts	Internal				0
כ	67131	ad	min8 on win2k12tfs	W	in2k12tfs.halox	net ad	min8	Window	IS			\Infrastru Admin Ac	cture\Server Local	Internal			•	0
	Change page: 🙀	••	н														Page 1 of 51, ite	ms 1 to 10 of 510
port	Grid Layout Ac	tions	•															
Action	ns Queued At		- PasswordID		Title		Domain or H	ost	UserNa	me	Account Ty	pe	Description		TreePath	Sit	e Location	Dependencies
		100	-	*		Ŧ		T		-								

Perform Bulk Processing - Mobile Access Bulk Permissions

If you need to make many changes to Mobile Access Permissions at once, you can use the 'Mobile Access Bulk Permissions' feature.

This feature allows you to query all the permissions applied to one or more Password Lists, select the appropriate permissions (Guest, View, Modify or Admin), and then either enable or disable access for Mobile Apps.

would like to Enable Disable Mobile Access for the	Permissions I select below.	
Password List(s)	Permissions	(Select All
Filter \Abigail Brown's Passwords \Active Directory Accounts \Business Systems\Credit Cards \Business Systems\Credit Cards \Business Systems\Database Accounts \Business Systems\Oracle ERP Accounts \Business Systems\Shared Team Passwords \Business Systems\SharePoint Accounts \Business Systems\SharePoint Accounts \Business Systems\SharePoint Accounts \Business Systems\SharePoint Accounts \Business Systems\Station Accounts \Customers\Contoso\DBAs\Database Credentials \Customers\Contoso\Infratructure\Active Directory Accout \Customers\Contoso\Infratructure\Domain Passwords \Customers\Contoso\Infratructure\SP Details 	 & Business Systems\SSL Certificates \ Image Capture (Modify) & Business Systems\SSL Certificates \ Lee Sandford (Modify) & Business Systems\SSL Certificates \ Lee Sandford (Modify) & Business Systems\SSL Certificates \ Lee Sandford (Modify) & Business Systems\SSL Certificates \ Paul Bassett (Modify) & Business Systems\SSL Certificates \ Paul Bassett (Modify) & Business Systems\SSL Certificates \ Video Capture (Modify) & Business Systems\SSL Certificates \ Video Capture (Modify) 	

2.23 Password List Templates

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

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.

selow are	all the Password List Templates stored with	in Passwordstate.					
Actions	Password List	Description	Linked Password Lists	Deny Export	Time Based Access	Prevent Password Reuse	In-Built Templat
	т	T					1
0	🔎 A Security Test 🖦		0			×	×
0	O 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	KeePass Template		0				×
0	Villiple Approvers		0			✓	×
0	One-Time Password Authenticator	Generate One-Time Passwords based off scanned QR Codes	0			✓	×
0	PasswordSafe Import		0			✓	×
0	Secret Server Template	Used for importing Secret Server Data	0			✓	×
0	G Software Licenses	Store various metadata related to software licensing	0			✓	*
	Ω.A.		Page: 1 of 2	Go Page size: 1	Change		item 1 to 10 of

Adding and Editing Templates

Adding or editing templates in the Administration area is identical to the normal Password List Templates screens which standard user accounts have access to. For information on each of the settings which can be applied to a Template, please refer to the Passwordstate User Manual for creating Password Lists.

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.

Actions	Password List		Description	
	T		T	
0	🔎 A Security Test ጫ			
0	🔇 Alarm/Door Codes	Store building alarms codes, or d		
0	Credit Cards	Securely store credit card information		
0	Enabled for Password	Perform password resets on a sc		
0	🔎 KeePass Template			
💂 Vie	ew Permissions			
& Lin	ked Password Lists	thenticator	Generate One-Time Passwords b	
O De	PasswordSate Import			
0	Secret Server Template	2	Used for importing Secret Server	
0	Goftware Licenses		Store various metadata related to	
H I 2	H			
Add New Tem	plate Toggle ID Colun	nn Visibility Grid I	Layout Actions 🔻	

Linked Password Lists

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

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

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

Linked Password Lists

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

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 Pa 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

Available Password List(s)			Linked Password List(s)		
Filter	٢		Filter	E	•
≫\Abigail Brown's Passwords	*		>Business Systems\Test Password List		
શ \Active Directory Accounts					
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					
Customers\Allsand\Workstation Accounts					
🖳 \Customers\Contoso\DBAs\Database Credentials					
🖶 \Customers\Contoso\Infratructure\Active Directory Acco	u				
\Customers\Contoso\Infratructure\ISP Details					
Customers\Contoso\Infratructure\Network Devices	-				
Count: 90			Count: 1		

2.24 Password Strength Policies

Password Strength Policies are used as a set of rules for determining the strength of a Password. Once a policy is created, it can be applied to one or more Password Lists.

When adding or editing a Password Strength Policy, settings can be applied on 2 of the tabs, and there is 1 tab for testing the policy.

Policy Settings Tab

The Policy Settings Tab allows you to provide a name and description for the policy, plus the following settings:

- Minimum LowerCase Characters specifies how many lowercase characters are required as a minimum (abcd, etc)
- Minimum UpperCase Characters specifies how many uppercase characters are required as a minimum (ABDCD, etc)

- Minimum Numeric Characters specifies how many numeric characters are required as a minimum (1,2,3,etc)
- Minimum Symbol Characters specifies how many symbol characters are required as a minimum (%@:!, etc)
- Preferred Password Length specifies the minimum number of total characters the password should have
- Requires Upper And Lower Case indicates if the passwords string must have both lower and uppercase characters
- Password Strength Compliance indicates the desired Password Strength Complexity (Very Poor, Weak, Average, Strong or Excellent). With the following graphic when editing/adding a password, the 'Compliance Strength' indicator shows the user what password complexity is desired for the applied policy

Password *	•••••	😫 🔍 🖩 🌺
Confirm Password *	•••••	
Password Strength	$\star \star \star \star \star \star$ Compliance Strength $\star \star \star \star \star \star$	
Strength Status: Excelle	ent password strength	

• Compliance is Mandatory - if this option is set to Yes, the user will not be able to save the password record if the strength of the password they're creating does not meet the 'Password Strength Compliance' setting above

Edit Password Strength Policy

Please specify your password strength policy settings in each of the appropriate tabs below, and click on the 'Save' button.

Note: the policy is not enforced when entering a password, instead it's used as a visual representation of password strength.

test password strength	policy settings	calculation weighting						
Please specify details for the F	Please specify details for the Password Strength Policy Below.							
Policy Name *	: Defau	It Policy						
Policy Description	: Defau	It policy if no specific policy is set for a Password List						
Minimum LowerCase Characte	ers * : 1							
Minimum UpperCase Charact	ers * : 1							
Minimum Numeric Characters	* : 1							
Minimum Symbol Characters	* : 1							
Preferred Password Length *	: 8							
Requires Upper And Lower Ca	ise* : 🖲 Ye	es 🔍 No						
Password Strength Compliance	e * 🔍 🗄 Stror	ng 👻						
Compliance is Mandatory * 🖷	: • Y	es 🖲 No						
		Save Cancel						

Calculated Weighting Tab

The Calculated Weighting Tab allows you to specify the weighting of a strength characteristic of a password for length, numeric, case and symbols. The higher the weighting, the more important the category is deemed to be.

Rote: The 4 values specified must total 100.

Edit Password Strength Policy

Please specify your password strength policy settings in each of the appropriate tabs below, and click on the 'Save' button.

Note: the policy is not enforced when entering a password, instead it's used as a visual representation of password strength.

test password strength	policy settings	calculation weighting
Calculation Weighting allows numeric, case and symbols. The second symbols of the second	you to determine the he 4 values specified	e weighting of a strength characteristic of a password for length, must total 100.
Length Weighting *	: 50	
Numeric Weighting *	: 15	
Casing Weighting *	: 15	
Symbol Weighting *	: 20	
		Save Cancel

Test Password Strength Tab

The Test Password Strength Tab allows you to test the policy settings you've specified on the other two tabs, and shows you a graphical representation of the strength of the password you type, based on the policy settings you've specified.
Edit Password Strength Policy

Please specify your password strength policy settings in each of the appropriate tabs below, and click on the 'Save' button.

Note: the policy is not enforced when entering a password, instead it's used as a visual representation of password strength.

test password strength	policy settings	calculation weighting		
To test this Password Strength	n Policy, simply being	typing a password below.		
		_		
Rain*97	acters			
			Save	e Cancel

2.25 Privileged Account Credentials

Various processes in Passwordstate require a 'Privileged Account' to perform certain tasks i.e. Resetting Passwords, querying active directory, etc. This screen allows you to add those accounts to be used.

Once you have specified the details for one or more of the relevant Privileged Account Credentials, and applied permissions for users or security groups who are allowed to use these accounts, then they can be used for Password Resets and Discovery jobs, etc.

If you "link" the Privileged Account to a password stored in Passwordstate, when the password is updated in Passwordstate and Active Directory, it will also be automatically updated on this screen as well.

Please Note: As of build 8650, there are two new System Setting options to hide the value of Passwords for Privileged Accounts, and also restrict making changes to them if you do not have explicit permissions to them. These options can be found on the screen Administration -> System Settings -> Miscellaneous tab.

of Privileged Account Credentials

Below are all the Privileged Account Credentials which can be used for Active Directory Account lookups, Host and Account Discove

ite Loca	tion Account Type				
All Site Locations 🔻 - All Account Types -					
Show	Credentials I have access to O Show all Credentials				
ctions	Description				
	Τ				
0	Azure AD Priv Account for Contosp				
0	Cisco Admin Account - Root				
0	Cisco Admin Account - Root				
0	Cisco Admin Account - tsandx				
0	Cisco Enable Secret for Resetting Named Accounts				
0	Cisco Named Account for Resetting Enable Secret				
0	cvsinfotech Domain Admin2				
0	Halox Site Location Account				
0	Internal Linux - Root Account				
0	Linux Privileged Account - Putty with Private Key				
(H)	<123 (►) (H)				

Note: When apply permissions to Privileged Account Credentials, you can also specify Time-Based Access as well - so user's access to the account can automatically be removed after a set period of time.

♂ Privileged Account Credentials

Below are all the Privileged Account Credentials which can be used for Active Directory Account lookups, Host and Account Discovery, and Passwo

Site Loca	ation	Account Type	
All Sit	e Locations	 All Account Ty 	vpes - 💌
Show	Credentials I have ad	ccess to OShow all Credentials	
6 -ti	Description		Handland
Actions	Description		Osername
	T		T
0	Azure AD Priv Acco	ount for Contosp	
💄 Vi	ew Permissions	Root	root
🕴 D	elete	Root	root
0	Cisco Admin Accou	int - tsandx	tsand
0	Cisco Enable Secret	t for Resetting Named Accounts	enable
0	Cisco Named Acco	unt for Resetting Enable Secret	tsand
0	cvsinfotech Domain	n Admin2	
0	Halox Site Location	Account	
0	Internal Linux - Root Account		root
0	Linux Privileged Ac	count - Putty with Private Key	marlee
н	• 1 2 3 • •		

of Edit Privileged Account Details

Please update details as appropriate below for the Privileged Account Details.

Note: If no permissions are applied to this account, then it cannot be used to perform any Account Discovery or Password Resets.

privileged accoun	t credentials public key authentication	
Description: *	Update Active Directory Account Passwords	
UserName: *	and the second se	
	For Active Directory Accounts, specify the format of domain\userid.	
Site Location:	Internal	•
Account Type:	Active Directory	Ŧ
Password:		. · ·
Confirm Password:		
Link To Password.	Not Required	*
\subset	If you link this Privileged Account to a password record which is enabled for Passw Privileged Account Credential password will be updated once the password reset passwords which have been enabled for Reset, plus match the UserName above, v	vord Resets, then the is complete. Note: Only will be visible here.
		Save Cancel

2.26 PowerShell Scripts

Each of the various default PowerShell scripts for Account Discovery, Password Resets and Account Heartbeat are available on this screen.

PowerShell Scripts								
PowerShell scripts are the ba	sis for the Password Rese	t, Validation, and Account Di	covery engine	e built in Pa	asswordsta	te.		
By clicking on one of the but	tons below you can view	& test the default scripts pro	vided by Click	Studios, or	r you can o	reate and e	edit your owr	
3y clicking on one of the but	tons below you can view	& test the default scripts pro	vided by Click	Studios, or	r you can d	reate and e	edit your owr	

In addition to these default scripts, you can also add your own scripts for your own Infrastructure or Applications. See the Images and Account Types section of this manual for information about how to add in a custom **Managed Account**. Adding in your own custom Managed Account into Passwordstate means you will then be able to set your custom Powershell scripts on Password Records.

Powershell scripts can also be assigned to Password Records as a Dependency, which means upon a successful reset of a password record, you can have your custom Powershell script execute.

Examples of these Password Dependency scripts could be emailing a distribution list of a successful reset, or maybe updating a ticketing system.

Testing Scripts

Testing your Powershell scripts manually can be performed via the Actions menu, and this feature could be used for troubleshooting purposes, as it is quicker than executing scripts via a Discovery job or Password Reset for example.

Script Filters Show all Scripts O Show only Inbuilt Scripts Actions Script Name Description Reset SQL Password Reset Windows COM+ Component Password Reset Windows IIS Application Pool Password Reset Windows Scheduled Task Password Reset Windows Scheduled Task Password Reset Windows Scheduled Task Password Reset Windows Service Password Reset Windows Service Password 	elow are all	I the Password Reset Scripts you can associate with a password record, to be executed when the password is updated	d.
 Show all Scripts O Show only Inbuilt Scripts Actions Script Name 2 Reset SQL Password 2 Reset Windows COM+ Component Password 2 Reset Windows IIS Application Pool Password 2 Reset Windows Password 2 Reset Windows Scheduled Task Password 2 Reset Windows Scheduled Task Password 3 Reset Windows Scheduled Task Password 3 Reset Windows Service Password 3 Reset Windows Service Password 	Script Fi	lters	
Actions Script Name Description 	Show	v all Scripts O Show only Inbuilt Scripts	
	Actions	Script Name	Description
Image: Component Password Reset the Image: Component Password Reset the	0	≥ Reset SQL Password	Reset Micr
 Reset Windows IIS Application Pool Password Reset Windows Password Reset Windows Sassword Reset Windows Scheduled Task Password Reset Windows Scheduled Task Password Reset Windows Service Password Reset Windows Service Password Reset Windows Service Password 	0	2 Reset Windows COM+ Component Password	Reset the p
 Reset Windows Password Reset Windows Scheduled Task Password Reset Windows Scheduled Task Password Reset Windows Service Password Reset the 	0	2 Reset Windows IIS Application Pool Password	Reset the p
	0	2 Reset Windows Password	Reset pass
Reset Windows Service Password Reset the	0	2 Reset Windows Scheduled Task Password	Reset the
		2 Reset Windows Service Password	Reset the p

When test a script, you should populate the appropriate fields and then click the **Run Script** button. You will either get a successful result, or an error. In this example below, we are executing a reset on a local Administrator account on a Windows machine - this will reach out to the remote host (webserver01) and perform the actual reset on the account (testuser)

	Script Parameters	
	Specify parameters here to pass to the script as Hools Webserver01	ppropriate - multiple Hosts can be specified by adding one per line. UserName: UserName: UserName: UserName: Did Password: New Password: Privileged Account UserNime: haloxpws_write Privileged Account Password:
Name	Script Output Executing for Host 'webserver01' at Success	9/02/2021 12:51:21 FM.

Code Signing PowerShell Scripts

Powershell has optional security to only allow scripts that have been digitally signed to be executed. Under normal circumstances, setting the policy on the machine via the **Set_executionPolicy AllSigned** option will deny scripts from being run unless they are signed with a trusted certificate. Passwordstate does not execute its Powershell scripts directly from the file system, so the "**AllSigned**" policy does not affect the scripts that Passwordstate executes. Rather, it loads the script directly from the Passwordstate database and executes in memory.

For this reason, you can still set your Passwordstate server execution policy to any value you like, and this will not affect Powershell operations within Passwordstate.

SSH Template Scripts

If you are hoping to build scripts that connect to devices using the **SSH** protocol, then there is a feature you can use called **SSH Templates** which are predefined scripts built in to Passwordstate. With these scripts, all you need to do is set some SSH commands you wish to issue to your SSH device, and then also set some Error Capturing commands. This makes building custom scripts for SSH devices very easy, and more information about how to build these scripts can be found in Section 16 of this manual:

https://www.clickstudios.com.au/downloads/version9/Passwordstate_Privileged_Account_Mana gement_Manual.pdf

2.27 Remote Session Management

On the Remote Session Management screen, you can:

- See all Remote Session Credentials which have been added into Passwordstate, regardless of whether your account has been give access to them or not
- View and play back recorded remote sessions (for the browser based version of the Remote Session Launcher)
- And configure various settings for the Gateway for the browser based version of the Remote Session Launcher
- Or follow instructions for configuring the Browser Based Remote Session Launcher Gateway separate to your normal Passwordstate web site

Remote Session Manage	nent	
Passwordstate has two types of Remot	e Session Launchers available, with the following features:	
Browser Based Launcher		
 Runs from within your Browser RDP & SSH Sessions All sessions are initiated (proxie Session Recording and Playbac 	- can be used on all Operating Systems d) from the Passwordstate web server	
Client Based Launcher		
 Requires Client Install - Windov RDP, SSH, Telnet, VNC, SQL and All sessions are initiated from ti No Session Recording 	s Operating Systems only Teamviewer Sessions ie user's PC	
By clicking on one of the buttons belo	w you can view any saved Remote Session Credentials or Recordings, or you can configure the Gateway settings for the Browser Based ver:	rsion.
Remote Session Credentials	Recorded Sessions Based Gateway Settings Install Browser Based Gateway	

Note: For Remote Session Credentials via this page, if you are changing the 'Link to Credential' field for the record, only Password records that your account has access to will show here - just the same as on the Hosts tab as well.

low are all	the Remote Session Crede	entials added to Passwordstate	- used for the Remote Sessior	Launcher feature.		
Actions	Description	Host Name Match	Site Location	Connection Type	Linked To Password	Permission Count
	Т	Т	Т	Т	T	
0	Cisco Devices		Internal	SSH	eisco account	7
0	Domain Account		Internal	RDP	Domain	1
0	Linux Sessions	P	Internal	SSH	👌 Linux Login	7
0	RDP		Internal	RDP	Domain	8
0	SQL		Internal	SQL	SA Account on	7
0	SSH Key test	🖵 udesktop	Internal	SSH	Δ	3
0	VNC		Internal	VNC	d Domain	7

2.28 Reporting

On the Reporting screen, there are many pre-defined reports you see below which can be run. Various reports allow filtering on various fields, and data can also be exported to Excel if required.

These reports can also be scheduled via the screen Reports -> Scheduled Reports, or can be executed via the API (either using the Reporting API Key, or without if accessing via the Windows Integrated API).

Note: No password values are exported in any of the reports on this screen.

✓ Reporting

To view details of a report, select it from the list below, and click on the 'Run Report' button to execute.

Note: These reports can also be scheduled from the 'Reports -> Scheduled Reports' menu - if you've been given access to this menu.

ser Reports	Password Reports
Vhat passwords can a user see?	What passwords have failed Heartbeat?
Vhat passwords does a user still know?	What passwords have failed Reset?
/hat has a user been doing lately?	What passwords require checkout?
/hat Failed login attempts have there been?	What passwords are currently checked out?
/ho hasn't logged in recently?	What passwords require a Reason to be specified for access?
/ho has one or more Security Administrator roles?	What passwords are expiring soon?
/hat Remote Sessions has a user been doing lately?	What passwords have recently been reset?
/hat user accounts are currently disabled?	What password values have been reused?
/hat user accounts are set to expire?	What passwords have not been used lately?
/hich users have logged in using the Emergency Access account?	What Passwords are not being synced?
/hat user account impersonation has been occurring?	Show Passwords configured for resets and their dependencies
/hat authentication option is applied for each user?	Passwords Strength Compliance Status
	Have I Been Pwned Compromises
ermission Reports	
/hat permissions exist (all users and security groups)?	Activity Reports
/hat permissions exist for a user?	Remote Session Launcher Activity
/hat Permissions exist for a Security Group?	Browser Extension Activity
/hat permissions have changed recently?	Mobile Client Actviity
/hat permissions exist for all shared password records	API Activity
numerated permissions report)?	Self Destruct Activity
/hat permissions exist for all Host Folders?	Passive High Availability Module Activity
/ho has been approved access to passwords recently?	
/ho has been denied access to passwords recently?	Occument Reports
ow many Administrators are there for each Shared Password List?	
ow many Administrators are there for each Password Folder?	What documents have been uploaded into Password Folders?
	What documents have been uploaded into Password Lists?
iscellaneous Reports	What documents have been uploaded into Password records?
	What documents have been uploaded into Host Folders?
Inere are Privileged Account Credentials currently being used?	What documents have been uploaded into Host records?
nat security groups exist, and who are their members?	
hat Host records exist in Passwordstate, and what are each of peir configuration items?	Scheduled Reports
ien conniguration (tellis)	You and Manager all Cale and a Department of the
	View and Manage all Scheduled Reports created by users

2.29 Security Administrators

The 'Security Administrator' role in Passwordstate provides access to one or more features in the Administration area. If a user's account is not set up as a Security Administrator, the Administration Tab will not be visible to them.

There is a one-to-one mapping of Security Administrator roles to each of the Nodes/Features you see in the Administration Navigation Tree.

Note : To ensure there is a clear separation of elevated privilege responsibilities within Passwordstate, you cannot modify any Security Administrator role settings for your own account another Security Administrator will need to do this for you. As such, Click Studios recommends you have at least 2 Security Administrators assigned, otherwise you may need to use the Emergency Access account to make changes to this role if required.

Security Administrators

Listed below are the Security Administrators of Passwordstate, and their respective roles.

Menu Visib If a user does Disable t	ility s not have a specific Security Administrator role, select if you would like to disable or hide the appro he menus OHide the menus	priate menu item(s).
Actions	User or Security Group	Number of Roles
0	& Image Capture (halox\images)	45
0	2	45
0	2	45
0	2	45
0	& P.	45
0	& Video Capture (halox\videos)	45
Add Grid L	Layout Actions 🔻	

2.30 Security Groups

Security Groups allows you to manage either local security groups created within Passwordstate, or Active Directory security groups. These groups can then be used for applying permissions to Password Lists, or to give/deny access to various features.

On the Security Groups screen, you have the following features available:

Add Local Security Group

Allows you to add a "local" security group to Passwordstate, which you can then assign one or more user accounts to the security group.

Note: Once you have added the local security group, you can assign user account membership by selecting the 'Manage Members' menu item from the appropriate Actions menu

Add New Local Security Group

To add a new Local Security Group to Passwordstate, please fill in the details below.

Note: Once the Security Group is created, you can then begin to assign members.

security group details	
Please specify a Name an	d Description for this Local Security Group.
Site Location *	Internal 💌
Security Group Name *	
Description	
Hide Group in UI	Hide on all screens in UI where you can apply permissions
	Save Save & Add Another Cancel

Add Active Directory Security Group

To add an Active Directory Security Group, you simply need to search for the group you require, then click on the appropriate Save button.

Note 1: When you add a security group, if there are any new user accounts found which do not already exist in Passwordstate (on the <u>User Accounts</u> screen), there is on option on the screen Administration -> <u>System Settings</u> -> <u>Active Directory Options Tab</u> which allows you to also automatically add these user accounts.

Note 2: Cross domain membership in Security Groups is not supported

Add Active Directory Security Group

To add a new Active Directory Security Group to Passwordstate, please use the search feature below.

security group detail	s			
secondy group detail	5			
Please use the search f	eature below to search for an Active Director	ry Security Grou	p.	
Security Group Name *	core			<mark>,</mark>
AD Domain *				Ŧ
LDAP Filter :				0
Description				
Hide Group in UI	Hide on all screens in UI where you ca	n apply permiss	ions	
Security Groups Search	Results			46
🗏 CoreAdmins				

Nested Security Groups

Nested Security Groups are supported in Passwordstate, but we do not maintain the nesting structure of those security groups. Instead, all the members of the nested Security Groups, will show in Passwordstate as members of the "parent" security group.

Please Note: Nested Security Groups are only supported within the same Active Directory Domain i.e. you cannot nested a Security Group from Domain B, beneath a Security Group from Domain A.

Debug Security Group Membership

In the event you are having some issue synchronizing the membership of an Active Directory Security Group, the 'Debug Security Group Membership' screen allows you to query the members of the security groups, and provide some additional debug information which may be useful for determine the cause of the issue.

is page will allow you test querying the membership of	An Active Directory Security Group, and provide additional debug information during the process.
use this feature you will need to first search for the ap	propriate Security Group. When you click on a Security Group in the search results, it will attempt to enumerate all the members for y
security group details	
Please use the search feature below to search for an A	ctive Directory Security Group.
Security Group Name * CoreAdmins	P
AD Domain *	
Security Groups Search Results	Debug Information
E CoreAdmins	Debug 1: ctx = New PrincipalContext(ContextType.Domain, FQDN, ADUserName, Password)
	Debug 2: FQDN = clicksec.net, ObjectSID = S-1-5-21-311937828-3021193869-608170936-1670
Ç₂	Debug 3: Using members As PrincipalSearchResult(Of Principal) = GroupPrincipal.GetMembers(True)
	Debug 4: Dim strUserID As String = Passwordstate.ActiveDirectory.GetUsersDomainNetBIOSFromDistinguishedNamerADDomainsTable
	strSamAccountName, p.DistinguishedName.ToString(),,)
	Mag. Lorden. Star Son Sortine in Acars Soliday
	interactions and lighters. Mile Acceptable for
	Debug 6: Dim strUserID As String = Passwordstate.ActiveDirectory.GetUsersDomainNetBIOSFromDistinguishedName(ADDomainsTable, strSamAccountName, p.DistinguishedName.ToString(),,)

Local Security Group Actions Menu

Once you have created a Local Security Group, the 'Actions' drop-down menu has two features you can use:

- Manage Members allows you to add or remove members from the security group
- Delete delete the security group from Passwordstate. This does not delete any user accounts, only the security group itself

Note: If the Security Group has been used to apply permissions anywhere within Passwordstate, removing members from the security group, or deleting the Security Group itself, will remove one or more user's access



Active Directory Security Group Actions Menu

Once you have add a new Active Directory Security Group, the 'Actions' drop-down menu has two features you can use:

- Manual Synchronization synchronization membership of an Active Directory Security Group can be done in one of 3 ways:
 - $\,\circ\,$ When you first add an AD Security Group to Passwordstate
 - The Passwordstate Windows Service can perform the synchronization on the schedule you have specified on the screen Administration - > <u>System Settings</u> -> <u>Active Directory Options</u> <u>Tab</u>
 - \circ Or by clicking the 'Manual Synchronization' menu item
- Delete delete the security group from Passwordstate. This does not delete any user accounts in Passwordstate, and does not touch your Active Directory environment in any way



Clone Security Group Permissions

It's possible to clone the permissions from one Security Group to another using the 'Clone Permissions' feature.

Note 1: When cloning occurs, the Destination Security Group's permissions are first removed – otherwise duplication would occur

Note 2: Security Group Memberships will not be cloned with this process, as you need to manage these memberships yourself - either manually for Local Security Groups, or by letting the AD synchronization work for AD groups.

During the cloning process, the following types of permissions will be cloned:

- Any memberships to Email Notification Groups
- Any of the 'Features' permissions for what menus the user is allowed access to at the bottom of the screen
- Any permissions to Password Lists (auditing records are added)
- Any Password Permissions (auditing records are added)
- Any permissions to Password Lists Templates (auditing records are added)
- Any Security Admin Roles (auditing records are added)
- Any User Account Policy permissions

†† Clone Security Group Permissions

To clone permissions for a Security Group, you need to select the Source and Destination Groups below, then click on the 'Clone' button.

Please Note: Please refer to the Security Administrators' manual for what processing occurs when you clone a Security Groups's permissions (Important)

ource Security Groups	Destination Security Groups
ilter	S Filter
💂 CoreAdmins (halox)	💂 CoreAdmins (halox)
💂 Desktop Team (halox)	💂 Desktop Team (halox)
Human & Resources	🐣 Human & Resources
IS Department (halox)	💂 IS Department (halox)
Local Domain Group (halox)	💂 Local Domain Group (halox)
A My Group 2	and My Group 2
Nested Group 1	🐣 Nested Group 1
Network Team	🐣 Network Team
Passwordstate-Auditing Security Group	🐣 Passwordstate-Auditing Security Group
Passwordstate-Export-All-Password Security Group	asswordstate-Export-All-Password Security Group
😫 Radius Users	🐣 Radius Users
SecurityGroup1	🐣 SecurityGroup 1
SecurityGroup2	and SecurityGroup2
Sydney-TestGroup	🐣 Sydney-TestGroup
e Test	🐣 Test

Debug Active Directory User Account and Security Groups Synchronization Process

By clicking on the 'Debug AD Sync Data' button, it allows you to turn on some debug capturing when the Passwordstate Windows Service performs the Active Directory User Account and Security Group synchronization process.

🗏 Debug AD Sync Data

By enabling the Debug option below, the scheduled AD Synchronization process will add debug information to the grid below. The scheduled AD Synchronization process is performed by the Passwordstate Windows Service.

Search Debug Da	ata			
Debug Information	:	✓ Information	Warning 🗷 Error Search	
ate	Debug Inf	iormation	Event Type	
Ē	T	T	T	

2.31 System Settings

System Settings are used to specify any number of system wide settings in Passwordstate, which can affect the majority of users within the system.

Active Directory Options Tab	Various settings for synchronizing Active Directory user accounts and security groups with Active Directory
Allowed IP Ranges Tab	Specify which IP Addresses or IP Address Ranges are allowed to access the Passwordstate web site or API
<u>API Tab</u>	Create various API Keys for making calls to the Passwordstate API, and also various settings for the Standard API and also Windows Integrated API
Auditing Data	Various options for archiving auditing data
Authentication Options Tab	Various options and settings for authenticating to the Passwordstate web site
Branding Tab	Specify your own Logos and Page Titles to use on various screens and dialogs
<u>Check for Updates Tab</u>	Specify how frequently Passwordstate should check for new versions
Email Alerts & Options Tab	Multiple options for various email notifications
Folder Options	Specify various settings for Folders within the main Navigation Tree.
High Availability Options Tab	Specify how frequently the High Availability instance of Passwordstate should check for new/update Custom Images and Logos, and write these to disk
Hosts Tab	The Hosts tab has a few options for showing or hiding all the Hosts users have access to, on the Password Home and Remote Session Launcher pages
<u>Miscellaneous Tab</u>	Various settings which don't fall into any other of the 'Tab' categories
Mobile Access Options	Specify various system wide settings for the Mobile App
Password List Options Tab	Settings which are specific to Password Lists
Password Options Tab	Settings which are specific to individual password records

Password Reset Options	Specify various settings when updating passwords in Active
	Directory, and specify who is allowed to enable the 'Password
	Reset' option on Password Lists
Email, Proxy & Syslog Servers Tab	Email Server settings, proxy and syslog settings
Self Destruct Messages	Various settings for the Self Destruct Message feature
Usage Tracking Tab	Allows you to specify your own JavaScript code to be inserted
	into the main /default.aspx page
User Acceptance Policy Tab	Specify a popup 'User Acceptance Policy' which users must read
	when they access the Passwordstate web site

2.31.1 Account Discoveries

90

The Account Discoveries screen allows you to configure the number of simultaneous threads to use when executing Account Discovery Jobs i.e. how many hosts to query in parallel, as well as purging settings for the history of jobs.

1 Settings:									
count discoveries nail alerts & options ssword reset options	active directory optio folder options proxy & syslog se	ns allowed high availabilit rvers self d	ip ranges y options lestruct mess	api hosts ages	auditing data miscellaneous usage tracking	authentication options mobile access options user acceptance policy	branding che password list op	eck for updates ptions password optic	ons
word reset options	proxy & syslog se	rvers self d	lestruct mess	ages	usage tracking	user acceptance policy			
specify appropriate s	ettings for the Account I	Discovery feature	in Passwords	tate.					
e specify appropriate s	settings for the Account I	Discovery feature	e in Passwords	tate.					
e specify appropriate s count Discovery	ettings for the Account i	Discovery feature	e in Passwords	tate.					
e specify appropriate s count Discovery /hen performing Acc	settings for the Account v Settings ount Discoveries, use the	Discovery feature	e in Passwords mber of mult	tate.	d processes for con	necting to hosts:			
e specify appropriate s count Discovery /hen performing Acc I Thread	settings for the Account r Settings ount Discoveries, use th	Discovery feature	n Passwords	tate.	d processes for con	necting to hosts:			
e specify appropriate s count Discovery Vhen performing Acc 1 Thread urge Discovery Job H	settings for the Account r Settings ount Discoveries, use the listory older that (x) da	Discovery feature he following nu	e in Passwords mber of mult	tate.	d processes for con	necting to hosts:			

2.31.2 Active Directory Options Tab

The Active Directory Options tab allows you to specify an account to interact with Active Directory, and various options for User Accounts & Security Groups.

Passwordstate AD User Account and Security Group Membership Options

The 'Passwordstate User Account and Security Group Membership Options' settings allows you to specify various options for synchronizing User Account enabled/disable status, and security group memberships within Passwordstate.

If a User Account is found within a Security Group which hasn't already been added to Passwordstate, would you like to automatically add the User Account;

When the Passwordstate Windows Service synchronizes the membership of any Security Groups you've added on the <u>Security Groups</u> screen, it's possible there will be user accounts in the Active Directory security group which have not yet been added to the <u>User Accounts</u> screen. If this is the case, you can use this option to automatically add the accounts to Passwordstate, or simply ignore the account.

Note: If you reach the maximum number of Client Access License as recorded on the <u>License</u> <u>Information</u> screen, the user accounts will not be added to Passwordstate.

Synchronize the enabled/disabled status of Active Directory user accounts with the user accounts in Passwordstate;

Using this option, if the enabled/disabled status of a user account in Active Directory is changed, you can also synchronize that change to the account stored in Passwordstate.

When a new Active Directory user account is added to Passwordstate as part of the synchronization process, immediately disable the account:

If you have a requirement to disable Active Directory User Accounts when they are initially added into Passwordstate as part of the AD synchronization process, then you can enable this option.

When an account in Active Directory is deleted, perform the following in Passwordstate:

If a User Account in Active Directory is deleted, you can choose either you want to delete it in Passwordstate, or simply do nothing.

When a user is removed from a Security Group, and that user no longer belongs to any Security Groups, perform the following in Passwordstate:

If a user no longer belongs to any Active Directory Security Groups, which have been added to Passwordstate, you can choose to disable it, or do nothing with their account.

When performing an AD Sync, synchronize the email field for the user (AD attribute is called mail):

If you do not wish to populate the email address field in Passwordstate with what's stored in AD, set this option to No.

For User Accounts which are disabled in Passwordstate, automatically delete these accounts after the number of specified days below, based on the date the account was disabled

For this setting, you can choose not to automatically delete disabled accounts, or delete after a set period of time.

Synchronize Security Group Memberships, and User Account status at:

Synchronizing of Active Directory security group memberships, and the status of user accounts (either enabled, disabled or deleted status), can be done either once a day or more frequently if required, by choosing the appropriate option here.

When synchronizing Security Groups, or querying the status of an AD User Account, pause for (x) seconds between consecutive calls to Active Directory:

So the Passwordstate Windows Service doesn't perform too many consecutive queries to Active Directory too quickly, you can add a pause for this.

Performance Tip: If you have many Active Directory User Accounts added to Passwordstate, the synchronization of the features above will perform significantly better if these user accounts belong to one or more Security Groups, and these Security Groups have also been added to Passwordstate via the page Security Groups. The reason for this performance improvement is because all the users can be enumerated with one call to Active Directory for the Security Group, instead of making separate calls for every single account. If you have many AD users added to Passwordstate (i.e. 200+), it is recommended you add one or more Security Groups even if you don't use them to apply permissions anywhere.

2.31.3 Allowed IP Ranges Tab

The Allowed IP Ranges Tab allows you to specify a range of IP Addresses where clients are allowed to access the Passwordstate web site, make calls to the Passwordstate API, or access to the Emergency Access login page.

Specifying IP Ranges can be done in the following format:

- 192.168.1.* (all addresses in the range of 192.168.1.0 to 192.168.1.255)
- 192.168.*.* (all addresses in the range of 192.168.0.0 to 192.168.255.255)
- 192.*.*.* (all addresses in the range of 192.0.0.0 to 192.255.255.255)
- 192.168.1.1-192.168.2.50 (just the addresses in the range of 192.168.1.1 to 192.168.2.50)
- 192.168.1.50 (just a single IP Address)

Note 1: Regardless of the settings you specify here, you will always be able to access
 Passwordstate if logged into your web server directly, or via the Emergency Access account
 Note 2: If making an API call from an IP Address which is not authorized, then API will return a HTTP Status Code of 403 - Forbidden

You can set the Allowed IP Ranges separately for each of the 3 features (web site, API and Emergency Access Login), and the features below are also possible for further restricting access to the Passwordstate web site.

If the Passwordstate web site is accessed outside of one of the IP Ranges listed above, force the user to authenticate using the following method

If you would like to choose a different authentication method when your users our outside of your internal network, then you can choose the option from here.

By default, access from IP Addresses which aren't listed as 'Allowed' will be blocked. By selecting an authentication option instead, you can enforce a different authentication mechanism. This is a

more secure option if you use Passthrough Authentication within the office, but want to further secure access to Passwordstate when outside of the office.

Authentication Option:	Deny Access Altogether	-		
API Allowed IP Ran pecify the Allowed IP Ran topecify the Allowed IP Ran Note : Each individual Pas	Deny Access Altogether Manual AD Authentication Manual AD and Google Authenticator Manual AD and RSA SecurID Authentication Manual AD and ScramblePad Authentication Manual AD and Email Temporary Pin Code Manual AD and AuthAnvil Authentication Manual AD and Duo Push Authentication Manual AD and Duo Push Authentication Manual AD and SafeNet Authentication Manual AD and SafeNet Authentication Manual AD and One-Time Password Manual AD and RADIUS Authentication Google Authenticator RSA SecurID Authentication ScramblePad Authentication Email Temporary Pin Code	Status Code 403 Iges by editing t	(Forbidden) will be he settings for the P	return if outside of these IP assword List, and specifyin <u>c</u>

Inactivity Time Out for sessions outside the Allowed IP Ranges above (mins)

The default Inactivity Timeout setting can be found on the <u>Miscellaneous Tab</u>. If you have restricted access to Passwordstate to specify IP Subnets/Addresses, it's also possible to specify an alternate timeout value when users are out of the office (allowed IP ranges)

2.31.4 API Tab

There are two types of APIs available in Passwordstate:

- Standard API One in which requires the use of API Keys, and is not 'user account' aware (all auditing records will be recorded as Web API Account)
- Windows Integrated API One which is integrated with Active Directory and is 'user account' aware (all auditing records will be recorded as the user account making the call)

The API tab in System Settings allows you to specify the following:

- Create various API Keys for the Standard API
- Whether API Keys are allowed to be used in QueryString URLs
- Whether or not the 'PreventAuditing' parameter on certain API calls is allowed to be used or not
- Which users are allowed to access the 'Toggle Visibility of Web API IDs' menu option on each Password List
- API Keys can also be specified per Password List. If you don't want all 'Administrators' of Password Lists to be able to create these keys, you can also restrict access on the <u>Feature Access</u> screen
- If you want to be able to use Two-Factor Authentication with your API(s).

- On the screen <u>Authorized Web Servers</u> you can also specify if either of the Standard or Windows Integrated API's are allowed to be used at all
- You can also restrict which users are allowed to use the Windows Integrated API on the <u>Feature</u> <u>Access</u> screen

	sers in Passwordstate. To mod	lify the system settings, pleas	e make changes within th	e appropriate tabs below, the	click on the 'Save' button.	
Settings:						
count discoveries nail alerts & options ssword reset options	active directory options folder options high	allowed ip ranges a	bi auditing data sts miscellaneous	authentication options mobile access options	branding check for updates password list options password options	
	proxy a system servers		, addge addang			
ommon API Setti	ngs	2				
Allow the use of the 'F	reventAuditing' parameter	when retrieving passwords	via the API:			
inable the 'Toggle Vis access to this menu): Yes ONo	ibility of Web API IDs' menu	a for users with Modify or A	dmin rights to the Pass	word List only (if set to No, al	users, regardless of their access rights, will also have	
indows Integrate	ed API Settings					
One-Time Password an	e required when making ca	lls to the Windows Integrat	ed API:			
andard API Setti	ngs					
Prevent API Keys bein Note: Specifying the Al O No O Yes	j included in the QueryStrin ग Keys in the QueryString is le	ng of the API Method call, ir ess secure than the Header Re	stead of in the Header quest)	Request:		
PFA with One-Time Pa n order to use One-Tim	ssword: 1e Password Two-Factor authe	entication when executing call	s to the Standard API, yo	u will need do:		
	ode/secret key o your 2FA App on your mobi [!]	le device, or manually type in	the displayed Secret Key			
 Generate a new barco Scan the barcode into Click on the 'Save' bu Include the 6 digit Or 	tton ve-Time Password with all call:	s to the Standard API.				
Generate a new barco Scan the barcode into Click on the 'Save' bu Include the 6 digit Or Secret Key: (not case-s)	tton ne-Time Password with all call New c ensitive)	s to the Standard API. Clear				
I. Generate a new barco S. Scan the barcode init O. Click on the 'Save' bu I. Include the 6 digit Or Gecret Key: (not case-s	tton ne-Time Password with all call ensitive)	s to the Standard API.				
1. Generate a new barco 2. Scan the barcode into 3. Click on the 'Save' bu 3. Include the 6 digit Or Geret Key: (not case-s andard API Keys	tton ne-Time Password with all call ensitive) New (s to the Standard API.				
1. Generate a new barcz 2. Scan the barcode into 3. Click on the 'Save' bu 3. Include the 6 digit Or Secret Key: (not case-s tandard API Keys Name	tton ne-Time Password with all call ensitive) Description	s to the Standard API.				
1. Generate a new barcz 2. Scan the barcode into 3. Click on the 'Save' bu 3. Include the 6 digit Or Secret Key: (not case-s Candard API Keys Name System Wide Usate	tton ne-Time Password with all call ensitive) Description The System W	s to the Standard API.	y Password List and Pass	word record related calls, for a	II Shared Password Lists	~

2.31.5 Auditing Data

To help with the performance of the User Interface, and Archive table is also used for Auditing data. Certain rules for the archival can be configured for this feature, as per the options you see below in the screenshot.

System Settings System Settings apply to all users in Passwordstate. To modify the system settings, please make changes within the appropriate tabs below, then click on the 'Save' button. Search Settings: account discoveries active directory options allowed ip ranges api auditing data branding check for updates authentication options niscellaneous mobile access options password list options password options Nease specify appropriate settings below for archiving Auditing data into the AuditingArchive table - by keeping the number of rows in the main Auditing table to a reasonable level, will help with performance of the User Interfa Auditing Archive Settings Specify the maximum number of rows you would like to keep in the Auditing table - any quantity of records exceeding this, will be moved to the AuditingArchive table 500000 (setting to 0 will disable any archiving) Archive API Auditing data daily, regardless of the number of 'active' records specified above: O Yes ⊙ No Specify what time of data the archiving occurs: 08 - Hour 10 - Minute Miscellaneous Settings Show Auditing data in the Recent Activity Grid to users with the following permissions: ✓ List Administrator ✓ Modify ✓ View ✓ Guest ✓ Security Administrator Save Save & Close

2.31.6 Authentication Options Tab

The **Authentication Options** Tab provides various settings for when your users first authenticate to the Passwordstate web site. There are multiple different types of authentication options you can choose from, and some will need extra configuring on remote systems such as the SAML or Radius options.

By Default, the authentication option you select from the **System Settings** -> **Authentication Options** tab will apply to all users in the system. The users are also able to change the authentication type under their own personal preferences, but if you do not want users to have the ability to choose their own authentication option, please consider setting up a User Account Policy (**UAP**). User Account Policies in Passwordstate are similar to Windows Group Policies - You create some settings and then apply the policy to the one or more users.

An example could be you will create one **UAP** to force one set of users to authenticate using **Google Authenticator**. You then set up a second **UAP** to apply to a second set of users who will simply log in with their Active Directory Username and Password.

More information about User Account Policies can be found further on in this manual: <u>User</u> <u>Account Policies</u>

Note 1: Certain options on this screen will be disabled by default, due to Anonymous Authentication being enabled for the Passwordstate web site in IIS

Note 2: If in the event you lock yourself out of authenticating against the Passwordstate web site for any reason, you can always use the <u>Emergency Access</u> account to gain access to the system and revert out any change.

Note 3: If using Active Directory accounts for authentication, users can also login using the userPrincipleName AD attribute for this account. If doing this, it is recommended to hide the Domain Drop down list on login screens, as this may confuse users. This setting can be found under the Authentication Options tab.

Authentication Option

There are multiple different authentication options available for when your users first access the Passwordstate web site, and they are:

AD Single Sign-On Authentication

If DNS, your browser, and the site in IIS is configured correctly, your browser should not prompt you for your account details when using this authentication method, instead it should pass your account details to the Passwordstate web site in IIS, and IIS ensures your account exists in Active Directory.

In IIS on your web server, you will need to disable Anonymous Authentication for Single Sign-On Authentication to work. First, open IIS and click on your Passwordstate website, and then select the Athentication Options button:



Now make sure you have Anonymous Authentication **Disabled**, and Windows Authentication **Enabled**:

Internet Information Services (IIS) Manager				
← → ● ► PSSERVER01 ► Sites ► p	asswordstate 🕨			
File View Help				
Connections	Group by: No Grouping			
 SSERVER01 (CLICKSEC\lsand) Application Pools Sites Default Web Site Passwordstate Passwordstateappserver PasswordstateResetPortal PasswordstateSelfDestruct 	Name Anonymous Authentication ASP.NET Impersonation Forms Authentication Windows Authentication	Status Disabled Disabled Disabled Enabled	Response Type HTTP 302 Login/Redirect HTTP 401 Challenge	

Manual Login Authentication

• With Manual Login Authentication, users can either authenticate with their Active Directory account, or Local Accounts which have been created within Passwordstate

Manual Login and Google Authenticator

- Both Manual Login and Google Authenticator is required for this option
- The QR Code for Google Authenticator can either be generated on the user's Preferences screen, or upon initial authentication of not already set. The user required the Google Authenticator app on their smart phone, or equivalent app which supports one-time password authentication

Manual Login and RSA SecurID Authentication

- Both Manual Login and RSA SecurID authentication is required for this option
- To use this authentication method, the user must have a valid SecurID account and token, and must have specified their SecurID UserID field on their Preferences screen. If not specified on the Preferences screen, you will be prompted to provide this on initial authentication

Manual Login and YubiKey Authentication

- Both Manual Login and Yubikey authentication is required for this option
- Yubico supports the following protocols OTP, OATH HOTP or OATH TOTP
- Yubico OTP protocol requires further configuration on the section below labeled 'YubiKey Authentication Settings'
- To use this authentication method, the user must select which protocol they want to use on their Preferences screen, as configure settings as per documentation provided in the Passwordstate User Manual. If not specified on the Preferences screen, you will be prompted to provide this on initial authentication

Manual Login and ScramblePad Authentication

- Both Manual Login and ScramblePad authentication is required for this option
- To use this authentication method, the user must specify their ScramblePad Pin number on the Preferences screen, or Security Administrators can do it for them on the <u>User Accounts</u> screen
- When authenticating, the user needs to enter the corresponding letter that is displayed on the screen, matching the numerals specified for their Pin Number

Manual Login and Email Temporary Pin Code

- Both Manual Login and Email Temporary Pin Code authentication is required for this option
- The user must specify on their Preferences screen, what email address they want their temporary pin code emailed to
- The length of the Pin Code, and the time in which it expires, can also be set on this Authentication Options tab screen

Manual Login and Duo Authentication

- Both Manual Login and Duo authentication is required for this option
- User's must have specified their Duo Username on the Preferences screen in order to authenticate. If you have more than one device assigned to your Duo again, you will be presented with a list of devices to choose from
- Please refer to the following document as to how to configure Duo Authentication in both the Duo Portal and Passwordstate <u>Duo Auth API Configuration</u>

Manual Login and One-Time Password

- Both Manual Login and One-Time Password authentication is required for this option
- One Time Password is a generic authentication option that can work with any software that supports it, such as **Microsoft Authenticator**.
- 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
- When using One-Time Password as your Authentication option, any new user will be presented with a QR code on their log in screen when first logging into Passwordstate. They should scan this code into their phone, and when logging in for the first time successfully, this will save the QR code into the Passwordstate database for that particular user. The user can clear this QR code under their own personal preferences, or a Security Administrator can clear the code on the user's behalf from under Administration -> User Accounts -> Open the User -> Authentication Options tab
- Clearing the code will present them with a new one to scan in, either under their own personal preferences, or on the Passwordstate log in screen.

Manual Login and RADIUS Authentication

• Both Manual Login and RADIUS authentication is required for this option

• Passwordstate can authenticate to a RADIUS server, and your RADIUS server can be configured for specific authentication methods for different accounts

Please Note: If you are using the FIPS Enabled version of Passwordstate, RADIUS Authentication is not possible - If you enforce FIPS compliance on your systems, there is currently no supported authentication protocol for communicating with a RADIUS server. PAP and CHAP use the MD5 algorithm to encode their responses, and one step in the construction of the MS-CHAPv2 response requires using the MD4 algorithm to match how NT systems hash their passwords. Neither of these algorithms are permitted by FIPS-compliant mode.

AD Single Sign-On

- When Anonymous Authentication for the Passwordstate web site in Internet Information Services (IIS) is disabled, it is possible to use any one of the Active Directory Single Sign-On authentication options available in Passwordstate
- Single Sign-On allows your browser to pass your authenticated domain credentials from your browser to IIS, which validates your authentication, and allows you to login to Passwordstate without any manual username and password authentication
- The following AD Single Sign-On and secondary authentication options are available in Passwordstate, with the same criteria mentioned above for the 'Manual Logins' being relevant here also:
 - AD Single Sign-On and Google Authenticator
 - \circ AD Single Sign-On and RSA SecurID Authentication
 - AD Single Sign-On and YubiKey Authentication
 - AD Single Sign-On and ScramblePad Authentication
 - AD Single Sign-On and Email Temporary Pin Code
 - o AD Single Sign-On and Duo Authentication
 - AD Single Sign-On and One-Time Password
 - $\,\circ\,$ AD Single Sign-On and RADIUS Authentication
- When using any of the combinations above, both authentication options can be displayed on the one screen, or split over two separate screens. See Various Authentication Options below for more information

Various Authentication Options

Some of the authentication methods above also have various options which can be set, and they are:

If one of the Manual Login authentication options are selected, auto-populate the UserID field based on the current logged in Active Directory account

If you select one of the 'Manual Login' authentication options for your users, you can automatically populate the UserID field for them if required.

If one of the Manual Login Authentication options are selected, show a 'Domains' dropdown list to form part of the UserName field

This option provides a Domain drop down list on all the Manual Login Authentication screens so the user doesn't need to type the domain prefix for their account

When Anonymous Authentication is disabled for the Passwordstate web site in IIS, make the authentication a two-step process where the user first validates their AD or Login Login Account, and then the additional Authentication option on the following screen

By choosing this option, the authentication process will be executed in two-steps - initially just authenticating the user's Active Directory Domain credentials, and then any other additional authentication options selected for their account. This is useful if users need to log into Passwordstate with more than just one account

When Anonymous Authentication is disabled for the Passwordstate web site in IIS, disable the UserID field on authentication screens so it cannot be changed

If Passwordstate is configured for Single SignO-n with Active Directory i.e. Anonymous Authentication in IIS is disabled, then you can use this option to disable the UserID field on AD Authentication screens if required.

When using Local Login accounts, disable the feature where users need to regularly change their login password

When using Local Login accounts to login to Passwordstate, be default users will be required to regularly change their login password. The frequency of the required change can vary from 15 to 90 days, depending on the strength of the password they enter. If you wish to disable this feature, you can do so by selecting 'Yes' here.

Hide 2FA Secrets on the User's Preference screen (Yubikey, One-Time Passwords, and Google Authenticator)

To further strengthen the security of Passwordstate, you can hide 2FA Secrets on the user's Preferences screen.

For either Forms Based authentication accounts, or Local Login accounts, select which Password Strength Policy the user's login passwords must adhere to

Password Strength Policies can also be used for passwords for user's accounts they authenticate with into Passwordstate - this is only local accounts, and not Active Directory ones.

Protect against brute force dictionary authentication attempts by locking out an active session after the following number of failed login attempts

You can configure the maximum number of failed login attempts, which will trigger a redirect to a brute force lockout screen for the current session. The Brute Force detection feature works for all authentication options in Passwordstate.

Please note the following with regards to the Brute Force login feature:

- In the main Passwordstate UI, Brute Force login will be tracked against the authenticating user i.e, via their UserID. So if two users are authenticating from the same IP Address, one user will not lock out another user
- After a brute force lockout, the Passwordstate Security Administrator must clear the blocked record on the screen Administration -> Brute Force Blocked IPs

When tracking failed logins for Brute Force Login detection, track by

When tracking failed login attempts, you can track based on a combination of UserID and IP Address, or just the IP Address only.

If selecting 'IP Address Only', and you are using Load Balancers or Proxy Servers, please ensure you have configured Passwordstate and your network devices for X-Forwarded-For Support.

In the event of a failed Active Directory Login attempt, delay the returned error message by the number of seconds below - to obfuscate whether the failed login was caused by an unknown account, or incorrect password

Active Directory responds with different times compared to an incorrect Username or Password. This setting allows you to mask which type of authentication failure is happening, to prevent someone knowing whether the Active Directory account exists or not

Hide the following Authentication Options on User's Preferences screen

If you wish to restrict which Authentication options user's can select on their Preferences screen, then you can do so with this Dropdown list.

Time-Based One-Time Password Settings

With Time-Based One-Time Passwords, you can specify the following settings:

Allow hardware tokens to have a maximum Clock Drift of

As hardware tokens age, then can lose time - which is known as Clock Drift. This setting allows Passwordstate to check (x) number of seconds ahead of what the current time is, to detect if there is any clock drift for the users hardware token. If there is, then the user's preferences will be updated to to reflect their token's time is out of sync with the current time.

Specify the default Time Step setting (seconds) which will apply to new user accounts added to Passwordstate

Tokens generally use 30 or 60 second time-steps, and you can specify the default value here for all new user accounts which are added to Passwordstate.

Counter-Based One-Time Password Settings

With Counter-Based One-Time Passwords, you can specify the following settings:

Specify the Look Ahead Window Size for finding a Counter match

Each time the user clicks on the button on their Counter-Based Token, it increments their counter by 1. As the token may be used for other systems as well, there needs to be a look ahead value to try and find a match. When the user successfully authenticates with a Counter-Based token, their Preferences in Passwordstate are updated again to track what this counter value is - you can edit this on the user's Preferences screen.

Specify the default number of Digits used for the One-Time Password

By default, most Counter-Based tokens use 6 digits for authentication, but this can be configured to any value your tokens support - this value is used when creating new user accounts in Passwordstate, and each user can edit their own settings if needed

YubiKey Authentication Settings

If you are wanting to use the cloud based Yubico OTP authentication option, then this requires your to obtain a Client ID and and Secret Key to use. You can get these from the following page on Yubico's web site, and you must use your YubiKey to do this - https://upgrade.yubico.com/getapikey/

Once you have done this, you can enter those details below, and then Save you changes.

Yubico also provide different API Urls as well if needed. The servers that Yubico provides are:

api.yubico.com api2.yubico.com api3.yubico.com api4.yubico.com api5.yubico.com

On Yubico's web site, they document that "These servers are hosted in different places and by different organizations."

YubiKey Authenticat	ion Settings
Please specify settings for	YubiKey OTP Authentication - this is for communicating with Yubico's API, and not needed if using either YubiKey TOTP or HOTP.
Yubico API URL:	https://api.yubico.com/wsapi/2.0/verify
Yubico API Client ID:	53247
Yubico API Secret Key:	

Primary Site's SAML2 Authentication Settings

In order to use SAML2 authentication in Passwordstate, you must specify the following settings - each of these settings can be obtained within the 'Application' configured in your SAML2 Provider account:

- Certificate Type either SHA1 or SHA256
- X.509 Certificate
- IDP Target URL
- IDP Issuer URL
- Audience Restriction (Mandatory for Azure AD and ADFS, and For Azure AD, it is the 'Identifier' value, and ADFS is the 'Relying party trust identifier' setting) generally your Passwordstate URL is specified for this.

SAML User Identifier

Passwordstate can be configured to match certain "identifiers" for a user's account i.e. UserID, Email Address or UserPrincipalName

Additional Authentication Option

If required, you can also enforce an additional authentication option on user's, once they have successfully finished their SAML Authentication

Require users to re-authenticate even when they have an active session at the Identity Provider - disables Single Sign On

When this option is set to Yes, any attempts to initiate a new session to Passwordstate, will require the user to r-authenticate to their SAML provider - even if they are already authenticated to their SAML provider. Effectively setting this option to Yes disables the Single Sign On design for the SAML specification.

Single Logout URL

If you specify a Logout URL for your SAML Provider, then when users log out of Passwordstate they will also be redirected to your SAML provider to log out of the active SAML session.

If you leave this field blank, it will end your session in Passwordstate when you log off, but it will not end your session(s) and the Identity Provider's end.

Note 1: If the user is logged out of Passwordstate based on the 'Inactivity Time Out' setting on the Miscellaneous tab, then they will be redirected to the SAML logout URL is specified here, regardless of whether SAML Authentication is enabled for their account - when Anonymous Authentication is disabled for the site in IIS, it's possible SAML Authentication can be enabled for a user via their Preferences screen, or a User Account Policy within the Administration area.

Note 2: When anonymous authentication is enabled for the site in IIS (which includes forms based authentication as well), you cannot use a User Account Policy to specify the authentication type of SAML - User Account Policies first need to validate who the user is, before the policy can be applied - which defeats the purpose of SAML.

Note 3: Audience Restriction can be any value, but most commonly your Passwordstate URL is specified here

Each SAML2 Provider has different terminology for configuring the required URLs in their 'Application', and you can view several examples in the following section - <u>SAML2 Provider</u> <u>Examples</u>

High Availability Site's SAML2 Authentication Settings

If you are also using the High Availability Module and SAML Authentication, then you only need also configure SAML settings for HA if you are using different URLs to access each of your sites. This would also require a secondary "application" setup at your SAML Providers end, so they redirection to the correct URL works.

• Certificate Type - either SHA1 or SHA256

- X.509 Certificate
- IDP Target URL
- IDP Issuer URL

RADIUS Authentication

You can also configure Passwordstate to authenticate to a RADIUS Server, by specifying the relevant field values for your RADIUS server.

Note 1: Remember to configure a 'Client' for your RADIUS Server with the Host Name or IP Address of your Passwordstate web server

Note 2: On the user's Preferences screen, they can specify what their RADIUS Username is, and then this will be used on each of the RADIUS authentication screens

Note 3: You can also set the UserName field on Authentication screens to be read-only as well Note 4: If you are using the FIPS Enabled version of Passwordstate, RADIUS Authentication is not possible - If you enforce FIPS compliance on your systems, there is currently no supported authentication protocol for communicating with a RADIUS server. PAP and CHAP use the MD5 algorithm to encode their responses, and one step in the construction of the MS-CHAPv2 response requires using the MD4 algorithm to match how NT systems hash their passwords. Neither of these algorithms are permitted by FIPS-compliant mode.

Duo Security Two-Factor Settings

Specify the Integration and Secret Key for your 'Auth API' integration settings, as well as your API HostName

Note: You must have an Enterprise Duo Security account to use this feature, and you need to create a **'Auth API'** integration for your Duo subscription via their web site. Information about configuring the API in Duo's portal can be found here <u>Duo Auth API Configuration</u>

Make the Duo Push Username field on the login screen read only

This option prevents a user from walking up to another user's computer, authenticating with their own Duo Push Username, but then logging into Passwordstate as the other user - this can happen when the Passthrough authentication occurs after the Duo Push authentication happens

Email Temporary Pin Code Settings

The Temporary Pin Code Settings allows you to specify the length of the Pin Code, and also how long until the temporary Pin Code will expire if not used.

Minimum ScramblePad Pin Length

By default, the ScramblePad Pin length is 4 characters, but can be changed if required.

2.31.6.1 Duo Auth API Configuration

In order to use the Duo Authentication feature, you must have an Enterprise account with Duo Security, and your need to create an 'Auth API' Application in the Duo Portal, so you can add these settings into Passwordstate. The following instructions will show you how to do this.

• First, login to your Duo Portal, and click on the 'Applications' menu

Applications			+ Protect an Application
			٩
Name 🔨	Туре 🛇	New User Policy 🛇	Additional Information
Passwordstate	Auth API	Require Enrollment	
Show 25 • applications 1–	1 of 1 total		« < 1 > »
	© 2015 Duo Security. /	All rights reserved. Terms of service	

• Click on 'Protect an Application'

• Chose the 'Auth API' Application

Protect an Application			
Filter by keywords: VPN, Microsoft, SAML			
Array	Array SSL VPN Protect this Application Read the documentation		
əyə	Auth API Protect this Application Read the documentation		

• Create the Secret Key and Name the Auth API as appropriate

Auth API	Authenticatio	on Log × Remove Application
(j) See the <u>Auth API documentation</u>	to integrate Duo into your custom application.	
Details		Reset Secret Key
Secret key DIYVSHE4VU Secret key Click to to Don't write d API hostname api-0e51fe	JYLRCFM1574 riew. own your secret key or share it with anyone. sc9.duosecurity.com	
Settings		
General Type Auth AP	1	
Name Passw	ordstate	
Duo Push Username normalization No cl	n users will see this when approving transactions. ne bases are made to the username	

• Now in Passwordstate, select the appropriate authentication option you want, and populate the Duo Two-Factor Settings section.

ive directory options	allowed ip ranges	api auditin <u>o dat</u>	a authentication option	s branding	check for updates	email alerts & options	folder options
h availability options	hosts miscellane	ous mobile acces	s options password list	ontions nassw	ord ontions pass	word reset options	folder options
xv & syslog servers	self destruct messages	usage tracking	user acceptance policy				
	Jen det net met dy						
lefault authentication op	tion in Passwordstate is 'Pa	assthrough AD Authentio	cation'. This authentication op	tion automatically pa	sses your domain cred	entials from the browser to the	Passwordstate we
and does not require any	input from the user.	5		51	,		
2							
eb Authentication	Options						
ease specify which 'Syste	em Wide' Authentication m	nethod will apply to use	rs who do not have any optior	is selected as per of	their 'Preferences' or via	a a 'User Account Policies'.	
hoose Authentication (Option:						
Manual AD Authenticatio	n	•					
Annual AD and AuthAnu	il Authontication						
Manual AD and AuthAnv	hontication						
Manual AD and EafoNot	Authentication	lected, auto-populate the UserID field based on the current logged in Active Directory account: (only possible if the Anonymous					
Manual AD and One-Tim	A Dassword	_					
Manual AD and DADIUS	Authoritication						
Vanual AD and VubiKey	Authentication	lected, show a 'D	omains' dropdown list to fo	rm part of the User	Name field:		
Socale Authenticator	Authentication						
Sougle Authenticator	ion						
CrambleDad Authenticat	tion	asswordstate, and Passthrough Authentication is not selected, make the authentication a two-step process where the user first rthentication option on the following screen:				he user first	
imail Tomporary Din Cod							
mail temporary Pin Cou	e						
AuthAnvii Authentication							
Duo Authentication		asswordstate, and only Windows Authentication is enabled in IIS, disable the UserID field on authentication screens so it cannot		s so it cannot			
SafeNet Authentication							

Duo Security Two-Factor Settings						
Enter your Duo Sec	Enter your Duo Security Authentication API settings below.					
Integration Key : Secret Key :	[]•				
API HostName :	api-0e51fec9.duosecurity.com					
Make the Duo Username field on the login screen read only:						

• And on the user' Preferences screen in Passwordstate, on the 'Authentication Options' tab, just must have the Duo username matching the UserName which has been created in the Duo Portal.

2.31.6.2 SAML2 Provider Examples

Following are some example of how you enable SAML2 to authenticate to different Providers.

Okta.com URLs

Below is an example of the URLs to use in 'Application' you've created in the Okta.com portal.

- Single Sign On URL <u>https://<YourURL>/logins/saml/default.aspx</u>
- Recipient URL <u>https://<YourURL>/logins/saml/default.aspx</u>
- Destination URL <u>https://<YourURL>/logins/saml/default.aspx</u>
- Audience Restriction <u>https://<YourURL></u> (but can be any value you like you also need to set this value in Passwordstate as well if you want to validate this attribute)
- Default Relay State <a href="https://<YourURL>/logins/saml/default.aspx">https://<YourURL>/logins/saml/default.aspx

OneLogin.com URLs

Below is an example of the URLs to use in 'Application' you've created in the OneLogin portal.

- RelayState <u>https://<YourURL>/logins/saml/default.aspx</u>
- Audience <u>https://<YourURL></u> (but can be any value you like you also need to set this value in Passwordstate as well if you want to validate this attribute)
- Recipient <u>https://<YourURL>/logins/saml/default.aspx</u>
- ACS (Consumer) URL Validator <u>^https:///YourURL/logins//saml//default.aspx//\$</u>
- ACS (Consumer) URL <u>https://<YourURL>/logins/saml/default.aspx</u>

Active Directory Federation Services 3.0 (ADFS)

Below are some instructions for configuring ADFS to use with Passwordstate's SAML authentication option.

Important: ADFS requires you to specify the Audience Restriction SAML Attribute on your System Settings -> Authentication Options tab, to match what you have specified in the 'Relying party trust identifier' setting you see below.

Active Directory Federation Services 3.0 Relying Party Trust Configuration for Passwordstate SAML2 Authentication

- Right click on "Relying Party Trust" in "AD FS Management" under "Trust Relationships" and select "Add Relying Party Trust..."
- Click "Next"
- Select "Enter data about the relying party manually"
- Enter a display name, this is visible to end users depending on whether they use the Passwordstate URL directly, or login via the ADFS Idp login (no one uses this)
- Select "AD FS profile" (SAML 2.0)
- Do not configure a certificate
- Select "Enable support for the SAML 2.0 WebSSO protocol." For the URL, use the following format <u>https://<YourURL></u>/logins/saml/default.aspx
- For the Relying party trust identifier, enter the URL of the passwordstate instance: <u>https://<YourURL></u>
- Configure Multi-Factor authentication if necessary.
- Configure Issuance Authorization Rules if necessary.
- Click "Next"
- Leave "Open the Edit Claim Rules dialog for this relying party trust when the wizard closes" and click "Close"
- Click "Add Rule..."
- Select "Send LDAP Attributes as Claims" and click "Next"
- Enter a name for the "Claim rule name"
- Select "Active Directory" from the "Select an attribute store..." drop down
- Select "E-Mail-Addresses" under "LDAP Attribute (Select or type to add more)"
- Select "Name ID" under "Outgoing Claim Type (Select or type to add more)"
- Click "Finish"
- Click "OK"
- Right click on the new Relying Party Trust and select "Properties"
- Select the "Endpoints" tab
- Select the only SAML Assertion Consumer Endpoint entry and select "Edit"
- Check the box "Set the trusted URL as default"
- Click "OK"
- Select the "Advanced" tab
- Select "SHA-1" or 'SHA-256" from the "Secure hash Algorithm" drop down
- Click "OK"

Passwordstate SAML2 Configuration for ADFS

- Right click the "Token-signing" certificate in "Certificates" under "Service" in "AD FS Management"
- Select "View Certificate..."
- Select the "Details" tab
- Select "Copy to File"
- Click "Next"
- Select "Base-64 encoded X.509 (.CER)"
- Click "Next"
- Select a file path to save the certificate
- Click "Next"
- Click "Finish"
- Click "OK"
- Open the .CER certificate file with Notepad or another text based editor.
- Copy all of the text in the file
- Go to "authentication options" in "System Settings" in "Administration" in Passwordstate
- Paste the text from the .CER file in "X.509 Certificate:" under "SAML2 Authentication Settings"
- Set "IDP Target URL" to "https://<YourADFSURL>/adfs/ls/idpinitiatedsignon.aspx? loginToRp=<u>https://<YourURL></u>"
- Set "IDP Issuer URL" to "http://<YourADFSURL>/adfs/services/trust"

Azure Active Directory

When logged into your Azure Dashboard, you need to create a new 'Non-Gallery Application' in the 'Enterprise Applications' area as per the screenshots below.



■ Microsoft Azure	
Home > msandfordclickstudioscom (Defau	ult Directory) Ov
i msandfordclickstudiosco	m (Default [
	👁 Switch d
0verfinew	Overview
🚀 Getting started	
🗙 Diagnose and solve problems	msand msandfordcl
Manage	Tenant ID 7
🚨 Users	
🎎 Groups	💝 Az
🏮 Organizational relationships	Status N
🚨 Roles and administrators	
👢 Enterprise applications 🗙	Last sync
Devices	
App registrations	
Identity Governance	
Application proxy	Sign-ins 4
🔓 Licenses	3.5
🚸 Azure AD Connect	3
📮 Custom domain names	2.5
③ Mobility (MDM and MAM)	1.5

≡ Microsoft Azure					
Home > msandfordclickstudioscom (Defau	It Directory) > Enterprise application	ons All applications			
Enterprise applications A msandfordclickstudioscom (Default Directory)	All applications Azure Active Directory				
«	+ New application ≡≡ C	Columns			
Overview	Try out the new Enterprise A	pps search preview! Click to enable t	he preview. \rightarrow		
() Overview					
🗙 Diagnose and solve problems	Application Type	Applications status	Application visibility	Apple	Poset
Manage	Enterprise Applications	Any	Any	Арріу	Reset
All applications	First 50 shown, to search all of	your applications, enter a display	hame or the application ID.		
Air applications	Name				Homepa
Application proxy					



Add your own application	
Name * 🛈	
Passwordstate	~
Once you decide on a name for your new application, click the "Add" button below and we'll walk you through some simple configuration steps to get the application working.	
Supports: (i)	
SAML-based single sign-on Learn more	
Automatic User Provisioning with SCIM Learn more	2
Password-based single sign-on Learn more	_
Add	





With the fields you see below, these map to certain fields within Passwordstate on the screen Administration -> System Settings -> Authentication Options tab -> Primary Site's SAML2 Authentication Settings. Below is a table which summarizes these mappings.

Important 1: If you also use the High Availability Module of Passwordstate, where the HA server uses a different URL compared to your primary Passwordstate web site, then you will need a secondary SAML Application in Azure AD, and you need to specify settings in the section 'High Availability Site's SAML2 Authentication Settings' in Passwordstate.

Important 2: Azure AD requires you to specify the Audience Restriction SAML Attribute on your System Settings -> Authentication Options tab, to match what you have specified in the 'Identifier' setting you see below.

Basic SAML Configuration

Azure AD Field	Passwordstate Field
Identifier (Entity ID):	Audience Restriction (normally your Passwordstate URL)
Reply URL:	https://passwordstate.mydomain.com/logins/saml/default.aspx
Sign on URL:	https://passwordstate.mydomain.com
Relay State:	https://passwordstate.mydomain.com/logins/saml/default.aspx
Logout Url	If you want Azure AD to redirect back to a logout page in
	Passwordstate, you would specify the URL of
	https://passwordstate.mydomain.com/loggedout.aspx here

User Attributes & Claims

Azure AD Field	Passwordstate Field
Unique User Identifier:	Select which field in Passwordstate you want to compare against. In
	Passwordstate, this setting is labeled as "Select which field in
	Passwordstate you want to compare against the SAML Response's
	Name Identifier - NameID"

SAML Signing Certificate

Azure AD Field	Passwordstate Field	
Certificate (Base64):	X.509 Certificate	

Set up Passwordstate

Azure AD Field	Passwordstate Field
----------------	---------------------

Login URL: Azure AD Identifier: Logout URL: IDP Target URL IDP Issuer URL Single Logout URL

Set up Single Sign-On with SAML

Read the configuration guide 🖉 for help integrating Passwordstate.





And finally in Azure, you need to grant users access to this 'Application'.

Google Workspace / GSuite

When logged into your Google Dashboard, click on the **Apps** button:



Click the **SAML Apps** button:

\equiv Google Admin	Q Search for u			
Apps				
G Suite		Additional Google	G Suite Marketplace apps	SAML apps
G Suite Core services		Blogging, photos, video, social tools and more	Add and manage third party apps	Manage SSO and User Provisioning
12 SERVICES		55 SERVICES	NO SERVICES MANAGE	1 SERVICE
		-		

Next, click the **Add a Service** button:

Status 🔺	Certificate
	No services/Apps configured for SAML. Add a service/App to your domain

Set up your own **Custom App**:



Click Next:

Step 2 of 5 Google IdP Infor	mation	×
Choose from either option config for the service prov	n to setup Google as your identity provider. Please add details in th rider. Learn more	ne SSO
Option 1		
SSO URL	https://accounts.google.com/o/saml2/idp?idpid=C03yrzeuk	
Entity ID	https://accounts.google.com/o/saml2?idpid=C03yrzeuk	
Certificate	Google_2025-10-22-102349_SAML2.0	
Continuate	Expires Oct 22, 2025	
	▲ DOWNLOAD	
	OR	
Option 2		
IDP metadata	▲ DOWNLOAD	
		X

Name your App and click Next:

Step 3 of 5		×
Please provide the basi viewed by end-users of	on for your Custom App c information needed to configure your Cus the application.	tom App. This information will be
Application Name *	Passwordstate	app-id: passwordstate
Description		
upload logo	This logo will be displayed for all users wh	no have access to this application.
	Please upload a .png or .gif image of size	256 x 256 pixels.
PREVIOUS		CANCEL NEXT

Enter your ACS URL and Entity ID as follows, but substitute in your own Passwordstate URL. Example is <u>https://passwordstate.contoso.com/logins/saml/default.aspx</u>. Also ensure you set the Name ID and Name ID Format as per screenshot below, and click Next:

Please provide service ID are mandatory.	provider details to configure S	SO for you	r Custom App. The AC	S url and Entity
ACS URL *	https://passwordstate8.1	nalox.net/lo	gins/saml/defaı	
	ACS URL has to start with I	https://		
Entity ID *	https://passwordstate8.h	nalox.net		
Start URL				
Signed Response				
Name ID	Basic Information		Primary Email	
Name ID Format	EMAIL	~		
			×	
				\mathbf{N}

Click Finish:

Step 5 of 5 Attribute Mapping	
Provide mappings between service provider attributes to available user profile fields.	
Some providers require you to map application attributes to user fields. You should check the application's documentation to see if this is required. You can always come back later to complete the mapping.	
There are currently no mappings for this application	
ADD NEW MAPPING	
PREVIOUS CANCEL FINISH	

You should now turn on this App for all users in your Google Workspace. To do this, first click on this text:

To make the managed app available to select use	ers, choose a group or organizational unit. Learn more		
View details			
OFF for everyone			
Service provider details			~
	ACSTID	Entity ID	Ť
Google_2025-10-21-165349_SAML2_0	https://sandbox.halox.net/logins/saml/default.aspx	https://sandbox.halox.net	
(Expires Oct 22, 2025)			
SAML attribute mapping			
Map Google directory user profile fields to SAMI	service provider attributes Learn more		
······································			

And now select **On for Everyone** and click **Save**:

n all organizational units		
		^
ON for everyone		
O FF for everyone		
() Changes may take up to 24 hours to propagate to all users.		
	1 unsaved change CANCEL	SAVE
	 all organizational units ON for everyone OFF for everyone Changes may take up to 24 hours to propagate to all users. 	 all organizational units ON for everyone OFF for everyone Changes may take up to 24 hours to propagate to all users.

Now click Download MetaData:

SAML	Service provider details			^
G Passwordstate	Settings	SSO configuration ACS URL and entity ID are required		
TEST SAML LOGIN		ACS URL *		
■ DOWNLOAD METADATA ▲		https://passwordstate8.halox.net/logins/saml/default.aspx		
DELETE APP		Entity ID * https://passwordstate8.halox.net		
		Start URL		
		Certificate Select a certificate for this app		
		Certificate		
		Google_2025-10-21-165349_SAML2_0 (Expires Oct 22, 2025)		
		Manage certificates		
		Name ID		
		Name ID format		
		EMAIL		Ţ
		Name ID		
		Basic Information > Primary email		
			CANCEL	SAVE

You'll then use this Metadata as follows in Passwordstate, under Administration -> System Settings -> Authentication b -> Primary Site's SAML2 Authentication Settings:

	Download metadata
Primary Site's SAML2 Authentication Settings Please specify settings for your SAM2 Proceed bolls of ryour Primary instance of Passwordstate. Select which field to Encouncidate you want to compare against the SAML Response's Name Identifier - NameID; (this is also used for other SAML Settings below as well). Chef MAIL Authentication is complete, require users to also perform the selected authentication option below: (this is also used for other SAML Settings below as well). Setext which field to Encouncidate you want to compare against the SAML Response's Name Identifier - NameID; (this is also used for other SAML Settings below as well). Setext which field to Encouncidate you want to compare against the SAML Response's Name Identifier - NameID; (this is also used for other SAML Settings below as well). Setext which field to Encouncidate you want to compare against the SAML Response's Name Identifier - NameID; (this is also used for other SAML Settings below as well). Setext which field to Encouncidate you want to compare against the SAML Response's Name Identifier - NameID; (this is also used for other SAML Settings below as well). Setext which field to Encouncidate you want to compare you want to compar	Download Interaction To configure single sign-on (SSO) for SAML apps, follow your service provider's instructions. Learn more Option 1: Download IdP metadata Download METADATA OR Option 2: Copy the SSO URL, entity ID, and certificate SSO URL https://accounts.google.com/o/sam/2/idp/idp/id-003yrzeuk Intps://accounts.google.com/o/sam/2/idp/idp/idp/idp/idp/idp/idp/idp/idp/idp
	SHA-256 fingerpint 19:50;#574178;#54;46;4541 3:06:24:24:E0:20:19:F2:16:88:B0:B9:12 CLOSE

2.31.7 Branding Tab

The Branding Tab allows you to hide/show the Passwordstate Build Number at the top of the screen, specify your own custom Logos to use at the top left-hand side of the page, and on various Dialog windows, as well as your own custom Page Titles.

The following branding options are available:

- Show Passwordstate Build Number you can show this build number to all users of Passwordstate, or just Security Administrators
- Main Page Title and Logo Change the Passwordstate logo to your own custom logo, plus the Page Title displayed in Tab of your browser
- Dialog Title and Logo Change the Passwordstate logo in each of the Authentication Dialog windows, plus the Page Title
- Color Scheme Change the color scheme you see in Passwordstate the Base color, as well as your own custom CSS styling as well if needed
- Background Image for Authentication Screens if you want to display a custom background image on each of the Passwordstate Authentication screens, you can do so by uploading an image on the screen

Note 2: The logos are stored within the database, and restarting the Passwordstate Windows Service will recreate the logos on the file system if they are accidentally deleted for any reason.

You can also change the default colors in Passwordstate, by specifying your own 'Base' color, and Page Background color. <u>User Account Policies</u> can also be used to apply different colors for different sets of users.

Base Color		Custom CSS
Please select the Base Color to use thro	oughout Passwordstate.	If you would like to customize certain CSS for Passwordstate as well, you can by creating a file called
Apex Base Color: #0080af	Pefault color is #0080af.	You may also need to include the '!important' rule on your css styling, so they take precedence over existing styling in Passwordstate.

2.31.8 Check for Updates Tab

The Check for Updates Tab allows you to specify how frequently the Passwordstate web site should check for new updates, and who it should display the new build notification to.

This feature queries the following file - <u>https://www.clickstudios.com.au/NewBuildInfo.xml</u>, and if a new build is found, the notification will be displayed at the top left-hand side of the screen, just next to the main logo.

Note: Depending upon your environment, you may need to specify proxy authentication details on the <u>Proxy & Syslog Servers Tab</u> for this feature to work.

2.31.9 Email Alerts & Options Tab

The Email Alerts & Options Tab allows you to specify your email servers settings, so emails can be generated from Passwordstate, as well as multiple settings and notifications relating to emails being sent.

Send email alerts to Security Administrators (who have User Accounts role) for Failed Login Attempts, for the following conditions

When their are failed login attempts, Security Administrators can be emailed based on either of the following options. Failed login attempts are also recorded and reportable on the Auditing screens.

- 1. Every failed login attempt
- 2. Only when Brute Force login threshold is reached

With the Self Destruct Message feature, and Emailing Permalinks, send these emails via the Email Address of:

When sending emails for Self Destruct messages or for password permalinks, you can choose to send the emails on behalf of the user who is sending the emails, or via the mailbox configured on this screen. If you wish to send via the user, they must have an email address associated with their account.

Alert Security Administrators if there are an excessive number of events (from a single user) for Viewing, Copying or Exporting Passwords. Alert if the following condition is met

Another option which alerts to uncommon behavior is to notify Security Administrators when an individual user is viewing, copying or exporting a lot of password data within a set period of time i.e. if a user views 10 password records within a single minute, then this is not common behavior and you may have an issue with potential information leakage/theft.

When users 'Request Access' to Passwords or Password Lists, in addition to emailing the request to Password List Administrators, also email it to Security Administrators with the following roles

By default, Password or Password List Access Requests are routed to the Administrators of the relevant Password Lists. If you would also like the access requests to be sent to various Security Administrators, you can use this option to choose which Security Administrator roles will receive the requests

When users 'Request Access' to Passwords or Password Lists, if there are no Administrators assigned to the Password List, email the request to Security Administrators with the following roles

It's possible that there may be no 'Administrator' permissions assigned to a Password List for your users - only Modify or View permissions. If this is the case, someone needs to be notified when users request access to passwords in a Password List which is configured this way. You can use this option to specify where the request is routed i.e. which Security Administrators will receive the 'Request Access' email and popup notification.

Send email alerts to Security Administrators (with the following role) when passwords are exported

If you would like to alert your Security Administrators when users are exporting password data, you can use this option to do so.

2.31.10 Folder Options

The Folder Options tab allows you to specify various settings for Folders within the main Navigation Tree.

When creating nested Folders, users must have the following permissions on the parent Folder (Admin access is always allowed)

By default, if a user had Administrator access to a Folder, then they can created nested Folders beneath it. If the user either has View or Modify access to the folder, then this setting allows you to specify if they are allowed to create any other Folders beneath it.

2.31.11 High Availability Options Tab

If you have purchased the High Availability option for Passwordstate, the High Availability Options Tab allows you to specify the following settings:

• How frequently the High Availability instance should check for new or updated logos and custom images. If there are any new or updated images, they will be written to disk on the schedule provided

 When a user accesses the High Availability instance of Passwordstate, you can send email alerts to Security Administrators with the selected following role(s). This is useful as it gives you the opportunity to investigate why the user is accessing the High Availability instance, when they should be accessing the Primary instance.

Note: If you are using an Active/Passive configuration for High Availability, your HA instance will be 'Read-Only' for users. When in Read-Only mode, all actions are still audited, with audit data being merged back into the primary database. Even if the primary database is offline, it will be merged back in later when the database is once again available.

2.31.12 Hosts Tab

The Hosts tab has a various options for default settings for newly created Hosts records, and also various connectivity settings when making connections to Hosts during Account Discovery, or Password Resets.

em Settings apply to all	users in Passwordstate. 1	o modify the system settings	, please make ch	nanges within the	appropriate tabs below, the	n click on the 'Save' button.	
ch Settings:							
account discoveries email alerts & options password reset options	active directory opti folder options proxy & syslog s	ons allowed ip ranges high availability options ervers self destruct me	api au hosts us essages usa	uditing data miscellaneous age tracking	authentication options mobile access options user acceptance policy	branding check fo password list options	r updates password options
ease specify settings for	Hosts below as appropri	ate.					
New Host Record	Default Settings						
When adding new Hos	t records into Password O Google Cloud O Hy	dstate, use the following as perV ○VirtualBox ●VMw	the Default Vir are OXen	tual Machine Ty	pe:		
Host Heartbeat P	olling						
Each Host will be polled Administration -> Passw	daily to check the online ordstate Administration	e status, during the hours spe -> Host Types and Operating	cified for the rel g Systems.	evant Operating	System. The polling hours pe	r Operating System can be	changed on the screen
If a Managed Host can	not be reached for 60	Days in a row, then	Do Nothing	○ Set the Host t	to Unmanaged ODelete the	Host	
If an Unmanaged Host	cannot be reached for	365 Days in a row, t	nen O Do Noth	ing 💿 Delete th	e Host		
For the Heartbeat Ping	Test, use a Packet Size	of 32 bytes					
For the Heartbeat Ping	Test, send 2 e	cho requests, with a timeou	it of 1000 I	milliseconds			
For the Heartbeat Ope	n Port Test, use a timed	out of 3000 millisecond	ls (port test is or	nly executed if pir	ng test fails)		
Host Connectivity	Timeout Settings	5					
Specify timeout settings	for the execution Discov	very, Reset and Password Vali	dation Scripts.				
	riod for establishing a	connection to the remote H	lost: 1000	milliseco	onds		
Specify the timeout pe	nou for establishing a						

2.31.13 Miscellaneous Tab

The Miscellaneous Tab has multiple settings which don't necessarily apply to any of the other Tabs.

Default Locale (Date Format)

Applies date formatting rules to any date fields you see in Passwordstate. If users are located in a different region to what is set system wide, they can specify their own date format as part of their 'Preferences'.

Inactivity Time Out (mins)

Allows you to specify the period in which users will be automatically logged out of Passwordstate if their session is inactive.

Specify the Base URL used in any emails generated by Passwordstate

This URL field is used for several features within Passwordstate, and must be accurate for the following features to work properly:

- Links in emails
- Browser Extensions
- Upgrading High Availability instances of Passwordstate
- Permalinks
- Self Destruct Messages
- SAML Authentication (for redirection during authentication)

Force the use of an SSL Certificate (HTTPS)

When set to Yes, if the user types HTTP into the browser address bar, they will be redirected to HTTPS - which securely encrypts all traffic between the user's browser and the web site. The API will return a 403 Forbidden message if HTTPS is not used.

Show Auditing data in the Recent Activity Grid to users with the following permissions

Beneath each Password List grid you see on the Password screens, there is a 'Recent Activity' grid. This data in the 'Recent Activity' grid is all auditing data specify to the Password List you are viewing. You can choose to hide this grid be deselecting the relevant role for this setting.

When expanding/collapsing nodes in the Passwords Navigation Tree, show a loading animation icon when the count of nodes in the tree is greater than

If you have many Password Lists and Folders visible in the Navigation Tree for your users, there may be a small delay in expanding/collapsing tree nodes. If this is the case, you can display a loading animation icon during the expand/collapse process - so your users are aware something is in progress. This generally isn't required, but may be desirable if you have 500+ Password Lists/Folders.

When generating a password based on a Password Generator Policy, perform the following number of retries to ensure the password meets the strength of the selected Password Strength Policy

When using the Password Generator feature to generate new passwords for a Password List, the Password Generator tries to create a password which matches the Password Strength Compliance level set for the Password List. Depending on the settings for the selected Password Generator Policy, it's possible the generating of passwords may get itself in an endless loop trying to match the Password Strength Compliance level, so this setting tells the generator when to give up trying and simply use the last generated password.

Enable the -UseSSL parameter in PowerShell scripts for the Invoke-Command cmdlet

Enable the -UseSSL parameter for PowerShell script usage, which uses the Secure Sockets Layer (SSL) protocol to establish a connection to the remote computer.

WS-Management encrypts all PowerShell content transmitted over the network. The UseSSL parameter is an additional protection that sends the data across as HTTPS, instead of HTTP.

Please see following Microsoft documentation for more information - <u>https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.core/invoke-command?view=powershell-7.3</u>

Use regular expressions when matching 'Bad Passwords'

If the use of 'Bad Password' detection is enabled on the <u>Password Options Tab</u>, the use of regular expression matching means the bad password can be detected anywhere within the string, not just the bad password on it's own i.e. mypassword would be deemed as a bad password, as it contains the word password.

Prevent Security Administrators from adding themselves to Local Security Groups, and prevent them from adding new or existing User Accounts to Local Security Groups on the User Accounts screen:

If you wish to allow or restrict Security Administrators from adding their own account to any Local Security Groups, or adding accounts to Local Security Groups on the screen Administration -> User Accounts, then you can use this setting for that purpose.

In the Passwords Navigation Tree, sort alphabetically by

By default, sorting in the Passwords Navigation Tree is done by Folders first (at the top), and then Password Lists beneath them - just like a Windows File System. You can change this behavior if

required, where sorting is simply done alphabetically, regardless of Folder/Password List node type.

When displaying URL columns in grids, display the URL value as a

If you have chosen the URL field for any one of the Password Lists, there are two formats the URL can be displayed in when viewed in the Passwords grid - either a hyperlink text field, or hyperlink Icon - both of which will launch the URL when clicked on. They are displayed in the following manner:

URL
T
ftp.iinet.net.au/debian/ debian-cd /
ftp.iinet.net.au/debian/debian-cd/
www.borland.com
http://www.telerik.com
https://www.telerik.com
ftp://ftp.iinet.net.au/debian/debian-cd/

Or



Allow Documents to be uploaded into Passwordstate

If you don't want your users uploading documents into the Passwordstate database, you can set this option to No.

On the screen Administration -> Privileged Account Credentials, hide the value of the password field when editing details for a Privileged Account Credential

This option further strengthens the security of Passwordstate, by now showing passwords on the screen for these highly privileged accounts.

On the screen Administration -> Privileged Account Credentials, only allow the user to manage credentials they have been explicitly given access to

If you have multiple teams who need to add/edit Privileged Account Credentials, but each team is not meant to see or have access to each other's credentials, then this option allows this.

Purge Discovery Job History older that (x) days

If needed, you can also limit the size of documents which can be uploaded into Passwordstate

Limit the Size of Documents which can be uploaded

If needed, you can also limit the size of documents which can be uploaded into Passwordstate

Restrict Documents of Various Types

In addition to limiting the size of documents, you can also limit the type via their extensions i.e. docx, pdf, etc.

Disable the popup Guided Tour for new user accounts

If you do not wish new user accounts to see the popup Guided Tour window when they first log into Passwordstate, then you can disable this feature - the guided tour is still available under the Help menu if required.

On the Permalink screens, allow the following types of user roles to see the list of email addresses stored in Passwordstate

If you wish to hide all the email addresses registered in Passwordstate on the Permalink screens, you can restrict visibility to just Security Administrators by selecting this option

2.31.14 Mobile Access Options

The Mobile Access Options tab allows you to specify multiple settings for how the Passwordstate native apps for iOS and Android behave for your users.

In order to use the native iOS and Android Apps for Passwordstate, you must install the Passwordstate App Server. This is generally installed in your DMZ, so users have access to it when outside of the office. Please follow the instructions on the screen to install the Passwordstate App Server, and please ensure you use a purchased trusted SSL for the Passwordstate App Server's site in IIS - internal CA certificates are generally not trusted by mobile phones, which is why we recommend purchasing a SSL certificate.

Protect against brute force dictionary authentication attempts by locking out an active session after the following number of failed login attempts:

As the Mobile Access web site is generally externally accessible from your internal network, this setting will mitigate against any brute force authentication attempts by locking out authentication attempts when this setting has been reached.

When adding new permissions to Password Lists, enabled Mobile Access by default:

When adding new permissions to a Password List, you can use to enable/disable Mobile Access by selecting the appropriate option here.

Select whether you would like Passwords Masked or Visible:

You can choose whether to automatically show passwords in the Mobile App by default, or mask them. To view a masked password, you simply press and hold over the top of the masked password, and then you will be given various options.

Prevent Password Lists with "Additional Authentication" option set from being used within the Mobile App:

Password Lists have a setting where you can choose to use an additional authentication method, before getting access to the credentials in the Password List. The Mobile App does not have the same feature as the main UI, and this setting allows you to prevent, or allow, these Lists to be available in the Mobile App.

Select the Password Strength Policy the user's Master Password for Authentication must adhere to:

User's authenticate to the Mobile App using a master password of their own, which can be set on their Preferences screen. To ensure user's are using strong passwords, you can select which Password Strength Policy their master password must adhere to.

Specify the number of days the user can access their offline cache before they need to re-authenticate again to the Passwordstate App Server:

When the number of days is reached for this setting, the user's will need to re-authenticate to the Passwordstate App Server to re-synchronize their data.

Specify the URL for your Passwordstate App Server installation:

Once you have installed your Passwordstate App Server, you need to specify your URL here.

Reset App Pairing Secret for Passwordstate App Server:

This is a security feature, with the App Pairing secret being automatically created for you.

Passwordstate App Server's SSL Public Key:

This is another security feature, for mitigating against Man-in-the-middle attacks. Anytime you update your SSL Certificate for the App Server, you must re-query the SSL's public key.

F Important: Changing the Passwordstate App Server's URL, SSL Certificate, or the App Pairing secret, will require your users to rescan the Mobile App Server QR Code on their Preferences screen.

2.31.15 Password List Options Tab

The Password List Options Tab provides multiple settings which are applicable to Password Lists in Passwordstate.

Allow users to export details from their private Password Lists

If you wish to prevent users from exporting passwords from their Private Password Lists, you can do so by selecting this option.

Allow Password List Administrators to export passwords from Shared Password Lists:

If you wish to prevent users from exporting passwords from any Shared Password Lists, you can do so by selecting this option.

Select which Code Page to use when Importing or Exporting data

When importing or exporting data, you can specify the default Code Page which will be used for character encoding - A Code Page consists of a table of values that describes the character set for a particular language. By default, all Password Lists will use the Code Page you specify here, but can be changed to use a different Code Page by editing the Password Lists settings.

When creating nested Password Lists, users must have the following permissions on the parent Folder (Admin access is always allowed)

By default, if a user had Administrator access to a Folder, then they can created nested Password Lists beneath it. If the user either has View or Modify access to the folder, then this setting allows you to specify if they are allowed to create any Lists beneath it.

Modify permissions for Password Lists can

When a user is given 'Modify' permissions to a Password List, the default options allows the user to add new passwords, and edit or delete existing passwords. You can modify this default behavior by unchecking one or more options here.

To access the Recycle Bin for Password Lists, you must have the following permissions on the Password List:

With this option, you can control which users are allowed access to the Password List Recycle Bin, based on their permissions on the Password List - either Administrator or Modify rights

When users create a Password List and copy permissions from another Password List or Template, also add permissions for the user creating the Password List

When creating new Shared Password Lists, if permissions are being copied from another Password List or Template, this option allows you to also add permissions for the user who is creating the Password List - so instead of just cloning permissions, you can clone plus add the 'creator's account as well.

Hide the Inbuilt Password List Templates from all users

Passwordstate comes with some default Inbuilt Password List Templates which can be used as a basis for creating new Password Lists. If you do not want your users to use these Inbuilt Templates, this option allows you to hide them.

When administering Password List permissions from within the 'Administration' area, prevent Security Administrators from granting themselves permissions to passwords - either via their own account, or security groups which they are a member of

If you wish to prevent Security Administrators with the 'Password Lists' role from being able to grant themselves access to Password Lists via the Administration area, you can check this option.

When copying settings from a Template to a Password List, also copy the following field values

By default, the Password List Name and Description fields aren't populated when copying settings from another Password List or Template. With these two options you can choose to copy them if needed.

When copying settings from a Template to a Password List, allow a different image for the Password List to be selected

If you want to be able to select a different image to be associated with a Password List when copying settings from a Template, then set this option to Yes

Allow users to copy/move/link passwords to Password Lists which they have View access to

It's possible for your users to copy or move passwords around between different Password Lists they have access to. By selecting this option, you allows them to copy/move/link passwords into Password Lists they only have View Access to. If deselected, they will only be able to do so to Password Lists they have Modify or Admin access to.

When copying/moving/linking passwords between Password Lists, allow users to view all Password Lists, not just the ones they have access to

When your users copy/move/link passwords between different Password Lists, by default they will only be able to see the 'destination' Password Lists on the screen which they have been given access to. It's possible you may have a requirement to allow them to copy/move/link into Password Lists they don't have access to, and by selecting this option they will be allowed to do this.

When searching for users in order to grant them access to Password Lists, only show users who are in the same Security Groups as the person granting the access

In the main 'user' screens of Passwordstate (i.e. not the Administration area), there are various screens where you can apply permissions for users accounts. By selecting this option, they will only be able to see/search for users who are in the same Local or Active Directory Security Groups as themselves - as they are recorded in Passwordstate.

When creating new Shared Password Lists, if there is a User Account Policy or a User Preference setting which copies settings/permissions from a Template, allow the user to override these setting

It's possible for users via their Preferences screen, or Security Administrators via a User Account Policy, to specify which template settings to be used as a basis for newly created Shared Password Lists. If one of these settings are in place for the user, this option allows them to specify a different template if needed

When creating new Private Password Lists, if there is a User Account Policy setting which copies settings from a Template, allow the user to override these setting

It's possible for Security Administrators via a User Account Policy, to specify which template settings to be used as a basis for newly created Private Password Lists. If this User Account Policy is in place for the user, this option allows them to specify a different template if needed

When creating a new Password List, and copying settings from a Template, automatically select the option to link the Password List to the Template

When creating a new Password List, and you copy settings from an existing Password List Template, you can choose to automatically link the Password List to the template if required.

When creating a new Password List, and the settings are being Linked to a Template, allow users to uncheck the option for linking it to the Template

If you want to enforce a Password List to be linked to a template, then you can set this option to No - the user's will then not be able to uncheck the option which links the Password List

When a new User Account is added to Passwordstate, automatically create a Private Password List for the user

If you would like all new User Accounts added to Passwordstate have a Private Password List created for them, you can set this option to Yes - and also name what the Password Lists should be titled as. Users can then make modifications to settings on these Password Lists when they first access them if required

When a new User Account is added to Passwordstate, automatically create a Shared Password List for the user

Similar to the above feature, you can also create a new Shared Password List for the user, when their account is created/added into Passwordstate

Hide the 'Password Last Updated' column on each of the Password Grids

If you do not want the 'Password List Updated Column' showing in each of your Password Lists, you can set this option to 'Yes'.

Show the Account Types label next to the Image within each of the Password Grids

In each of the different Password Grids, it's possible to display the Account Type column. In this column you can show just the image for the Account Type, or the image and the label for the Account Type

Allow permissions to be applied multiple times for a user/security group to the same Password, Password List or Folder

Under certain circumstances, you may wish to allow the application of multiple permissions to a Password List, Password record or Folder, for user accounts or security groups. If this is a requirement, you can check this option.

Allow users to view Password List and Folder permissions when they are not Administrators of the Password List

Under each Password List grid there is a drop-down list called 'List Administrator Actions'. The majority of options in this drop-down list are only accessible to Administrators of the Password List. If a user does not have Administrators rights to the Password List, it might still be useful if they can see what other users or security groups have access to the Password List. By enabling this option, the 'View Password List Permissions' feature will be available to them - they will only be able to view permissions, not change them.



When a new Password List is created, apply the following permission to the user who created the list

When new Password Lists are created, the default option is to provide the user Administrative rights to the Password List. If required, you can change this default behavior to either Modify or View permissions

When new Shared Password Lists are created, grant Security Administrators with the selected role below admin rights to the Password List

As new Password Lists are created, you can also choose to automatically grant one or more Security Administrators of Passwordstate administrative rights to the Password Lists. You can do this by selecting the 'All Security Administrators' option, or just the ones who are assigned a specific Security Administrator role.

2.31.16 Password Options Tab

The Password Options Tab has multiple settings applicable to Password values being visible on the screen, and Bad Password detection.

Synchronize the 'Deleted' status of Linked Password records across all affected Password Lists

When Password records are copied & linked between different Password Lists, you can use this option to specify whether all of the 'linked' records are moved to the Recycle Bin when one of them is deleted. If the option is not selected, the other linked records will remain visible in each of their respective Password Lists.

Enable the 'View & Compare History of Changes' menu option for Password records for users who have the following permissions to the Password List

There is a 'View & Compare History of Changes' menu action for each and every Password record. You can control which users are allowed to access this menu, based on their permissions to the relevant Password List.

On the 'View & Compare History of Changes' screen for Password records

When viewing the History of changes to a Password record, you can choose to either show, mask, or hide the password field on the screen

Show the menu 'Copy or Email Password Permalink' in the Actions menu for Password records:

If you do not wish users to email password permalinks directly from Passwordstate, you can disable this using this option

Prevent users from using their 'Personal' Password Generator Policy settings:

If you don't want user to be able to user their Personal Password Generator policy settings, you can disable it my setting this option to no.

When adding new password records where the Password List is configured for Password Resets, do you want to automatically check the Password Reset and Account Heartbeat checkboxes

On the Add/Edit Password screens, you can choose the default behaviour for the Enabled for Resets and Heartbeat checkboxes - this will apply to all Password Lists which are enabled for resets.

When clicking on the Password Generator icon on the Edit Password screen, animate and reveal the new password to indicate to the user a new password has been generated

The intention of this feature is to make it obvious to the user they have clicked on the Password Generator icon, and that the password has changed. Please note the highlight does not occur with the Chromium Based version of Microsoft Edge.

For Password records in the Recycle Bin, automatically delete these records after the number of specified days below, based on the date the record was deleted

With this feature, you can choose to not automatically purge records from the Recycle Bin, or you can purge them after a set period of time.

With the Password Generator on the menu Tools -> Password Generator, select the following Password Generator Policy as the default:

You can also select which is the default Password Generator Policy the users can use, and prevent them from selecting a different policy as well. If a Password List is configured to 'Force' the use of a specific policy, then that setting will override this one.

With the Password Generator icon in the top right-hand side of the screen, use the following Password Generator settings to generate random passwords:

If you do not want users to use their personal Password Generator settings for the Password Generator on the top right-hand side of the screen, then you can force the use of a different one using this setting.

When users add/edit passwords, alert them when a 'Bad Password' is specified and rate it as

When your users add or edit password records, you can choose to either alert them when 'bad passwords' are detected, as per the list stored in the <u>Bad Passwords</u> screen, or you can allow bad passwords to be used. If a bad password is detected, you can specify why Password Strength indicator you would like to be assigned to the password record.

When users are 'Requesting Access' to passwords, hide the following fields due to possible sensitive information being stored in them

From the 'Passwords' menu at the bottom of the screen, users are able to request access to either Password Lists or individual Passwords they don't already have access to - assuming you have enabled this feature for them. As viewing password related data can be sensitive by its very nature, you can choose to hide various fields on the screen from your users, either the Username, Description or Notes fields.

Allow users to create password records when they only have Guest permissions to the Password List

When a user is given access to individual passwords in a Password Lists, as opposed to permissions being applied to the Password List itself, the user is given 'Guest' rights to the entire Password List. This is so the Password List will show in the Navigation Tree on the left-hand side of the main screen. By selecting this option, you will allow users who have Guest access to also create new passwords in the selected Password List.

Note: If this option is enabled a user creates a new Password record, they will be given Modify rights to the individual Password record they are creating.

Allow users to create password records when they only have View permissions to the Password List

When a user is given View access to a Password List, by default they cannot add password records to the List. By setting this option to Yes, they will be able to add new records.

Note: Even after the user adds new records when using this option, they will still only have View access to all records in the Password List

When Password masking is displayed on the grid views (*****) show a fixed character length of

It's possible to use 'Fixed Length Password Masking' in Passwordstate, as an added security measure. By using this feature, the screens which show a masked password like ***** will all be of the same length, regardless of how many characters the Password field consists of.

Automatically hide visible passwords based on the following conditions (in seconds)

By clicking on any masked passwords in the grid view, i.e. ******, or the \bigcirc icon on any of the add/edit/view password screens, the password will be revealed to you. There are 3 different options for how quickly you wish to password to again be masked, and they are:

- Set Time one set time period for all passwords, regardless of their length and complexity
- Password Complexity here you can specify 5 different time intervals, each for the different Password Strength ratings
- Password Length here you can specify up to three different time periods based on the length of the password fields i.e. if the password field is 20 characters in length, you probably would need it to be displayed longer on the screen compare to a record which is only 5 characters long

2.31.17 Password Reset Options

Passwordstate can perform Password Reset for Active Directory accounts, as well as for many other account types. The Password Reset Options tab allows you to specify various settings when updating passwords in Active Directory, and specify who is allowed to enable the 'Password Reset' option on Password Lists

Active Directory Accounts

When a password is configured as an 'Active Directory' account, and you wish to perform passwords resets for these accounts in AD, there are a couple of options you can apply here:

- To validate the password stored in Passwordstate matches what's stored in AD, before a password reset is to occur. This can act as a security measure to prevent users of Passwordstate making changes to AD accounts if they don't know what the password currently is i.e. prevents them from adding a record with any password value, and then performing a reset after that
- Enable the Password List setting of 'Show Active Directory Actions for Passwords which are enabled for Reset' If this option is enabled, then it can be selecting a part of the settings for a Password List. When selected, it will provide a new Tab on the Edit Password screen which allows you to do the following to the account in Active Directory
 - Unlock the account if locked
 - Set the option 'User must change password at next logon'
 - Disable the account
 - Enable the account
- As Active Directory Accounts can be used as 'Identities' for Windows Services, IIS Application Pools, Scheduled Tasks, etc, after an AD account has been reset, you may want to pause for a
specific amount of time before executing any associated Password Reset Tasks for the account. This would generally be used to allow your Domain Controllers to replicate changes for the account, before password resetting of any Windows Services, etc, were to happen.

Miscellaneous Settings

You can also specify what types of Password Lists can have the option 'Enable Password Reset' enabled - you can restrict this for either Private or Shared Password Lists if required

If you are also performing Password Resets and Account Validation for Oracle accounts, you can set the path to the installed Oracle Access Data Components here (ODAC) - this only needs to be modified if you've installed to a different path other than C:\oracleodp

2.31.18 Email, Proxy & Syslog Servers Tab

The Email, Proxy & Syslog Servers tab allows you to specify details for sending emails from Passwordstate, or specifying any proxy and syslog servers if required.

Mail Server Selection

Allows you to choose whether you wish to use an SMTP mail server for sending emails, or Exchange Online.

Microsoft Exchange Online Details

If you have a valid Microsoft subscription that allows you to use Exchange Online, then you can use the Microsoft Graph to send various Passwordstate emails. The instructions below show you how to configure the Graph API and grant permissions to allow mail to be sent out on behalf of a Azure AD User.

Please note, these instructions to create an Application in Azure and assign the correct permissions are only guide. Please refer to official Microsoft documentation to obtain the most current information and best practices, when it comes to using the Microsoft Graph API.

- Log into your Azure portal, and select Azure Active Directory
- Now click on App registrations menu on the left hand pane, and select "New Registration"
- Type in any name of your choice for the application you are creating, and then click Register

\equiv Microsoft Azure		
Home > Default Directory App regist	rations >	
Register an application)	
	- -	
* Name		
The user-facing display name for this appl	cation (this can be changed later).	
Demo Emails	\checkmark	
Supported account types		
Who can use this application or access this	API?	
• Accounts in this organizational direct	ory only (Default Directory only - Single tenant)	
O Accounts in any organizational direct	ory (Any Azure AD directory - Multitenant)	
Accounts in any organizational director	ory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)	
Personal Microsoft accounts only		
Help me choose		
Redirect URI (optional) We'll return the authentication response to changed later, but a value is required for r	o this URI after successfully authenticating the user. Providing this now is optional and it can be nost authentication scenarios.	
Select a platform \checkmark e	g. https://example.com/auth	
Register an app you're working on here. Ir	tegrate gallery apps and other apps from outside your organization by adding from Enterprise applications	i.
By proceeding, you agree to the Microsoft	Platform Policies 📑	
Register		

• Take note of the Application (client) ID and Directory (tenant) ID, and the click on the Add a certificate or secret link

		${\cal P}$. Search resources, services, and docs (G+/)	
Home > Default Directory App registration	ns >		
₽ Search «	🔋 Delete 🌐 Endpoints 👪 Preview features		
Cverview	Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for d	eveloper). \rightarrow	
 Quickstart Integration assistant 			
Manage	Display name : Demo Emails		Client credentials : Add a certificate or segret
📕 Branding & properties	Application (client) ID 069e0ae0-348c-408b-a564-de0f9090faef		Redirect URIs : Add a Redirect URI Add a certificate or secret
Authentication	Directory (tenent) ID 7530eedc.463b-4736.9645-9262706479c		Application ID ONI : Add an Application ID ONI
📍 Certificates & secrets	Supported account types : My organization only		managed approached in the statement
Token configuration			
 API permissions 	1 Welcome to the new and improved App registrations. Looking to learn how it's changed from App	registrations (Legacy)? Learn more	
 Expose an API 			
App roles	Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authenti Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authenti Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authenti Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authenti Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authenti Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authenti Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authenti Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authenti Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authenti Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authenti Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authenti Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authenti Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentian Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentian Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Ac	cation Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security up	dates but we will no longer provide feature updates. Applications will need to be upgraded to Mi
A Owners	Get Started Documentation		
& Roles and administrators			
Manifest		Build your application with th	e Microsoft identity platform

• Click "New Client Secret", give it a description, and expiry date and click Add

Microsoft Azure		./P Search resource	ces, services, and docs (G+/)			S 6 C	E 6 🖓 🕸 Ø	5 6 0 R
Home > Default Directory App regist	ions > Demo Emails					Add a client secret	Add a client secret	Add a client secret
🔶 Demo Emails Cert	icates & secrets 👒 …							
	R					Description	Description Demo E	Description Demo Email
2 Search c	R ² Got heedback/					Expires	Expires Recomm	Expires Recommended: 180
Controller	Credentials enable confidential applications to identify themselves to t	he authentication service when receiving tokens at a	web addressable location (using an HTTPS					
Integration assistant	scheme). For a higher level of assurance, we recommend using a certif	icate (instead of a client secret) as a credential.			L			
					Г			
Branding & properties	Application registration certificates, secrets are redevated credential	s can be found in the tabs below.	×					
Authentication				D-				
Certificates & secrets	Certificates (0) Client Crets (0) Federated credentials (0							
Token configuration	A secret string with the application uses to prove its identity when re-	questing a token. Also can be referred to as applicati	on password.					
API permissions	+ New client secret							
Expose an API	Description Expires	Value	Secret ID					
App roles	No client secrets have been created for this application							
Owners								
Roles and administrators								
Manifest								
port + Troubleshooting								
Troubleshooting								
lew support request								
					Add	Cancel	Cancel	Cancel

After the client secret is created, take note of the Value which will be used later in Passwordstate. You can only view this once when you create the secret:

Home > Default Directory App re	gistrations > Demo Emails			
🔶 Demo Emails C	ertificates & secrets 👒 …			
₽ Search	« R Got feedback?			
Overview				
n Quickstart	Got a second to give us some feedbac	$_{\rm k?} \rightarrow$		×
💉 Integration assistant				
Manage	Credentials enable confidential application scheme). For a higher level of assurance, w	is to identify themselves to re recommend using a cert	the authentication service ificate (instead of a client s	when receiving tokens at a web addressable location (using an HTTPS ecret) as a credential.
📑 Branding & properties				
Authentication	 Application registration certificates, se 	crets and federated credentia	als can be found in the tabs l	below.
📍 Certificates & secrets				
Token configuration	Certificates (0) Client secrets (1)	Federated credentials ())	
→ API permissions	A secret string that the application uses t	o prove its identity when re	equesting a token. Also ca	n be referred to as application password,
Expose an API				
App roles	+ New client secret			K
🎎 Owners	Description	Expires	Value 🛈	Copy to clipboard et ID
& Roles and administrators	Demo Email	11/19/2023	DHX8Q~G7MP41glz	XycpDj1THScDFNSy 🕅 acd9c957-3b18-47ff-bcb6-9313a14bd451 🗈 📋
🔟 Manifest				\bigcirc
Support + Troubleshooting				
Troubleshooting				
New support request				

• Now click on API Permissions, click Add Permission and the click on the Microsoft Graph button.

Microsoft Azure		P Search resources, services, and docs (G+ℓ)		5 G 🦃	@ @ <i>R</i>
Home > Default Directory App registratio	ons > Demo Emails		Request API permission	15	×
₋ Demo Emails API pe	ermissions 🖉 🗠				-
			Select an API		
Search «	Refresh A ² Got feedback?		Microsoft APIs APIs my organization	t uses My APIs	
Overview			Commonly used Microsoft APIs		
4 Quebitart	1 De Admin consent required* column shows the datent value for an organization. However, user cons	nt can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be us	ed.		
 Insegration assistant 			Microsoft Graph Take advantage of the tree	nendous amount of data in Office 365, Enterpris	e Mobility + Security, and Windows 10.
Manage	Configured permissions	the assessed sectors. The first of conferenced according to the bill industry	Access Azure AD, Excel	une, Outlook/Eschange, OneDrive, OneNote, St	sarePoint, Planner, and more through a
Branding & properties	all the permissions the application needs. Learn more about permissions and consent	ure content process, me los on comgunes permisionis situad intrave	-		
Authentication	+ Add a permission 🗸 Grant admin consent for Default Directory				
	API / Permissions name Type Description	Admin consent requ Status	Azure Batch	Azure Communication	Azure DevOps
API permissions	Microsoft Graph (1)		Schedule large-scale parallel and HPC	Rich communication experiences with	Integrate with Azure DevOps and Azure
 Expose an API 	UserRead Delegated Sign in and read user profile	No ····	appreasors in the cloud	by Microsoft Teams	Divops sever
App roles					
A Owners	To view and manage consented permissions for individual apps, as well as your tenant's consent settin	ps, try Enterprise applications.	Azure Rights Management		
 Roles and administrators 			Services	Acure Service Management	Shows marchada collaboration
III Marifest			protected content	functionality available through the Azure portal	data lake storage for unstructured and servi-structured data
Support + Troubleshooting					
New support request			Data Export Service for Microsoft Dynamics 365	Oynamics 365 Business Central	Dynamics CRM
			Export data from Microsoft Dynamics CRM organization to an external	Programmatic access to data and functionality in Dynamics 365 Business	Access the capabilities of CRM business software and ERP systems
			destration	Central	
			-	•	_
			Inture	Office 365 Management APIs	Power Automate

• Click on Application Permissions

		<u>>_</u>	Ŗ	<u>(</u> 2	ŝ	?	ନ୍ଦି		
	Request API permissions								×
is where this app will be used.	Delegated permissions Your application needs to access the API as the signed-in user. $\label{eq:poly} \Box_{\!S}$		Applic Your a signed	ation per pplication -in user.	mission	ns as a bac	kground	service or daemon without	a

• Search for "mail", tick the Mail.Send option, and click Add Permissions

	[5 tr 🖓 🕸 🕐 🖉 🥥
	Request API permissions	×
	 ✓ All APIs Microsoft Graph https://graph.microsoft.com/ Docs c³ What type of permissions does your application require? 	
anizations where this app will be useष्ट्रा. 	Delegated permissions Your application needs to access the contast the signed-in user.	Application permissions Your application runs as a background service or daemon without a signed-in user.
	Select permissions	expand all
	Permission	Admin consent required
	> MailboxSettings	
	V Mail (1)	
	Mail.Read ① Read mail in all mailboxes	Yes
	Mail.ReadBasic ① Read basic mail in ar mailboxes	Yes
	Mail.ReadBasic All O Read basic mail in all mailboxes	Yes
	MainReadWrite ① Read and write mail in all mailboxes	Yes
	Mail.Send ① Send mail as any user	Yes
	Add permissions Discard	

• Under API Permissions page, click the Grant Admin Consent for the Default Directory button

\equiv Microsoft Azure				م	Search resources, servic	es, and docs (G+/)	
Home > Default Directory App registrati	ions > Demo Emails						
_{Ə-} Demo Emails API pe	ermissions 🖈 …						
 Search « Overview Quickstart 	C Refresh R Got feedb A You are editing permission(state)	ack? ;) to your applicatio	n, users will have	o consent even if they've already done so pr	eviously.		
 Integration assistant Manage 	() The "Admin consent require	d" column shows th	e default value fo	r an organization. However, user consent ca	Se customized per permi	ssion, user, or app. This column may not reflec	t the value in yc
 Branding & properties Authentication Certificates & secrets Token configuration 	Configured permissions Applications are authorized to ca all the permissions the applicatio + Add a permission	II APIs when they n needs. Learn mo ant admin consent	are granted perr re about permis for Default Dire	nissions by user admins as part of the co sions and onsent	nsent process. The list o	f configured permissions should include	
API permissions	API / Permissions name	Туре	Description	Grant admin consent for Default Directory	Admin consent re	qu Status	
🙆 Expose an API	✓Microsoft Graph (2)						
App roles	Mail.Send	Application	Send mail as a	ny user	Yes	🛕 Not granted for Default •••	
A Owners	User.Read	Delegated	Sign in and rea	ad user profile	No		
♣ Roles and administrators ■ Manifest Support + Troubleshooting ⑦ Troubleshooting ▲ New support request	To view and manage consented p	permissions for inc	ividual apps, as	well as your tenant's consent settings, try	Enterprise applications.		

• Open any user you wish to send on behalf of, and take note of their **Object ID**. This user should have a valid email address assigned to their account:



Log into Passwordstate, and go to Administration -> System Settings -> Email, Proxy and Syslog Servers. Add in all the details of your application under Microsoft Exchange Online Details section, and click the Test Email button to confirm emails are sending. If you select the Save Emails to Sent Items option, you can log into your email client as the user you are sending emails from, and you will see any email Passwordstate sends out in their Sent items. This can be good for troubleshooting if the end user is not receiving any emails.

h Settings:		
count discoveries ac	ctive directory options allowed ip ranges api auditing da authentication options branding	check for updates
nail alerts & options	folder options high availability options hosts miscellaneous mobile access options password li	st options password options
is word reset options	entail, proxy cospond servers sen destruct messages asage dacking aser acceptance poincy	
/lail Server Selection	1	
elect the type of mail serv	ver to use within Passwordstate:	
SMTP Mail Server	v	
/icrosoft Exchange	Online Details	
Aicrosoft Exchange	Online Details onfiguration to send emails from within Passwordstate using Exchange Online via Microsoft's Graph API:	
licrosoft Exchange	Online Details onfiguration to send emails from within Passwordstate using Exchange Online via Microsoft's Graph API:	
Aicrosoft Exchange	Online Details onfiguration to send emails from within Passwordstate using Exchange Online via Microsoft's Graph API: : 069e0ae0-348c-408b-a564-de0f9090faef	
Aicrosoft Exchange of the following OAuth of the following OAuth of the following OAuth of the following OAuth of the following of the followi	Online Details onfiguration to send emails from within Passwordstate using Exchange Online via Microsoft's Graph API: : 069e0ae0-348c-408b-a564-de0f9090faef : 7530eadc-463b-4736-9f45-02627c06d79c	
Aicrosoft Exchange of the following OAuth of Application ID Tenant ID Client Secret	Online Details onfiguration to send emails from within Passwordstate using Exchange Online via Microsoft's Graph API: : 069e0ae0-348c-408b-a564-de0f9090faef : 7530eadc-463b-4736-9f45-02627c06d79c : Client Secret saved to database	
Aicrosoft Exchange (se the following OAuth of opplication ID enant ID Tient Secret Jser Object ID to Send Mail	Online Details onfiguration to send emails from within Passwordstate using Exchange Online via Microsoft's Graph API: : 069e0ae0-348c-408b-a564-de0f9090faef : 7530eadc-463b-4736-9f45-02627c06d79c : Client Secret saved to database I From : 48abb	
Aicrosoft Exchange of Ase the following OAuth of Application ID Tenant ID Client Secret Jser Object ID to Send Mail Save Emails to Sent Items	Online Details onfiguration to send emails from within Passwordstate using Exchange Online via Microsoft's Graph API:	

SMTP Mail Server Details

As various functions are performed in Passwordstate, email records will be generated and stored in the QueuedEmail table. The Passwordstate Windows Service checks this table once every minute, and sends the emails if any exist. In order for emails to be sent, you need to specify various settings for your email server. In particular:

- Host Name and Port Number
- Which SMTP address you would like the emails to be sent from
- Whether or not your email server is configured to send via TLS (Transport Layer Security)
- And if you need to specify an account to send from i.e. Sending Anonymous SMTP emails is not allowed from your email server

Note: If the account stored for this setting is also stored in a Password List which is enabled for synchronizing of passwords into Active Directory or local Windows Servers, then this password below will also be updated when a synchronization occurs.

Proxy Server Details

To check for new builds of Passwordstate, you may need to specify your internal proxy server details, and possibly an account which can authenticate with your proxy server if required.

Note 1: If the account stored for this setting is also stored in a Password List which is enabled for synchronizing of passwords into Active Directory or local Windows Servers, then this password below will also be updated when a synchronization occurs.

Note 2: If you are concerned about your Passwordstate web site accessing the Internet, the only file we access is <u>https://www.clickstudios.com.au/NewBuildInfo.xml</u>. No data can be sent or captured by reading an XML file, and you can run a program such as WireShark on your web server to confirm this is the only file Click Studio's checks

X-Forwarded-For Support

When Passwordstate adds auditing data to the database, it records the IP Address of the client who initiated an action which triggered the audit event.

As Passwordstate supports the "X-Forwarded-For (XFF) HTTP header field" for identifying the originating IP address of a client, if you use any form of Load Balancing, Firewalls or Proxy Server caching, you may need to make configuration changes to your device/appliance to ensure the correct IP Address of the client is reported, instead of the load balancer or proxy server.

You must also specify the IP Address of these devices, so they are "trusted" to add this header to the HTTP request.

Syslog Server Details

If required, you can send all Auditing data to one of your own internal SysLog servers. It is the Passwordstate Windows Service which checks every minute for new data to send, and the Windows Service keeps track of the latest auditing record which was successfully sent, and only send subsequent records.

Communication to Syslog servers can also be done over UDP or TCP, against the port number specified.

If needed, you can also modify the date/time formatting of the messages sent to Syslog servers.

Note: The only auditing data which is not sent to your syslog server, is auditing data related to Private Password Lists

2.31.19 Self Destruct Messages

The Self Destruct Messages features allows you to send password record related messages to recipients, or just general messages with what ever content you like.

There are two types of Self Destruct Message web sites which can be used, and they are:

- Embedded within your normal Passwordstate installation, or used in conjunction with the deployment of your Passwordstate App Server. In both cases here, the Self Destruct Message web site communicates directly back to your Passwordstate SQL database
- Push/Pull Deployment option. With this version, the site is installed separately to your main Passwordstate web site, or App Server, and all data to the Self Destruct Message web site is "pushed/pulled" from your main Passwordstate instance. This install of the Self Destruct message web site uses a local SQLite database, and has no requirements to communicate back to your Passwordstate web server or database.

A few notes about this feature are:

- Recipients of Self Destruct Messages does not need a license in Passwordstate in order to view messages
- The intention of the Self Destruct Message is that it will automatically be deleted (Self Destruct) if not view in the specified time period
- On this System Setting screen, there are various options for Passphrase protection on Self Destruct Messages, information about a separate install of the Self Destruct web site, and also various branding for the Self Destruct site as well i.e. logo, color scheme, and background image. When users view Self Destruct Messages, the web site is also mobile friendly.

Please follow the instructions on the System Settings screen below, if you wish to deploy the Self Destruct web site with the Passwordstate App Server, or the separate Push/Pull version.

System Settings	
System Settings apply to all users	in Passwordstate. To modify the system settings, please make changes within the appropriate tabs below, then click on the 'Save' button.
Search Settings:	
account discoveries ac email alerts & options password reset options	tive directory options allowed ip ranges api auditing data authentication options branding check for updates folder options high availability options hosts miscellaneous mobile access options password list options password options email, proxy & syslog servers self destruct messages usage tracking user acceptance policy
Please specify settings below as	s appropriate for the Self Destruct Message Site.
Self Destruct Site Inst	tallation Instructions
By default, the Self Destruct N	Vessage web site is accessible as part of an "embedded" URL within your main Passwordstate web site i.e. with /selfdestruct appended to the end of your URL.
In addition to the embedded	Self Destruct Message web site, this site can also be installed separately from your normal Passwordstate instance in two ways:
1. As part of the Passwordsta 2. As a stand-alone solution,	te Application Server install - Please click on the 'Mobile Access Options' tab above, for instructions on how to install the Passwordstate App Server where all data is "pushed/pulled" from your Passwordstate instance, to the Self Destruct web site.
Self Destruct Settings	3
Please specify settings for the	2 Self Destruct Message Web Site below as appropriate.
Enforce the use of Passphra	se protection for every Self Destruct Message sent:
Allow users to see the value	e of Passphrases when composing Self Destruct Messages:
Select default value for opt 3 days 🔹	ion 'Automatically self-destruct this message if not viewed in':
Select default value for opt Once	ion 'Allow the self-destruct message to be viewed (x) times':
Allow users to send Self De	struct Messages via the API:
Specify which users are allo	wed to use the 'Send Self Destruct Message' Actions menu item for Password records:
Send Self Destruct Message	2 Permissions
Default Passphrase:	assphrase protection is mandatory, and no Passphrase is associated with the contact you are sending a message to, then this Passphrase will be used to protect the ssage.
Separate Site URL:	cify the URL here when using a separate install of the Self Destruct Site - either your Passwordstate App Server URL, or the URL of your Push/Pull deployed site.

2.31.20 Usage Tracking Tab

The Usage Tracking tab allows you to specify your own JavaScript code to be inserted into the main /default.aspx page.

This is useful if you have your own wiki, or similar, to track page hits for your various web sites.

This feature also provides a few options for where to insert the code on the page - either within the <head> tag, or just before the end of the <body> tag.

2.31.21 User Acceptance Policy Tab

The User Acceptance Policy Tab allows you to specify a popup 'User Acceptance Policy' (UAP) which users must read when they access the Passwordstate web site.

A default body of text is provided, but it can be customized to suite your organization.

There are also a couple of options for the UAP:

- No policy Required
- Yes Mandatory for each new session (every time your users initiate a new session when they visit the site, they will be presented with the UAP popup)
- Yes Acceptance Required (Once the user has read and accepted the policy, they will not be prompted again)

2.32 User Accounts

Prior to any of your users being able to access the Passwordstate web site, you must first register their accounts in the User Accounts screen.

There 4 different ways user accounts can be added to Passwordstate, and they are:

- Adding them manually by clicking on the 'Add' button
- Importing them from Active Directory by clicking on the 'Add from AD' button
- Importing them from a csv file by clicking on the Import button
- Or, when membership of an Active Directory Security Groups is synchronized please see the <u>Security Groups</u> screen for information on this method

Performance Tip: If you have many Active Directory User Accounts added to Passwordstate, the synchronization features on the <u>Active Directory Options Tab</u> on the System Settings page will perform significantly better if these user accounts belong to one or more Security Groups, and these Security Groups have also been added to Passwordstate via the page <u>Security Groups</u>. The reason for this performance improvement is because all the users can be enumerated with one call to Active Directory for the Security Group, instead of making separate calls for every single account. If you have many AD users added to Passwordstate (i.e. 200+), it is recommended you add one or more Security Groups even if you don't use them to apply permissions anywhere.

Note 1: When you first add a user's account to Passwordstate, they will receive an email informing them they have access, and what URL to access the site with - assuming the email notification category is not disabled on the screen <u>Email Templates</u>.

Note 2: If you need to purchase additional Client Access Licenses, you can click on the 'Buy More Licenses' button and it will provide you with some instructions

otal Licen	se Co	unt: Enterprise	(Unlin	nited) 📜 🛤	vailable	License Count: I	lot A	pplicable											
Actions		UserID		First Name		Surname		Site Location		Email	Department		Office	Last Logged In	Date Created		UAP Accepted On	Enabled	Expire
			T		T		Ŧ		т	Т		T	T	Ť		ĒΤ	1 T	T	
0		halox\aagui		Abigail		Aguilar		Internal							8/11/2015 10:38	AM		×	23
0		halox\aandr		Adrian		Andrade		Internal							8/11/2015 10:38	AM		*	
0		halox\abair		Adrian		Baird		Internal						23/12/2016 2:41 PM	8/11/2015 10:38	AM	23/12/2016 2:42 PM	×	
0		halox\abark		Abigail		Barker		Internal							8/11/2015 10:38	AM		×	
0		halox\abass		Adrian		Bass		Internal							8/11/2015 10:55	AM		×	
0		halox\abrow		Abigail		Brown		Internal						7/06/2017 2:57 PM	8/11/2015 10:38	AM	7/06/2017 2:57 PM	×	
0		halox\achan		Adam		Chandler		Internal							16/02/2016 11:09	AM		×	
0		halox\afinl		Adam		Finley		Internal							16/02/2016 11:09	AM		×	
0		halox\ahend		Abigail		Henderson		Internal		testing@clickstudios.com.au					8/11/2015 10:38	AM		×	
0		halox\ahoov		Abigail		Hoover		Internal							8/11/2015 10:38	AM		×	

Once you have added the user's account to Passwordstate, there are certain functions which can be performed against it.

Local Login Accounts

When using the Active Directory Integrated version of Passwordstate, it's still possible to create Local Login Accounts, which aren't tied to Active Directory. This would only ever get used in rare circumstances when you have users wanting to use Passwordstate, but don't have an AD Account. In order to take advantage of this feature you need to:

- For the Passwordstate web site in IIS, you need to set the Authentication for the site to 'Anonymous'
- You need to add, or import via a csv file, 'Local Login Accounts' to Passwordstate these behave similar to Forms-Based accounts

Note: There are some limitations when you configure Passwordstate in this manner. In particular, user's won't be able to set their own Authentication options in the Preferences screen, Security Administrators won't be able to configure any Authentication options for a User Account Policy, and certain System Wide Authentication options will also be disabled.

User Account Actions Menu

The following 'Actions' menu items are available for a user's account:

- Delete deleting a user's account will remove all access for them, so please use with caution
- Impersonate Users Account this feature should only be used when trying to troubleshoot issues with the affected user. By selecting this option, an email will be send to the user informing them you are "impersonating" them, as we as to all Security Administrators. Audit

records are also added. When you are impersonating a user, being able to see, edit or add passwords will be disabled

- **Resend Welcome Email** if you need to resend the initial Welcome email to the user (the email they first receive when their account is first added to Passwordstate), then you can use this menu item
- Reset any Accepted UAPs for User If needed, it's possible to reset the 'accepted' status of the User Acceptance Policy for a user. The User Acceptance Policy can be configured on the screen <u>System Settings</u> -> <u>User Acceptance Policy Tab</u>
- Set Expiry Date it is possible to set a date in which the user's account can either by disabled, or deleted from Passwordstate. This is a useful feature if you know an employee is leaving the organization on a specific date
- **Toggle Status Enabled or Disabled** this will either enable or disable the user's account, preventing them from accessing the Passwordstate web site
- View Email Notifications allows you to enable/disable email notifications for the user, assuming an Email Notification Group hasn't been applied to their account

Note 1 : The status (enabled or disabled) of a user's account may also change depending on the Active Directory synchronization settings on the screen <u>System Settings</u> -> <u>Active Directory</u> <u>Options Tab</u>

Note 2 : When a user's account has been disabled, it no longer counts towards the number of licenses used

🚨 User Accounts

Listed below are all users who have been granted access to Passwordstate.

	Actions		UserID	First Name	Surname
			T		T
l	0		halox\aagui	Abigail	Aguilar
	0		halox\aandr	Adrian	Andrade
	0		halox\abair	Adrian	Baird
	0		halox\abark	Abigail	Barker
	٥		halox\abass	Adrian	Bass
		Add to	Local Security Grou	ps	Brown
	8	Delete	e de la companya de la		Chandler
	£	Imper	sonate Users Account	t	Finley
		Resen	d Welcome Email	orliser	Henderson
	Ø	Set Ex	piry Date	01 0301	Hoover
	4	Toggle	Status - Enabled or	Disabled	
_		View E	mail Notifications	Import Local //	ccounte l Export I

Editing User Account Settings

By clicking on the UserID hyperlink in the grid, you will be directed to a screen where you can edit multiple properties for the user's account.

Note 1: Any changes to a user's account will not be in effect until the user logs off, then back in to the Passwordstate web site.

Note 2: The Miscellaneous, Email Notifications and Authentication Options tabs are almost identical to what the user sees when they view their own Preferences

Note 3: <u>User Account Policies</u> may override any number of settings for the user, in which case the relevant controls on each of the tabs will be disabled

Account Details Tab

The Account Details Tab has some basic information about the user's account which you can edit, but should rarely need to be touched.

Note: At this stage it's not possible to rename a user's UserID value due to the way this field is encrypted throughout a lot of the tables in the Passwordstate database.

🖁 Edit User Detai	ls				
To modify the user's de	tails, please make ap	propriate changes	in each of the tabs below and	click on the 'Save' button.	
test tester (halox [\]	\testtester)				
account details	miscellaneous	color theme	authentication options	mobile access options	
Please specify appro	priate accounts deta	ils for the user belo	w.		
UserID	halox\testteste	r			
Site Location *	Internal			-	
First Name *	test				
Surname	tester				
Email Address	test.tester@ha	lox.net			
UserPrincipalName	testtester@hal	lox.net			
	Leave blank if r	not being used for a	authentication]	
Department					
Office					
Created	10/12/2018 10:	22 AM			
Role	🚨 Standard Ad	count			
Status	🖌 Enabled				
					Save Cancel

Miscellaneous Tab

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

Password Visibility on Add/View/Edit Pages	When you add a new Password or edit an existing one, by default the password value is masked i.e. ****** If you choose, you can instead show the password value instead of the masked one
Auto Generate New Password When Adding a New Record	When adding a new Password record, you can automatically generate a new random password instead of having to specify one yourself. The format/complexity of the new random password will be determined by which Password Generator Policy is applied to the Password List
Enable Search Criteria Stickiness Across Password Screens	When using the search textbox found at the top of most Password screens, you can choose to make this search

	value you type sticky across different Password Lists i.e. if you search for 'test' in one Password List, when you click on another Password List in the Navigation Tree, the contents of the Passwords grid will also be filtered by the term 'test'. You can also clear the search criteria by clicking on the cicon
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 and all Folder screens, 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 and and Folder pages
When creating new Shared Password Lists, base the settings on the following Template's settings	When creating new Password Lists, you can choose to automatically specify all the settings based on one of the Templates you select here
When creating new Shared Password Lists, base the permissions on the following Template's permissions	When creating new Password Lists, you can choose to automatically base all the permissions on one of the Templates you select here
Locale (Date Format)	Allows you to specify a date format for any date fields - you may need different format based on your region, compared to that of what Passwordstate is current set to use system wide

🚨 Edit User Details

To modify the user's details, please make appropriate changes in each of the tabs below and click on the 'Save' button.

st tester (halox	\testtester)				
account details	miscellaneous	color theme	authentication options	mobile access options	
Please select which o	f the following misc	ellaneous options v	vithin Passwordstate you wou	d like to enable for the user.	
Password Visibility Ovisible • Mask	on Add/Edit Pages:				
u to Generate New ⊖Yes ●No	Password When A	dding a New Reco	vrd:		
nable Search Crite ● Yes ○ No	ria Stickiness Acros	s Password Screen	15:		
how the 'Actions' ● Bottom ○ Top	toolbar on the Pass O Bottom & Top	words pages at th	e:		
)n all Password Lis	t screens, sort the g	rid by the followi	ng column:		
Do not sort by defa	ult		-		
On the Decewords h	lomo and all Foldor	scroops sort the	Sourch Posults and Favorita	Preswards grids by the following column:	
Do not sort by defa	ult	screens, sort the		rasswords grids by the following column.	
When creating new	Shared Password L	ists, base the setti	ings on the following Templ	ate's settings:	
Do not use template	e		-		
When creating new	Shared Password L	ists, base the perr	nissions on the following Te	mplate's permissions:	
Do not use template	e		v		
.ocale (Date Forma	t):				
Use System Wide Lo	cale Setting		-		
f you would like to	use a different Kou	board layout for l	RDP sessions when using the	Browser Based Launcher, please select it here	
i you would like to	ase a unrerent Key	source rayout for i	tor sessions when using the	alowari aasta taulitilei, piease selett it liele.	
Select Keyboard I	avout	-			

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.

🎗 Edit User Details

To modify the user's details, please make appropriate changes in each of the tabs below and click on the 'Save' button.

count details	miscellaneous	color theme	authentication options	mobile access options	
the System Wi	de color theme, or o	hoose a different	t one for the user:		
System Wide	Choose My Own				
Base Color					
lease select the	Base Color to use thr	oughout Password	lstate.		
olor Palette					
Apex	$\overline{\mathbf{v}}$				
Base Color:					
no color	2 🔼				

Authentication Options Tab

The Authentication Options Tab allows you to:

- Specify which Authentication Option should be used for the user's account details and screenshots for each of the different authentication options can be found on the screen <u>System</u> <u>Settings</u> -> <u>Authentication Options Tab</u>
- Specify SecurID and AuthAnvil account details
- Create/clear/email the user their ScramblePad Pin number
- Create/clear/email the user their Google Authenticator Secret Key

♣ Edit User Details

To modify the user's details, please make appropriate changes in each of the tabs below and click on the 'Save' button.

	miscellaneous	color theme	auther	ntication options	mobile access options		
e select the prefe	rred Authenticatior	n Option for the us	er for acce	essing the Passwords	state web site.		
e Note: you only they have selected	need to specify the d a secondary auth	entication option f	or a Passw	ord List they have a	the available Authentication options has been applied to the users ac ccess to.		
ab Authentica	tion Option						
ed Authentica	tion Option						
lease specify whi	ch Authentication o	ption which will a	Il apply Please Note:		with Department with antipation mathe of the only true way to survive		
o this user when t	they first authentica	ite to Passwordsta	te.	a user's login creder	itials after logging out is to close the browser window. Clicking on		
Choose Authentie	tication Option:			the 'Log Back In' but	ton, or refreshing the page, simply re-authenticates the user. Please		
Use the System V	Vide Authentication	Settings 🔹		to their own.	are of this if they log into Passwordstate from different computers		
cramblePad Pir If you have choser ScramblePad Pin	n Number n to use ScramblePa Number:	ad Authentication,	please spe Email	ecify a Pin Number fo	or the user to use. /inimum length is : 4)		
ScramblePad Pir If you have choser ScramblePad Pin Dne-Time Passw	n Number n to use ScramblePa Number: vord Settings	ad Authentication,	please spe Email	ecify a Pin Number fo	or the user to use. Ainimum length is : 4)		
ScramblePad Pir If you have choser ScramblePad Pin One-Time Passw Select which type if the One-Time Pa	n Number n to use ScramblePa Number: vord Settings of One-Time Passw assword Authentica	ad Authentication,	please spe Email	ecify a Pin Number fr New Clear () the user will use, and d to the users accour	or the user to use. Ainimum length is : 4) various settings as appropriate - these settings are only applicable it.		
GramblePad Pir If you have choser ScramblePad Pin One-Time Passw Select which type i if the One-Time Pa Token Type:	n Number n to use ScramblePa Number: vord Settings of One-Time Passw assword Authentica Time-Based	ad Authentication, ord authentication tion option has be	please spe Email	ecify a Pin Number for New Clear (N the user will use, and d to the users accourt	or the user to use. Ainimum length is : 4) various settings as appropriate - these settings are only applicable it.		
icramblePad Pir If you have choser ScramblePad Pin One-Time Passw Select which type if the One-Time Pa Token Type: Time Step:	n Number n to use ScramblePa Number: vord Settings of One-Time Passw assword Authentica Time-Based 30	ad Authentication,	please spe Email	ecify a Pin Number fo New Clear () the user will use, and d to the users accour 60 seconds	or the user to use. Ainimum length is : 4) various settings as appropriate - these settings are only applicable it.		
GramblePad Pir If you have choser ScramblePad Pin One-Time Passw Select which type if the One-Time Pa Token Type: Time Step: Token Clock Drif	n Number n to use ScramblePa Number: vord Settings of One-Time Passw sssword Authentica Time-Based 30 tt 0	ad Authentication,	please spe Email	ecify a Pin Number for New Clear (f the user will use, and d to the users accour 60 seconds	or the user to use. Minimum length is : 4) various settings as appropriate - these settings are only applicable it.		
ScramblePad Pir If you have choser ScramblePad Pin One-Time Passw Select which type i if the One-Time Pa Token Type: Time Step: Token Clock Drif Counter:	n Number n to use ScramblePa Number: vord Settings of One-Time Passw assword Authentica Time-Based 30 t: 0 0	ad Authentication,	please spe Email	ecify a Pin Number for New Clear () the user will use, and d to the users accour 60 seconds onds the user's toker nt Counter is for the	or the user to use. Ainimum length is : 4) various settings as appropriate - these settings are only applicable it.		
GramblePad Pir If you have choser ScramblePad Pin One-Time Passw Select which type i if the One-Time Pa Token Type: Time Step: Token Clock Drif Counter: HOTP Digits:	n Number n to use ScramblePa Number: vord Settings of One-Time Passw assword Authentica Time-Based 30 t: 0 0 6	ad Authentication, ord authentication tion option has be Gene How What Gene	please spo Email method t en applied rally 30 or many seco the curren rally 6 or 8	ecify a Pin Number for New Clear (N the user will use, and d to the users accour 60 seconds onds the user's toker nt Counter is for the 3 digits (for Counter-	or the user to use. Ainimum length is : 4) various settings as appropriate - these settings are only applicable it. I has drifted over time user's token Based authentication)		

Mobile Access Options Tab

The Mobile Access Options tab allows you to specify various Mobile App settings for the user, and to also set their Mobile Pin Number for them if required. The Pin Number can then be emailed to their account.

Save Cancel

🤱 Edit User Details

To modify the user's details, please make appropriate changes in each of the tabs below and click on the 'Save' button.

test tester (halox	est tester (halox\testtester)					
account details	miscellaneous	color theme				

Mobile App Settings		
Set the Mobile default home page to: Password List Search O Password Search		
Specify the number of days the user can acce will override the System Wide setting for this fea	ss their offline cache before they need to ture):	o re-authenticate again to the Passwordstate App Server (this
Use System Wide Setting	-	

authentication options mobile access options

Clone User Permissions

It's possible to clone one user's permissions to another, by using the 'Clone User Permissions' feature. This feature is generally used in one of two ways:

- You've had a new employee start who has replaced another employee, and you wish to give them the same access
- If you need to modify the UserID for a user i.e. a Domain Migration, someone gets married, etc.

Note 1: When cloning occurs, you have the option of first deleting all the existing permissions the Destination User has, or you can retain them and simply clone across additional permissions
 Note 2: Active Directory Security Group Memberships will not be cloned with this process, as you need to manage these memberships within Active Directory.

During the cloning process, the following types of permissions will be cloned:

- Any Blocked Email Notification settings
- Any memberships to Email Notification Groups
- Any Favorite Passwords
- Any of the 'Features' permissions for what menus the user is allowed access to at the bottom of the screen
- Any Grid Settings which columns to see, width, etc.
- Any permissions to Shared Password Lists (auditing records are added)
- Any Password Permissions (auditing records are added)
- Any permissions to Password Lists Templates (auditing records are added)
- Any Security Admin Roles (auditing records are added)
- Any membership to Local Security Groups (auditing records are added)
- The expand/collapse status of the Password Lists Navigation Tree

- Any User Account Policy permissions
- Any Scheduled Reports

clone permissions		r T	,,,		
e Location : Internal		v			
you wish to remove all permissions fo	r the Destination User pr	ior to starting the clone proc	255:		
Ves ONo		Destination Users			
ilter	8	Filter		8	
	-				

Note: If you need to clone more than one user's permissions at a time, you can use the 'Clone' Multiple Users' button. This will allows you to import a CSV file to process multiple users.

Reset Accepted UAPs for All Users

It's also possible to reset the status of accepted User Acceptance Policies for your users as well. It's possible you will want to do this periodically, as you may need to modify the policy based on business requirements. Resetting this accepted value means the user will be prompted again to read and accept the updated policy - assuming you have this option enabled on the System Settings <u>User Acceptance Policy Tab</u>. In the User Accounts grid as well, you can see the data and time each of the users last accepted the User Acceptance Policy.

Managed Service Accounts (MSA) and Group Managed Service Accounts (gMSA)

You can also import/add either MSA or gMSA accounts into Passwordstate, and then grant these accounts access to various Password Lists or Password records.

The primary reason you would do this, is to use the service accounts in conjuction with our Windows Integrated API. You cannot log into passwordstate using these types of service accounts, but you can execute PowerShell scripts against the API, under the security context of these accounts.

2.33 User Account Policies

User Account Policies allow you to manage a specific set of settings for a groups of users at a time. The settings relate to various User Preferences, and how the Password Lists, Home Page screens appear to the user.

An example of how User Account Policies can be used is to hide all graphs on all screens from the users.

When a User Account Policy is applied to a user's account, the controls/settings on the screen will be disabled, informing the user a User Account Policy is in effect for their account.

Adding a User Account Policy

When you add a User Account Policy, you can choose to set any number of the following settings:

User Preferences

Mask Password Visibility on Add/View/Edit Pages Auto Generate New Password When Adding a New Record Enable Search Criteria Stickiness Across Password Screens Show the 'Actions' toolbar on the Passwords pages at the Locale (Date Format) Specify which Authentication option will apply to the user's account Specify the Base Color to be used throughout Passwordstate In the Passwords Navigation Tree, use the following Expand status for Nodes In the Passwords Navigation Tree, show or hide all Nodes In the Passwords Navigation Tree, Limit the number of displayed Nodes In the Passwords Navigation Tree, Use Load On Demand Feature In the Hosts Navigation Tree, Use Load On Demand Feature Show the Permission Model icon indicators next to Folders and Password Lists in the Passwords Navigation Tree	
Auto Generate New Password When Adding a New Record Enable Search Criteria Stickiness Across Password Screens Show the 'Actions' toolbar on the Passwords pages at the Locale (Date Format) Specify which Authentication option will apply to the user's account Specify the Base Color to be used throughout Passwordstate In the Passwords Navigation Tree, use the following Expand status for Nodes In the Passwords Navigation Tree, show or hide all Nodes In the Passwords Navigation Tree, Limit the number of displayed Nodes In the Passwords Navigation Tree, Use Load On Demand Feature In the Hosts Navigation Tree, Use Load On Demand Feature Show the Permission Model icon indicators next to Folders and Password Lists in the Passwords Navigation Tree	Mask Password Visibility on Add/View/Edit Pages
Enable Search Criteria Stickiness Across Password Screens Show the 'Actions' toolbar on the Passwords pages at the Locale (Date Format) Specify which Authentication option will apply to the user's account Specify the Base Color to be used throughout Passwordstate In the Passwords Navigation Tree, use the following Expand status for Nodes In the Passwords Navigation Tree, show or hide all Nodes In the Passwords Navigation Tree, Limit the number of displayed Nodes In the Passwords Navigation Tree, Use Load On Demand Feature In the Hosts Navigation Tree, Use Load On Demand Feature Show the Permission Model icon indicators next to Folders and Password Lists in the Passwords Navigation Tree	Auto Generate New Password When Adding a New Record
Show the 'Actions' toolbar on the Passwords pages at the Locale (Date Format) Specify which Authentication option will apply to the user's account Specify the Base Color to be used throughout Passwordstate In the Passwords Navigation Tree, use the following Expand status for Nodes In the Passwords Navigation Tree, show or hide all Nodes In the Passwords Navigation Tree, Limit the number of displayed Nodes In the Passwords Navigation Tree, Use Load On Demand Feature In the Hosts Navigation Tree, limit the number of displayed Nodes In the Hosts Navigation Tree, Use Load On Demand Feature Show the Permission Model icon indicators next to Folders and Password Lists in the Passwords Navigation Tree	Enable Search Criteria Stickiness Across Password Screens
Locale (Date Format) Specify which Authentication option will apply to the user's account Specify the Base Color to be used throughout Passwordstate In the Passwords Navigation Tree, use the following Expand status for Nodes In the Passwords Navigation Tree, show or hide all Nodes In the Passwords Navigation Tree, Limit the number of displayed Nodes In the Passwords Navigation Tree, Use Load On Demand Feature In the Hosts Navigation Tree, limit the number of displayed Nodes In the Hosts Navigation Tree, Use Load On Demand Feature Show the Permission Model icon indicators next to Folders and Password Lists in the Passwords Navigation Tree	Show the 'Actions' toolbar on the Passwords pages at the
Specify which Authentication option will apply to the user's account Specify the Base Color to be used throughout Passwordstate In the Passwords Navigation Tree, use the following Expand status for Nodes In the Passwords Navigation Tree, show or hide all Nodes In the Passwords Navigation Tree, Limit the number of displayed Nodes In the Passwords Navigation Tree, Use Load On Demand Feature In the Hosts Navigation Tree, limit the number of displayed Nodes In the Hosts Navigation Tree, Use Load On Demand Feature Show the Permission Model icon indicators next to Folders and Password Lists in the Passwords Navigation Tree	Locale (Date Format)
Specify the Base Color to be used throughout Passwordstate In the Passwords Navigation Tree, use the following Expand status for Nodes In the Passwords Navigation Tree, show or hide all Nodes In the Passwords Navigation Tree, Limit the number of displayed Nodes In the Passwords Navigation Tree, Use Load On Demand Feature In the Hosts Navigation Tree, limit the number of displayed Nodes In the Hosts Navigation Tree, Use Load On Demand Feature Show the Permission Model icon indicators next to Folders and Password Lists in the Passwords Navigation Tree	Specify which Authentication option will apply to the user's account
In the Passwords Navigation Tree, use the following Expand status for Nodes In the Passwords Navigation Tree, show or hide all Nodes In the Passwords Navigation Tree, Limit the number of displayed Nodes In the Passwords Navigation Tree, Use Load On Demand Feature In the Hosts Navigation Tree, limit the number of displayed Nodes In the Hosts Navigation Tree, Use Load On Demand Feature Show the Permission Model icon indicators next to Folders and Password Lists in the Passwords Navigation Tree	Specify the Base Color to be used throughout Passwordstate
In the Passwords Navigation Tree, show or hide all Nodes In the Passwords Navigation Tree, Limit the number of displayed Nodes In the Passwords Navigation Tree, Use Load On Demand Feature In the Hosts Navigation Tree, limit the number of displayed Nodes In the Hosts Navigation Tree, Use Load On Demand Feature Show the Permission Model icon indicators next to Folders and Password Lists in the Passwords Navigation Tree	In the Passwords Navigation Tree, use the following Expand status for Nodes
In the Passwords Navigation Tree, Limit the number of displayed Nodes In the Passwords Navigation Tree, Use Load On Demand Feature In the Hosts Navigation Tree, limit the number of displayed Nodes In the Hosts Navigation Tree, Use Load On Demand Feature Show the Permission Model icon indicators next to Folders and Password Lists in the Passwords Navigation Tree	In the Passwords Navigation Tree, show or hide all Nodes
In the Passwords Navigation Tree, Use Load On Demand Feature In the Hosts Navigation Tree, limit the number of displayed Nodes In the Hosts Navigation Tree, Use Load On Demand Feature Show the Permission Model icon indicators next to Folders and Password Lists in the Passwords Navigation Tree	In the Passwords Navigation Tree, Limit the number of displayed Nodes
In the Hosts Navigation Tree, limit the number of displayed Nodes In the Hosts Navigation Tree, Use Load On Demand Feature Show the Permission Model icon indicators next to Folders and Password Lists in the Passwords Navigation Tree	In the Passwords Navigation Tree, Use Load On Demand Feature
In the Hosts Navigation Tree, Use Load On Demand Feature Show the Permission Model icon indicators next to Folders and Password Lists in the Passwords Navigation Tree	In the Hosts Navigation Tree, limit the number of displayed Nodes
Show the Permission Model icon indicators next to Folders and Password Lists in the Passwords Navigation Tree	In the Hosts Navigation Tree, Use Load On Demand Feature
Navigation Tree	Show the Permission Model icon indicators next to Folders and Password Lists in the Passwords
	Navigation Tree

For RDP Sessions, use the following performance settings For SSH Sessions, select the font size you would like to use in the terminal

Password List Screen Options

Show the 'Header' row on all Passwords Grids Show the 'Filter' controls in the Header of the Passwords Grids Show the 'Header' row on all Recent Activity Grids Make the Recent Activity Grid visible to the user Selects the Paging Style controls for Password and Recent Activity grids Make the Pie Charts visible to the user Sort the grid by the following column Select the color theme for the Pie Charts

Home Page Screen Options

Dashboard Layout Settings Show the Password Statistics Chart Choose the Style of the Password Statistics Chart Stack the data points on top of each other for the Password Statistics Chart Select the color theme for the Password Statistics Chart Sort the Search Results and Favorite Passwords grids by the following column

Password List Options

When creating new Shared Password Lists, base the settings on the following Template's settings When creating new Shared Password Lists, base the permissions on the following Template's permissions

If copying settings from a Template to a Shared Password List, also link them

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

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

User Account Policy Actions

Once you have created a Policy with the desired settings, the following Actions Menu items are available to you:

- Apply Policy to Users allows you to assign the selected policy to a group of users, or security groups
- Toggle Status either enable or disable the policy
- Delete delete the policy

🔏 User Account Policies

User Account Policies are used to control various user settings as they relate to their 'Preferences' area, and 'Screen Options'

Note 1: By applying a User Account Policy to a user, it will disable the user's ability to modify these settings themselves. **Note 2:** You can have the same setting applied to a user multiple times via different policies, and you can re-order them for

	Actions	Order	Policy Name
			T
>	٥		Charts Disabled
>	💂 Ар	ply Policy t	to Users
>	💲 То	ggle Status	- Enabled or Disabled
>	😢 De	lete	
5	0		Password Lists - Shared

Re-Ordering Execution of Policies

You can drag and drop the rows within the User Accounts Policies screen, and re-order the execution of policies. This way, it is possible to have 'conflicting' settings for a user, and it will be the last (most bottom) policy which will be in affect for the setting.

Check For Conflicts

As it's possible to apply more than one User Account Policy to a user's account, or a security group, it is recommended that you use the 'Check for Conflicts' button to determine if this is the case - it would cause confusion if different values for the same settings were being applied via different policies.

3 Remote Site Administration

Welcome to the 'Remote Site Administration' area of Passwordstate.

The Remote Site Administration module allows you to manage account credentials on sites (networks) that are not part of your standard internal network, and are either separated via the Internet, or a firewalled environment.

Once licensed to use this module, an Agent can be deployed to each of your remote sites, allowing communication back to your Passwordstate instance securely over one single port. Below are some of the features available with the Remote Site Administration module.

• Discovery of accounts in Active Directory, Windows Desktop and Servers, Linux, databases and network devices

- Password Resets for many different account types
- Account Heartbeat Status for many different account types
- Free Licenses for "Clients' to login an view their own password credentials
- Process for identifying which passwords need resetting after one of your technicians leaves your company, and automatically reset them all with a few clicks
- In-Transit encryption of data between the Agent and Passwordstate API
- Optionally install a Browser Based Remote Session laauncher, so you can RDP or SSH into machines over on that remote site
- Reporting for Privileged Account Management on that site. For example, what accounts have had their passwords reset in the last 30 days.

3.1 Remote Site Locations

Prior to tagging Folders, Passwords, Hosts, etc to belong to a Remote Site Location, you first need to add one or more Remote Site Locations on this screen.

Once you have added a Remote Site, then you can also deploy the agent to that site, allowing communication back to your Passwordstate API. Please refer to the section 'Installing Remote Site Agent' below for instructions for how to deploy the agent.

Note: Under the Help Menu in Passwordstate, some of the information below and more can be found in the 'Remote Site Agent Manual'.

Below are all	the Remote Sites	where an Agent o	an be deployed to perform Ac	count Discoveries, Pas	ssword Resets, and Account	and Host Heartbeats.		
'his feature i	is designed for site	es that are not par	rt of your standard internal net	work, and are either s	eparated via the Internet, o	r a firewalled environment.		
Actions	Site Location	Agent Health	Last Agent Poll Time	Agent Build No	Last Discovery Duration	Last Account Heartbeat Duration	Last Host Heartbeat Duration	Last Password Reset Duration
0	Fabrikam	٠			NA	NA	NA	NA
0	Halox		12/06/2017 9:13:00 AM	8000	00:00:02	00:00:01	00:00:01	00:00:01
	Canddomain	-	18/04/2017 10:43:35 AM	8000	NA	NA	NA	NA

Remote Site Locations Actions Menu

Below is a description for each of the Remote Site Locations Actions menus:

- Clear All Progress Indicators this menu should rarely need to be used, but will clear any in progress indicators on the screen, if one of the relevant poll jobs where to fail for any reason
- Delete This will delete your remote site and all data for that site out of Passwordstate.
- **Refresh Remote Tables** all remote tables are refreshed during the maintenance window, but selecting this menu option means they will be refreshed again during the next agent poll. Below is a list of tables synchronized to the Remote Site Location on Agent Start-up and during the Maintenance Window:

AccountTypes

- DiscoveryOUs (also synchronized just prior to any Host Discovery Jobs)
- DiscoveryScripts
- Hosts (also synchronized just prior to any Discovery Jobs)
- HostTypes

○ OperatingSystems

- Scripts
- \circ ValidationScripts

(The majority of these tables should be fairly static, meaning the once a day synchronization should be enough. If however you add/modify any of your own PowerShell scripts for Password Resets and Account Heartbeats, then it is recommended you use the 'Refresh Remote Tables' menu option.

 View Agent Installer Instructions - For instructions on how to add a New Remote Site Location and install it on your remote network, see this complete guide: https://www.clickstudios.com.au/downloads/version9/Passwordstate_Agent_Manual.pdf

",	Remot	e Site Locatio	ons			
Belo This	ow are all	the Remote Sites is designed for site	where an Agent c es that are not par	an be deployed to perform Ac	count Discoveries, Pas work, and are either s	ssword Resets, and Acco eparated via the Interne
ļ	Actions	Site Location	Agent Health	Last Agent Poll Time	Agent Build No	Last Discovery Duratio
	0	Fabrikam	•			NA
	0	Halox	0	12/06/2017 9:13:00 AM	8000	00:00:02
	👲 Cl	ear All Progress In	dicators	/04/2017 10:43:35 AM	8000	NA
Re	O De C Re C Vi	elete efresh Remote Tab ew Agent Installer	les Instructions	All Remote Tables To	ggle Visibility of IDs	Grid Layout Actions

Logging

In addition to the standard audit records the Remote Site Agent can feed back to the API, there is also local logging for the Agent as well - to help identify any issues with the Agent if needed. The available local logs are (please note that no sensitive data is added to these log files):

- General General logging not related to any of the other log files below
- Discovery Logging related to Account and Host Discovery Jobs
- Heartbeat Logging related to Account and Host heartbeats
- PasswordResets Logging relating to Password Resets

Each of the log files can be found in the folder "C:\Program Files (x86)\Passwordstate Agent\logs"

4 Password Reset Portal Administration

Welcome to the 'Password Reset Portal Administration' area of Passwordstate.

The Password Reset Portal is a Self-Service Portal for your users to unlock, or reset the password for their Active Directory Domain account, in the event they are no longer able to authenticate. The portal can be accessed via Mobile Phones and Desktops.

There are multiple Verification Policies available for the portal to 'Identify' your users in order for them to unlock or reset their account, which are listed below. With these Verification Policies, you can also assign different policies to different sets of users if required.

- Duo Authentication
- Email Temporary PIN Code
- Google Authenticator
- One-Time Passwords (TOTP or HOTP)
- PIN Number
- Questions and Answers
- RADIUS Authentication
- RSA SecurID Authentication
- SAML Authentication

Included in your dowload of Passwordstate, or available on the Click Studios' web site, is the installer for the Password Reset Portal. Please refer to the 'Password Reset Portal Installation Instructions' for more information.

4.1 Active Directory Domains

In order for users to reset or unlock their domain accounts, you must first add the required number of Active Directory Domains on this screen.

Note 1: Your domain must be at 2012 functional level or higher.
 Note 2: Only unique domains are supported i.e. NetBIOS Name and FQDN need to be unique across domain records

Trusted and non-trusted domains can be added on this screen, and the following ports are required to be open on any firewalls for this module to function:

Password Reset Portal Ports

• The Password Reset Portal only needs to communicate back to your Passwordstate API, so generally Port 443 is required to be open. If you are using a different port for your Passwordstate web site, then this port will instead need to be open

Passwordstate Web Site and API

• Port 636 (TCP) - this is required for LDAP over SSL, so the Passwordstate UI and API can communicate with Active Directory to reset and unlock accounts

- Ports 88 aand 464 (UDP/TCP) are required to be open to your domain controllers, in order to use Kerberos authentication
- To query Event Logs on Domain Controllers for account lockouts, Port 135 needs to be open, and also the existing Windows Firewall rule "Remote Event Log Management (RPC)", which uses dynamic ports
- Please note all authentication options require UDP Port 389 to be open, in order to find the nearest domain controller

Adding a New Active Directory Domain

Prior to adding a new domain, you must first add one or more required <u>Privileged Account</u> <u>Credentials</u> so Passwordstate can reset/unlock accounts in the domain, and also query event logs on your domain controller.

Add New Active Directory Domain

To add a new Active Directory Domain for the Password Reset module, please fill in the details below.

active directory details ev	ent log monitoring
Please specify appropriate details	for your domain below.
AD Domain NetBIOS Name *	
	e.g. clickstudios
FQDN *	
	e.g. clickstudios.com.au
Domain Label	
	There is a System Setting to allow showing of a Domains dropdown list on screens in the Password Reset Portal. When enabled, you can either show the NetBIOS value of the domain, or a different label by specifying one here.
Domain Controller FQDN	
	e.g. adserver1.clickstudios.com.au (this should only be required if you are having issues contacting the domain over restricted networks like the Internet)
AD Domain LDAP Query String *	
	e.g. dc=clickstudios,dc=com,dc=au
Privleged Account Credential	Corp Domain Priv 💌
	This account must have permissions to query Security Group memberships, and also to reset the password for user's accounts in Active Directory.
Protocol	● LDAPS (TCP Port 636) ○ Kerberos (UDP/TCP Ports 88 and 464)
	UDP Port 389 is required to be open for all Protocols above.

Add New Active Directory Domain

To add a new Active Directory Domain for the Password Reset module, please fill in the details below.

active directory details	event log monitoring
If you would like to monitor separated on each line (mor screen).	for account lockouts, you can specify one or more Domain Controllers below, e domain controllers can be added later if required editing the domain on the previous
Domain Controller(s)	
	<i>h</i>
	(Generally you only need to add the domain controller which holds the Primary Domain Controller (PDC) emulator role, but others can be added if needed)
Privleged Account Credenti	al Event Log Monitoring 🔹
	Please pick a Privileged Account Credential with sufficient permissions to query the event log on your Domain Controllers.
	Save Cancel

4.2 Auditing

The Auditing screen allows for real-time reporting of all audit events related to the Password Reset Portal.

There are multiple filtering options available, including each of the different platforms (Administration, Portal, Windows Service), as well as different Activity Types and date ranges.

🖾 Auditina							
To search for relevant audit record	ds please use the options below.						
Auditing Filters							
Additing filters							
Platform: All O Adminis	tration O Portal O Windows Service () api					
Max Records Activity T 5000 All Activit	ype Beg ies *	in Date End Date	Search				
Date	Platform	UserID	First Name	Sumame	IP Address	Activity	Description
Т	т	т	т	т	т	T	T
10/12/2020 8:14:26 AM	Windows Service	WindowsService	Windows Service	Account	10.0.0.125	User Account Added to Security Group	The Passwordstate Windows Service added James Farthing (halox/farja) to the Active Directory Security Group 'CoreAdmins'.
7/12/2020 2:05:46 PM	Windows Service	WindowsService	Windows Service	Account	10.0.0.125	Email Sent	Matthew Day (halox\daymt) has been sent a Password Expiry Reminder email as they have 2 days left the reset their account's password.
6/12/2020 2:05:21 PM	Windows Service	WindowsService	Windows Service	Account	10.0.0.125	Email Sent	Matthew Day (halox),daymt) has been sent a Password Expiry Reminder email as they have 3 days left the reset their account's password.
2/12/2020 2:05:54 PM	Windows Service	WindowsService	Windows Service	Account	10.0.0.125	Email Sent	Matthew Day (halox/daymt) has been sent a Password Expiry Reminder email as they have 7 days left the reset their account's password.
30/11/2020 9:04:36 AM	Windows Service	WindowsService	Windows Service	Account	10.0.0.125	User Account Added to Security Group	The Passwordstate Windows Service added Video Capture (halox/videos) to the Active Directory Security Group 'CoreAdmins'.
30/11/2020 9:04:36 AM	Windows Service	WindowsService	Windows Service	Account	10.0.0.125	User Account Added	The Passwordstate Windows Service added new user Video Capture (halox/videos).
30/11/2020 9:04:36 AM	Windows Service	WindowsService	Windows Service	Account	10.0.0.125	User Account Added to Security Group	The Passwordstate Windows Service added Image Capture (halox/images) to the Active Directory Security Group 'CoreAdmins'.
30/11/2020 9:04:36 AM	Windows Service	WindowsService	Windows Service	Account	10.0.0.125	User Account Added	The Passwordstate Windows Service added new user Image Capture (halox/jmages).
25/11/2020 10:24:42 AM	Portal	haloxymsand	Mark	Sandford	10.0.0.91	Identification Successful	screen. y
18/11/2020 4:02:30 PM	Administration	halox\msand	Mark	Sandford	10.0.0.91	Privileged Account Credentials Updated	Account).
10/11/2020 12:01:48 PM	Windows Service	WindowsService	Windows Service	Account	10.0.0.91	Email Sent	3.
7/11/2020 10:31:53 AM	Windows Service	WindowsService	Windows Service	Account	10.0.0.91	User Account Added to Security Group	The Passwordstate Windows Service added Robert Todd (halox/ytodd) to the Active Directory Security Group 'CoreAdmins'.
7/11/2020 10:31:53 AM	Windows Service	WindowsService	Windows Service	Account	10.0.0.91	User Account Added to Security Group	The Passwordstate Windows Service added Ashlee Sandford (halox/asand) to the Active Directory Security Group 'CoreAdmins'.
7/11/2020 10:07:12 AM	Portal	halox\msand	Mark	Sandford	10.0.0.91	Verification Successful	X
7/11/2020 10:07:04 AM	Portal	halox\msand	Mark	Sandford	10.0.0.91	Identification Successful	tify
H (12345	6 7 8 9 10 • H			Page: 1	of 334 Go Page size: 15 C	Thange	Item 1 to 15 of 5000
Export to Excel Grid Layout	Actions *						

4.3 Auditing Graphs

The Auditing Graphs screen gives you a visually representation of different audit events over time for the Password Reset Portal.

Similar to the Auditing screen, various filtering can be performed based on Platform, Activity and Duration.



4.4 Bad Passwords

If you would like to prevent users from using certain Passwords when resetting their Active Directory account, you can use the Bad Passwords feature for this.

There are two types of Bad Password databases you can use, and they are:

- Your own custom Bad Passwords, by adding them into your Passwordstate database
- Or you can use the online 'Have I been Pwned' database from this site -<u>https://haveibeenpwned.com/</u>. This is a list of known password from various security breaches

across the globe. If using this feature, your web server hosting the Passwordstate Reset Portal must be able to make calls to the internet.

• Or you can use both

ase select	which type of Bad Passwords database you would like to use to prevent users from using specific passwords.
Bad Pas	swords Database
Custo	om Database Below O Have I Been Pwned API O Both
Actions	Password
	Τ
0	1111
0	12345
0	88888
0	mats9119
0	olafur
0	password
0	qwerty

If using your own custom database, simply add in which passwords you would like to prevent the user of, and then users will be notified in the Portal if a match is found.

If required, you can also prevent partial matches on these values as well, but enabling the RegEx pattern matching on the System Settings screen.

System Settings

To modify the system settings for the Password Reset module, please make changes within the appropriate tabs below, then click on the 'Save' button.

·	api bran	iding error customiza	tions miscellaneous	password expiry reminder template	syslog server
e select various Miscellar	eous settings be	low as appropriate.			
scellaneous Settir	igs				
pecify the URL for the I	assword Reset I	Portal, which will be used (used within the body of ap	propriate emails:	
ttps://passwordresetpor	tal.halox.net				
y specifying a 'Return' ou've specified below:	JRL below, Exit	buttons will be visible on o	each screep in the portal, a	nd clicking the Exit button will return you	i to the URL
uery Domain Controlle	r event logs for	account lockov, events ev	ery: 5 - Minutes		
The querying of event log	data will only re	turn the past (x) minutes of	data, the same as the time-fi	rame selected above)	
se regular expressions	when matching	'Bad Passwords': 👳			
🔾 Yes 💿 No					
Vith the Password Reset	Portal, protect ollowing numbe	against brute force diction er of failed login attempts:	nary authentication attemp (Blocked IP Addresses can b	ets on the initial Identification screen by lo e removed on the screen Administration ->	ocking out an Brute Force
locked IPs)					

4.5 Password Policies

Password Policies can be used to provide on screen guidance as to what type of Passwords are expected, and prevent resetting your account if the policy is not met.

The type of criteria you can specify is:

- Minimum LowerCase Characters
- Minimum UpperCase Characters
- Minimum Numeric Characters
- Minimum Symbol Characters
- Preferred Password Length
- Requires Upper And Lower Case

Ideally these Policies should match the domain policies applied to the user's accounts - either the default domain policy, or any Fine-Grained Password Policies.

Once a policy is created, you need to apply permissions for which users or security groups are to receive it. And as the policies can be "Ordered" in precedence, you could set the 'Default Password Policy' to match your default Domain Password Policy, and if you have any Fine-Grained Password Policies in use, you can also create Password Policies here to match. This way your users can get specific details for what's expected for their account.

If the Password Policy is a match for the user, but resetting their account on the domain still fails (possibly they've reused a previous password), then you can also customize the error message which will be displayed on the screen for them.

Password Policies

Listed below are all the Password Policies which can be used for the Password Reset Portal. Please note:

1. You cannot delete the 'Default Password Policy'

2. You need to apply appropriate permissions to the policies

3. If more than once policy is in effect for a user, you can change the order by dragging and dropping the Order icon i.e. policies lower in the grid will take affect compared to policies higher in the grid.

	Actions	Order	Policy Name	Min Lowercase	Min Uppercase	Min Numerics	Min Symbols	Preferred Length	Requires Upper/Lower
>	0		Default Password Policy 👼	1	1	1	1	8	<
>	0		Second Policy 👼	0	0	0	0	4	×
Ad	d Grid L	ayout Actio	ons 🔻						

Edit Password Policy

Please specify your password policy settings below, and click on the 'Save' button.

Please specify details for the Password	l Policy Below.
Policy Name *	: Default Password Policy
Policy Description	[:] Default Domain Password Policy for All Users
Minimum LowerCase Characters *	: 1
Minimum UpperCase Characters *	: 1
Minimum Numeric Characters *	: 1
Minimum Symbol Characters *	: 1
Preferred Password Length *	: 8
Requires Upper And Lower Case *	: • Yes O No
Failed Reset Message *	Password could not be reset - The value provided for the new password does not meet the length, complexity, or history requirements of the domain.
	If the user passes the Password Policy criteria above when resetting their password, but their password is still rejected by the domain, then you can use this field to customise the error message they will see on the screen.

4.6 Privileged Account Credentials

Privileged Account Credentials are used for two things with the Password Reset Portal:

• To allow unlocks and resets of user's Active Directory Domain accounts

 To allow Passwordstate to query Event Logs on Domain Controllers for bad login attempts, or account lockouts

When adding a Privileged Account, please ensure it has sufficient permissions to perform the functions above - generally the account being used for resets/unlocks needs to be in the 'Account Operators' group at a minimum, but may require Domain Admin rights depending on the privilege set of the account being unlocked/reset, or if your admins have restricted access to certain accounts. Querying event logs generally requires a Domain Admin account, or the account needs to be in the 'Event Log Readers' built-in Security Group.

If you are also using the Password Reset features built into the core of the Passwordstate product, then you can also link this Privileged Account Credential to an account in an existing Password List - to ensure the password for the account is always updated.

or A	١dd	Privil	eged	Account	Details
------	-----	--------	------	---------	---------

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

privileged account	credentials	
Please specify appropr	ate details below, the click on the Save Button.	
Description *)
UserName *		0
	Please specify account in the format of domain\userid.	,
Password *) 🎔 👘
Confirm Password *)
Link To Password	Not Required *	
	If you link this Privileged Account to a password record which is enabled for Passwor then it will be updated here once the Password Reset is complete.	d Resets,
	Note: Only passwords which have been enabled for Reset, plus match the UserNam will be visible here.	e above,
	Save	Cancel

If you use any Fine Grain Password Policies in your organization, then you're privileged account credential also needs access to the policy in order to read certain attributes from it. Below is a screenshot of where this can be applied, if permissions do not already exist.

Password Settings	Password Settings		? 🙁
Directly Applies To Extensions	Name: Precedence:	Password age options: Enforce minimum password age User cannot change the password within (days): User must change the password age User must change the password after (days): User must change the password after (days): Tenforce account lockout policy: Number of failed logon attempts allowed: Reset failed logon attempts allowed: Reset failed logon attempts allowed: For a duration of (mins): For a duration of (mins): Until an administrator manually unlocks the account	* 2 * 2 * 30 * 30
	Directly Applies To Name Mail Short Password Users		? 8
			Remove
	Extensions		Remove

4.7 Reporting

The Reporting screen provides various pre-defined reports showing a graphical representation of data over time, or various raw data reports are also available.

Below is a screenshot of the reports available, as well as an example of trend and data reports. Note: When you click on a report, it will provide more detailed instructions for the purpose of the report.
🗠 Password Reset Portal Reporting

Please choose the appropriate report, and reporting parameters as appropriate.

Enrollment

- Show trend of Total Users vs Enrolled Users
- Show trend of Enrolled Users
- Show users who are yet to enroll
- Show the enrolled status for all users
- Show users who are having issues enrolling
- Show summary of which enrollment emails have been sent

Verification Policies

Users who have multiple policies Show users who have no policy Show policies and assigned members

Reset Activity

Show trend of Account Unlocks for Portal vs Admin Show trend of Account Unlocks via the Portal Show trend of Account Unlocks by an Admin Show trend of Account Resets for Portal vs Admin Show trend of Account Resets via the Portal Show trend of Account Resets by an Admin

Users & Security Groups

Show users with 'User cannot change' or 'Password Never Expires' Show members of each Security Group Show members not in any Security Groups

🗠 Password Reset Portal Reporting

Report Name: Show summary of which accounts have non-recommended account settings Report Description: Shows a summary of which accounts either have the 'Password Never Expires' or 'User Cannot Change Password' option set in Active Directory.

User ID	First Name	Surname	Email Address	User Cannot Change Password	Password Never Expires
T	T	T	T	T	T
halox\afran	Alexandra	Franklin			2
halox\mbarn	Michael	Barnes			
halox\jalva	Jake	Alvarado			
halox\msand	Mark	Sandford			
halox\jcisn	John	Cisneros			
halox\farja	James	Farthing			
halox\udit	Udit	Khullar			
halox\dkels	Dave	Kelsey	tesetgggggg		
halox\awils	Adam	Wilson	_		
halox\tboggs	Tim	Boggs			
H + 1 2 3 P H	Page size: 10 🔻				

Return to Reports | Export to Excel | Export to Excel (97 - 2003)

🗠 Password Reset Portal Reporting



4.8 Security Groups

182

It is recommended that you use Active Directory Security Groups to apply permissions to <u>Verification Policies</u>. By doing this, you can automate adding new users into the Password Reset Portal, apply a Verification Policy to their account, and send them automatic Enrollment emails.

If required, there are also some debugging options available, if you experience any issues with importing and synchronizing Security Groups.

sted below	are all the Active Directory Security Groups which are current	y synchronizing for the Password Reset module.	
Actions	Security Group	Description	Last AD Sync
	Т	Т	
0	E CoreAdmins (halox) (2)	Used for the core team only	11/06/2017 11:07 AM
0	E Desktop Team (halox) (11)		11/06/2017 11:07 AM
0	E Finance Team (halox) (1)		11/06/2017 11:07 AM
0	Portal Users (allsand) (1)	Test Description	11/06/2017 11:08 AM

Nested Security Groups

Nested Security Groups are supported in Passwordstate, but we do not maintain the nesting structure of those security groups. Instead, all the members of the nested Security Groups, will show in Passwordstate as members of the "parent" security group.

Please Note: Nested Security Groups are only supported within the same Active Directory Domain i.e. you cannot nested a Security Group from Domain B, beneath a Security Group from Domain A.

4.9 System Settings

System Settings are used to specify any number of system wide settings for the Password Reset Portal, with each section being detailed below.

Active Directory Options

The Active Directory Options tab allows you to specify a schedule for when Passwordstate should synchronize members of Active Directory Security Groups, as well as the frequency as to when new users receive each of the 3 different enrollment emails.

System Settings

To modify the system settings for the Password Reset module, please make changes within the appropriate tabs below, then click on the 'Save' button.

ective directory options	арі	branding	error customizations	miscellaneous	password expiry reminder template	syslog server
ase specify the schedule op counts and Enrollment Stat	ptions belo us' screen,	ow for synchror , the user can e	nizing the membership of Se nrol to use the Password Re	ecurity Groups below. set Portal feature.	Once accounts have been synchronized and	d added to the 'User
Active Directory Sec	urity G	roup Memb	pership Options			
When a user is removed following:	from a S	ecurity Group,	and that user no longer b	elongs to any Secur	ity Groups in the Password Reset Portal, p	perform the
O Delete the User's Acco	ount from	Password Rese	t Portal 💿 Do Nothing			
Show a Domain dropdov	wn List or	the Password	Reset Portal screens:			
When new users are add Enrollment emails by:	led as par	t of the Securi	ty Group synchronization	process (performed	by the Passwordstate Windows Service),	space out the 3
When new users are add Enrollment emails by: 7 T Days	led as par	t of the Securi	ty Group synchronization	process (performed	by the Passwordstate Windows Service),	space out the 3
When new users are add Enrollment emails by: 7 Days (Selecting 0 will disable au process performed via the Management screens)	led as par utomatic e Password	t of the Securi mails being ser Istate Windows	ty Group synchronization nt. These automatic emails a Service. You can also send	process (performed ire also only sent to n these emails manually	by the Passwordstate Windows Service), ew users who have been added as part of th y to users either via the Verification Policies of	space out the 3 ne AD Sync or User Account
When new users are add Enrollment emails by: T Days (Selecting 0 will disable at process performed via the Management screens) Synchronize Security Gr (You can also perform a N Groups)	led as par utomatic e Password roup Mem Manual Syr	t of the Securi mails being ser Istate Windows Isberships at: nchronization fo	ty Group synchronization It. These automatic emails a Service. You can also send or specific security groups o	process (performed ire also only sent to n these emails manually n the screen Adminis	by the Passwordstate Windows Service), ew users who have been added as part of th y to users either via the Verification Policies of tration -> Password Reset Portal Administrat	space out the 3 ne AD Sync or User Account tion -> Security
When new users are add Enrollment emails by: 7 Days (Selecting 0 will disable au process performed via the Management screens) Synchronize Security Gr (You can also perform a N Groups) Once a day at:	led as par utomatic e e Password Youp Men Manual Syn	t of the Securi mails being ser Istate Windows Iberships at: tchronization fo	ty Group synchronization It. These automatic emails a Service. You can also send or specific security groups o Minute	process (performed are also only sent to n these emails manually n the screen Adminis	by the Passwordstate Windows Service), ew users who have been added as part of th / to users either via the Verification Policies of tration -> Password Reset Portal Administrat	space out the 3 he AD Sync or User Account tion -> Security
When new users are add Enrollment emails by: Days (Selecting 0 will disable au process performed via the Management screens) Synchronize Security Gr (You can also perform a N Groups) Once a day at: Or on a schedule every:	led as par utomatic e Password Manual Syn 00 * 5 Minut	t of the Securi mails being ser Istate Windows Iberships at: nchronization fo Hour 00 v	ty Group synchronization It. These automatic emails a Service. You can also send or specific security groups o Minute V	process (performed ire also only sent to n these emails manually n the screen Adminis	by the Passwordstate Windows Service), ew users who have been added as part of th y to users either via the Verification Policies of tration -> Password Reset Portal Administrat	space out the 3 ne AD Sync or User Account tion -> Security

Branding

The Branding tab allows you to select a color scheme and background wallpaper for the Password Reset Portal, as well as your own custom logo.

Note 1: In order to use the custom logo feature, 'Anonymous' authentication must be enabled on your Passwordstate web site. If this is not the case, please refer to Note 2

Note 2: You can also copy your own logo file across to the portal web site. Name the file 'logo.png' and copy it to the file 'c:\inetpub\PasswordResetPortal\Content\assets\images' - this method can sometimes help with Load Balancers and Proxies. Recommended dimensions are 360W x 75H, and if using this method, please ensure you use the 'Restore Default Logo' button, to ensure the custom logo you've uploaded to the PasswordState core web site, is not used.

System Settings

To modify the system settings for the Password Reset module, please make changes within the appropriate tabs below, then click on the 'Save' button.

ctive directory options	арі	branding	error customizations	miscellaneous	password expiry reminder template	syslog server
ise choose the color sch	eme and ba	ckground image	e for the Password Reset Po	ortal below.		
olor Scheme & C	ustom C	SS				
ease select the color sch	ieme you w	ould like to sho	w on the Password Reset Po	ortal.		
Blue	₩ P	Preview Mobile	Preview Desktop			
you would like to custor content/assets/css/glol	nize certair sal folder w	n CSS for the Pas vithin your Passw	sword Reset Portal site, you vord Reset Portal folder.	u can by creating a file	called custom.css and placing it in the	
ou may also need to incl	ude the '!in	nportant' rule on	your css styling, so they ta	ike precedence over e	xisting styling in the Password Reset Portal	Site.
ortal Logo						
	o for the p	ortal balaw (Baa	ommondod cizo – 260W v	75U and either png	rif or ing format)	
ou can upload a new log	o ioi uie pi	Jital Delow (Reci	Uninended Size – Souw X	i on, and either sprig a	gir or gpg formag	
lease note that your Pass	wordstate	web site must ha	ave 'Anonymous' authentic	ation enabled in IIS fo	r this to work - which is the default setting.	For other options,
Please note that your Pass please refer to the Securit	wordstate y Administr	web site must ha rator's Manual u	ave 'Anonymous' authentic nder the Help menu - look	ation enabled in IIS fo in section Password F	r this to work - which is the default setting. eset Portal Administration -> System Settin	For other options, gs.
lease note that your Pass lease refer to the Securit PAS PAS	swordstate y Administr SSW S S W C	web site must ha rator's Manual un ORD RD	ave 'Anonymous' authentic nder the Help menu - look Cate s e t	ation enabled in IIS fc in section Password F	r this to work - which is the default setting. eset Portal Administration -> System Settin	For other options, gs.
Please note that your Pass please refer to the Securit Pass Pass Pass	swordstate y Administr SSW S W C	web site must ha rator's Manual un ORD R B	ave 'Anonymous' authentic nder the Help menu - look Cate S E T	ation enabled in IIS fc in section Password R	r this to work - which is the default setting. eset Portal Administration -> System Settin	For other options, gs.
Please note that your Pass please refer to the Securit PAS PAS Restore Default Logo	y Administr SSVV S W C	web site must harator's Manual un ORDRDRE	ave 'Anonymous' authentic nder the Help menu - look Cate S E T	ation enabled in IIS fo in section Password R	r this to work - which is the default setting. eset Portal Administration -> System Settin	For other options, gs.
ease note that your Pass lease refer to the Securit PAS PAS Restore Default Logo	y Administr SSW S W C	web site must hi rator's Manual u ORDRDRE	ave 'Anonymous' authentic nder the Help menu - look	ation enabled in IIS fc in section Password R	r this to work - which is the default setting. eset Portal Administration -> System Settin	For other options, gs.
ease note that your Pass lease refer to the Securit PAS Restore Default Logo	y Administr SSVV S S W C	web site must hi rator's Manual u ORDRDRE	ave 'Anonymous' authentic nder the Help menu - look	ation enabled in IIS fc in section Password F	r this to work - which is the default setting. eset Portal Administration -> System Settin	For other options, gs.
Please note that your Pass please refer to the Securit Place Place Place Place Place Place Restore Default Logo Background Image Please select the backgrou	Wordstate y Administr SSVV S S W C Upload Ne	web site must hi rator's Manual un ORDRDRE w Logo	ave 'Anonymous' authentic nder the Help menu - look cate s e t o show on the Password Re	ation enabled in IIS fc in section Password R sect Portal.	r this to work - which is the default setting. eset Portal Administration -> System Settin	For other options, gs.
Please note that your Pass please refer to the Securit PAS PAS Restore Default Logo Background Image Please select the backgrou	Administr SSVV SSVV Upload Ne und image	web site must hi rator's Manual un ORDRDRE w Logo	ave 'Anonymous' authentic inder the Help menu - look cate s E T	ation enabled in IIS fo in section Password R eset Portal.	r this to work - which is the default setting. eset Portal Administration -> System Settin	For other options, gs.

Error Customizations

The Error Customizations tab allows you to customize the text on various error screens within the Password Reset Portal. The intention is to allow you to provide a custom relevant body of text, informing your users the appropriate action to take if an error were to occur.

System Settings

To modify the system settings for the Password Reset module, please make changes within the appropriate tabs below, then click on the 'Save' button.

e customize the text pre	sented to users (on the vario	ous portal screens below.			
rollment Error Sc	reen					
e following text will be v main account.	isible to the user	r if they try a	and use the Password Res	et Portal feature, but	they have not finished the initial enrollme	ent process for their
rollment Error ✓ En ⊜ B Z II		= 1 1= :=	達達してある。	ent Name - Paul	_ abç	
our user account has no	t been enrolled t	to use this S	Self Service Reset feature.	Please contact your IS	Service Desk for more information	
′ou can now close your b	rowser.					
🔨 Design 🛛 🔍 Preview						
Design Preview Description Error S e following text will be v ve not purchased the rev	Screen isible to the user	r if there are or this modu	e any issues with the licen ule.	sing for the Password	Reset Portal module i.e. your subscription	n has expired, or you
Design Preview Description Error e following text will be v ve not purchased the red bscription Error	creen isible to the user quired licenses fo	r if there are or this modu	e any issues with the licen ule.	sing for the Password	Reset Portal module i.e. your subscription	n has expired, or you
Design Preview Description Error S e following text will be v ve not purchased the re- description Error	creen isible to the user quired licenses fo	r if there are or this modu ■ }= :=	e any issues with the licen ule. 譯 譯 A 、 M 、 Fi	sing for the Password ont Name • Real	Reset Portal module i.e. your subscription	n has expired, or you
✓ Design	isible to the user quired licenses fc 이 토 클 클 텔 sue with the sub	r if there are or this modu ■ $\frac{1}{3}$ = := pscription fo	e any issues with the licen ule. 達 詳一A・の・ F r this Self Service Reset fe	sing for the Password ont Name • Real eature.	Reset Portal module i.e. your subscription	n has expired, or you
✓ Design	isible to the user quired licenses for $ \blacksquare \equiv = = 1$ sue with the sub rvice Desk to inve	r if there are or this modu ■ $\frac{1}{3}$ = := oscription fo restigate.	e any issues with the licen ule. 建 醇 A、�、 マ F ir this Self Service Reset fe	sing for the Password ont Name Real eature.	Reset Portal module i.e. your subscription	n has expired, or you
Cesign Preview Preview Construction Error Construction Constructin Construction Construction Construction	Screen isible to the user juired licenses for I E E E I I sue with the sub rvice Desk to inve	r if there are or this modu ■ }= := sscription fo restigate.	e any issues with the licen ule. 達 译 A、 の 、 F r this Self Service Reset fe	sing for the Password ont Name Real eature.	Reset Portal module i.e. your subscription	n has expired, or you

Miscellaneous

The Miscellaneous tab has various settings for URLs, the frequency of query Event Logs on Domain Controllers, and also bruce force lockout counters for the Password Reset Portal Identification and Verification screens.

ch Settings:						
ctive directory option	ns api	branding	error customizations	miscellaneous	password expiry reminder template	syslog server
ase select various Misc	ellaneous set	tings below as a	ppropriate.			
∕liscellaneous Se	ettings					
Specify the URL for https://passwordrese	the Password	l Reset Portal, v net	which will be used used wi	ithin the body of ap	propriate emails:	
By specifying a 'Reto below:	ırn' URL bela	ow, Exit button:	s will be visible on each sc	reen in the portal, a	nd clicking the Exit button will return you	to the URL you've specified
Query Domain Cont (The querying of ever	r oller event l it log data wil	ogs for accoun I only return the	t lockout events every: 5 past (x) minutes of data, th	 Minutes same as the time-fr 	ame selected above)	
Use regular expressi	ons when ma	atching 'Bad Pa	sswords': 👼			
With the Password F the following numb	leset Portal, er of failed lo	protect against ogin attempts:	brute force dictionary au Blocked IP Addresses can b	thentication attemp e removed on the scr	ts on the initial Identification screen by lo een Administration -> Brute Force Blocked I	ocking out an active session after
3			(Setting to 0 will disable	this feature, and it is	not recommended - it should only be disab	led for troubleshooting purposes)
When tracking failed configured Passwords	d logins for B	Frute Force Log	in detection, track by: (If s es for X-Forwarded-For Supp	electing 'IP Address C port)	only', and you are using Load Balancers or Pr	roxy Servers, please ensure you have
UserID and IP Ad	dress O IP A	ddress Only				

Password Expiry Reminder Template

The Password Expiry Reminder Template tab allows you to specify settings so users can get reminders that their Active Directory account password must soon be reset. The intention of this feature is to proactively remind the user to reset their password, prior to it expiring.

Syst Syst	em Settings	
-----------	-------------	--

To modify the system settings for the Password Reset module, please make changes within the appropriate tabs below, then click on the 'Save' button.

ate below as required, a	nd also specify the freq	uency and timing of the emails	being sent.	to do so, please customize the Password	a Expiry Reminder
ssword Expiry Rer	ninder Settings				
Send emails on the nun It Days	aber of days prior to a ☑ 3 Days ☑ 2 Days ☑	password reset being require 1 Day	ed: Specify th	e time of day the emails are sent: our 05 • Minute	
ssword Expiry Rer	ninder Template				
ease customize the ema	il to be send to the use	rs below			
the literation		IS DEIOW.			
mail Subject: Password	Expiry Reminder				
🗙 🛍 🏚 B Z 🛛	∐ ≣ ≣ ≣ ≡ ੈ;	E 🗏 🚝 🗐 A - 🔊 - 🛛 Fe	ont Name 🔹 Real	- abc	
Hello [FirstName],					
The password for your A	active Directory account	[UserID] needs to be reset with	hin the next [Days].		
If your password expires	, you will not be able to	log on to the network and per	rform your work.		
Please reset your passw	ord either via the Windo L].	ows Login screen, or via the Pas	ssword Reset Portal b	y clicking on the following URL -	
[PasswordResetPortalUR					
[PasswordResetPortalUR Regards IS Service Desk					
[PasswordResetPortalUR Regards IS Service Desk					
[PasswordResetPortalUH Regards IS Service Desk					
[PasswordResetPortalUH Regards IS Service Desk					
[PasswordResetPortalUH Regards IS Service Desk ✓ Design ♥ Preview	,				

For users to receive this email notification, certain event must be met:

- Their account must be listed on the User Account Management screen
- They must have an email address associated with their account
- And both of the options you see in the screenshot below must not be selected

Prop	erties				?	×
Published Certificates	Member Of	Password	l Replicat	tion	Dial-in	Object
Security En	vironment	Sessi	ons	R	emote co	ontrol
Remote Desktop Se	rvices Profile	CC	DM+	A	Attribute E	Editor
General Address	Account	Profile	Teleph	ones	Orga	nization
User logon name:						
						\sim
User logon name (pre-	Windows 2000)):				
Logon Hours	Log On To)				
Unlock account				/		
Account options:						
User must chang	ge password at	next logor	ı			^
User cannot cha	ange password					
Password never	expires 🔔					
Store password	using reversible	e encryptio	n			~
Account expires						
Never						
	Caturday 21)	2021			
	Saturday , 23	s January	2021			
OI	K C	ancel	Ap	ply		Help

Syslog Server

The Syslog Server tab allows you to specify Syslog server details to send all auditing data to a Syslog server for event correlation.

If needed, you can also modify the date/time formatting of the messages sent to Syslog servers.

ctive directory opt	ions api	branding	error customizations	miscellaneous	password expiry reminder template	syslog server
Syslog Server D)etails					
If you would like to (Note: Specifying a	send all Audit syslog server f	log details to a S or the first time v	syslog server, please specify will send all audit records to	a Host Name and Poi your syslog server)	rt number below:	
	·					
Sysiog Server :						
	i look					
Port Number (UDP)	504					
Port Number (UDP) Date Formatting:	yyyy-MM	-dd HH:mm:ss	O			
Port Number (UDP) Date Formatting:	yyyy-MM 2020-12-0	-dd HH:mm:ss)9 14:05:05	Ç.			

4.10 User Account Management

The User Account Management screen allows you to add new user accounts so they can use the Password Reset Portal, sent Enrollment Emails to them, and also see various attributes relating to the user's AD account, and unlock/reset their account if required.

When importing user accounts, we also query the following domain and account attributes. If you experience any issues importing accounts, i.e. errors like AD attribute blank or not found, possibly it is a permission issue within your domain:

Domain Attributes

maxPwdAge (Default Domain Password Policy) msDS-ResultantPSO (Fine Grained AD Password Policy) msDS-PasswordSettings (Fine Grained AD Password Policy) msDS-MaximumPasswordAge (Fine Grained AD Password Policy)

User Account Attributes

SAMAccountName givenname sn (Surname) name objectSid mail objectCategory=person objectClass=user user.UserCannotChangePassword user.PasswordNeverExpires user.LastPasswordSet user.UserPrincipalName

Solar Account	wanager	nent					
sted below are all us	ers who can u	ise the Password Reset module in Pi	asswordstate.				
User Search and	l Filtering	● All Users O	Enrolled ONat Enrolled Search				
Total License Cour	t: Enterprise	(Unlimited) 👎 Available License	Count: Not Applicable				
Actions		UserID T	First Name	Sumame	Email	Last Used Portal	Enrolled
0		halox\abrow	Abigail	Brown			×
0		haloxi,afran	Alexandra	Franklin			×
0		halox/agent	Abigail	Gentry			¥
0		halox\asand	Ashlee	Sandford			×
0		halox/,awils	Adam	Wilson			×
0		halox\bboev	Boyan	Boev	the second s		×
0	0	halox\camal	Alistair	Cameron			¥
0		halox/,campt	Pete	Campbell			×
0		halox\daymt	Matthew	Day			×
0		halox\dkels	Dave	Kelsey	tesetgggggg		×
		- 00			Paner 1 of 7 Go Pane sizer 10 Channe		item 1 to 10 of 65

Account Details

On the Account Details tab for a user, you can see various attributes for their Active Directory account, as well as unlock/reset their account if required.

Ideally the user should be using the Portal to reset/unlock their own account, but under certain conditions this may not be possible. If an Administrator of Passwordstate is required to unlock/reset a user's account, they must specify a reason as to why they need to do this - that way a report can be generated to see if there are any trends which can be addressed, which would hopefully increase the use of the Password Reset Portal.

el Palmer (halox\rpal	mer)				
count details verification	on methods account lockout	monitori	ng		
User's Account Details			Unlock or Reset Accou	int	
UserID :	halox\rpalmer		Account Locked Status	:	Unlock account (Account is not locked)
First Name :	Rachel		New Password	:	
Surname :	Palmer		Confirm Password		
Email Address :			Chaosa Baasan		
UserPrincipalName :			Choose Reason		
Office :				:	Resetting of their password failed - Known Error
Department :				:	Resetting of their password failed - Password Reuse
Enrolled :	✓ User is enrolled				User could not remember the Answer to a selected Question
Account Disabled :	No				User could not remember the URL for the Self Service Reset Port
Bad Password Attempts :	0				User did not enroll to use service
Password Never Expires :	Option is not set				User did not have network access
Cannot Change Pwd :	Option is not set				User does not know now to use self service Reset Portal
Last Logon :	9/01/2018 10:18:43 AM				User was not aware of the Self Service Reset Portal
Password Last Set :	7/04/2018 1:15:23 PM				Verification Method for user account is failing
					Other

Verification Methods

The Verification Methods tab allows an Administrator of Passwordstate to specify settings for any one of the available <u>Verification Policies</u> for the user. Ideally the user would be specifying the relevant settings when they Enroll to use the Portal, but Administrators can change/override these settings if required.

🚨 Edit User Details

To modify the user's details, please make appropriate changes in each of the tabs below and click on the 'Save' button.

	erification methods	account lockout monitoring
w are the user's sett	ings for each of the ava	ilable Verification Method. Generally the user specifies the appropriate settings during the encollment process. But you can also
ige them here if requ	uired.	nune vermaation metriou, oenerang ale user speenes ale appropriate setangs aannig ale enroinnene process, bat you can also
IN Number		
Please specify the us	er's users PIN Number I	pelow.
PIN Number:		
no Timo Passuo	rd Cottings	
ne-Time Passwo	ra Settings	
Select which type of Time Password Auth	One-Time Password au entication option has be	hentication method the user will use, and various settings as appropriate - these settings are only applicable if the One- een applied to the users account.
Token Type:	Time-Based	×
Time Step:	30	Generally 30 or 60 seconds
Token Clock Drift:	0	How many seconds the user's token has drifted over time
Counter:	0	What the current Counter is for the user's token
HOTP Digits:	6	Generally 6 or 8 digits (for Counter-Based authentication)
Secret Key:		Show Generate Clear
oogle Authentic	ator	
In order for the user	to use two-factor autho	antication with Google Authenticator and their mobile/cell device you will need to:
an order for the user		Initiation with boogle Authenticator and their hibble/cell device, you will need to.
 Select the appropr 	rate Google Authentica acret Key and email it to	tor option above them
2. Generate a new Se	button	
2. Generate a new Se 3. Click on the 'Save'	button.	
2. Generate a new Se 3. Click on the 'Save'	button.	
2. Generate a new Se 3. Click on the 'Save' Secret Key: (not cas	e-sensitive)	iow Generate Clear
2. Generate a new Se 3. Click on the 'Save' Secret Key: (not case	e-sensitive)	how Generate Clear
2. Generate a new Se 3. Click on the 'Save' Secret Key: (not case) ADIUS Username	e-sensitive)	how Generate Clear
2. Generate a new Se 3. Click on the 'Save' Secret Key:	e-sensitive)	how Generate Clear
2. Generate a new Se 3. Click on the 'Save' Secret Key:	e-sensitive) e-sensitive) e-sensitive)	how Generate Clear
2. Generate a new Se 3. Click on the 'Save' Secret Key:	e-sensitive) e-sensitive) e- er's RADIUS Username [palmer	how Generate Clear
2. Generate a new Se 3. Click on the 'Save' Secret Key: (not cas ADIUS Username Please specify the us RADIUS Username: ecurID UserID	e-sensitive) e-sensitive) e-sensitive) p	how Generate Clear

Account Lockout Monitoring

The Account Lockout Monitoring tab will show any bad login attempts, or account lockout events, for the user's account. Event ID's 4740 (account lockout) and 4771 (pre-authentication fail i.e. Bad Login attempt). This tab may help you identify where a user is getting locked out, if it continues to happen regularly.

Edit User Details

Below is auditing data rela	ted to failed Domain logon attempts		
	teu to falleu Domain logon attempts, o	account lockout events, for the user's Active I	Directory Account.
Quary Event Logs New	Quanting of Event Log(s) was last n	arformed at 11/06/2017 11/25/49 AM	
Query Event Logs Now	Querying or event Log(s) was last p	enomed at 11/00/2017 11:35:48 AM.	
Date	Activity	Descripti	on
T	Т		T
No records to display.			

4.11 Verification Policies

Verification Policies are used to 'identify' the user when using the Password Reset Portal. The basic 3 step process is:

- Identify specify their Active Directory Account
- Verify verify the account, based on the Verification Policy selected for their account
- Reset Password either reset the password for their account, or unlock the account also

There are 9 different Verification Policies available to be used, each requiring certain configuration settings to be specified/confirmed, before you apply the policy to any user's accounts. The basic process to follow here is:

- Specify appropriate settings for the Verification Policy you want to use
- Apply the policies to users (it is recommended you use Security Groups for this purpose)
- And then send the initial Enrollment Email 1 to all users of the policies assuming you are not using the Auto-Enroll feature for the Verification Policies.

Kote 1: Verification Policies can also be applied to users in a specific order, by dragging and dropping the rows from within the 'Order' column i.e. apply a certain policy to 'All Users and Security Groups', but then also apply a certain policy to only specific users or security groups. For example, you can configure the policies so the whole business uses a Pin Number to verify, but then force IT to use some form of Two-Factor Authentication instead.

Note 2: If you enable auto-enrollment when user accounts have already been added into Passwordstate, they will be auto-enrolled next time the scheduled AD sync occurs, assuming they are not enrolled already.

s v	erificatio	on Polici	es								
/erific	cation Polici	ies are use	d to correctly ident	ify the user when they n	eed to reset or unlock their domain account through the Password Reset Port	al. To use one or	e more Verificatio	n Policies, you nee	ed to:		
I. Cor 2. Cus 3. App 4. And	nfigure sett stomize eac ply the poli d order the	ings as app th of the En cy to the in policies if a	propriate for the Ve prollment emails, as itended users or se a user has been as	rification Method s required curity groups signed more than one, b	y dragging and dropping the Order icon i.e. policies lower in the grid will haw	e precedence ove	er policies higher	in the grid (only o	ne policy can eve	r be in effect for a	user).
	Actions	Order	Policy Name		Policy Description	Auto Enrollment	Total Users	Enrolled Users	Email 1 Sent	Email 2 Sent	Email 3 Sent
				T	T						
	0	::	One-Time Passw	ords (TOTP or HOTP)	Verification using either One-Time Password hardware of software tokens	×	0	0	0	0	0
	0		Google Authenti	cator	Verification using Google Authenticator	×	0	0	0	0	0
E	0		PIN Number		Verification using PIN Number	×	0	0	0	0	0
>			Questions and	nswers	Verification using a series of Questions and Answers	×	65	59	16	11	10
Г	🗽 🛓 Ар	ply Policy t	to Users	intication	Verification using RSA SecurID Authentication	×	0	0	0	0	0
	∑ Se	nd Enrollm	ent Email 1	n	Verification using Duo Authentication	×	0	0	0	0	0
Г	∑ Se	nd Enrollm	ent Email 2	ition	Verification using RADIUS Authentication	×	0	0	0	0	0
	Sei Sei	nd Enrollm	ent Email 3	. IN Code	Verification using Email Temporary PIN Code	×	0	0	0	0	0
	-		CANAL AUXILIARIA	ation	Verification using SAML Authentication	4	0	0	0	0	0

User Initiated Enrollment

By default, the Verification Policies are configured to allow users to enroll themselves to use the Password Reset Portal. This means a variety of enrollment emails can be sent to your users, reminding them to enroll.

On each Verification Policy screens, you can customize the 3 different Enrollment emails, specific to the selected Verification Policy. Below is a screenshot from the SecurID Verification Policy.

Note 1: Once the initial Enrollment email has been sent, the Passwordstate Windows Service will then send subsequent enrollment emails to users who are yet to enroll

Note 2: If one of the Enrollment emails is sent to a user, selecting that same Menu item again will not send the email a second time to them

Let Verification Policy

Please update the settings for policy 'RSA SecurID Authentication' on each of the Tabs below as appropriate, then click on the 'Save' button.

Home										
Ê a K ^{Cut}	verdana, s	n B	ΙÜ	A •	≣≣≢≢¶	Apply CSS Cl	5.6.	Insert Variable	•	
aste	13px	- abc	χ ² Χ,	Ø) •		Normal -	A			
Clipboard	THE OCL	Font	*		Paragraph	Styles	Editing	Variables		
llo [ToFirst]	Jamel									
elcome to th r enrolling to licker proces	ne Passwo o use this ss for you	rdstate S service,	Self Sei resetti	rvice I ng or	Reset Portal. unlocking the pa	assword for your	domain acc	ount will be a	much simpler an	d
elcome to th v enrolling to licker process our account l rvice, and a o enroll for th	ne Passwo o use this ss for you has been ill you nee his service	rdstate S service, configure d to do v ; please	Self Ser resetti ed to us when e click o	rvice I ng or se Se mrollir on the	Reset Portal. unlocking the pi curID Two-Fac ng is confirm you following link -	issword for your tor Authentica ir SecurID UserN PasswordResetP	domain acc tion as the lame is corr ortalURL]/e	ount will be a Verification mo ect. nroll.	much simpler an ethod for this	ıd
elcome to th y enrolling to uicker proces our account l ervice, and a o enroll for th ease contact	ne Passwo o use this ss for you has been ill you nee his service t the IS S	rdstate S service, configure d to do v e, please ervice De	Self Ser resetti ed to u: when e click o esk on	rvice I ng or se Se mrollin on the [inser	Reset Portal. unlocking the pa curID Two-Fac ng is confirm you following link - t phone number	issword for your tor Authentica Ir SecurID UserN PasswordResetP here] for furthe	domain acc tion as the lame is corr ortalURL]/e r informatio	ount will be a Verification m ect. nroll. n and advice i	much simpler an ethod for this f required.	ıd
elcome to th y enrolling to uicker proces our account l ervice, and a o enroll for th ease contact agards asswordstate	ne Passwor o use this ss for you has been III you nee his service t the IS S e Adminis	rdstate S service, configure d to do v 3, please ervice De rators.	Self Ser resetti ed to u: when e click o esk on	rvice I ng or se Se mrollin on the [inser	Reset Portal. unlocking the p: curID Two-Fac ng is confirm you following link - t phone number	issword for your tor Authentica Ir SecurID UserN PasswordResetP here] for furthe	domain acc tion as the lame is corr ortalURL]/e r informatio	ount will be a Verification m ect. nroll. n and advice i	much simpler an ethod for this f required.	ıd

Auto-Enrollment

6 out of the 9 Verification Policies can be configured for auto-enrollment, meaning your users do not need to enroll to use the Password Reset Portal. Google, One-Time Passwords, and Questions and Answers, all require user input to enroll, which is why auto-enrollment is not possible for these policies.

The Auto-Enrollment can be done in one of two ways:

- By specifying various settings on each Verification Policy, when the scheduled synchronization
 of Active Directory Security Groups occurs, then auto-enrollment will happen for any accounts
 not already enrolled. This process is initiated by the Password Windows Service, and the
 schedule for this can be found on the screen Administration -> Password Reset Portal
 Administration -> System Settings -> Active Directory Options tab. Please note the 'Manual
 Synchronization' menu option within the UI does not perform the auto-enroll process, on the
 Passwordstate Windows Service does this.
- Via the API(s), it's also possible to script the auto-enrollment for users (please refer to the API Documentation for more information)

Please refer to screenshots/descriptions for each policy of what's required for auto-enrollment.

4.11.1 Duo Authentication

Duo Authentication is a two-factor authentication option from Duo Security - https://duo.com/

For auto-enrollment, by default the 'sAMAccountName' Active Directory Attribute is queried for the user's account, but this can be changed to any AD attribute you like.

	enrollment email 1	enrollment email 2	enrollment email 3
Duo Security Tv	vo-Factor Settings		
Enter your Duo Sec	urity Authentication API set	tings below.	
Integration Key :	DI9MSR4539XIS8HFJ85V		7
Secret Key :	•••••		Q
API HostName :	api-0e51fec9.duosecurity.c	com	
If you would like to option below and s Note: If you ena automatically enroll manually.	auto-enroll users for this Ve pecify settings as appropria ble auto-enrollment, any us ed with the settings below t	erification Policy as part o te. ser's accounts which alrea then next time the Active	f the Active Directory synchronization process, please enable the ady exist in Passwordstate, but have not yet enrolled, they will be Directory Synchronization occurs - either via the schedule, or if run
If you would like to option below and sp Note: If you ena automatically enroll manually.	auto-enroll users for this Ve pecify settings as appropriat able auto-enrollment, any us ed with the settings below t Iment for this Verification	erification Policy as part of te. ser's accounts which alrea then next time the Active Policy:	f the Active Directory synchronization process, please enable the ady exist in Passwordstate, but have not yet enrolled, they will be Directory Synchronization occurs - either via the schedule, or if run
If you would like to option below and sp Note: If you ena automatically enroll manually. Enable Auto-Enrol Yes No	auto-enroll users for this Ve pecify settings as appropria able auto-enrollment, any us led with the settings below t Iment for this Verification	erification Policy as part o te. ser's accounts which alrea then next time the Active Policy:	f the Active Directory synchronization process, please enable the ady exist in Passwordstate, but have not yet enrolled, they will be Directory Synchronization occurs - either via the schedule, or if run
If you would like to option below and sp Note: If you ena automatically enroll manually. Enable Auto-Enrol @ Yes @ No Please specify the accounts.	auto-enroll users for this Ve pecify settings as appropriat able auto-enrollment, any us ed with the settings below t Iment for this Verification Active Directory Attribute	erification Policy as part of te. seer's accounts which alreat then next time the Active Policy: • Name that you would	f the Active Directory synchronization process, please enable the ady exist in Passwordstate, but have not yet enrolled, they will be Directory Synchronization occurs - either via the schedule, or if run
If you would like to option below and sp Note: If you ena automatically enroll manually. Enable Auto-Enrol Ves No Please specify the accounts. SAMAccountName	auto-enroll users for this Ve pecify settings as appropria able auto-enrollment, any us led with the settings below the Iment for this Verification Active Directory Attribute	erification Policy as part of te. ser's accounts which alree then next time the Active Policy: • Name that you would	f the Active Directory synchronization process, please enable the ady exist in Passwordstate, but have not yet enrolled, they will be Directory Synchronization occurs - either via the schedule, or if run
If you would like to option below and sp Note: If you ena automatically enroll manually. Enable Auto-Enrol @ Yes ® No Please specify the accounts. SAMAccountName	auto-enroll users for this Ve pecify settings as appropriat able auto-enrollment, any us ed with the settings below the Iment for this Verification Active Directory Attribute	erification Policy as part of te. ser's accounts which alreat then next time the Active Policy: • Name that you would	f the Active Directory synchronization process, please enable the ady exist in Passwordstate, but have not yet enrolled, they will be Directory Synchronization occurs - either via the schedule, or if run

4.11.2 Email Temporary PIN Code

196

Emailing a Temporary PIN Code can also be used, and will only be valid for a specified amount of time.

For auto-enrollment, by default the 'mail' Active Directory Attribute is queried for the user's account, but this can be changed to any AD attribute you like.

Email Temporary Pin Code Settings Please specify appropriate settings below for when one of the Email Temporary Pin Code authentication options are used. Pin Code Length: 5 Pin Code Expires in Minute(s): 3 Pin Code Expires in Minute(s): 3 Auto-Enrollment Settings If you would like to auto-enroll users for this Verification Policy as part of the Active Directory synchronization process, please enable the option below and specify settings as appropriate. This schedule for Synchronization can be found on the System Settings screen, under the Active Directory Options tab. Note: If you enable auto-enrollment, any user's accounts which already exist in Passwordstate, but have not yet enrolled, they will be automatically enrolled with the settings below then next time the Active Directory Synchronization occurs. This schedule for Synchronization can be found on the System Settings screen, under the Active Directory Options tab. Enable Auto-Enrollment for this Verification Policy: Ves No Please specify the Active Directory Attribute Name that you would like auto-populated into the 'Email Address' field for user's accounts.	
Please specify appropriate settings below for when one of the Email Temporary Pin Code authentication options are used. Pin Code Length: 5 Pin Code Expires in Minute(s): 3 Auto-Enrollment Settings If you would like to auto-enroll users for this Verification Policy as part of the Active Directory synchronization process, please enable the option below and specify settings as appropriate. This schedule for Synchronization can be found on the System Settings screen, under the Active Directory Options tab. Note: If you enable auto-enrollment, any user's accounts which already exist in Passwordstate, but have not yet enrolled, they will be automatically enrolled with the settings below then next time the Active Directory Synchronization occurs. This schedule for Synchronization are be found on the System Settings screen, under the Active Directory Options tab. Enable Auto-Enrollment for this Verification Policy: O Yes No Please specify the Active Directory Attribute Name that you would like auto-populated into the 'Email Address' field for user's accounts.	
Pin Code Length : 5 Pin Code Expires in Minute(s) : 3 Pin Code Expires in Minute(s) : 13 Pin Code Expires in Pin Code Expires	
Pin Code Expires in Minute(s) : 3 Auto-Enrollment Settings If you would like to auto-enroll users for this Verification Policy as part of the Active Directory synchronization process, please enable the option below and specify settings as appropriate. This schedule for Synchronization can be found on the System Settings screen, under the Active Directory Options tab. Note: If you enable auto-enrollment, any user's accounts which already exist in Passwordstate, but have not yet enrolled, they will be automatically enrolled with the settings below then next time the Active Directory Synchronization occurs. This schedule for Synchronization an be found on the System Settings screen, under the Active Directory Options tab. Enable Auto-Enrollment for this Verification Policy: Yes No Please specify the Active Directory Attribute Name that you would like auto-populated into the 'Email Address' field for user's accounts.	
Auto-Enrollment Settings If you would like to auto-enroll users for this Verification Policy as part of the Active Directory synchronization process, please enable the option below and specify settings as appropriate. This schedule for Synchronization can be found on the System Settings screen, under the Active Directory Options tab. Note: If you enable auto-enrollment, any user's accounts which already exist in Passwordstate, but have not yet enrolled, they will be automatically enrolled with the settings below then next time the Active Directory Synchronization occurs. This schedule for Synchronization can be found on the System Settings screen, under the Active Directory Options tab. Enable Auto-Enrollment for this Verification Policy: O Yes No Please specify the Active Directory Attribute Name that you would like auto-populated into the 'Email Address' field for user's accounts.	
If you would like to auto-enroll users for this Verification Policy as part of the Active Directory synchronization process, please enable the option below and specify settings as appropriate. This schedule for Synchronization can be found on the System Settings screen, under the Active Directory Options tab. Note: If you enable auto-enrollment, any user's accounts which already exist in Passwordstate, but have not yet enrolled, they will be automatically enrolled with the settings below then next time the Active Directory Synchronization occurs. This schedule for Synchronization can be found on the System Settings screen, under the Active Directory Options tab. Enable Auto-Enrollment for this Verification Policy: O Yes No Please specify the Active Directory Attribute Name that you would like auto-populated into the 'Email Address' field for user's accounts.	
 Note: If you enable auto-enrollment, any user's accounts which already exist in Passwordstate, but have not yet enrolled, they will be automatically enrolled with the settings below then next time the Active Directory Synchronization occurs. This schedule for Synchronization can be found on the System Settings screen, under the Active Directory Options tab. Enable Auto-Enrollment for this Verification Policy: Yes INO Please specify the Active Directory Attribute Name that you would like auto-populated into the 'Email Address' field for user's accounts. 	
Enable Auto-Enrollment for this Verification Policy: Ves No Please specify the Active Directory Attribute Name that you would like auto-populated into the 'Email Address' field for user's accounts.	
Please specify the Active Directory Attribute Name that you would like auto-populated into the 'Email Address' field for user's accounts.	
mail	
When a user is auto-enrolled, send them an email with the details under the 'Auto-Enrollment Email' tab above: (visible if you enable auto-enrollment)	

4.11.3 Google Authenticator

Google Authenticator is a free two-factor authentication option which can be used on most mobile phones, and desktops.

Rote: There is no Auto-Enrollment option available for this Verification Policy.

Letit Verification Policy

Please update the settings for policy 'Google Authenticator' on each of the Tabs below as appropriate, then click on the 'Save' button.

ise the Google Auth	enticator Verification Method.
olicy, as it requires i	interaction/input from the user to enroll.
	Save Cancel
- -	olicy, as it requires

4.11.4 One-Time Passwords (TOTP or HOTP)

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. If you enable this authentication option, and users have not configured their preferences for their token, they will be prompted to specify their own settings the next time they access Passwordstate.

Rote: There is no Auto-Enrollment option available for this Verification Policy.

S.	Edit	Verification	Policy
----	------	--------------	--------

Please update the settings for policy 'One-Time Passwords (TOTP or HOTP)' on each of the Tabs below as appropriate, then click on the 'Save' button.

		Une-Time Password Autre	ntication below - TOTP can be hardware token or software based.
Allow hardware tok 10	ens to have a maximum	Clock Drift of: specify in seconds	;
Specify the default	Time Step setting (secor	nds) which will apply to r	new user accounts added to Passwordstate:
32		Generally 30 or 60) seconds
ounter-Based (One-Time Password	d Settings	
ounter-Based (Dne-Time Password	d Settings	ithantication halow - HOTD can be hardware token or software based
ounter-Based (Dne-Time Password	d Settings ed) One-Time Password Au	uthentication below - HOTP can be hardware token or software based.
Ounter-Based (Please specify setting Specify the Look Al	Dne-Time Password as for HOTP (Counter-Base lead Window Size for fir	d Settings ed) One-Time Password Au Iding a Counter match:	uthentication below - HOTP can be hardware token or software based.
Ounter-Based (Please specify setting Specify the Look Al 100	Dne-Time Password as for HOTP (Counter-Base read Window Size for fir	d Settings ed) One-Time Password Au nding a Counter match: Look ahead (x) nu	uthentication below - HOTP can be hardware token or software based. mber of counters to find a match
ounter-Based (Please specify setting Specify the Look Al 100 Specify the default	Dne-Time Password as for HOTP (Counter-Base head Window Size for fir <u>number of Digits used for</u>	d Settings ed) One-Time Password Au ding a Counter match: Look ahead (X) nu or the One-Time Passwor	uthentication below - HOTP can be hardware token or software based. mber of counters to find a match rd which will apply to new user accounts added to Passwordstate:
Ounter-Based (Please specify setting Specify the Look Al 100 Specify the default 8	Dne-Time Password as for HOTP (Counter-Base nead Window Size for fir number of Digits used fo	d Settings ed) One-Time Password Au nding a Counter match: Look ahead (X) nu Dor the One-Time Passwor Generally 6 or 8 d	uthentication below - HOTP can be hardware token or software based. mber of counters to find a match rd which will apply to new user accounts added to Passwordstate: igits
Counter-Based (Please specify setting Specify the Look Al 100 Specify the default 8	Dne-Time Password	d Settings ed) One-Time Password Au ding a Counter match: Look ahead (X) nu Dor the One-Time Password Generally 6 or 8 d	uthentication below - HOTP can be hardware token or software based. mber of counters to find a match rd which will apply to new user accounts added to Passwordstate: igits
Counter-Based (Please specify setting Specify the Look Al 100 Specify the default 8 	Dne-Time Password s for HOTP (Counter-Base lead Window Size for fir number of Digits used for Settings	d Settings ed) One-Time Password Au ding a Counter match: Look ahead (x) nu or the One-Time Password Generally 6 or 8 d	uthentication below - HOTP can be hardware token or software based. mber of counters to find a match rd which will apply to new user accounts added to Passwordstate: igits

4.11.5 PIN Number

Similar to a PIN Number for credit cards, and PIN Number can also be used to verify the user's account.

For auto-enrollment, a randomly generated Pin Number, based on the Pin Length Specified, will be generated for the user. It's important the auto-enrollment email option is enabled here, otherwise the user will not know what their Pin Number is.

Letter Contraction Policy

Please update the settings for policy 'PIN Number' on each of the Tabs below as appropriate, then click on the 'Save' button.

verification method	auto-enrollment email
PIN Number Please select the mini	num length of the PIN Number to be used with this Verification Method.
Auto-Enrollment If you would like to au option below and spe Active Directory Optio	Settings to-enroll users for this Verification Policy as part of the Active Directory synchronization process, please enable the cify settings as appropriate. This schedule for Synchronization can be found on the System Settings screen, under the ins tab.
Enable Auto-Enrollm	ent for this Verification Policy:
Kote: A randomly	generated Pin Number, based on the Pin Number Length above, will be emailed to the user when they are auto-enrolled.
When a user is auto- auto-enrollment) Yes O No	enrolled, send them an email with the details under the 'Auto-Enrollment Email' tab above: (visible if you enable
	Save Cancel

4.11.6 Questions and Answers

The Questions and Answers Verification Policy allows the user to choose various questions to enroll with, and then when they attempt to reset their domain account, they must answer two of the questions successfully.

Note: There is no Auto-Enrollment option available for this Verification Policy.

You can also add your own questions, or delete any of the default questions.

🔏 Edit Verification Policy

Please update the settings for policy 'Questions and Answers' on each of the Tabs below as appropriate, then click on the 'Save' button.

	ueiete questions below as appropriate.
Actions	Question
0	In what city did your parents meet?
0	What is the first name of your best friend in school?
0	What is the last name of your favorite school teacher?
0	What is the name of the street where you grew up?
0	What is the name of your favorite sports team?
0	What is your dream job?
0	What is your favorite childrens book?
0	What was the first album that you purchased?
0	What was the first name of your first boss?
0	What was the model of your first car?
•	What was the pame of your first pot?
Add page O	uestion

4.11.7 RADIUS Authentication

If you have a RADIUS server available withing your organization, you can simply specify your RADIUS server configuration details on this screen.

For auto-enrollment, by default the 'sAMAccountName' Active Directory Attribute is queried for the user's account, but this can be changed to any AD attribute you like.

Letter Verification Policy

Please update the settings for policy 'RADIUS Authentication' on each of the Tabs below as appropriate, then click on the 'Save' button.

RADIUS Authentication Settings Please specify settings for your RADIUS server below. Server IP Address: 10.0.97 Server Port Number: 1645 RADIUS Secret: Test Number of Retrise: 3 Send Timeout: 5 S and Timeout: 5 Time to Live (TTL): 50 Auto-Enrollment Settings in seconds If you would like to auto-enroll users for this Verification Policy as part of the Active Directory synchronization process, please enable the option below and specify settings as appropriate. If you would like to auto-enroll users for this Verification Policy as part of the Active Directory synchronization process, please enable the option below and specify settings as a appropriate. If you would like to auto-enroll users for this Verification Policy as part of the Active Directory Synchronization occurs - either via the schedule, or if run manually. Enable Auto-Enrollment for this Verification Policy: W with the settings below then next time the Active Directory Synchronization occurs - either via the schedule, or if run manually. Enable Auto-Enrollment for this Verification Policy: W with the Active Directory Attribute Name that you would like auto-populated into the 'RADIUS Username' field for user's accounts. SMAAccountName When a user is auto-enrollment, send them an email with the details u	verification method	enrollment email 1	enrollment email 2	enrollment email 3				
RADIOS Authentication Settings Please specify settings for your RADIUS server below. Server IP Address: 10.0.097 Server Port Number: 1645 RADIUS Secret: Test Number of Retries: 3 Send Timeout: 5 Receive Timeout: 5 Time to Live (TTL): 50 Auto-Enrollment Settings If you would like to auto-enroll users for this Verification Policy as part of the Active Directory synchronization process, please enable the option below and specify settings as appropriate. If you would like to auto-enroll users for this Verification Policy as part of the Active Directory synchronization process, please enable the option below and specify settings as appropriate. If you would like to auto-enroll users for this Verification Policy as part of the Active Directory synchronization process, please enable the option below and specify settings as appropriate. If you enable auto-enrollment, any user's accounts which already exist in Passwordstate, but have not yet enrolled, they will be automatually enrolled with the settings below then next time the Active Directory Synchronization occurs - either via the schedule, or if run manually. Enable Auto-Enrollment for this Verification Policy: Yes No Please specify the Active Directory Attribute Name that you would like auto-populated into the 'RADIUS Username' field for user's accounts. SaMAccountName When a user is auto-enrollment, send them an email with the details under the 'Auto-Enrollment Email' tab above (visible if you enable auto-enrollment): Yes No 								
Please specify settings for your RADIUS server below. Server IP Address: 10.0.0.97 Server Port Number: 1643 RADIUS Secret: 1643 RADIUS Secret: 15 Send Timeout: 5 Send Timeout: 5 So Cutoe Enrollment Settings If you would like to auto-enroll users for this Verification Policy as part of the Active Directory synchronization process, please enable the option below and specify settings as appropriate. Rote: If you enable auto-enrollment, any user's accounts which already exist in Passwordstate, but have not yet enrolled, they will be automatically enrolled with the settings below then next time the Active Directory Synchronization occurs - either via the schedule, or if run manually. Enable Auto-Enrollment for this Verification Policy: ○ Yes No When a user is auto-enrollment, send them an email with the details under the 'Auto-Enrollment Email' tab above (visible if you enable auto-enrollment): ○ Yes No	RADIUS Authentication Settings							
Server IP Address: 100.0.97 Server Port Number: 1645 RADIUS Secret: Test Number of Retries: 3 Send Timeout: 5 Server Port Number: 1 in seconds Receive Timeout: 5 Server IT meout: 5 Server IT meout: 5 Time to Live (TTL): 50 Auto-Enrollment Settings If you would like to auto-enroll users for this Verification Policy as part of the Active Directory synchronization process, please enable the option below and specify settings as appropriate. Note: If you enable auto-enrollment, any user's accounts which already exist in Passwordstate, but have not yet enrolled, they will be automatically enrolled with the settings below then next time the Active Directory Synchronization occurs - either via the schedule, or if run manually. Enable Auto-Enrollment for this Verification Policy: If yes INO Please specify the Active Directory Attribute Name that you would like auto-populated into the 'RADIUS Username' field for user's accounts. EMMACCOUNTNAME When a user is auto-enrollment, send them an email with the details under the 'Auto-Enrollment Email' tab above (visible if you enable auto-enrollment): I ves INO No	Please specify setting	s for your RADIUS server b	pelow.					
Server Port Number: 1645 RADIUS Secret: Test Number of Retries: 3 Send Timeout: 5 Send Timeout: 5 Send Timeout: 5 Server Port Number: 5 Time to Live (TTL): 50 Auto-Enrollment Settings If you would like to auto-enroll users for this Verification Policy as part of the Active Directory synchronization process, please enable the option below and specify settings as appropriate. Note: If you enable auto-enrollment, any user's accounts which already exist in Passwordstate, but have not yet enrolled, they will be automatically enrolled with the settings below then next time the Active Directory Synchronization occurs - either via the schedule, or if run manually. Enable Auto-Enrollment for this Verification Policy: Yes No Please specify the Active Directory Attribute Name that you would like auto-populated into the 'RADIUS Username' field for user's accounts. SAMAccountName When a user is auto-enrollment, send them an email with the details under the 'Auto-Enrollment Email' tab above (visible if you enable auto-enrollment): * Yes No	Server IP Address:	10.0.0.97						
RADIUS Secret: Image: seconds Number of Retries: 3 Send Timeout: 5 Send Timeout: 5 Send Timeout: 5 Time to Live (TTL): 50 Auto-Enrollment Settings If you would like to auto-enroll users for this Verification Policy as part of the Active Directory synchronization process, please enable the option below and specify settings as appropriate. If you would like to auto-enrollment, any user's accounts which already exist in Passwordstate, but have not yet enrolled, they will be automatically enrolled with the settings below then next time the Active Directory Synchronization occurs - either via the schedule, or if run manually. Enable Auto-Enrollment for this Verification Policy: Ws Solo Please specify the Active Directory Attribute Name that you would like auto-populated into the 'RADIUS Username' field for user's accounts. SaMAccountName When a user is auto-enrollment, send them an email with the details under the 'Auto-Enrollment Email' tab above (visible if you enable auto-enrollment): Yes No 	Server Port Numbe	r: 1645						
Number of Retries: 3 Send Timeout: 5 Send Timeout: 5 Server Timeout: 5 Time to Live (TTL): 50 Auto-Enrollment Settings If you would like to auto-enroll users for this Verification Policy as part of the Active Directory synchronization process, please enable the option below and specify settings as appropriate. Note: if you enable auto-enrollment, any user's accounts which already exist in Passwordstate, but have not yet enrolled, they will be automatically enrolled with the settings below then next time the Active Directory Synchronization occurs - either via the schedule, or if run manually. Enable Auto-Enrollment for this Verification Policy: Yes No Please specify the Active Directory Attribute Name that you would like auto-populated into the 'RADIUS Username' field for user's accounts. sAMAccountName When a user is auto-enrollment, send them an email with the details under the 'Auto-Enrollment Email' tab above (visible if you enable auto-enrollment): Yes No 	RADIUS Secret:	Test						
Send Timeout: 5 in seconds Receive Timeout: 5 in seconds Time to Live (TTL): 50	Number of Retries:	3						
Receive Timeout: 5 in seconds Time to Live (TTL): 50 Auto-Enrollment Settings If you would like to auto-enroll users for this Verification Policy as part of the Active Directory synchronization process, please enable the option below and specify settings as appropriate. If Note: if you enable auto-enrollment, any user's accounts which already exist in Passwordstate, but have not yet enrolled, they will be automatically enrolled with the settings below then next time the Active Directory Synchronization occurs - either via the schedule, or if run manually. Enable Auto-Enrollment for this Verification Policy: • Yes • No Please specify the Active Directory Attribute Name that you would like auto-populated into the 'RADIUS Username' field for user's accounts. SAMAccountName When a user is auto-enrollment, send them an email with the details under the 'Auto-Enrollment Email' tab above (visible if you enable auto-enrollment): • Yes • No	Send Timeout:	5			in seconds			
Time to Live (TTL): 50 Auto-Enrollment Settings If you would like to auto-enroll users for this Verification Policy as part of the Active Directory synchronization process, please enable the option below and specify settings as appropriate. If Note: If you enable auto-enrollment, any user's accounts which already exist in Passwordstate, but have not yet enrolled, they will be automatically enrolled with the settings below then next time the Active Directory Synchronization occurs - either via the schedule, or if run manually. Enable Auto-Enrollment for this Verification Policy: • Yes • No Please specify the Active Directory Attribute Name that you would like auto-populated into the 'RADIUS Username' field for user's accounts. SAMAccountName When a user is auto-enrollment, send them an email with the details under the 'Auto-Enrollment Email' tab above (visible if you enable auto-enrollment): • Yes No	Receive Timeout:	5			in seconds			
Auto-Enrollment Settings If you would like to auto-enroll users for this Verification Policy as part of the Active Directory synchronization process, please enable the option below and specify settings as appropriate. Note: If you enable auto-enrollment, any user's accounts which already exist in Passwordstate, but have not yet enrolled, they will be automatically enrolled with the settings below then next time the Active Directory Synchronization occurs - either via the schedule, or if run manually. Enable Auto-Enrollment for this Verification Policy: Yes No Please specify the Active Directory Attribute Name that you would like auto-populated into the 'RADIUS Username' field for user's accounts. SAMAccountName When a user is auto-enrollment, send them an email with the details under the 'Auto-Enrollment Email' tab above (visible if you enable auto-enrollment): Yes No	Time to Live (TTL):	50						
Accounts. SAMAccountName When a user is auto-enrollment, send them an email with the details under the 'Auto-Enrollment Email' tab above (visible if you enable auto-enrollment): (a) Yes () No	 Note: If you enable automatically enrolled manually. Enable Auto-Enrollin Yes No Please specify the Automatical systems of the system	le auto-enrollment, any us d with the settings below t nent for this Verification	er's accounts which alrea then next time the Active Policy:	dy exist in Passwordstate, b Directory Synchronization (but have not yet enrolled, they will be occurs - either via the schedule, or if run			
SAMAccountName When a user is auto-enrollment, send them an email with the details under the 'Auto-Enrollment Email' tab above (visible if you enable auto-enrollment):	accounts.							
When a user is auto-enrollment, send them an email with the details under the 'Auto-Enrollment Email' tab above (visible if you enable auto-enrollment): Image: Wes Image: No 	sAMAccountName							
Cauco	When a user is auto enable auto-enrollm	enrollment, send them a lent):	an email with the details	under the 'Auto-Enrollm	eent Email' tab above (visible if you			
SAVE					Save Cancel			

4.11.8 RSA SecurID Authentication

RSA SecurID is a two-factor authentication option (hardware or software tokens) provided by EMC - <u>https://www.rsa.com/en-us/products/rsa-securid-suite</u>

For auto-enrollment, by default the 'sAMAccountName' Active Directory Attribute is queried for the user's account, but this can be changed to any AD attribute you like.

Please refer to the instructions provided by Click Studios to install the required SecurID agent files on your Passwordstate web server.

Letter Verification Policy

Please update the settings for policy 'RSA SecuriD Authentication' on each of the Tabs below as appropriate, then click on the 'Save' button.

erification method	enrollment email 1	enrollment email 2	enrollment email 3
SecurID Authent	ication		
	leation		
There are no options	that need to be configure	ed to use the SecurID Auth	entication Verification Method.
There are certain con to the Password Rese	figuration steps outside o t Portal manual for furthe	f the Passwordstate user in rinstructions.	nterface to allow this authentication method to work, and please refer
Auto-Enrollment	Settings		
If you would like to a option below and spe Active Directory Opti	uto-enroll users for this V ecify settings as appropria ons tab.	erification Policy as part of ite. This schedule for Syncl	the Active Directory synchronization process, please enable the pronization can be found on the System Settings screen, under the
Note: If you enable automatically enrolle can be found on the	le auto-enrollment, any u d with the settings below System Settings screen, u	ser's accounts which alrea then next time the Active nder the Active Directory (dy exist in Passwordstate, but have not yet enrolled, they will be Directory Synchronization occurs. This schedule for Synchronization Options tab.
Enable Auto-Enrolln	ent for this Verification	Policy:	
🔾 Yes 💿 No			
Please specify the A accounts.	ctive Directory Attribut	e Name that you would I	ike auto-populated into the 'SecurID User ID' field for user's
sAMAccountName			
When a user is auto auto-enrollment)	enrolled, send them an	email with the details u	nder the 'Auto-Enrollment Email' tab above: (visible if you enable
010 010			
			Save Ca

4.11.9 SAML Authentication

The Password Reset Portal can also authenticate to any SAML2 compliant provider for a verification policy.

In order to use SAML2 authentication, you must specify the following settings - each of these settings can be obtained within the 'Application' configured in your SAML2 Provider account:

- Certificate Type either SHA1 or SHA256
- X.509 Certificate
- IDP Target URL
- IDP Issuer URL
- Audience Restriction (Mandatory for Azure AD and ADFS, and For Azure AD, it is the 'Identifier' value, and ADFS is the 'Relying party trust identifier' setting) generally your Passwordstate URL is specified for this.

SAML User Identifier

Passwordstate can be configured to match certain "identifiers" for a user's account i.e. UserID, Email Address or UserPrincipalName

Additional Authentication Option

If required, you can also enforce an additional authentication option on user's, once they have successfully finished their SAML Authentication

Logout URL

If you specify a Logout URL for your SAML Provider, then when users log out of the Portal they will also be redirected to your SAML provider to log out of the active SAML session.

Each SAML2 Provider has different terminology for configuring the required URLs in their 'Application', and you can view several examples in the following section - <u>SAML2 Provider</u> <u>Examples</u>

When specifying settings for your SAML provider, there are specific URLs that need to be set for your Password Reset Portal URL - do not specify the URL for your normal instance of Passwordstate. Below is an example for Azure AD:

Azure AD Field	Passwordstate Value
Identi fier (Entit y ID):	Audience Restriction - normally your Reset Portal URL - let's call it <u>https://myportal.domain.com</u> for this example
Reply URL:	https://myportal.domain.com/account/SAMLLogin
Sign on URL:	https://myportal.domain.com
Relay State:	https://myportal.domain.com/account/SAMLLogin

5 KB Articles

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

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

Passwordstate Disaster Recovery Encrypt Settings in Configuration Files Export & Purging Auditing Data Export All Passwords and Import into KeePass Security Response Headers in Web.config Files

5.1 Passwordstate Disaster Recovery

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

Disaster Recover Process	Description
Passwordstate Web Site Restore	Reinstall the Passwordstate Web Site
Passwordstate Database Restore	Restore a copy of your database
Rebuilding the Web.config File	Rebuild the settings in the web.config file if required
Resetting Password for	Resetting the password for the SQL Account
Passwordstate_User SQL Account	passwordstate_user
Recovery Emergency Access Password	Recover your Emergency Access Password, if needed,
	to resolve Unauthorized Web Server message

5.1.1 Passwordstate Web Site Restore

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

- Download the latest build of Passwordstate from here Click Studios's web site here https://www.clickstudios.com.au/passwordstate-checksums.aspx. Please confirm the checksum of the file you are downloading using the PowerShell command of: Get-FileHash passwordstate.zip -Algorithm SHA256
- Unzip the Passwordstate.zip file from your download above
- Use the following document as a guide for reinstalling the software <u>https://www.clickstudios.com.au/downloads/version9/Installation_Instructions.pdf</u>
- Before you open your browser and point it at the site for the first time, you need to restore a copy of your web.config file over the top of the existing file which exists in the folder c: \inetpub\passwordstate. If you do not have a backup of this file, or you have encrypted the ConnectionString or AppSettings sections, then please follow these instructions for rebuilding this file with the correct configuration settings - <u>Rebuilding the Web.config File</u>. Note: if you are using the Backup feature in Passwordstate, the web.config file will be backed up and stored in your backup zip file
- If you also need to restore a copy of your database, then follow these instructions <u>Passwordstate Database Restore</u>
- Now when you open your browser and navigate to the Passwordstate web site, you may see a screen which indicates that your new web server is "Not Authorised" to host the Passwordstate web site. This will occur if your server name has changed, or if you did not have a backup of your web.config file to use above. To fix this issue, you can simple enter your Emergency Access login password. If you have forgotten this password, please follow these instructions for contacted Click Studios so we can help you recovery it <u>Recovery Emergency Access Password</u>

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

5.1.2 Passwordstate Database Restore

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

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



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

206	Passwordstate Security Administrators Manual
200	Tasswordstate Occurity Administrators Manuar

极	Restore Database -	_ D X
🐼 No backupset selected to be r	restored.	
Clear to be reacting the sector to be reacting to the sector to the sector to be reacting to the sector to be reacting to the sector to t	extore.	v m v Timeline
Connection WIN2K12TEST1 [HALOX\msand]		
View connection properties Progress		
Ready		Verify Backup Media
	ОК Се	ncel Help

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



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

5 <u>5</u>	Restore Database - passwordstate	_ _ ×
🕕 Ready		
ge resed ∰ General ∰ Files ∰ Options		
Connection		
View connection properties		
Progress		
Oone Done		Verify Backup Media
		OK Cancel Help

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



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

210 Passwordstate Security Administrators Manual



8	Login -	New 📃 🗖 🗙
Select a page	Script 📑 Help	
Server Roles	Login name:	passwordstate_user Search
Securables	Windows authentication SQL Server authentication	
	Password:	•••••
	Confirm password:	••••••
	Old password:	
	Enforce password policy	tion
	User must change passy	and at next login
	 Mapped to certificate 	✓
	 Mapped to asymmetric key 	✓
Connection	Map to Credential	✓ Add
Server: WIN2K12TEST1	Mapped Credentials	Credential Provider
Connection: HALOX\msand		
View connection properties		
Progress		Remove
Ready	Default database:	passwordstate
-4D-	Default language:	<default></default>
		OK Cancel

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

Object Explorer	▼ ∓ ×	
Connect 🕶 🛃 🜉 🔳 🍸 🛃 🍒		
 WIN2K12TEST1 (SQL Server 12.0.200) Databases Databases Database Snapshots Malabase Snapshots HALOX (Second State) HALOX	0 - HALOX\msand) singLogin## onLogin## ER	
A passwordstate_user A sa	New Login	
	Script Login as	/
Credentials Cryptographic Providers	Policies	
	Facets	
🕀 🚞 Server Audit Specification	Start PowerShell	
	Reports •	
🗉 🚞 AlwaysOn High Availability	Rename	
🗄 🧰 Management	Delete	
Integration Services Catalogs Sol Server Agent Sol Serv	Refresh	
in in second right	Properties	

• And select db_owner rights to the Passwordstate database

3	Login Properties - passwordstate_user	D X
Select a page General Server Roles User Mapping Securables Status	Script Help Users mapped to this login: Map Database User Default Schema master model msdb Passwordstate passwordstate_user tempdb Guest account enabled for: passwordstate	
Connection		
Server: WIN2K12TEST1 Connection: HALOX\msand Wiew connection properties	db_accessadmin db_backupoperator db_datareader db_datawriter db_ddladmin db_denydatareader db_denydatareader db_denydatareader db_denydatawriter ✓ db_owner	
Progress	db_securityadmin	
C Ready	✓ public	
	ок с	ancel

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

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

5.1.3 Rebuilding the Web.config File

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

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

- The database connection string
- The SetupStage key
- And the Secret1 and Secret2 keys



Modify Web.Config File

- The following settings need to be updated in the PasswordstateConnectionString
- Data Source this is the host name of your database server. If you have a specific Instance Name for you SQL install as well, this will need to be appended i.e. HostName\SQLExpress
- User ID this should be passwordstate_user
- The password for the passwordstate_user SQL account (if you are not sure of what this password would be, there are instructions below on how to reset this)
- The SetupStage key needs to be set to "Setup Complete"
- The PassiveNode key can be deleted, as this is only used during new installs of Passwordstate, and is removed after the install is complete
- Copy the Secret1 and Secret2 values across from a backup of your previous web.config file if available. If not, during the initial install of Passwordstate you would have been asked export your encryption keys to a password protected zip file - these encryption keys can also be exported anytime from the screen Administration -> Encryption Keys. Note: if you do not have these secrets, it is not possible to recover your system.

Reset Password for Passwordstate_User SQL Account

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

5.1.4 Resetting Password for Passwordstate_User SQL Account

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

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

Object Explorer	▼ ₽×					
Connect 🕶 🛃 🛃 🔳 🍸 🛃 🎿						
□ 🔂 WIN2K12TEST1 (SQL Server 12.0.2000 - HALOX\msand)						
🖃 🚞 Databases						
표 🚞 System Databases						
🕀 🧰 Database Snapshots						
🔄 📙 passwordstate						
E Security						
Logins ##MS PolicyEventProcess	inglogin##	-				
A ##MS_PolicyTsqlEvecutio	nl ogin##					
A HALOX\msand						
📕 HALOX\passmsa\$						
NT AUTHORITY\SYSTEM						
NT SERVICE\MSSQLSERVE	R					
A NT SERVICE\SQLSERVERA	GENT					
A NT SERVICE\SQLWriter						
A NT SERVICE\Winingmt						
passwordstate_user	New Login					
ra Server Roles	Script Login as					
Credentials	Delisies					
🗉 🚞 Cryptographic Providers	Policies F					
🕀 🧰 Audits	Facets					
🕀 🚞 Server Audit Specification	Start PowerShell					
Server Objects Penlication	Reports +					
AlwaysOn High Availability	Pename					
	Delete					
Integration Services Catalog	Delete					
🗉 📆 SQL Server Agent	Refresh					
	Properties 🥖					

đ	Login Properties - pa	asswordstate_user		– – X
Select a page	🖾 Script 🔻 📑 Help			
Server Roles User Mapping Securables Status	Login name: Windows authentication SQL Server authentication Password: Confirm password: Specify old password Old password: Enforce password policy Enforce password expira User must change passw Mapped to certificate Mapped to asymmetric key	passwordstate _user	~	Search
Connection	Map to Credential		~	Add
Server: WIN2K12TEST1 Connection: HALOX\msand Wiew connection properties	Mapped Credentials	Credential	Provider	
Progress				Remove
Ready	Default database: Default language:	passwordstate English	~	
	·		ок	Cancel

5.1.5 Recovery Emergency Access Password

If you need Click Studios' help in recovering your Emergency Access login password, please follow these instructions:

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

Use Passwordstate SELECT EA_Password, Secret3, Secret4 FROM SystemSettings

 Log a Support Ticket via the following page on our web site <u>https://www.clickstudios.com.au/support.aspx</u> and provide the results of the SQL Query above, and also a copy of your web.config file, which is generally located in the path of c: \inetpub\passwordstate (Note: If the appSettings section is encrypted in your web.config file, you will need to decrypt this before sending to us by following the instructions below)
Decrypt appSettings Section in Web.Config File

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

5.2 Controlling Settings for Multiple User Accounts

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

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

User Preferences

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

Password List Screen Options

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

Home Page and Folder Screen Options

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

Mobile Access Options

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

Password List Options

When creating new Shared Password Lists, base the settings on the following Template's settings When creating new Shared Password Lists, base the permissions on the following Template's permissions

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

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

Note 2: You can have more than one policy applied to a user's account, but you should use the **Check for Conflicts** button after applying permissions to the policy.

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

III Screen Options
Please review each of the tabs below, and customize the page as required.
Please note your Security Administrators of Passwordstate have set various preferences for you via a User Account Policy, which cannot be changed. These disabled options will have a Red flag displayed next to them.
password columns passwords grid recent activity grid grid paging style chart settings
Please select which Paging style you would like to use for the Passwords and Recent Activity Grids - The pagers will appear in the footer of the grid.
🔍 Next Previous Buttons 💿 Slider 🔍 Numeric Pages 📜
Next Previous Buttons Slider Numeric
Change page: H + H + 1 2 3 4 5 6 7 8 9 10
Save Cancel

5.3 Encrypt Settings in Configuration Files

To further strengthen the security of Passwordstate, it is strongly recommended you encrypt specific settings in various Passwordstate configuration files. This encryption is performed using commands in Internet Information Services (IIS), as provided by Microsoft Corporation.

Note: If you encrypt the AppSettings section of the web.config file for the Passwordstate Web Site, it is imperative you keep an exported copy of your encryption keys in a safe place, as they may be required in the event of a server rebuild, or server move. You can export your encryption keys to a password protected zip file under Administration -> Encryption Keys once you have access to your website.

Please follow these instructions for encrypting various configuration files, and the installation paths specified are the defaults, but may be different for you.

Encrypting the Web.config file for your Passwordstate Installation

These instructions relate to your standard installation of Passwordstate.

Database Connection String

- Open a command prompt and type CD C:\Windows\Microsoft.NET\Framework64\v4.0.30319
- Type the following:
- o aspnet_regiis.exe -pef "connectionStrings" "c:\inetpub\passwordstate"
- Then restart the Passwordstate Windows Service

appSettings Section

- Open a command prompt and type CD C:\Windows\Microsoft.NET\Framework64\v4.0.30319
- Type the following:
 o aspnet regils.exe -pef "appSettings" "c:\inetpub\passwordstate"
- Then restart the Passwordstate Windows Service

Encrypting the Web.config file for Passwordstate App Server Web Site

These instructions are only relevant for the Passwordstate App Server, which is used for the native iOS and Android Mobile Apps, and also for the Self Destruct Message web site if you wish to use a separate installation for this module.

Database Connection String

- Open a command prompt and type CD C:\Windows\Microsoft.NET\Framework64\v4.0.30319
- Type the following:
 - o aspnet_regiis.exe -pef "connectionStrings" "c:\inetpub\PasswordstateAppServer"
- Then restart the Passwordstate Windows Service

appSettings Section

- Open a command prompt and type CD C:\Windows\Microsoft.NET\Framework64\v4.0.30319
- Type the following:

- o aspnet_regiis.exe -pef "appSettings" "c:\inetpub\PasswordstateAppServer"
- Then restart the Passwordstate Windows Service

Encrypting the PasswordstateAgent.exe.config file for the Remote Site Locations Agent

These instructions relate to the Remote Site Locations module, if you have purchased licenses and deployed agents for this module.

appSettings Section

- Stop the Passwordstate Agent Service
- Rename the file PasswordstateAgent.exe.config to web.config
- Open a command prompt (as Admin) and type CD C: \Windows\Microsoft.NET\Framework64\v4.0.30319
- Type the following command to encrypt these settings: aspnet_regiis.exe -pef "appSettings" "C: \Program Files (x86)\Passwordstate Agent"
- Rename the web.config file back to PasswordstateAgent.exe.config
- Restart the Passwordstate Agent Service

Decrypting Configuration Files

In the event you need to decrypt any sections of the configuration files mentioned above. the same aspnet_regiis.exe file is used, but instead of the parameter of **-pef**, you instead use **-pdf**.

5.4 Export & Purging Auditing Data

Two tables are used for storing Auditing data - Auditing and AuditingArchive.

By default, when the number of rows in the Auditing table reach 500,000 the Passwordstate Windows Service will start moving records into the AuditingArchive, to ensure the number of records in the Auditing table do not get excessive - helping with performance within the UI.

To count the number of rows in each table, you can use the SQL commands below - use SQL Server Management Studio to execute these queries:

```
USE Passwordstate
SELECT COUNT(*) FROM Auditing
SELECT COUNT(*) FROM AuditingArchive
```

If the number of rows in the Auditing table have exceeded 500,000, then possible causes are:

1. The setting to move data between tables on the screen Administration -> System Settings -> Auditing tab, has been disabled

2. You do not have a "Primary" server configured on the screen Administration -> Authorised Web Servers

3. There is some sort of exception happening in the Passwordstate Windows Service, and these should be logged in the Windows Application Event Log, on your "Primary" Passwordstate web server.

If you require assistance in determining why you have excessive Auditing data, please log a support ticket here <u>https://www.clickstudios.com.au/support.aspx</u>

Exporting Data

If you would like to export some data from either table, before purging the data, you can follow these guidelines:

1. Below is a SQL Query that will query all Auditing data older than 3 years - you can modify the number of months as appropriate, or change the FROM clause to instead query the AuditingArchive table

2. With this query, you can then use the 'Export' functionality in SQL Management Studio, to export this data - see screenshot below of where to find this Export menu

3. When exporting, it is advised to use the text file format for the file, as Excel has row limitations

-- Select all Auditing records older than X months so they can be archived outside of the Passwordstate database

USE Passwordstate

DECLARE @OlderThanMonths int = 36 --3 years
SELECT * FROM [Auditing] (NOLOCK) WHERE (AuditDate <= DATEADD(month, @OlderThanMonths, GetDate())) ORDER BY AuditID ASC</pre>



Purging Data

Once you have exported the required data, you can use the SQL code below to purge this data from the database - again, change the table name to AuditingArchive, if you wish to remove data from that table:

```
DECLARE @LastID bigint = (SELECT TOP(1) AuditID FROM [Auditing] (NOLOCK) WHERE
(AuditDate <= DATEADD(month, -@OlderThanMonths, GetDate())) ORDER BY AuditID DESC)
WHILE @StartID < @LastID
BEGIN
    SET @EndID = @StartID + @BatchSize
        -- We don't want to exceed the number of specified rows to keep in the Auditing
table, so this If statement is to ensure the 'Batch Size' does not cause this
    IF @EndID > @LastID
    BEGIN
        SET @EndID = @LastID
    BEGIN
        SET @EndID = @LastID
    END
    DELETE FROM [Auditing]
    WHERE (AuditID BETWEEN @StartID AND @EndID)
    SET @StartID = @EndID + 1
END
```

Truncating All Data in the AuditingArchive table

If you do not wish to keep any records in the AuditingArchive table, you can remove them all by using the SQL code below:

USE Passwordstate TRUNCATE TABLE AuditingArchive

5.5 Export All Passwords and Import into KeePass

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

- Go to the page in Passwordstate Administration -> Export All Passwords
- Select the option 'KeePass Compatible CSV file', and check/uncheck the Auditing option as appropriate
- Save the exported csv file somewhere safe
- Open KeePass and create a new empty database
- From the 'File' menu, select 'Import'
- Select the 'Generic CSV Importer' option, browser to the saved csv file above, and click on the 'OK' button
- On the 'Structure' tab, select the 'Ignore First Row' option, deselect the option 'Interpret \ as an
 escape character', and ensure the fields selected match the screenshot below (you will need to
 use the 'Add Field' feature on this screen to do this). Make sure you create the 10 Generic Fields
 as well

Generic CSV Importer Import data from a file containing comma-separated values (CSV). Encoding Structure Preview Syntax Field separator:	Generic CSV Importer				×
Encoding Structure Preview Syntax Field separator: Field Semantics Semantics Semantics Separator the loyout fields on d their order) of the CSV file: Field Group Title User Name String (Description) String (AccountType) URL Expiry Time String (OTPUIn) Password Notes String (GenericField1) String (GenericField2) String (GenericField3) Field Add Field	Generic CS	V Importer m a file containing comma-sep	arated values (CSV).		00111
Semantics	Encoding Structure Previe Syntax Field separator: . Text qualifier: " Ignore first row Remove white space c	Record sep	barator: {New line} ∽ et "\" as an escape character of fields		
	Semantics Specify the layout fields an Field Group Title User Name String (Description) String (Account Type) URL Expiry Time String (OTPUri) Password Notes String (GenericField 1) String (GenericField 2) String (GenericField 3)	d their order) of the CSV file:	Add field Type: Name: Format:	String OTPUri	 ✓ Help Add

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

5.6 Multiple Options for Hiding Passwords

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

SQL S	erver		🔲 Favorite 🛛 🛡 Share	ed List (Admin Access) 🛛 🛟 S	ync Enabled 👘 🤏 Gui	ide 🛛 📸 Strength Pol
Actions	Title	User Name	Description	Password	Password Strength	Expiry Date
0	aaa-record		Test PS2	***********	****	
0	bank1		new description2	******* 😫	****	
0	gsand		Google Login	******	****	
0	sa 🧠	sa 😫	SQL Account 1	*****	****	3/03/2014
0	sql&	sqlrepl1 😫	SQL Replication Account	******	> * * * * *	
0	sql_pass2<= 🦏		SQL Account 2	******** 👱	****	27/01/2013
0	sqlaccount'1 🦏		SQL Server Prod Account 1	******	****	31/07/2009
0	sqlaccount3		SQL Account 3.2	******** 😢	****	4/03/2014
0	sqltest3	SQL Test 3 Account 😫	Test account for SQL 3.3	***************************************	****	

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

Option 1 – Hide Based on a Set Time

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

Automatically hide visible passwords based on the following conditions (in seconds):

● Set Time ○ Password Complexity ○ Password Length

_	
С	
-	•

specify 0 to disable

Option 2 – Hide Based on Complexity of the Password

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

Automatically hide visible passwords based on the following conditions (in seconds):

○ Set Time ● Password Complexity ○ Password Length

Very Poor	Weak	Average	Strong	Excellent
2	4	6	8	10

Option 3 – Hide Based on Password Length

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

Automatically hide visible passwords based on the following conditions (in seconds):						
○ Set Time ○ Password Complexity						
Length 1	Length 2	Length 3				
<= 5	<= 10	>= 11				
Hide in 5	Hide in 7	Hide in 15				

5.7 Security Response Headers in Web.config Files

The main Passwordstate web site, as well as the Password Reset Portal web site, all use web.config files to function.

Each of these files have some custom HTTP Response Headers added to them, to strengthen the security of each web site. If you have deployed the Self Destruct Web Site separately from your standard Passwordstate install, or if you are using the Password Reset Portal module, it's not possible to modify the contents of the web.config files during an upgrade, due to the manual nature of upgrading these installations.

Below is a description of the headers which should exist in each file, and we recommend you review these files and add these headers if they are missing. We've included the text values beneath each screenshot, so you're able to cut and paste the details if required.

Main Passwordstate Web Site (should already be included after an upgrade) Location: C:\inetpub\Passwordstate\web.config



<httpProtocol>

```
<customHeaders>
<add name="X-UA-Compatible" value="IE=edge" />
<add name="Cache-Control" value="max-age=0, no-cache, must-revalidate" />
<add name="Expires" value="Thu, 01 Jan 1970 00:00:00 GMT" />
<add name="Pragma" value="no-cache" />
<add name="Strict-Transport-Security" value="max-age=31536000" />
<remove name="X-Powered-By"/>
</customHeaders>
</httpProtocol>
```

Password Reset Portal Web Site

Location: c:\inetpub\PasswordstateResetPortal\web.config



<httpProtocol>

<customHeaders>

```
<add name="X-UA-Compatible" value="IE=edge" />
<add name="Strict-Transport-Security" value="max-age=31536000" />
<remove name="X-Powered-By"/>
</customHeaders>
</httpProtocol>
```