Passwordstate

Enterprise Password Management

Passwordstate Security Administrators Manual

Table of Contents

Part V KB Articles 203

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:

- Passwordstate Administration - Administration of the core of the product, relating to Privileged Account Management (PAM)
- Remote Site Administration - Creating and monitoring the status of any Remote Site Agent deployments
- Password Reset Portal Administration - 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
Backups	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
Error Console	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,

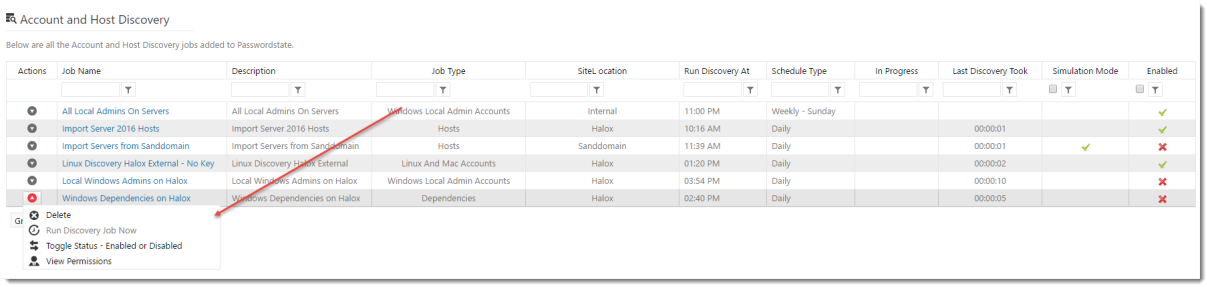
	querying active directory, etc. This screen allows you to add those accounts to be used
PowerShell Scripts	Each of the various default PowerShell scripts for Account Discovery, Password Resets and Account Heartbeat are available on this screen.
Remote Session Management	Manage permissions and settings 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
Reporting	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
System Settings	System Settings is used to manage the majority of system wide settings for Passwordstate
User Accounts	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



2.2 Active Directory Domains

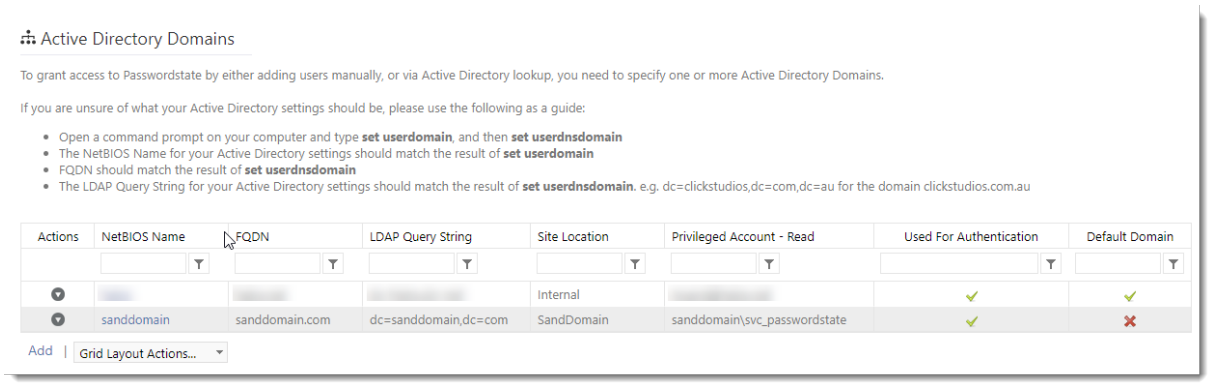
The Active Directory Domains screen is used primarily for two purposes:

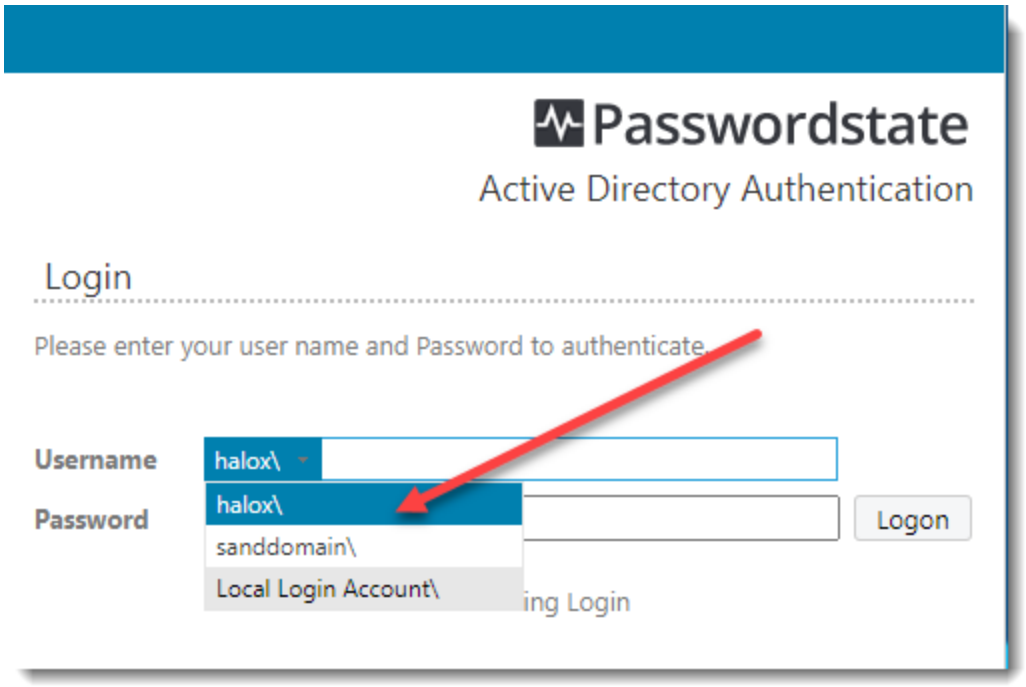
- Adding domains which will be used to authenticate to access the Passwordstate web site
- Adding domains which will be used to perform password resets for accounts on those domains

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 Privileged Account Credentials 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.



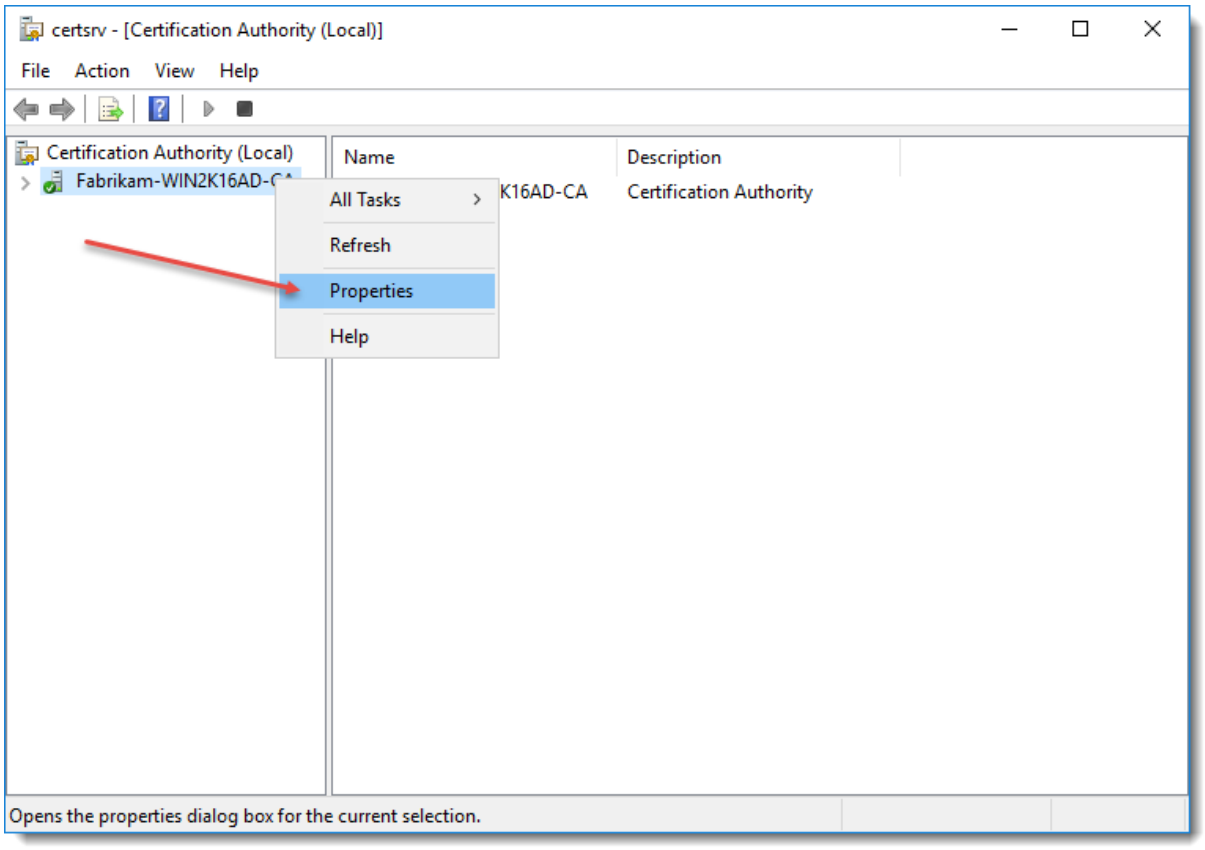


LDAPS and Non-Trusted Domains

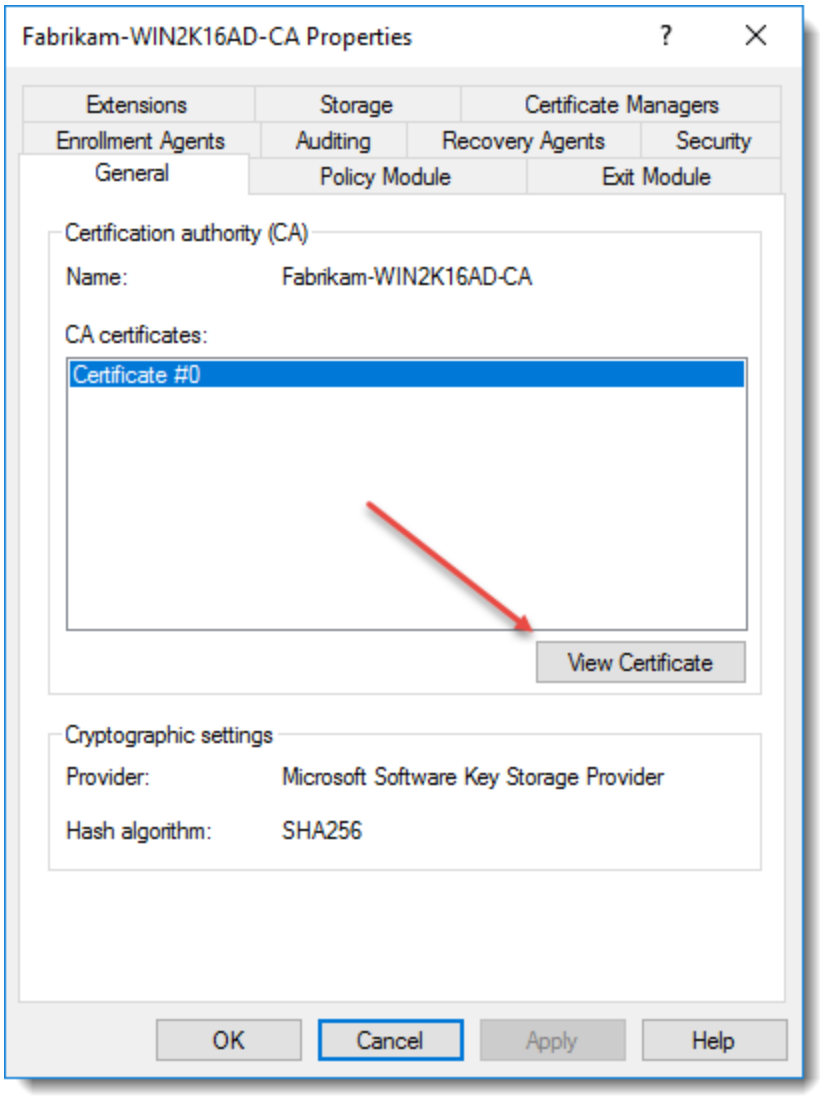
If you also want Passwordstate to communicate to non-trusted domains with LDAPS, i.e. other domains your web server is not a member of, then you will need to export the CA certificate from these domains, and import them onto your Passwordstate web server. If you have Passwordstate installed on a server 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

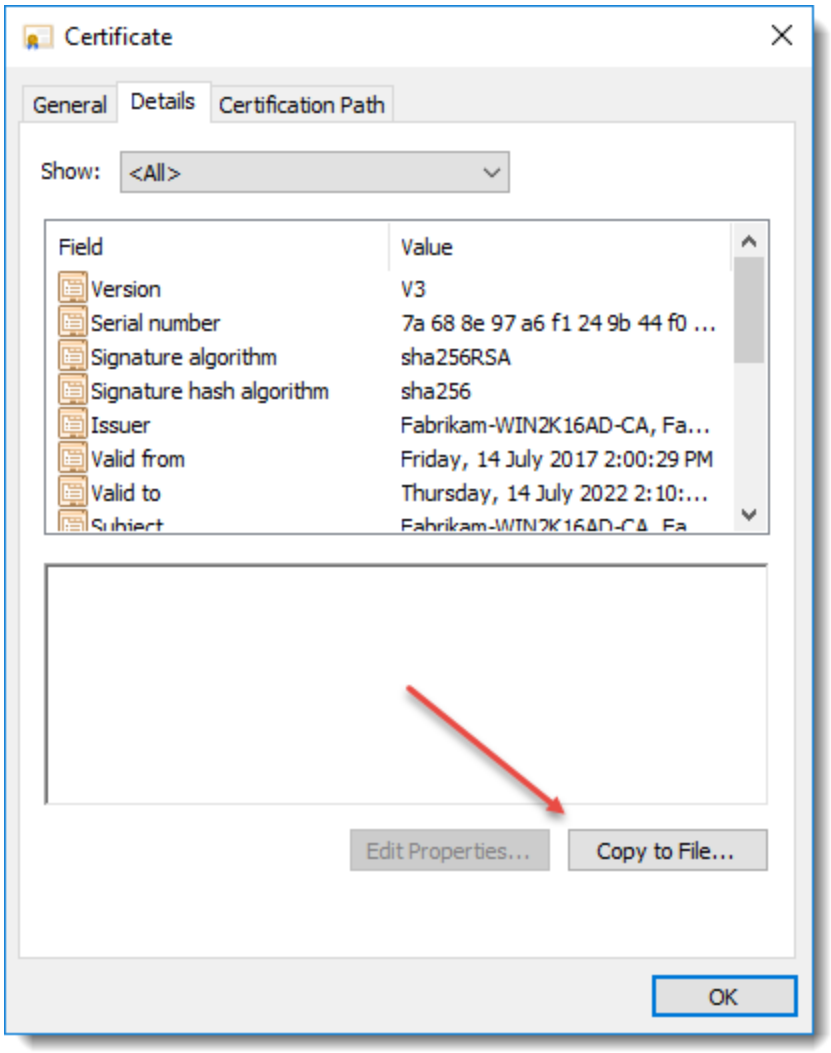
- On your server that has the CA installed, Click Start > Control Panel -> System and Security -> Administrative Tools > Certificate Authority to open the CA Microsoft Management Console (MMC) GUI
- Right-click the CA server and select Properties



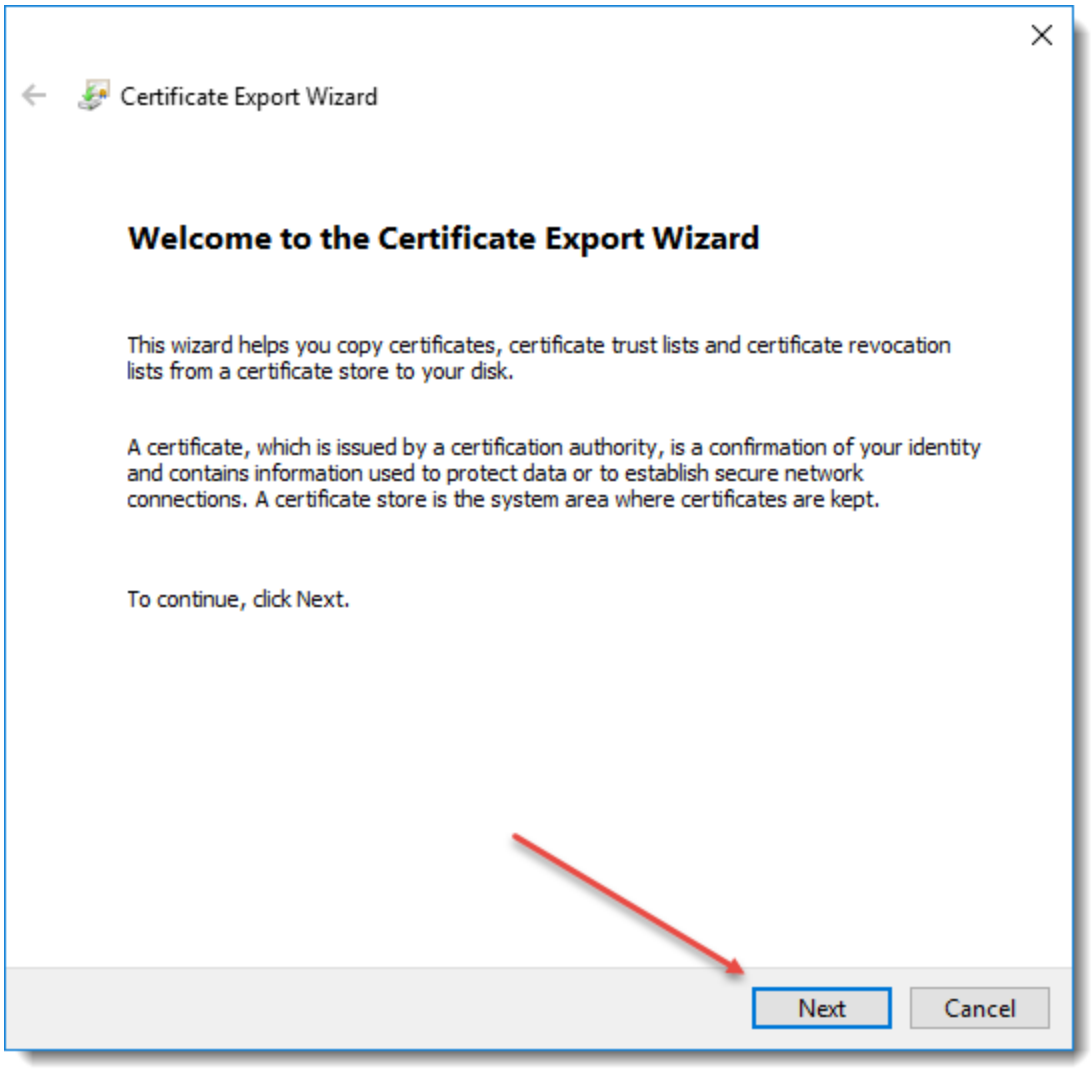
- From the General Menu, click View Certificate



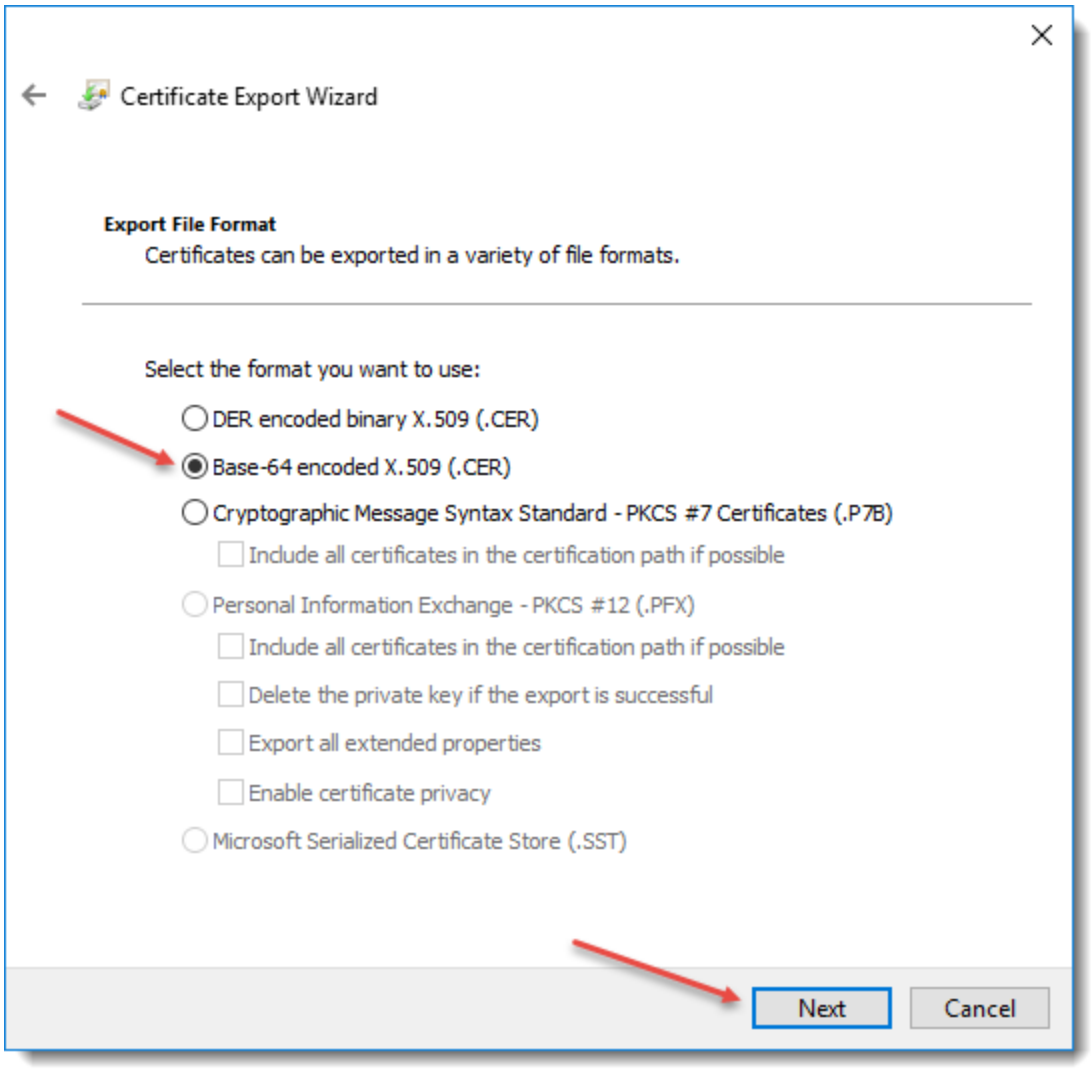
- On the Details tab, click Copy to File



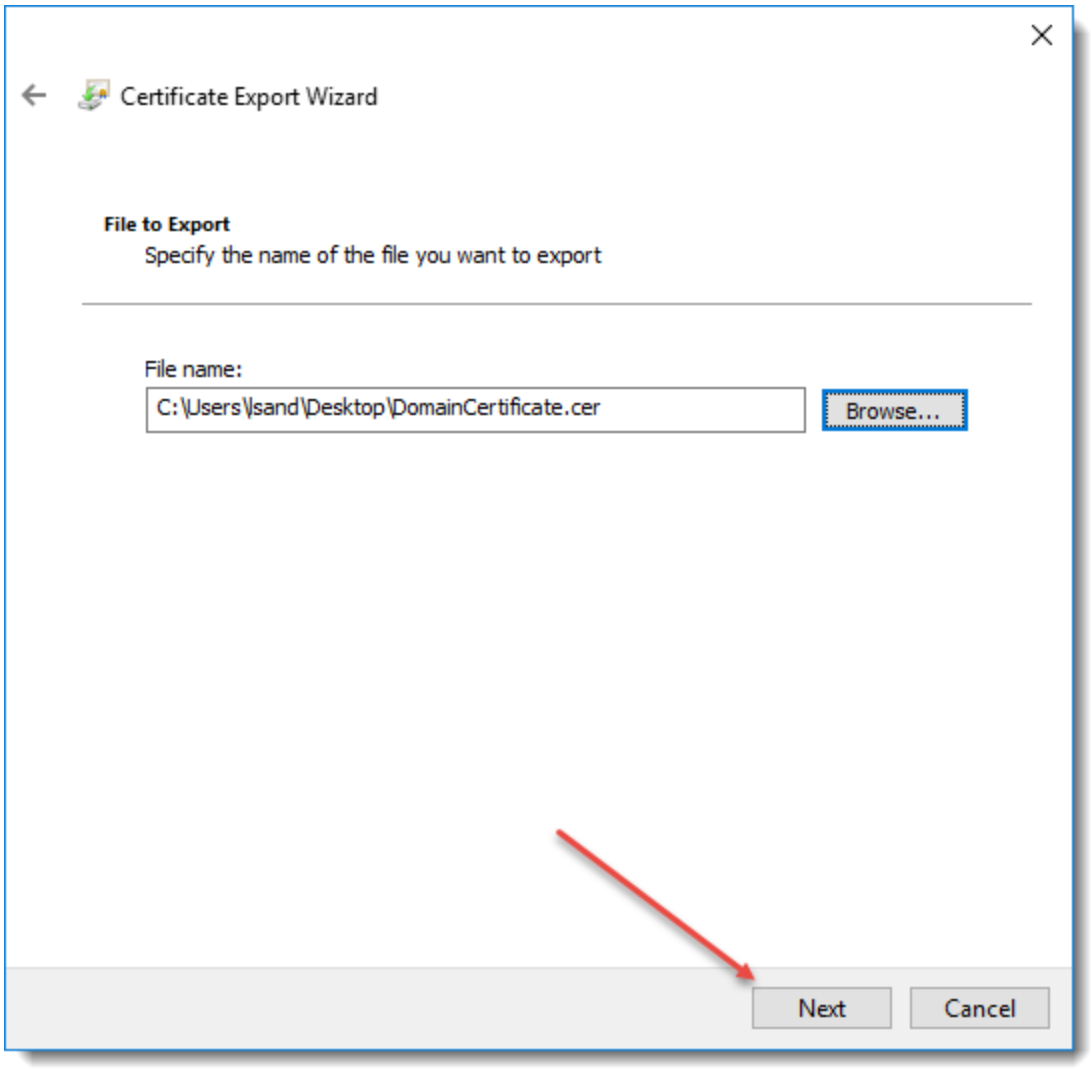
- Click Next



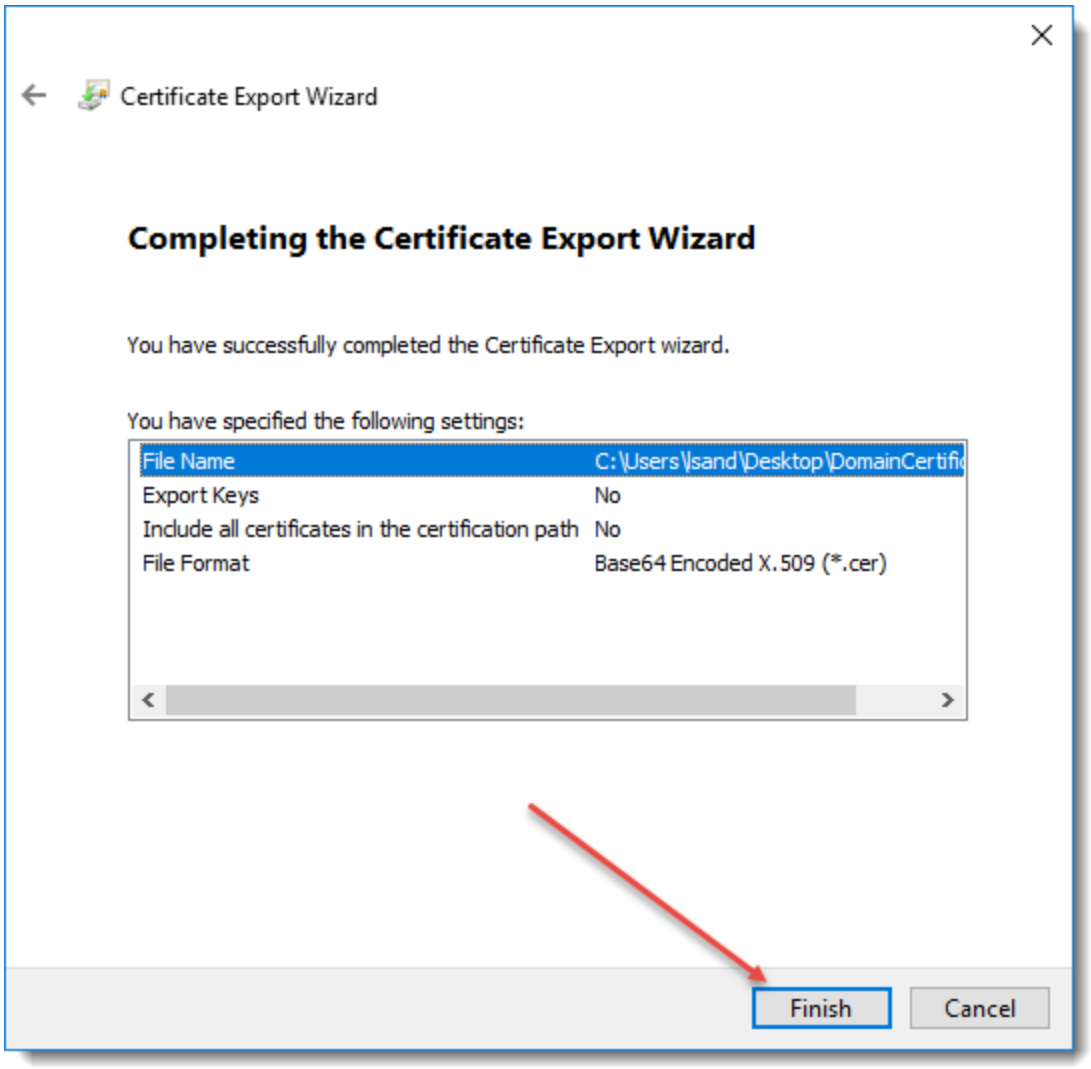
- Choose Base-64 encoded X.509(.CER) and click Next



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



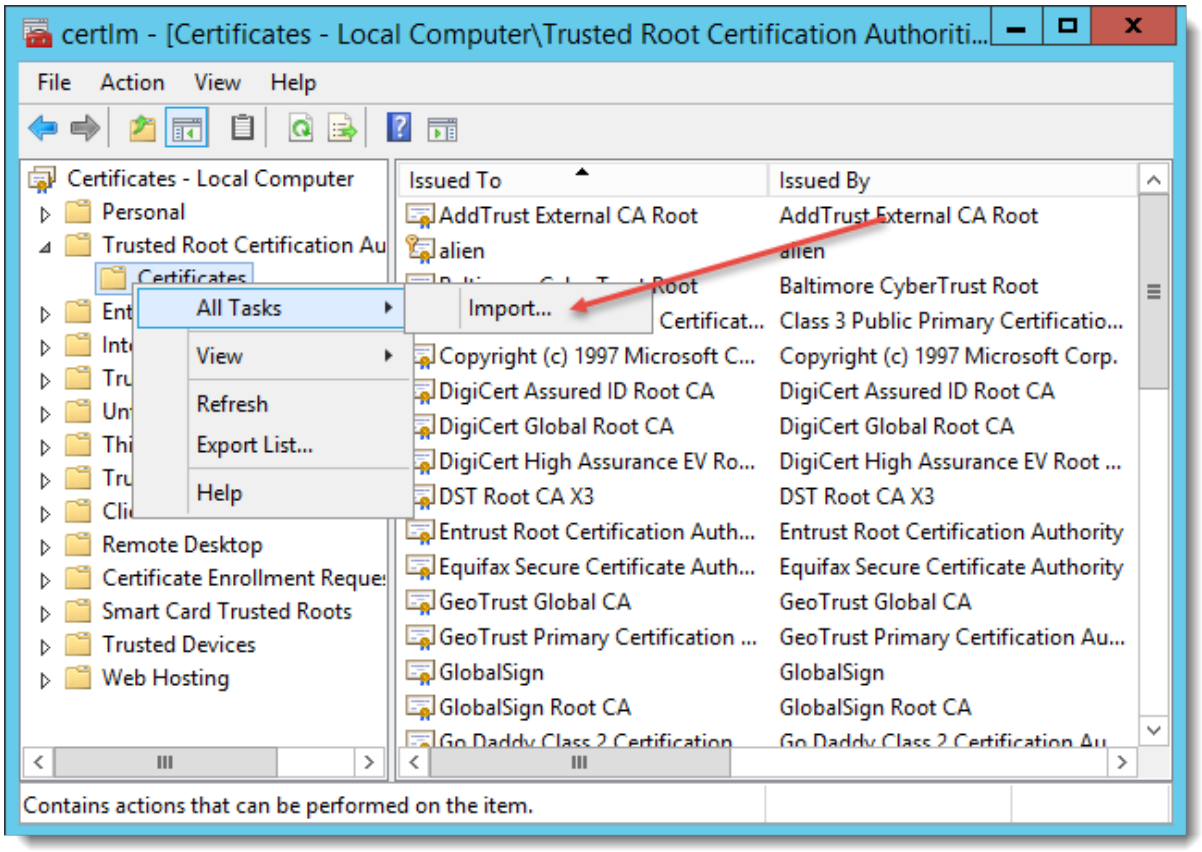
- Click Finish



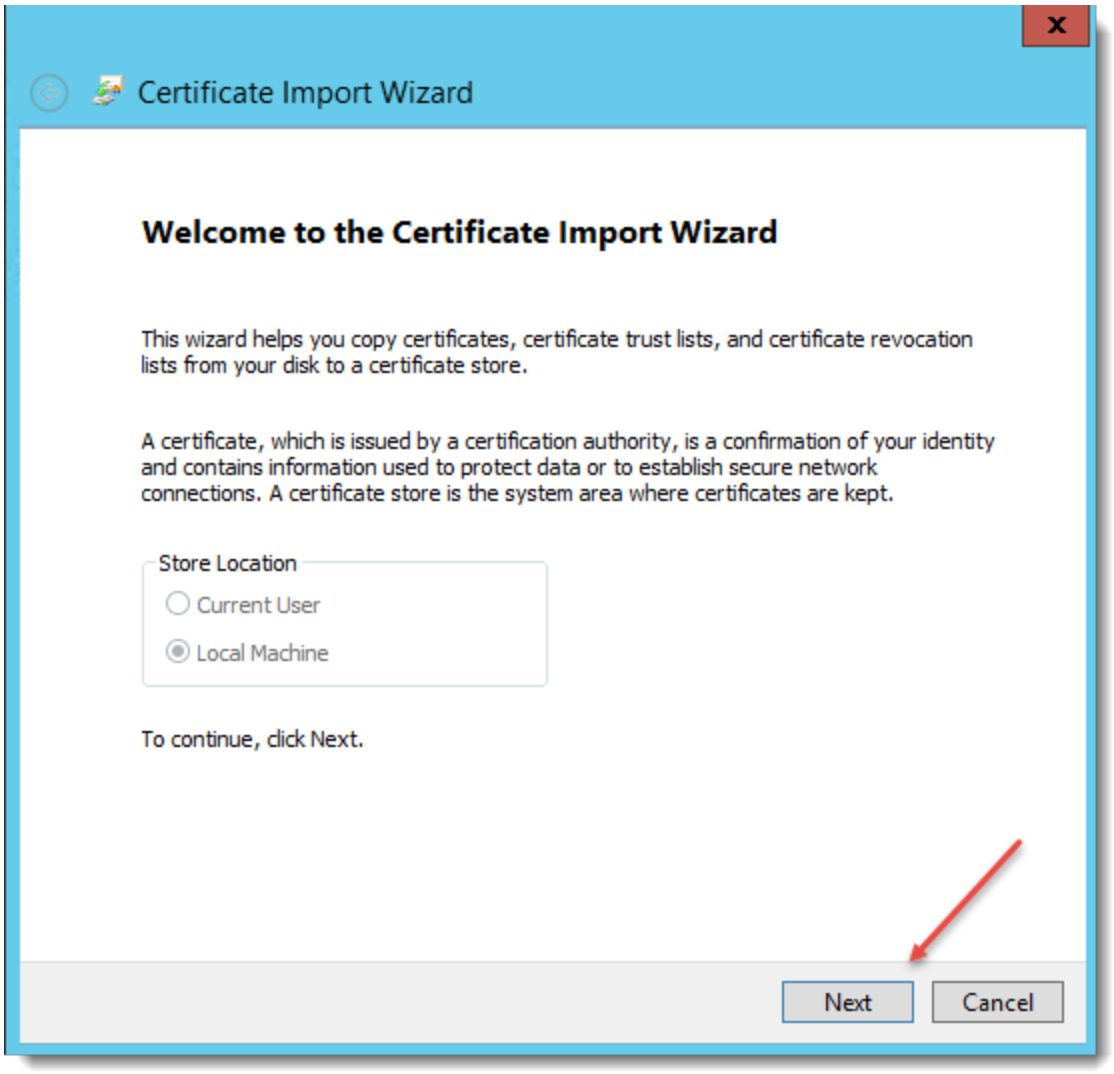
- Copy the certificate to your Passwordstate web server and close all windows.

Importing the Certificate into your Passwordstate web server

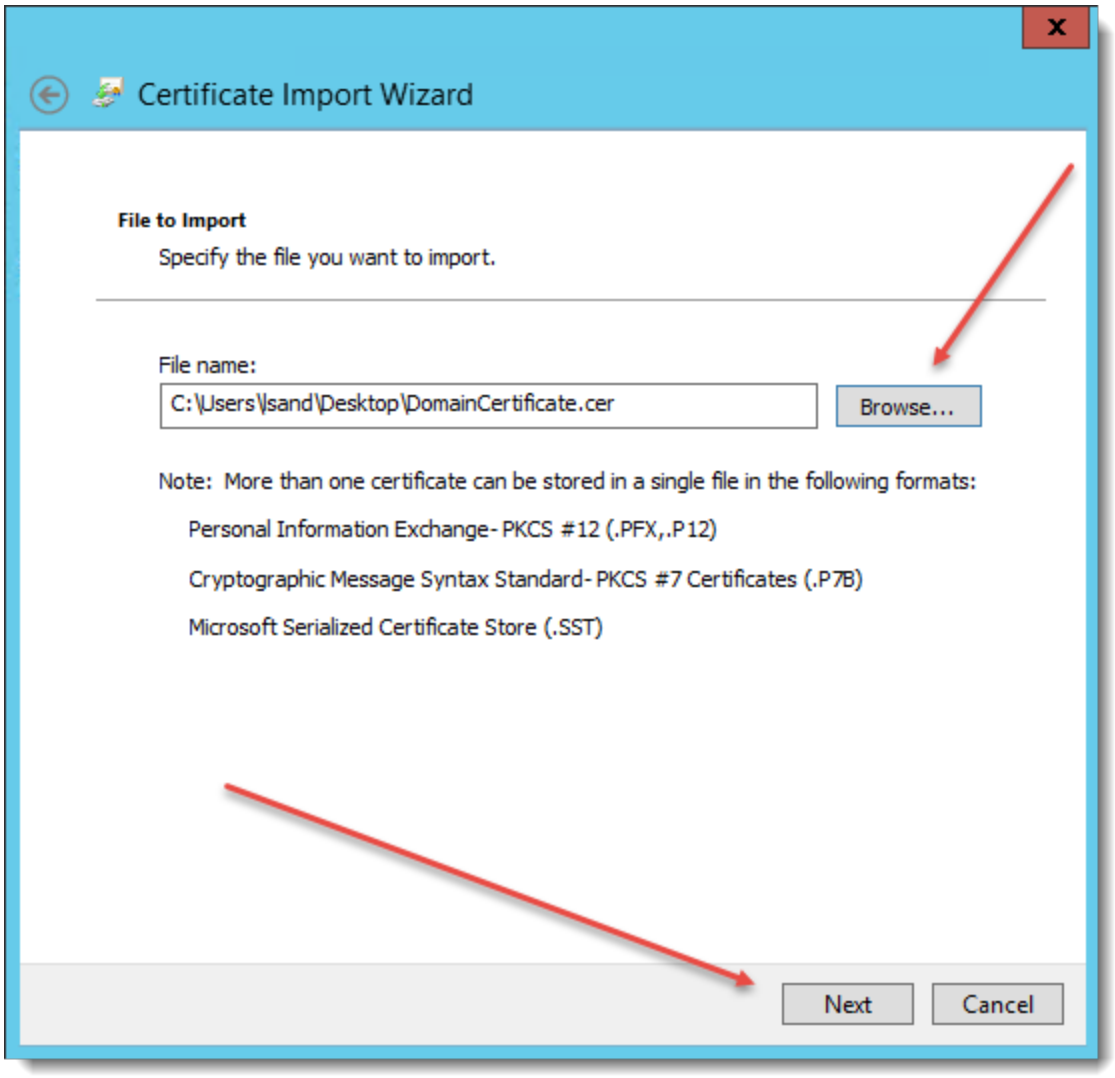
- On your Passwordstate web server, open Certificate Manager for Local computer by typing certlm.msc into your Run command bar
- Expand Trusted Root Certificate Authorities -> Certificates
- Right Click Certificates and select All Tasks -> Import



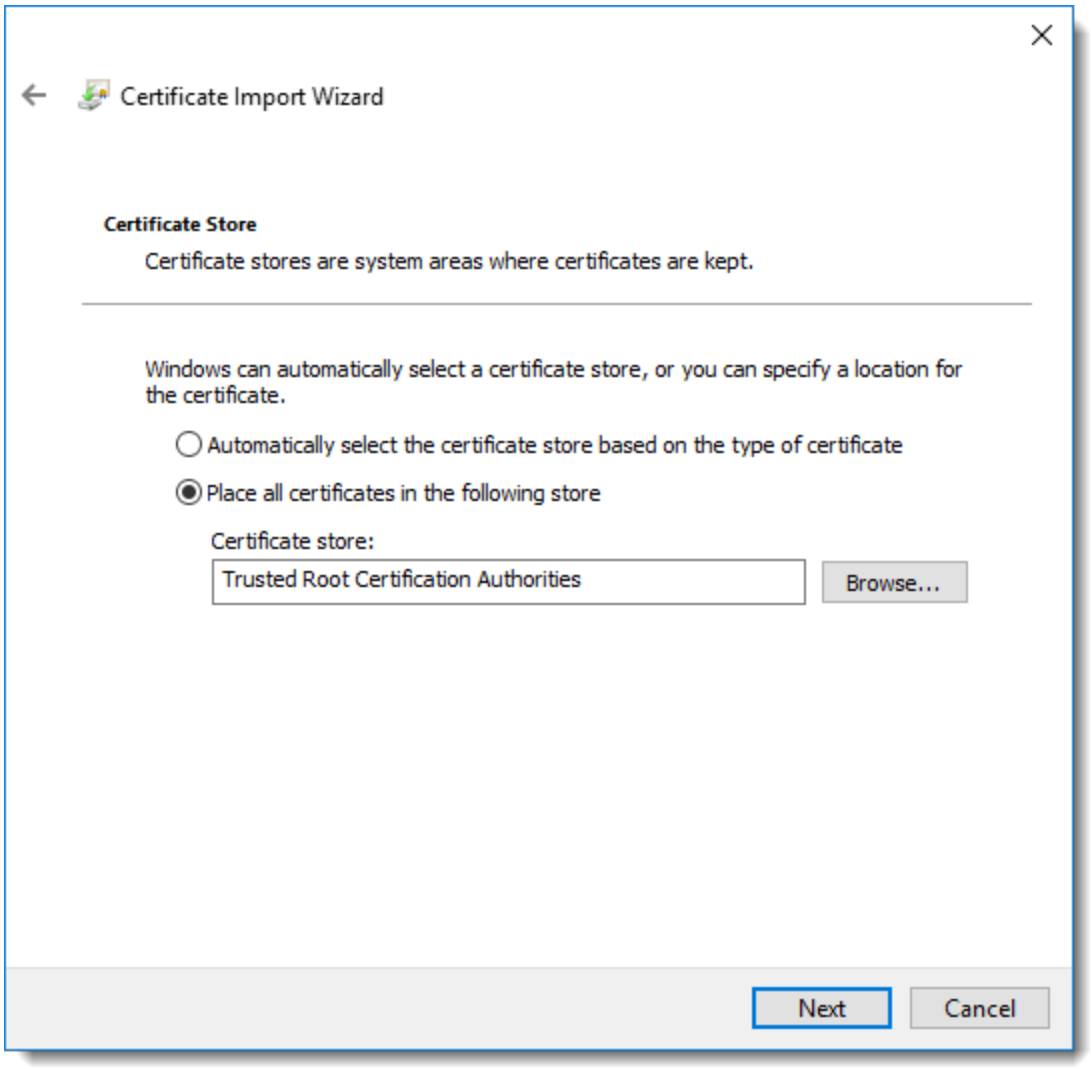
- Click Next



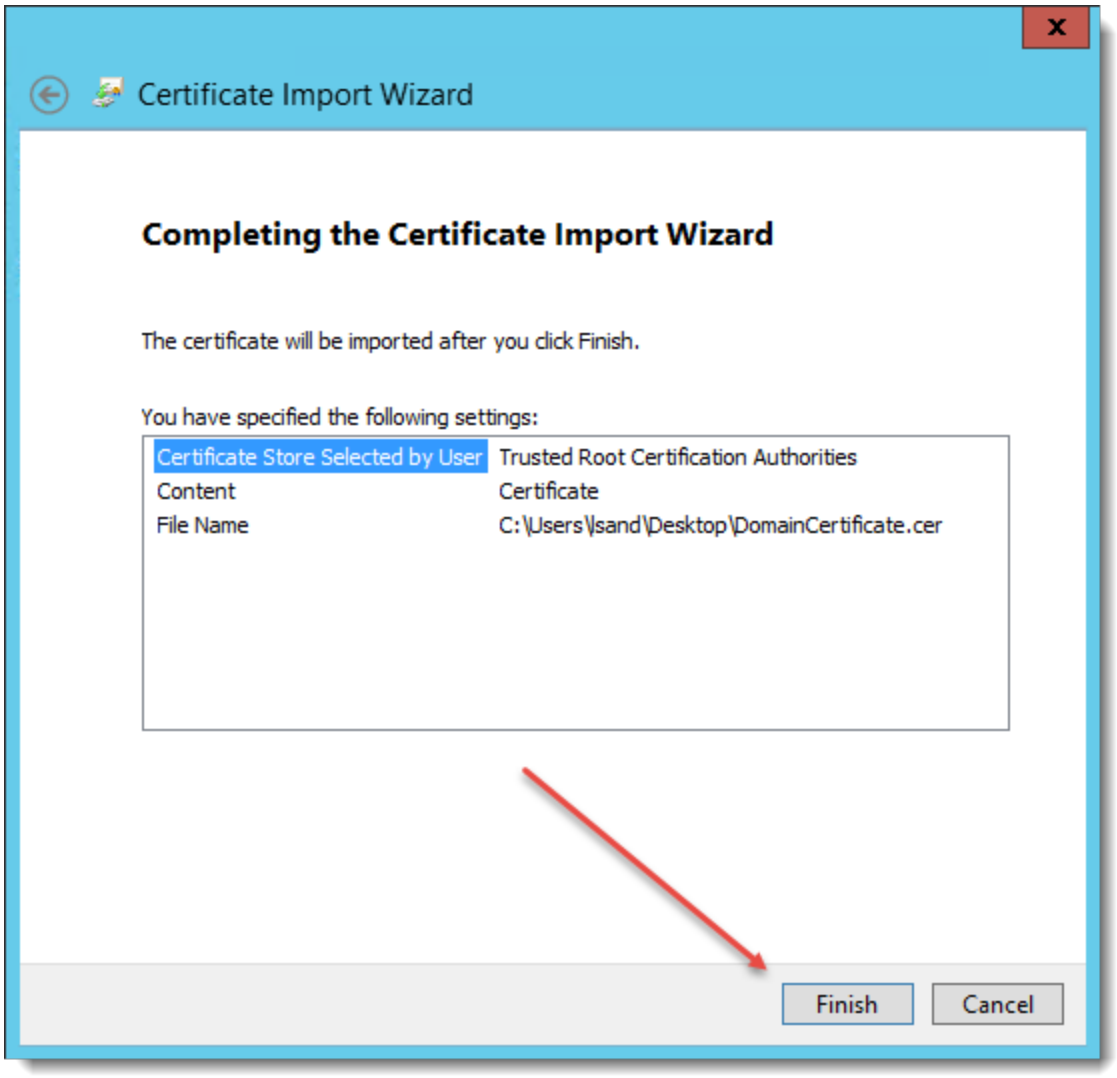
- Browse to the certificate and click Next



- Click Next



- Click Finish and then OK



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

2.3 Auditing

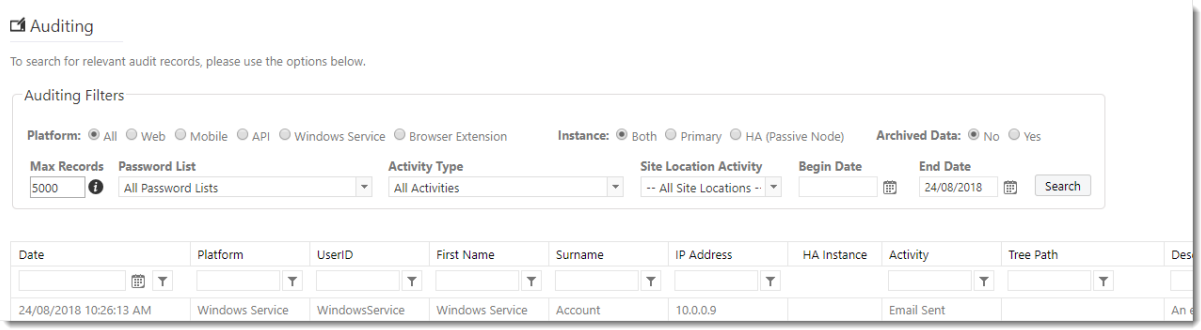
The Auditing screen allows you do report/filter on all auditing data within Passwordstate. Filtering can be done by:

- 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 Auditing Data

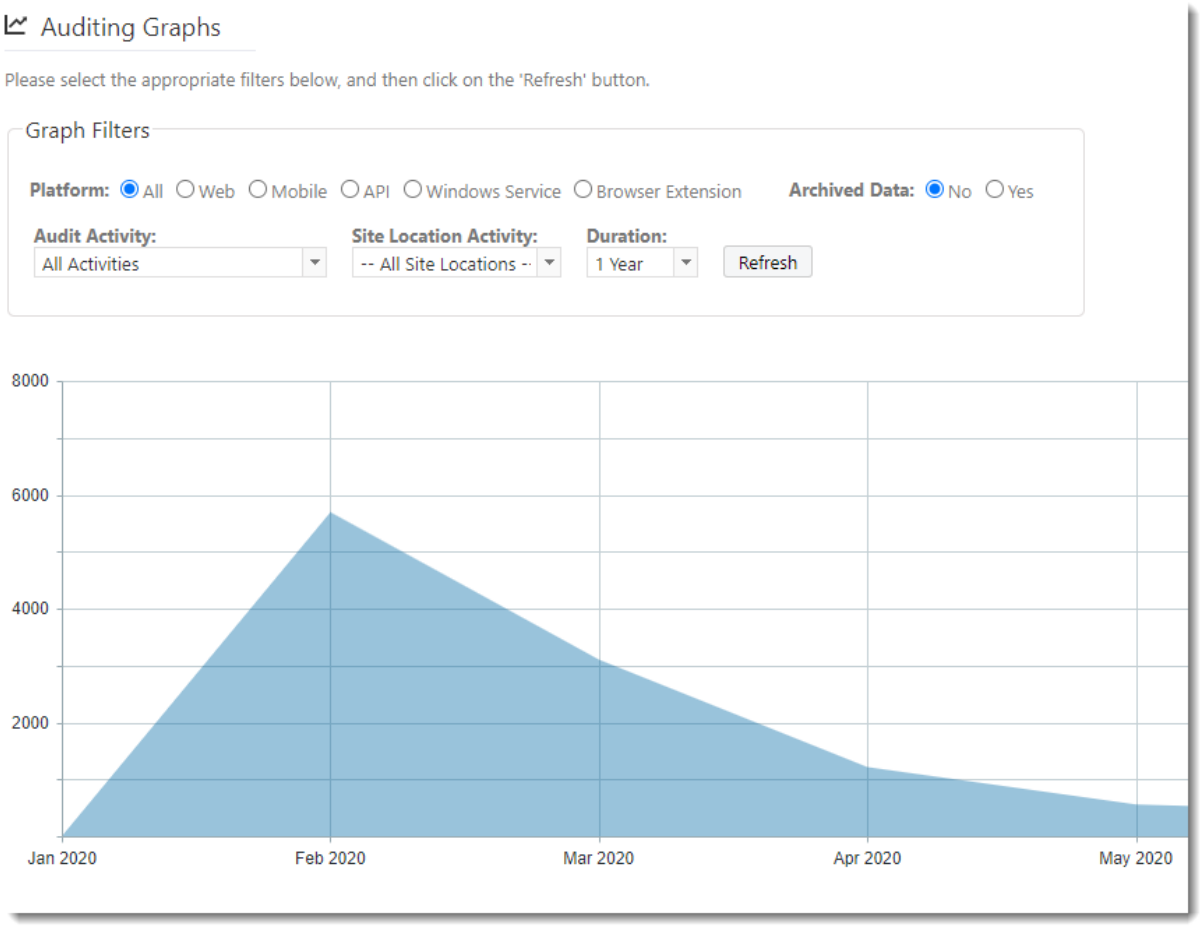
In addition to reporting on auditing data on the screen, you can export the data for further analysis to a CSV file if required.

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



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.



2.5 Authorized Web Servers

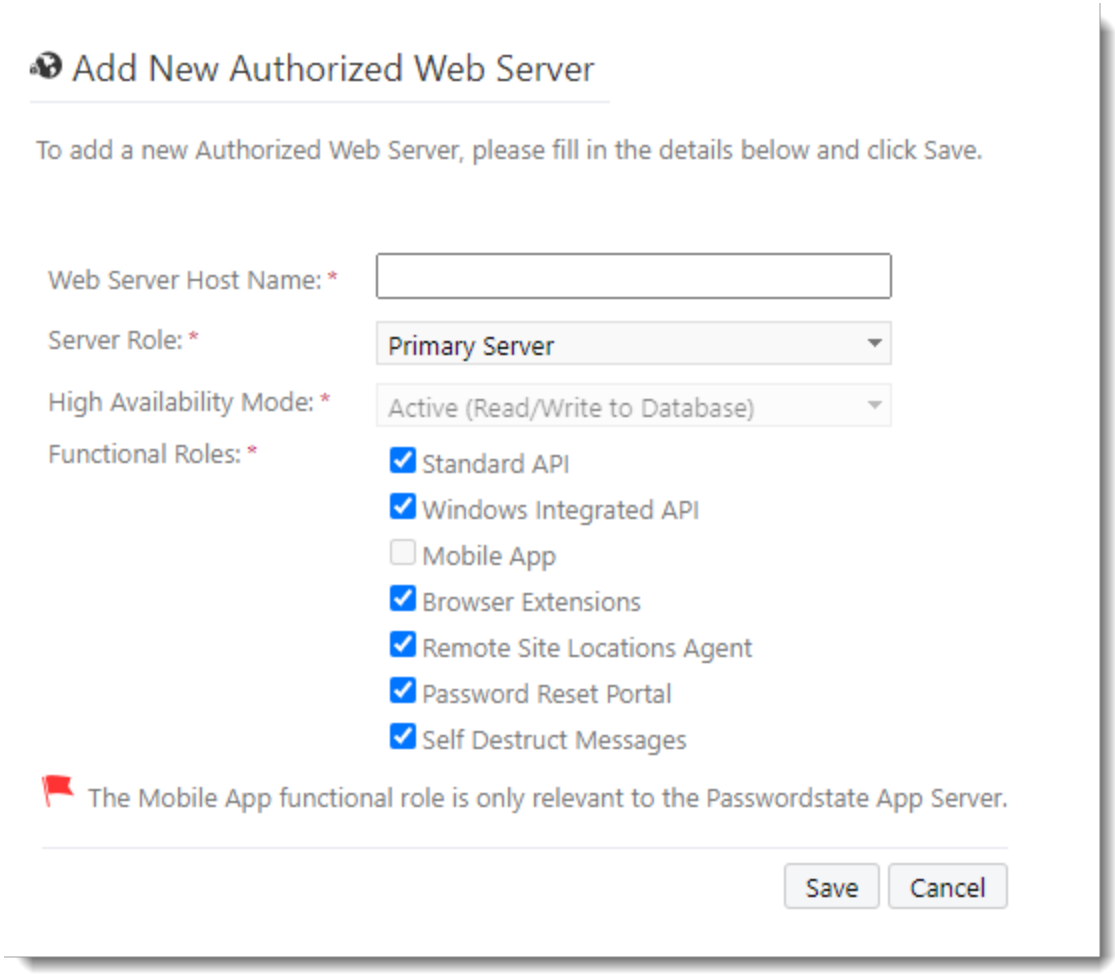
The Authorized Web Servers screen is where you can specify the host names of the web servers which are authorized to host the Passwordstate web site, or Passwordstate App Server.

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.



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**:
https://www.clickstudios.com.au/downloads/version9/Passwordstate_Automatic_Backups_Domain_Account.pdf

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

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 - https://haveibeenpwned.com/, 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.

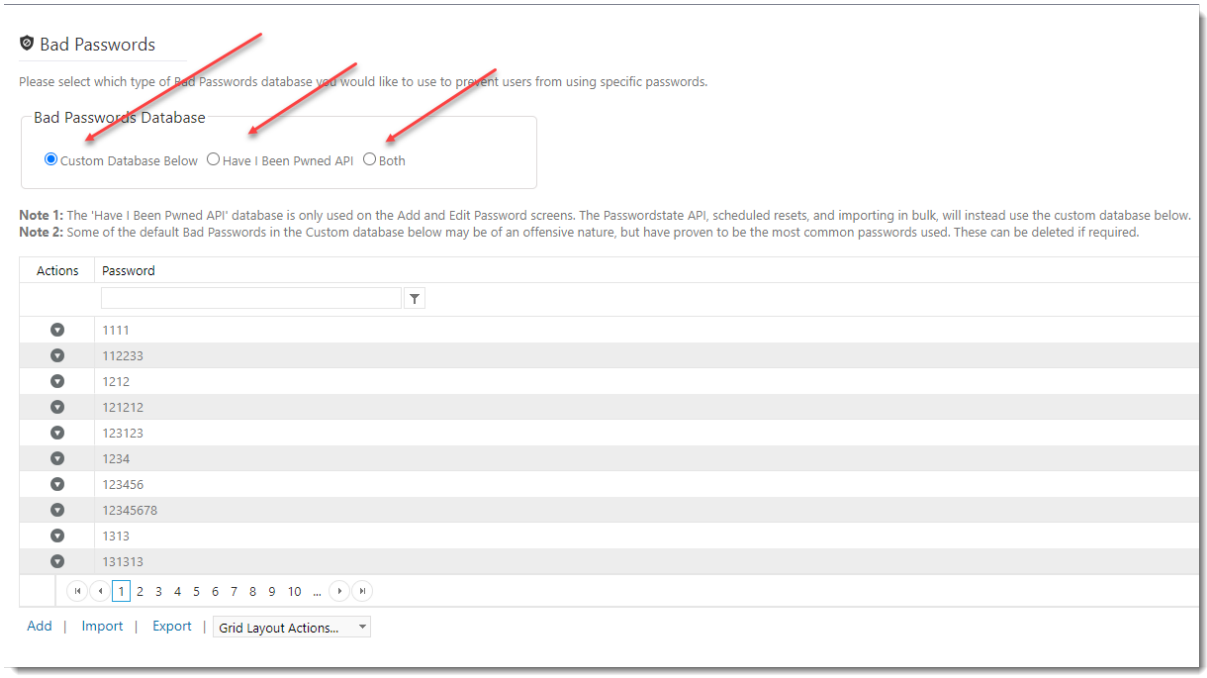
Note 1: If you use the 'Have I been Pwned' database, this is only available on the Add and Edit Passwords screens. The Passwordstate API, scheduled resets, and importing in bulk, will instead use the Custom Bad Passwords database

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 -> System Settings -> Miscellaneous Tab, and Password Options Tab for notifying your users when bad passwords are detected.

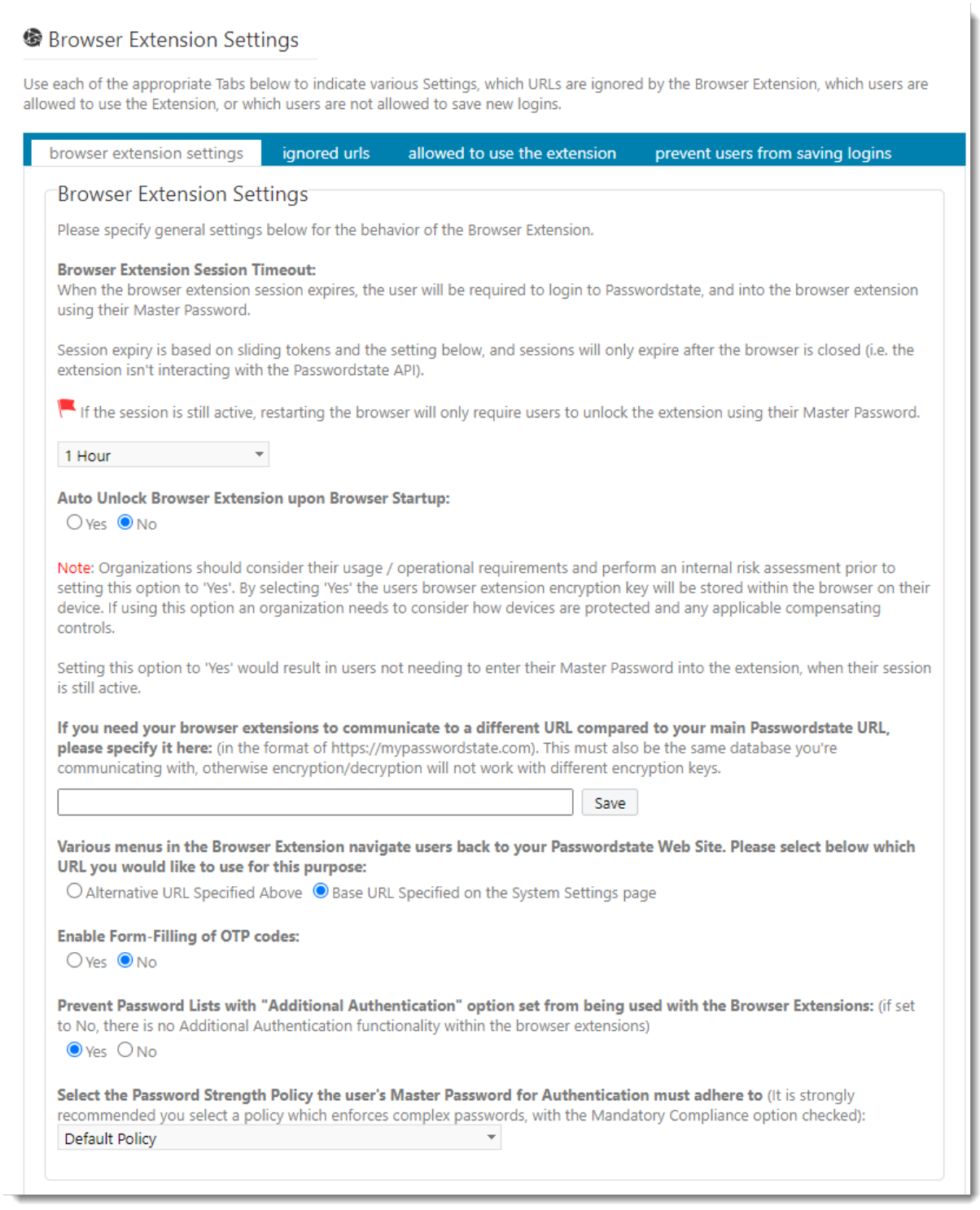
If required, you can also import multiple 'Bad Passwords' for the Custom Bad Passwords database, via the use of a csv file.



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

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.

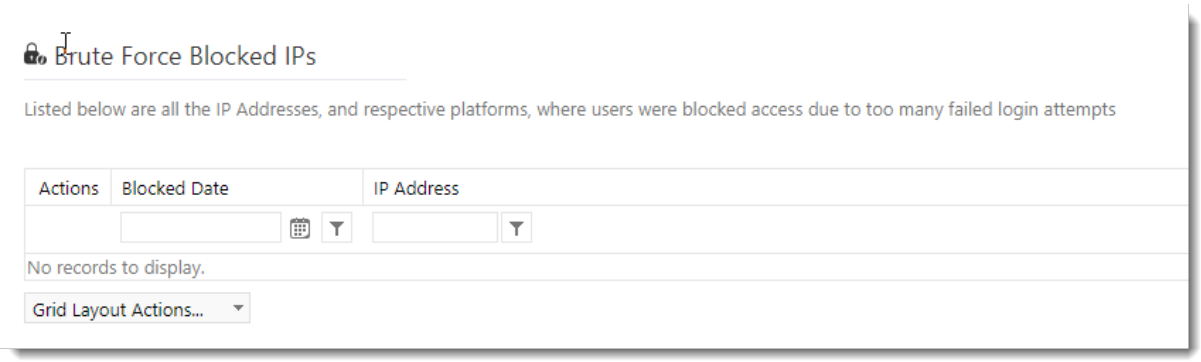
On this screen you can clear all tokens for all user accounts. Or, if you only want to clear an access token for a single user, you can do this from the screen Administration -> User Accounts, and then from the appropriate 'Actions' menu for the user.

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.



2.10 Email Notification Groups

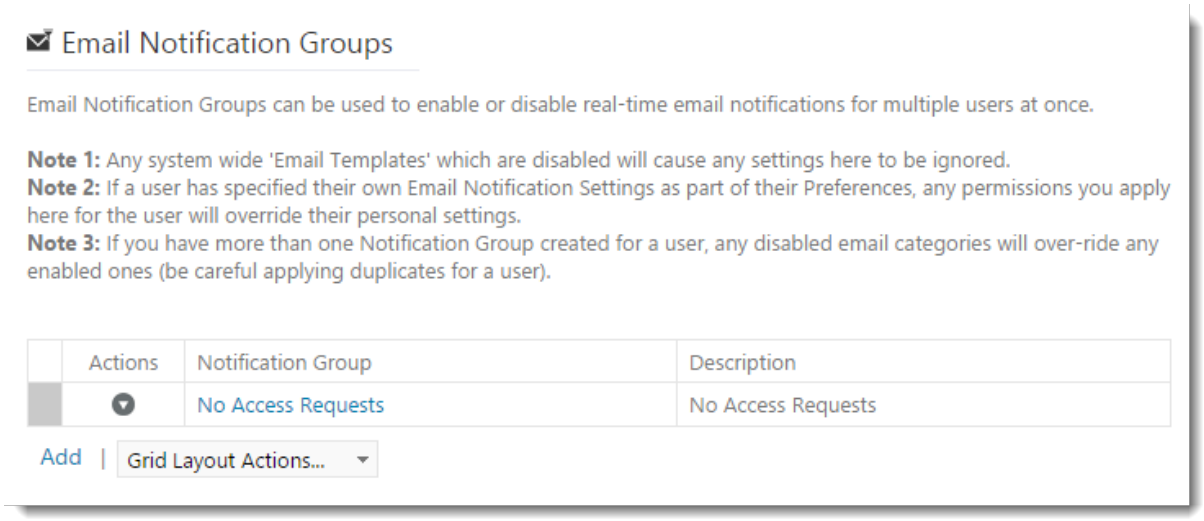
The Email Notification Groups screen is used to manage email notification settings for a group of individual users accounts, or members of security groups.

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.

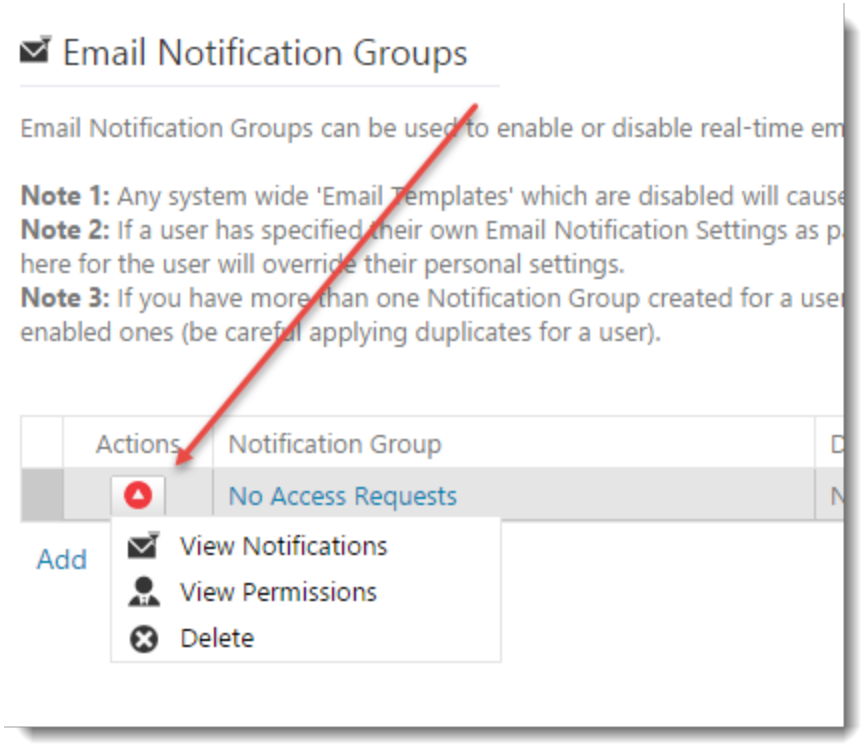
Note 1: Any system wide Email Templates which are disabled will cause any settings here to be ignored

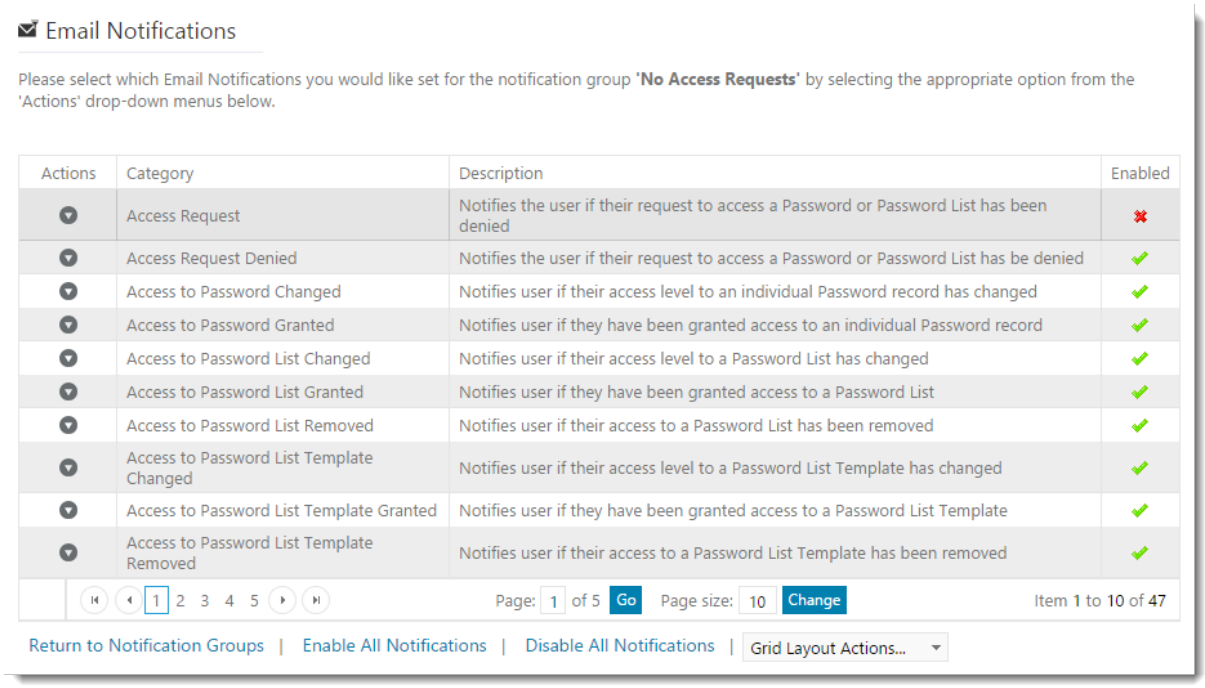
Note 2: If a user has specified their own Email Notification Settings as part of their Preferences, any permissions you apply here for the user will override their personal settings

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)



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.





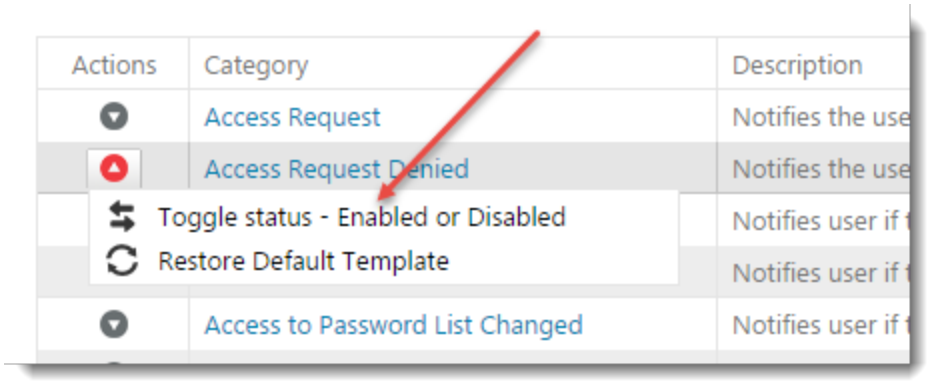
2.11 Email Templates

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

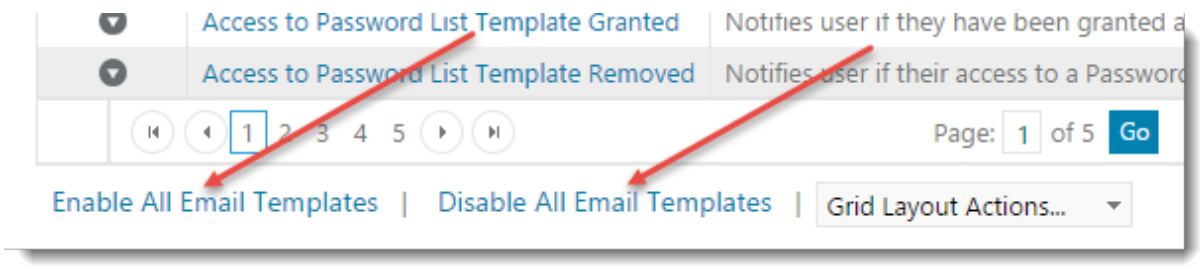
Enabling/Disabling Email Notifications

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

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



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



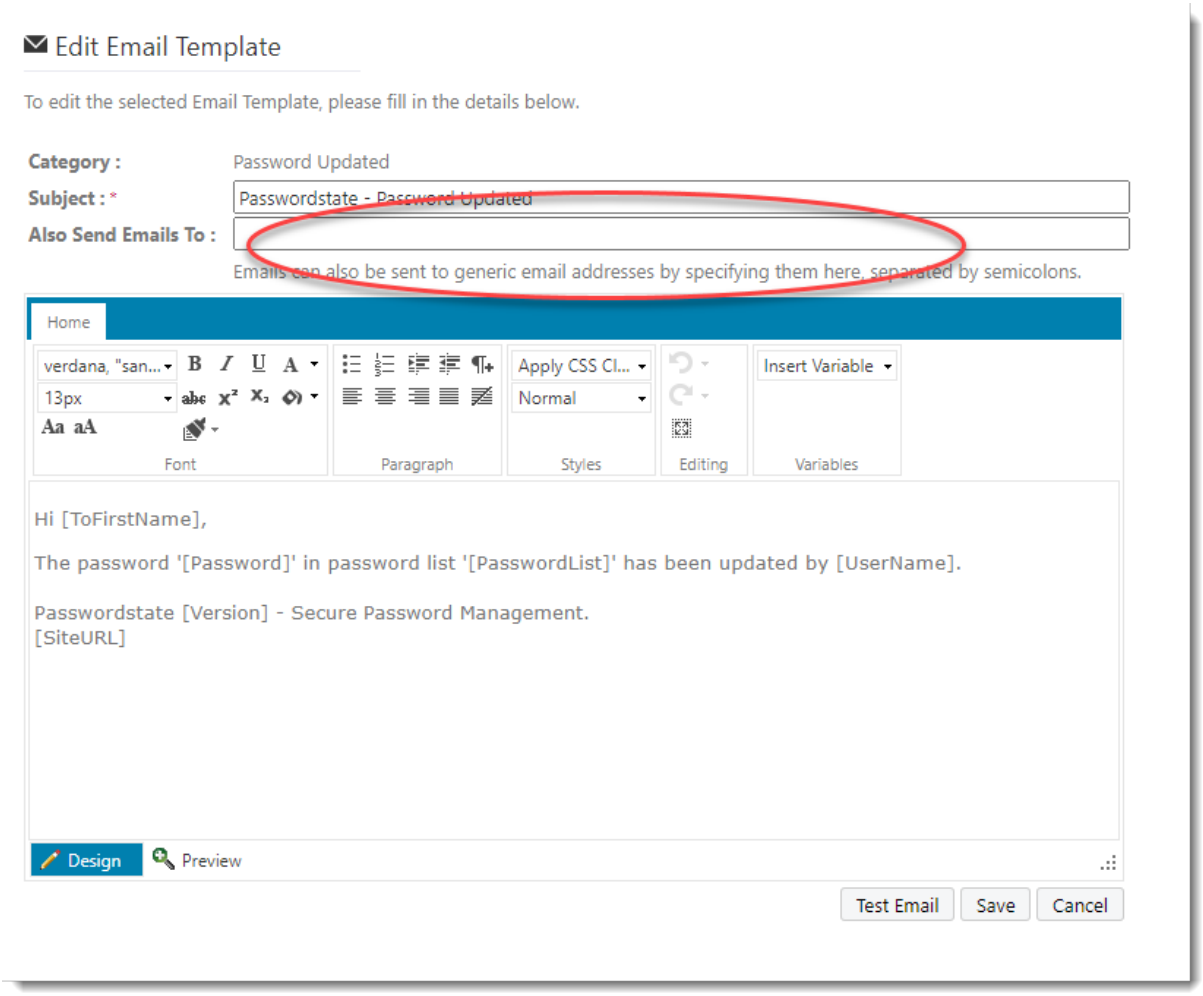
Editing Email Template Content

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.

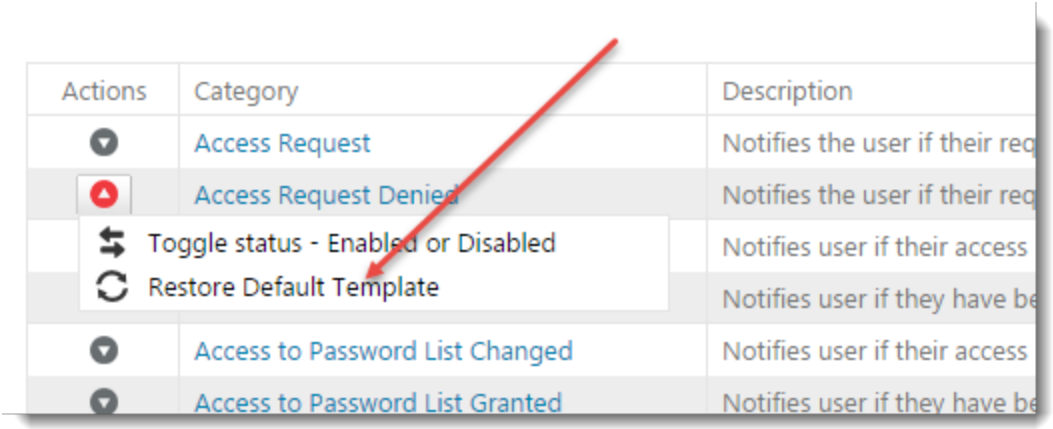
At the top right-hand side of the Editor you will notice the 'Variables' tab/ribbon bar. From this drop-down list, you can insert the following variables into your email templates:

- 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.



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.



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:

1. Check you have correctly specified your email server's settings on the screen Administration -> System Settings -> Email Alerts & Options Tab
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'
4. Check there aren't any Email Templates disabled, either on the screen Email Templates, or Email Notification Groups, or possibly the user has disabled an email notification in their Preferences area

2.12 Emergency Access

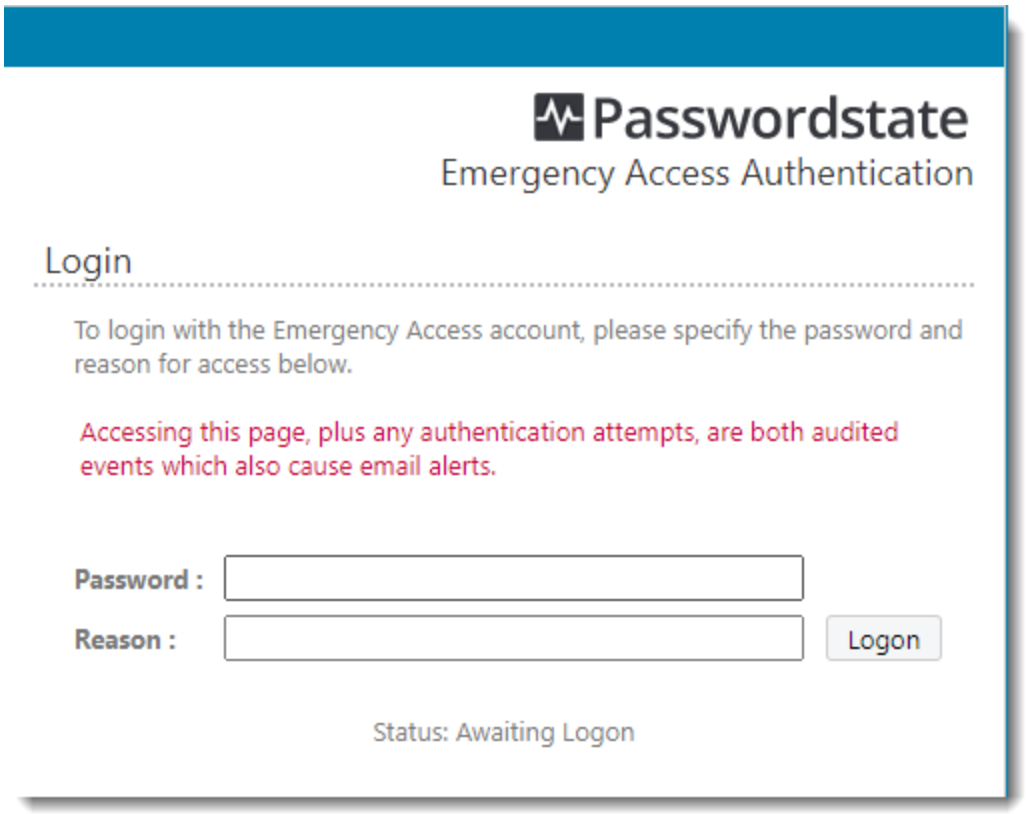
The Emergency Access screen allows you to specify a password for a separate 'Security Administrator' role login which can be used in the event other accounts are locked out, or inaccessible for any reason.

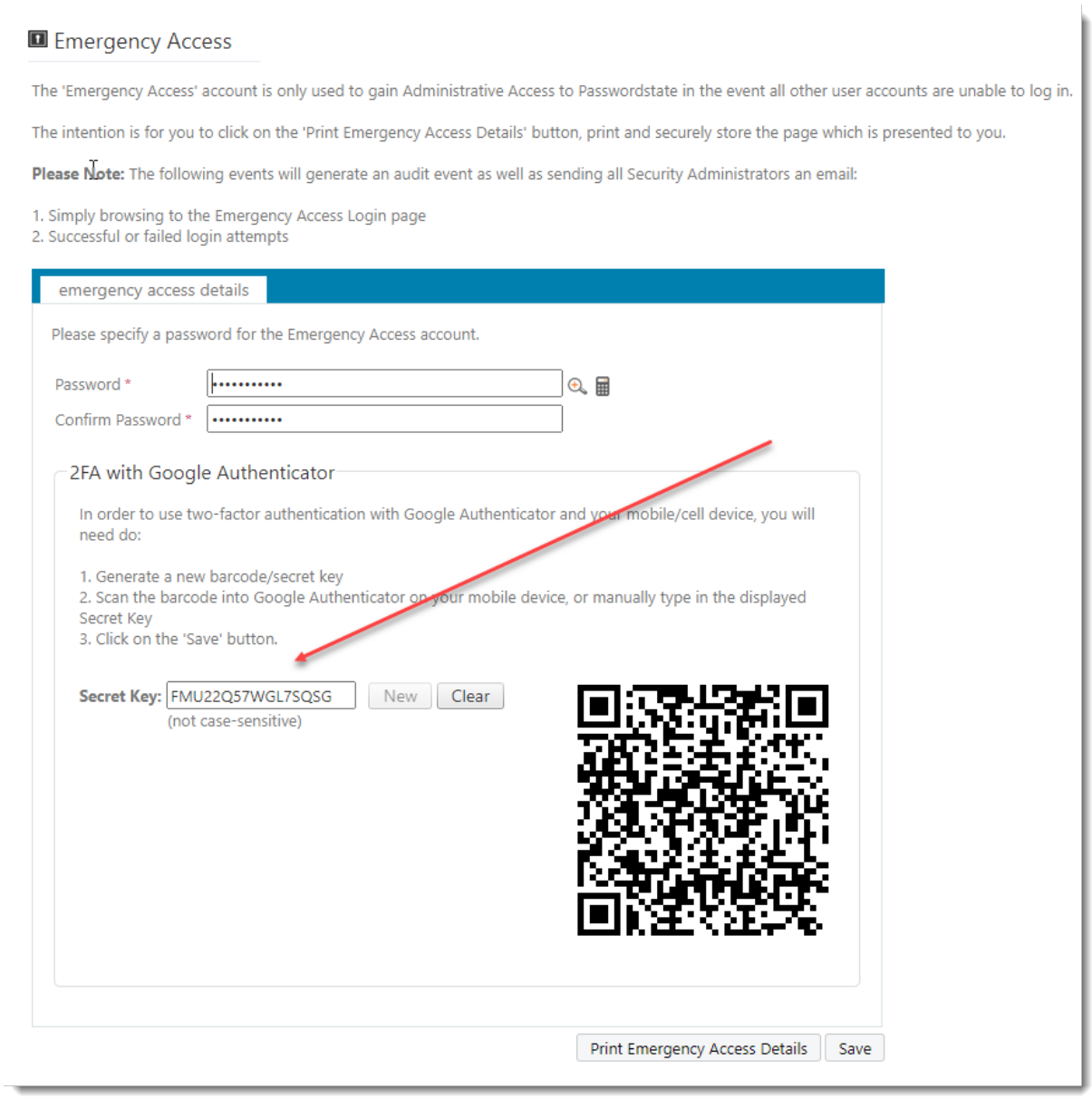
A couple of scenarios where this would be applicable is:

- 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.

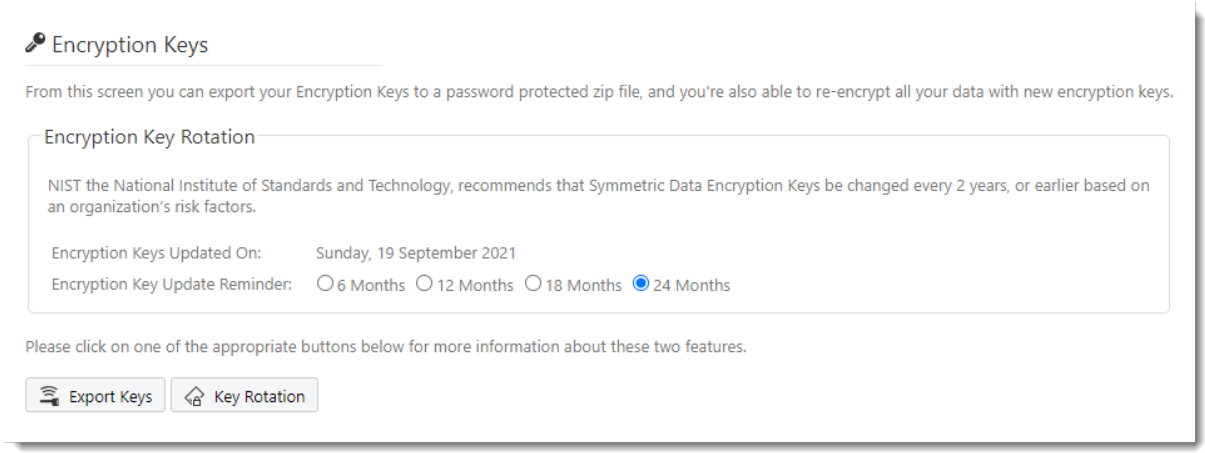




2.13 Encryption Keys

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 re-encrypting 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



Export Keys

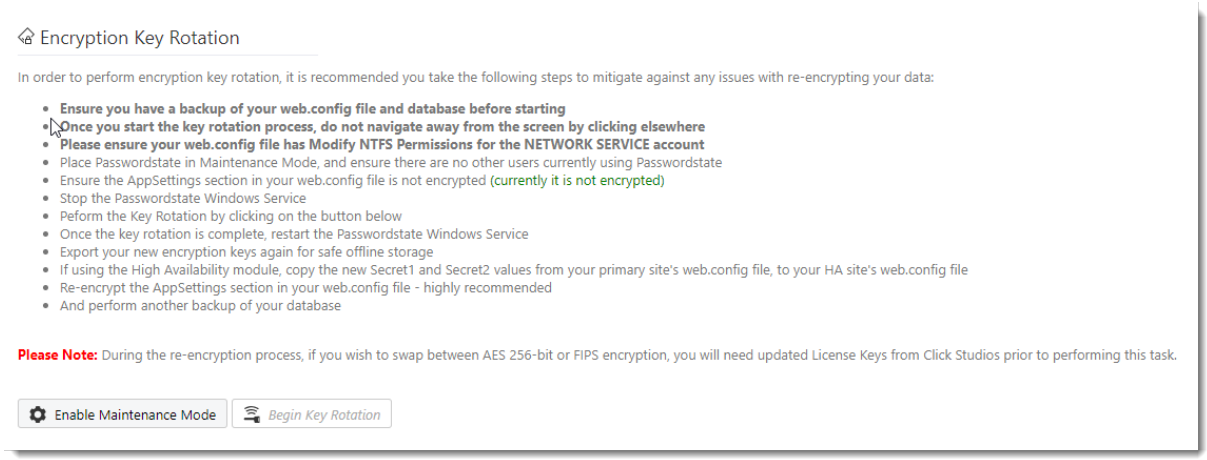
You can export your encryption keys, in the format of split secrets, to a password protected zip file.

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.

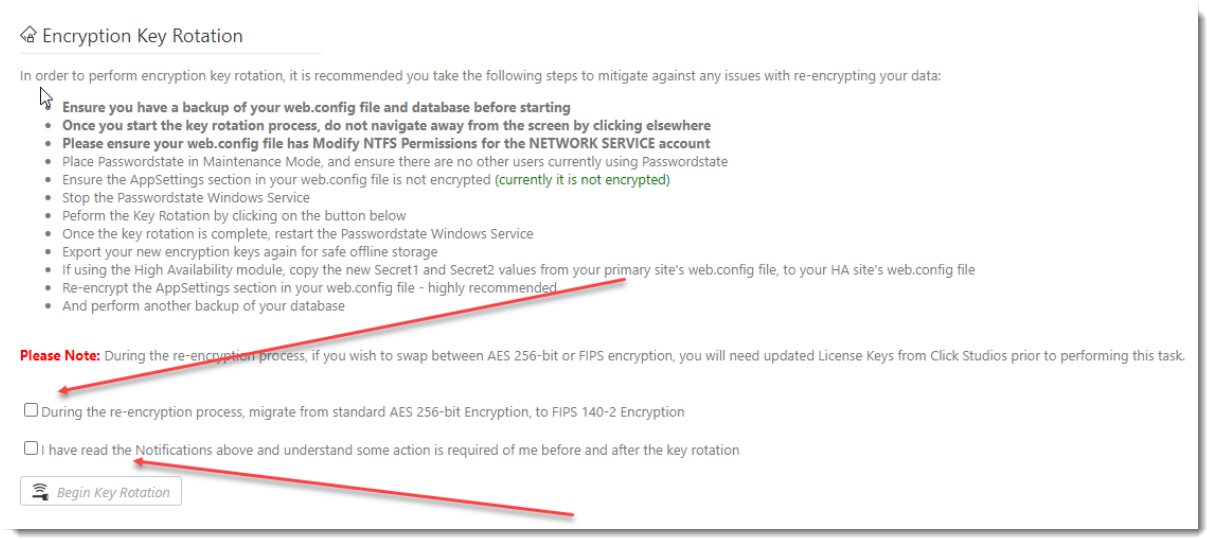
Key Rotation

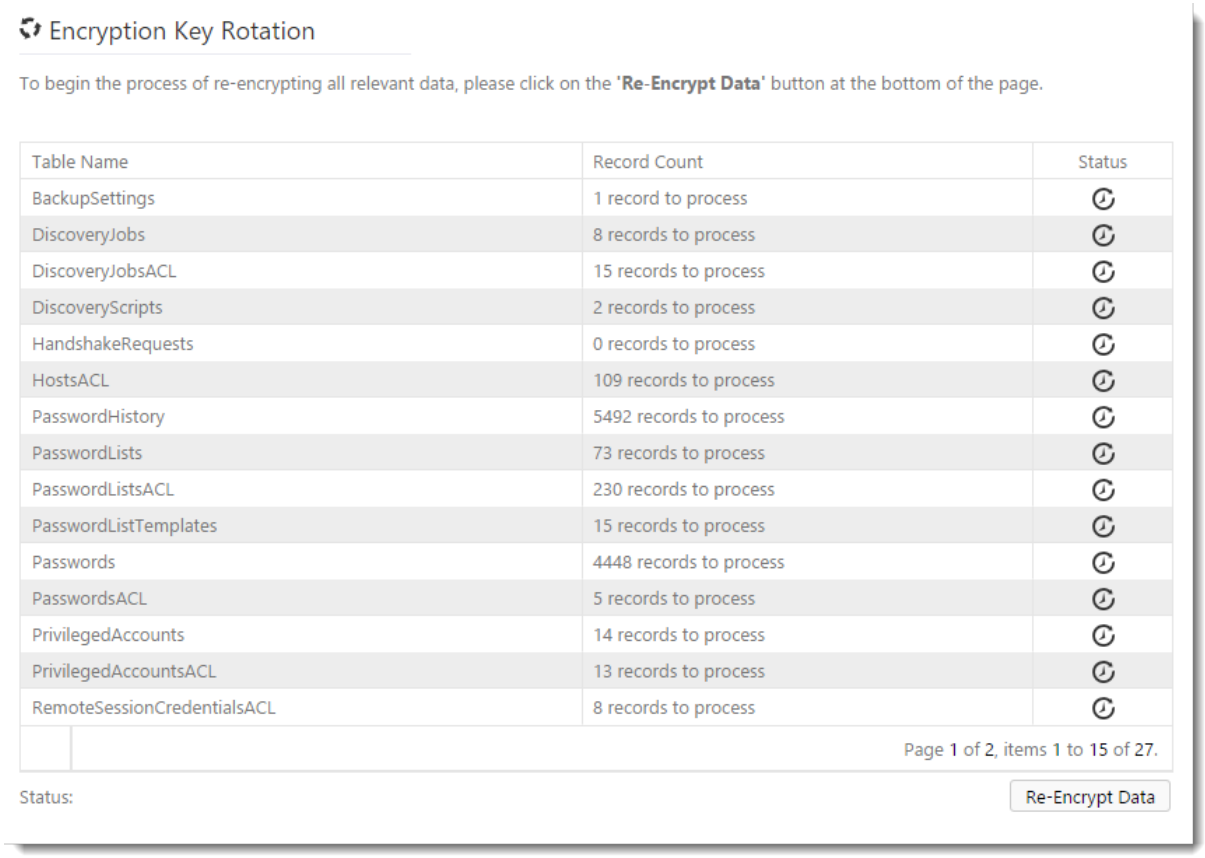
With this feature, you can update your Encryption Keys used in Passwordstate, and then re-encrypt all your data with these new encryption keys. When performing key rotation, it's very important your follow the on screen instructions so that the re-encryption process is not interfered with in any way.



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.

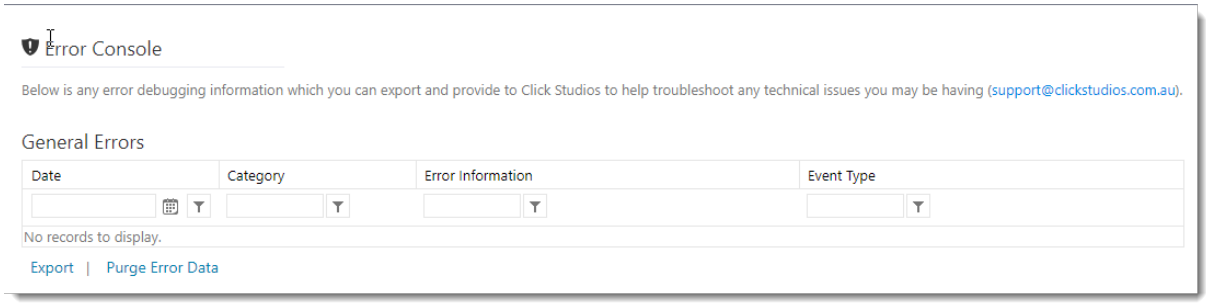
Note: If you do wish to change encryption methods, you first need to contact Click Studios and request updated License Keys for your software - as they will need to be updated on the screen, during this re-encryption process.





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.

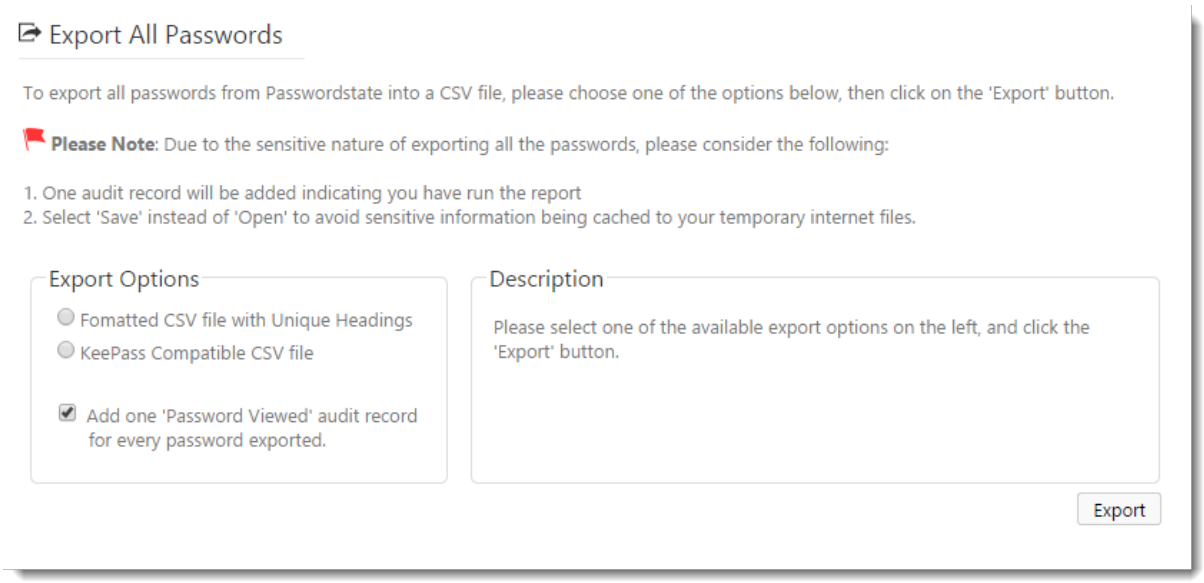


2.15 Export All Passwords

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



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

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:

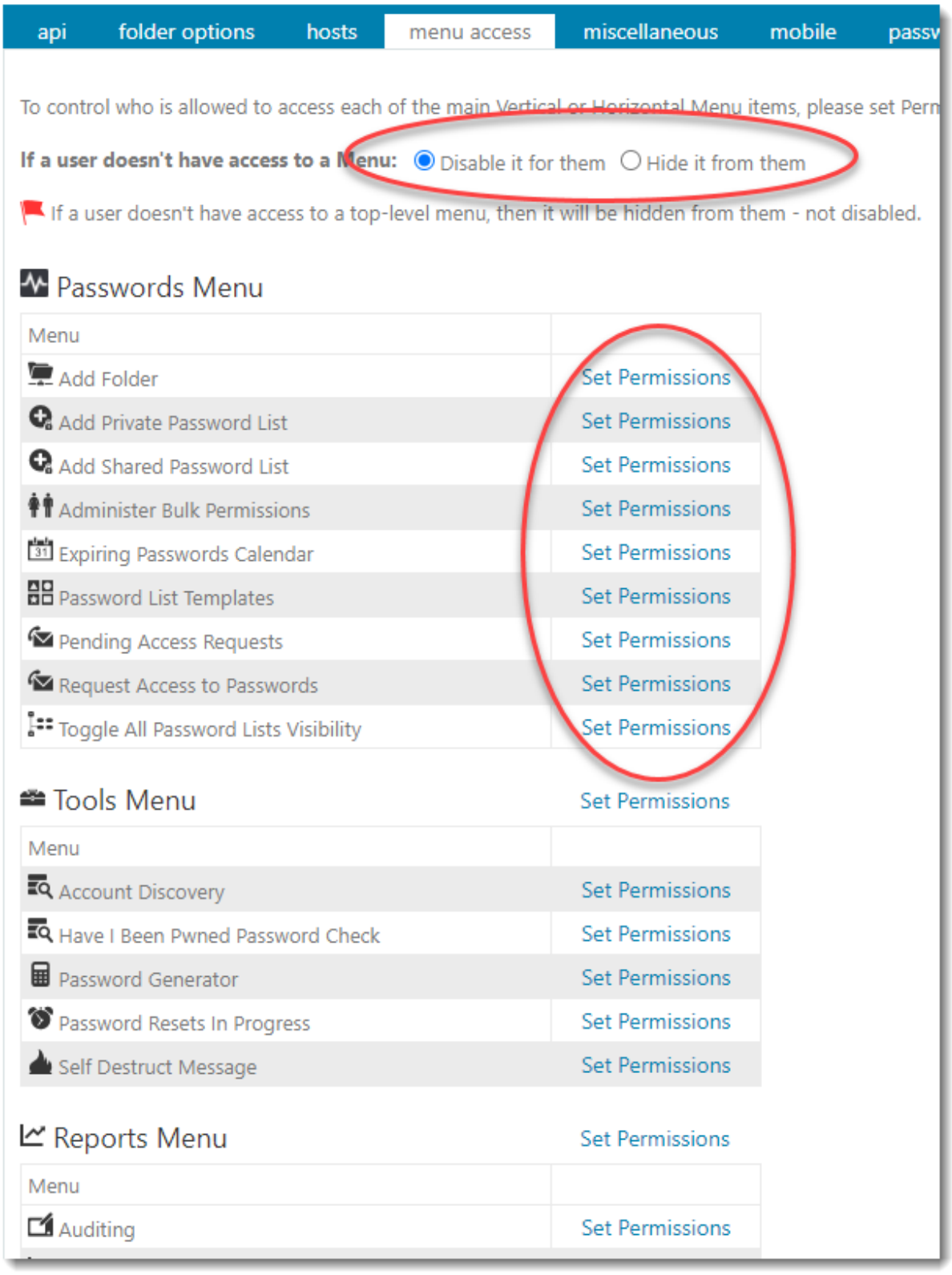
- Which users have access to the Hosts navigation tab itself
- Which users are responsible for managing Host records - add/edit/delete records, and Host Discovery Jobs
- Which users are allowed to manage Folders in the Hosts navigation tab
- Which users are allowed to see the buttons under the 'Host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

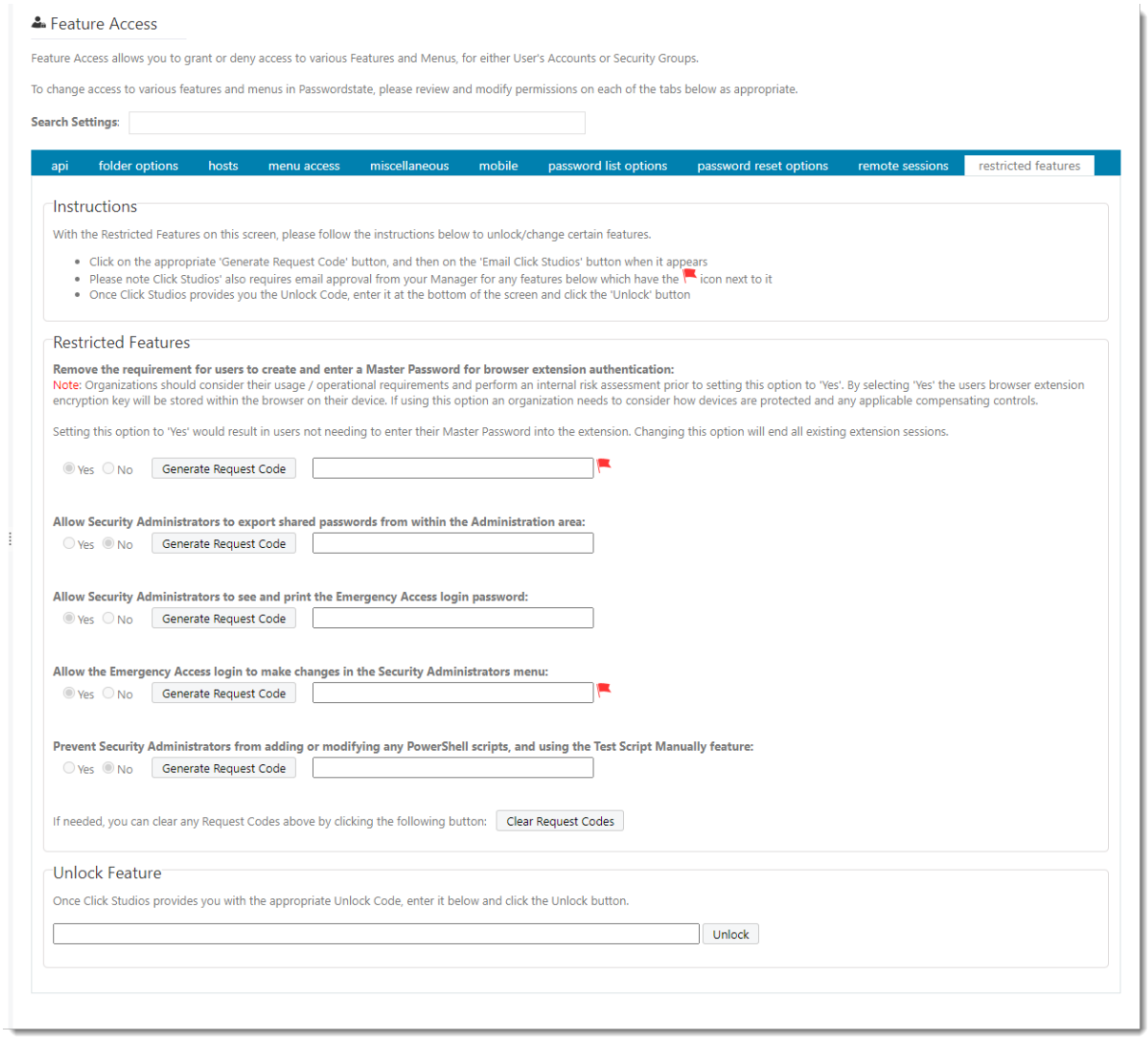
Note 1: If you are using the High Availability module for Passwordstate, it is recommended you save recorded sessions to a network share so both Passwordstate web servers are able to replay those session recordings.
Note 2: If you are using an active/passive configuration for Passwordstate with the High 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

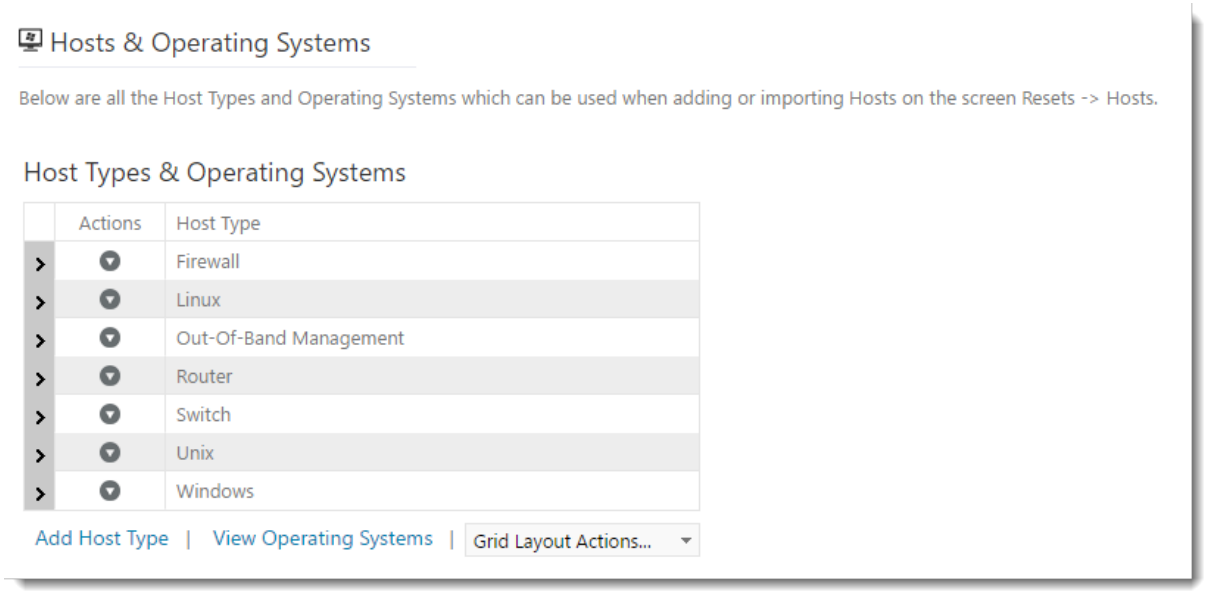
Note : Making any changes here adds an auditing record under the Activity Type of 'Restricted Feature Changes'.

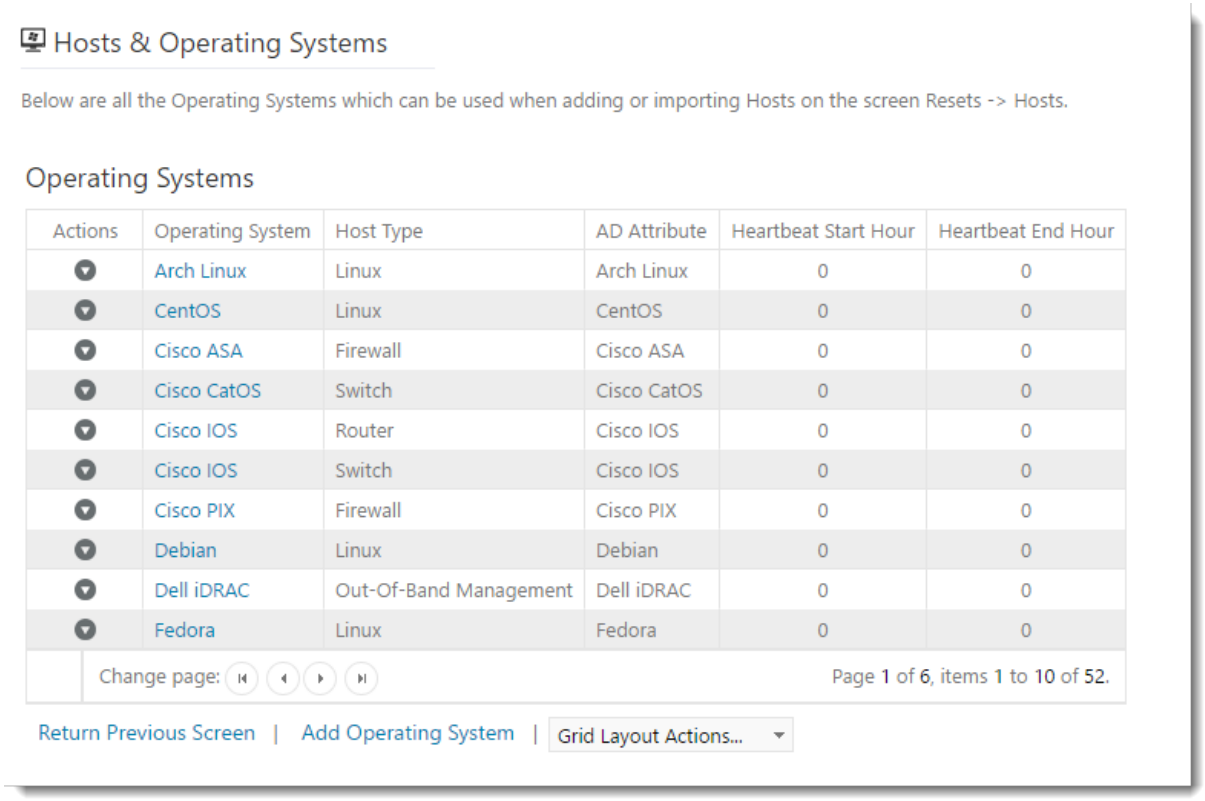


2.17 Host Types & Operating Systems

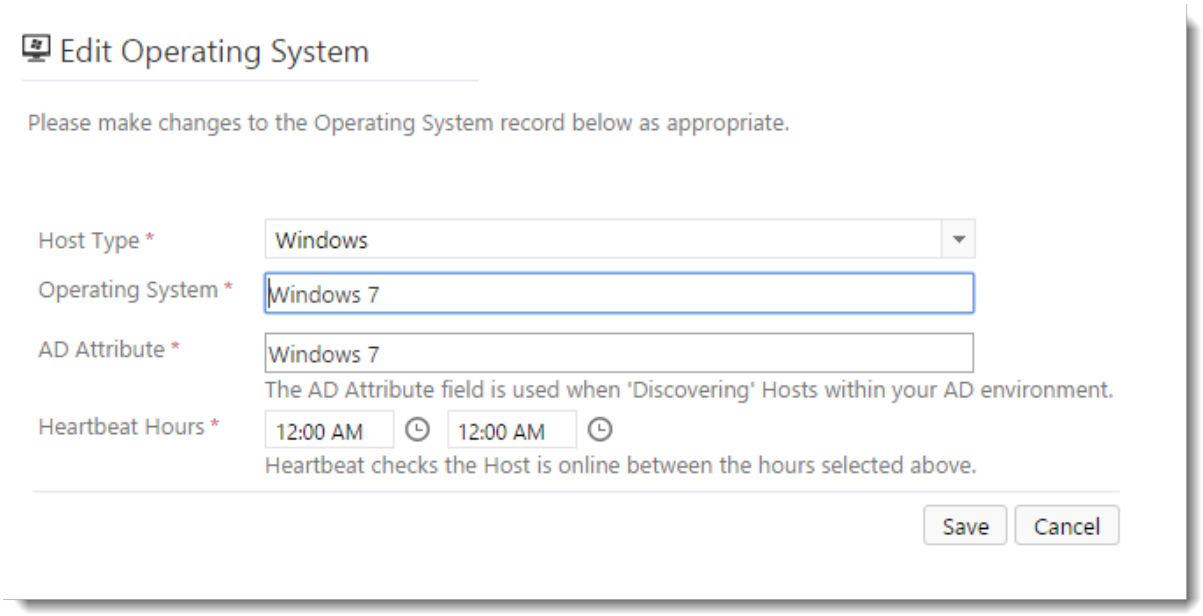
The Host Types & Operating Systems screen allows you to add additional Host Type and Operating System records which can be associated with Host records in Passwordstate.

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





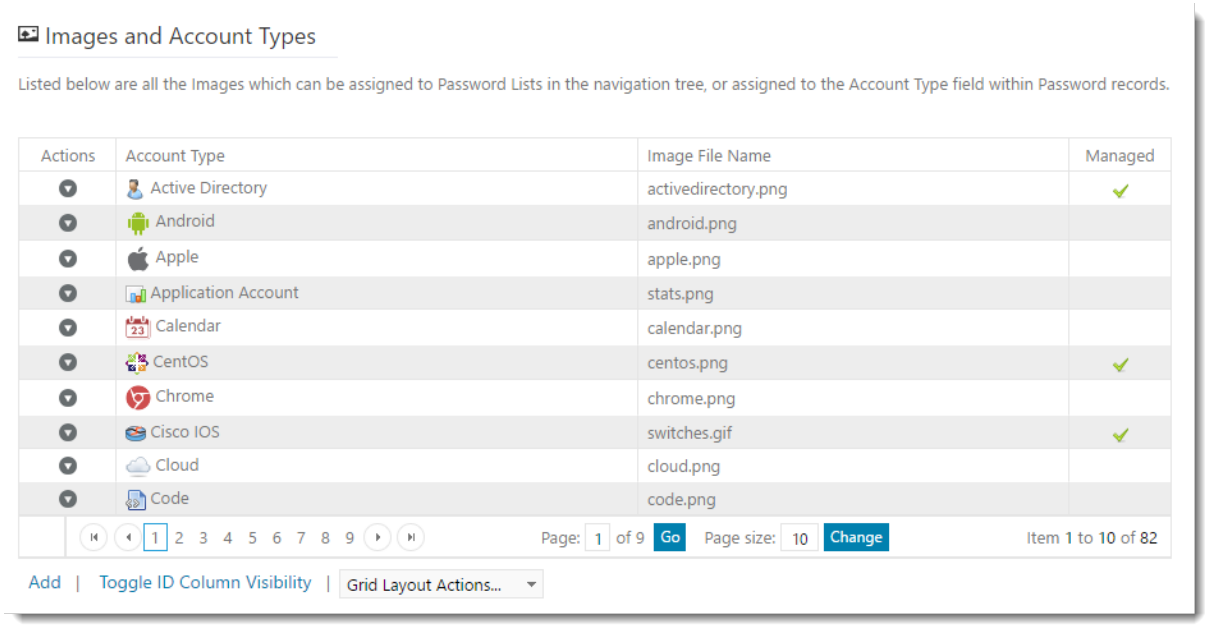
When using the Account Heartbeat validation feature for Password records, you may only want the Heartbeat poll to occur during certain times for different Operating Systems. By editing each of the Operating System records, you can change this poll time e.g. You only want to validate local administrator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



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.

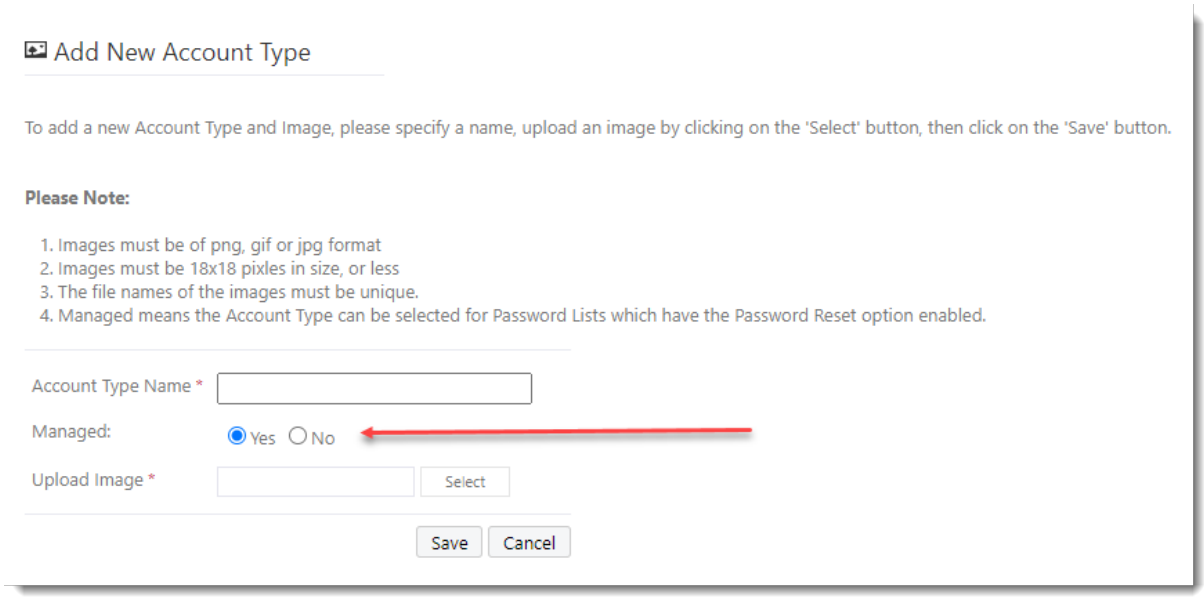
Note 1: All images exist on the web server file system in the path <Passwordstate Folder>\images\LookupImages, and are also stored within the Passwordstate database as well. Deleting them from the file system will caused them to be recreated by the Passwordstate Windows Service.
Note 2: It is recommended 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'



Managed Account Types

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

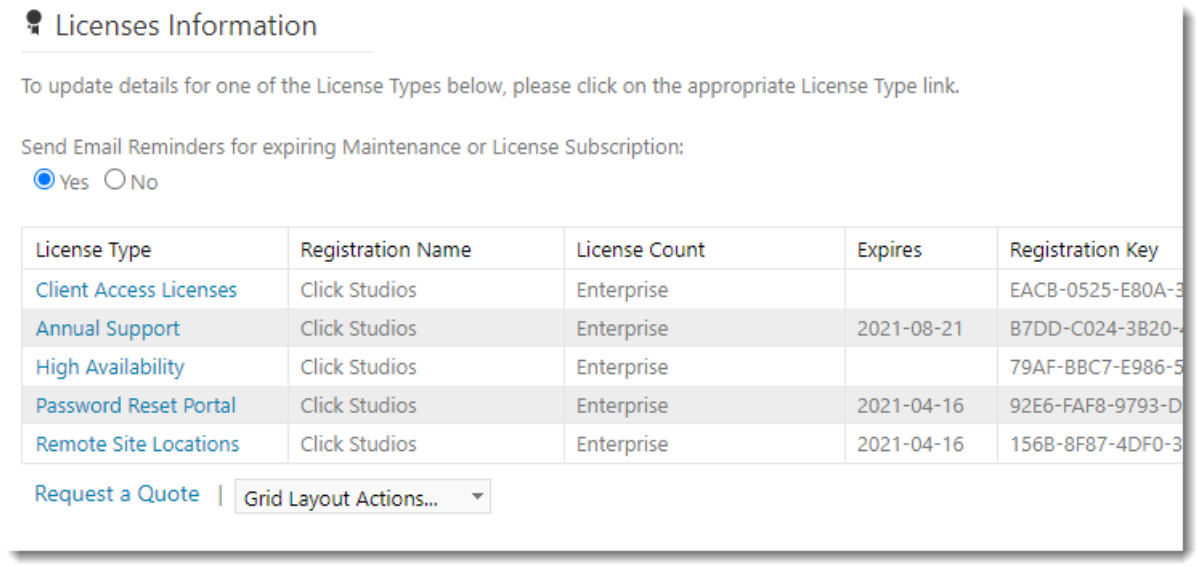
Having this option set to Yes means you can select these account types for password records which are stored in Password Lists that are configured for Resets - and then you can also select your own custom Reset and Validation PowerShell scripts if you have written some.



2.19 License Information

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



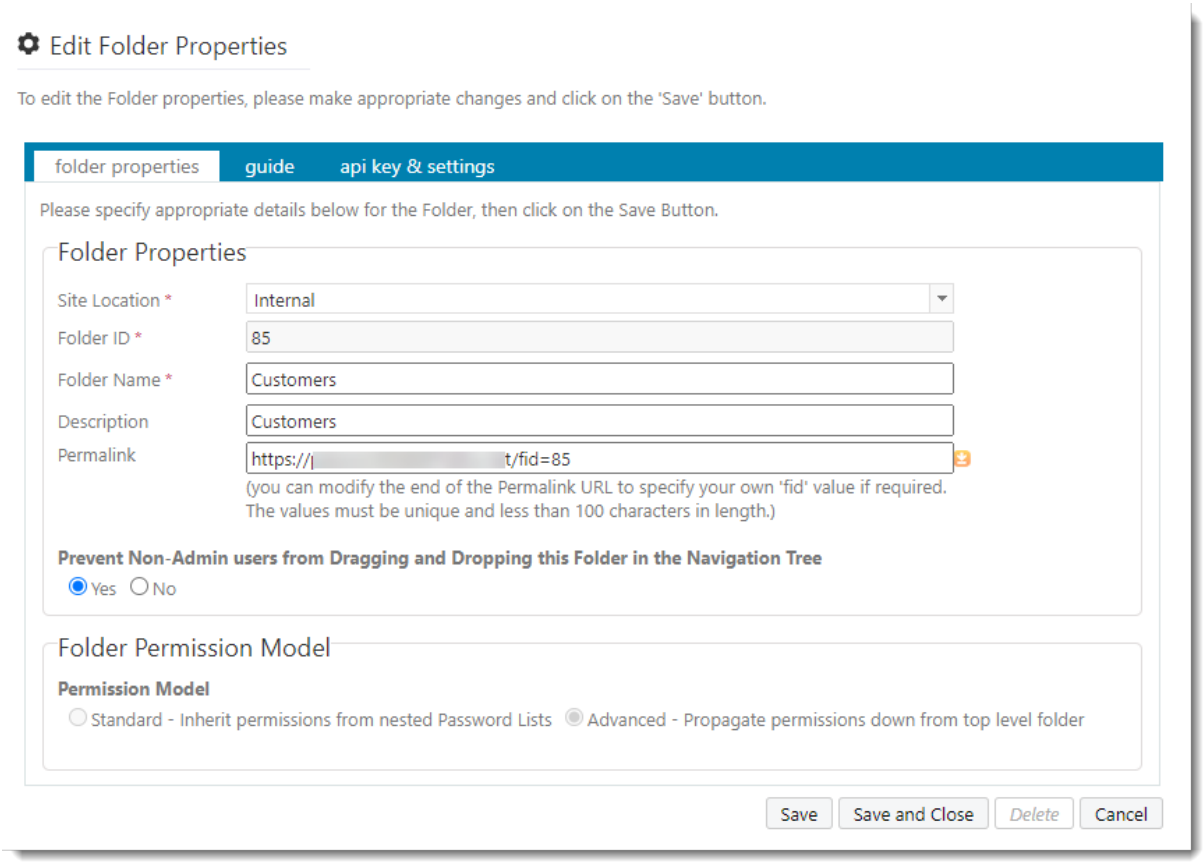
2.20 Password Folders

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

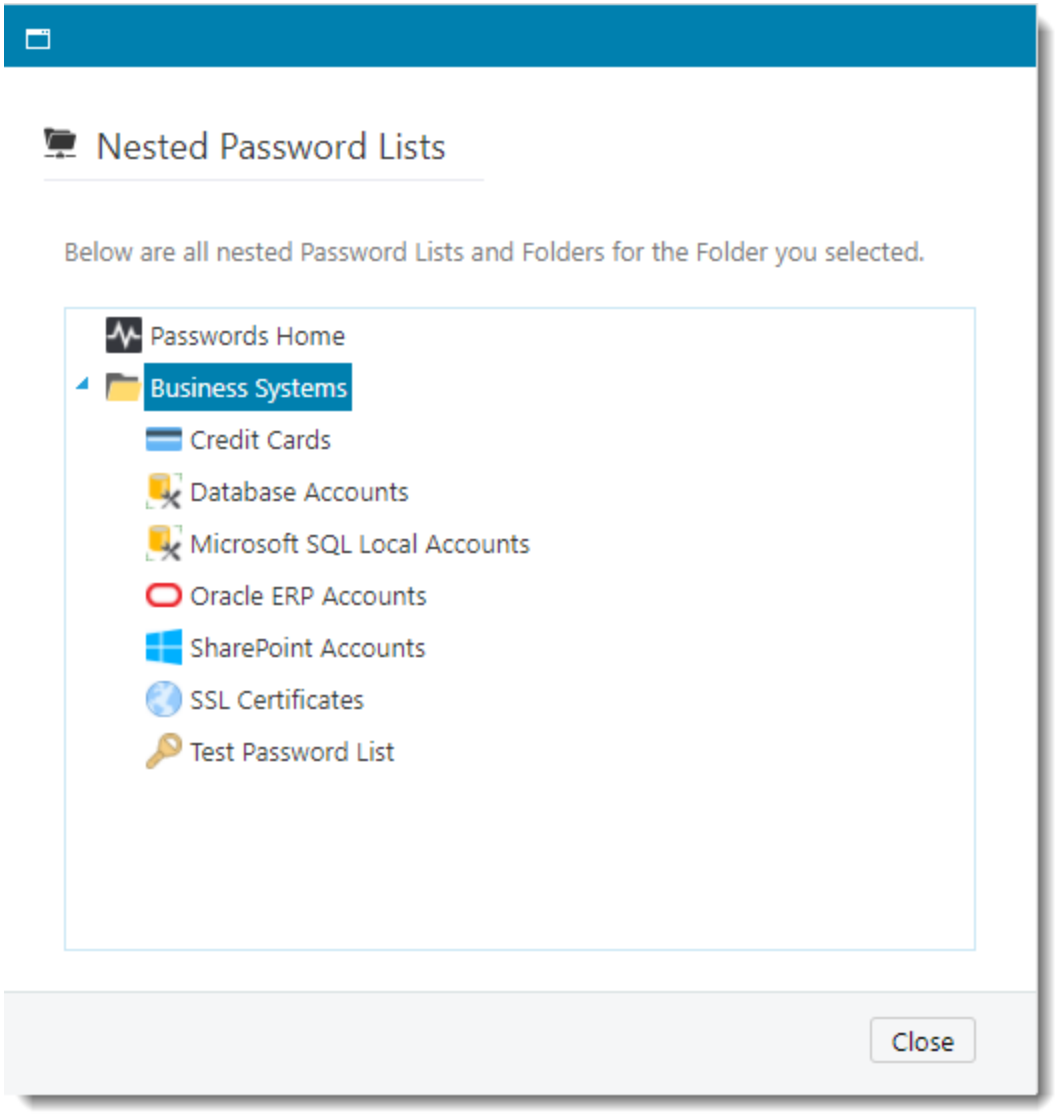
By clicking on the 'Password Folder' hyperlink you see in the grid, you will be taken to a screen where you can perform the following actions on the Folder:

- 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



View Nested Password Lists

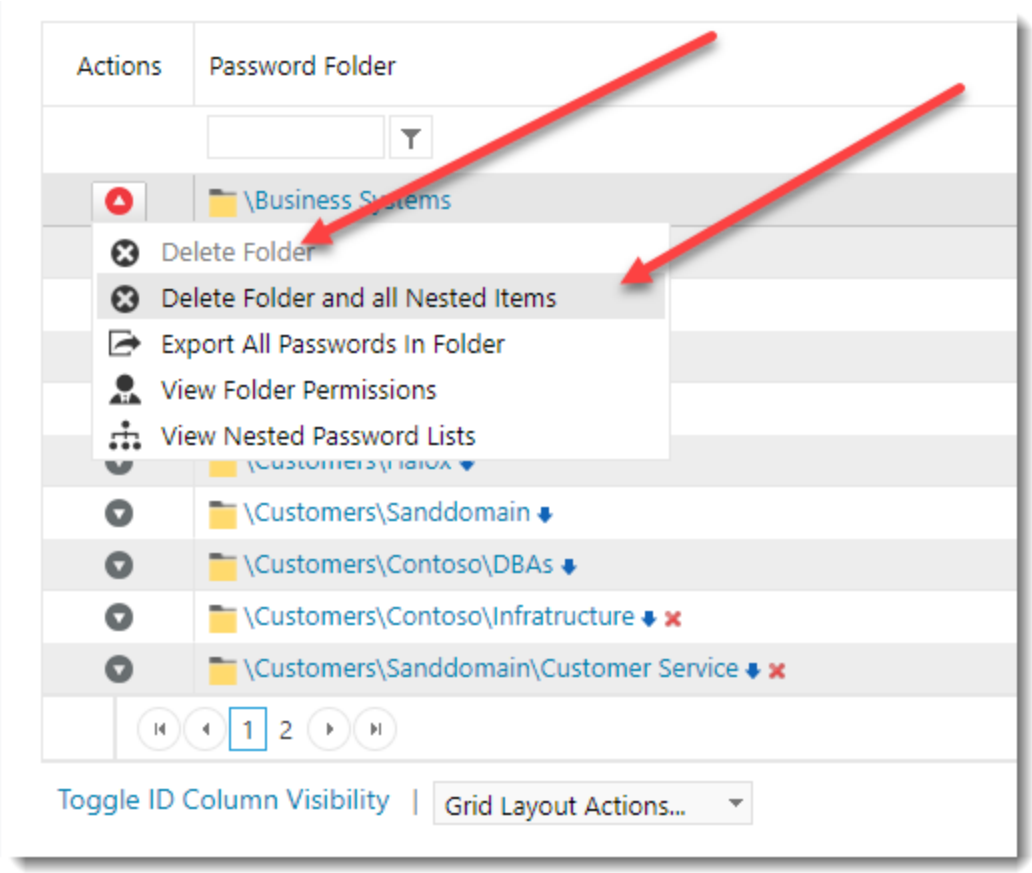
By selecting the option 'View Nested Password Lists' from the appropriate Actions drop-down menu, a popup screen will appear showing all Folders and Password Lists nested beneath the one you've chosen.



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



2.21 Password Generator Policies

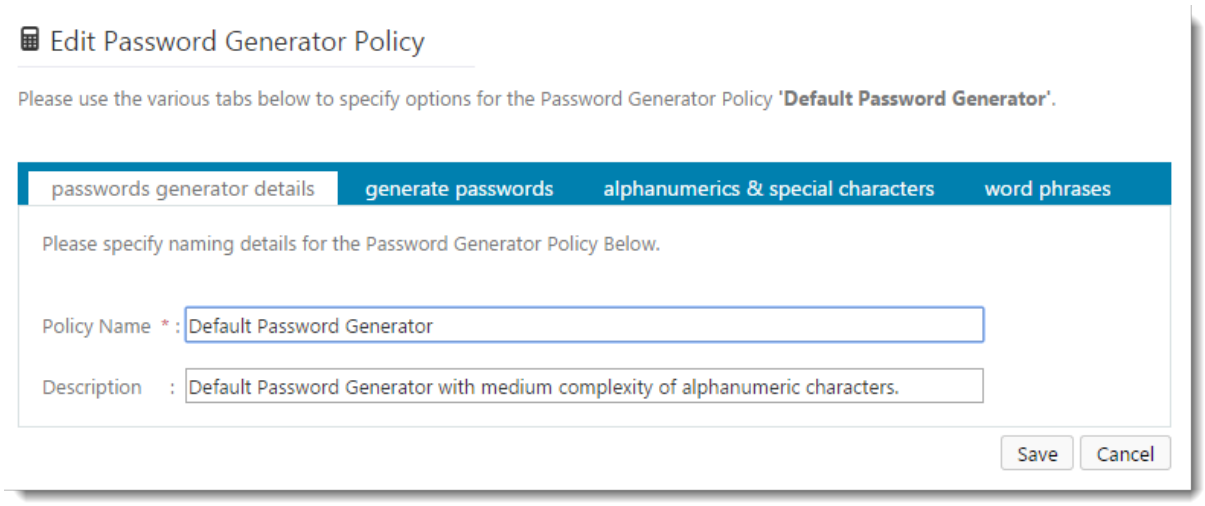
The Password Generator Policies screen allows you to create and manage multiple settings for the Password Generator, which can then be applied to one or more Password Lists.

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:

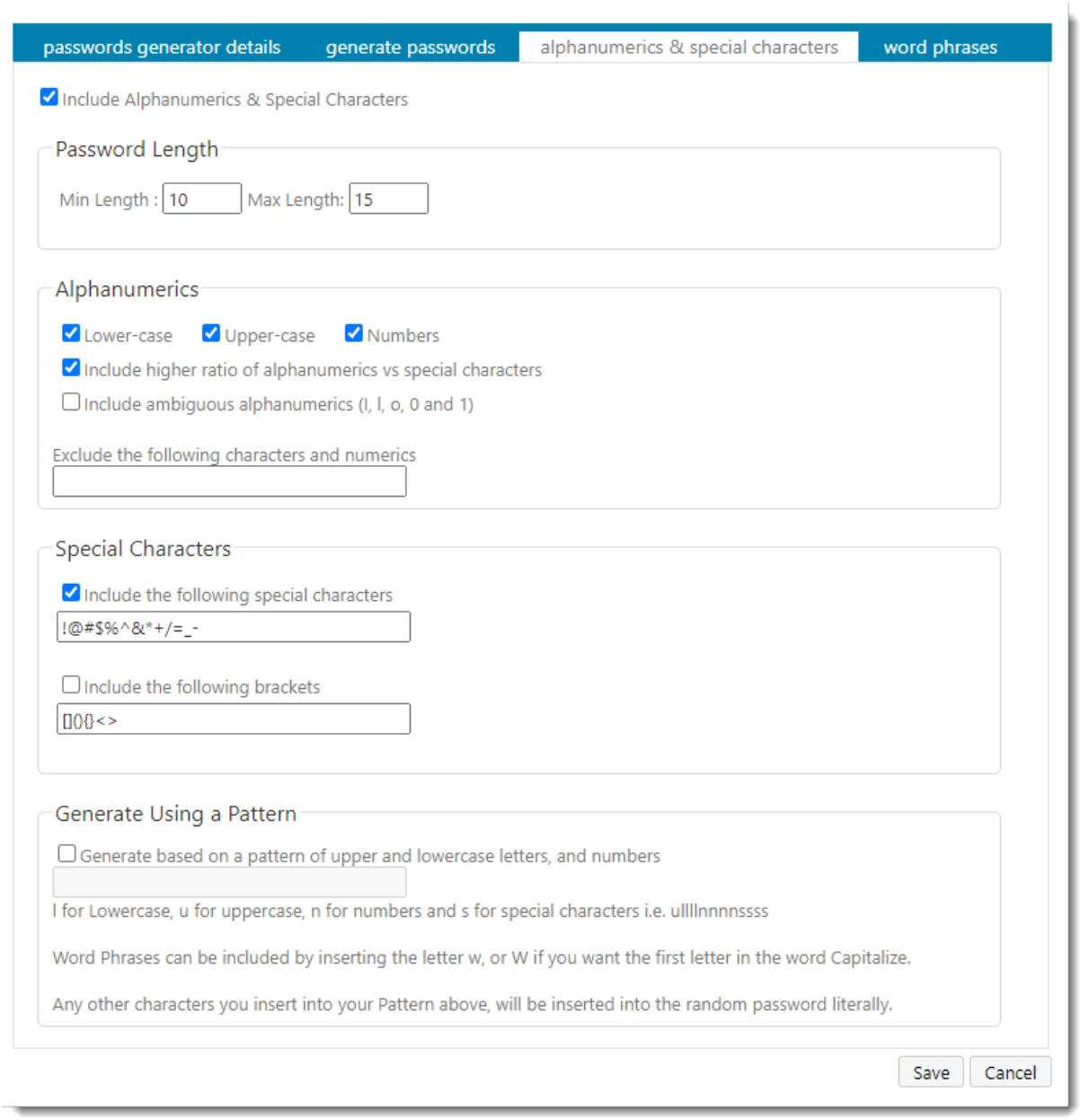
Password Generator Details

Edit the name and description for the Policy.



Alphanumerics & Special Characters

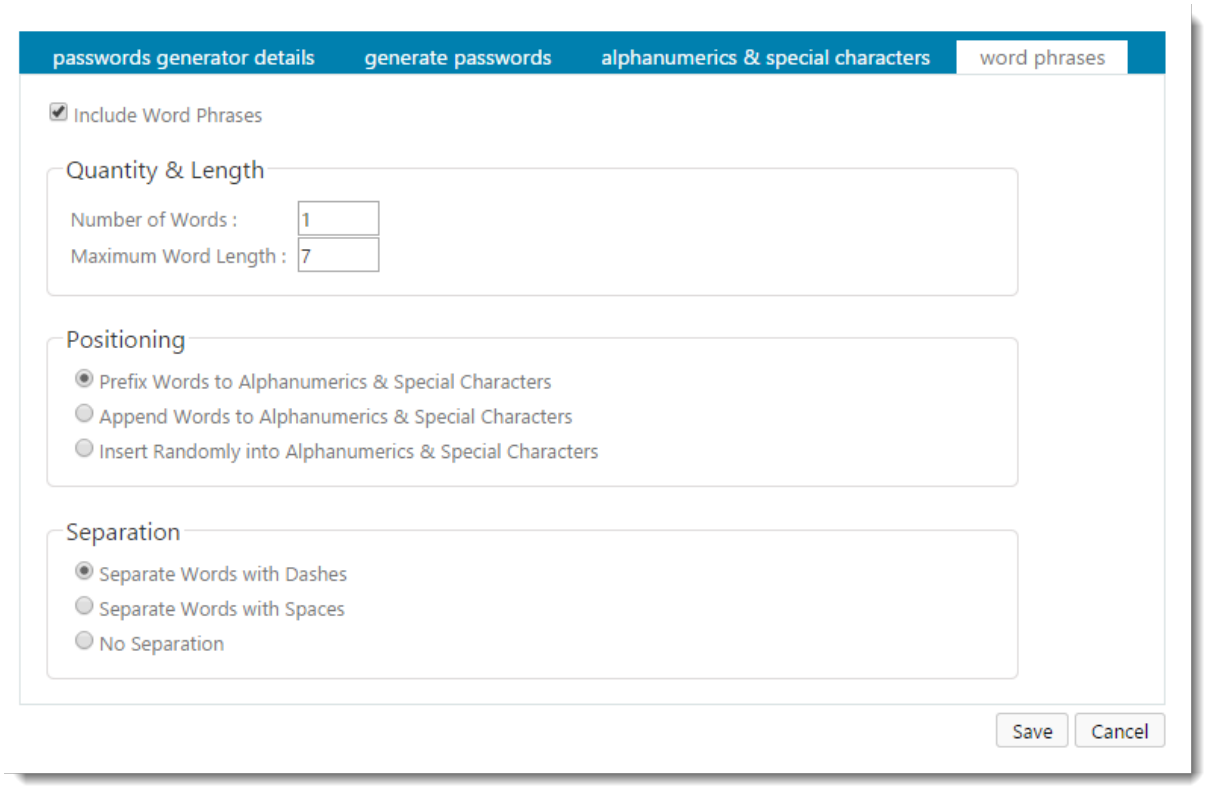
The Alphanumeric & Special Characters tab allows you to specify the desired length of the password you wish to generate, as well as settings for letters, numbers, special characters and various forms of brackets.



Word Phrases

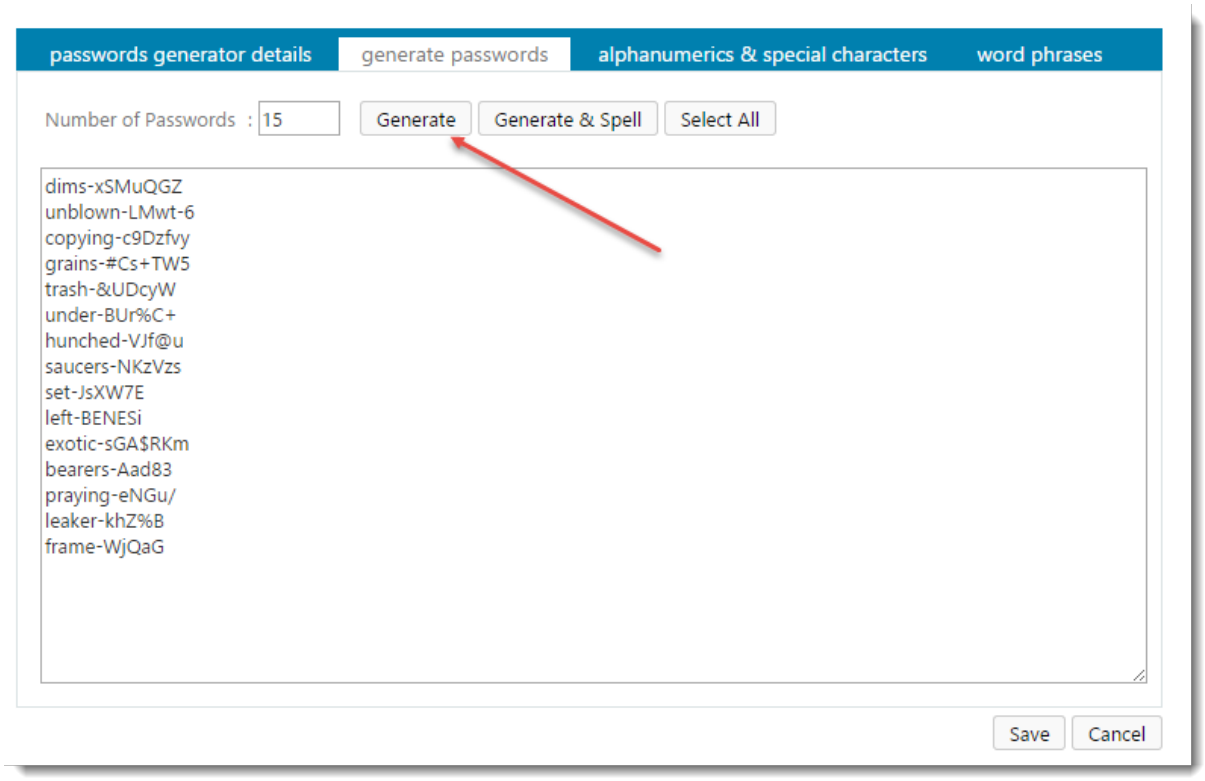
The Word Phrases tab allows you to insert a random word at the beginning of the password, somewhere in the middle, or at the end. You can specify how many words to create, what length, and what form of separation you would like between the word and the rest of the random password - either dashes, spaces or nothing.

Passwordstate has 10,000 different words it can choose from, all of different lengths.

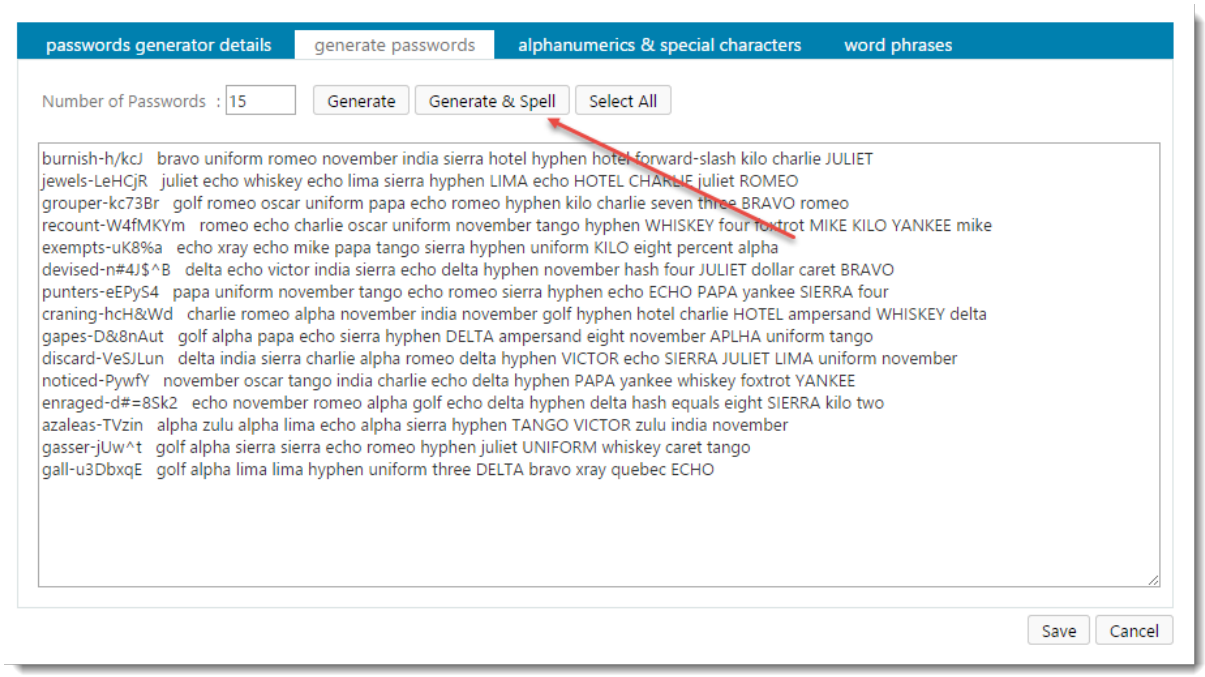


Generate Passwords

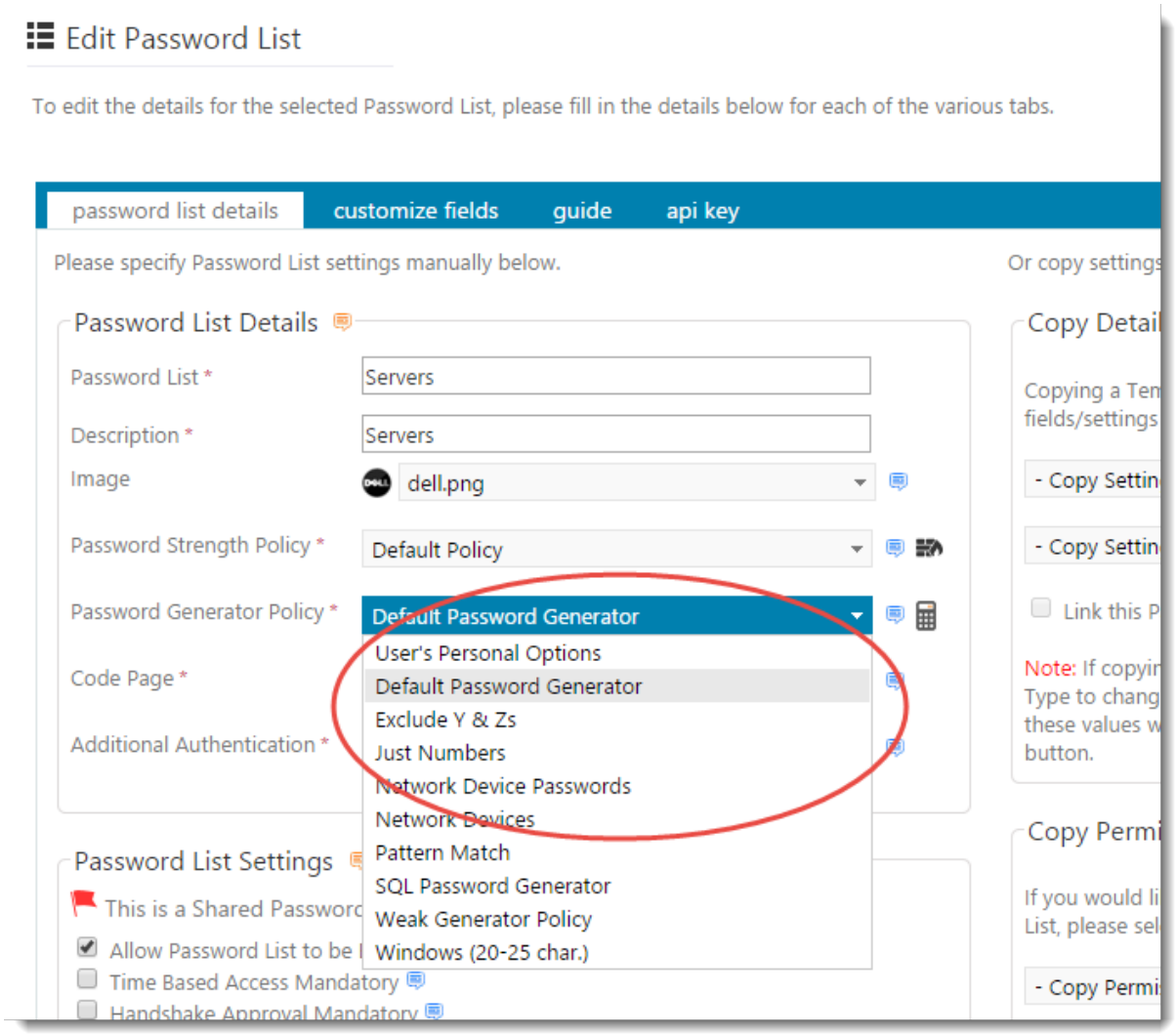
The Generate Passwords tab allows you to test the settings you have specified on the other tabs, and also generate any number of random passwords based on your settings. Click on the 'Generate' button just gives you the random passwords.



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

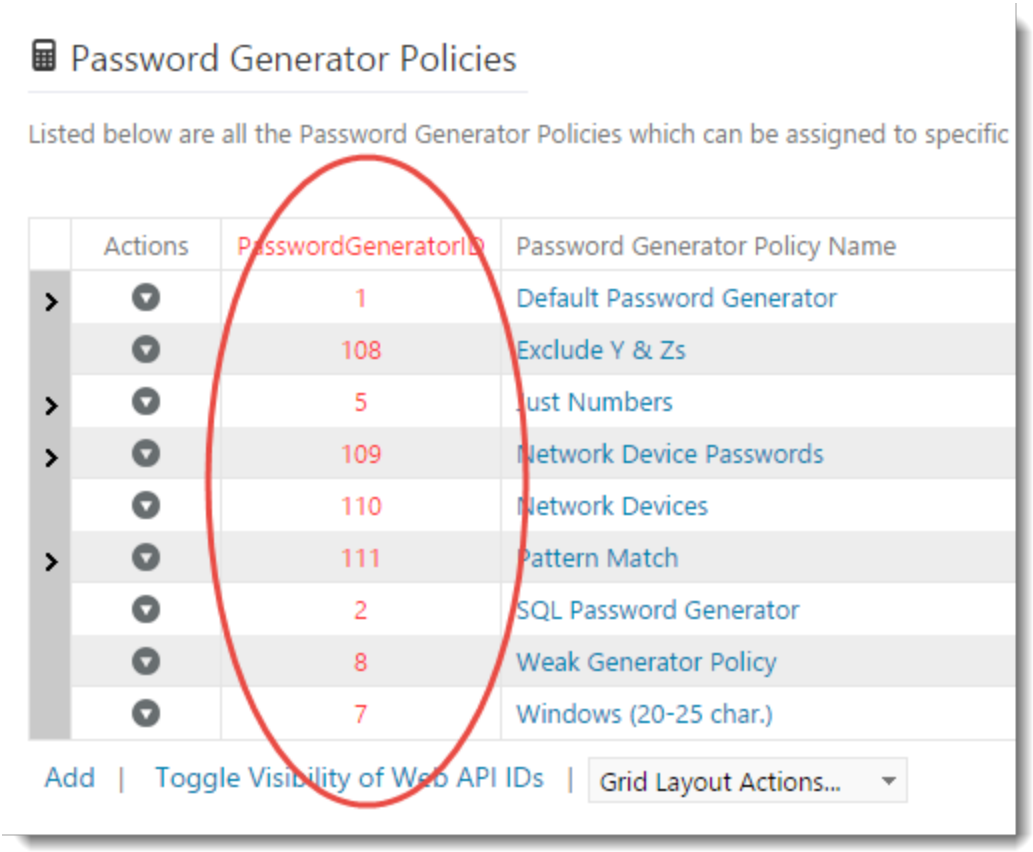


Once a Password Generator Policy has been created, it can be assigned to a Password List or Password List Template, by editing the appropriate settings, as per this screenshot below. When your users now click on the icon, the random password generated will be based on the selected Password Generator Policy.



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.

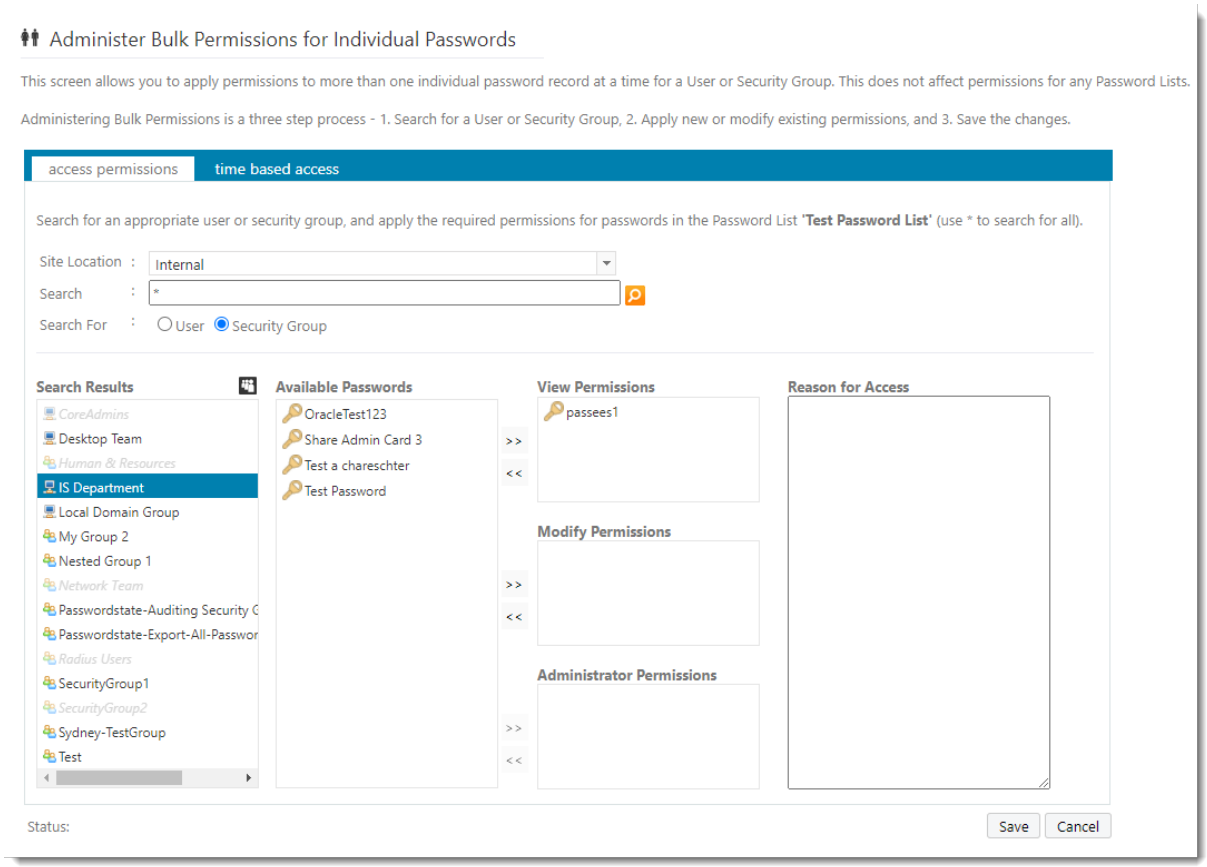
Note: Please refer to the Passwordstate User Manual for detailed instructions on settings which can be applied to a Password List or Template.

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' drop-down menu, you will be able to apply permissions for a user account or security group to multiple individual password records at once.



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

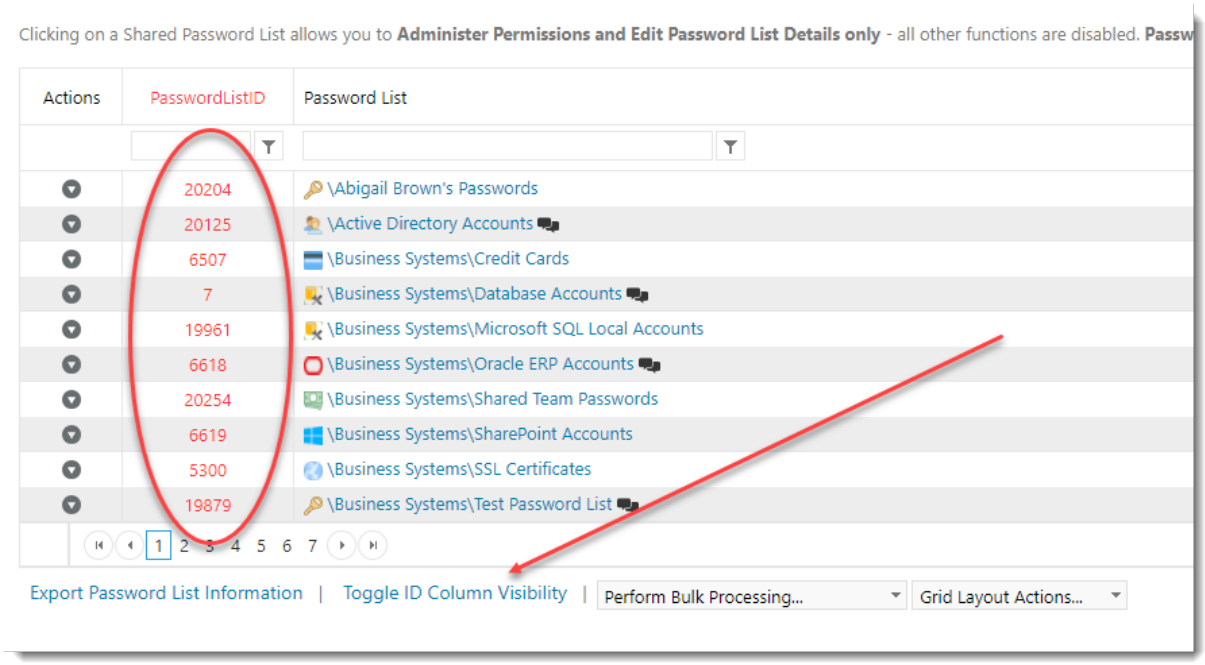
By selecting the 'Delete Password List' menu option in the 'Actions' drop-down menu, you will be given the opportunity to delete the selected Password List.

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.



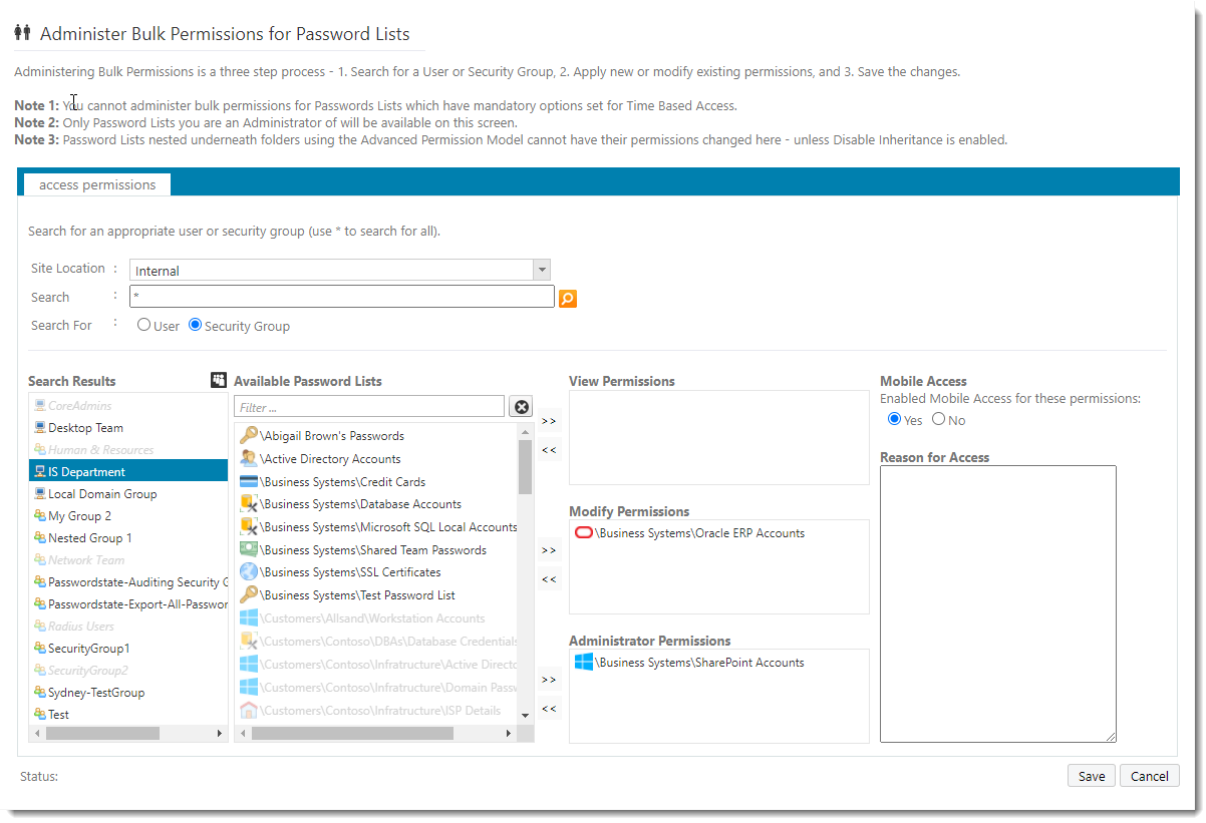
Perform Bulk Processing - Administer Bulk Permissions

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.

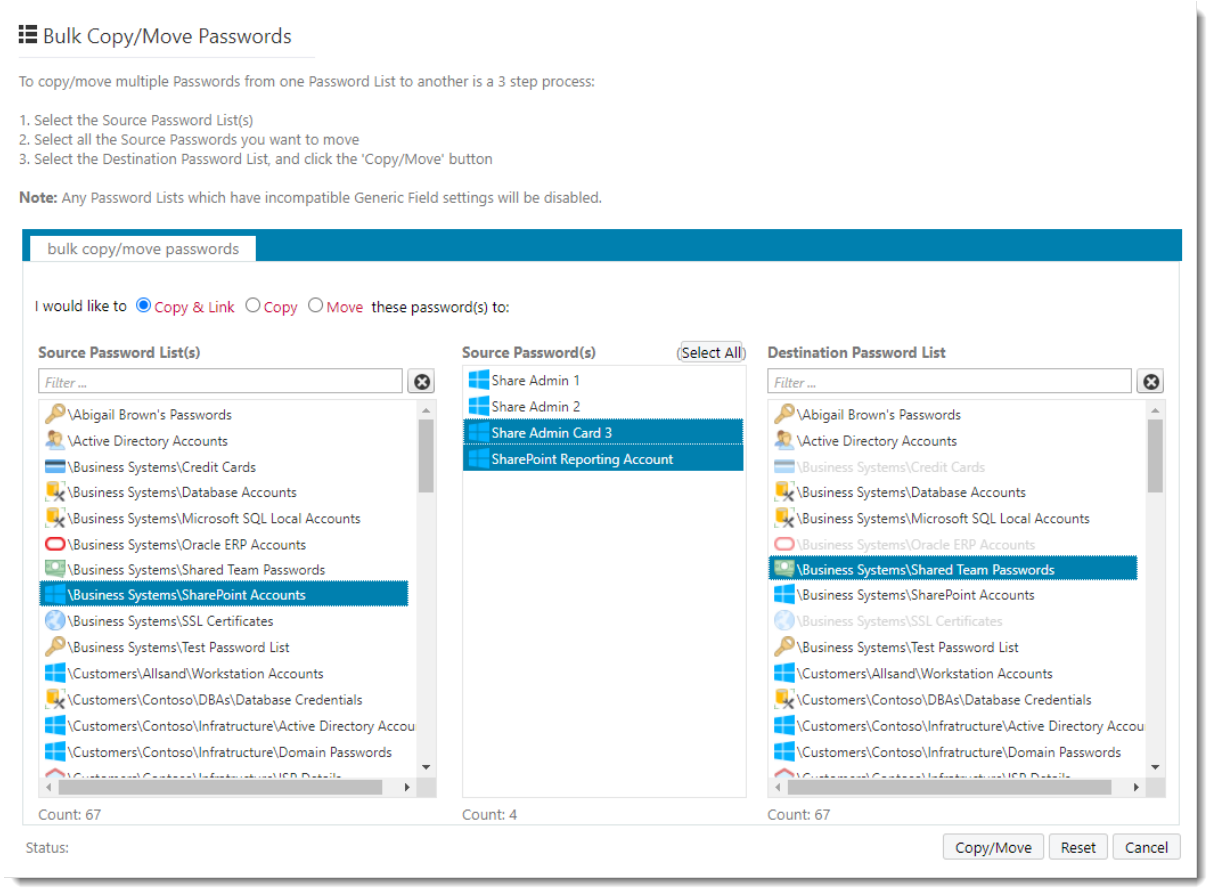
Note: You cannot manage permissions here for Password Lists which have mandatory options set for Time-Based Access.



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 re-organizing your Password Lists, and need to move records around in mass.

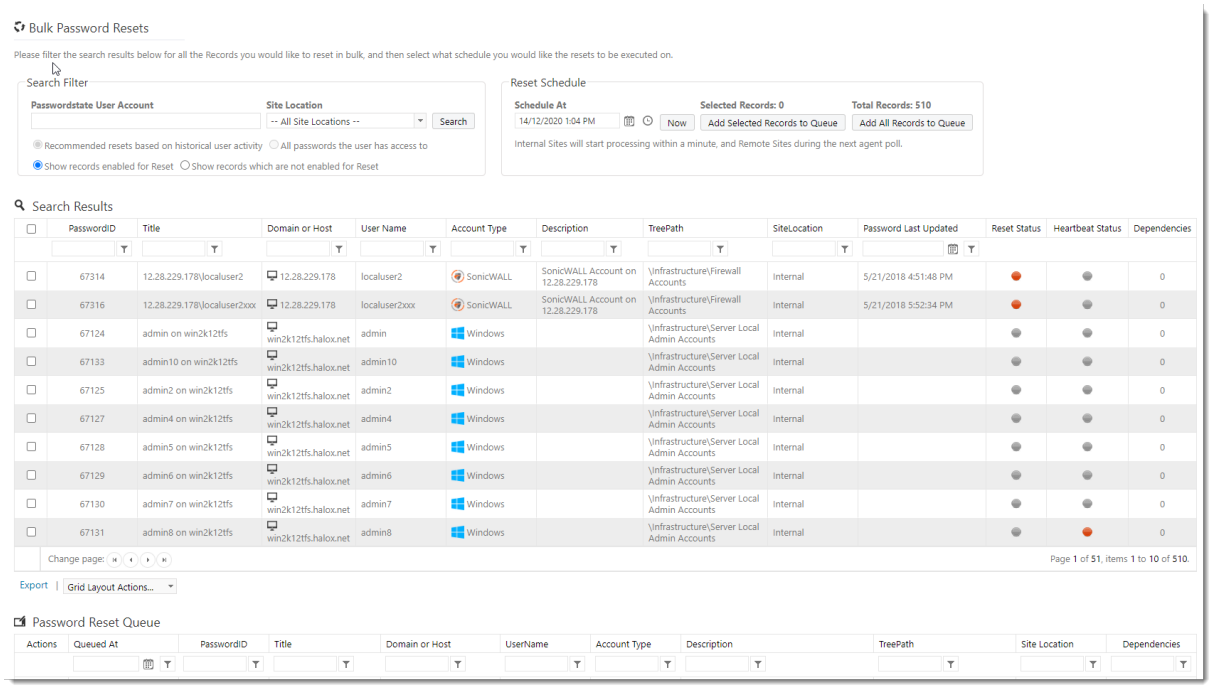
Note: You can only copy/move records between Password Lists which have similar fields configured. If the fields are not compatible, then the destination Password List will be disabled, preventing you from copying/moving records to it.



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.

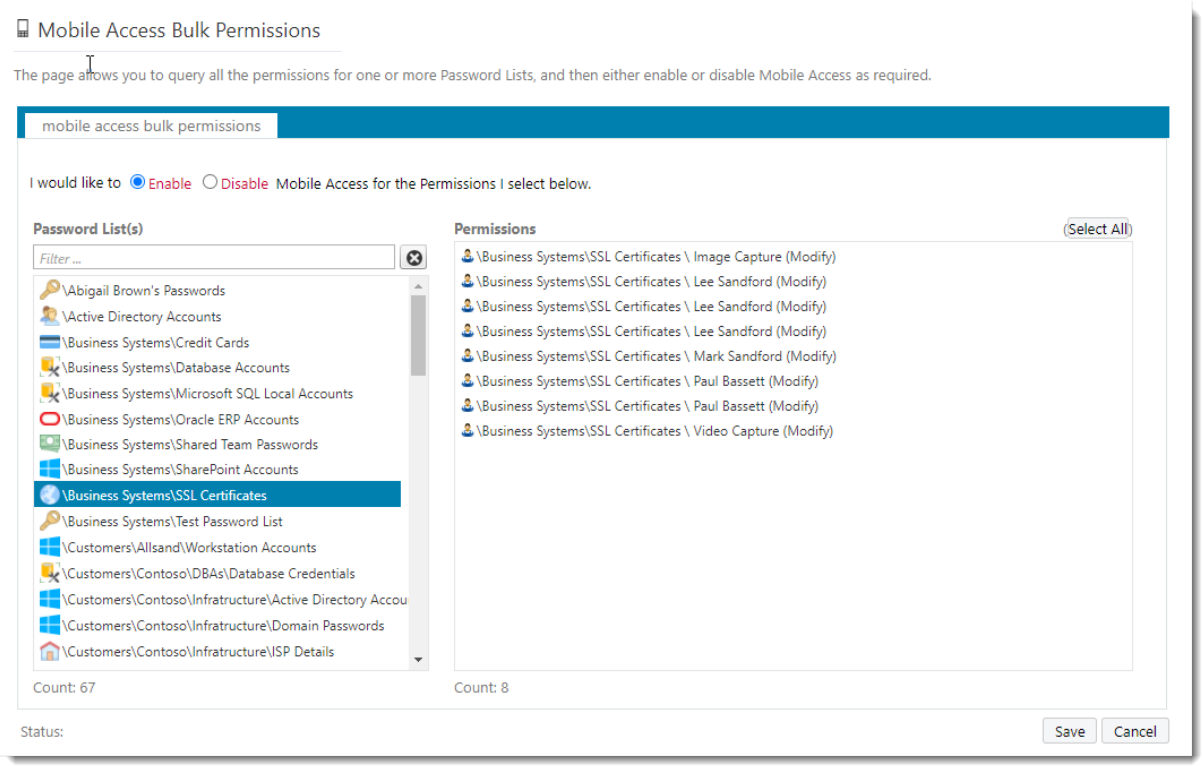
This feature is useful if you have an employ leave, and you can filter on password records the user has access to, as well as ones which are recommended to be reset based on the user's previous activity i.e. have they seen the value of the password since it was last reset.



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.

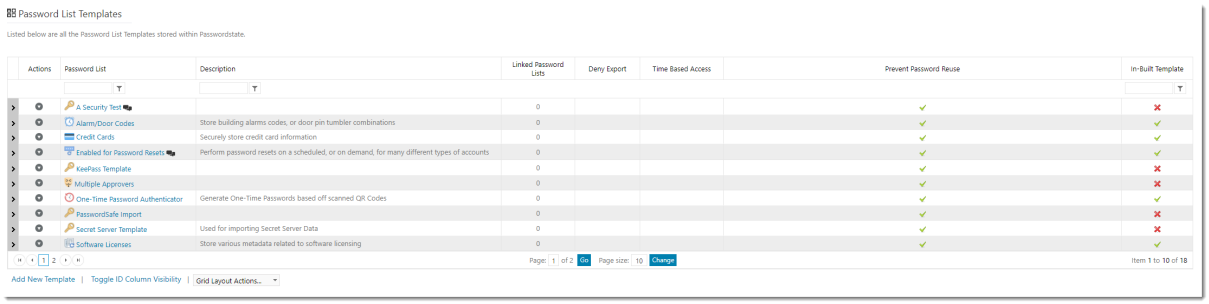


2.23 Password List Templates

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.



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.

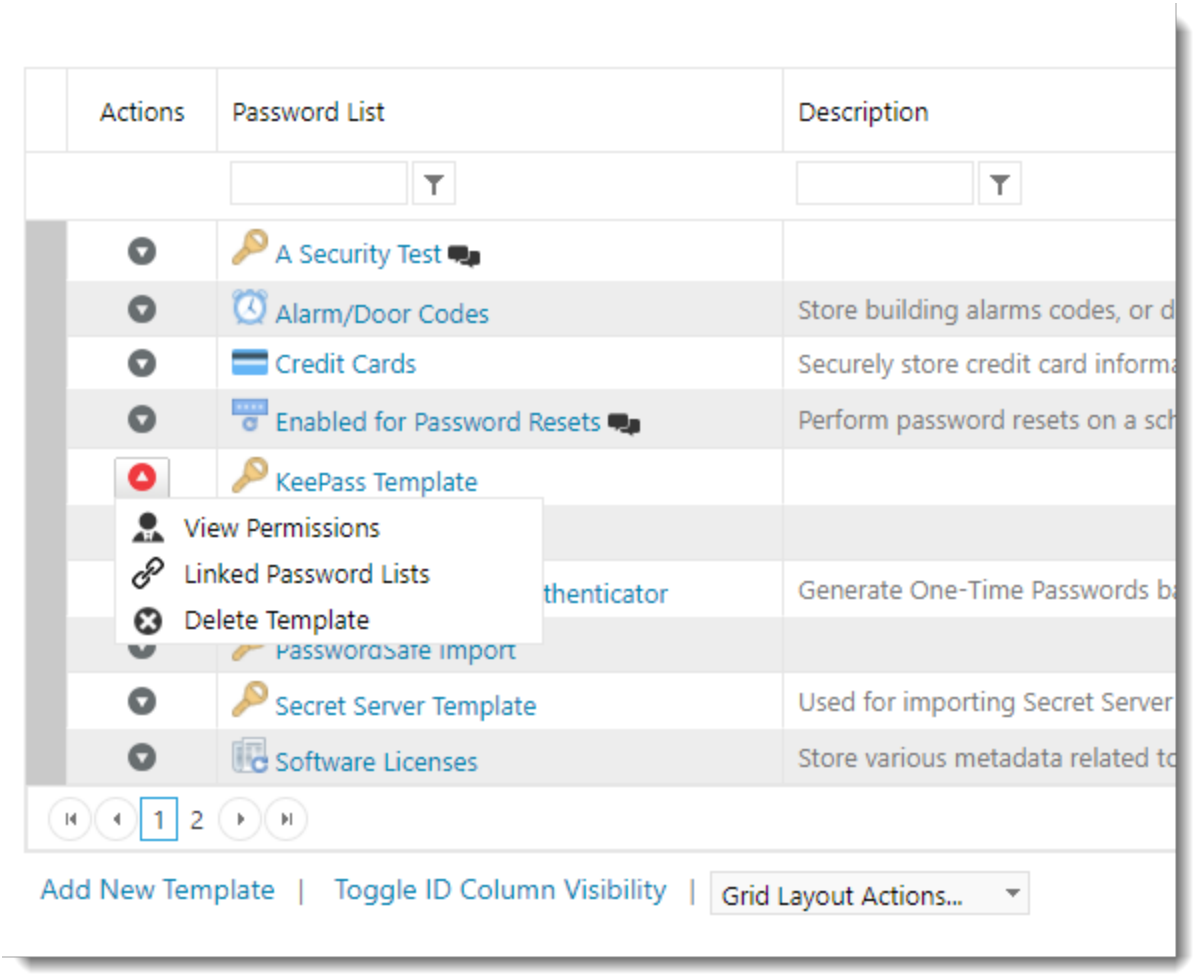
Caution: When editing a Template's settings when it is linked to other Password Lists, if you change any of the Field Types for any Generic Fields, these fields will have their data cleared/blanked in the database when you click on the 'Save' button. This is because the different Generic Field Field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

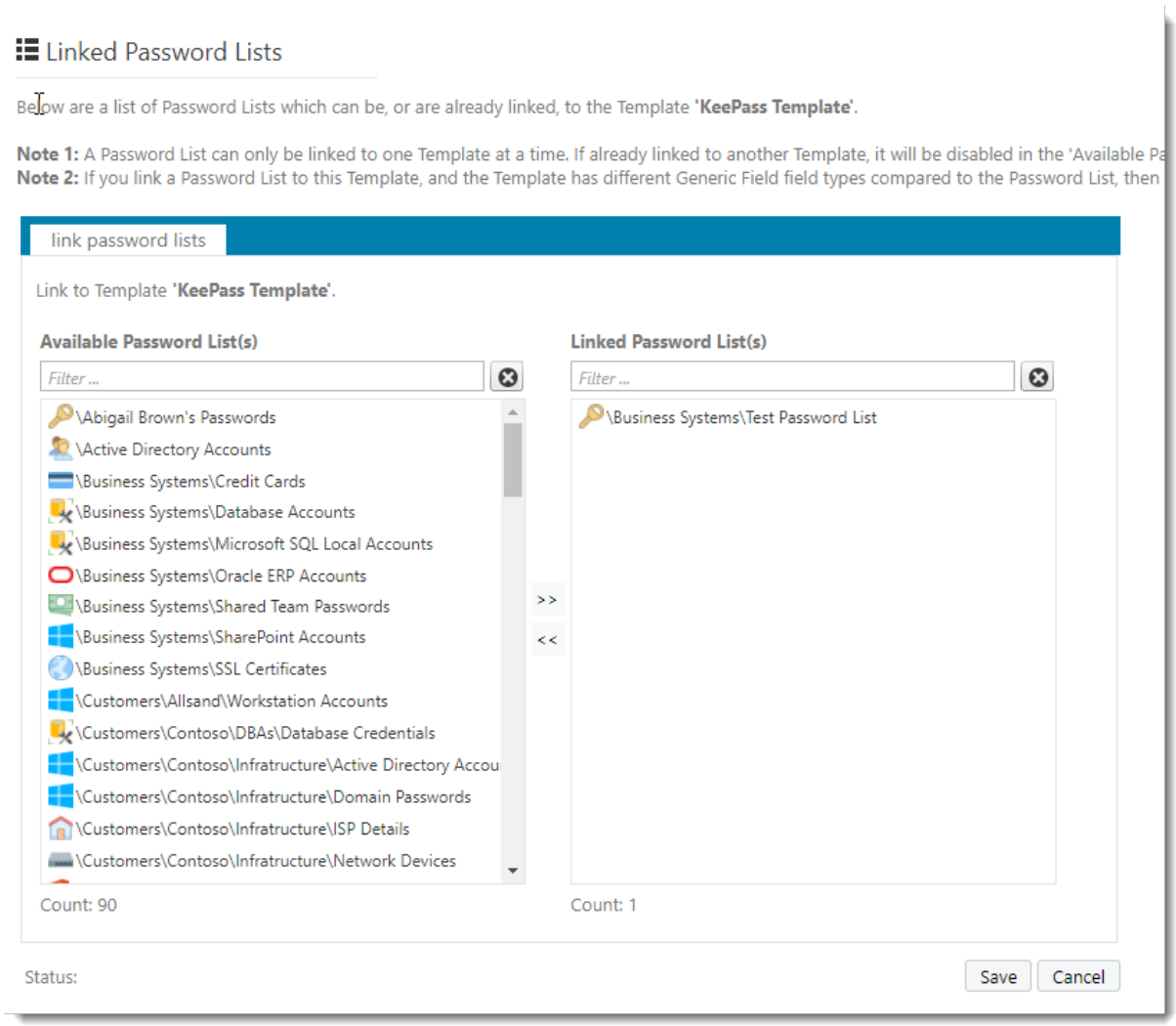


Linked Password Lists

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

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

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



2.24 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.

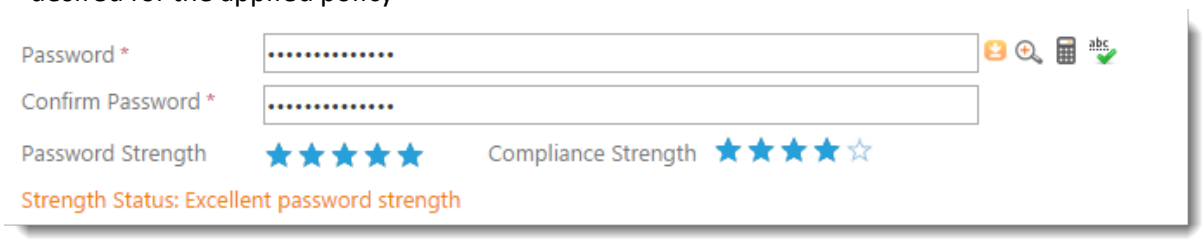
When adding or editing a Password Strength Policy, settings can be applied on 2 of the tabs, and there is 1 tab for testing the policy.

Policy Settings Tab

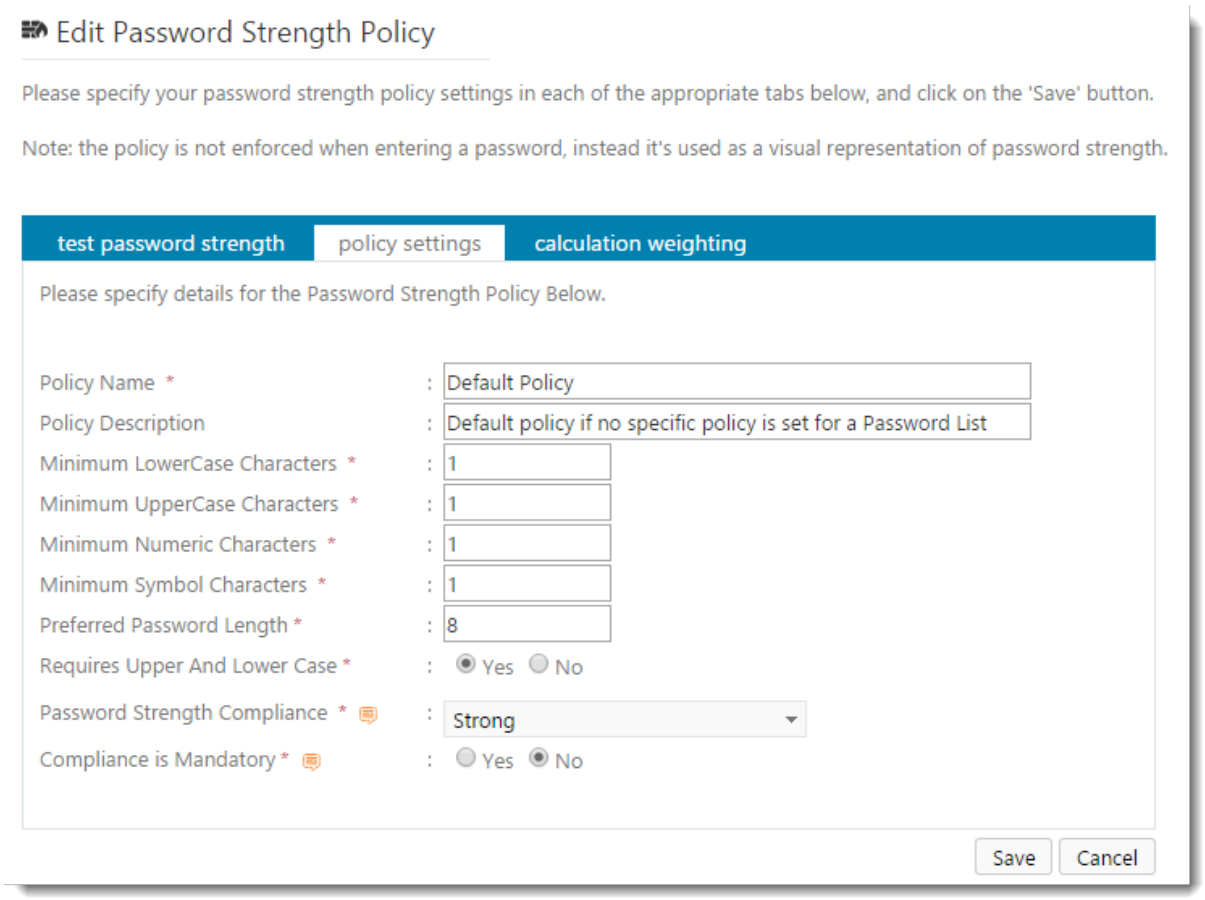
The Policy Settings Tab allows you to provide a name and description for the policy, plus the following settings:

- 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



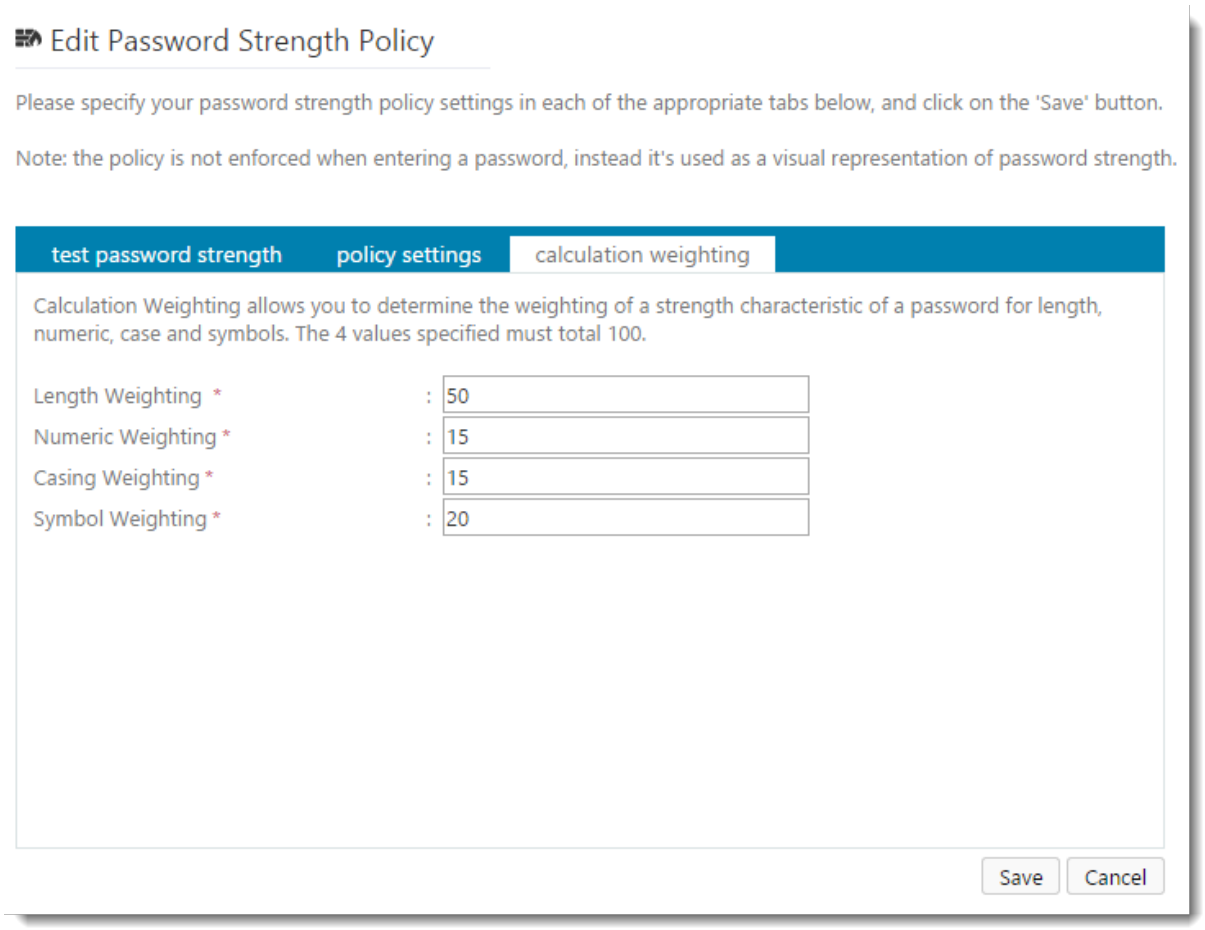
- Compliance is Mandatory - if this option is set to Yes, the user will not be able to save the password record if the strength of the password they're creating does not meet the 'Password Strength Compliance' setting above



Calculated Weighting Tab

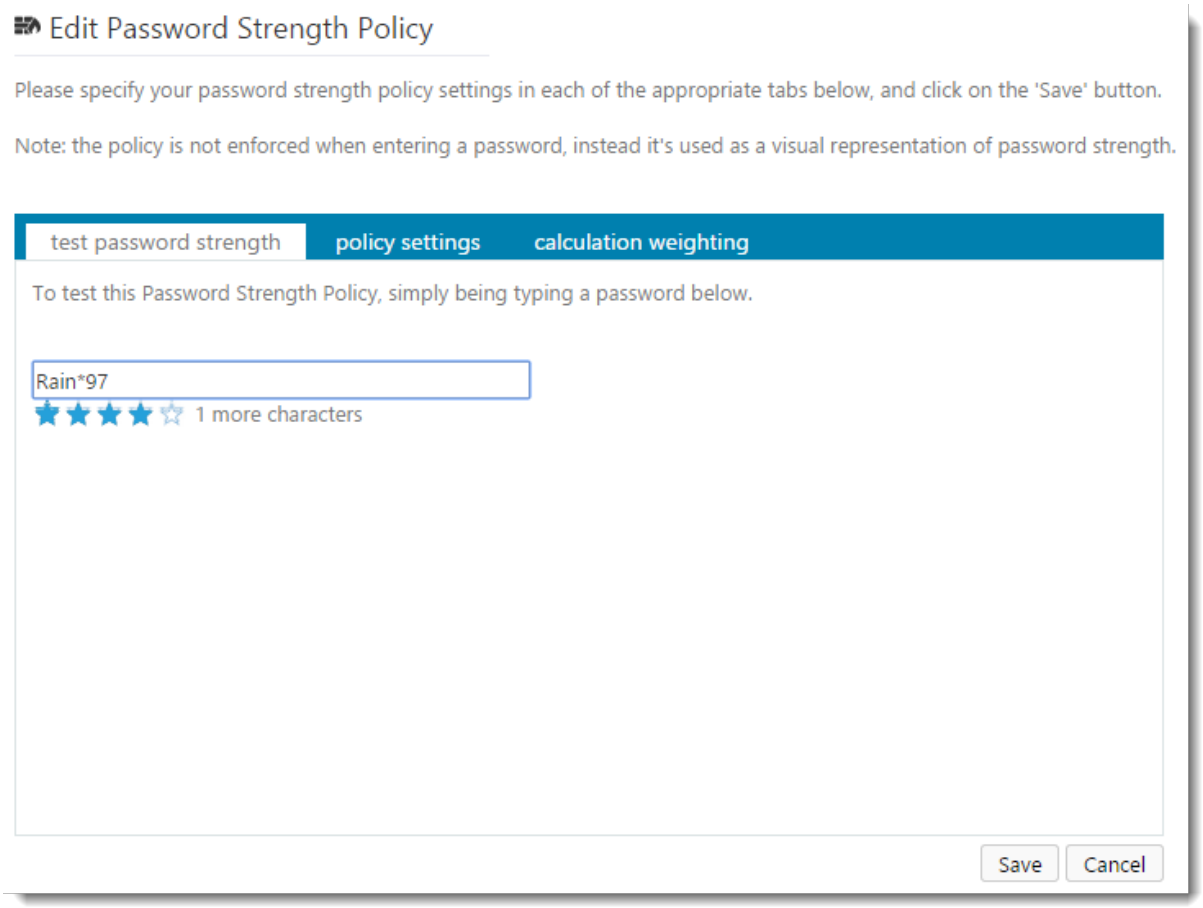
The Calculated Weighting Tab allows you to specify the weighting of a strength characteristic of a password for length, numeric, case and symbols. The higher the weighting, the more important the category is deemed to be.

Note: The 4 values specified must total 100.



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.



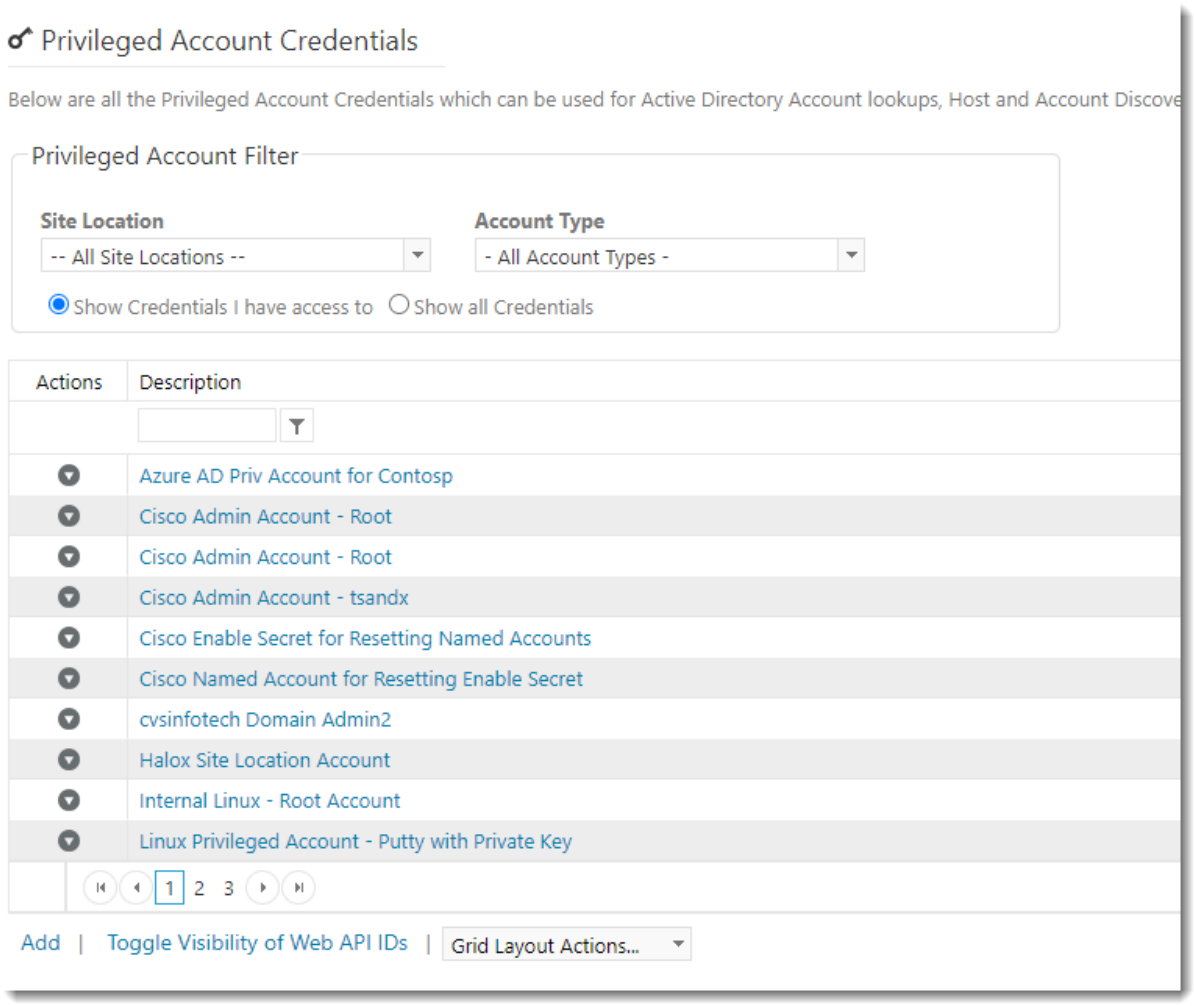
2.25 Privileged Account Credentials

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.

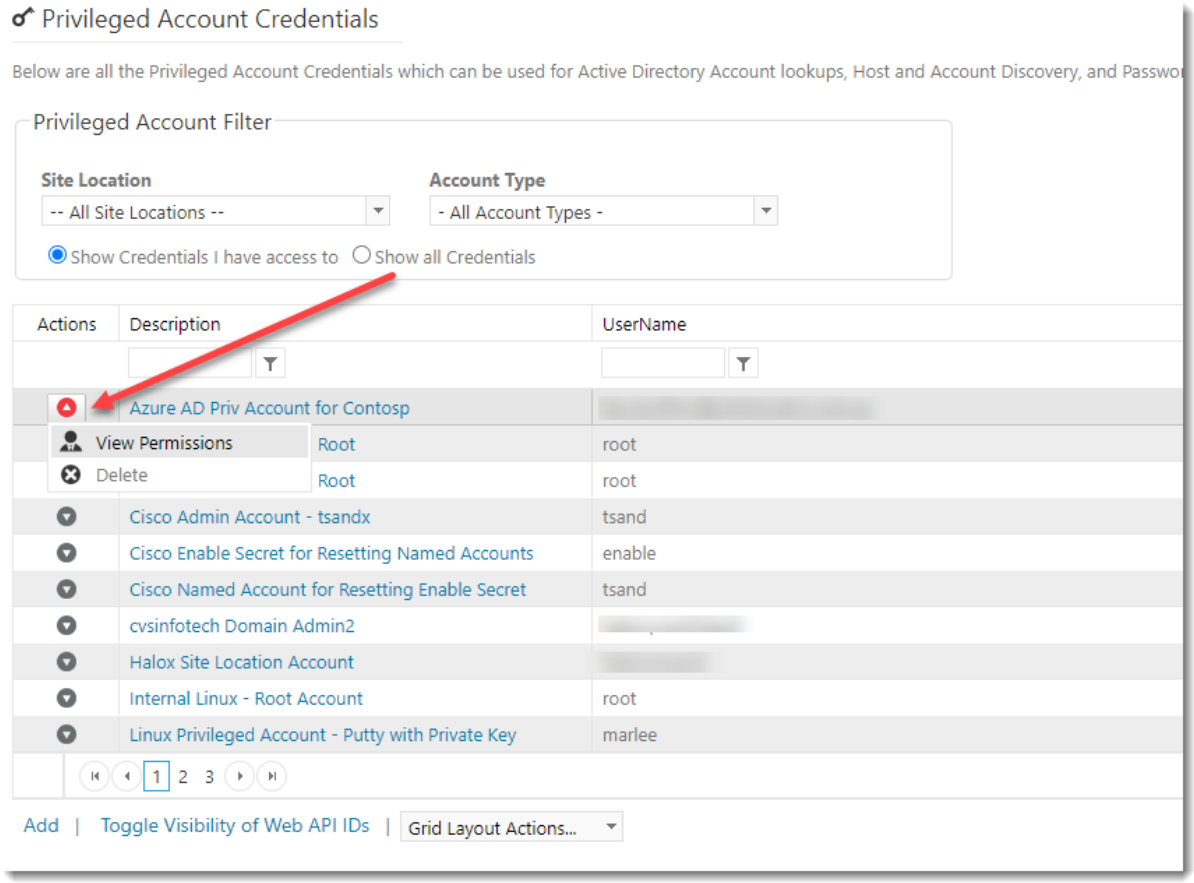
Once you have specified the details for one or more of the relevant Privileged Account Credentials, and applied permissions for users or security groups who are allowed to use these accounts, then they can be used for Password Resets and Discovery jobs, etc.

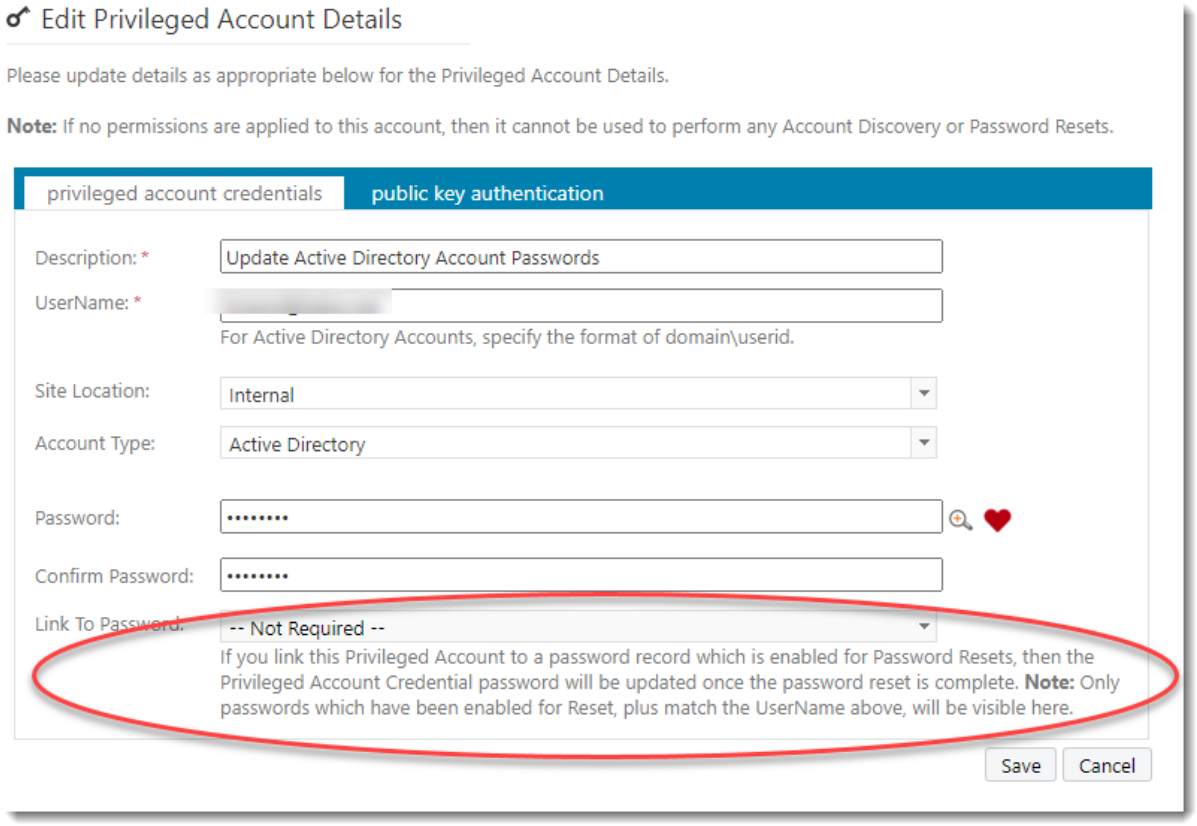
If you "link" the Privileged Account to a password stored in Passwordstate, when the password is updated in Passwordstate and Active Directory, it will also be automatically updated on this screen as well.

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.



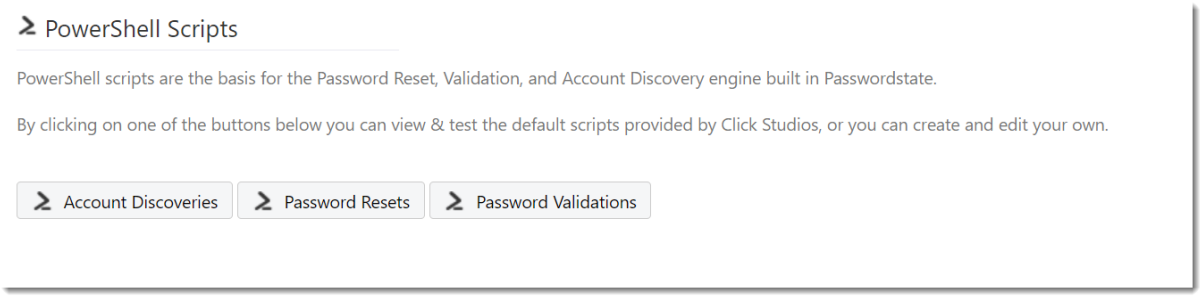
Note: When apply permissions to Privileged Account Credentials, you can also specify Time-Based Access as well - so user's access to the account can automatically be removed after a set period of time.





2.26 PowerShell Scripts

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



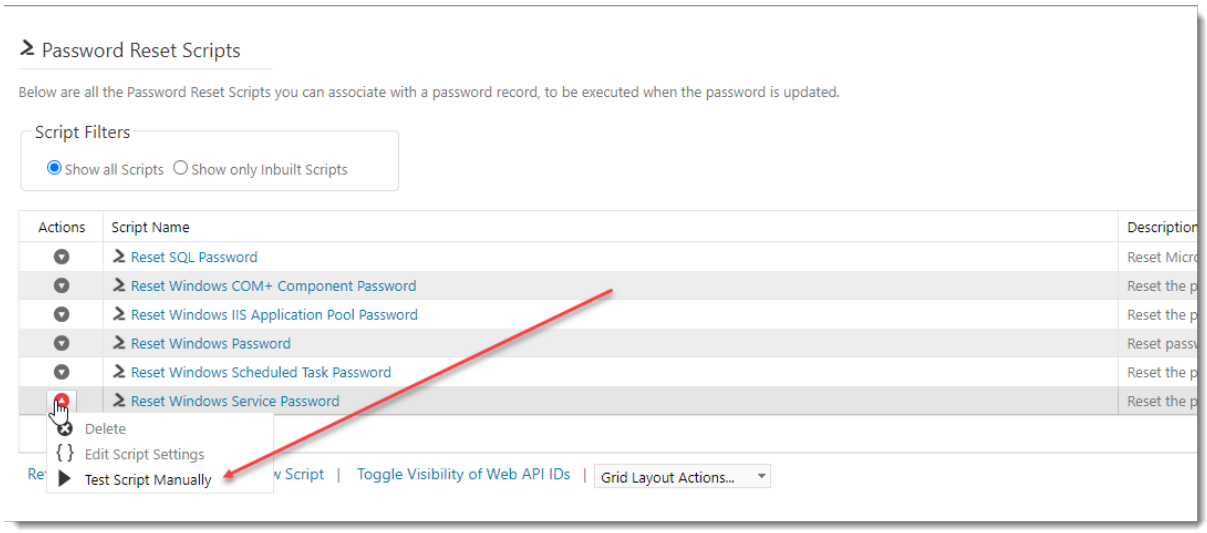
In addition to these default scripts, you can also add your own scripts for your own Infrastructure or Applications. See the Images and Account Types section of this manual for information about how to add in a custom **Managed Account**. Adding in your own custom Managed Account into Passwordstate means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

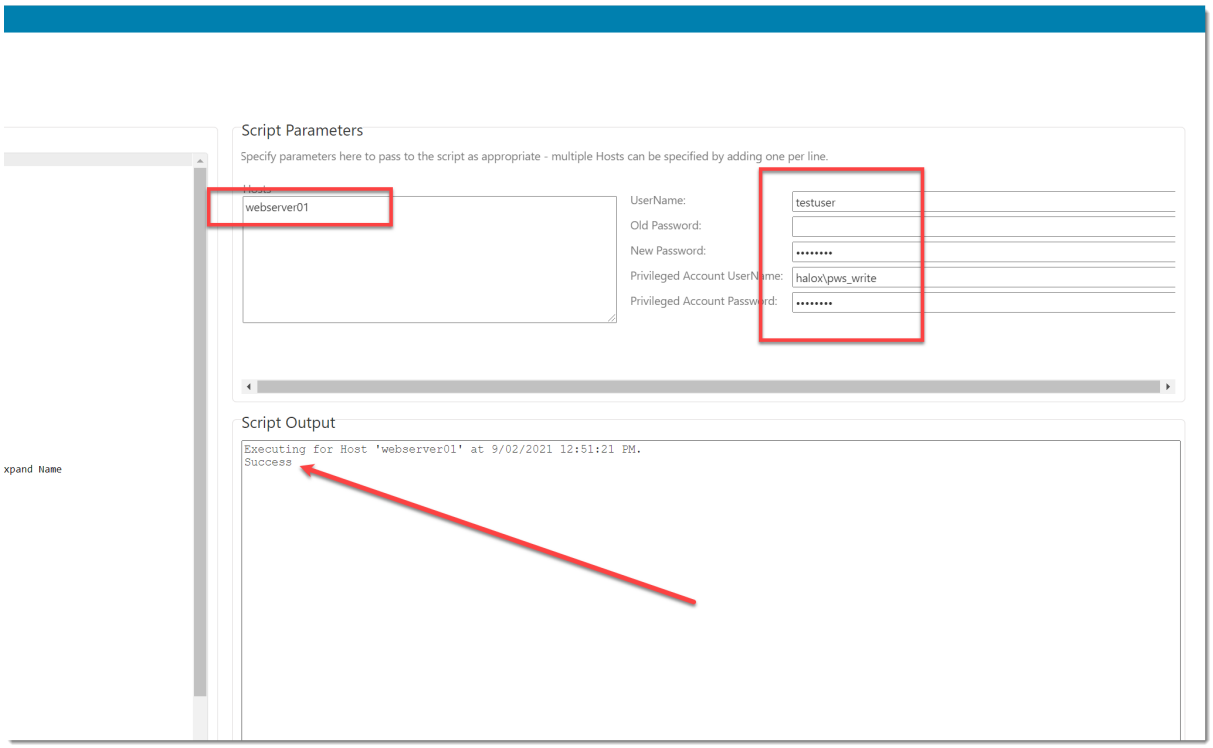
Examples of these Password Dependency scripts could be emailing a distribution list of a successful reset, or maybe updating a ticketing system.

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.



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)



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.

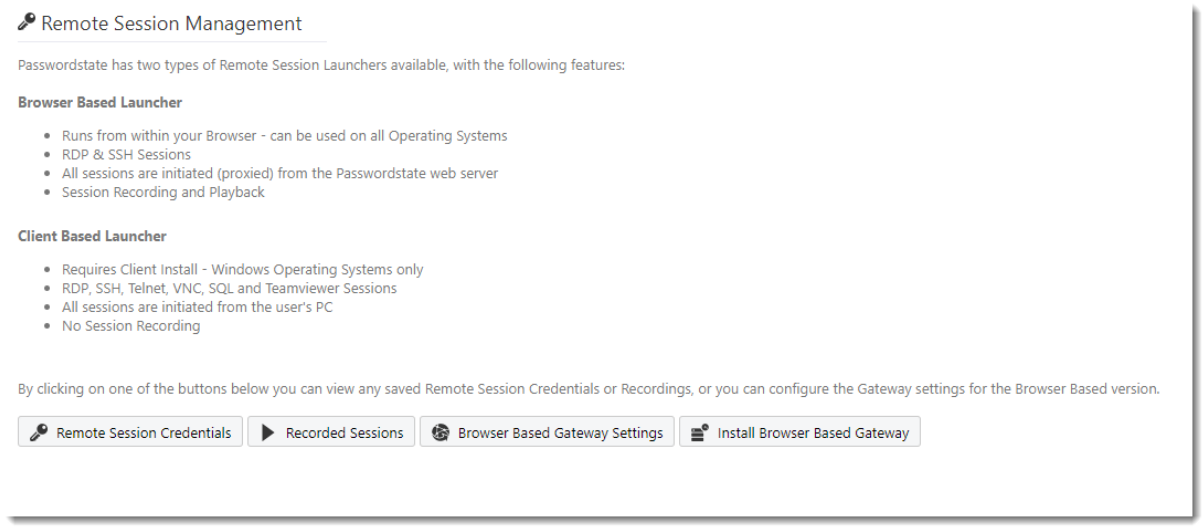
SSH Template Scripts

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_Management_Manual.pdf

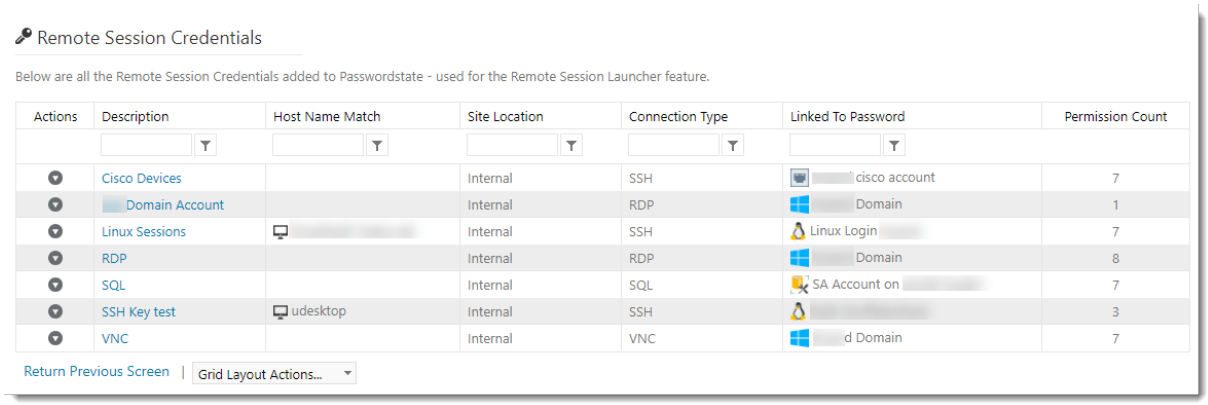
2.27 Remote Session Management

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



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.

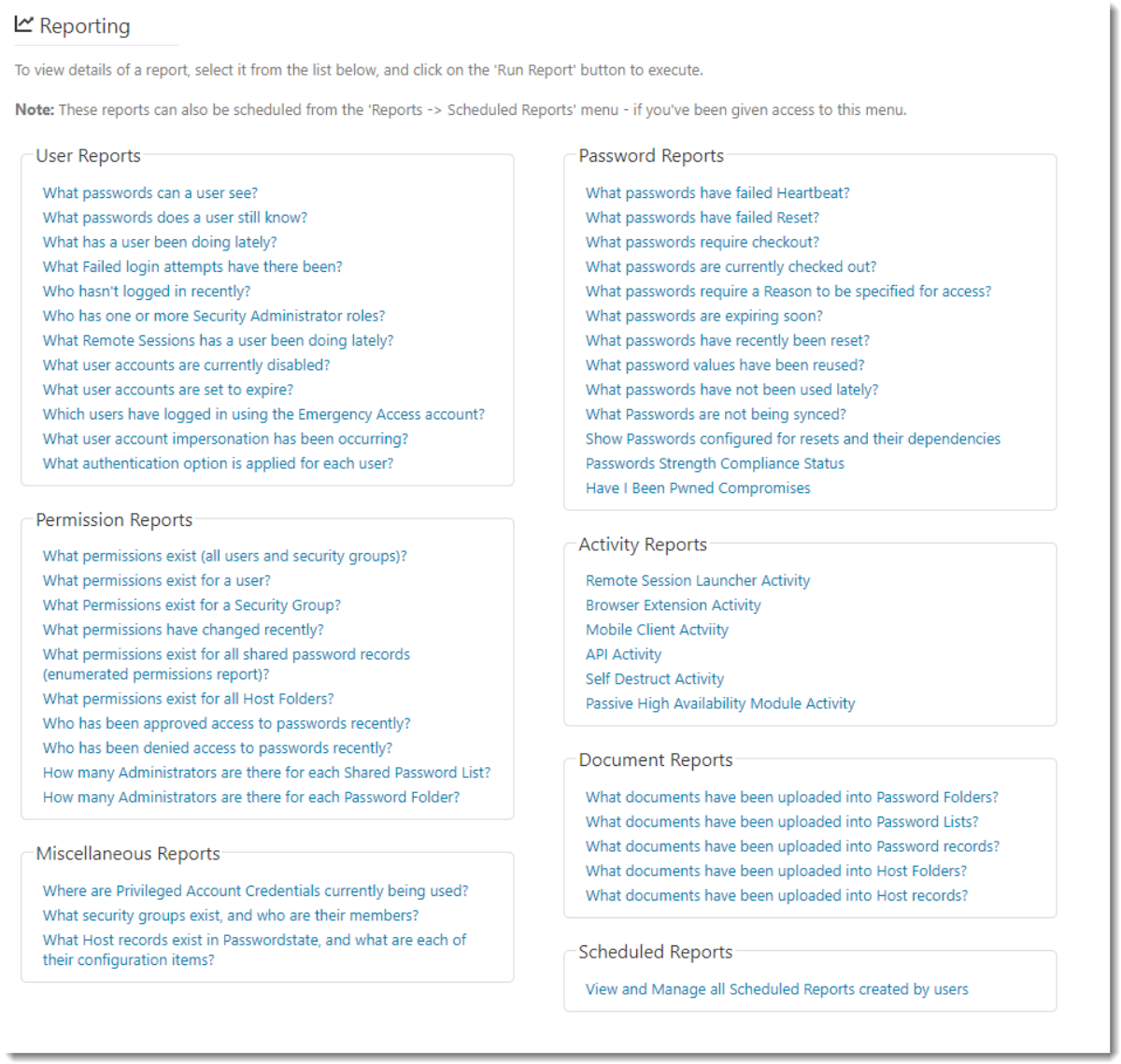


2.28 Reporting

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.

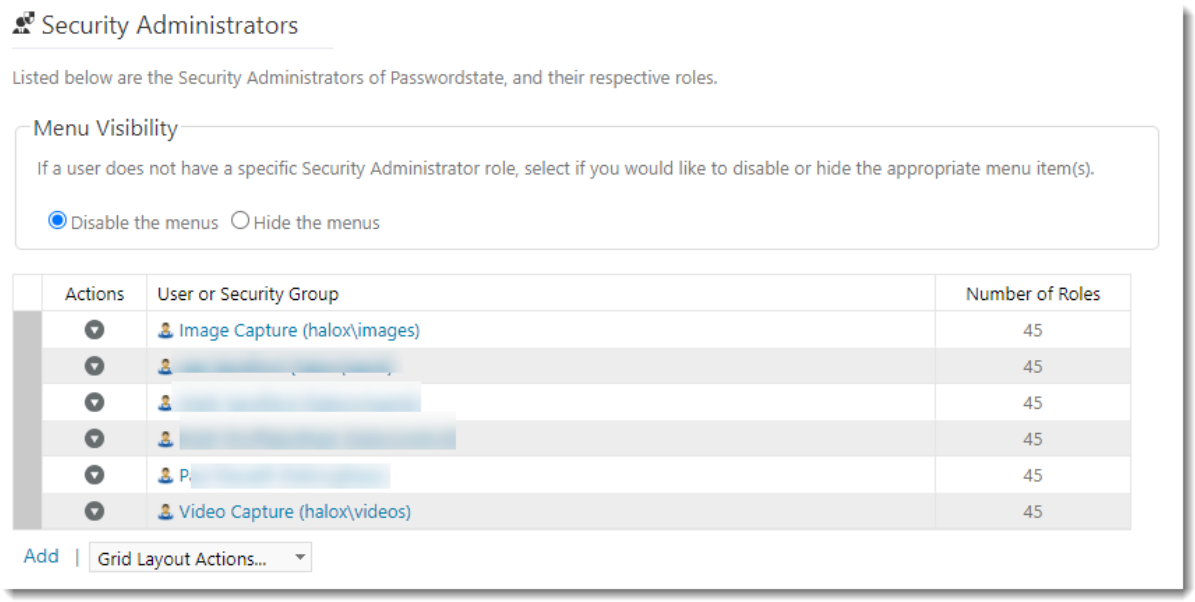


2.29 Security Administrators

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.



2.30 Security Groups

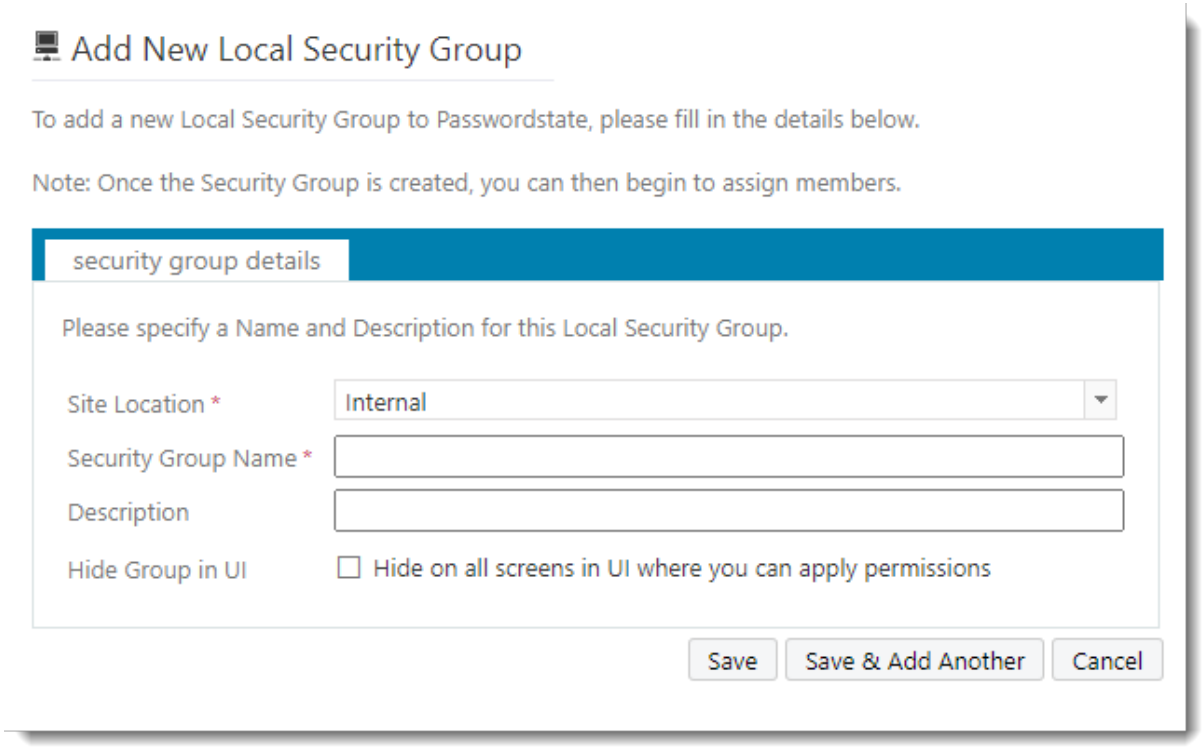
Security Groups allows you to manage either local security groups created within Passwordstate, or Active Directory security groups. These groups can then be used for applying permissions to Password Lists, or to give/deny access to various features.

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.

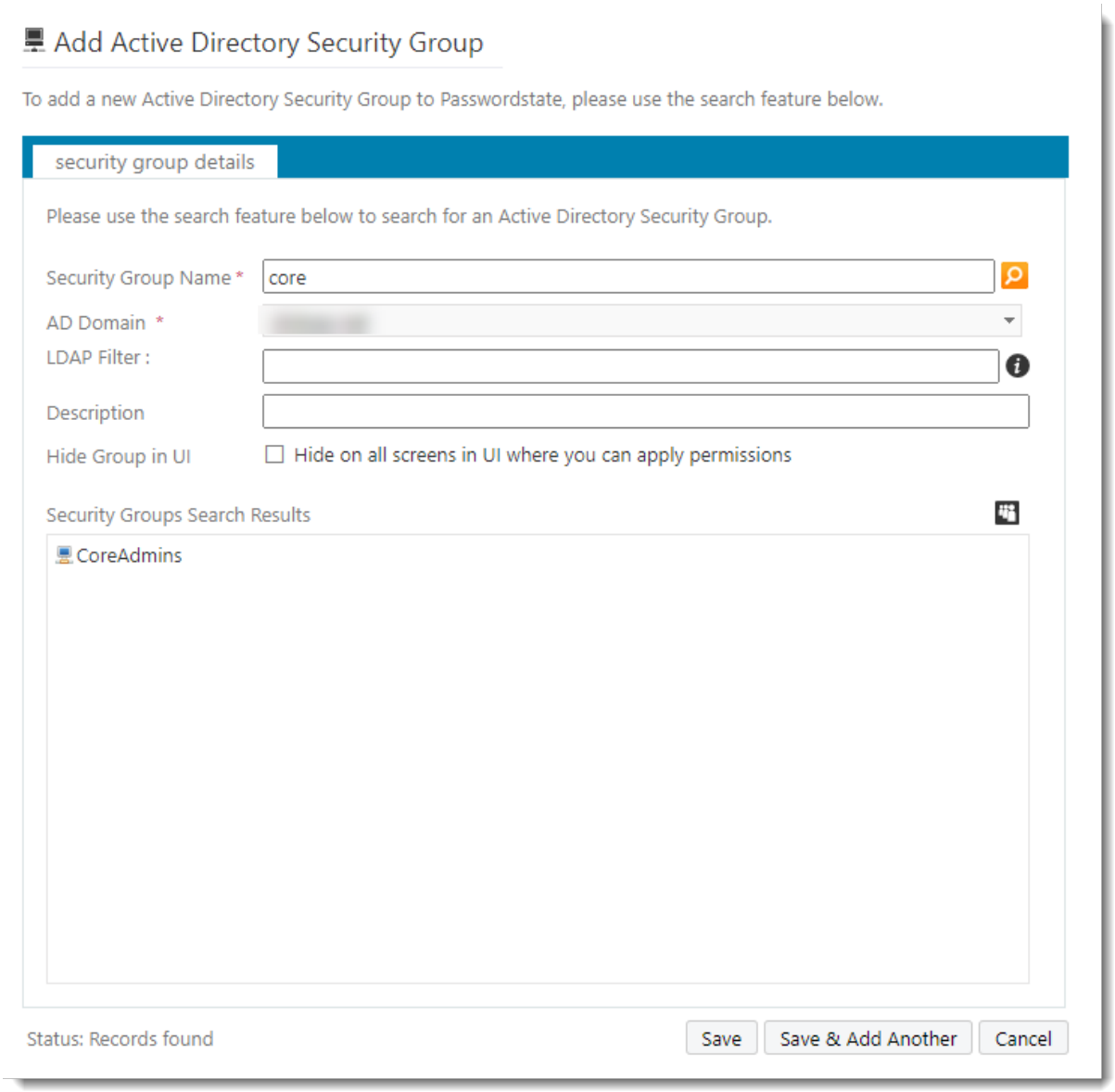
Note: Once you have added the local security group, you can assign user account membership by selecting the 'Manage Members' menu item from the appropriate Actions menu



Add 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 User Accounts screen), there is on option on the screen Administration -> System Settings -> Active Directory Options Tab which allows you to also automatically add these user accounts.
Note 2: Cross domain membership in Security Groups is not supported



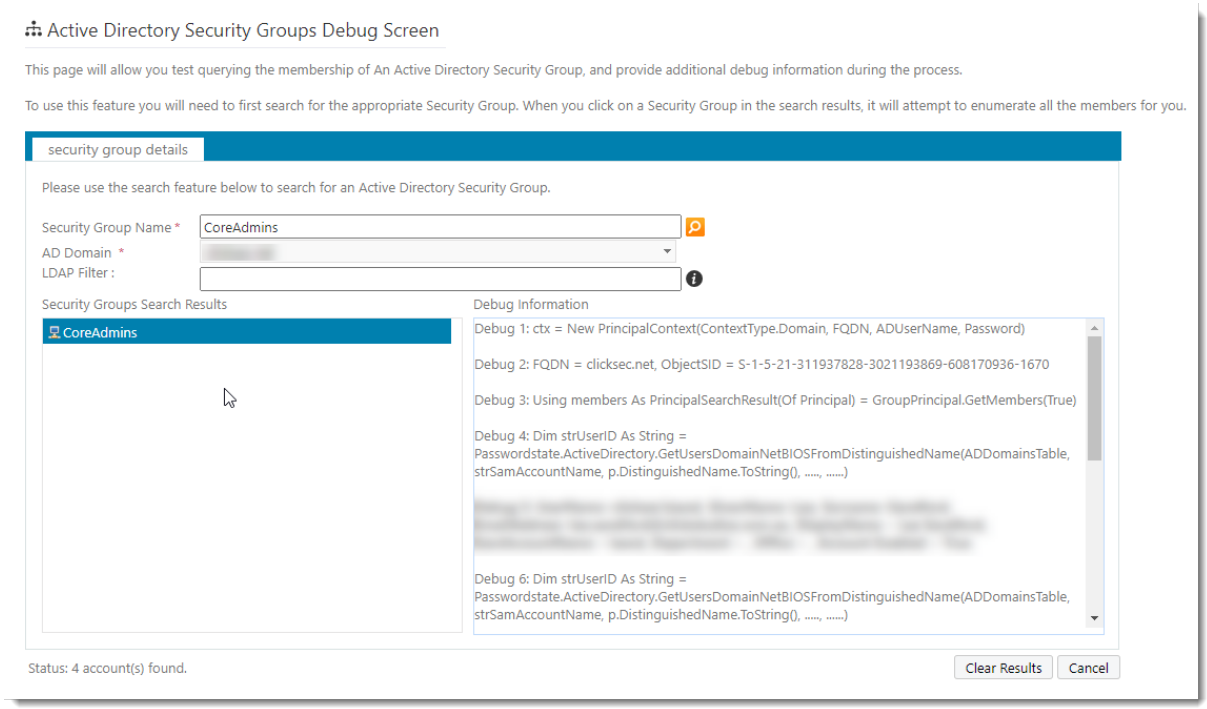
Nested Security Groups

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.

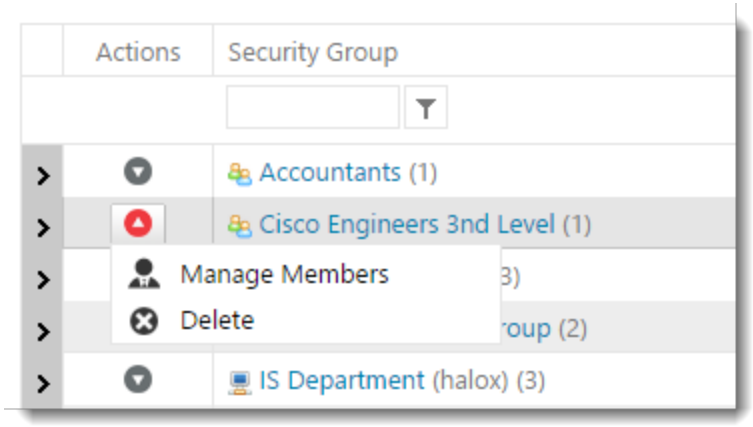


Local Security Group Actions Menu

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

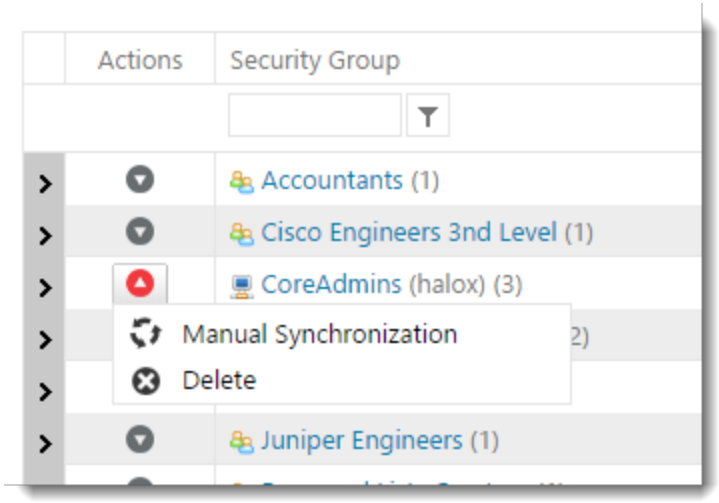
Note: If the Security Group has been used to apply permissions anywhere within Passwordstate, removing members from the security group, or deleting the Security Group itself, will remove one or more user's access



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:
  - 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 - > System Settings -> Active Directory Options Tab
  - 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



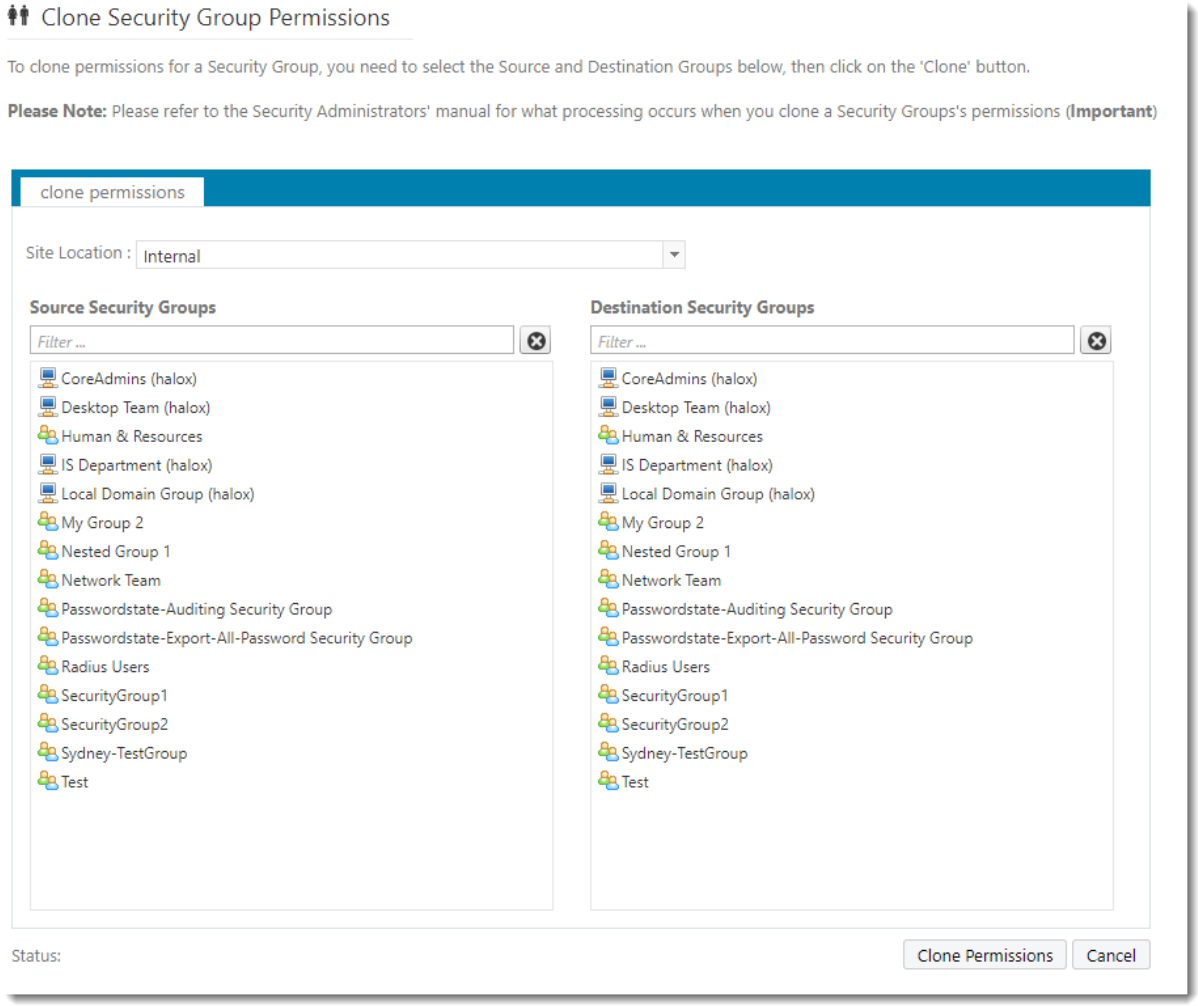
Clone Security Group Permissions

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.

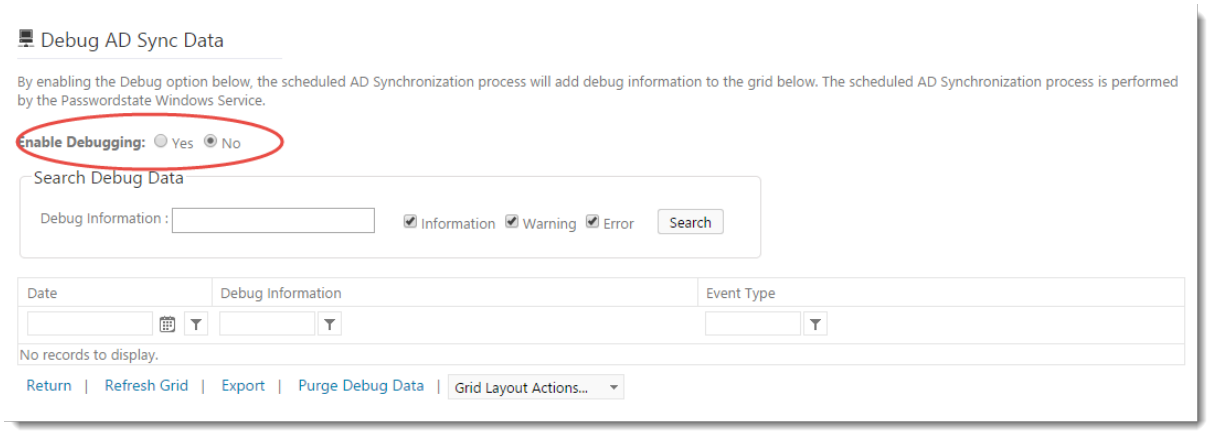
During the cloning process, the following types of permissions will be cloned:

- 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



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.



2.31 System Settings

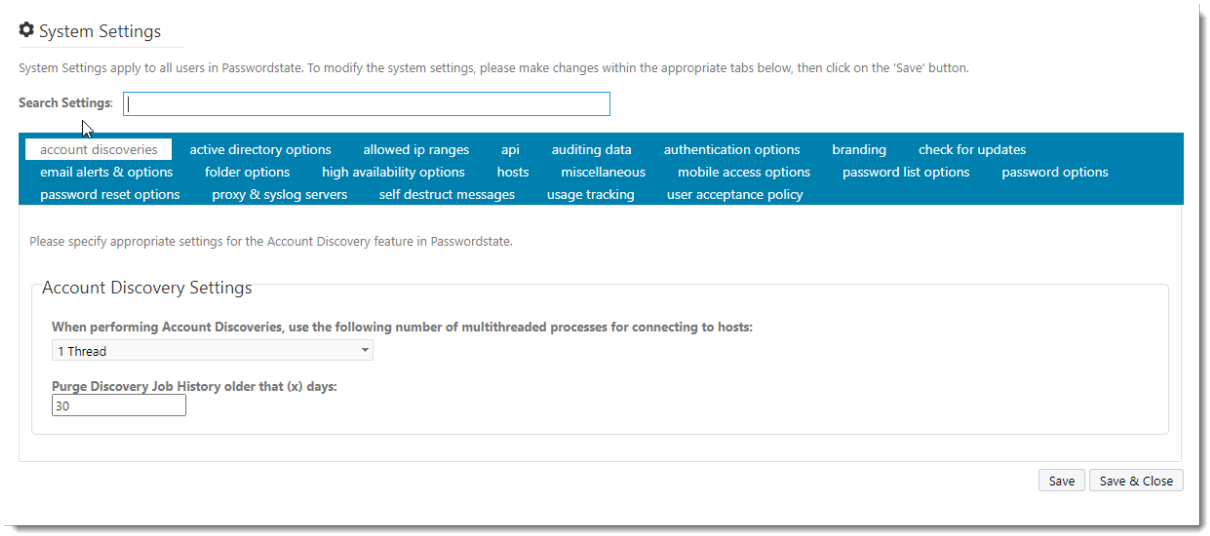
System Settings are used to specify any number of system wide settings in Passwordstate, which can affect the majority of users within the system.

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
API Tab	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
Check for Updates Tab	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
Miscellaneous Tab	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

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.



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 Security Groups screen, it's possible there will be user accounts in the Active Directory security group which have not yet been added to the User Accounts 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 License Information 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

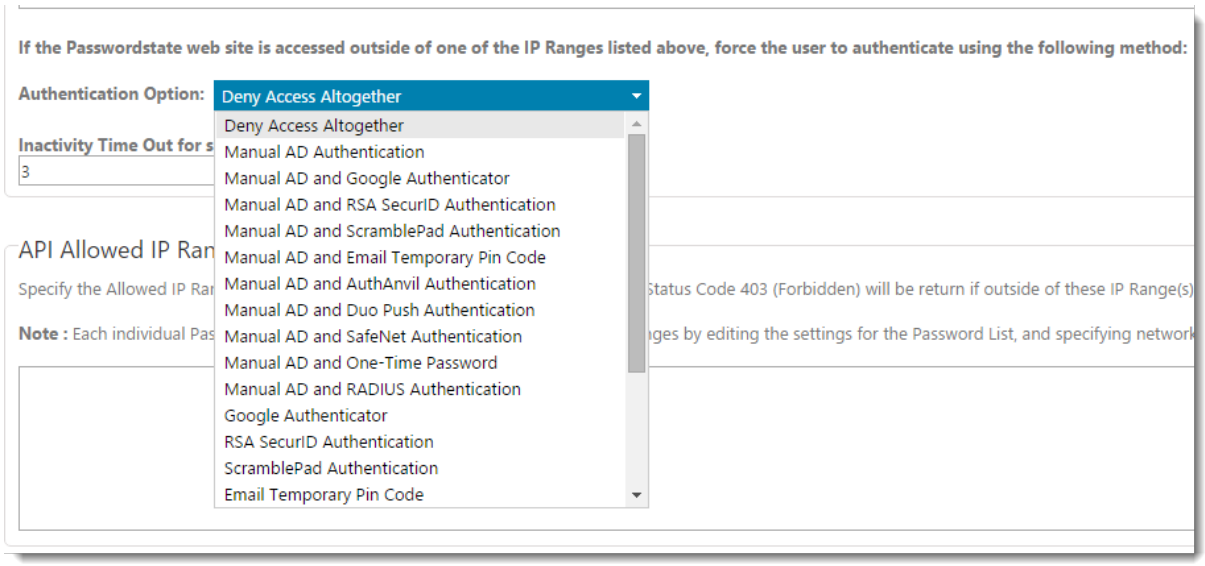
You can set the Allowed IP Ranges separately for each of the 3 features (web site, API and Emergency Access Login), and the features below are also possible for further restricting access to the Passwordstate web site.

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.



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

The default Inactivity Timeout setting can be found on the Miscellaneous Tab. 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

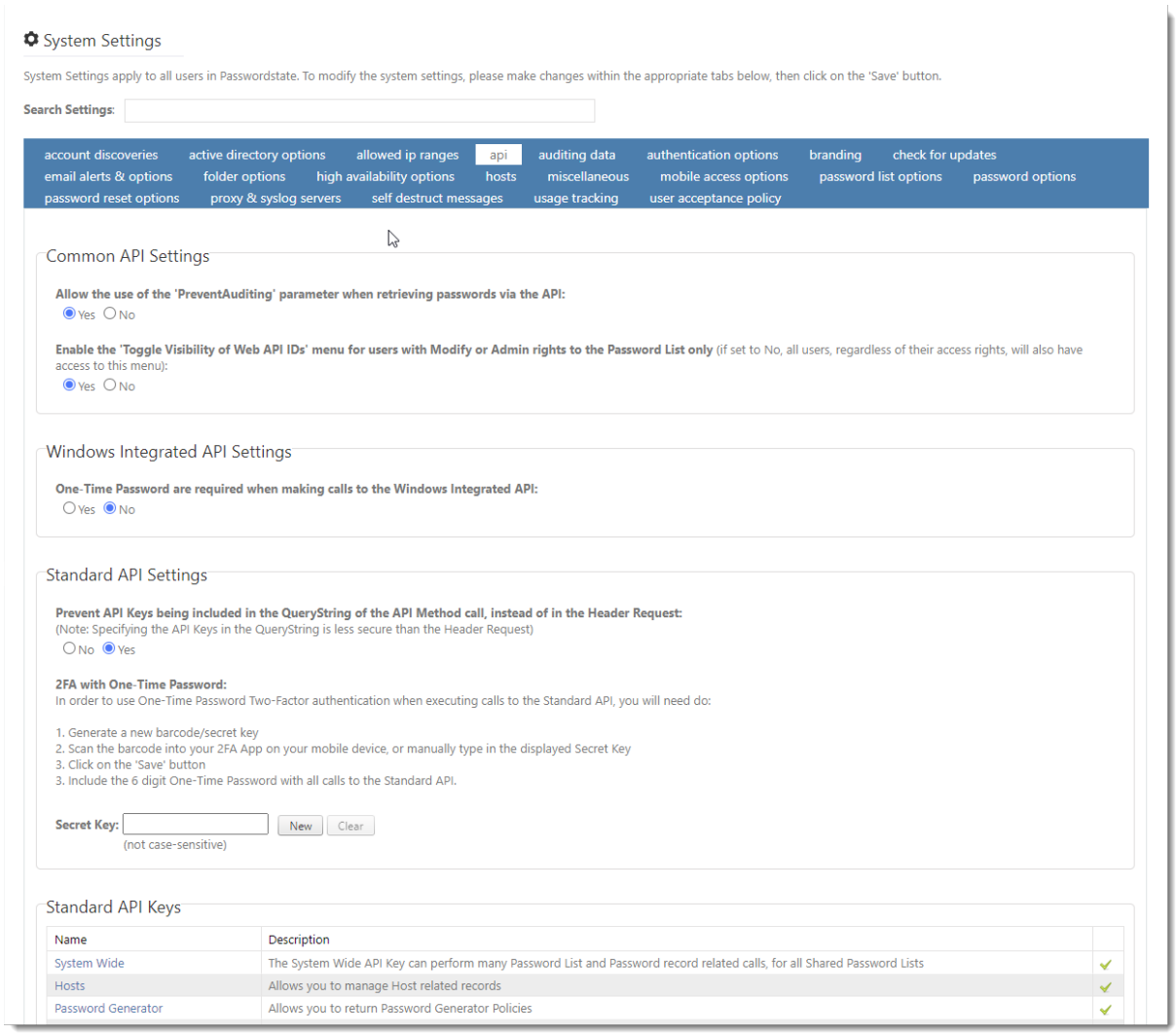
There are two types of APIs available in Passwordstate:

- 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:

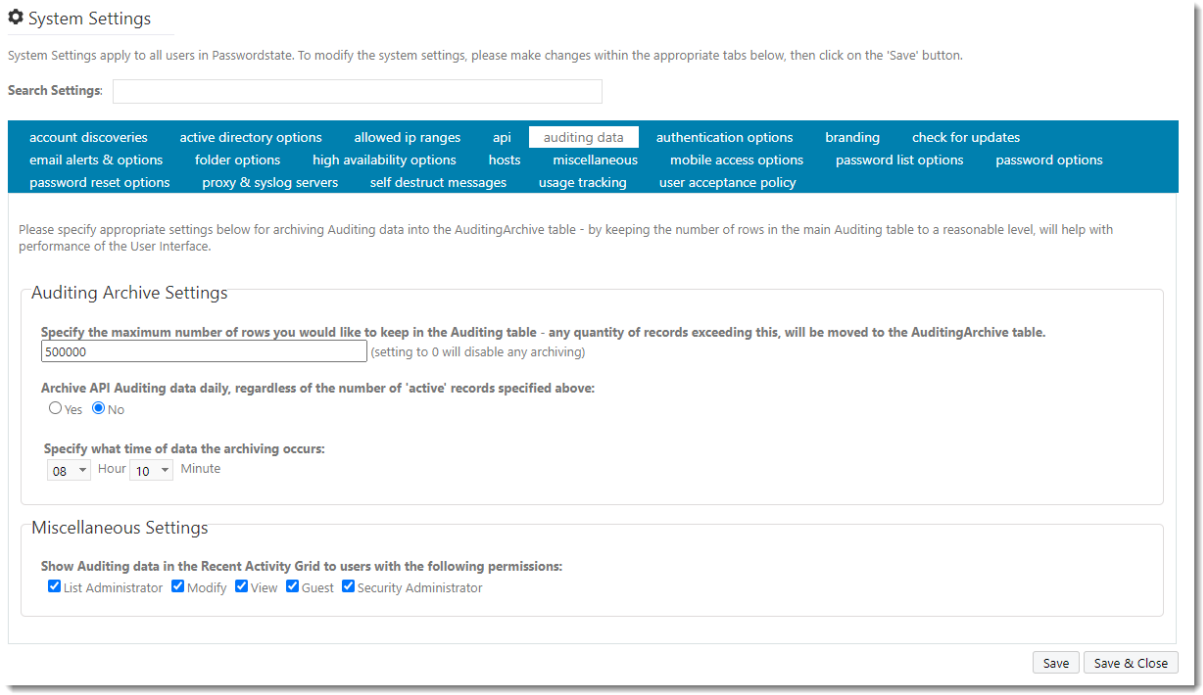
- Create various API Keys for the Standard API
- Whether API Keys are allowed to be used in QueryString URLs
- Whether or not the 'PreventAuditing' parameter on certain API calls is allowed to be used or not
- Which users are allowed to access the 'Toggle Visibility of Web API IDs' menu option on each 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 Feature Access screen
- If you want to be able to use Two-Factor Authentication with your API(s).

- On the screen Authorized Web Servers 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 Feature Access screen



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.



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: User Account Policies

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 Emergency Access account to gain access to the system and revert out any change.

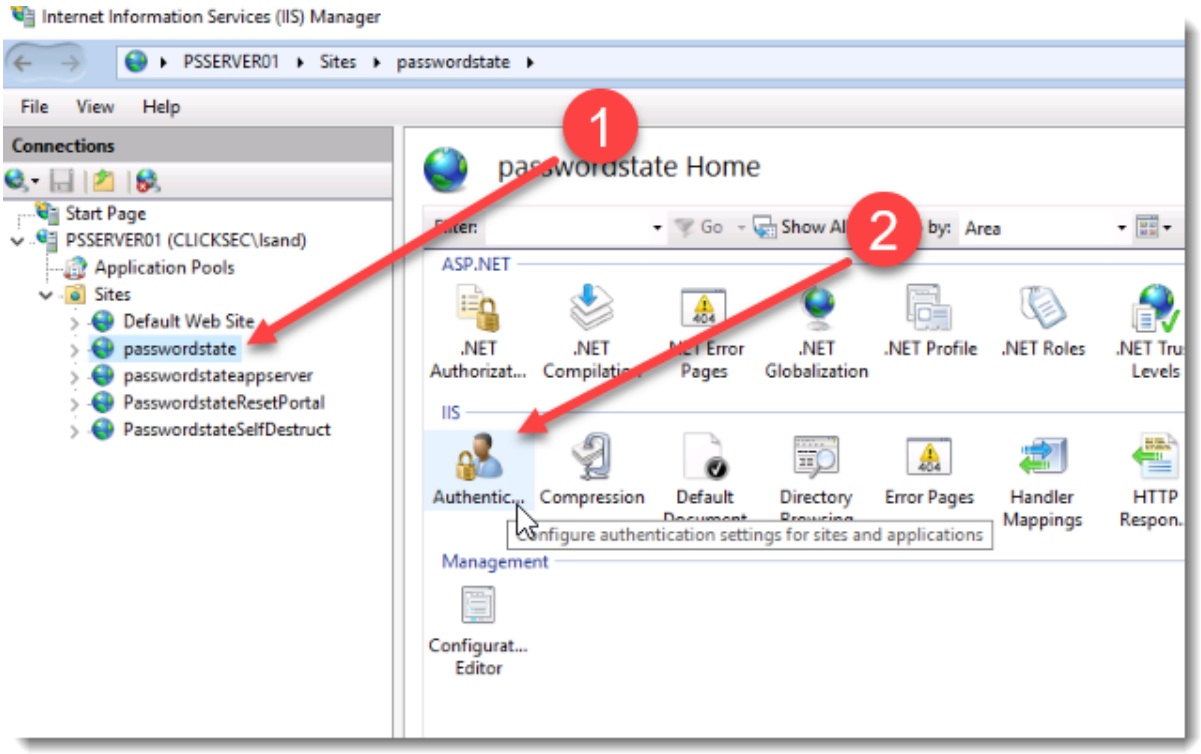
Note 3: If using Active Directory accounts for authentication, users can also login using the userPrincipleName AD attribute for this account. If doing this, it is recommended to hide the Domain Drop down list on login screens, as this may confuse users. This setting can be found under the Authentication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

Authentication Option

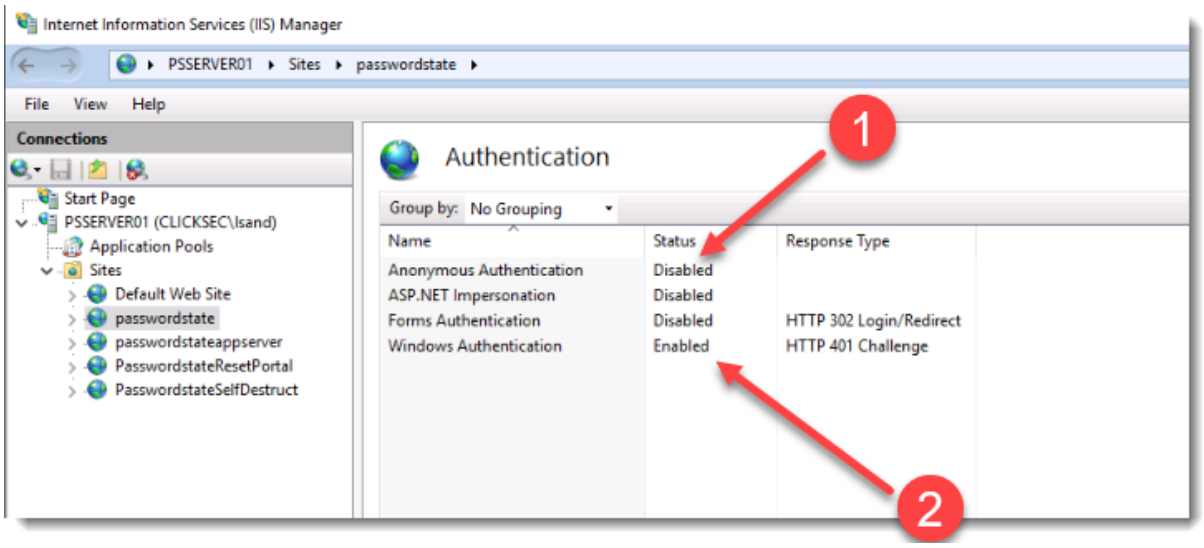
There are multiple different authentication options available for when your users first access the Passwordstate web site, and they are:

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**:



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 User Accounts 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 - Duo Auth API Configuration

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 time-based, 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
  - 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
  - AD Single Sign-On and Duo Authentication
  - AD Single Sign-On and One-Time Password
  - 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

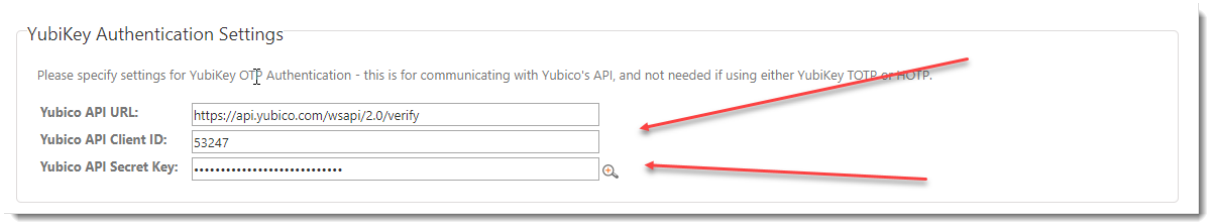
If you are wanting to use the cloud based Yubico OTP authentication option, then this requires your to obtain a Client ID and and Secret Key to use. You can get these from the following page on Yubico's web site, and you must use your YubiKey to do this - https://upgrade.yubico.com/getapikey/

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."



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 - SAML2 Provider Examples

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 Duo Auth API Configuration

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.

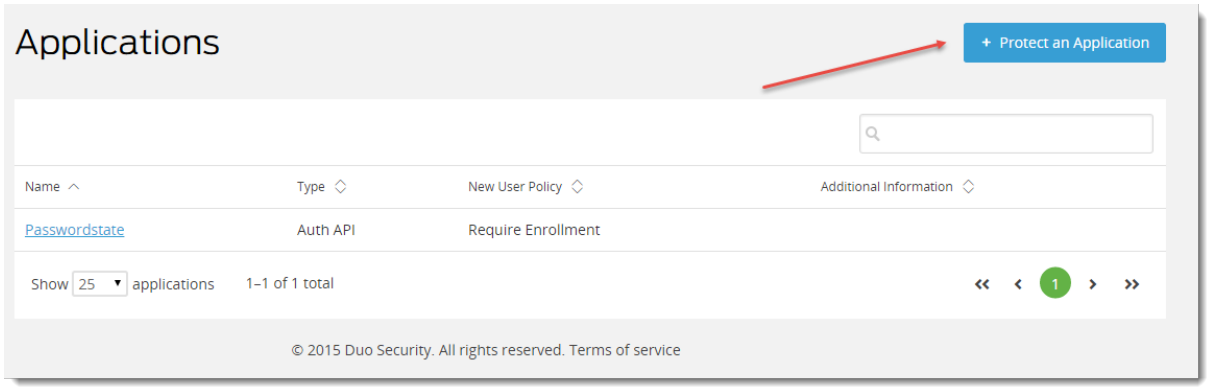
Minimum ScramblePad Pin Length

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

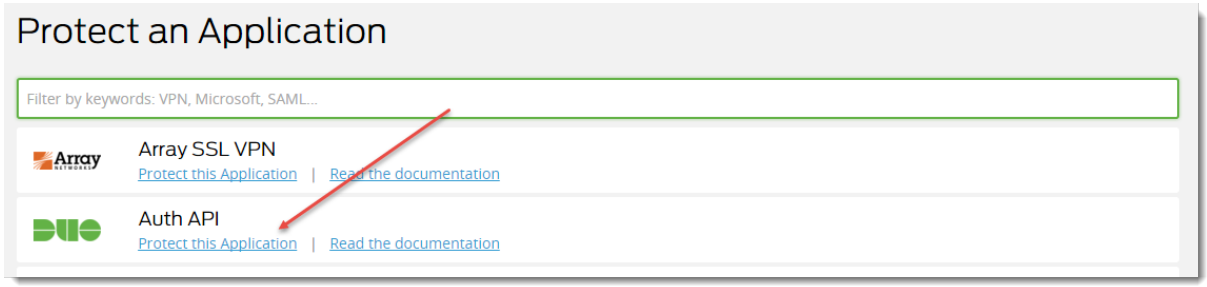
2.31.6.1 Duo Auth API Configuration

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.

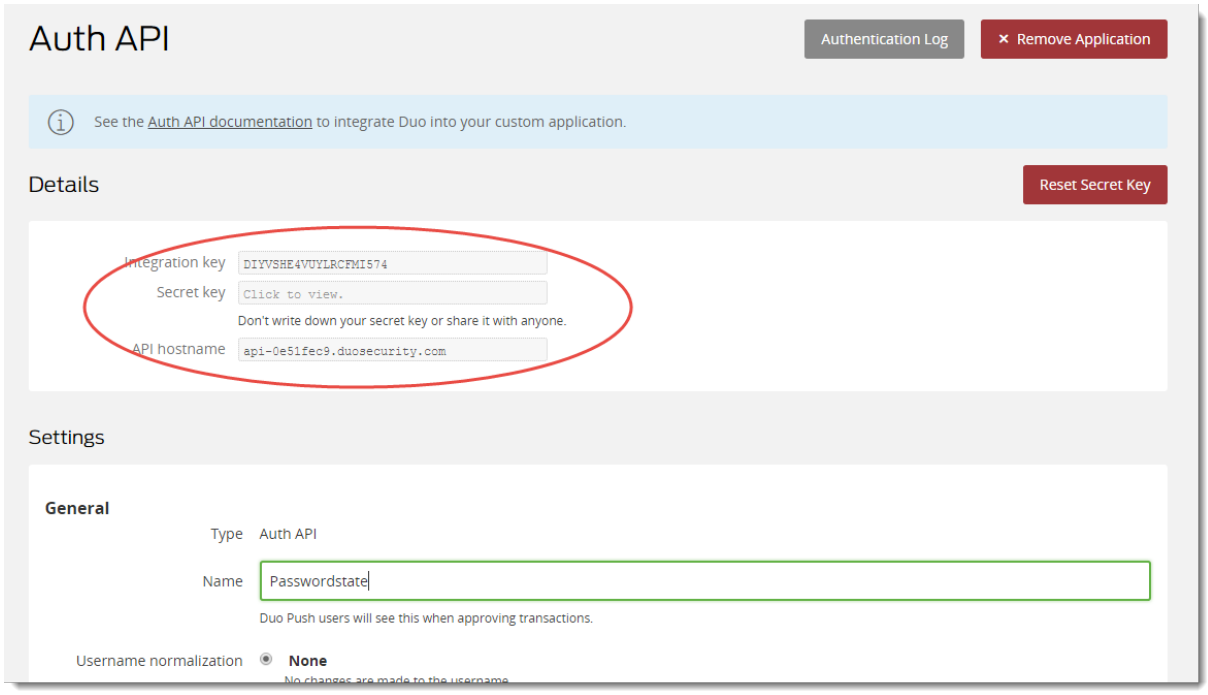
- First, login to your Duo Portal, and click on the 'Applications' menu
- Click on 'Protect an Application'



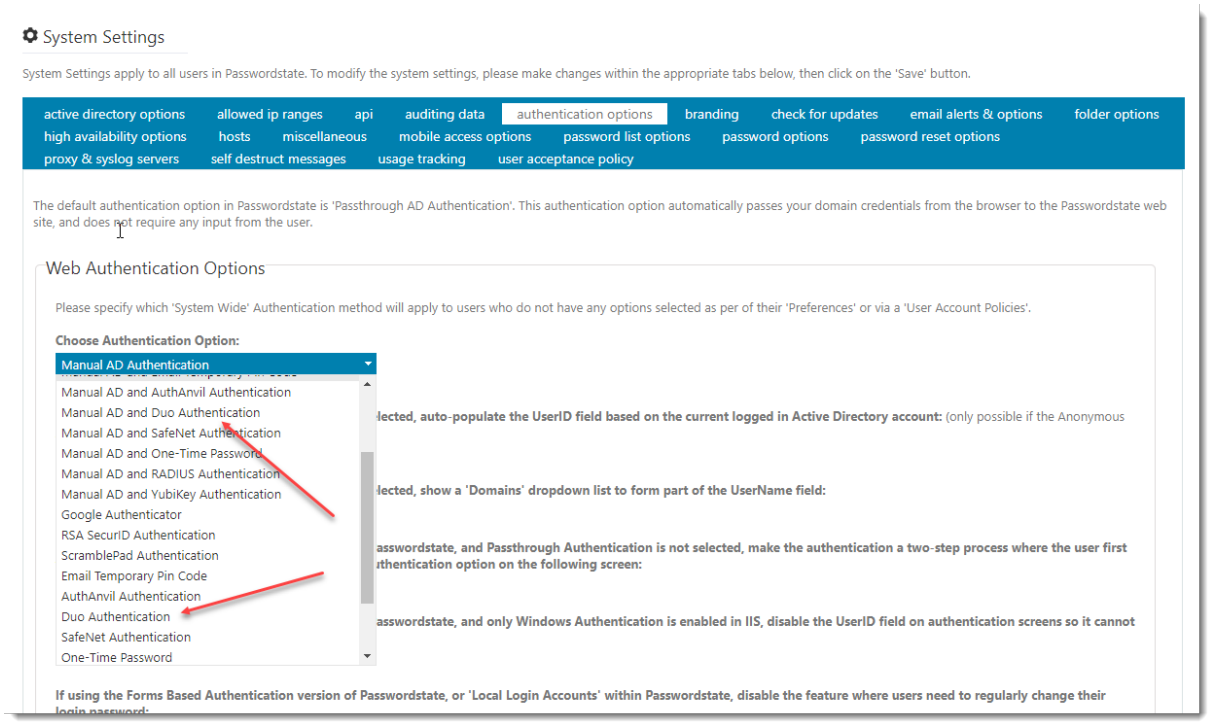
- Chose the 'Auth API' Application

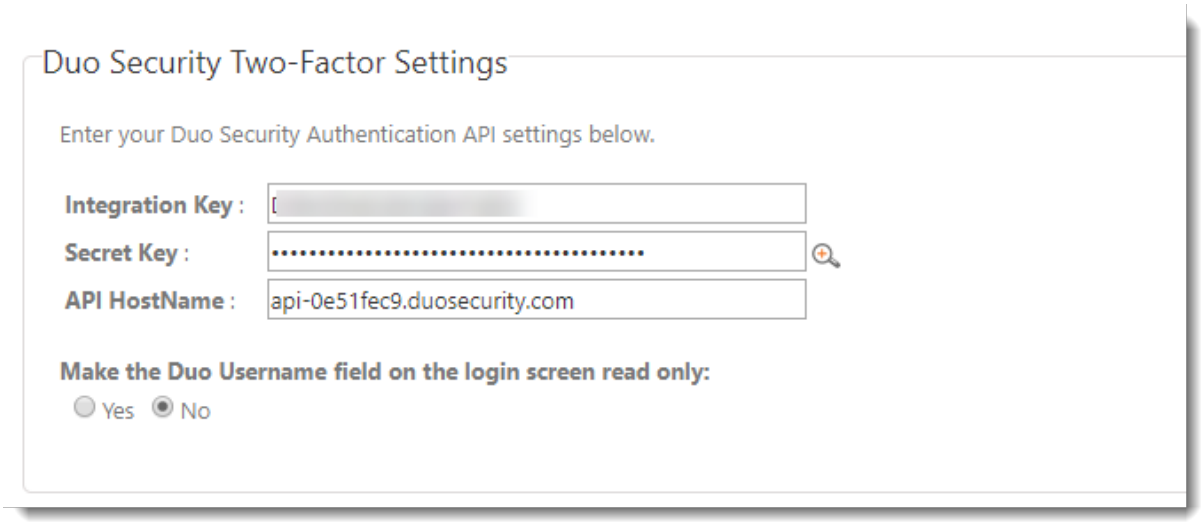


- Create the Secret Key and Name the Auth API as appropriate



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





- 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 - https://<YourURL>/logins/saml/default.aspx
- Recipient URL - https://<YourURL>/logins/saml/default.aspx
- Destination URL - https://<YourURL>/logins/saml/default.aspx
- Audience Restriction - https://<YourURL> (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 - 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 - https://<YourURL>/logins/saml/default.aspx
- Audience - https://<YourURL> (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 - https://<YourURL>/logins/saml/default.aspx
- ACS (Consumer) URL Validator - ^https:\/\/YourURL\/logins\/saml\/default.aspx\/$
- ACS (Consumer) URL - https://<YourURL>/logins/saml/default.aspx

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 https://<YourURL>/logins/saml/default.aspx
- For the Relying party trust identifier, enter the URL of the passwordstate instance: https://<YourURL>
- 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”

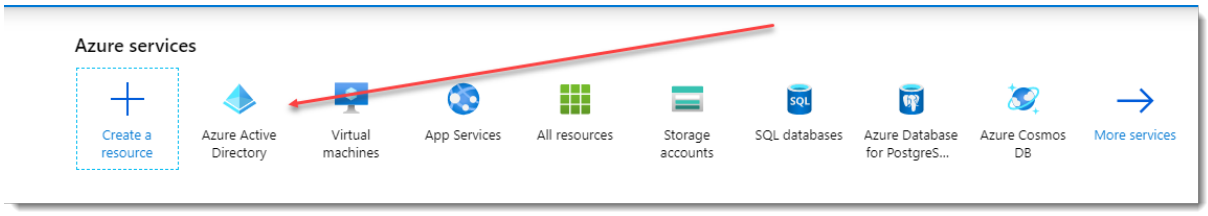
Passwordstate SAML2 Configuration for ADFS

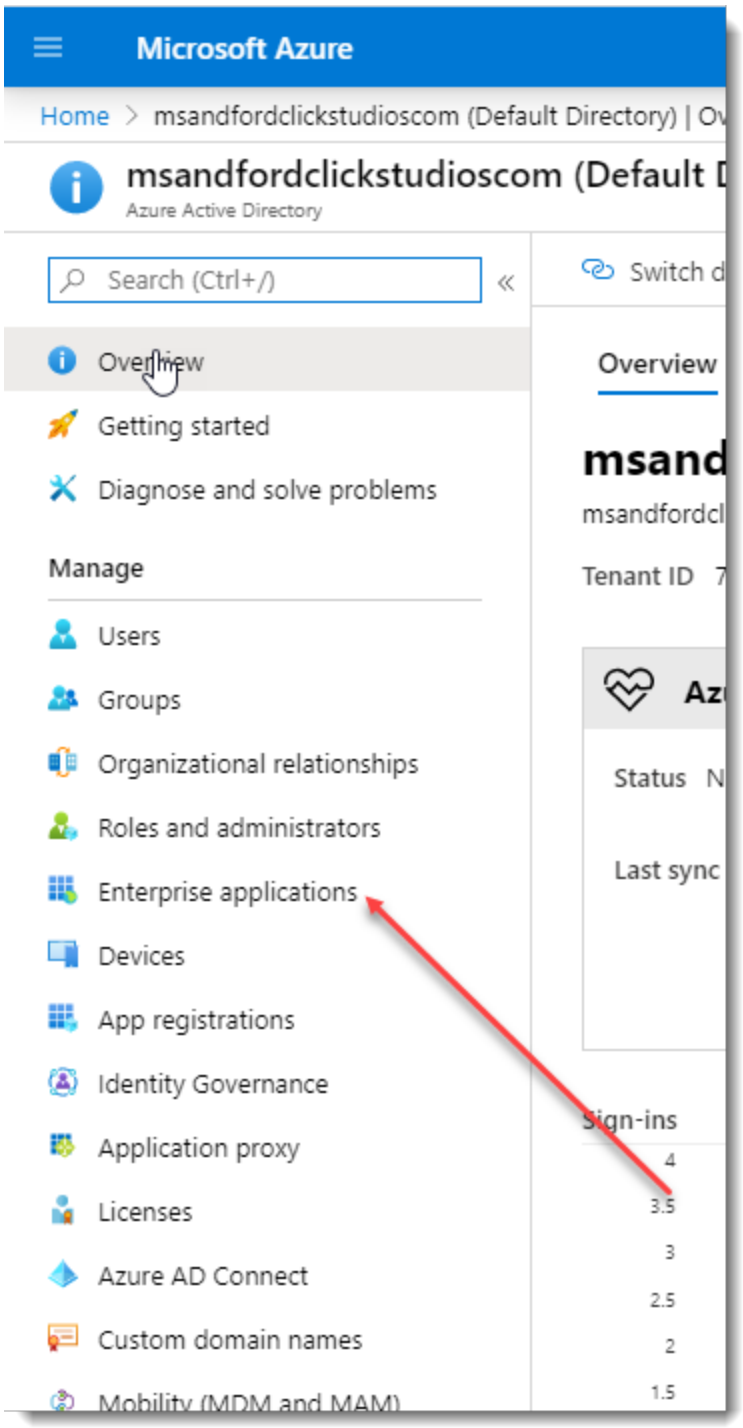
- Right click the “Token-signing” certificate in “Certificates” under “Service” in “AD FS Management”
- Select “View Certificate…”

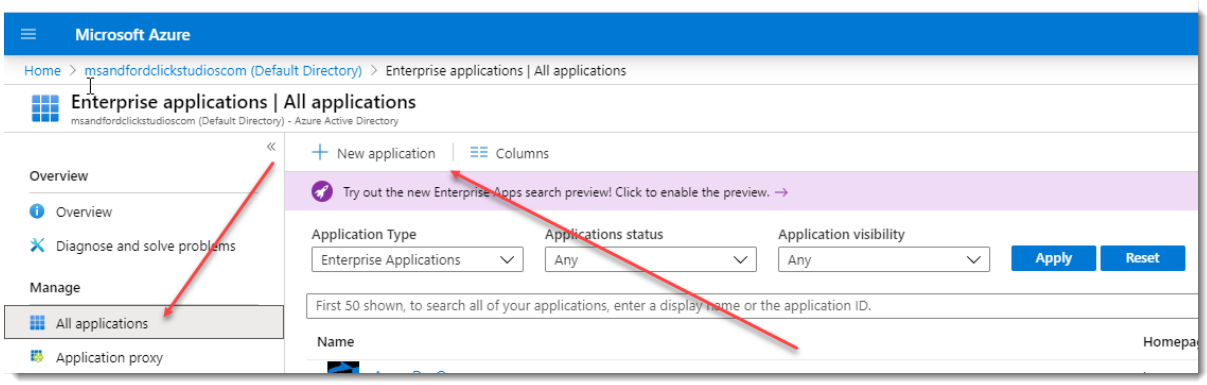
- Select the “Details” tab
- Select “Copy to File”
- Click “Next”
- Select “Base-64 encoded X.509 (.CER)“
- Click “Next”
- Select a file path to save the certificate
- Click “Next”
- Click “Finish”
- Click “OK”
- Open the .CER certificate file with Notepad or another text based editor.
- Copy all of 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=https://<YourURL>”
- Set “IDP Issuer URL” to “http://<YourADFSURL>/adfs/services/trust”

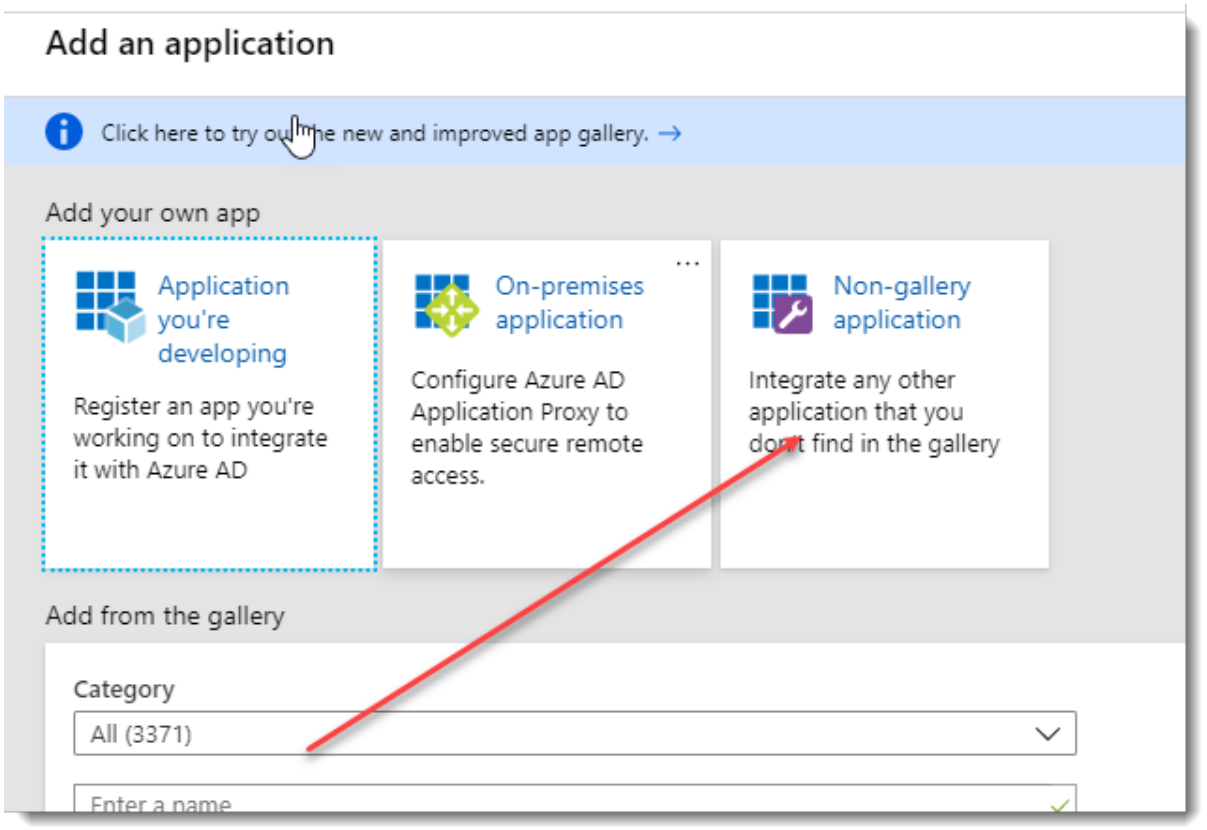
Azure Active Directory

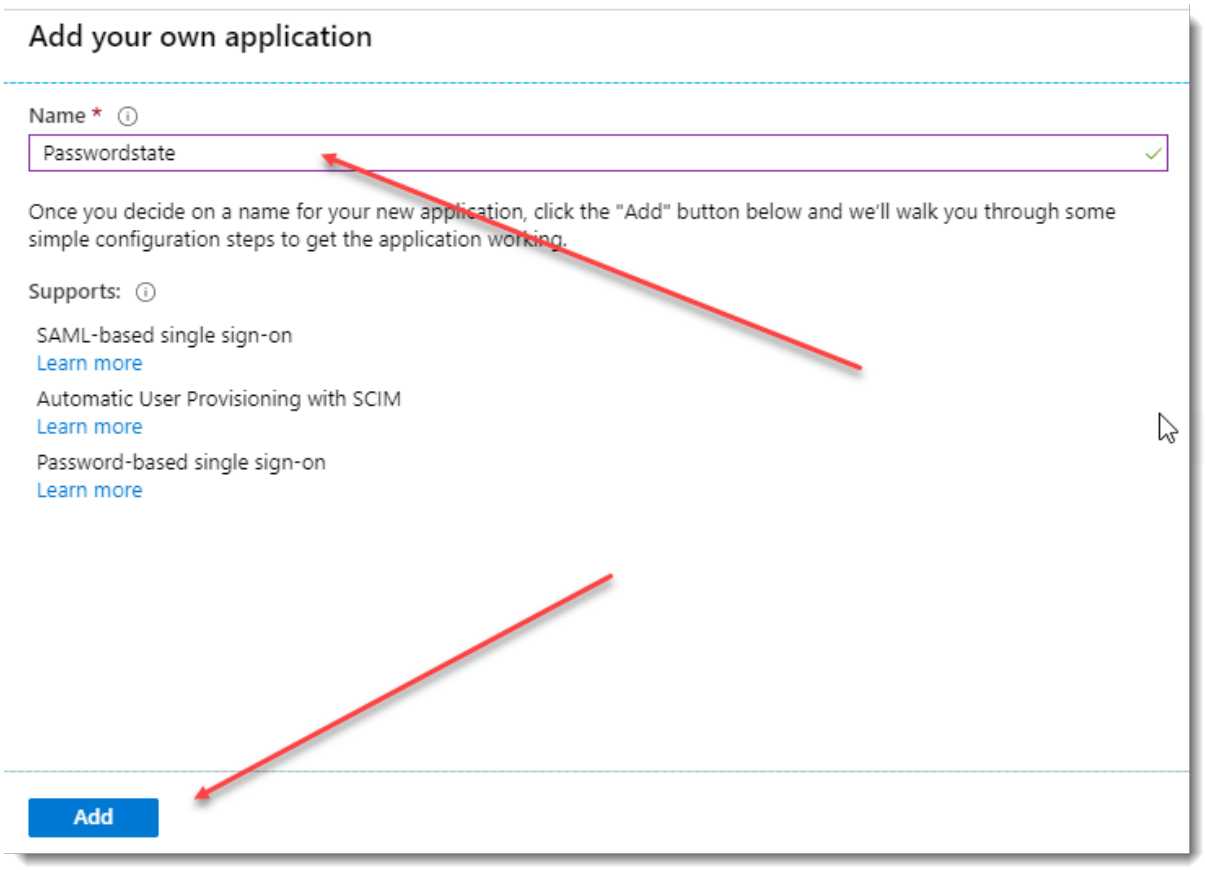
When logged into your Azure Dashboard, you need to create a new 'Non-Gallery Application' in the 'Enterprise Applications' area as per the screenshots below.

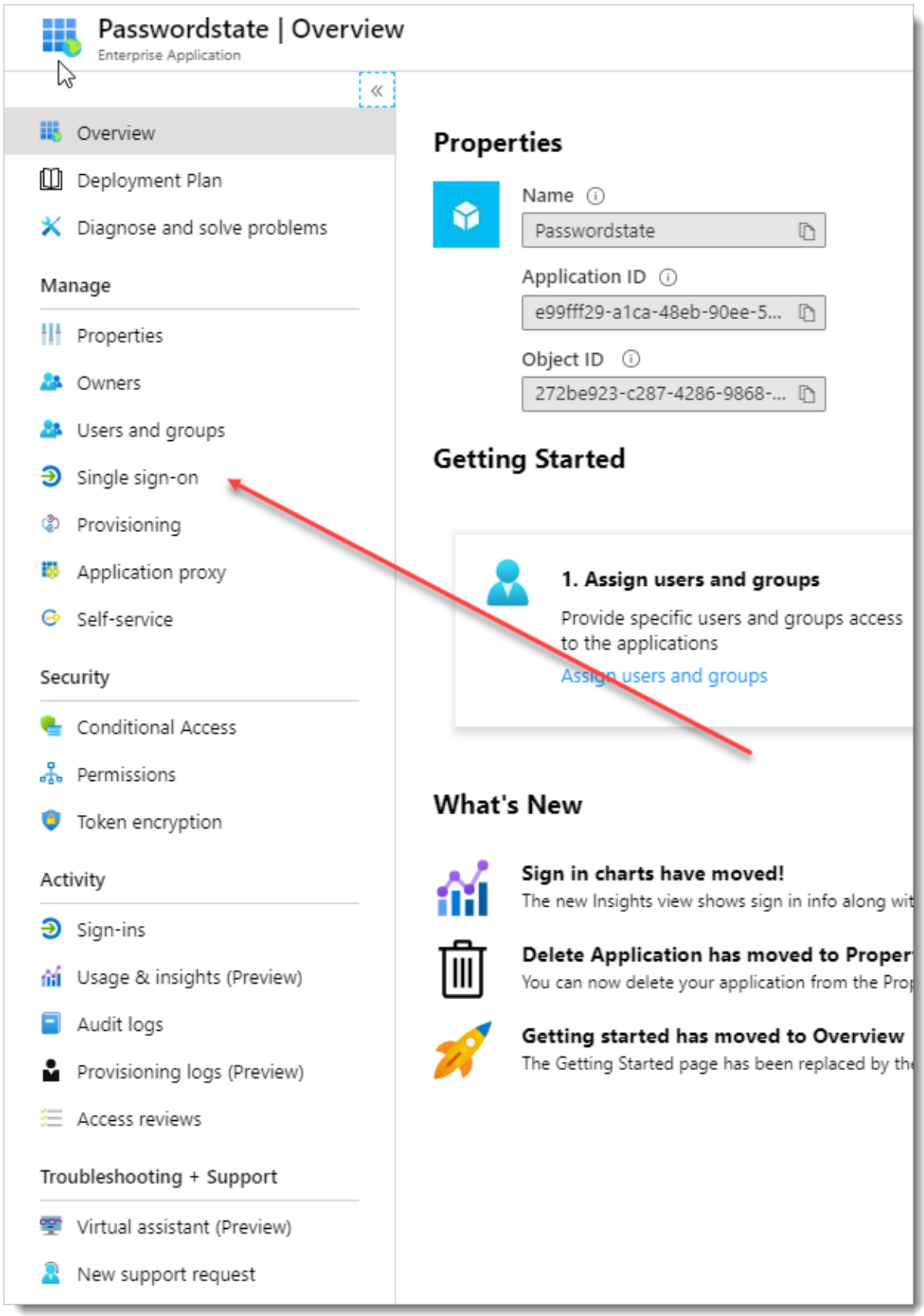


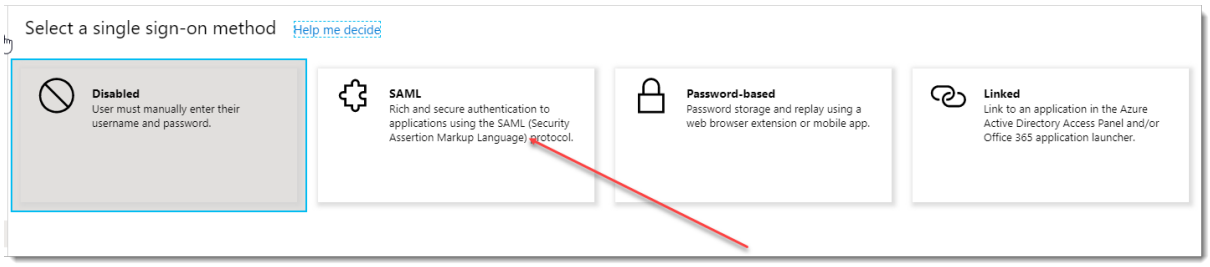












With the fields you see below, these map to certain fields within Passwordstate on the screen Administration -> System Settings -> Authentication Options tab -> Primary Site's SAML2 Authentication Settings. Below is a table which summarizes these mappings.

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"

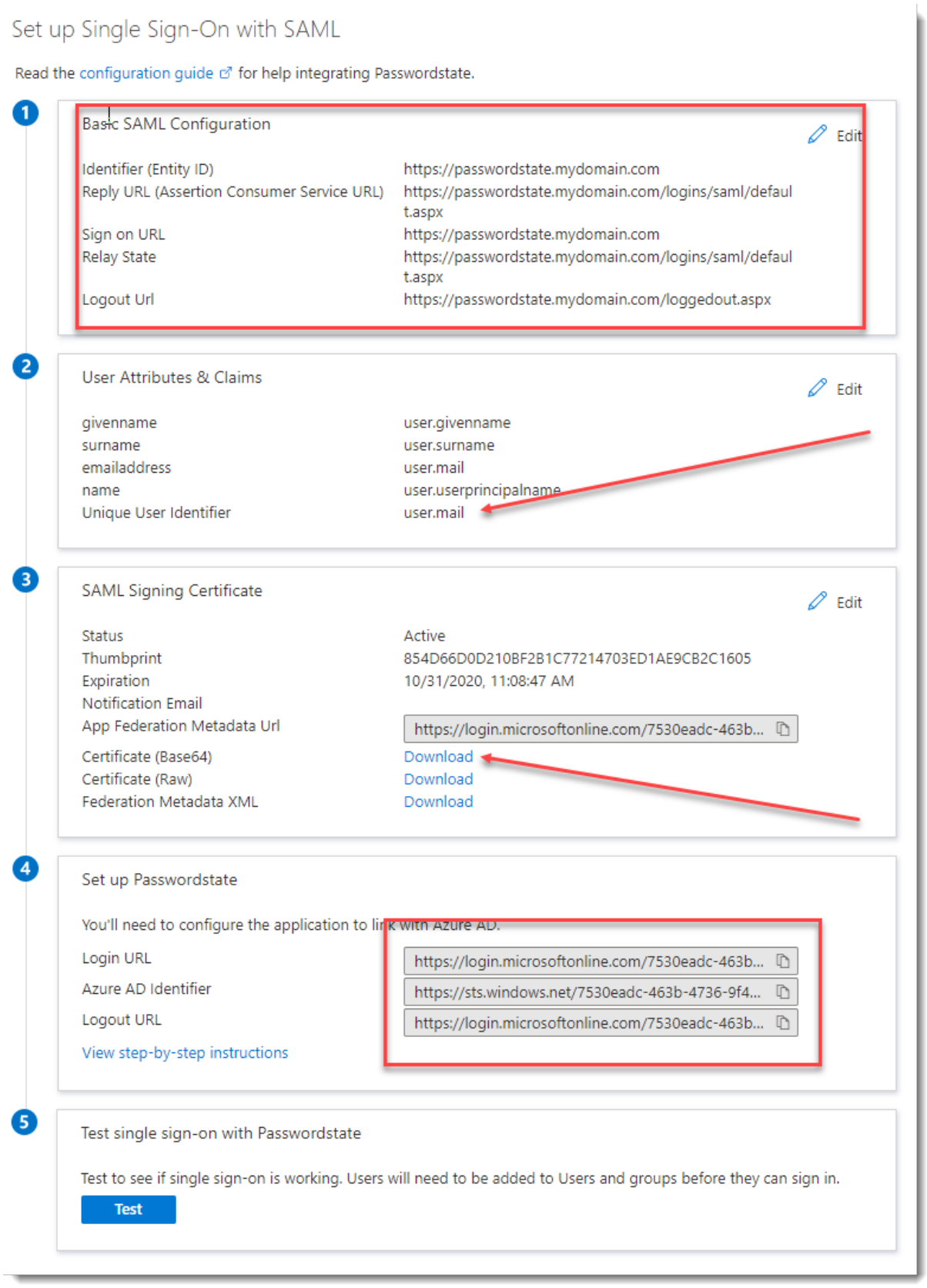
SAML Signing Certificate

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

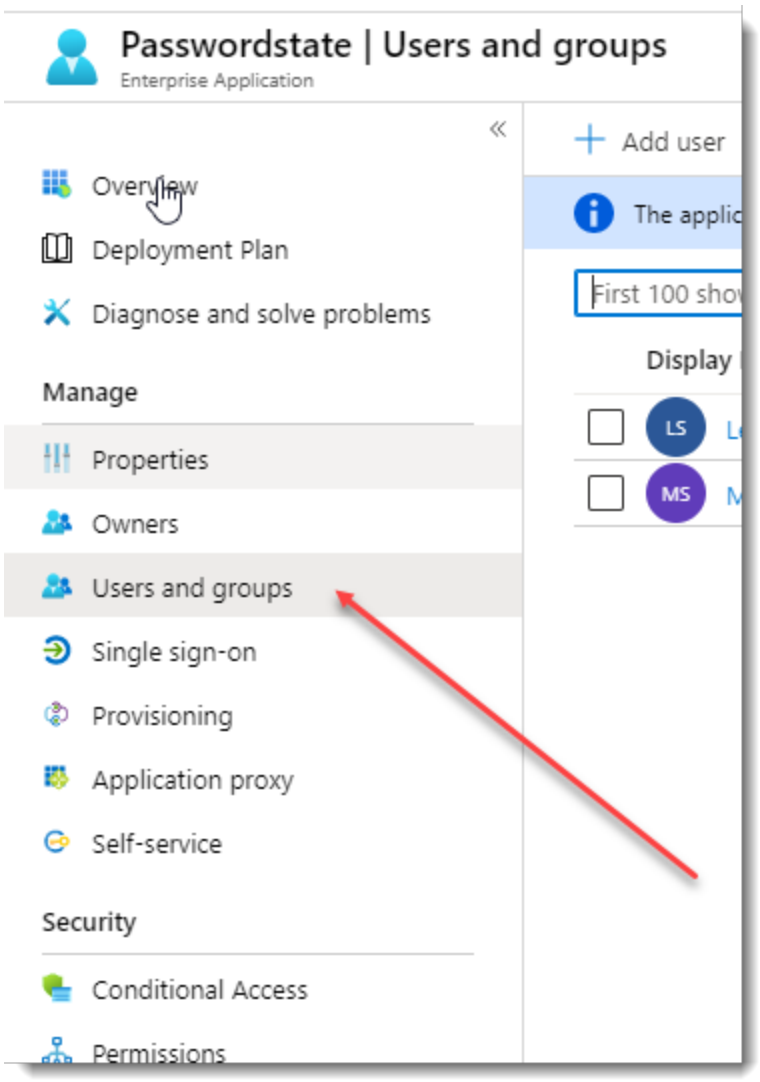
Set up Passwordstate

Azure AD Field	Passwordstate Field

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

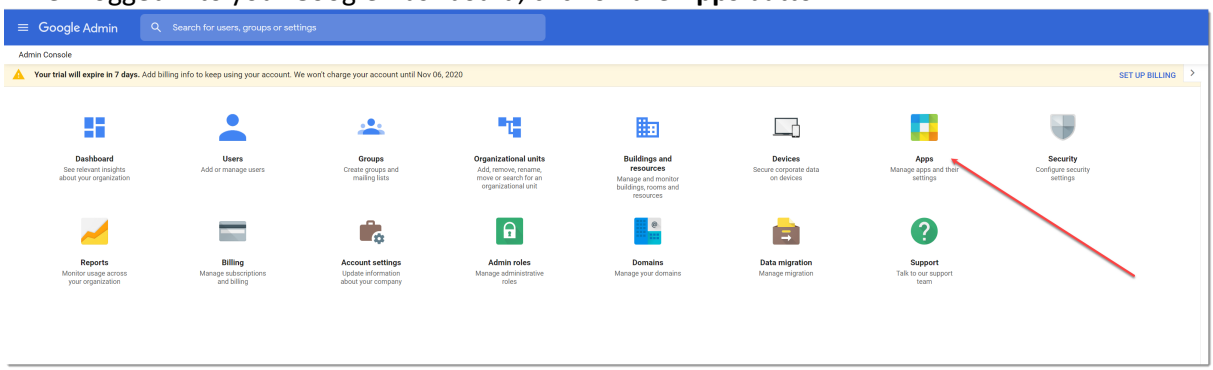


And finally in Azure, you need to grant users access to this 'Application'.

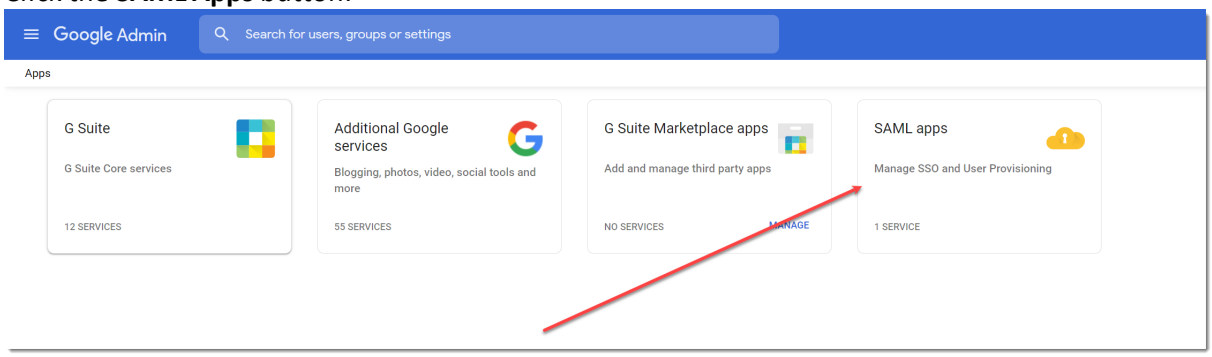


Google Workspace / GSuite

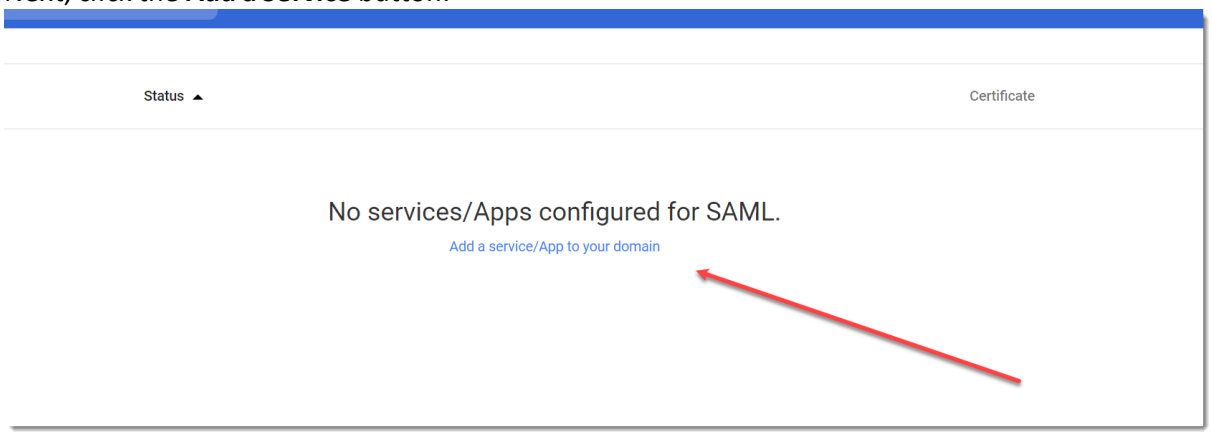
When logged into your Google Dashboard, click on the **Apps** button:



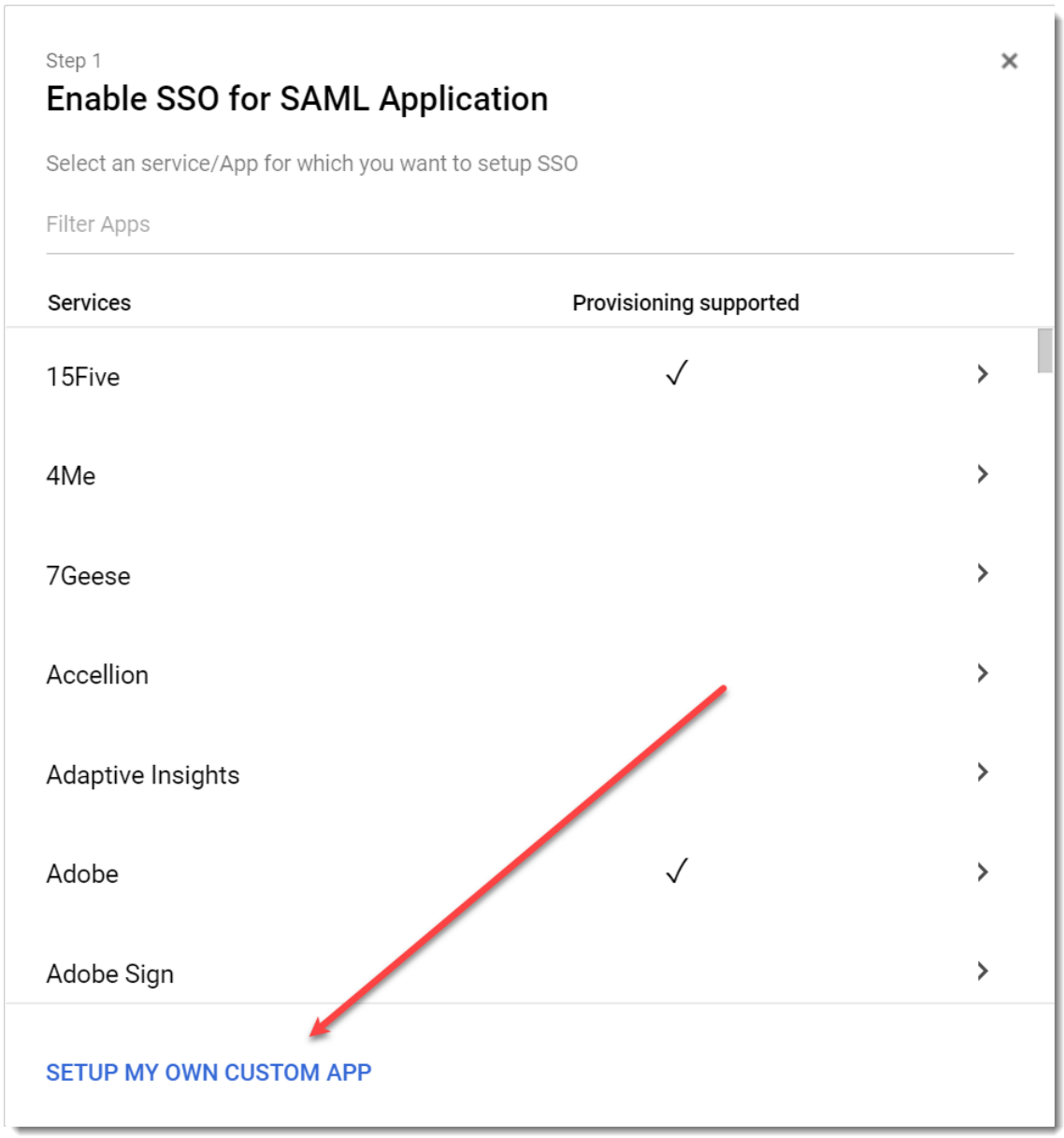
Click the **SAML Apps** button:



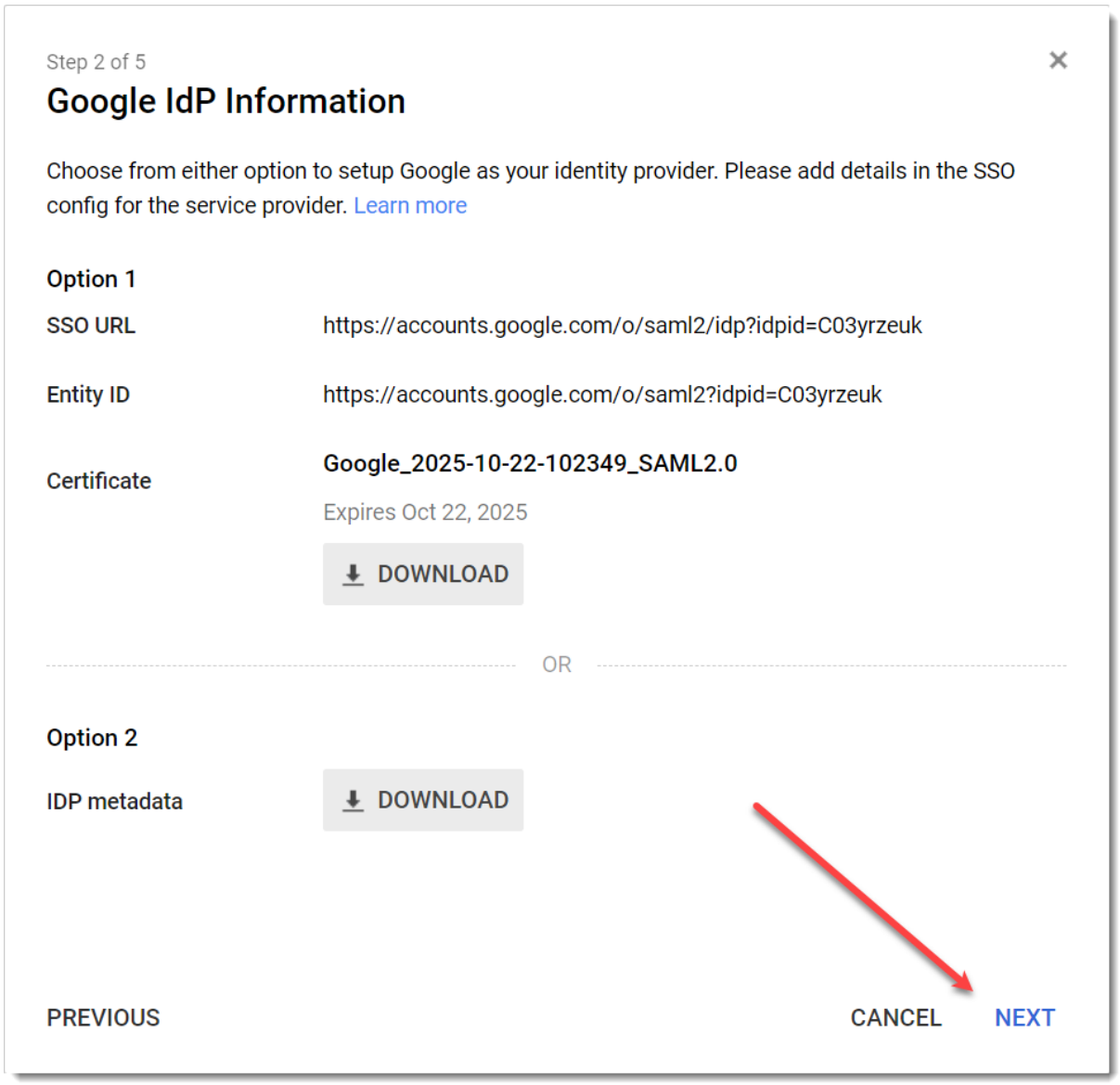
Next, click the **Add a Service** button:



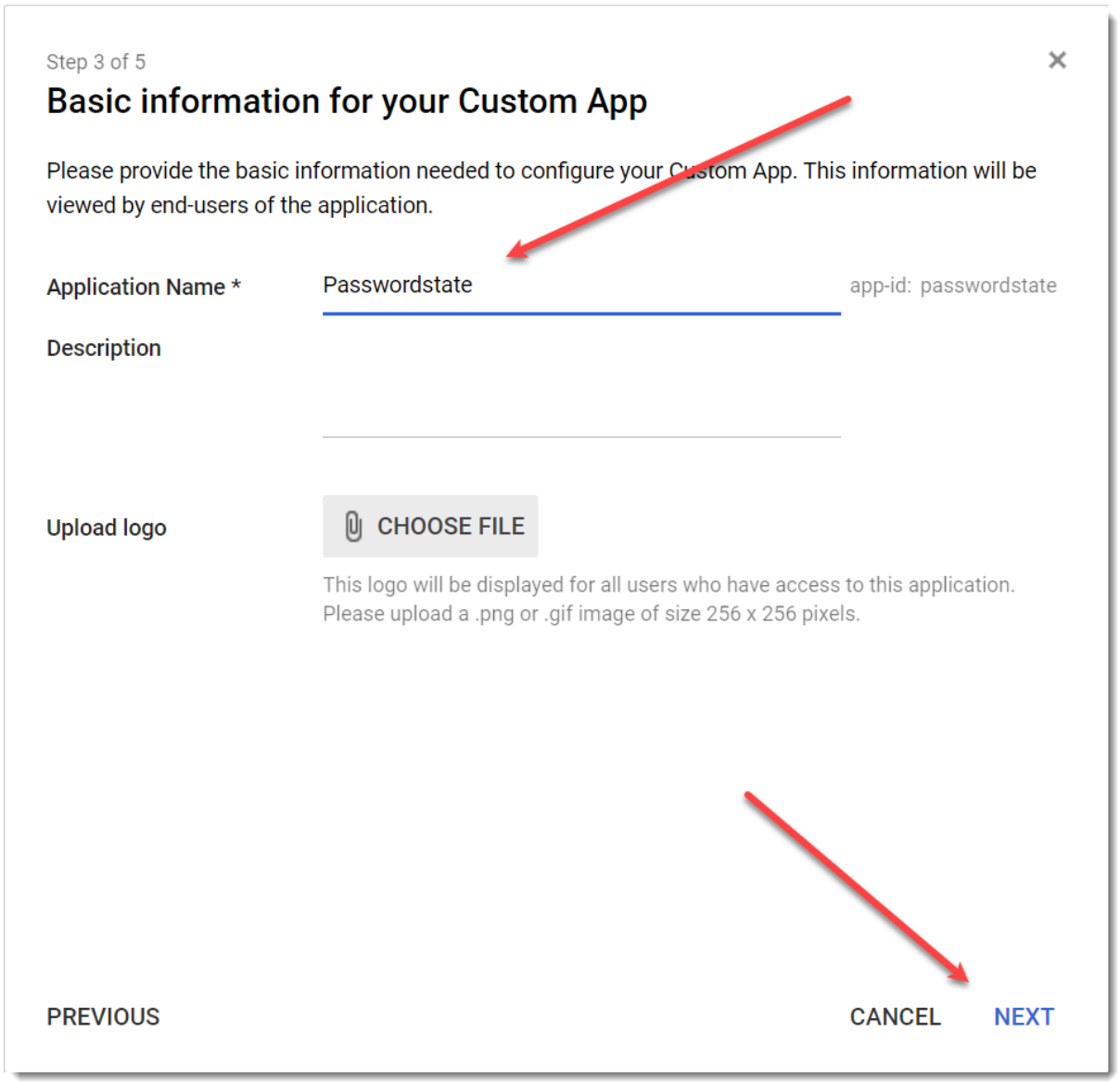
Set up your own **Custom App**:



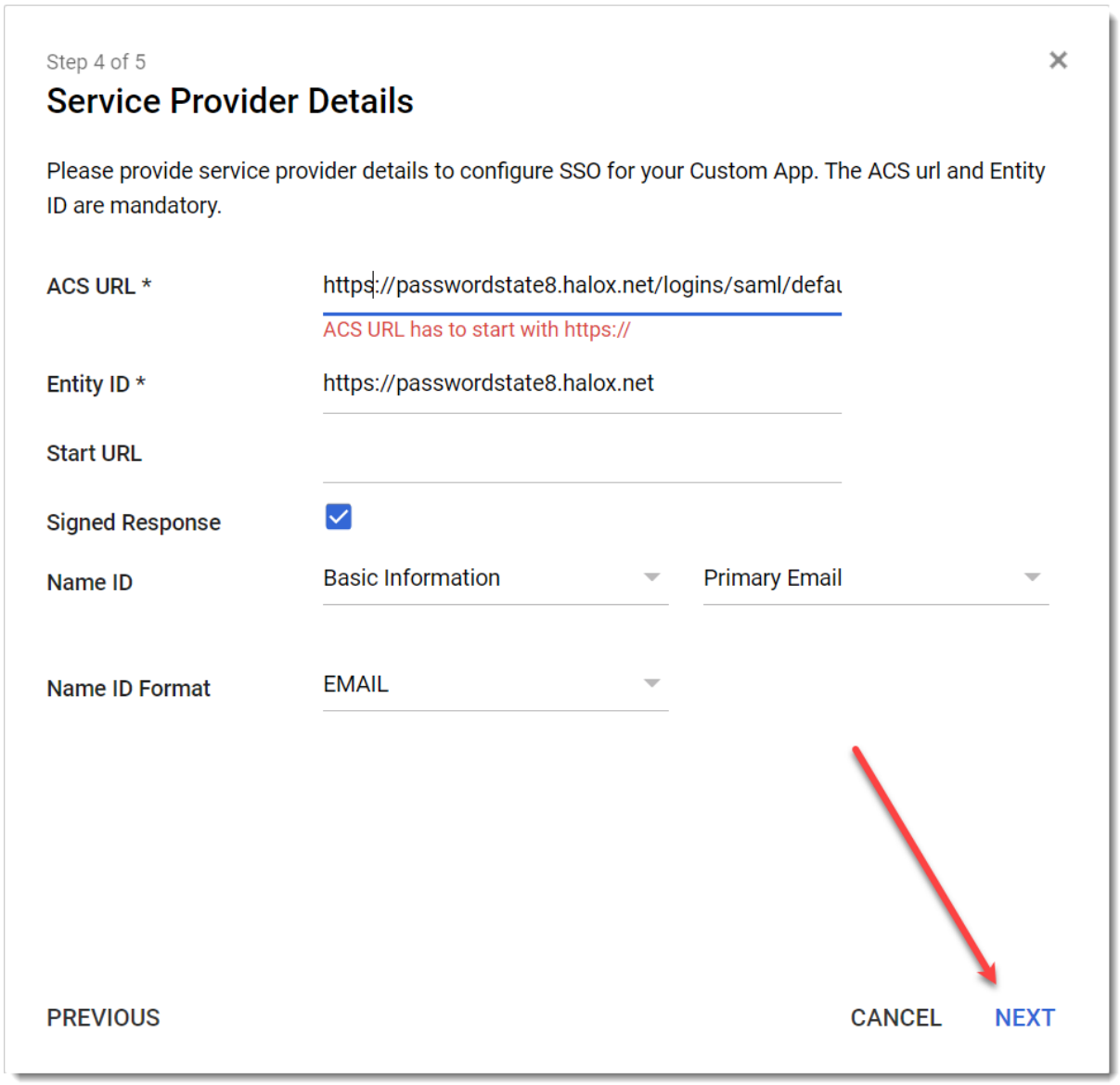
Click **Next**:



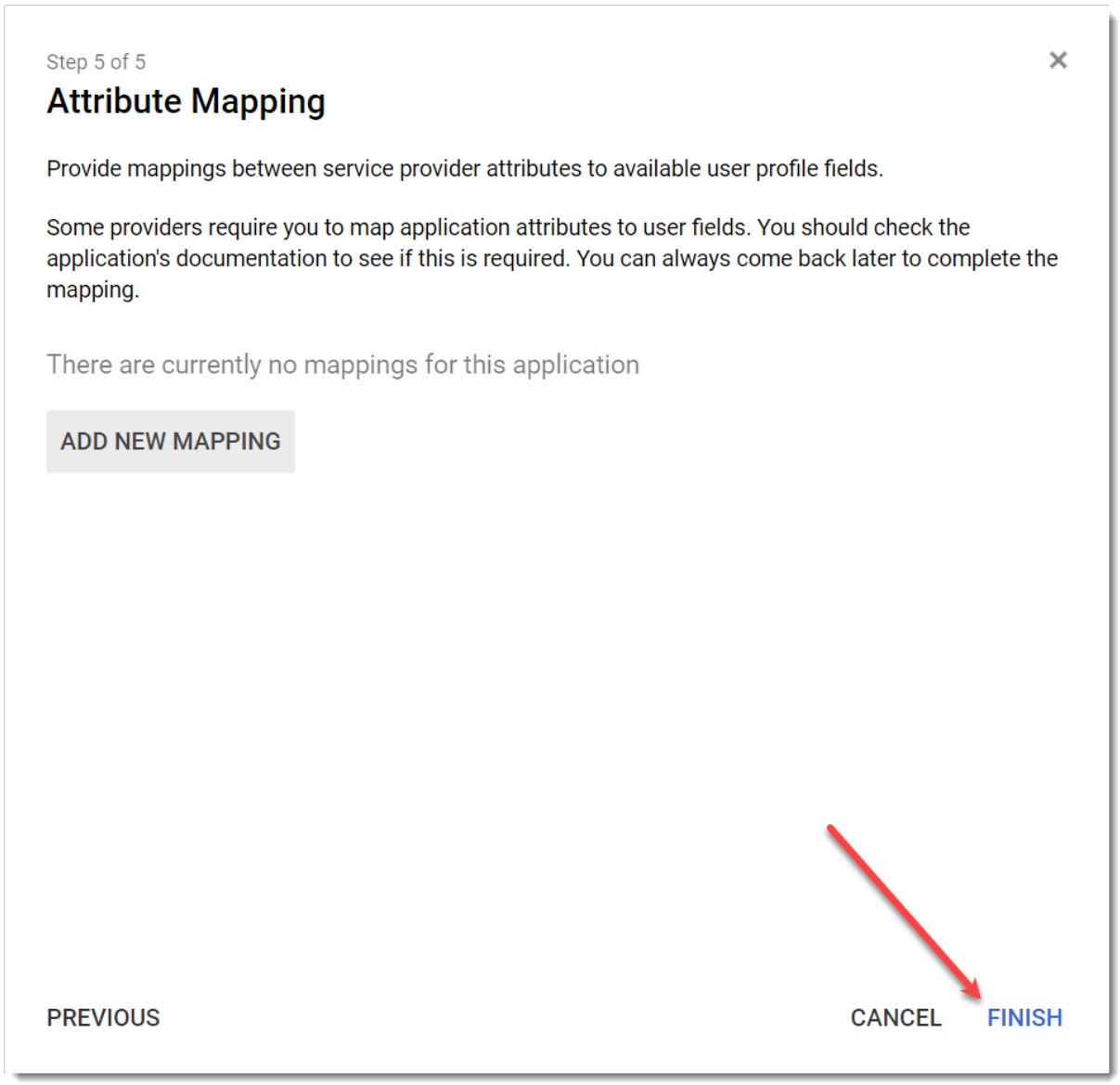
Name your App and click **Next**:



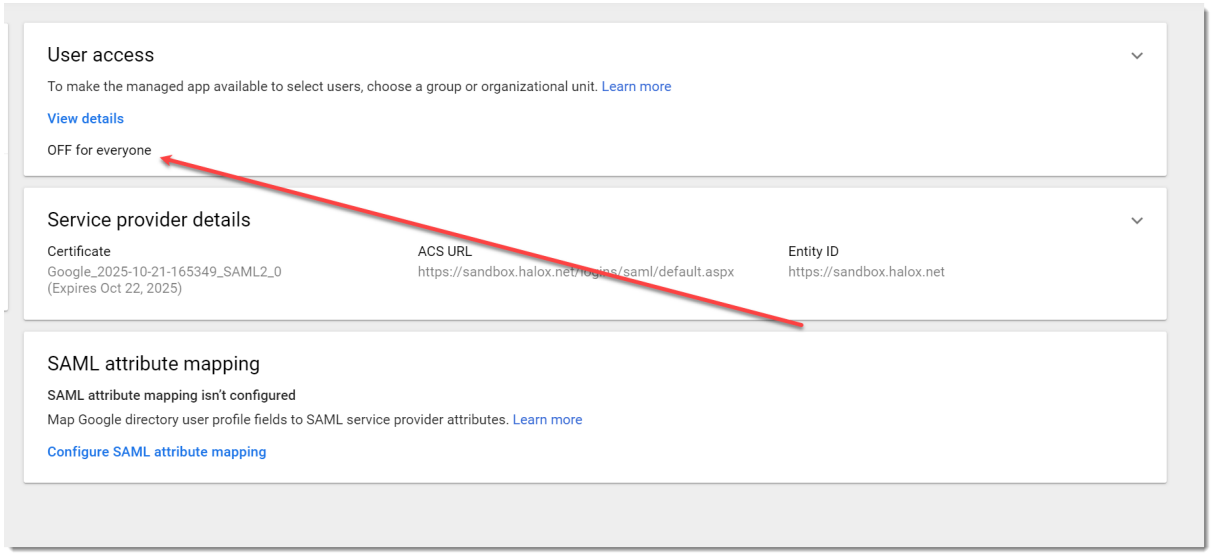
Enter your **ACS URL** and **Entity ID** as follows, but substitute in your own Passwordstate URL. Example is https://passwordstate.contoso.com/logins/saml/default.aspx. Also ensure you set the **Name ID** and **Name ID** Format as per screenshot below, and click **Next**:



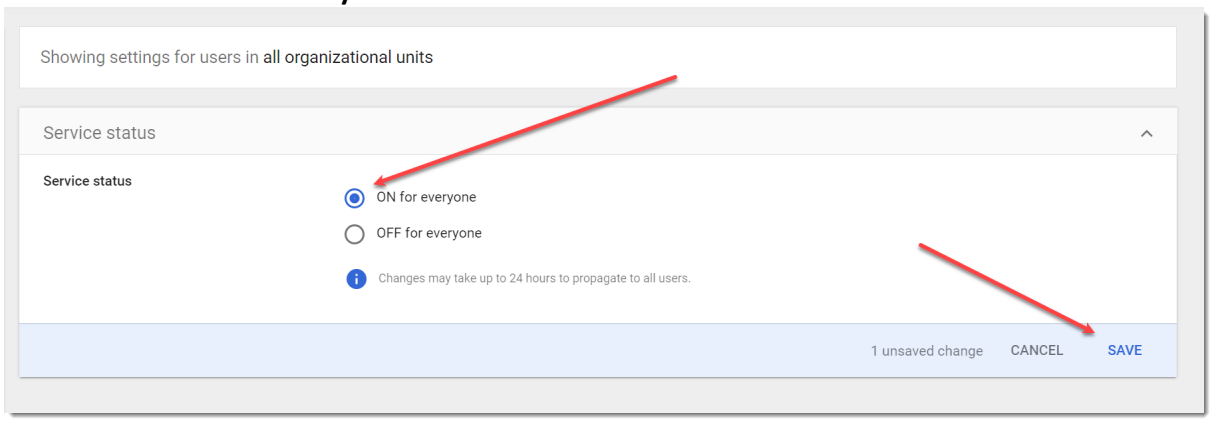
Click **Finish**:



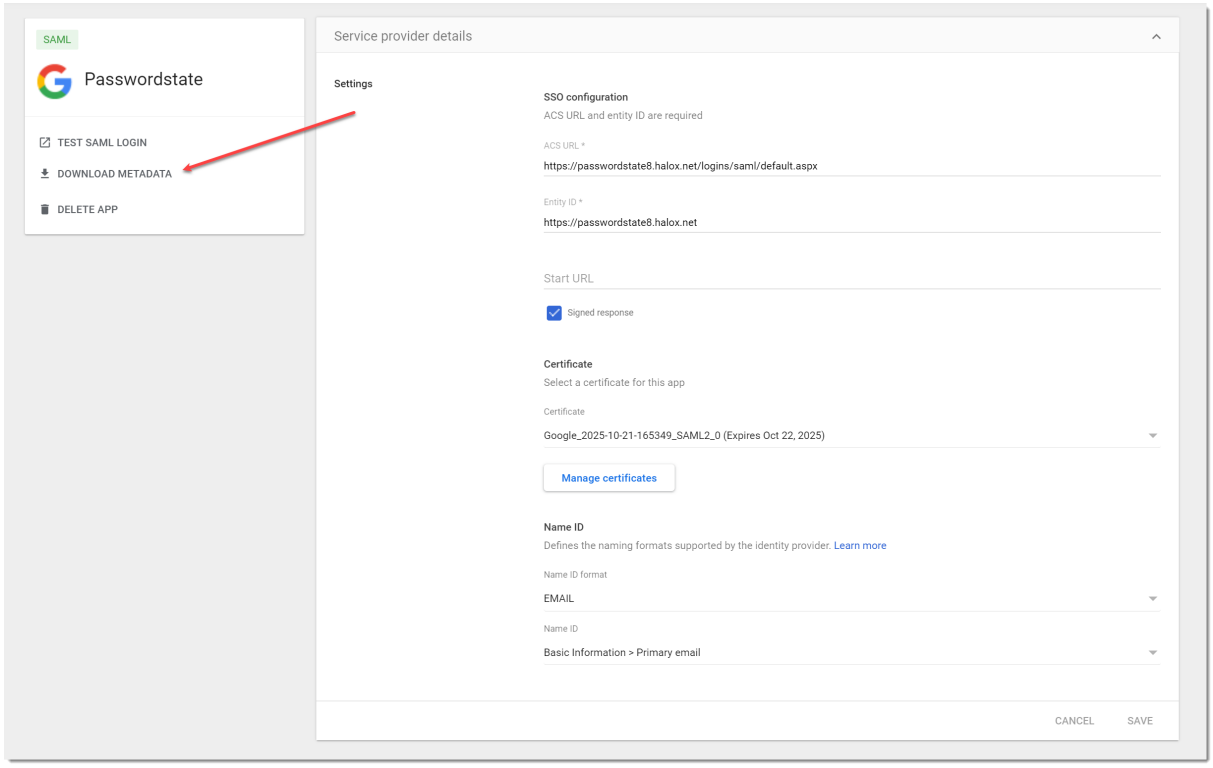
You should now turn on this App for all users in your Google Workspace. To do this, first click on this text:



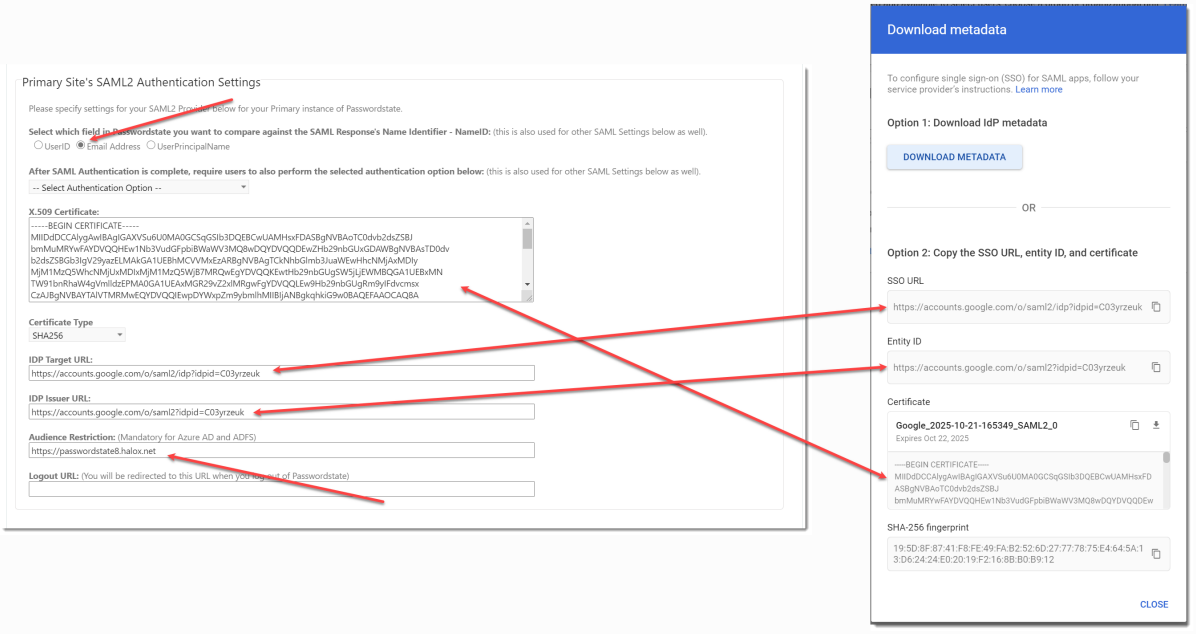
And now select **On for Everyone** and click **Save**:



Now click **Download MetaData**:



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



2.31.7 Branding Tab

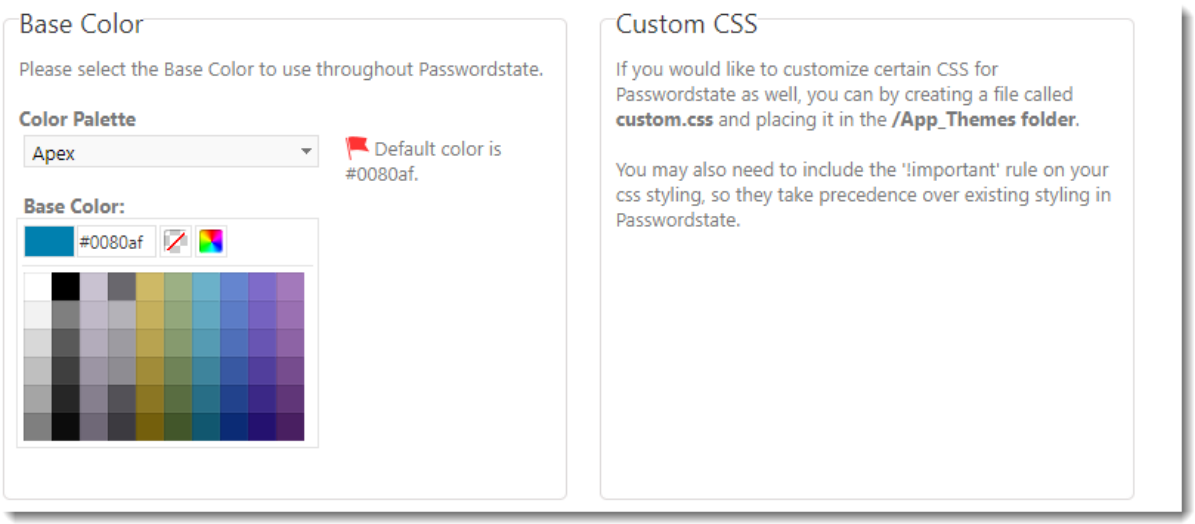
The Branding Tab allows you to hide/show the Passwordstate Build Number at the top of the screen, specify your own custom Logos to use at the top left-hand side of the page, and on various Dialog windows, as well as your own custom Page Titles.

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. User Account Policies can also be used to apply different colors for different sets of users.



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 - https://www.clickstudios.com.au/NewBuildInfo.xml, 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 Proxy & Syslog Servers Tab 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:

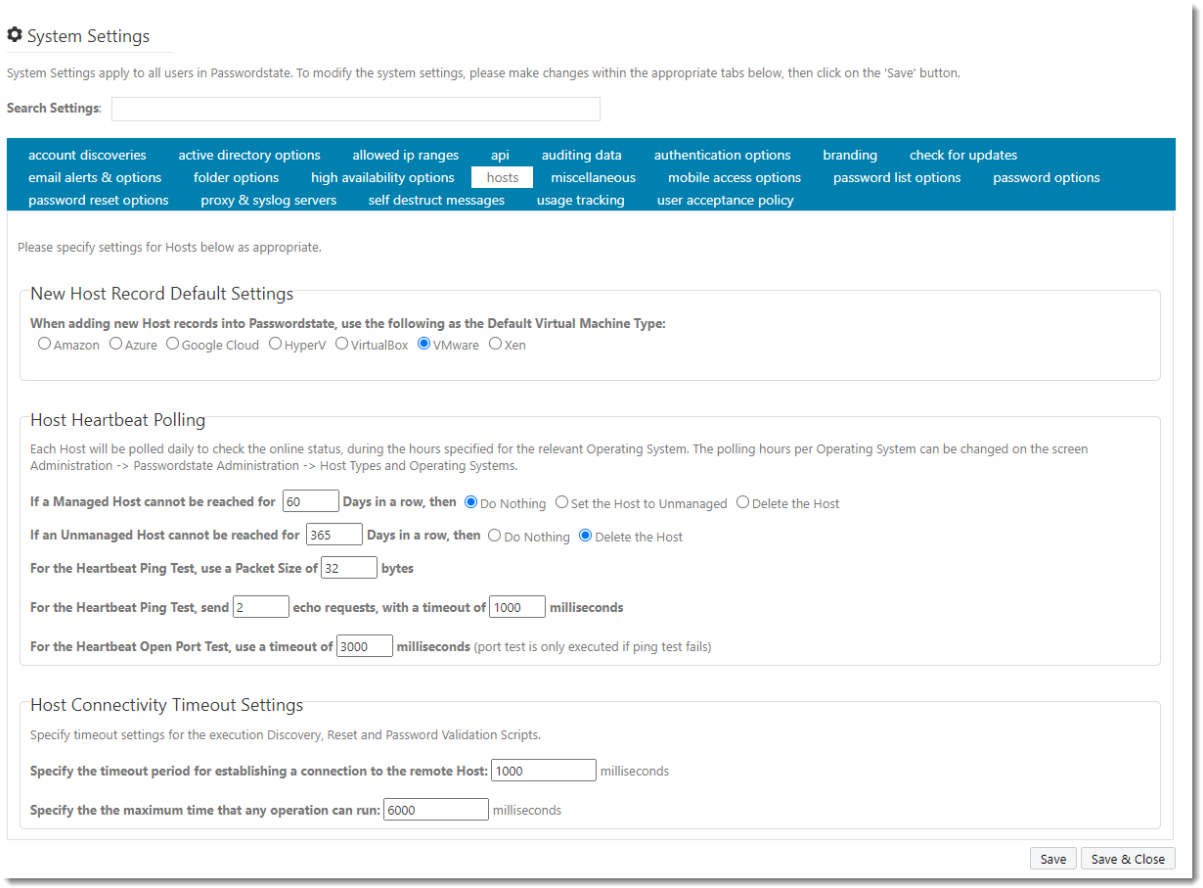
- How frequently the High Availability instance should check for new or updated logos and custom images. If there are any new or updated images, they will be written to disk on the schedule provided

- 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.



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 - https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.core/invoke-command?view=powershell-7.3

Use regular expressions when matching 'Bad Passwords'

If the use of 'Bad Password' detection is enabled on the Password Options Tab, 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.

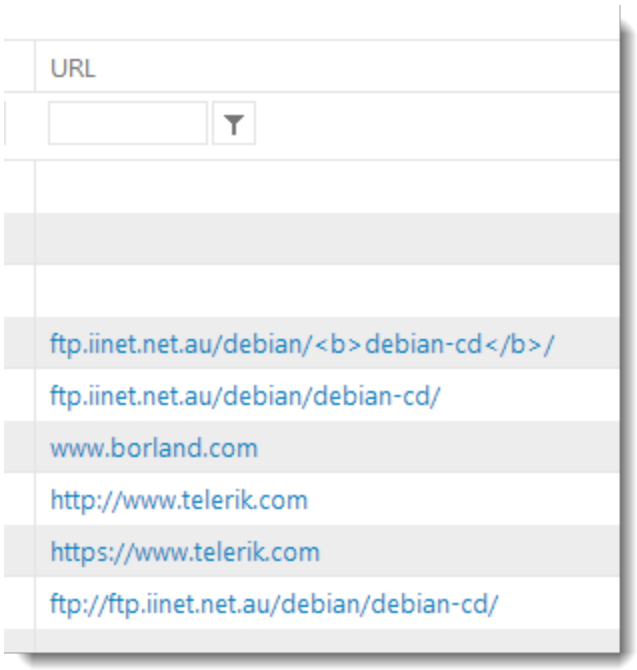
In the Passwords Navigation Tree, sort alphabetically by

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

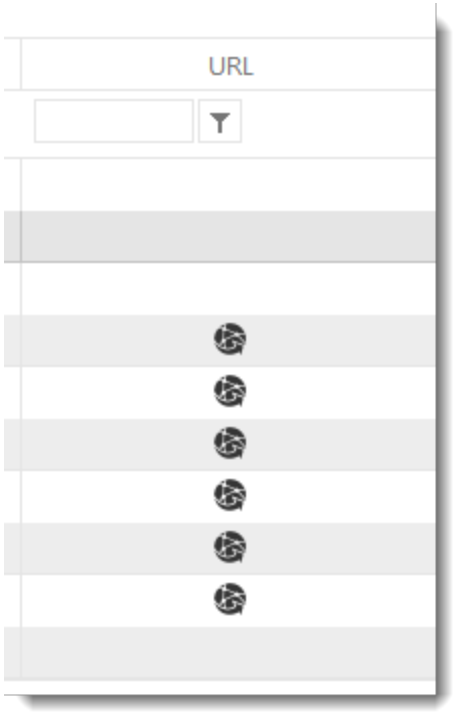
required, where sorting is simply done alphabetically, regardless of Folder/Password List node type.

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:



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.

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

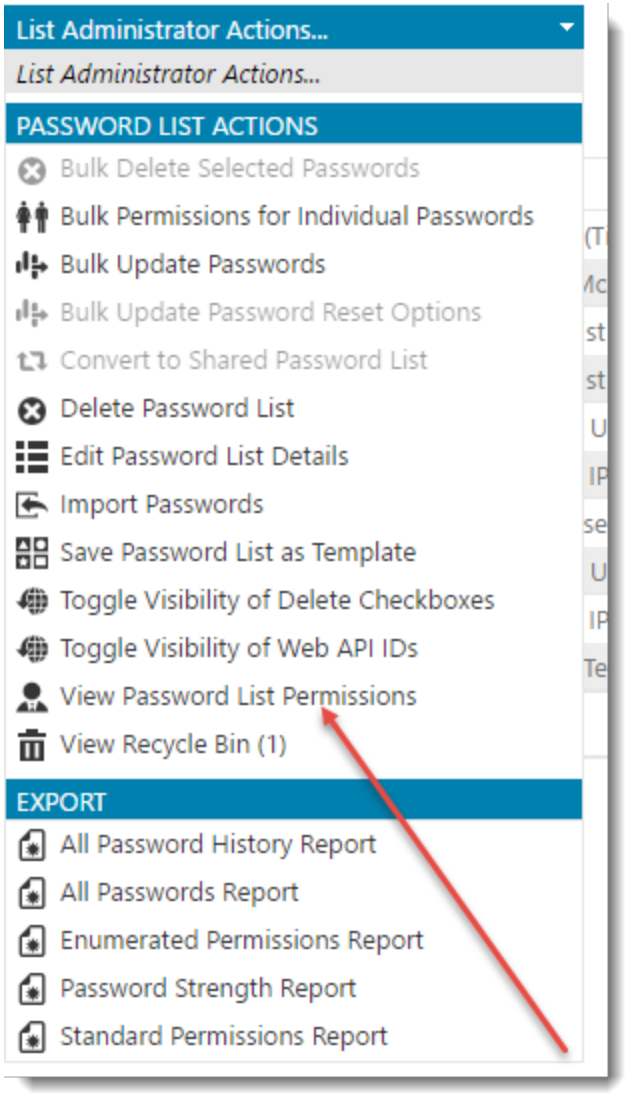
In each of the different Password Grids, it's possible to display the Account Type column. In this column you can show just the image for the Account Type, or the image and the label for the Account Type

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 Bad Passwords 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  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

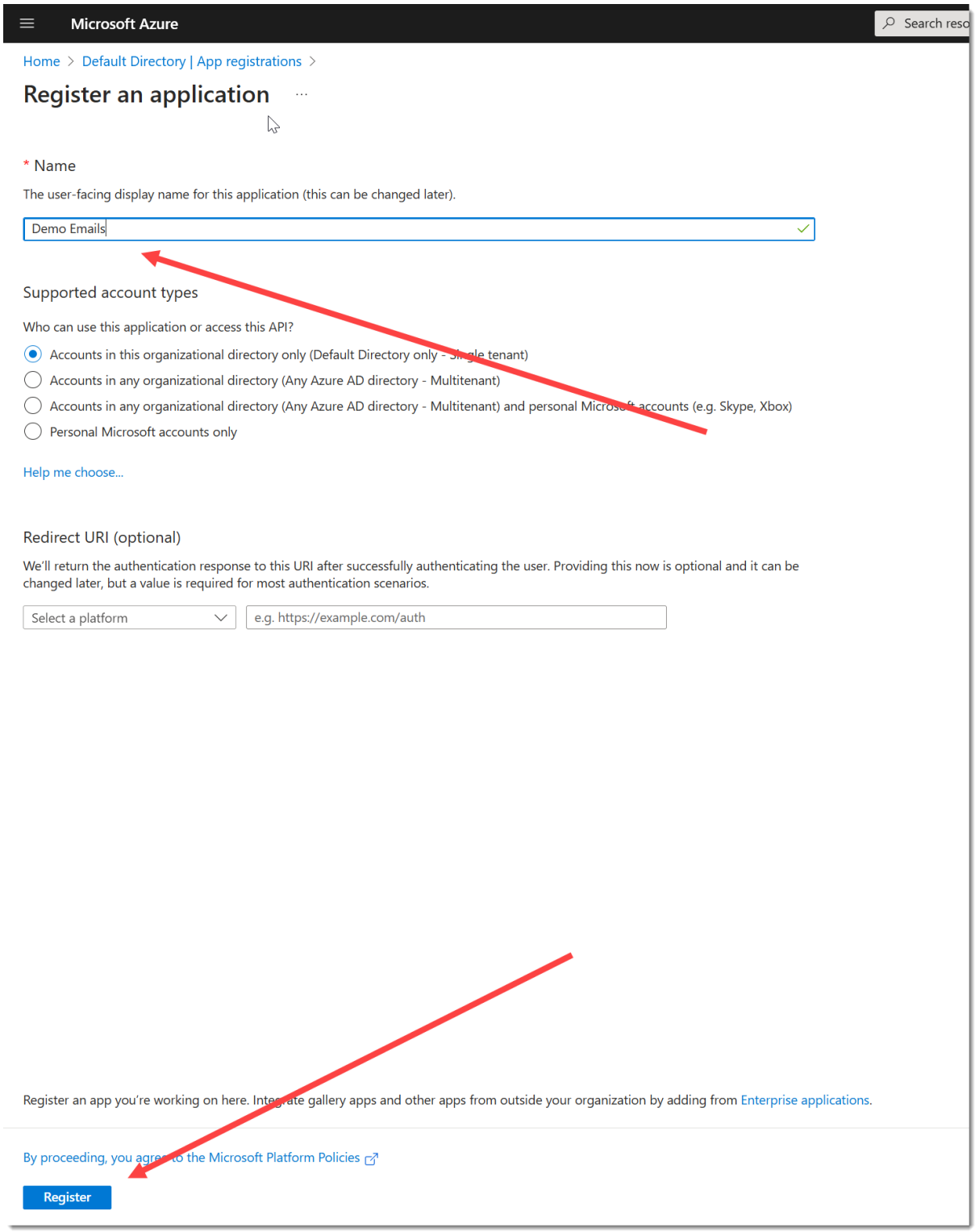
Allows you to choose whether you wish to use an SMTP mail server for sending emails, or Exchange Online.

Microsoft Exchange Online Details

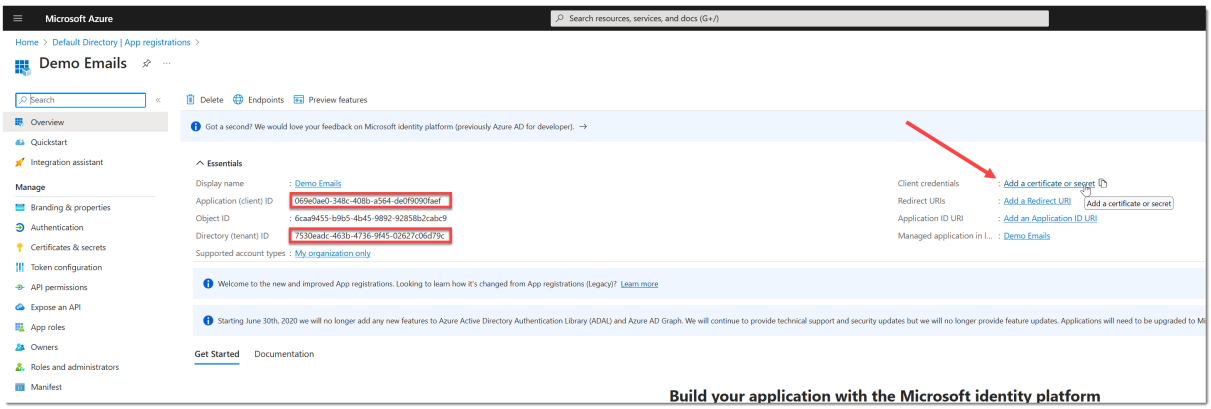
If you have a valid Microsoft subscription that allows you to use Exchange Online, then you can use the Microsoft Graph to send various Passwordstate emails. The instructions below show you how to configure the Graph API and grant permissions to allow mail to be sent out on behalf of a Azure AD User.

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.

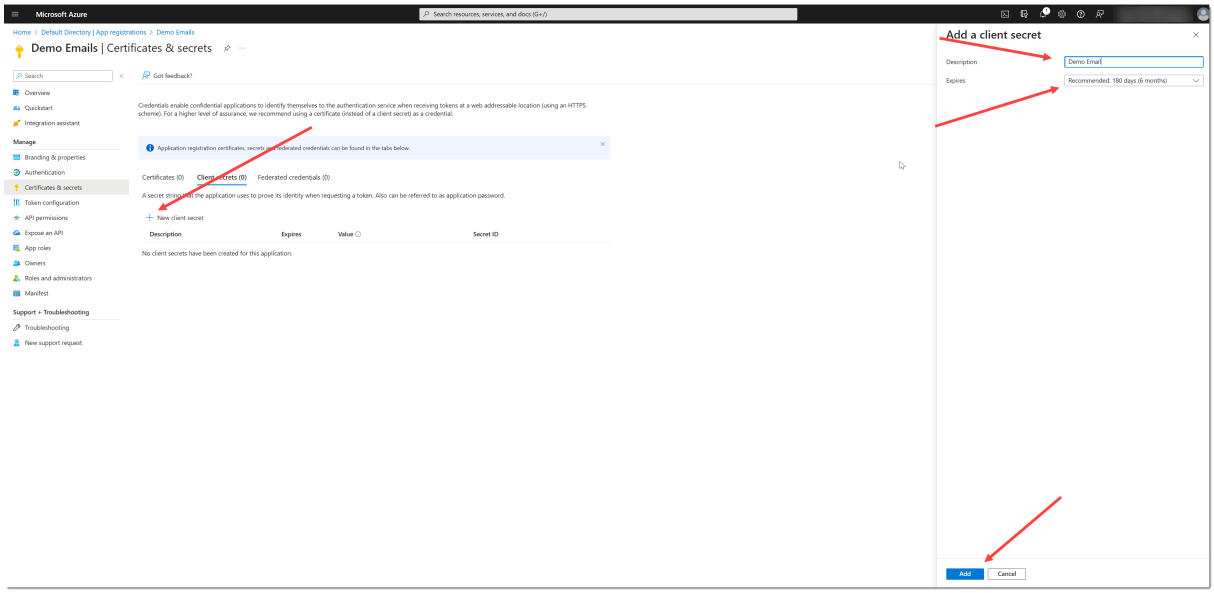
- Log into your Azure portal, and select Azure Active Directory
- Now click on **App registrations** menu on the left hand pane, and select "**New Registration**"
- Type in any name of your choice for the application you are creating, and then click **Register**



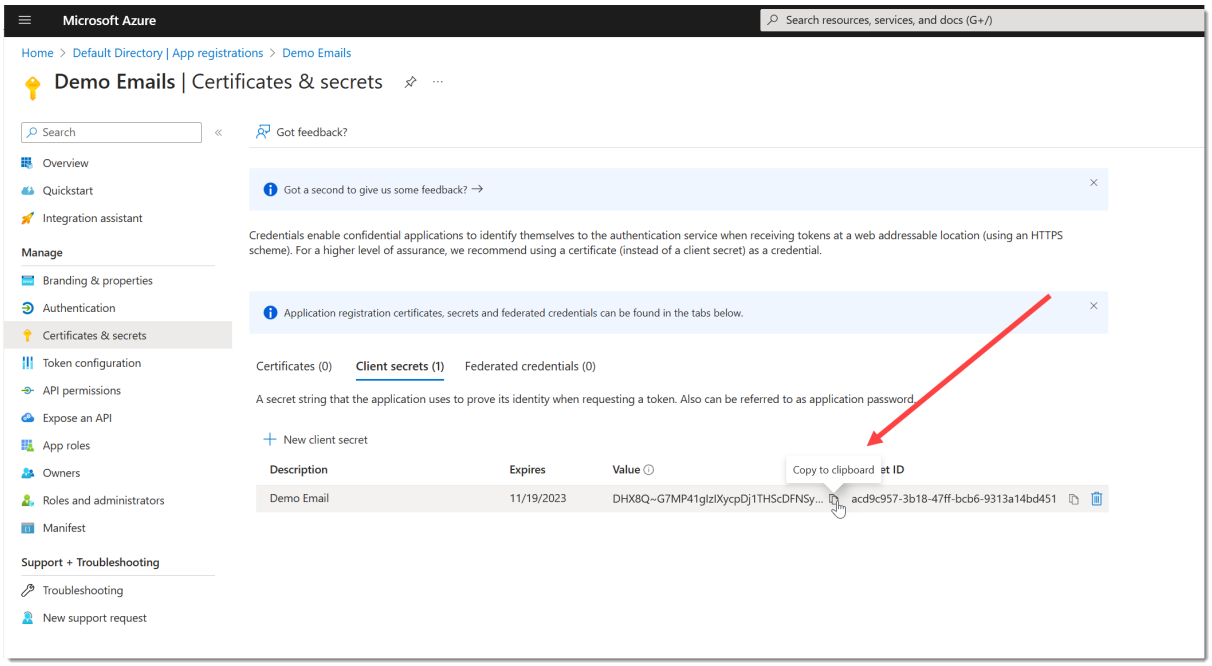
- Take note of the **Application (client) ID** and **Directory (tenant) ID, and the c**lick on the **Add a certificate or secret** link



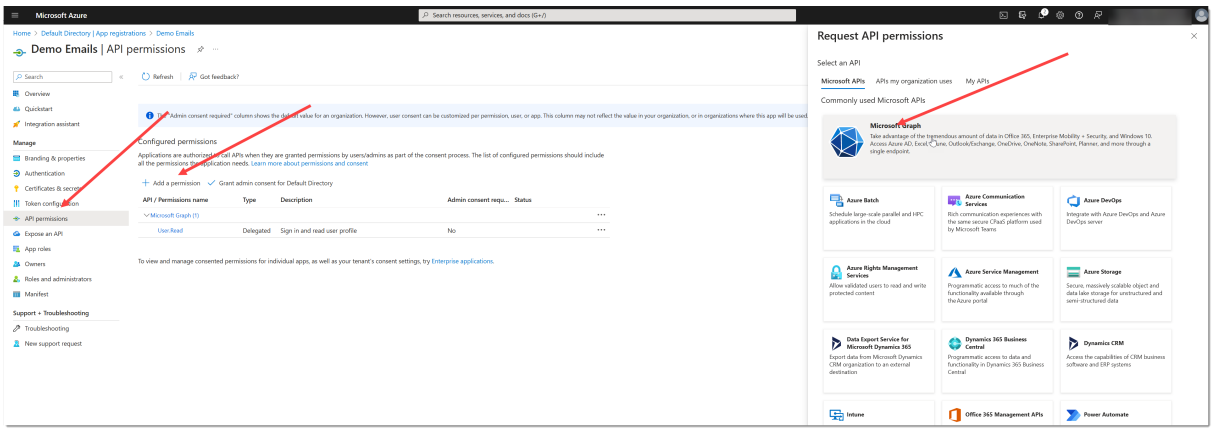
- Click "**New Client Secret**", give it a **description**, and **expiry date** and click **Add**



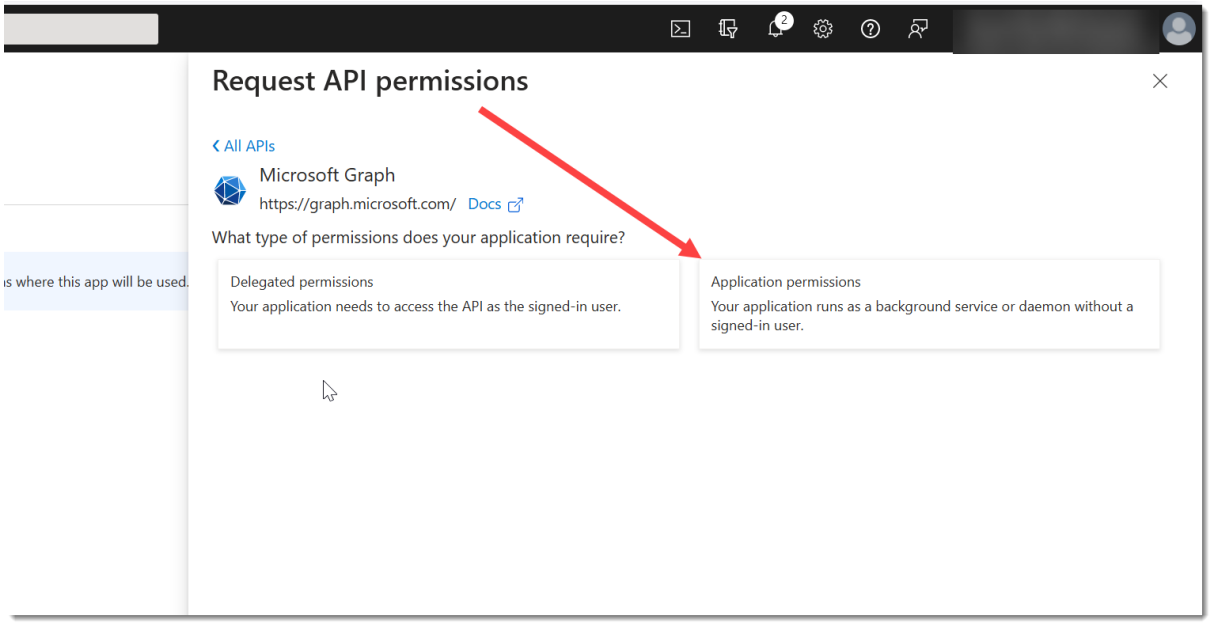
After the client secret is created, take note of the Value which will be used later in Passwordstate. You can only view this once when you create the secret:



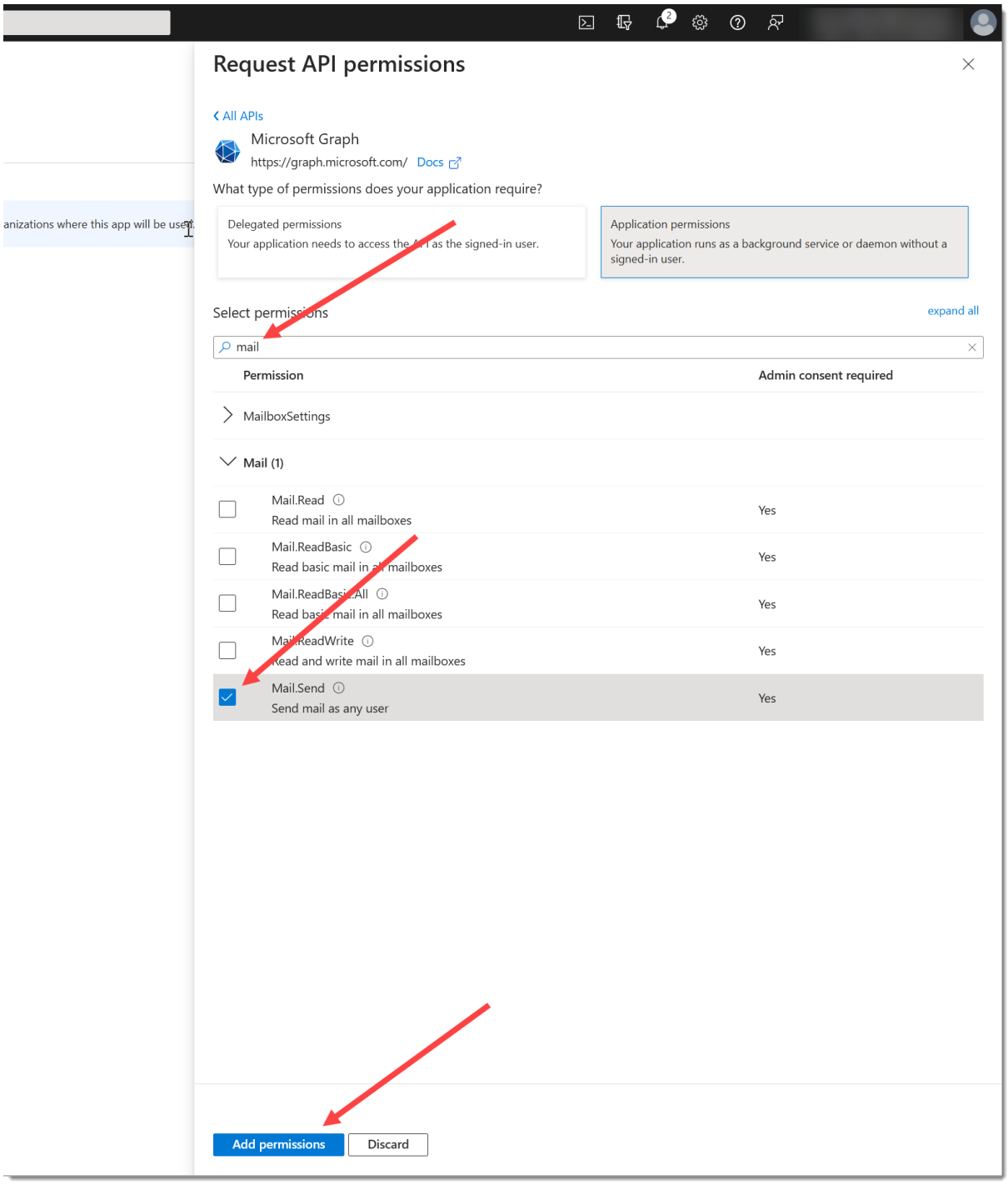
- Now click on **API Permissions**, click **Add Permission** and the click on the **Microsoft Graph** button.



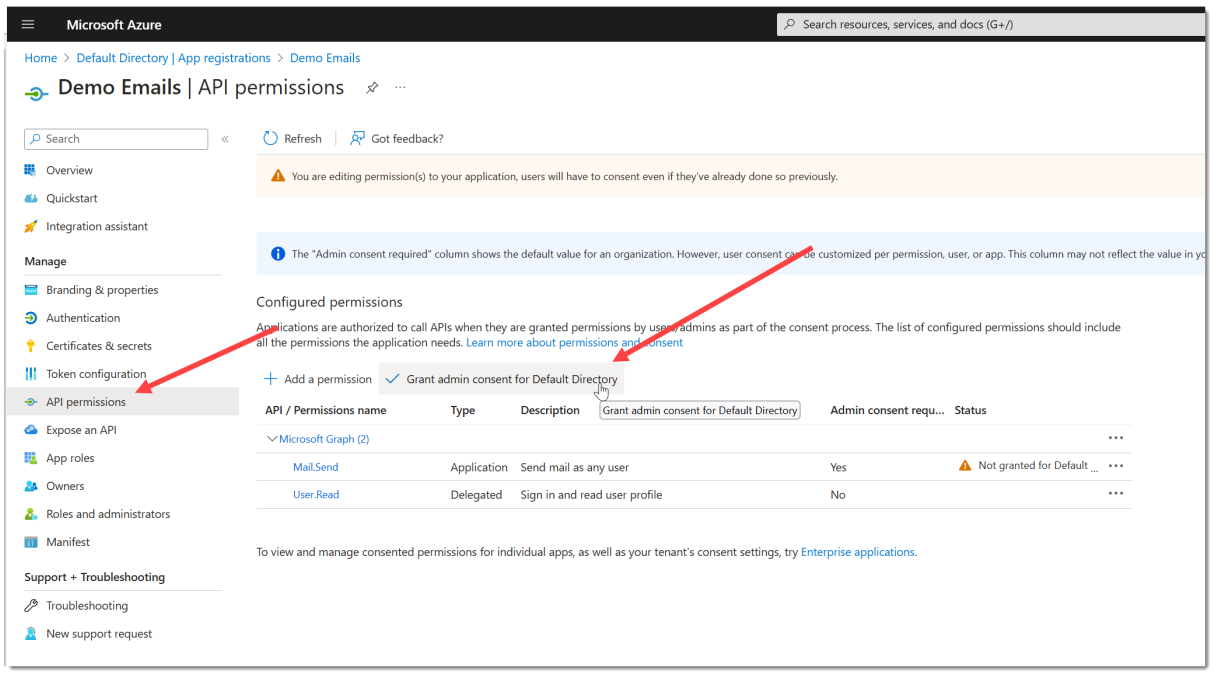
- Click on Application Permissions



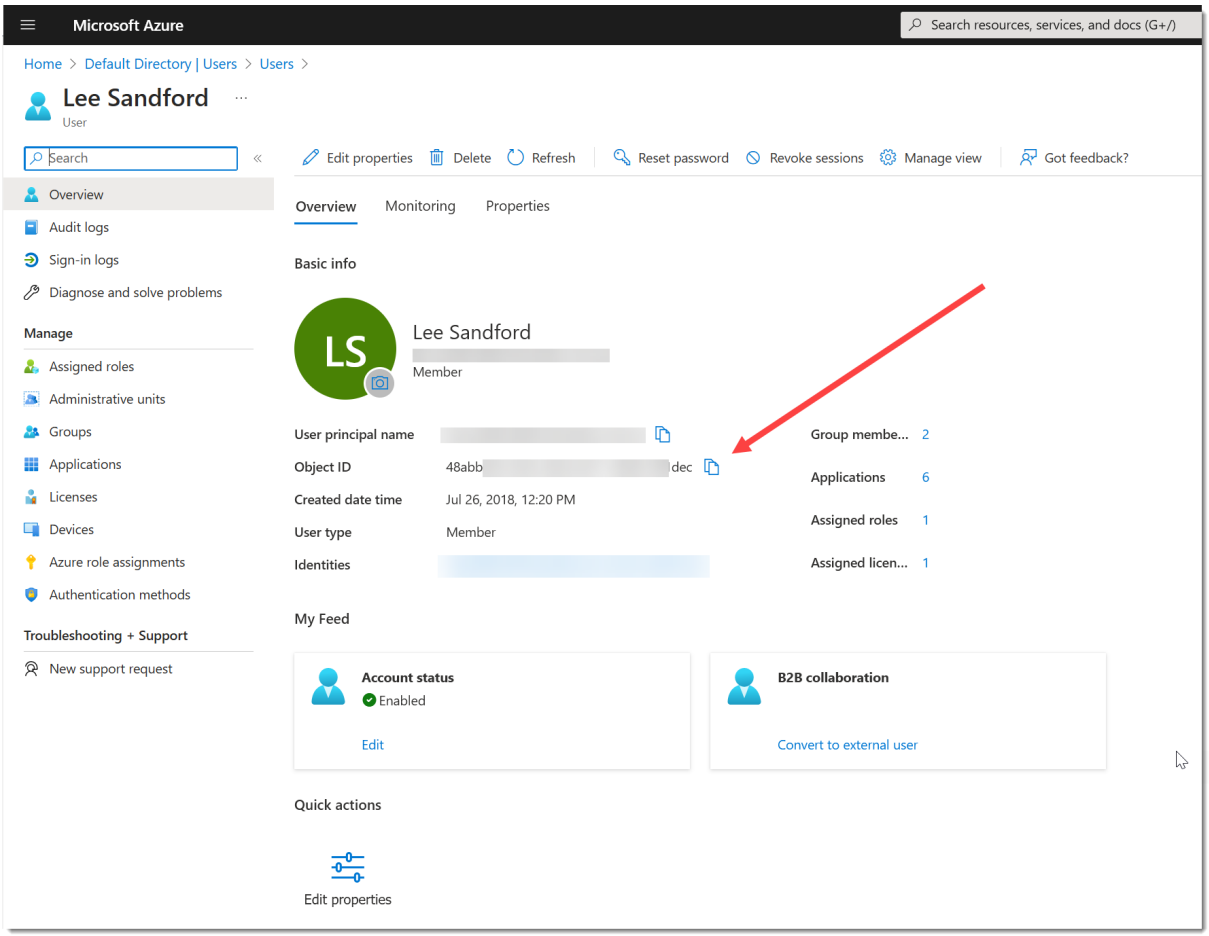
- Search for "**mail**", tick the **Mail.Send** option, and click **Add Permissions**



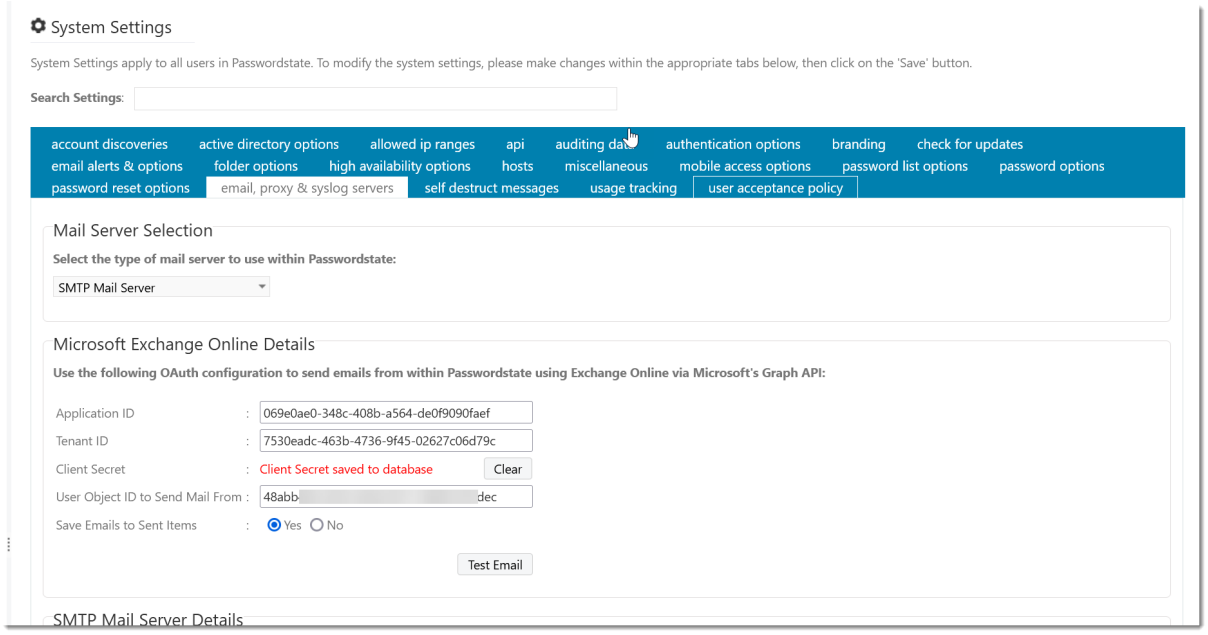
- Under **API Permissions** page, click the **Grant Admin Consent for the Default Directory** button



- 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.



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 https://www.clickstudios.com.au/NewBuildInfo.xml. 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.

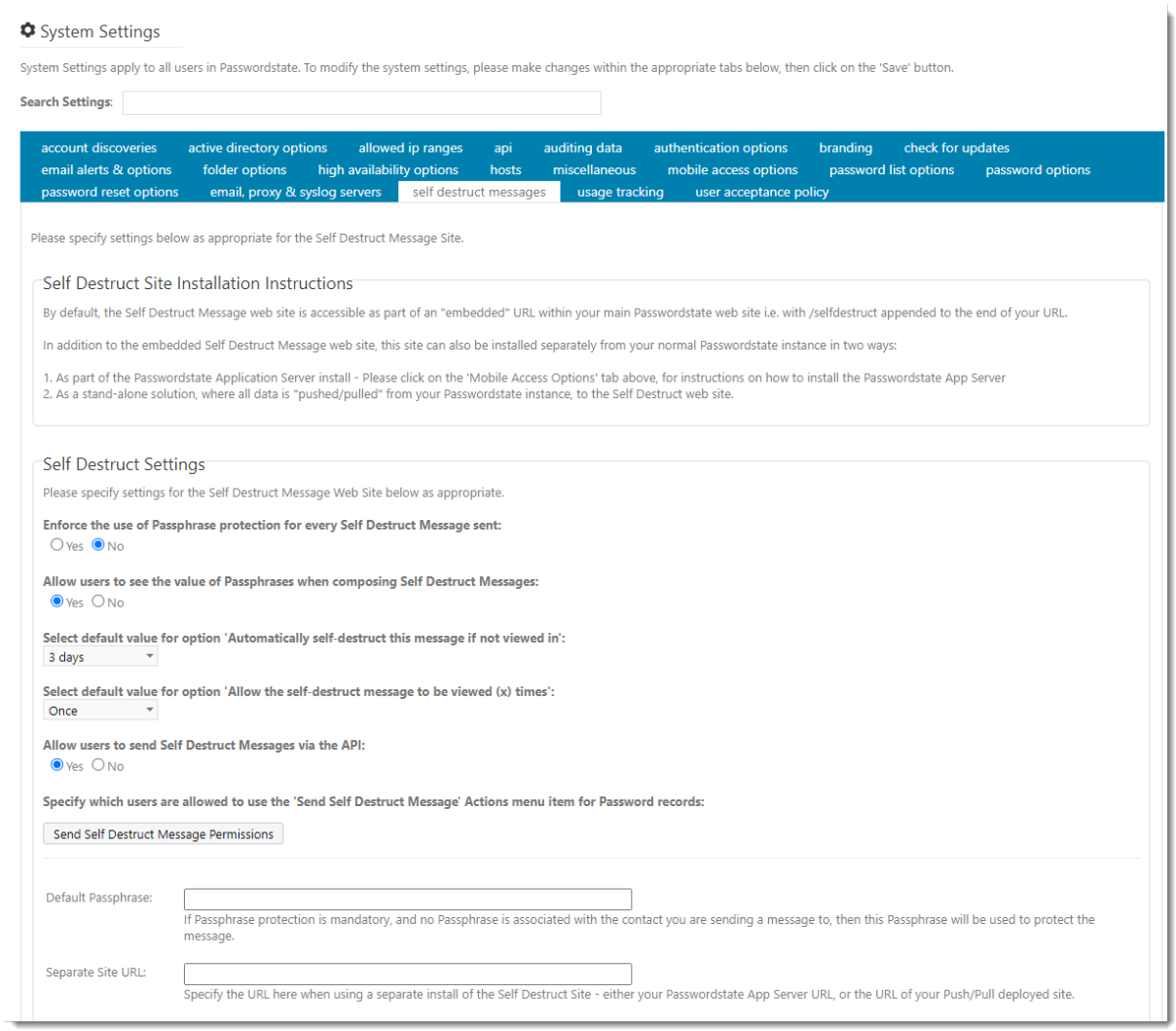
There are two types of Self Destruct Message web sites which can be used, and they are:

- 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.



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

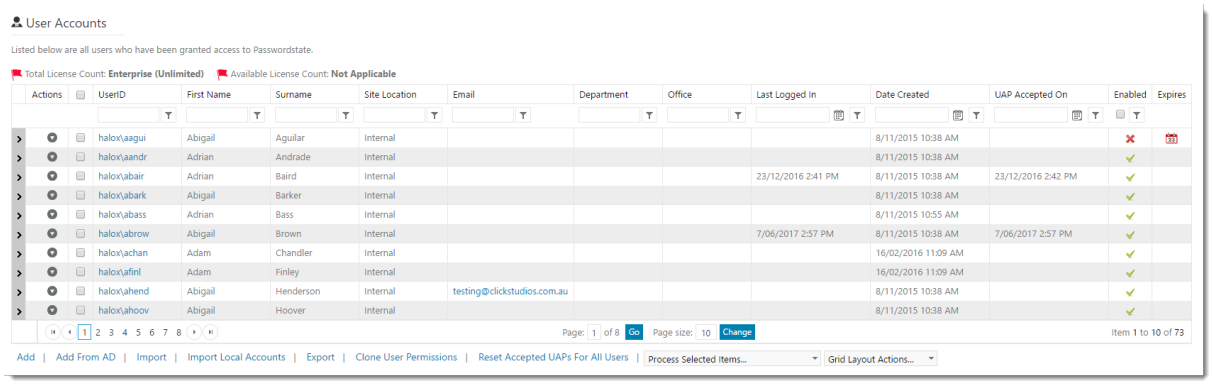
Prior to any of your users being able to access the Passwordstate web site, you must first register their accounts in the User Accounts screen.

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 Security Groups screen for information on this method

 Performance Tip: If you have many Active Directory User Accounts added to Passwordstate, the synchronization features on the Active Directory Options Tab 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 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.

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 Email Templates.
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



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:

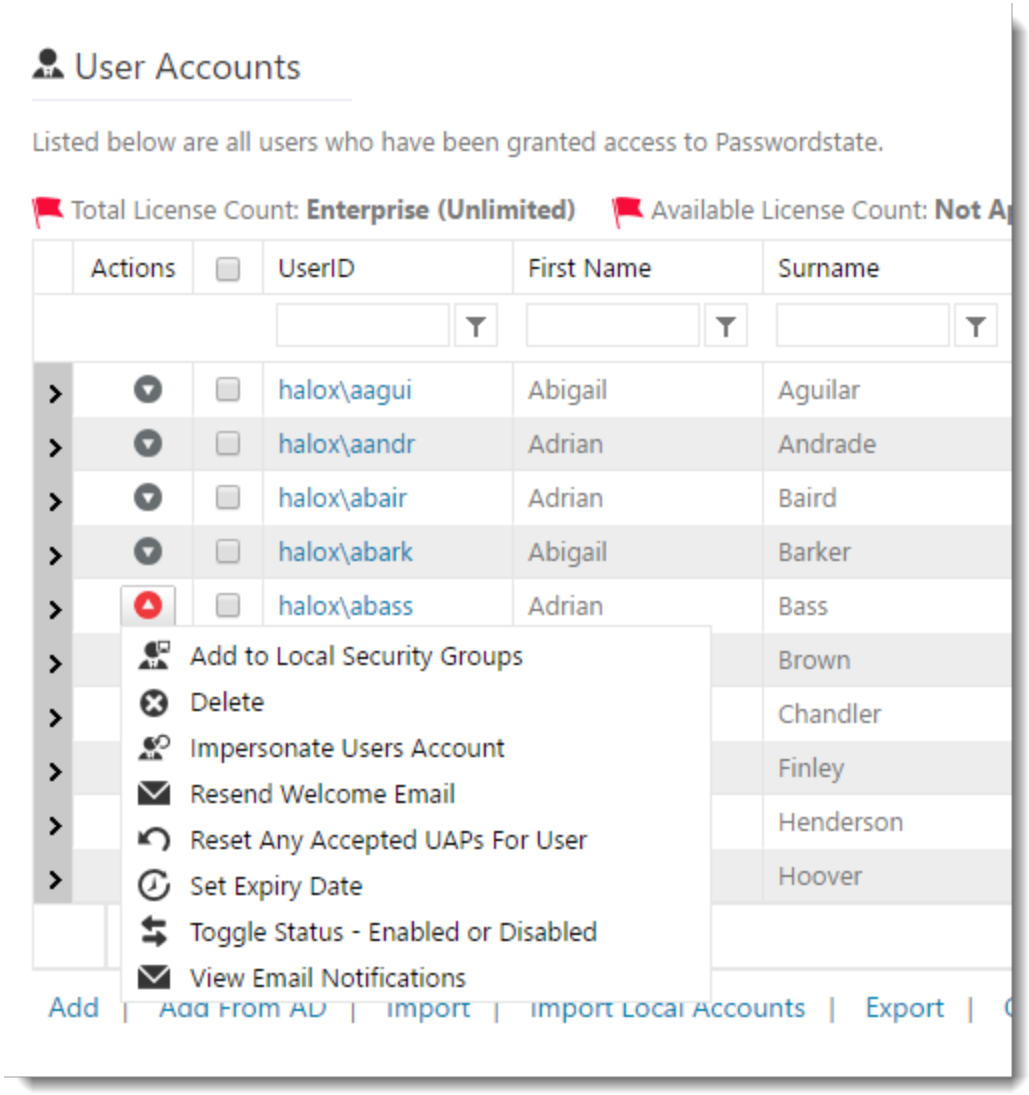
- **Delete** - deleting a user's account will remove all access for them, so please use with caution
- **Impersonate Users Account** - this feature should only be used when trying to troubleshoot issues with the affected user. By selecting this option, an email will be send to the user informing them 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 System Settings -> User Acceptance Policy Tab
- **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 System Settings -> Active Directory Options Tab

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



Editing User Account Settings

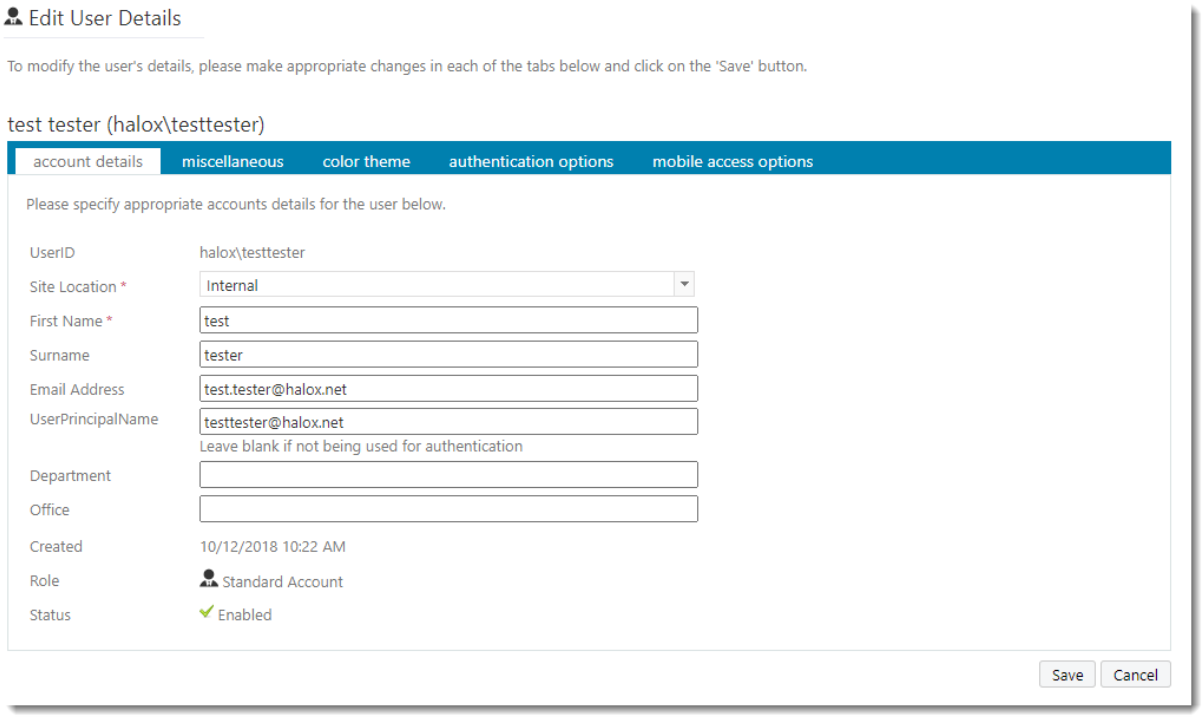
By clicking on the UserID hyperlink in the grid, you will be directed to a screen where you can edit multiple properties for the user's account.

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: User Account Policies 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.

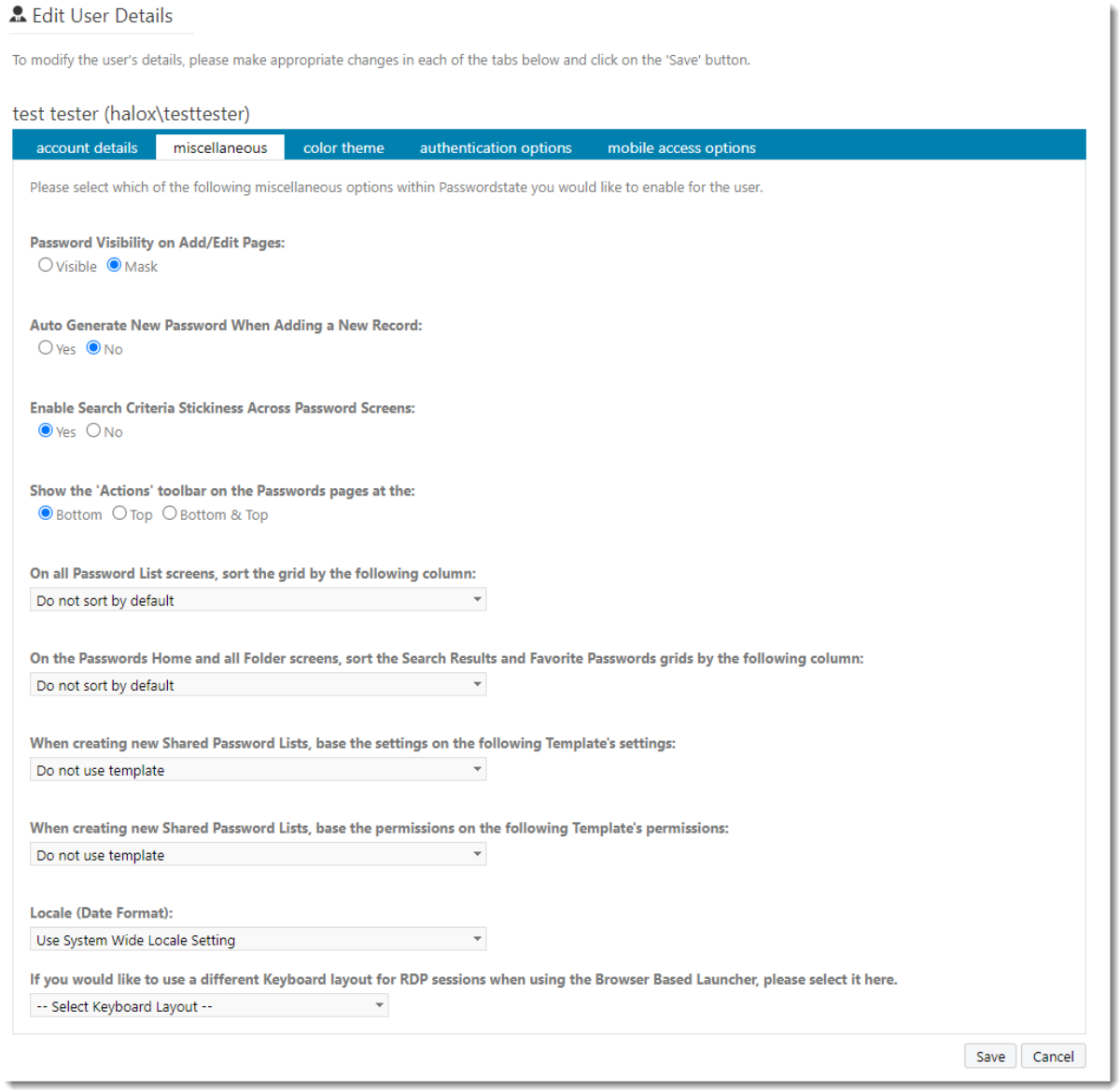


Miscellaneous Tab

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  icon
Show the 'Actions' toolbar on the Passwords pages at the	At the bottom of every Passwords grid there are certain buttons/controls for adding passwords, importing them, viewing documents, etc. With this option, you can choose to display the 'Actions' toolbar at the bottom of the Passwords grid, at the top, or both
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

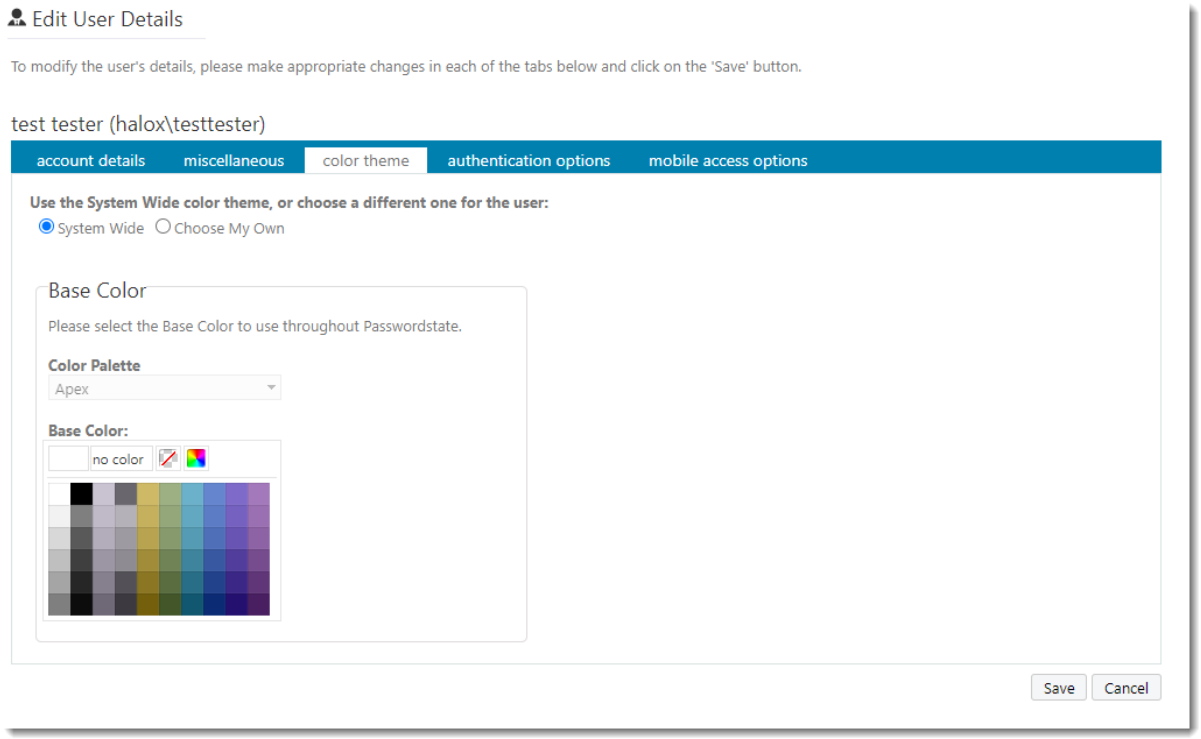


Color Theme Tab

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.

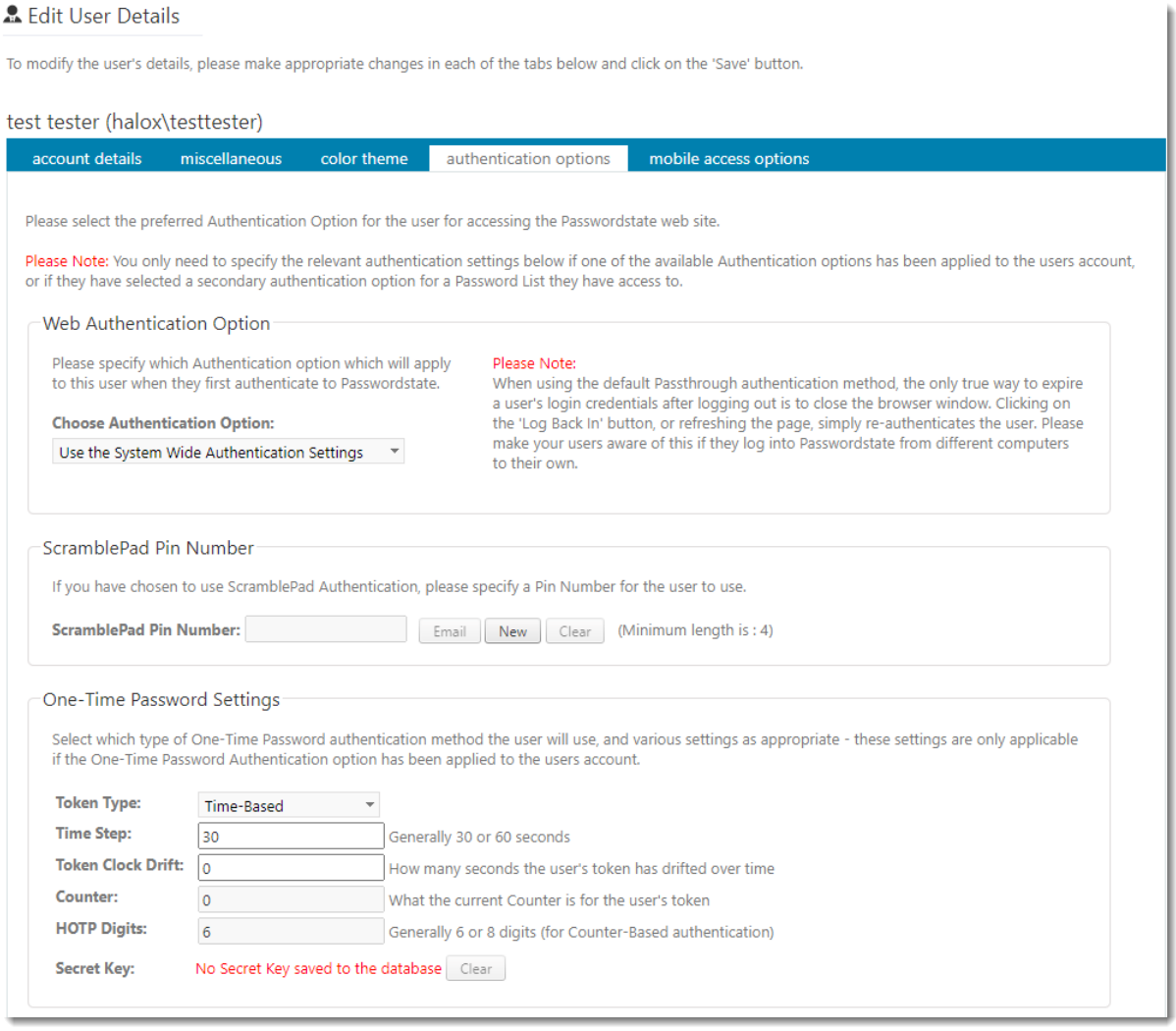
Note: The Security Administrators of Passwordstate can use a feature called 'User Account Policies', which may override any settings you specify here.



Authentication Options Tab

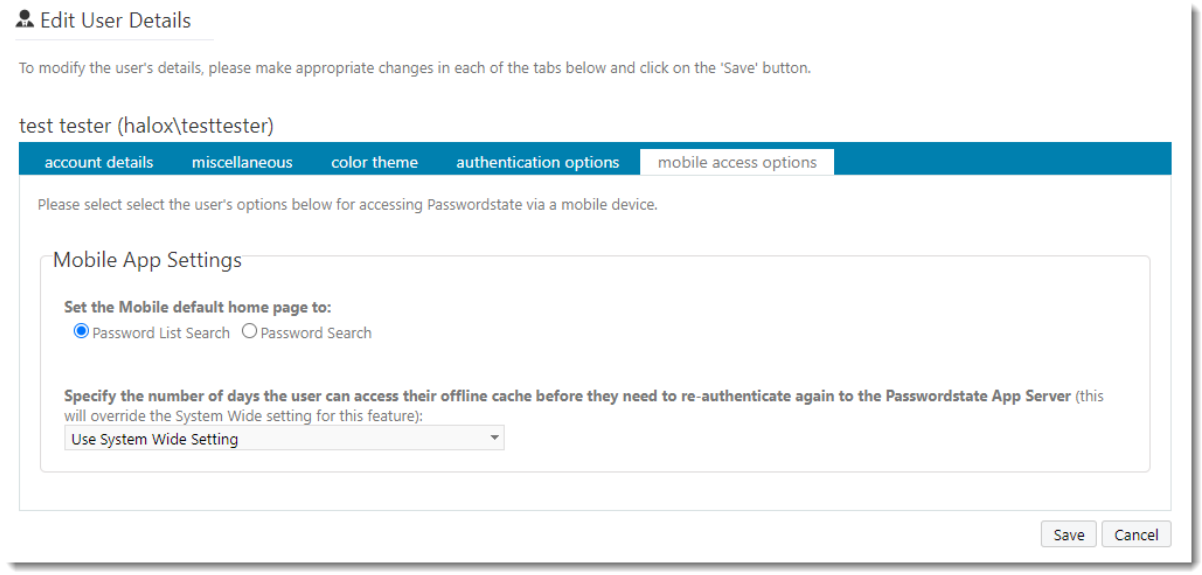
The Authentication Options Tab allows you to:

- 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 System Settings -> Authentication Options Tab
- 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



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.



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:

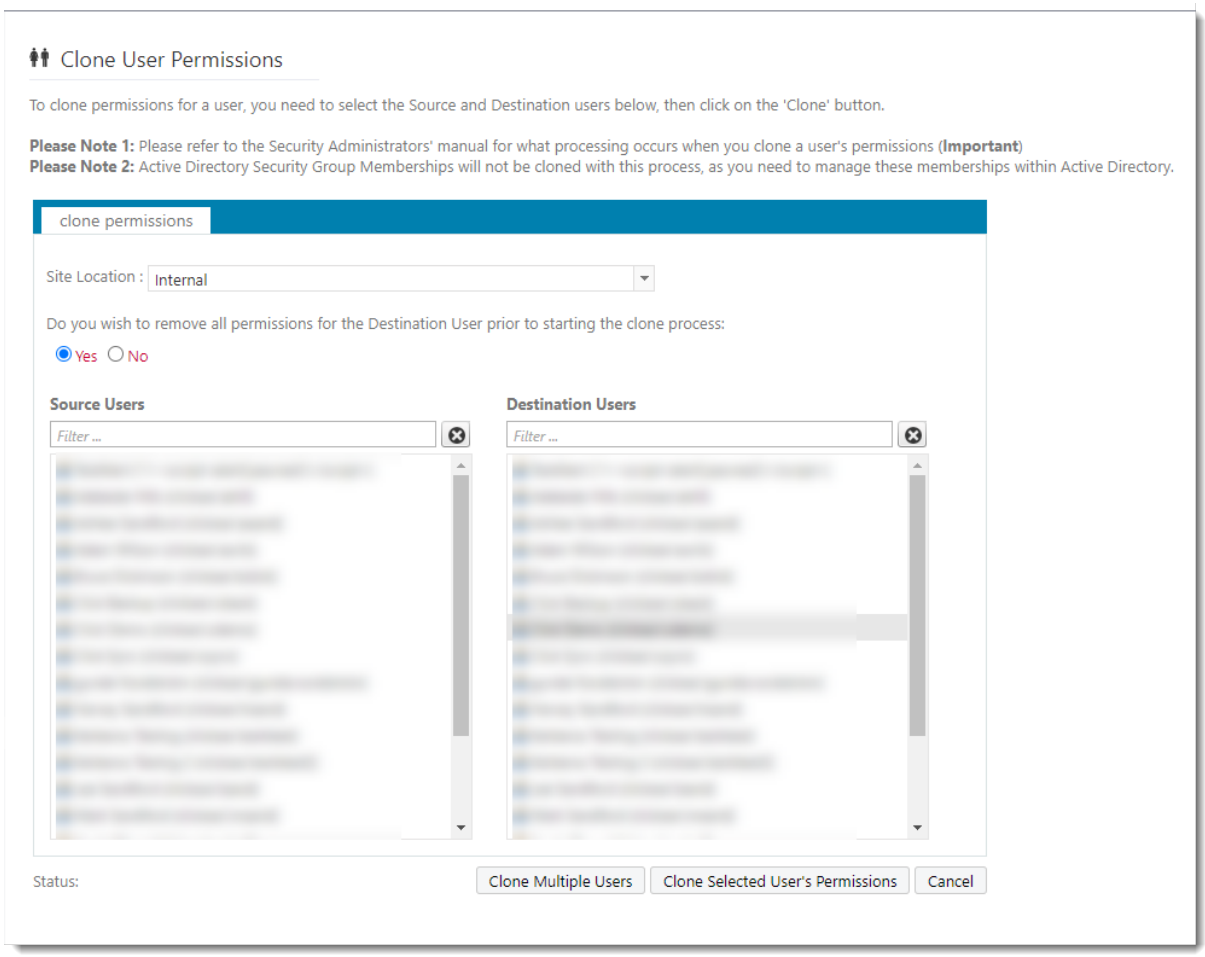
- You've had a new employee start who has replaced another employee, and you wish to give them the same access
- If you need to modify the UserID for a user i.e. a Domain Migration, someone gets married, etc.

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



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 User Acceptance Policy Tab. 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, 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

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

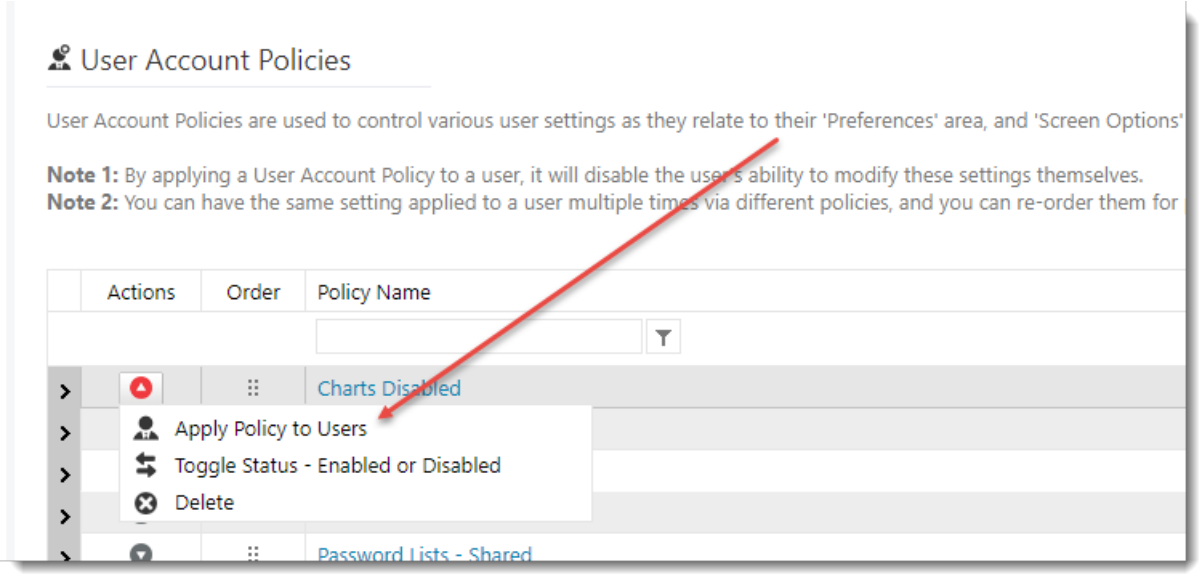
When creating new Shared Password Lists, base the settings on the following Template's settings
When creating new Shared Password Lists, base the permissions on the following Template's permissions
If copying settings from a Template to a Shared Password List, also link them
When creating new Private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



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

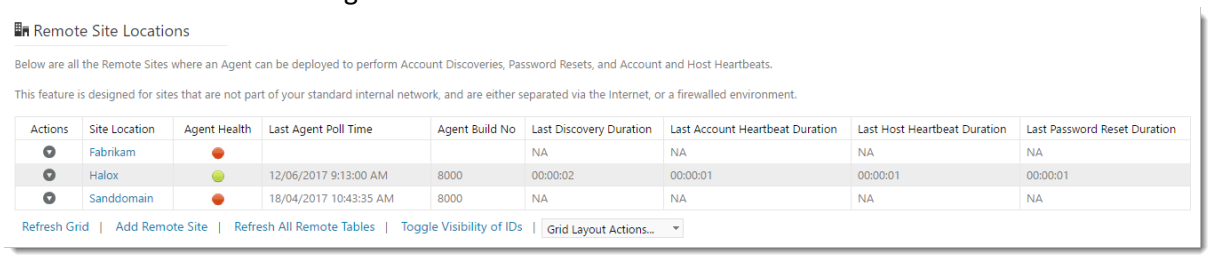
- Password Resets for many different account types
- Account Heartbeat Status for many different account types
- Free Licenses for "Clients' to login an view their own password credentials
- Process for identifying which passwords need resetting after one of your technicians leaves your company, and 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'.



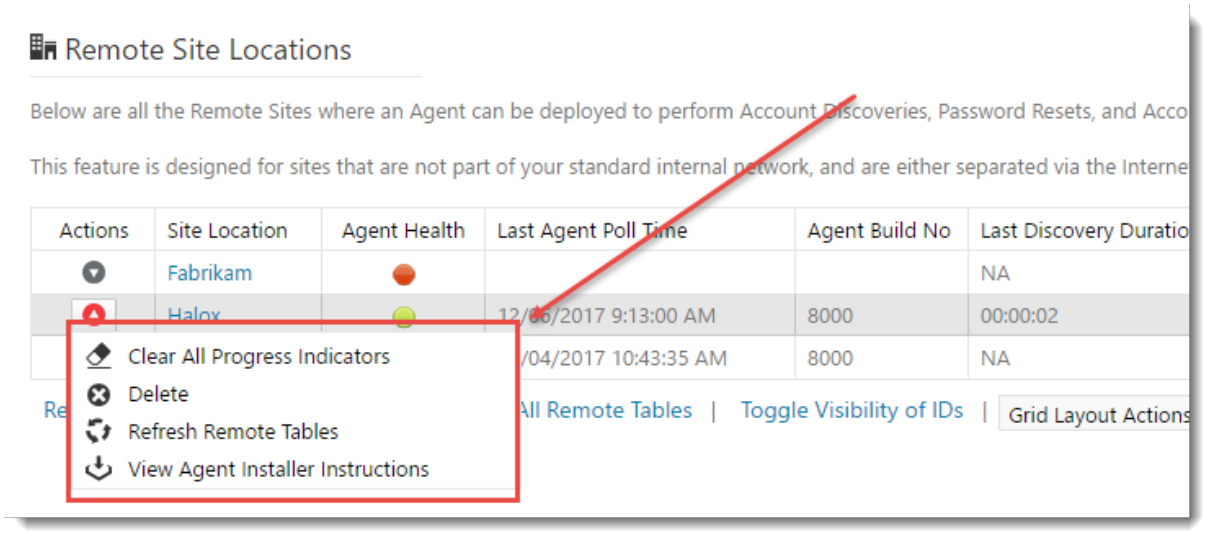
Remote Site Locations Actions Menu
Below is a description for each of the Remote Site Locations Actions menus:

- **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
- 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**



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

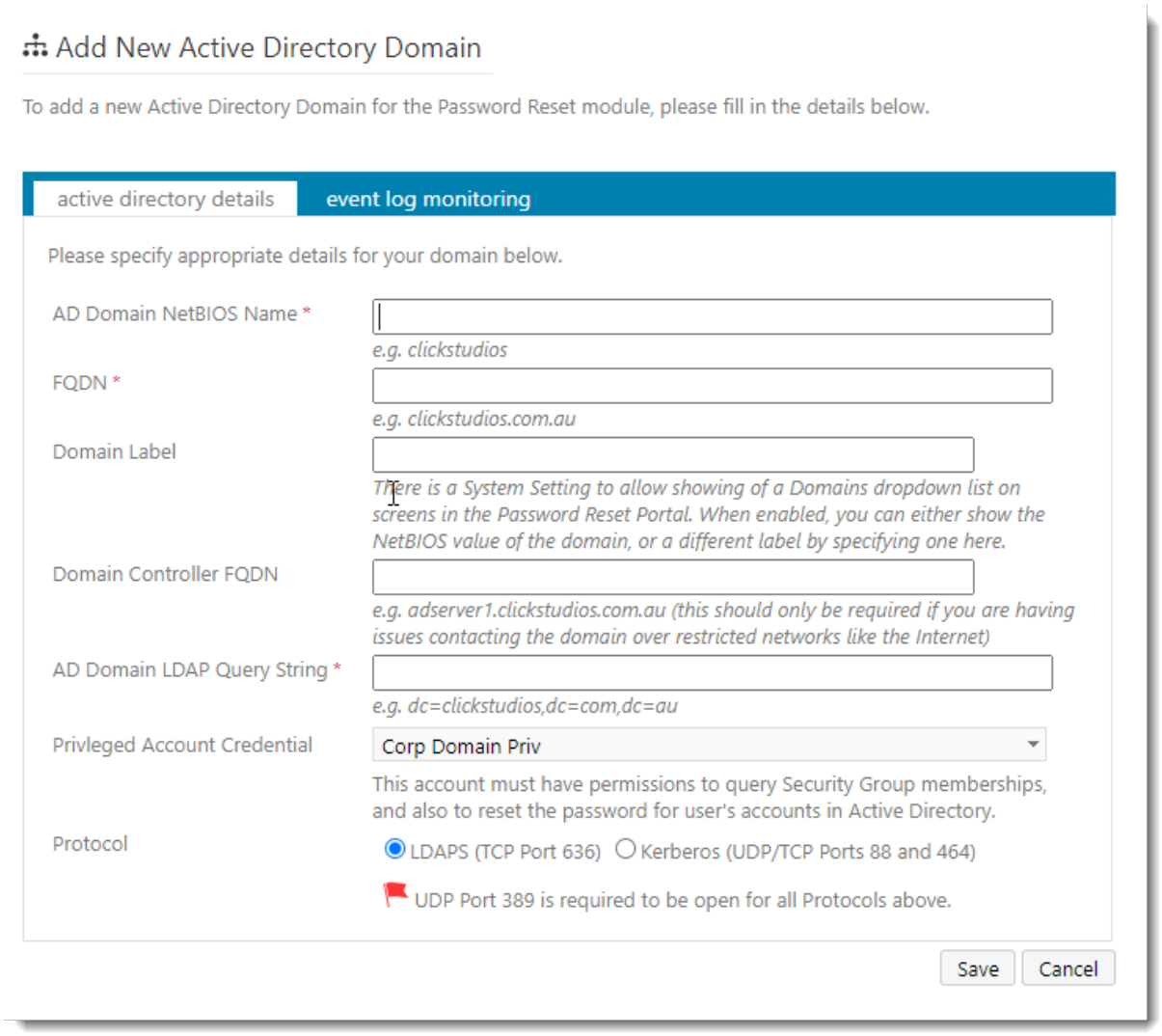
- The Password Reset Portal only needs to communicate back to your Passwordstate API, so generally Port 443 is required to be open. If you are using a different port for your Passwordstate web site, then this port will instead need to be open

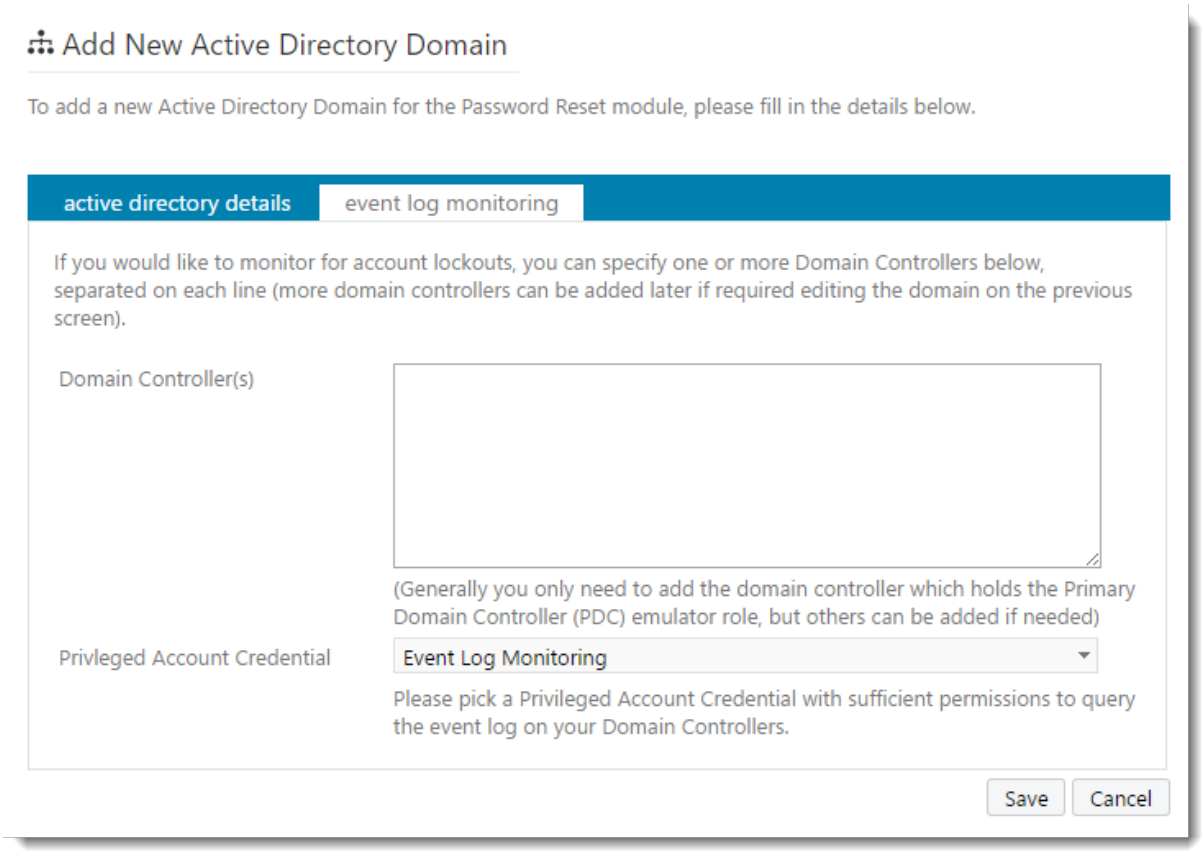
Passwordstate Web Site and API

- 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 Privileged Account Credentials so Passwordstate can reset/unlock accounts in the domain, and also query event logs on your domain controller.

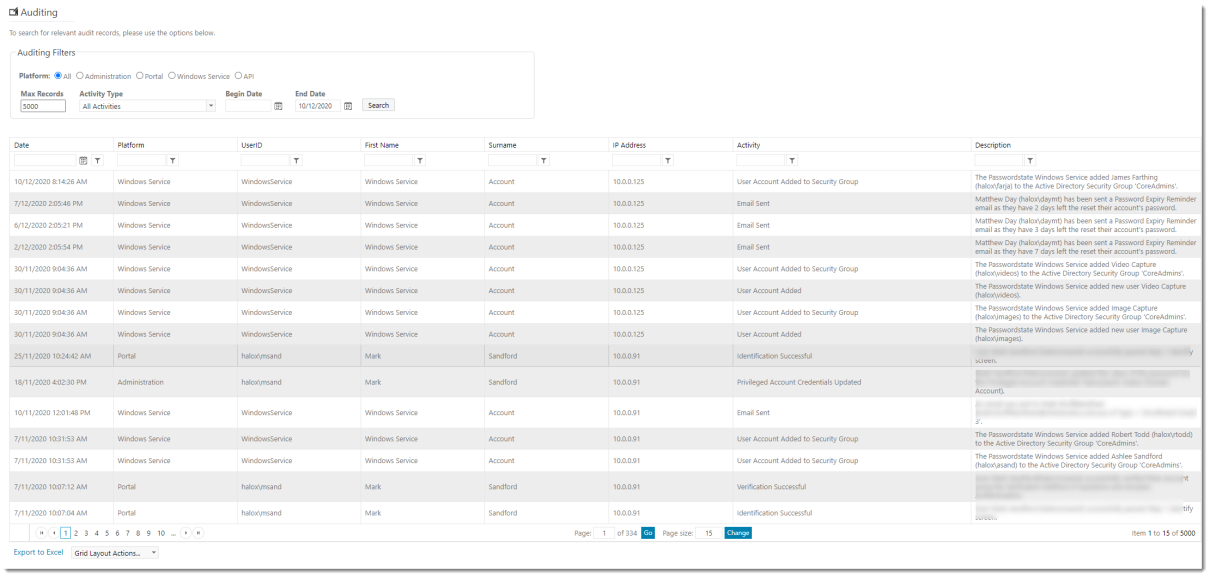




4.2 Auditing

The Auditing screen allows for real-time reporting of all audit events related to the Password Reset Portal.

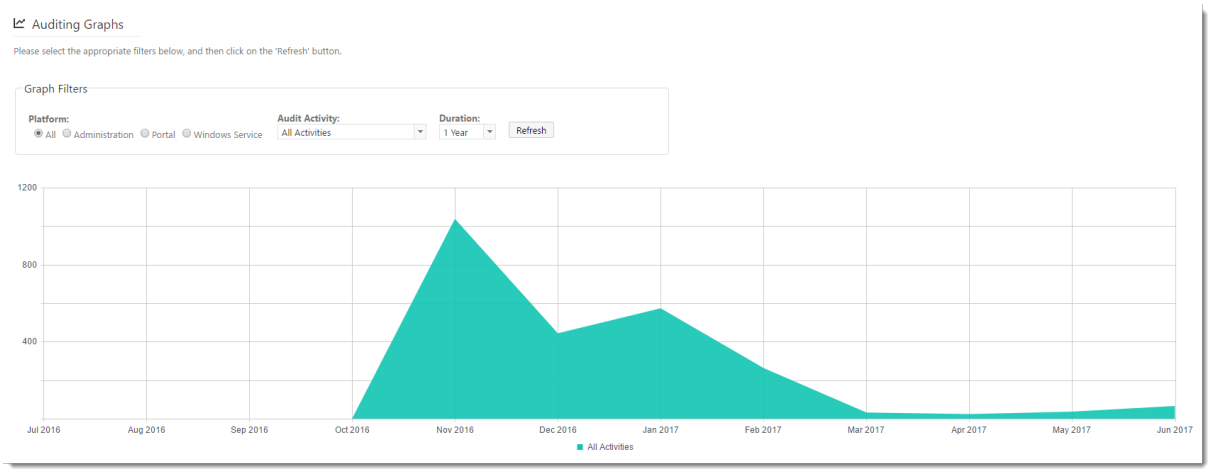
There are multiple filtering options available, including each of the different platforms (Administration, Portal, Windows Service), as well as different Activity Types and date ranges.



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

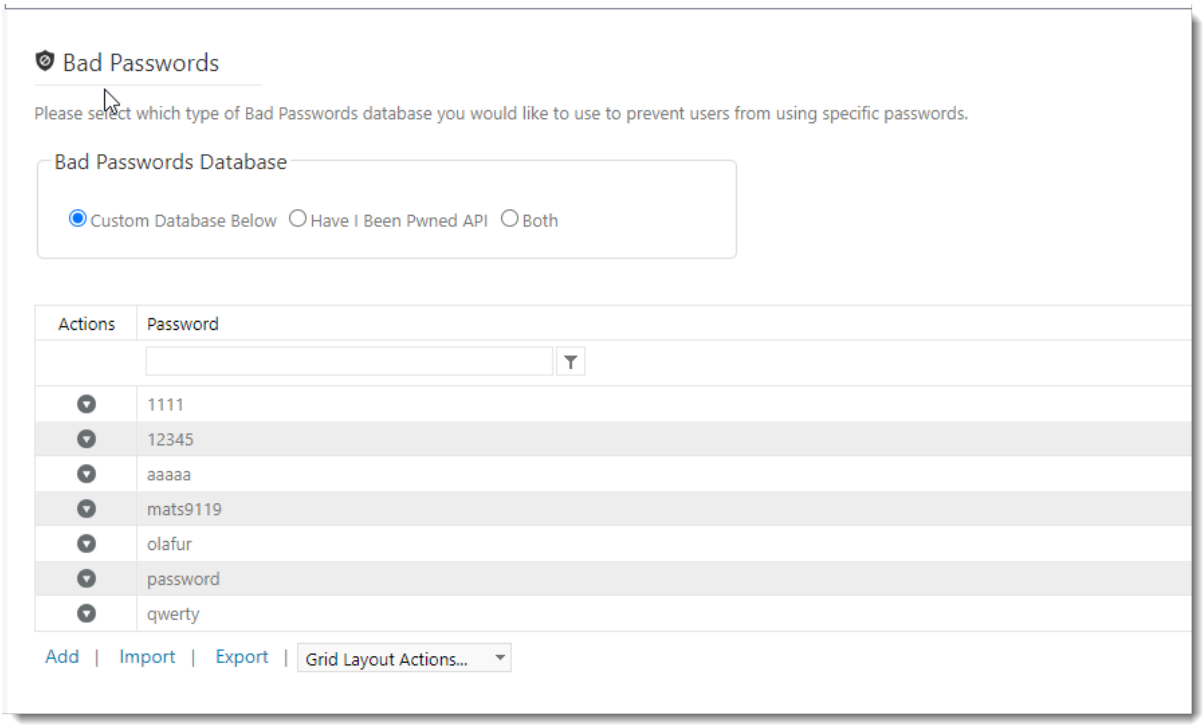
If you would like to prevent users from using certain Passwords when resetting their Active Directory account, you can use the Bad Passwords feature for this.

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 - https://haveibeenpwned.com/. This is a list of known password from various security breaches

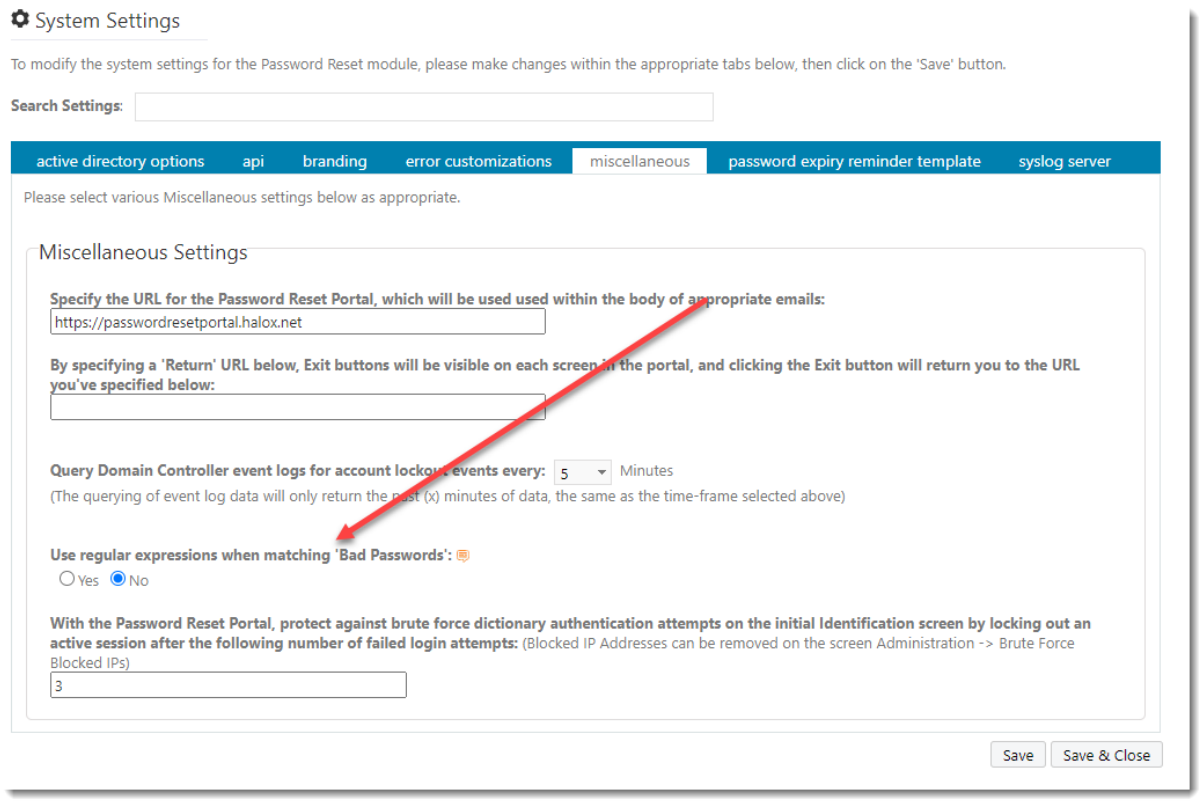
across the globe. If using this feature, your web server hosting the Passwordstate Reset Portal must be able to make calls to the internet.

- Or you can use both



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.



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.

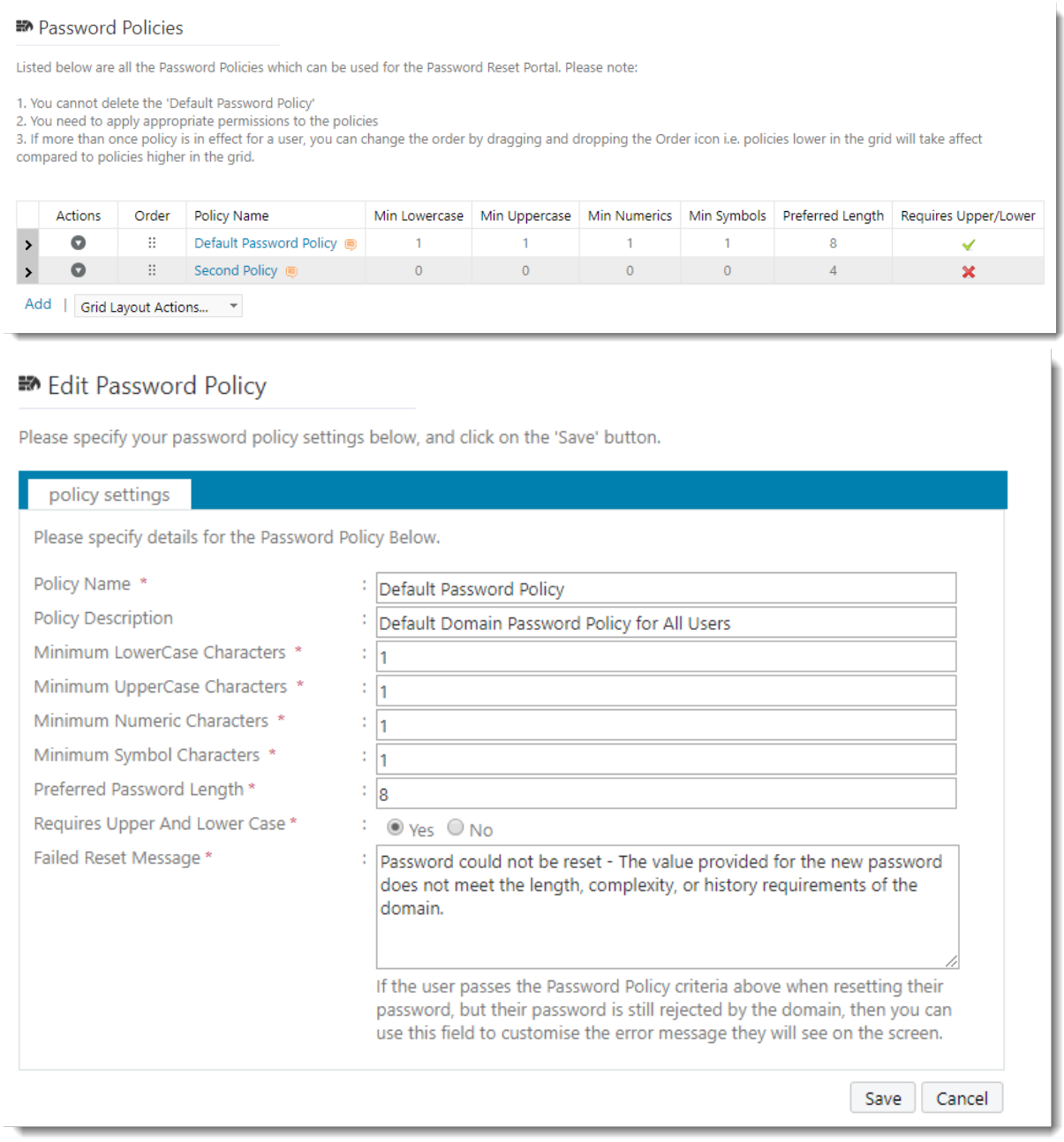
The type of criteria you can specify is:

- 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.



4.6 Privileged Account Credentials

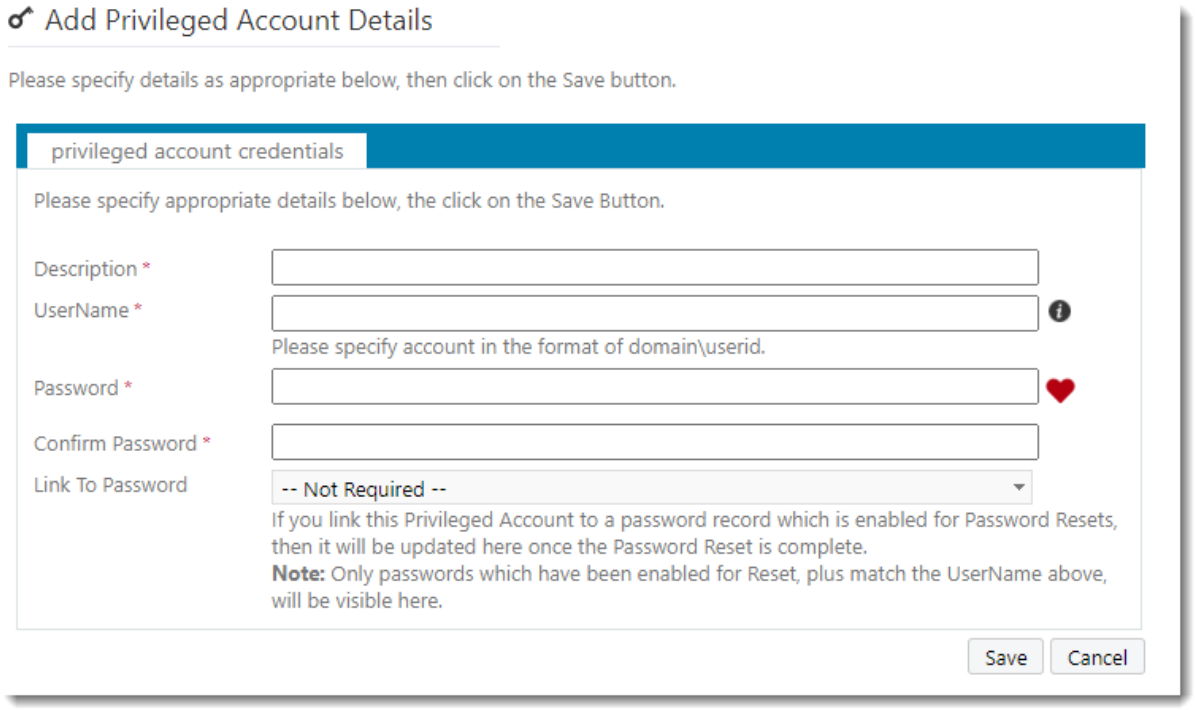
Privileged Account Credentials are used for two things with the Password Reset Portal:

- To allow unlocks and resets of user's Active Directory Domain accounts

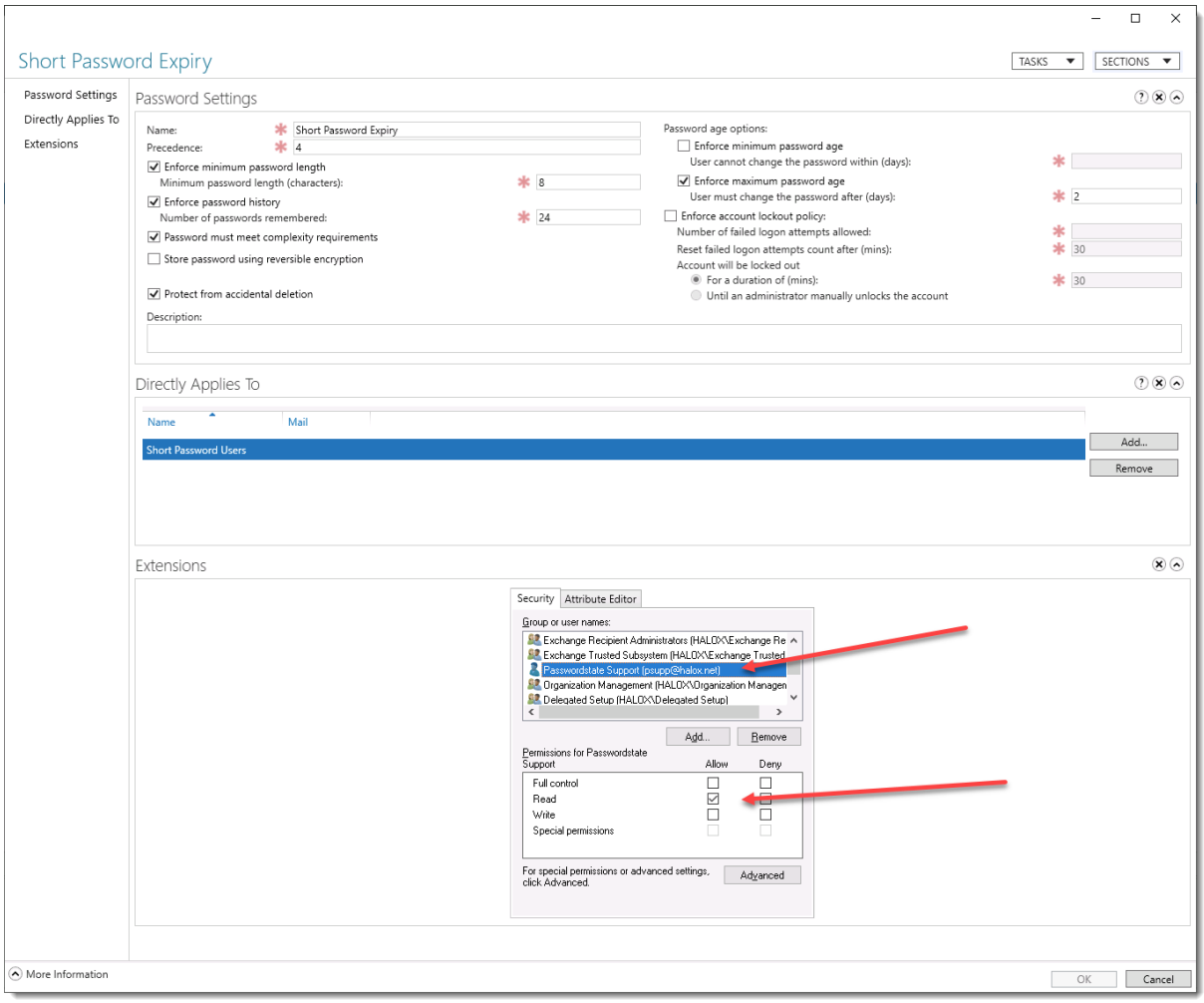
- To allow Passwordstate to query Event Logs on Domain Controllers for bad login attempts, or account lockouts

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.



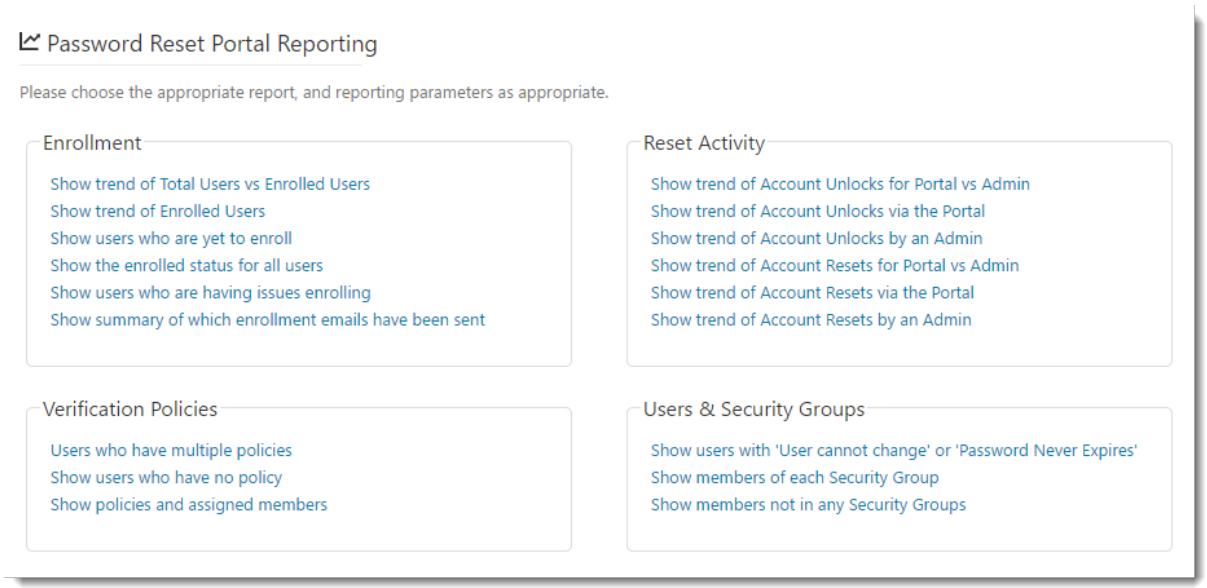
If you use any Fine Grain Password Policies in your organization, then you're privileged account credential also needs access to the policy in order to read certain attributes from it. Below is a screenshot of where this can be applied, if permissions do not already exist.

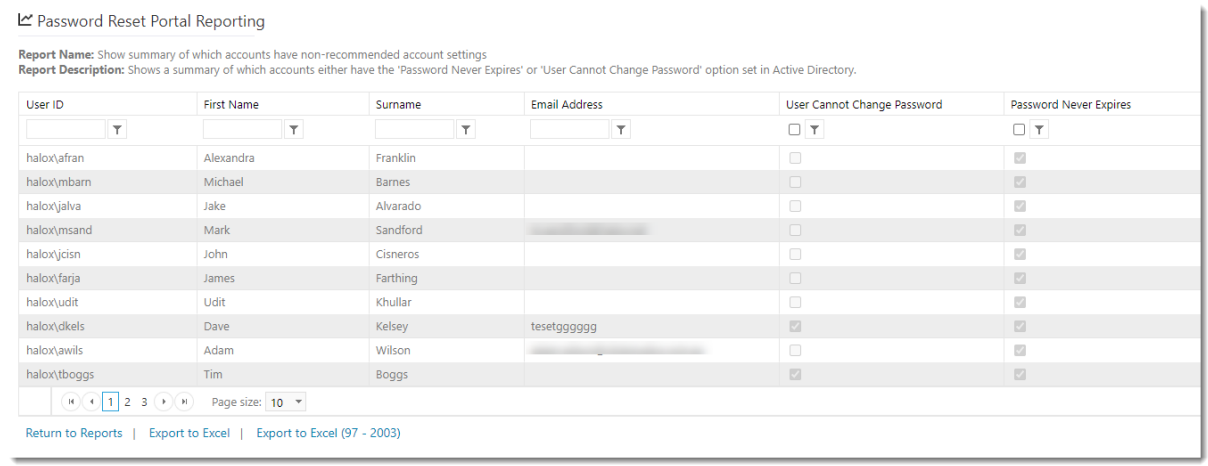


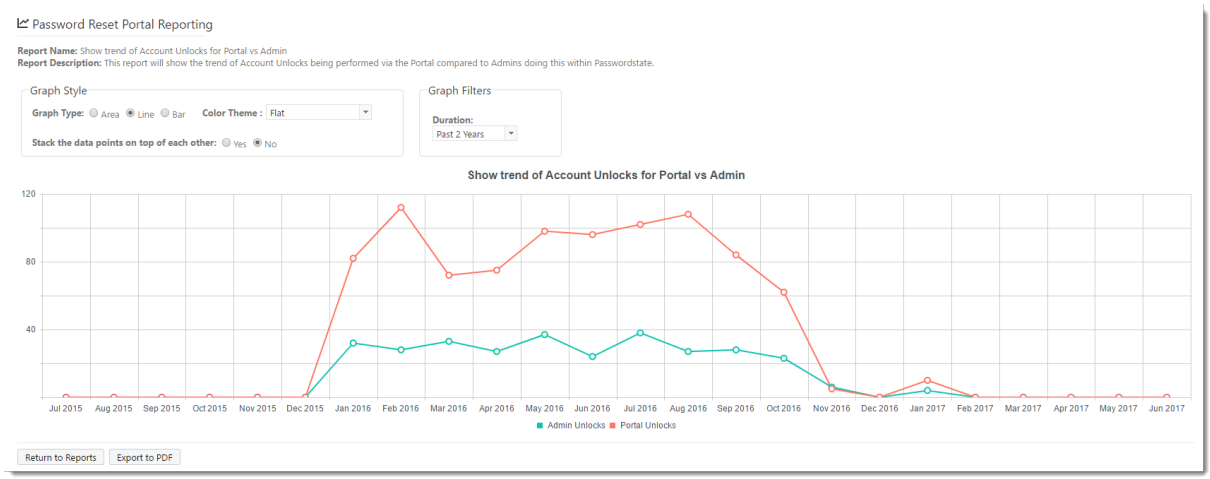
4.7 Reporting

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.



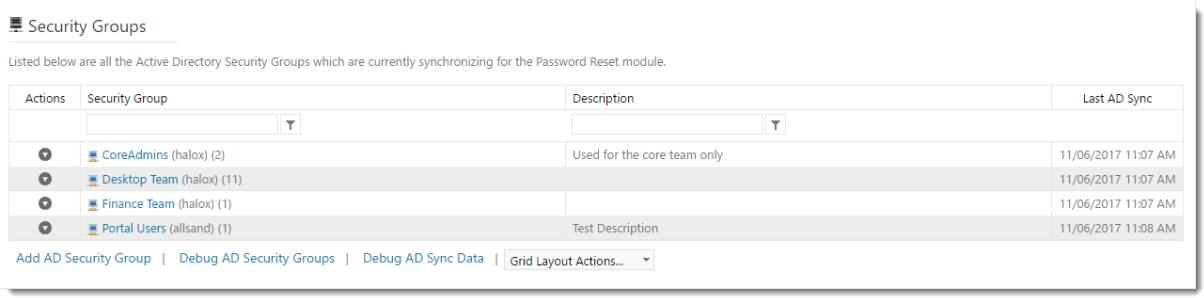




4.8 Security Groups

It is recommended that you use Active Directory Security Groups to apply permissions to Verification Policies. 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.



Nested Security Groups

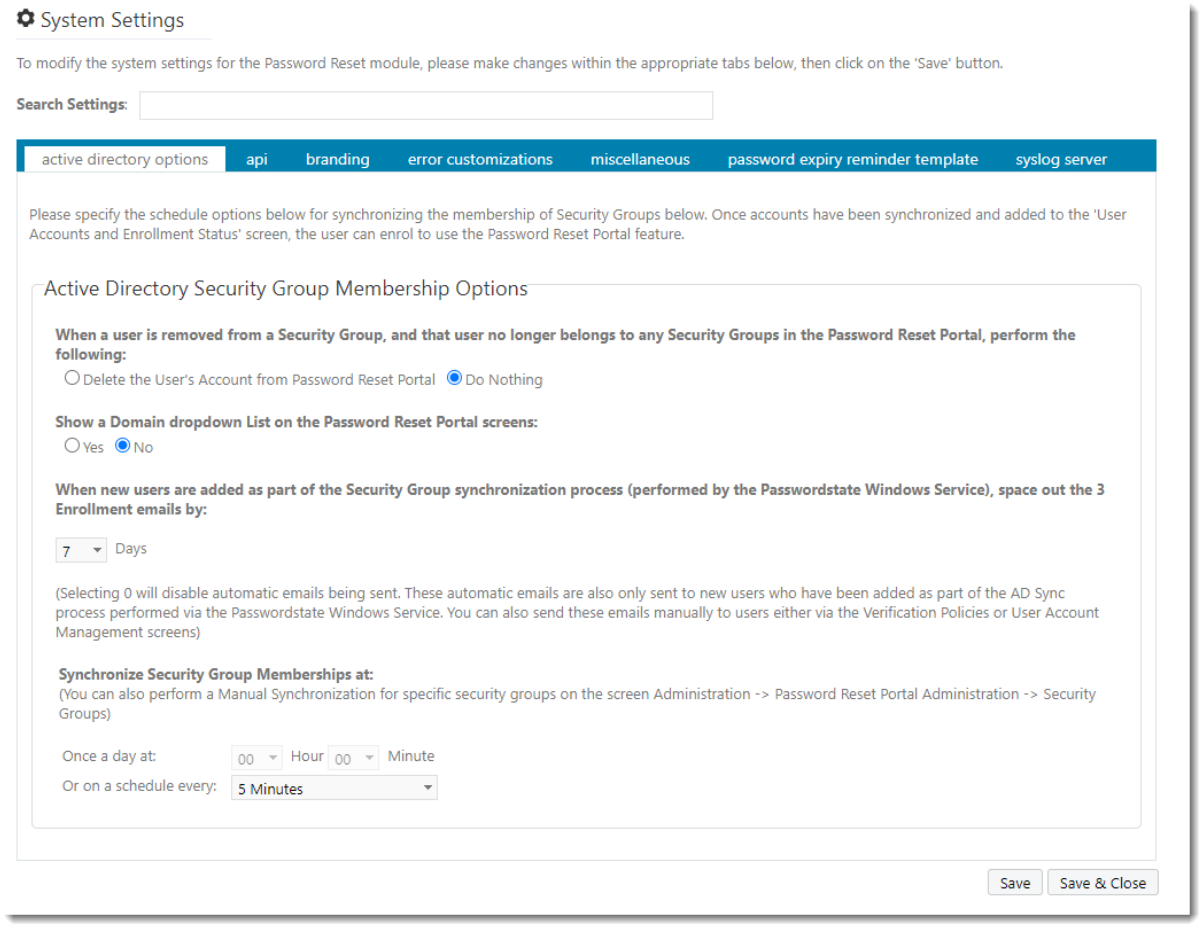
Nested Security Groups are supported in Passwordstate, but we do not maintain the nesting structure of those security groups. Instead, all the members of the nested Security Groups, will show in Passwordstate as members of the "parent" security group.

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.

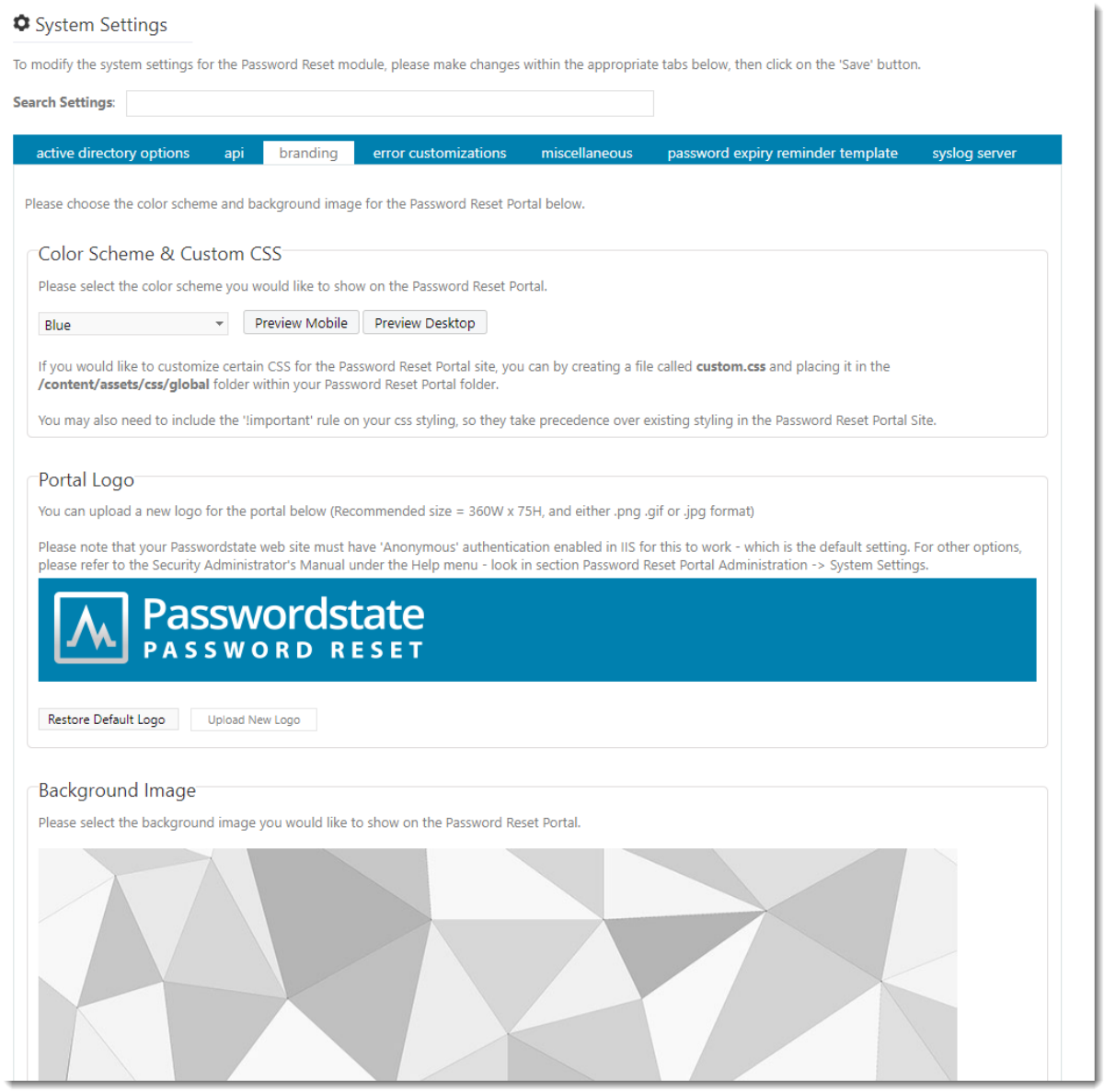


Branding

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.

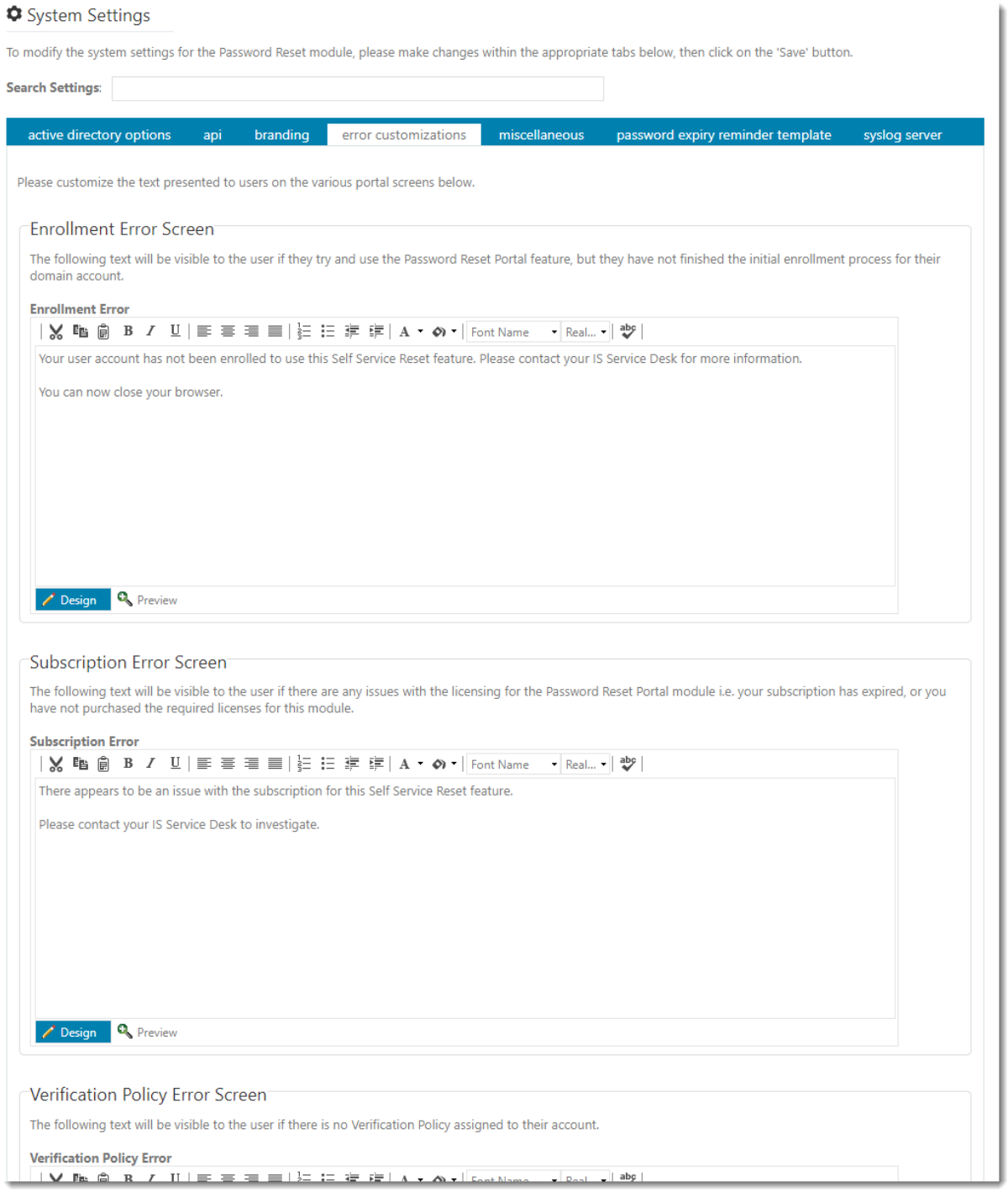
Note 1: In order to use the custom logo feature, 'Anonymous' authentication must be enabled on your Passwordstate web site. If this is not the case, please refer to Note 2

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.



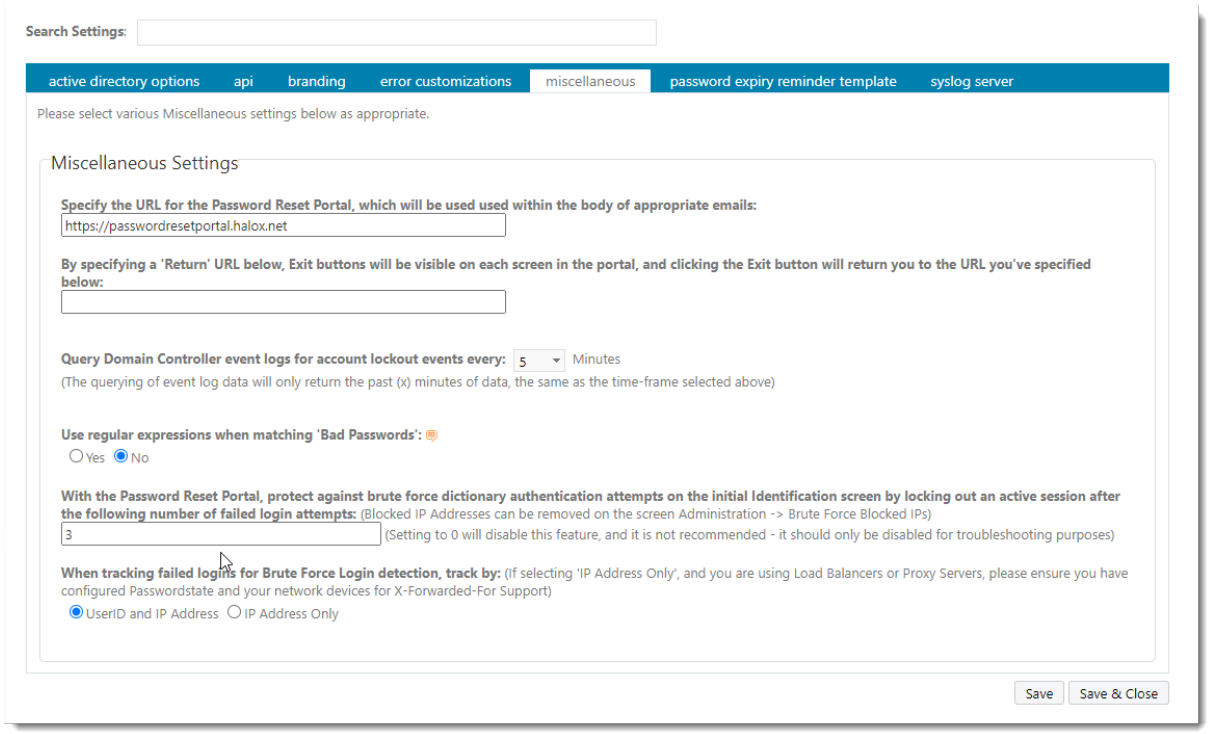
Error Customizations

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.



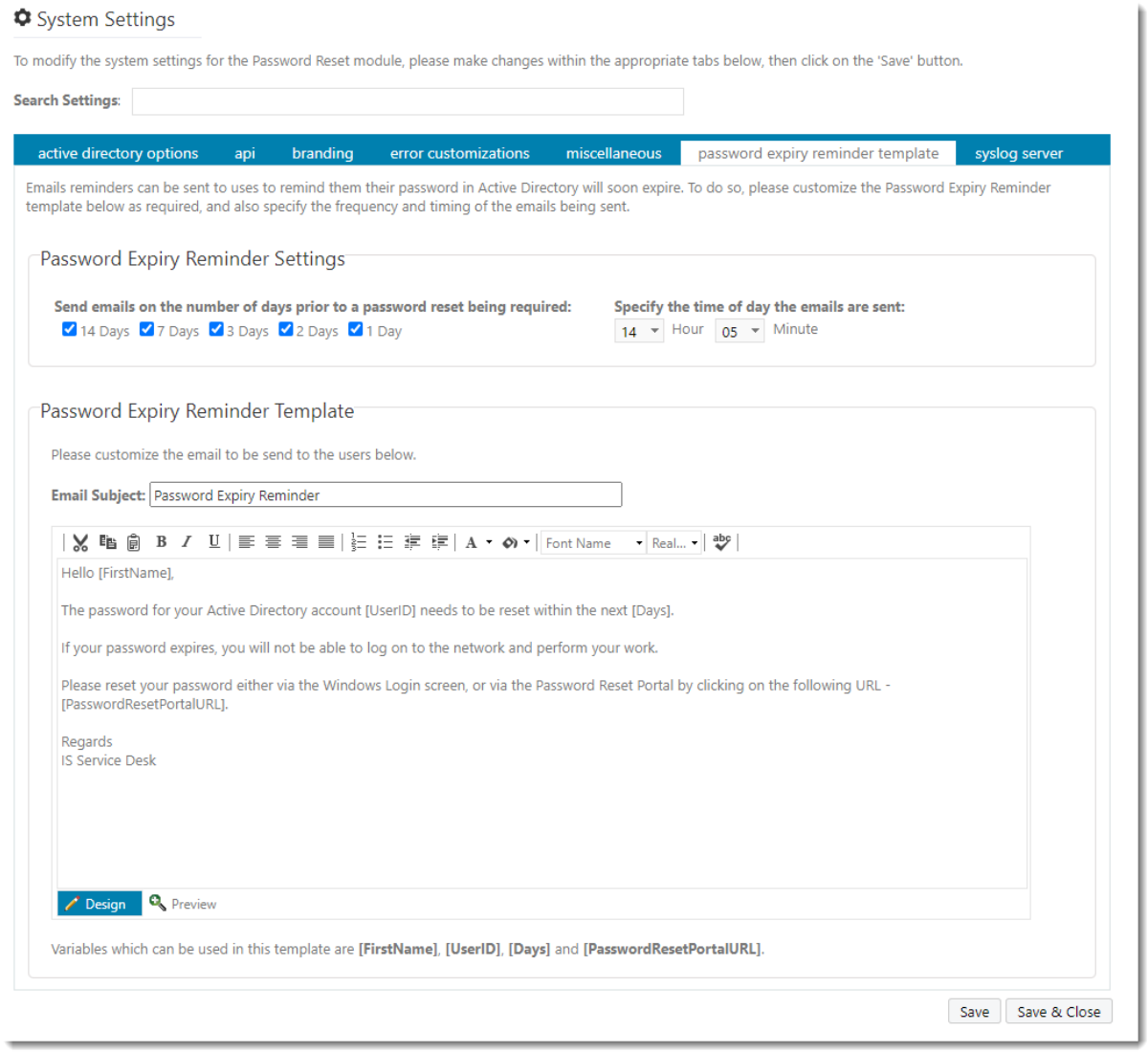
Miscellaneous

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.



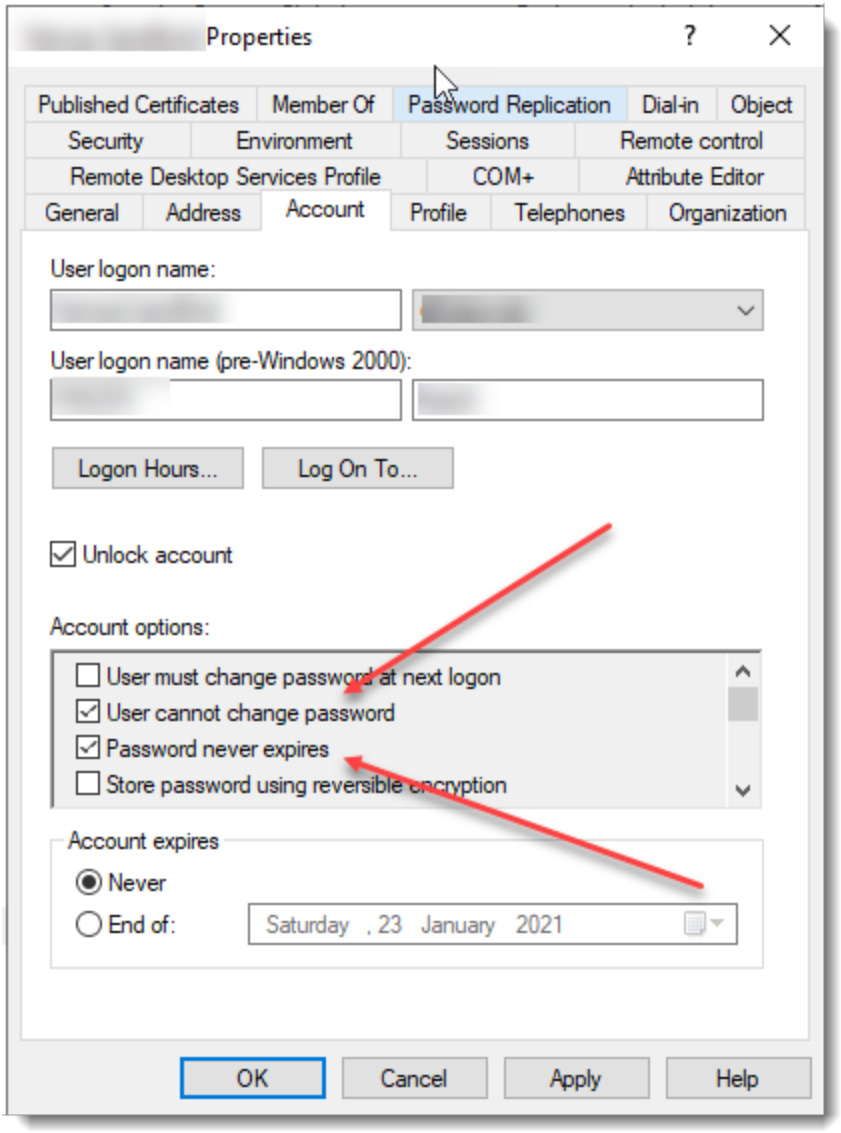
Password Expiry Reminder Template

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.



For users to receive this email notification, certain event must be met:

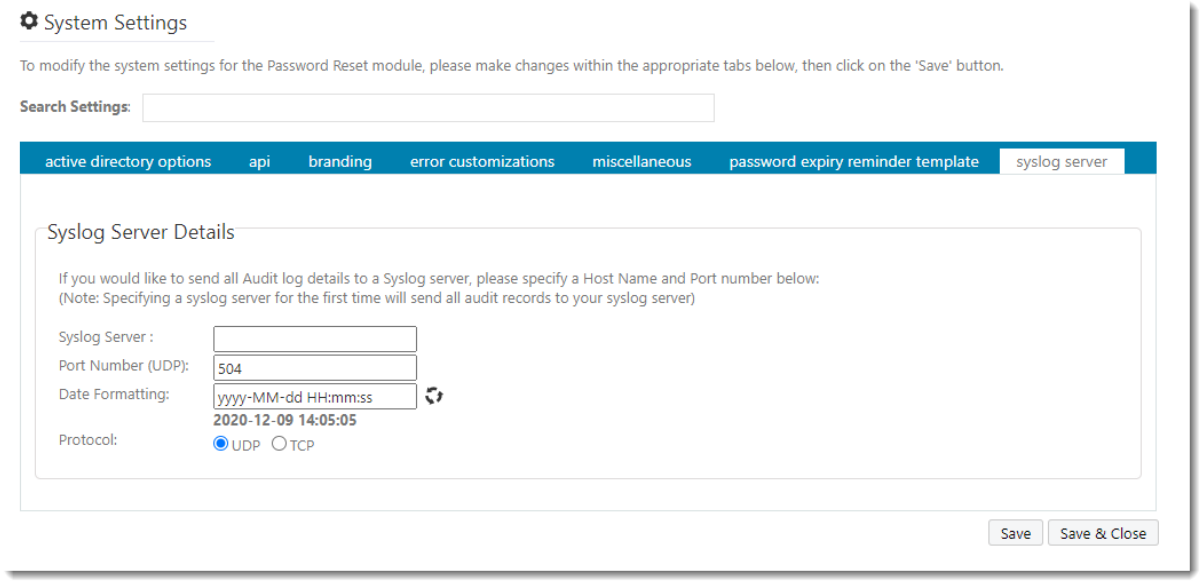
- Their account must be listed on the User Account Management screen
- They must have an email address associated with their account
- And both of the options you see in the screenshot below **must not be selected**



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.



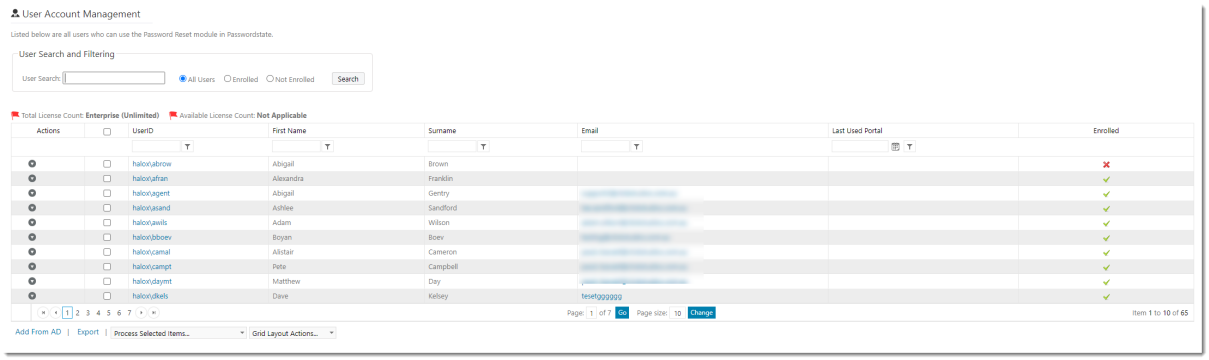
4.10 User Account Management

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)

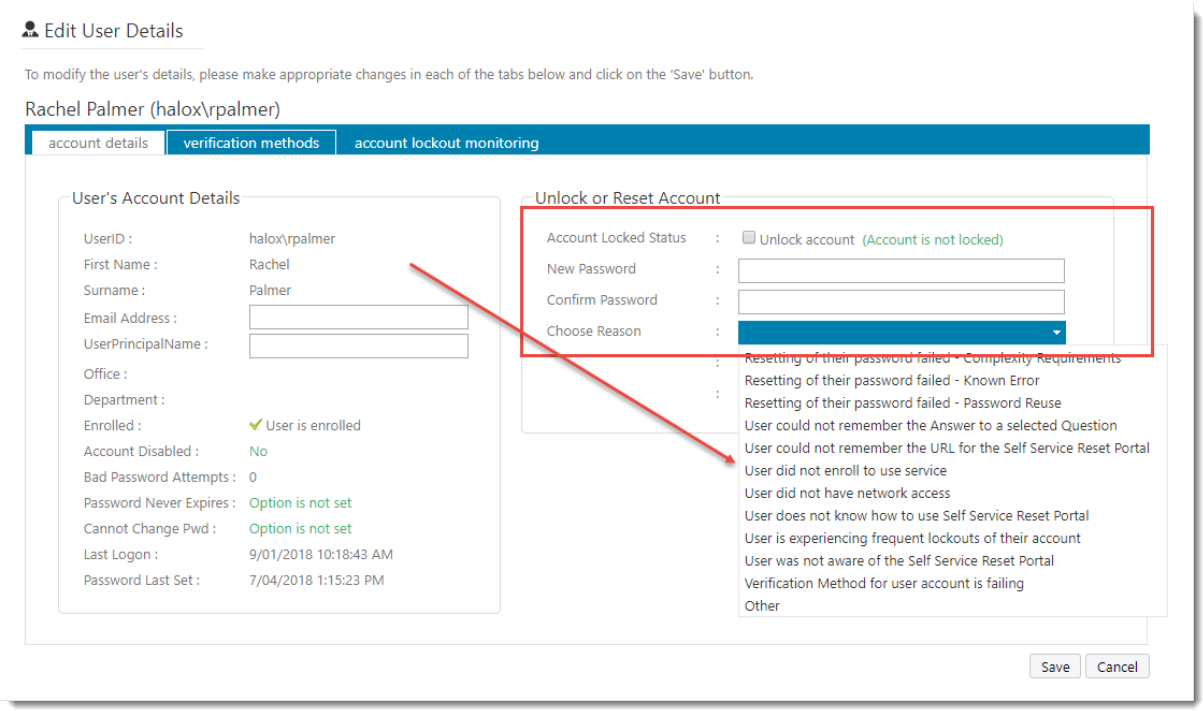
User Account Attributes
SAMAccountName
givenname
sn (Surname)
name
objectSid
mail
objectCategory=person
objectClass=user
user.UserCannotChangePassword
user.PasswordNeverExpires
user.LastPasswordSet
user.UserPrincipalName



Account Details

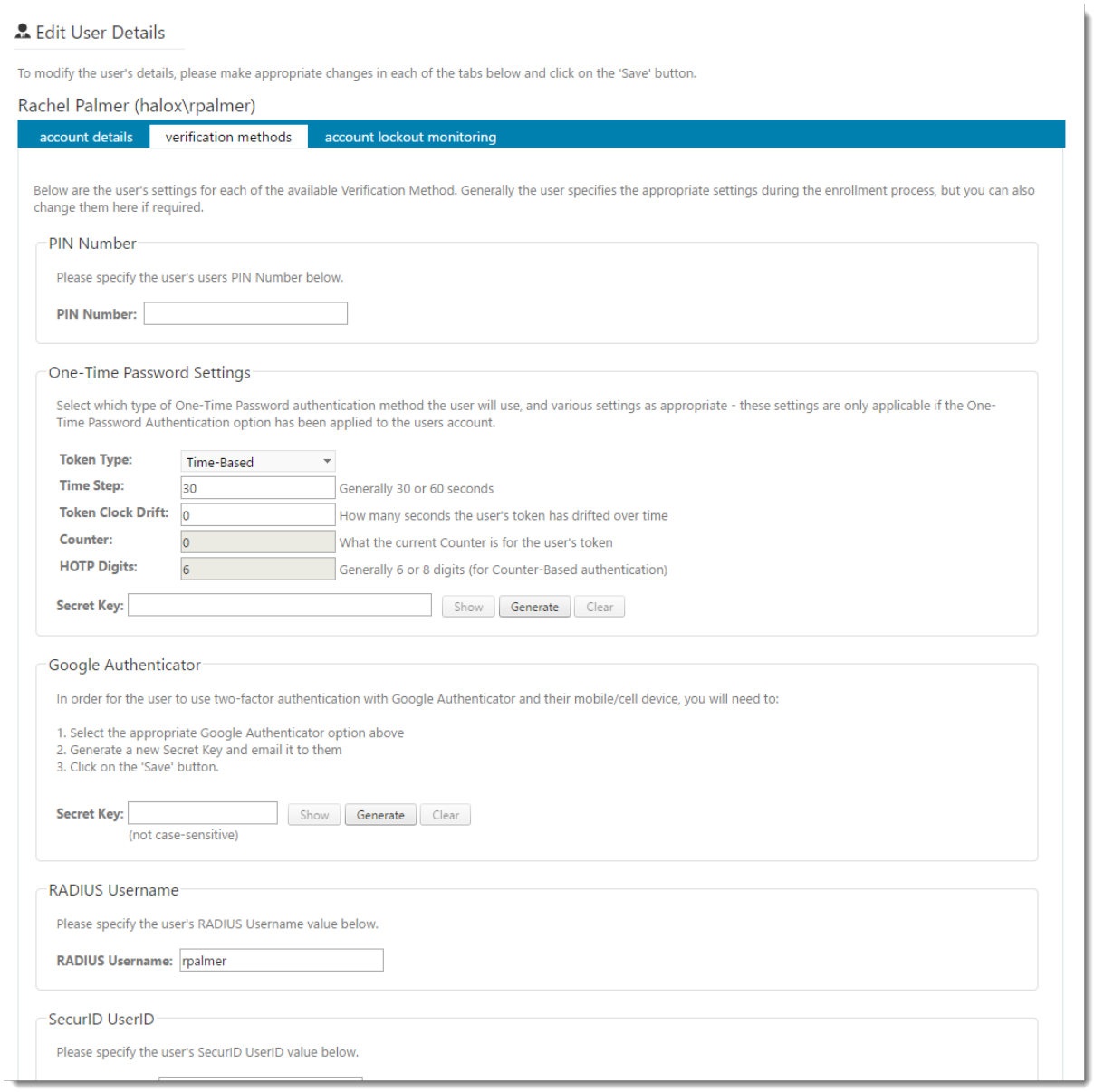
On the Account Details tab for a user, you can see various attributes for their Active Directory account, as well as unlock/reset their account if required.

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.



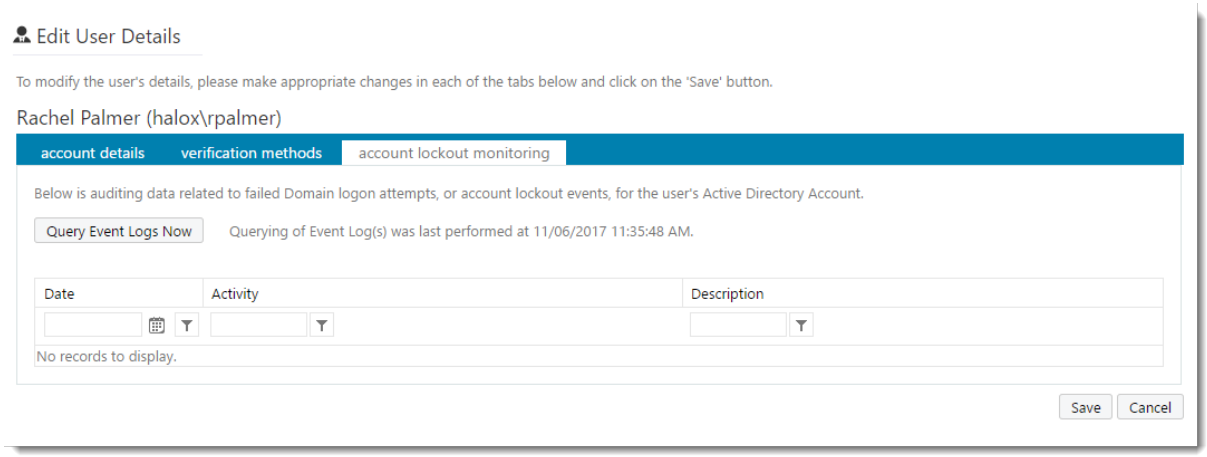
Verification Methods

The Verification Methods tab allows an Administrator of Passwordstate to specify settings for any one of the available Verification Policies 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.



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.



4.11 Verification Policies

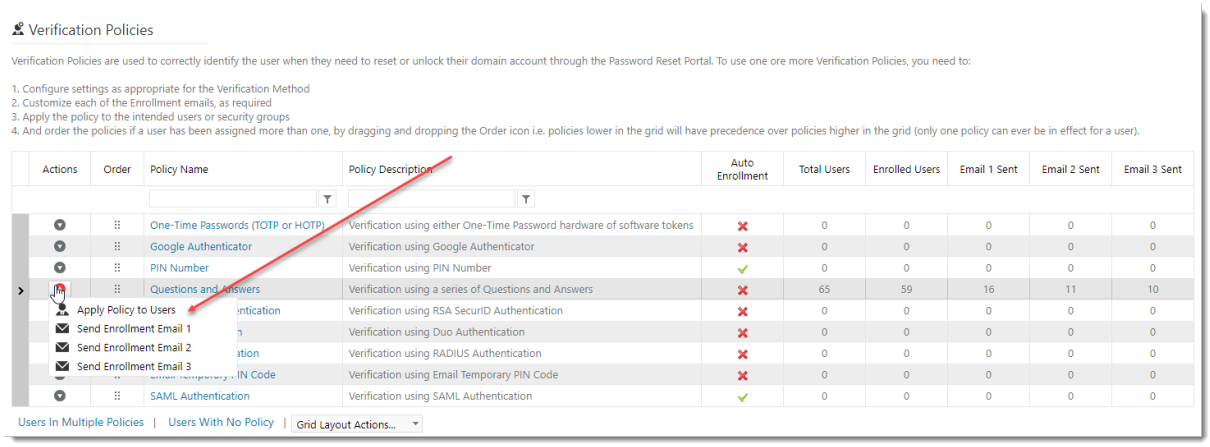
Verification Policies are used to 'identify' the user when using the Password Reset Portal. The basic 3 step process is:

- 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.

Note 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.



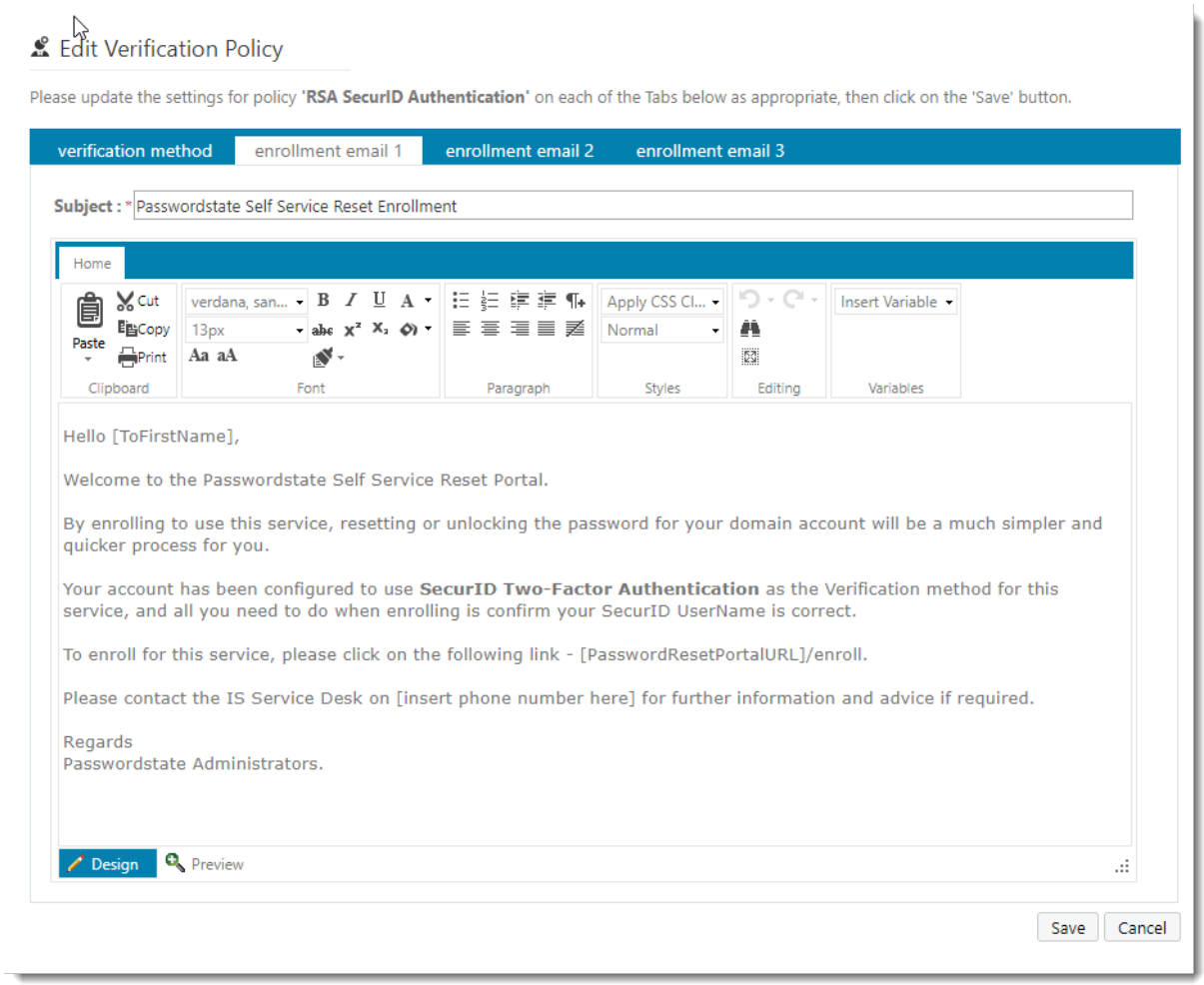
User Initiated Enrollment

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



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:

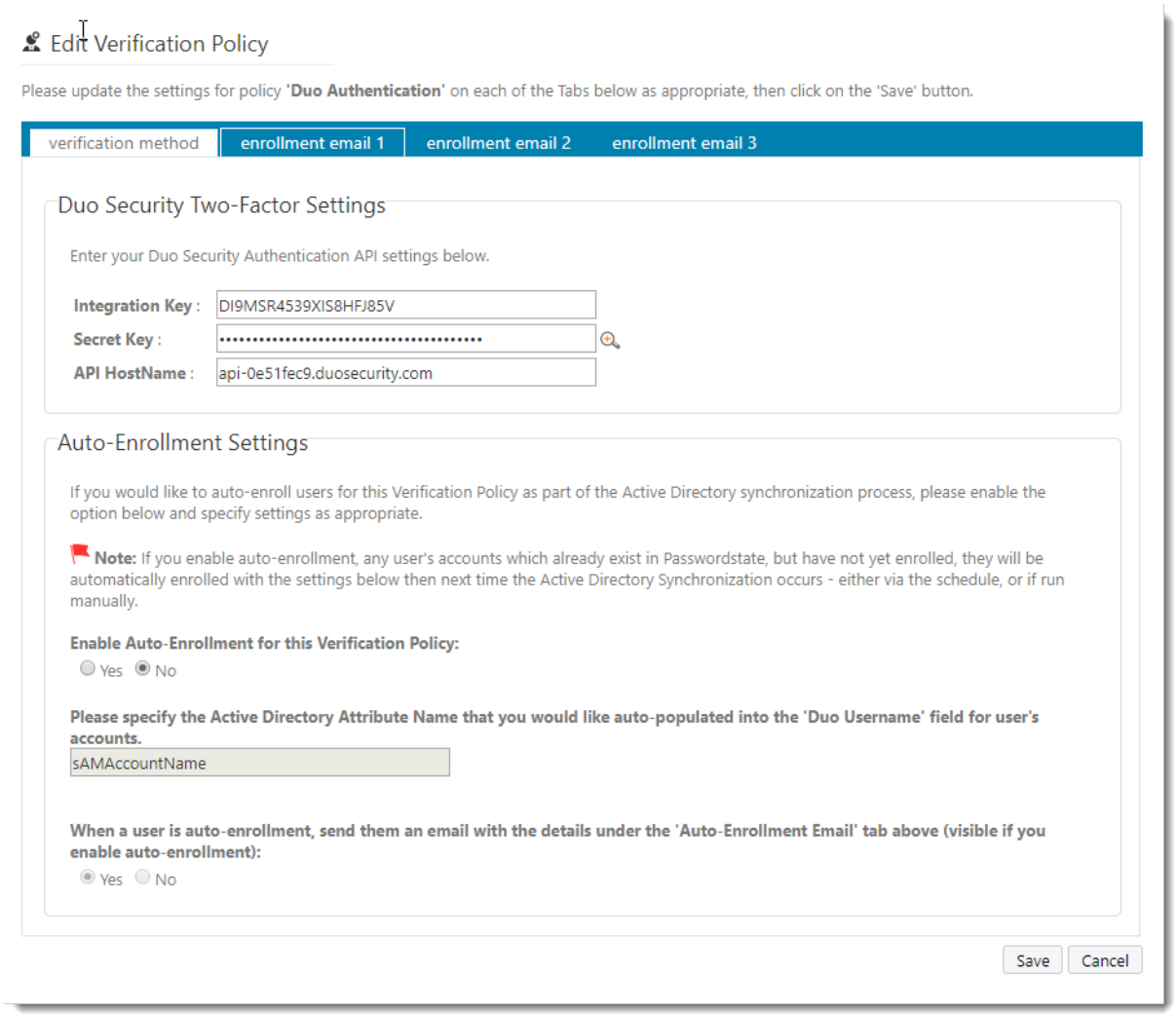
- By specifying various settings on each Verification Policy, when the scheduled synchronization of Active Directory Security Groups occurs, then auto-enrollment will happen for any accounts not already enrolled. This process is initiated by the Password Windows Service, and the schedule for this can 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/

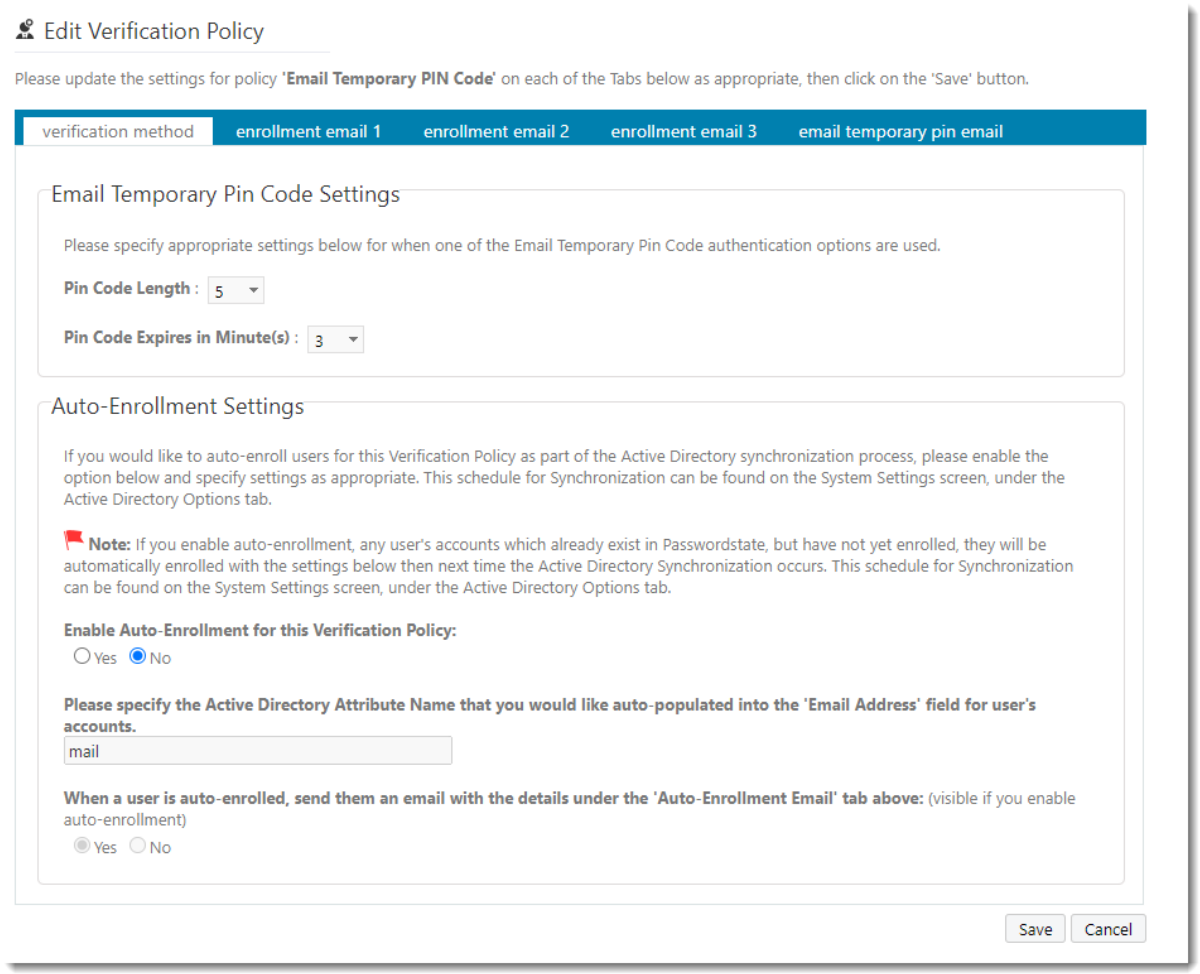
For auto-enrollment, by default the 'sAMAccountName' Active Directory Attribute is queried for the user's account, but this can be changed to any AD attribute you like.



4.11.2 Email Temporary PIN Code

Emailing a Temporary PIN Code can also be used, and will only be valid for a specified amount of time.

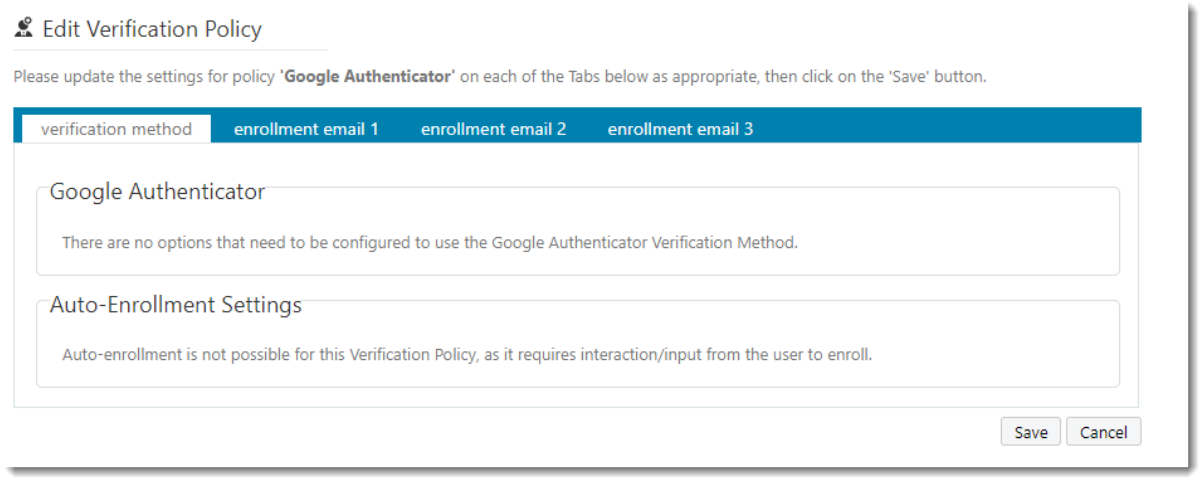
For auto-enrollment, by default the 'mail' Active Directory Attribute is queried for the user's account, but this can be changed to any AD attribute you like.



4.11.3 Google Authenticator

Google Authenticator is a free two-factor authentication option which can be used on most mobile phones, and desktops.

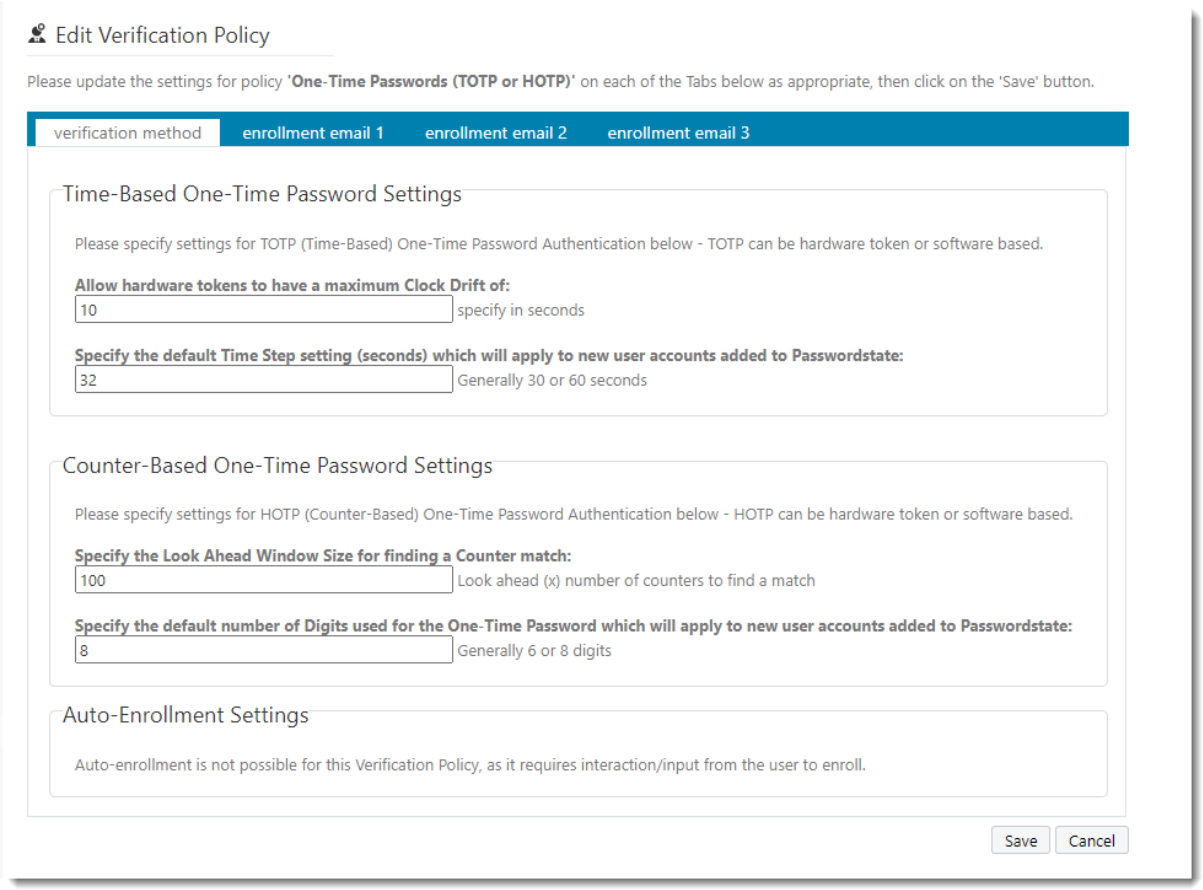
Note: There is no Auto-Enrollment option available for this Verification Policy.



4.11.4 One-Time Passwords (TOTP or HOTP)

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

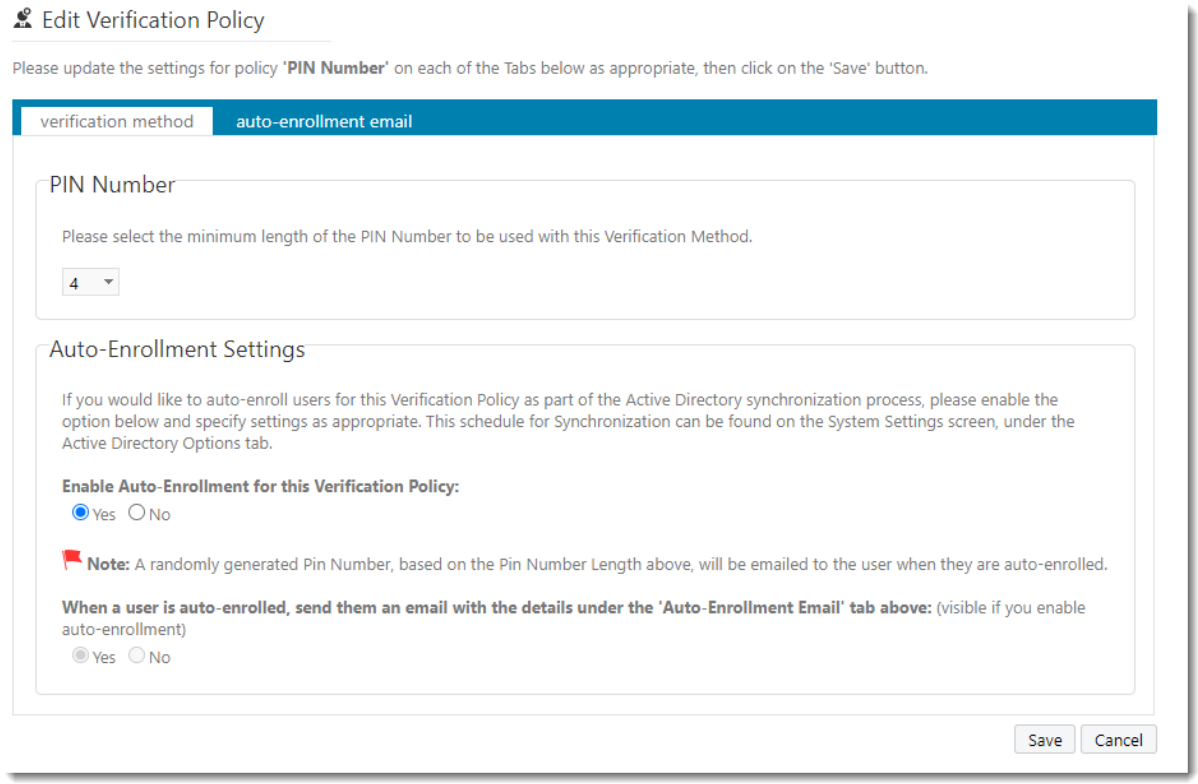
Note: There is no Auto-Enrollment option available for this Verification Policy.



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.

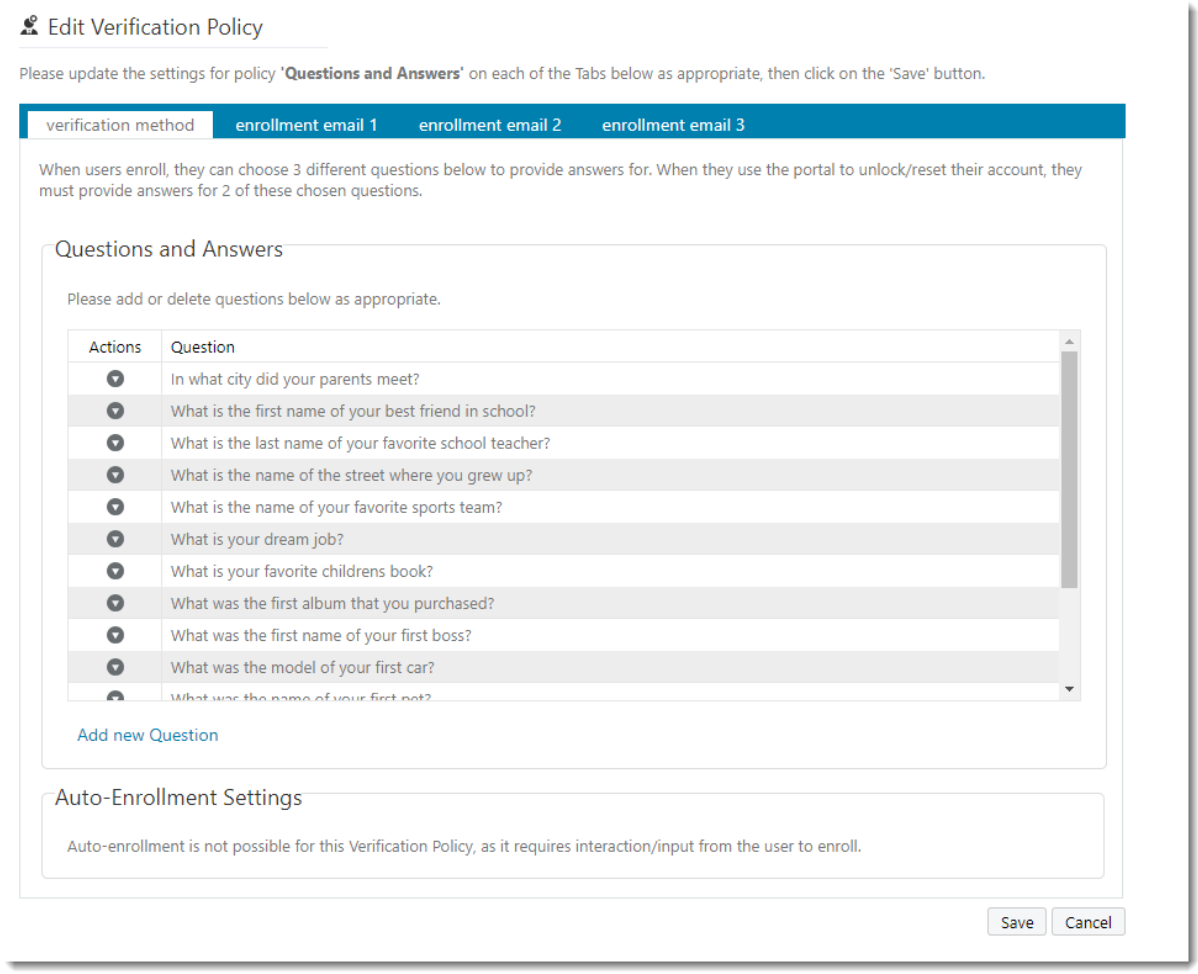


4.11.6 Questions and Answers

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.

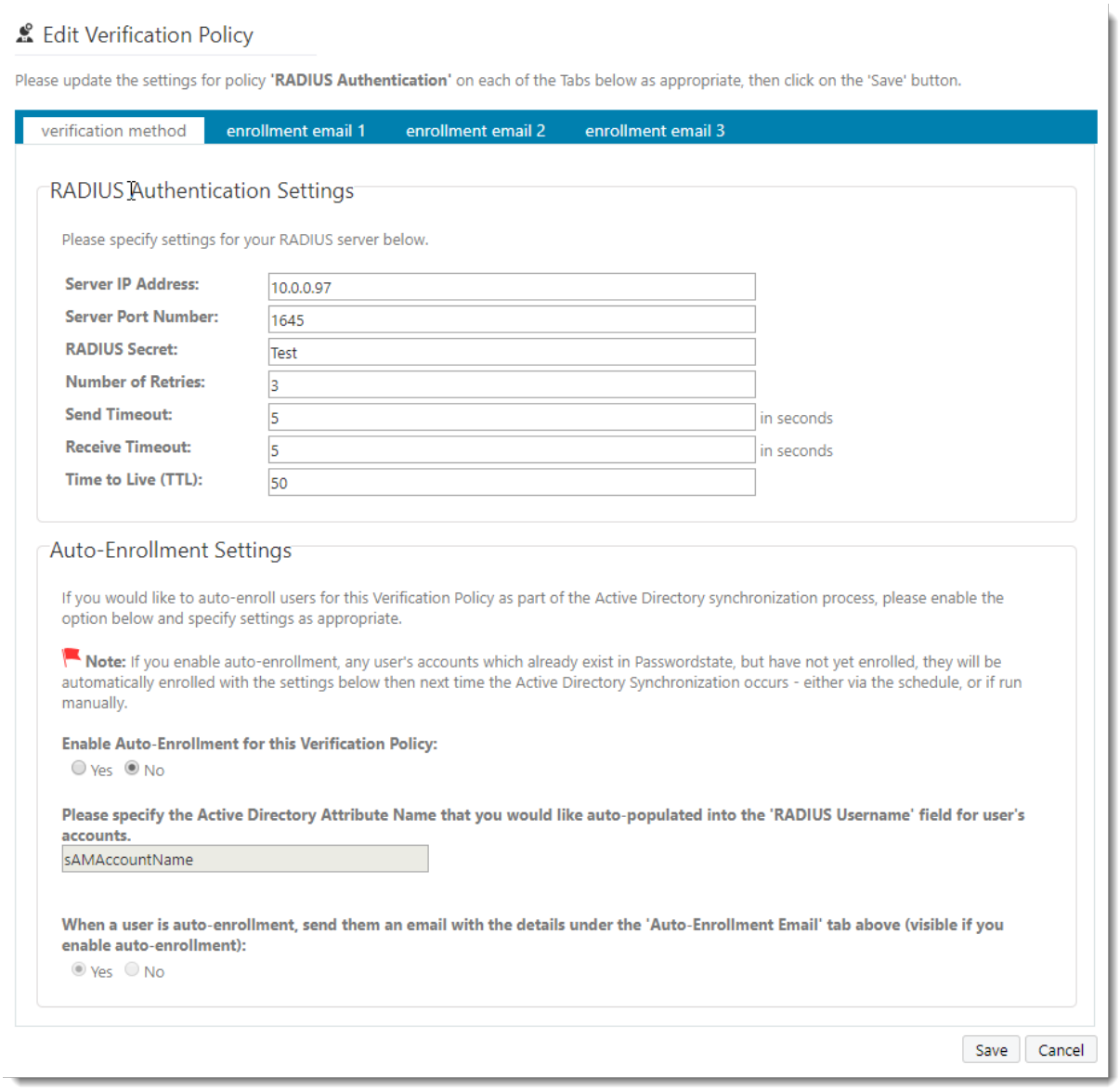
You can also add your own questions, or delete any of the default questions.



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.

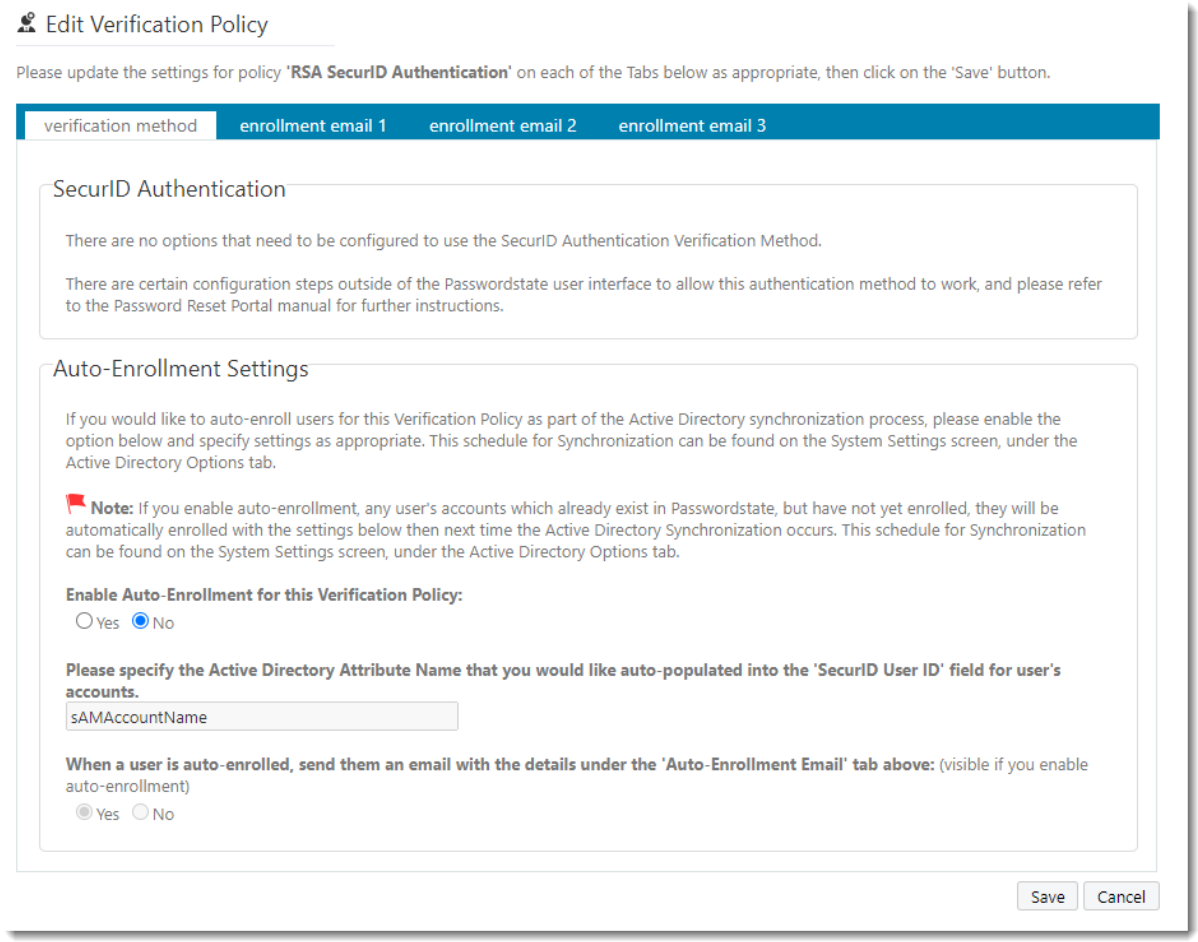


4.11.8 RSA SecurID Authentication

RSA SecurID is a two-factor authentication option (hardware or software tokens) provided by EMC - https://www.rsa.com/en-us/products/rsa-securid-suite

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.



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 - SAML2 Provider Examples

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
Identifier (Entity ID):	Audience Restriction - normally your Reset Portal URL - let's call it https://myportal.domain.com 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 Passwordstate_User SQL Account	Resetting the password for the SQL Account passwordstate_user
Recovery Emergency Access Password	Recover your Emergency Access Password, if needed, to resolve Unauthorized Web Server message

5.1.1 Passwordstate Web Site Restore

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

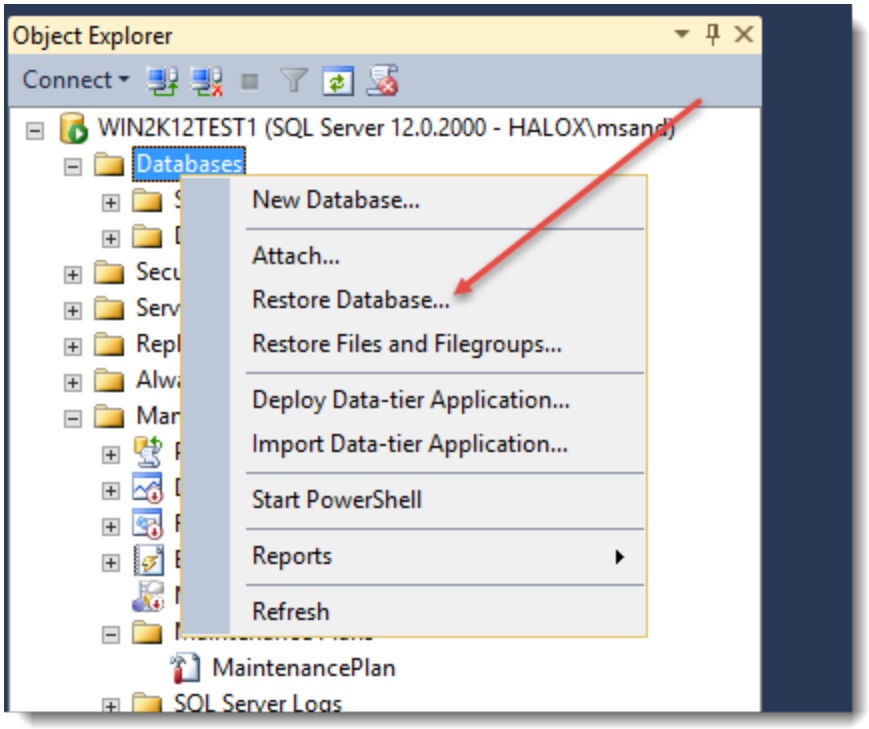
- Download the latest build of Passwordstate from here Click Studios's web site here - https://www.clickstudios.com.au/passwordstate-checksums.aspx. Please confirm the checksum of the file you are downloading using the PowerShell command of: Get-FileHash passwordstate.zip -Algorithm SHA256
- Unzip the Passwordstate.zip file from your download above
- Use the following document as a guide for reinstalling the software - https://www.clickstudios.com.au/downloads/version9/Installation_Instructions.pdf
- Before you open your browser and point it at the site for the first time, you need to restore a copy of your web.config file over the top of the existing file which exists in the folder c:\inetpub\passwordstate. If you do not have a backup of this file, or you have encrypted the ConnectionString or AppSettings sections, then please follow these instructions for rebuilding this file with the correct configuration settings - Rebuilding the Web.config File. Note: if you are using the Backup feature in Passwordstate, the web.config file will be backed up and stored in your backup zip file
- If you also need to restore a copy of your database, then follow these instructions - Passwordstate Database Restore
- Now when you open your browser and navigate to the Passwordstate web site, you may see a screen which indicates that your new web server is "Not Authorised" to host the Passwordstate web site. This will occur if your server name has changed, or if you did not have a backup of your web.config file to use above. To fix this issue, you can simple enter your Emergency Access login password. If you have forgotten this password, please follow these instructions for contacted Click Studios so we can help you recovery it - Recovery Emergency Access Password

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

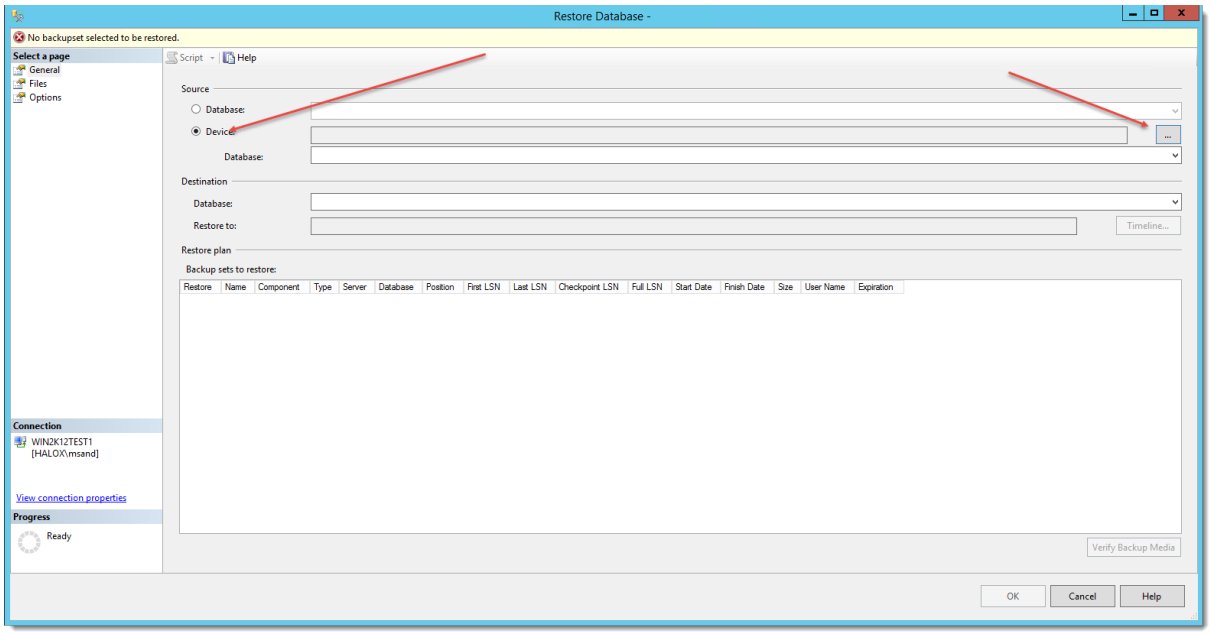
5.1.2 Passwordstate Database Restore

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

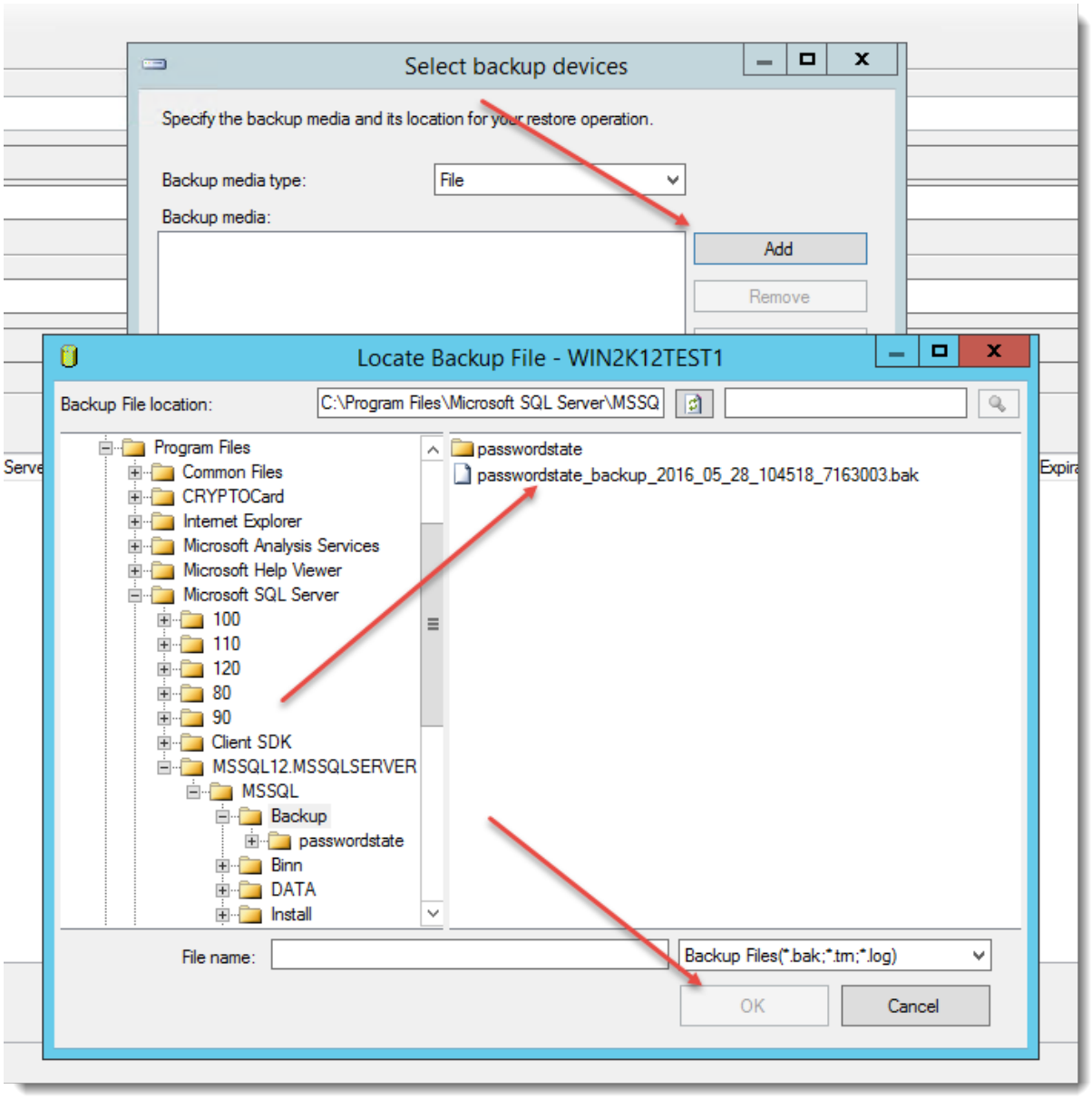
- Start SQL Server Management Studio
- Right click on 'Databases' and select 'Restore Database...'



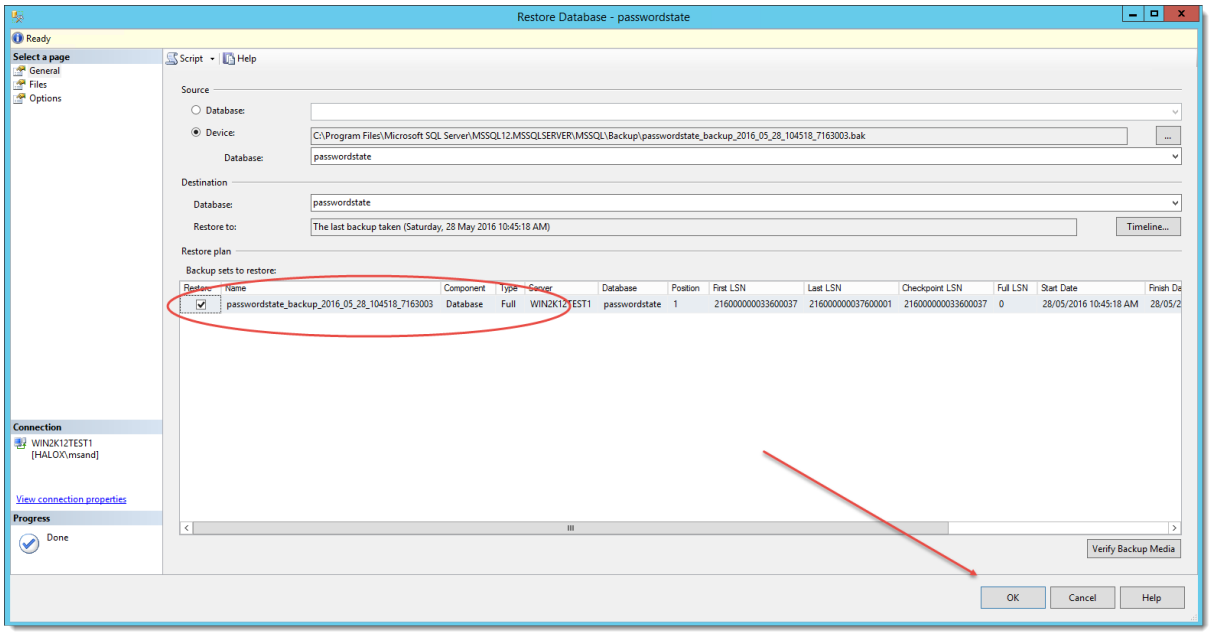
- Click on 'Device', and then on the Ellipsis button so you can select your database backup file



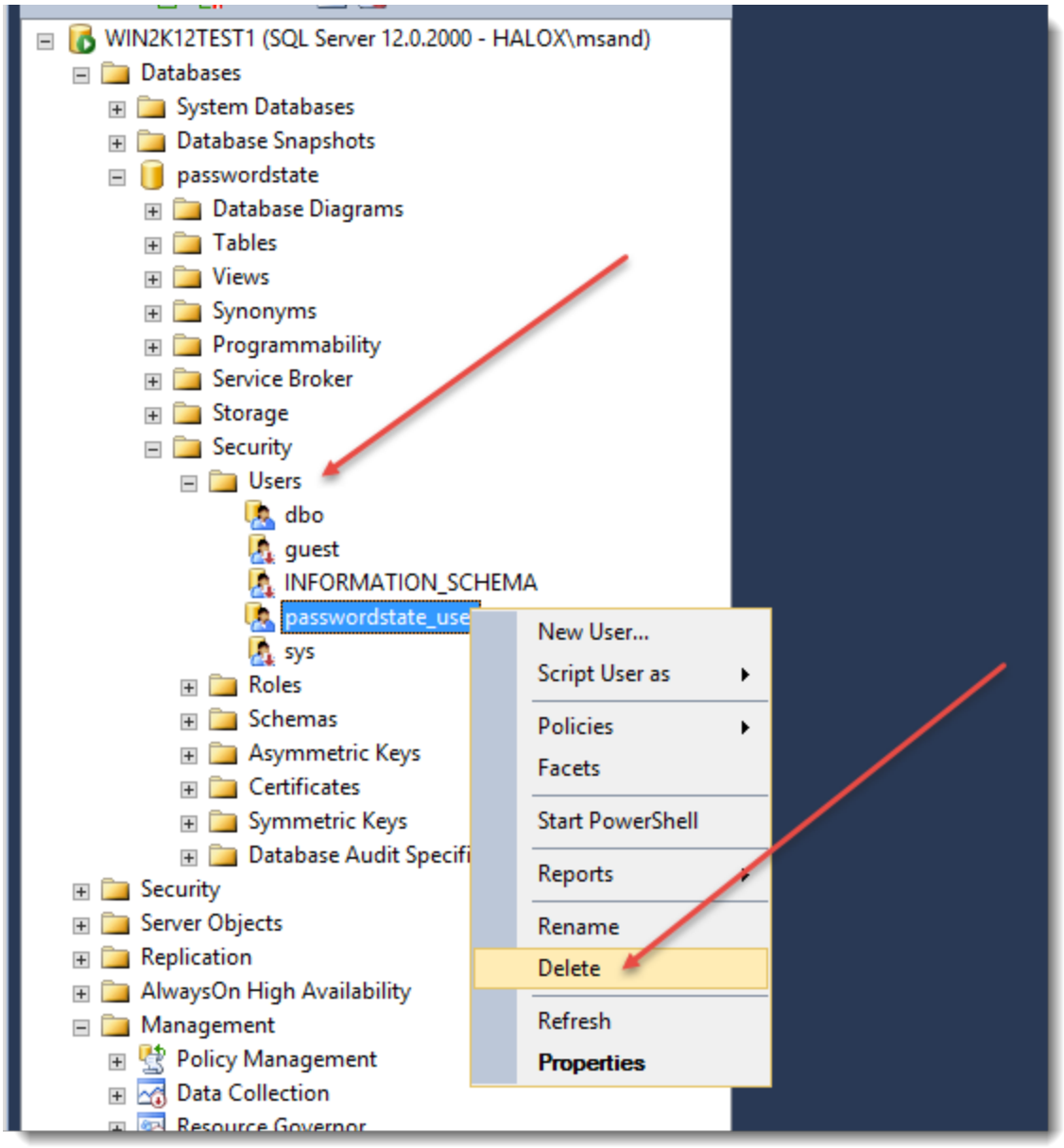
- Click on the 'Add' button and browse and select the location of your latest .bak file



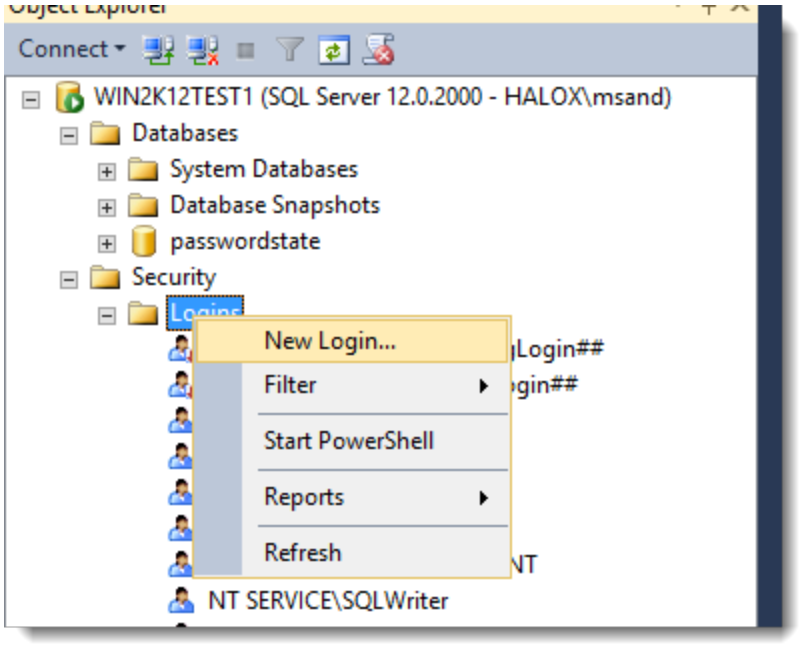
- Once the database is selected as per the screenshot below, click the 'OK' button to restore it

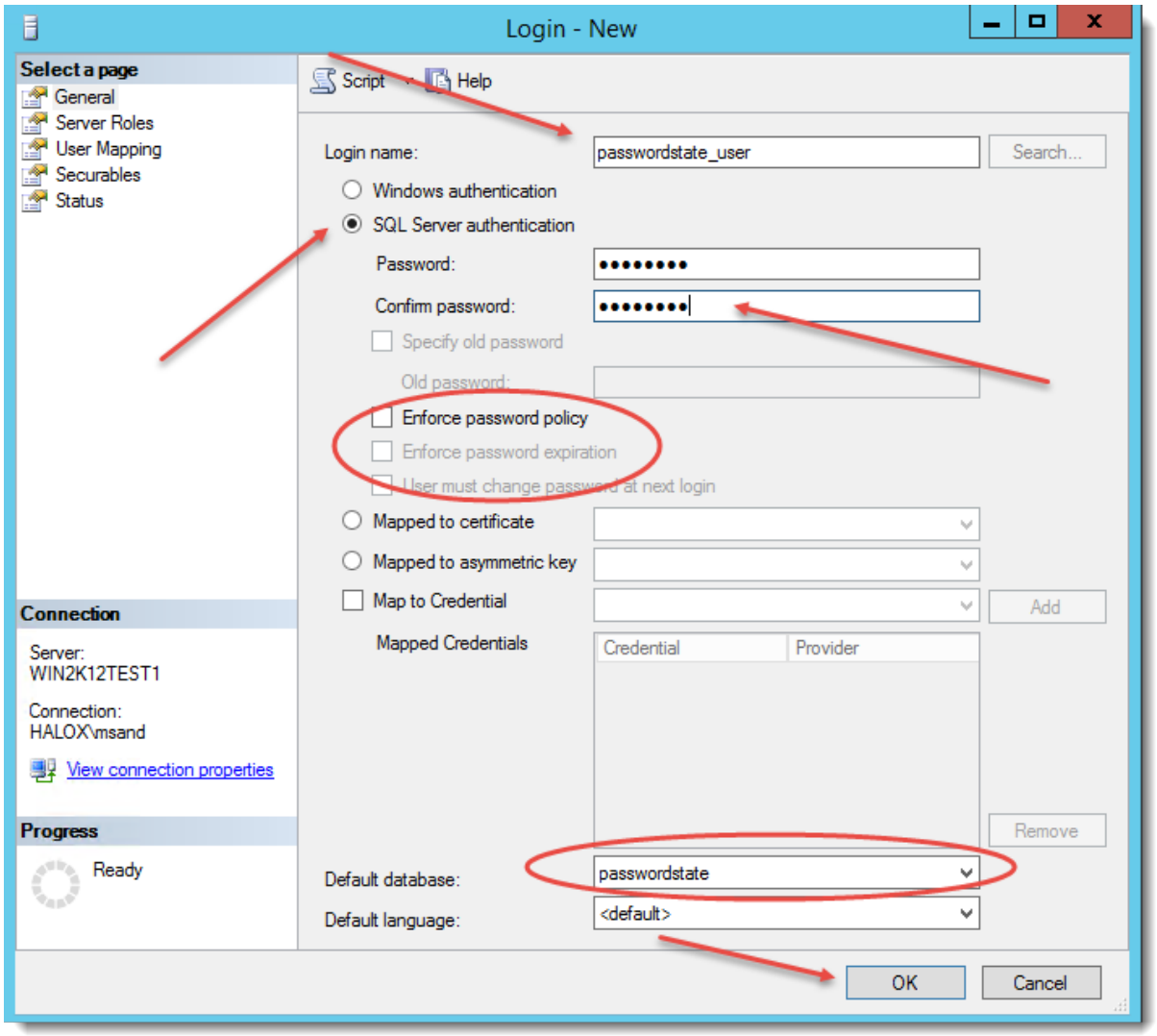


- Now expand the Security -> Users tree within the Passwordstate database, and delete the 'passwordstate_user' SQL Account

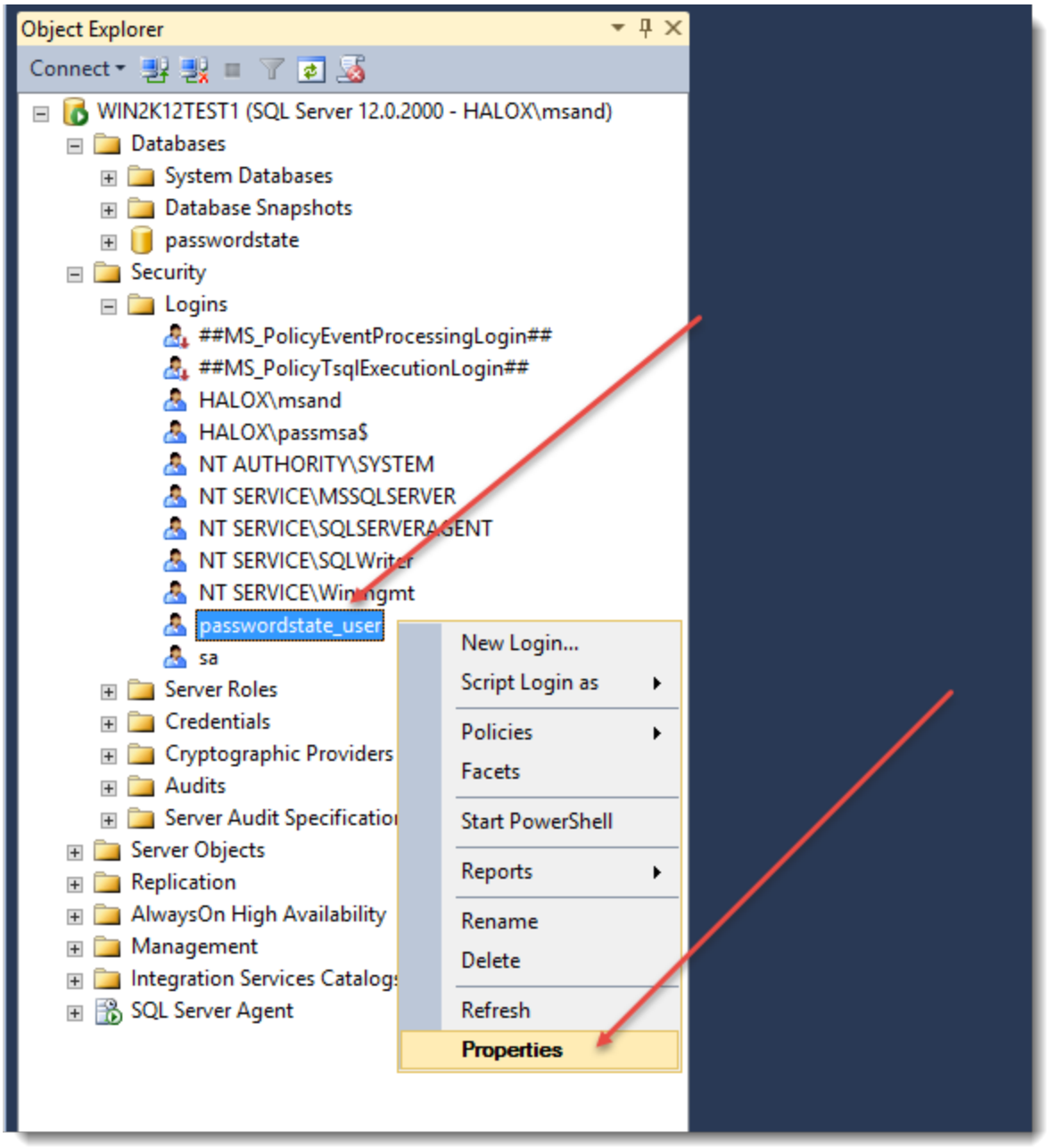


- Now expand the Security -> Logins tree. If you do not see the 'passwordstate_user' SQL Account, follow the next set of instructions for creating it. If it does exist, simply skip to the step below where we apply permissions for this account to the Passwordstate database

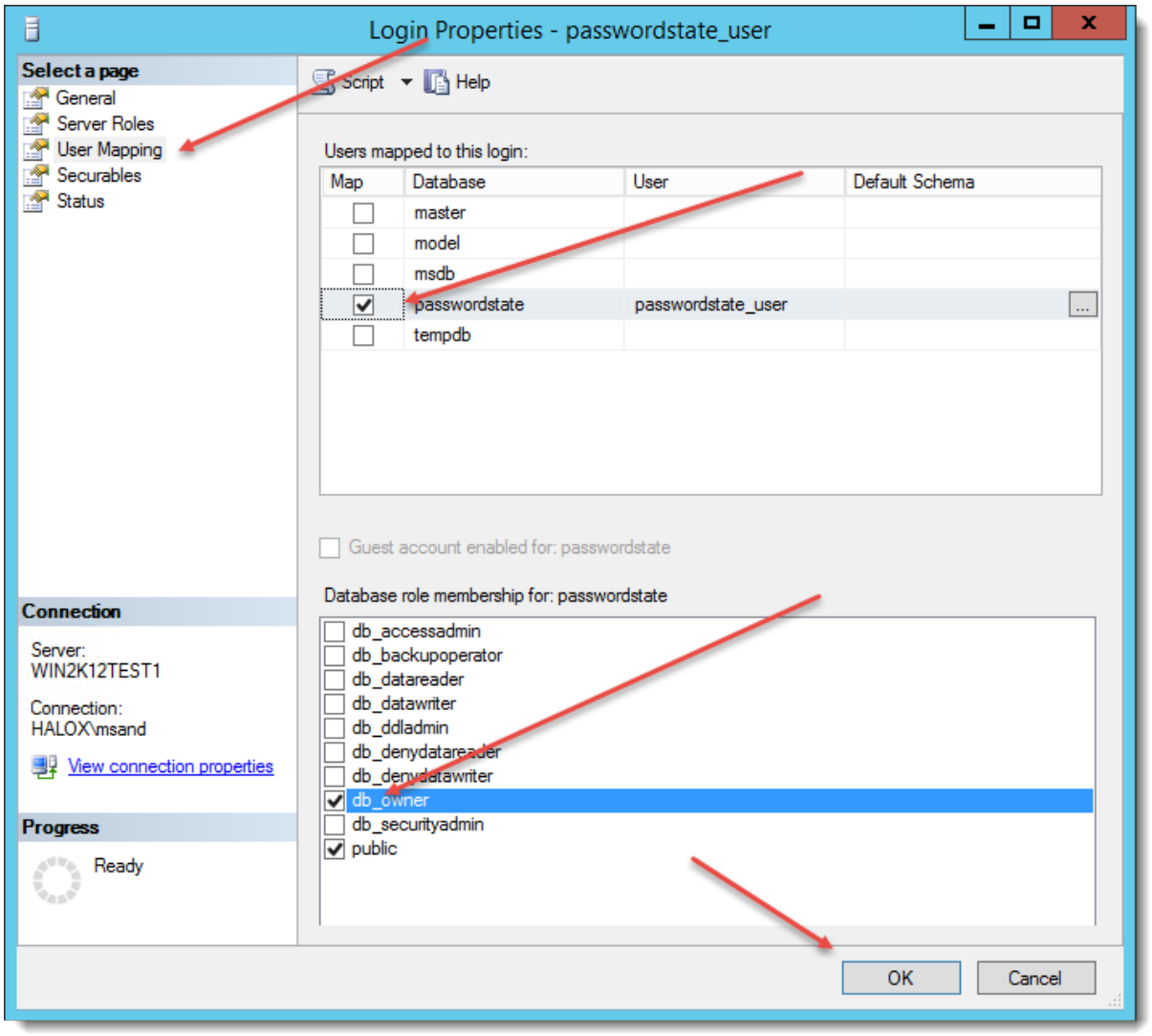




- Now select the 'Properties' menu option for the account



- And select db_owner rights to the Passwordstate database



- 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

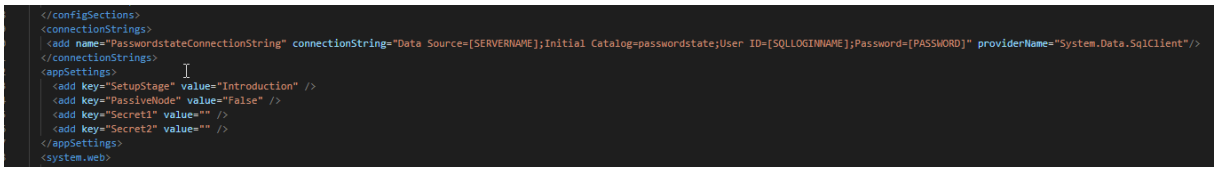
```
<connectionStrings>
 <add name="PasswordstateConnectionString" connectionString="Data Source=win2k12test1\sqlexpress;Initial Catalog=passwordstate;
  User ID=passwordstate_user;Password=randompassword" providerName="System.Data.SqlClient"/>
</connectionStrings>
```

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.

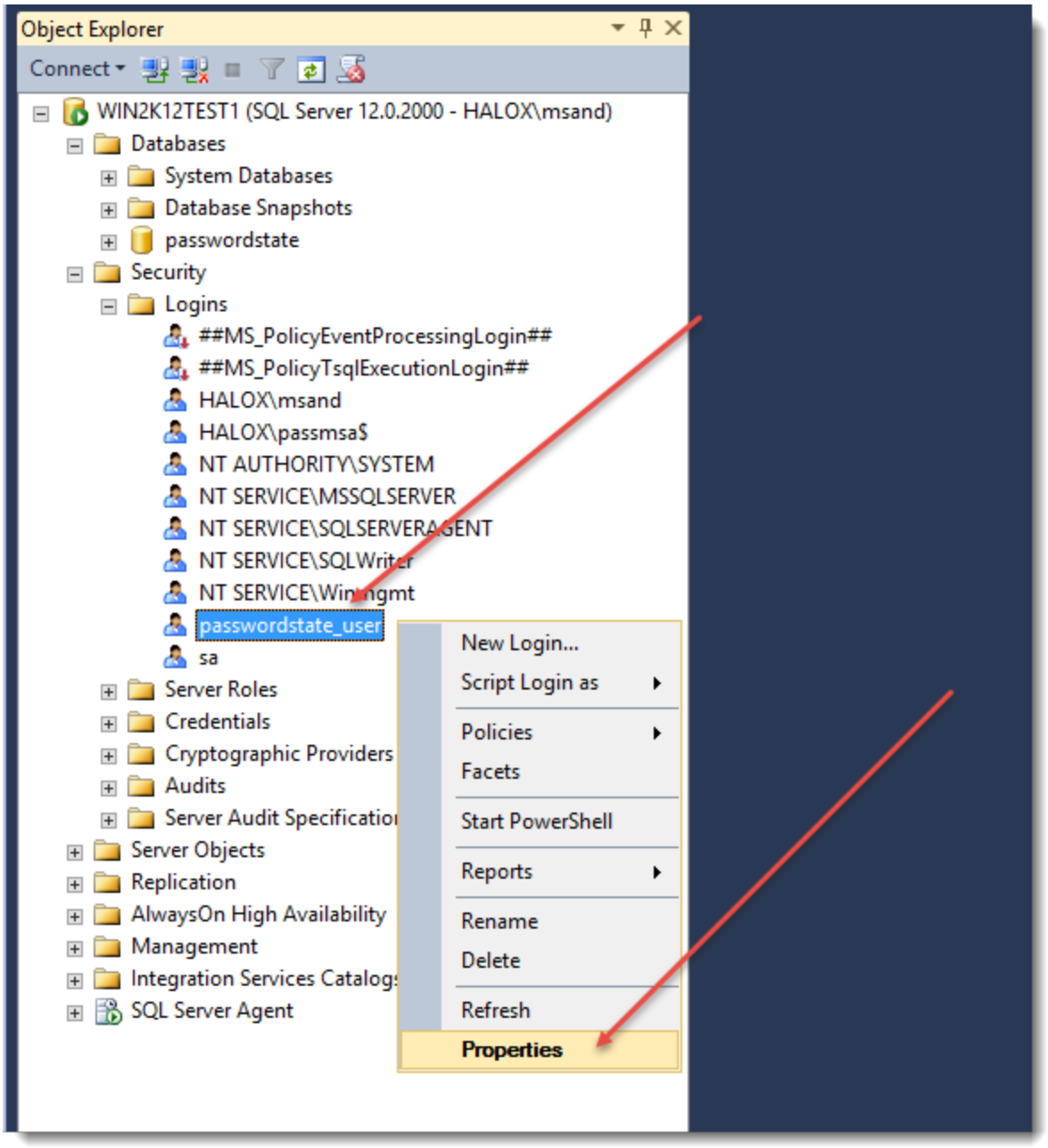
Reset Password for Passwordstate_User SQL Account

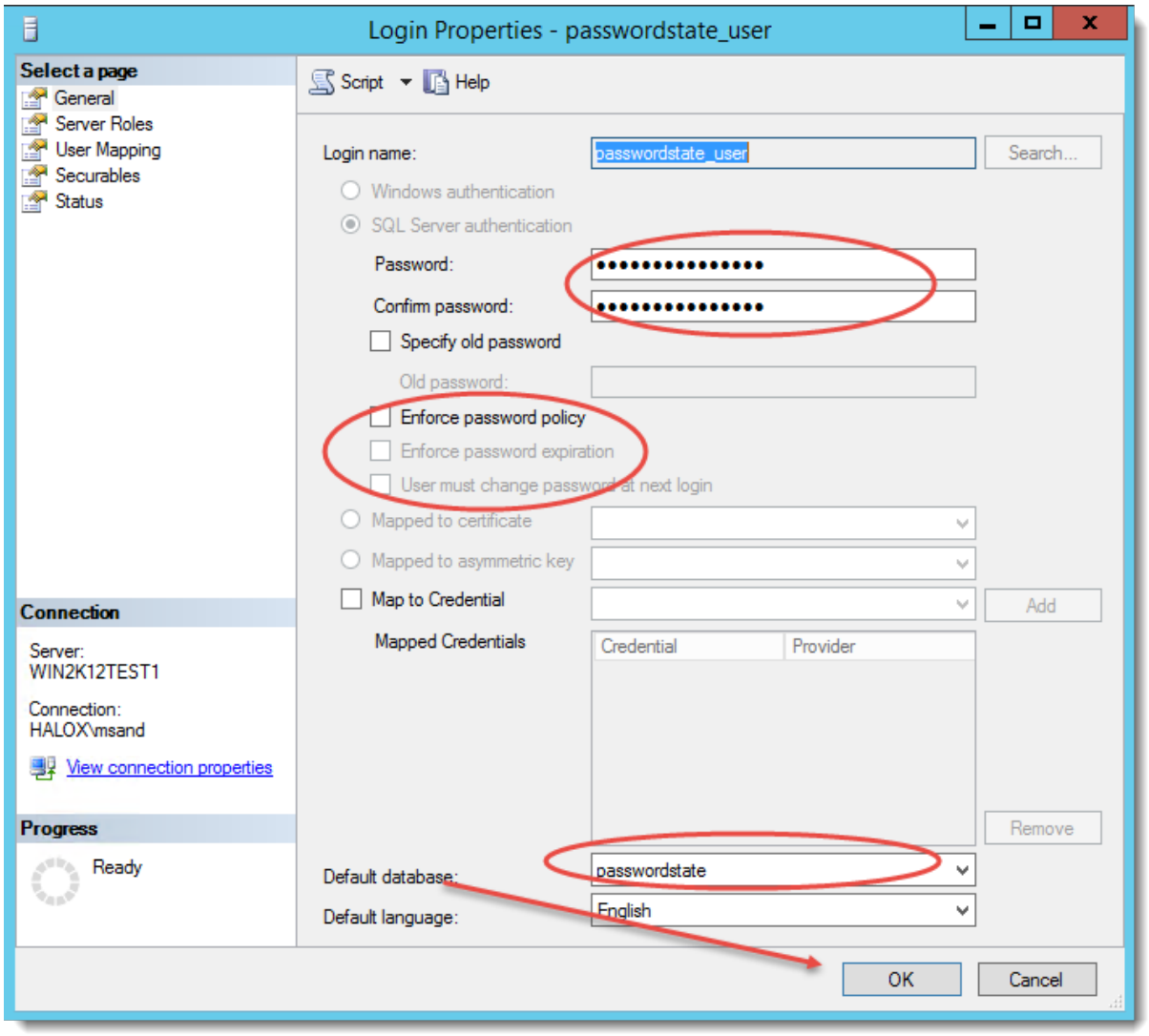
As you have specified what is most likely a new password for the passwordstate_user SQL Account, you will need to reset this password on your SQL Server. To do this, please follow these instructions - Resetting Password for Passwordstate_User SQL Account

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





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 https://www.clickstudios.com.au/support.aspx 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

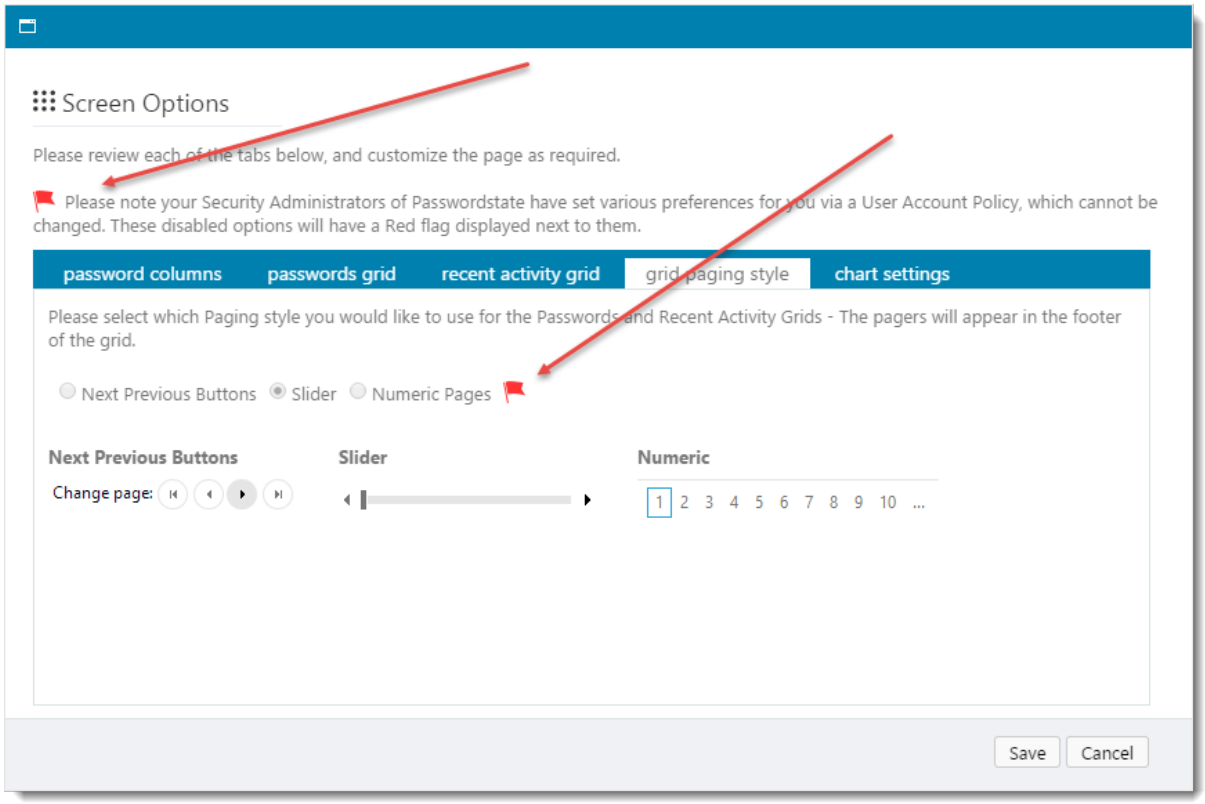
Set the Mobile default home page to
When searching for Password Lists or Passwords, limit the number of records displayed to

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.



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:
  - 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:
  - aspnet_regiis.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:
  - 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:

  - 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

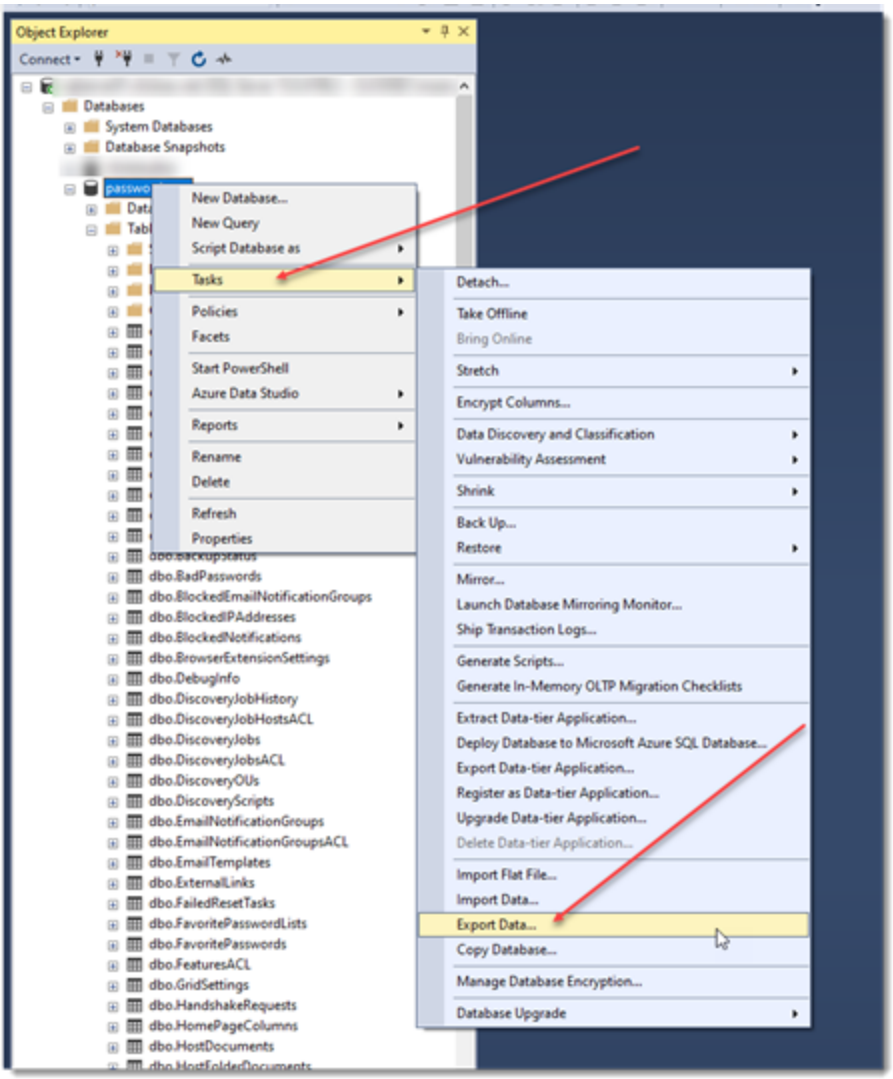
2. You do not have a "Primary" server configured on the screen Administration -> Authorised Web Servers
3. There is some sort of exception happening in the Passwordstate Windows Service, and these should be logged in the Windows Application Event Log, on your "Primary" Passwordstate web server.

If you require assistance in determining why you have excessive Auditing data, please log a support ticket here https://www.clickstudios.com.au/support.aspx

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
```



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:

```
-------------------------------------------------------------------------------------------
--------------------------
-- Where are using batches here to delete data, to prevent transaction log from
growing too large
-------------------------------------------------------------------------------------------
--------------------------
USE passwordstate
DECLARE @OlderThanMonths int = 36 --3 years
DECLARE @BatchSize int = 1000 -- This is the batch size for the number of records we
will process each time
DECLARE @EndID bigint
DECLARE @StartID bigint = (SELECT TOP(1) AuditID FROM [Auditing] (NOLOCK) WHERE
(AuditDate <= DATEADD(month, -@OlderThanMonths, GetDate())) ORDER BY AuditID ASC)
```

```
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
       END

    DELETE FROM [Auditing]
    WHERE (AuditID BETWEEN @StartID AND @EndID)

    SET @StartID = @EndID + 1
END
```

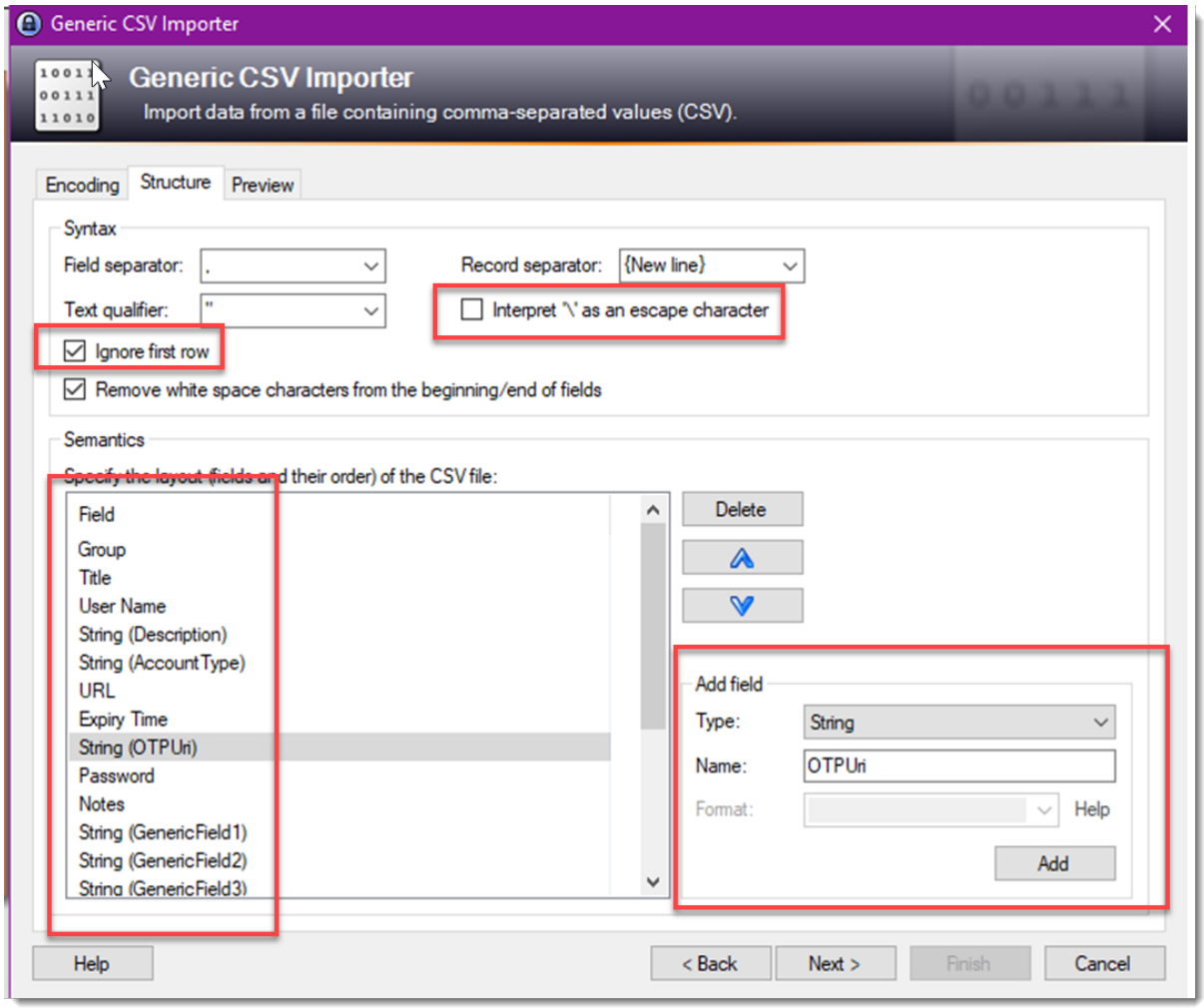
Truncating All Data in the AuditingArchive table
If you do not wish to keep any records in the AuditingArchive table, you can remove them all by using the SQL code below:

```
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.

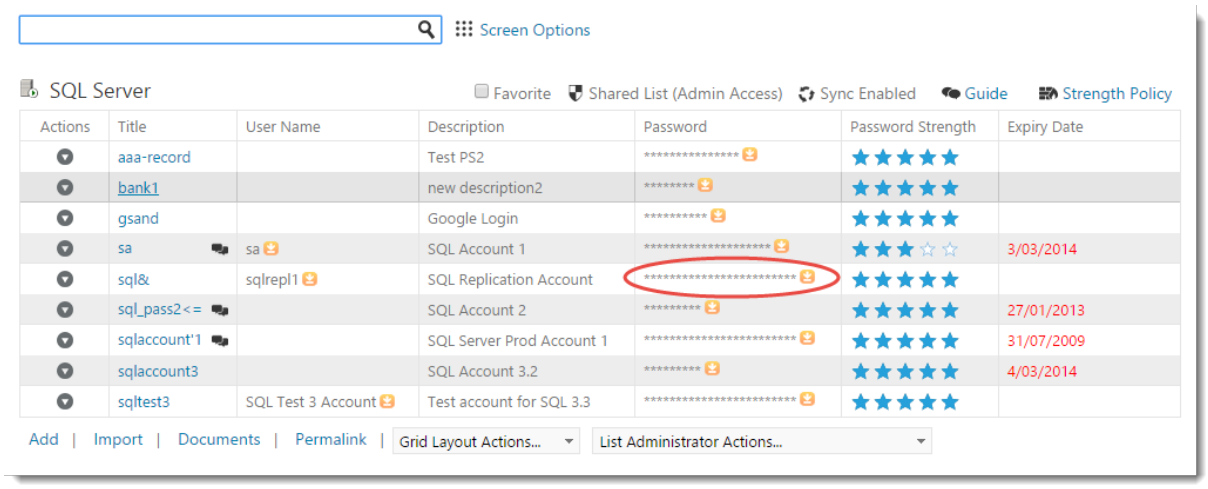
- Go to the page in Passwordstate Administration -> Export All Passwords
- Select the option 'KeePass Compatible CSV file', and check/uncheck the Auditing option as appropriate
- Save the exported csv file somewhere safe
- Open KeePass and create a new empty database
- From the 'File' menu, select 'Import'
- 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



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

5.6 Multiple Options for Hiding Passwords

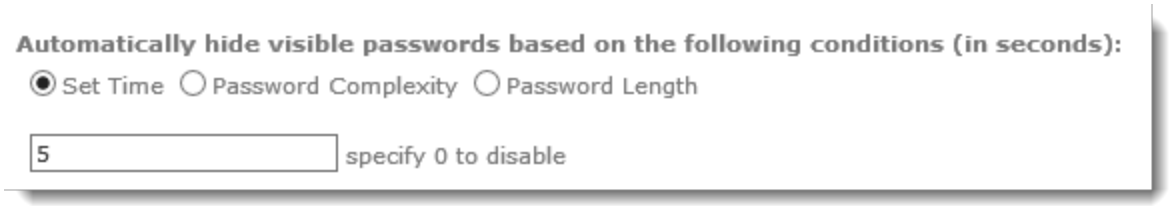
On each of the Password Lists screens, there is a 'Password' column which shows the masked password and provides a image for you to click on copy the Password to the clipboard – see image below. There are three options for how long the Password will stay visible on the screen when you click the masked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



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

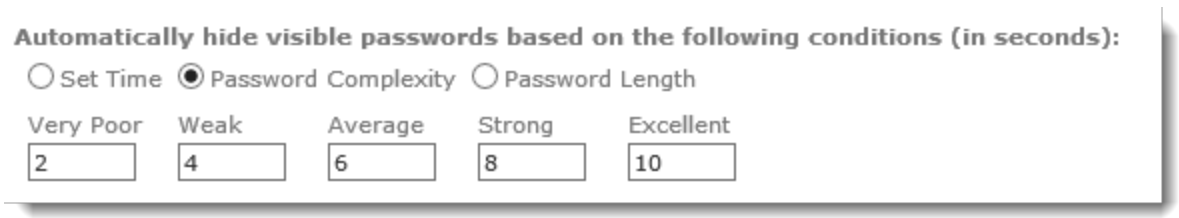
Option 1 – Hide Based on a Set Time

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



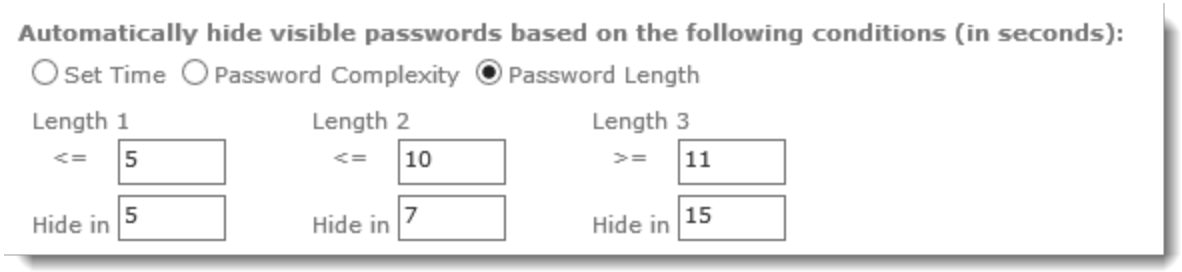
Option 2 – Hide Based on Complexity of the Password

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



Option 3 – Hide Based on Password Length

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



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.

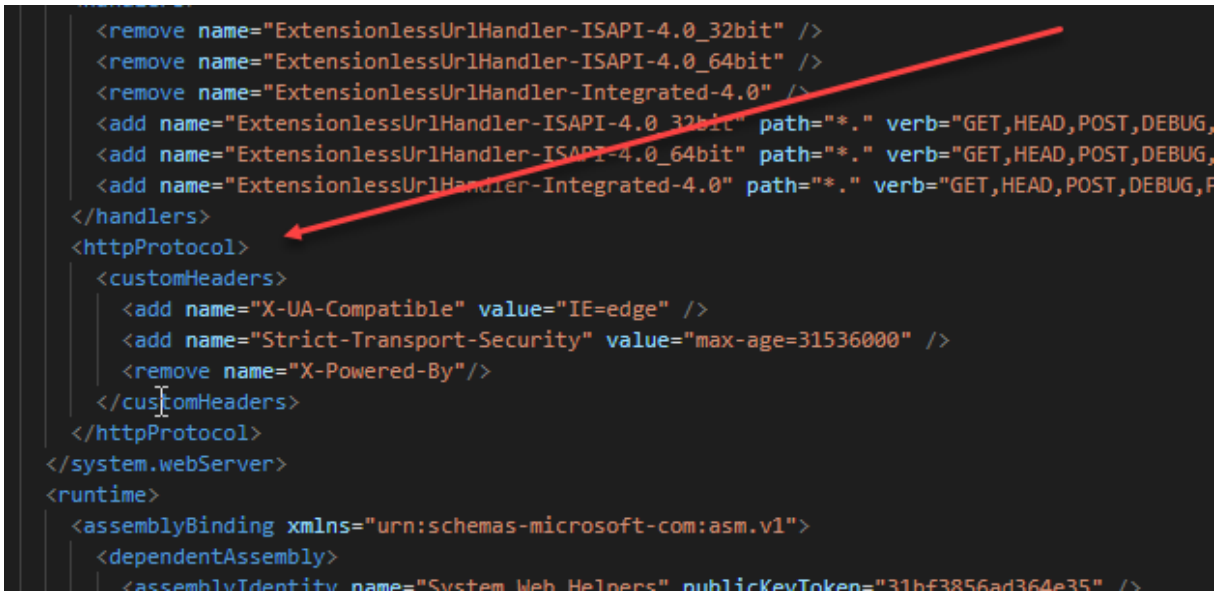
Main Passwordstate Web Site (should already be included after an upgrade)

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>
```