Passwordstate Security Administrators Manual

Table of Contents

1 Introduction

Welcome to the Passwordstate Security Administrators Manual.

This manual will provide instructions for Security Administrators of Passwordstate to configure user accounts, system wide settings, and various other features which managing the environment.

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

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 and Upgrades	Allows you to specify settings and a schedule for perform backups of all web files and the database, and also a place to perform In-Place Upgrades of Passwordstate
Bad Passwords	A list of password values which are deemed to be 'bad' and can educate your users not to use these values
Custom Images	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
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
Export All Passwords	Allows you to export all Password records from the system to a CSV file
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
Reporting	Various reports which can be exported to CSV files
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 Active Directory Domains

The Active Directory Domains screen is where you can specify which domain's user accounts and security groups can authenticate and interact with the Passwordstate website.

If you wish to use multiple domains with Passwordstate, you must have trust relationships configured for the domains, and cross-domain name resolution (DNS) must be working correctly.

Once you have added the relevant domains, you can them import User Accounts or Security Groups as appropriate.

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.

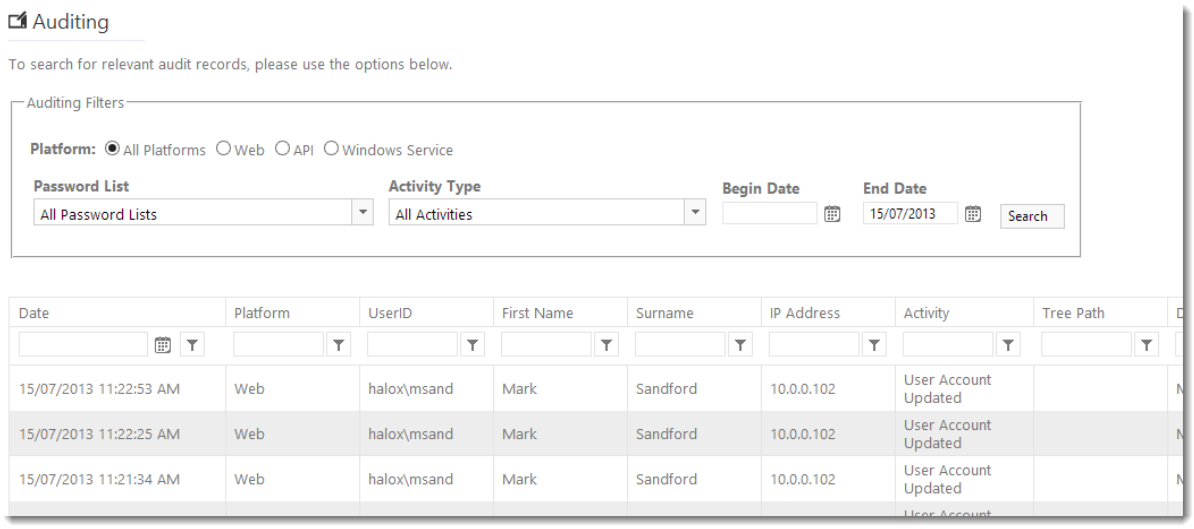
3 Auditing

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 API, or functions the Passwordstate Windows Service provides
- 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

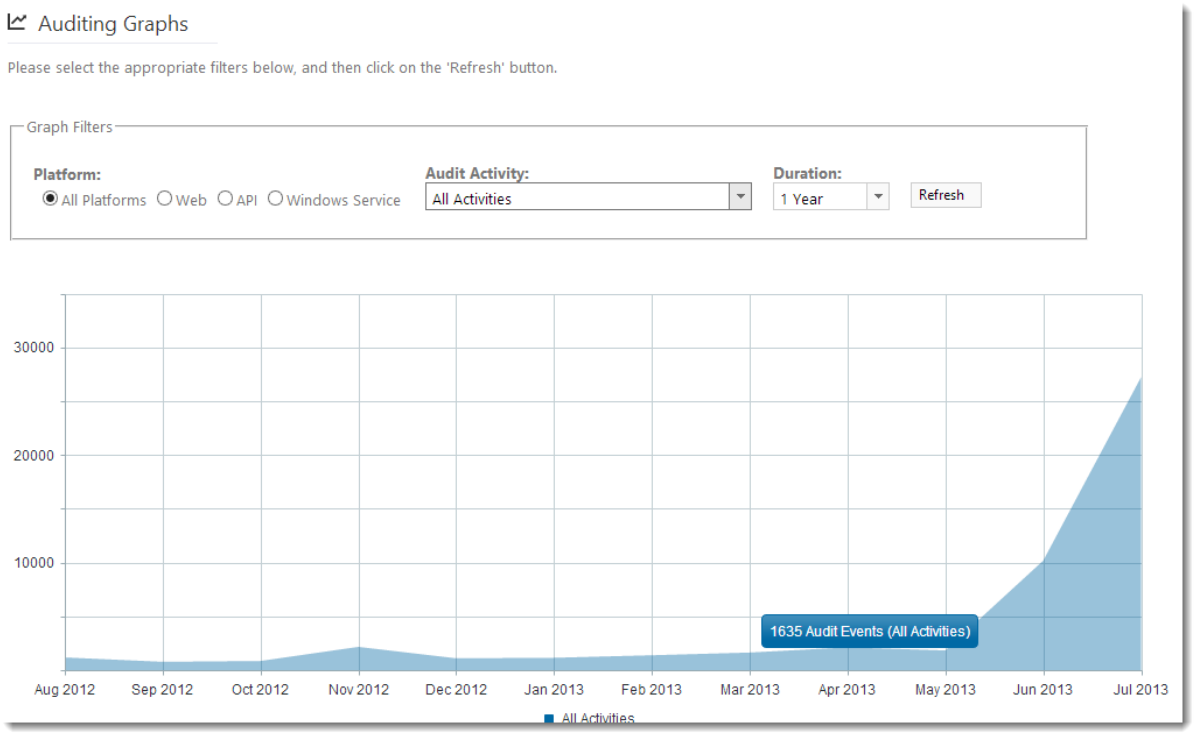
In addition to reporting on auditing data on the screen, you can export the data for further analysis to a CSV file if required.

Note: You can disable the feature allowing purging of auditing data on the screen System Settings -> Miscellaneous Tab



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.



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.

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
Note 3: The host names are not case sensitive

6 Backups and Upgrades

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

Note 1: You must have backups working correctly, otherwise you will not be able to perform In-Place Upgrades of Passwordstate.
Note 2: The 'Upgrade Now' button takes you to the same screen you would navigate to when

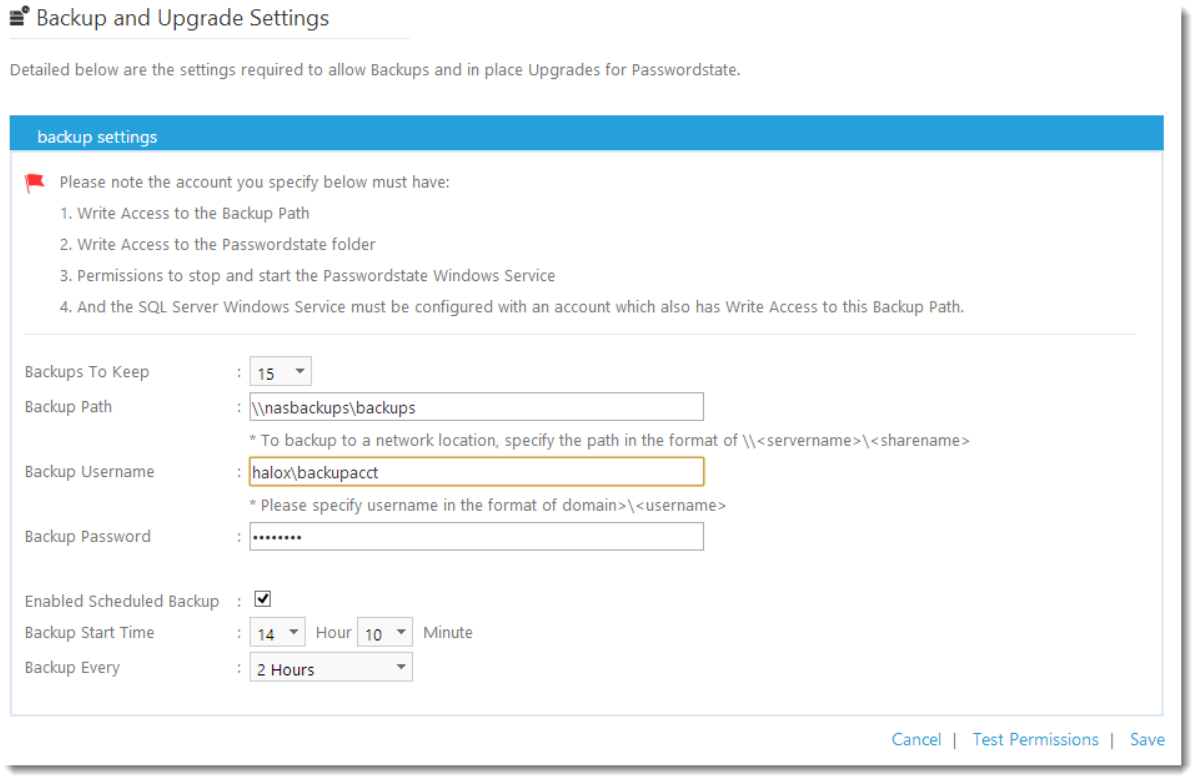
clicking on the new build notification hyperlink which 'may' appear at the top of the screen when new builds are available

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:

Backup Settings

On the Backup Settings screen, you have the following options available to you:

- How many backups to keep on the file system
- The path to where you would like to store the backups - please use UNC naming conventions here, not a literal path such as c:\backups
- Username and Password required for the backup (below is an explanation of the permissions required)
- Whether you want to enable a regular set-and-forget schedule for the backups to occur
- And finally, what time you would like the scheduled backups to begin, and how often you want a backup to occur



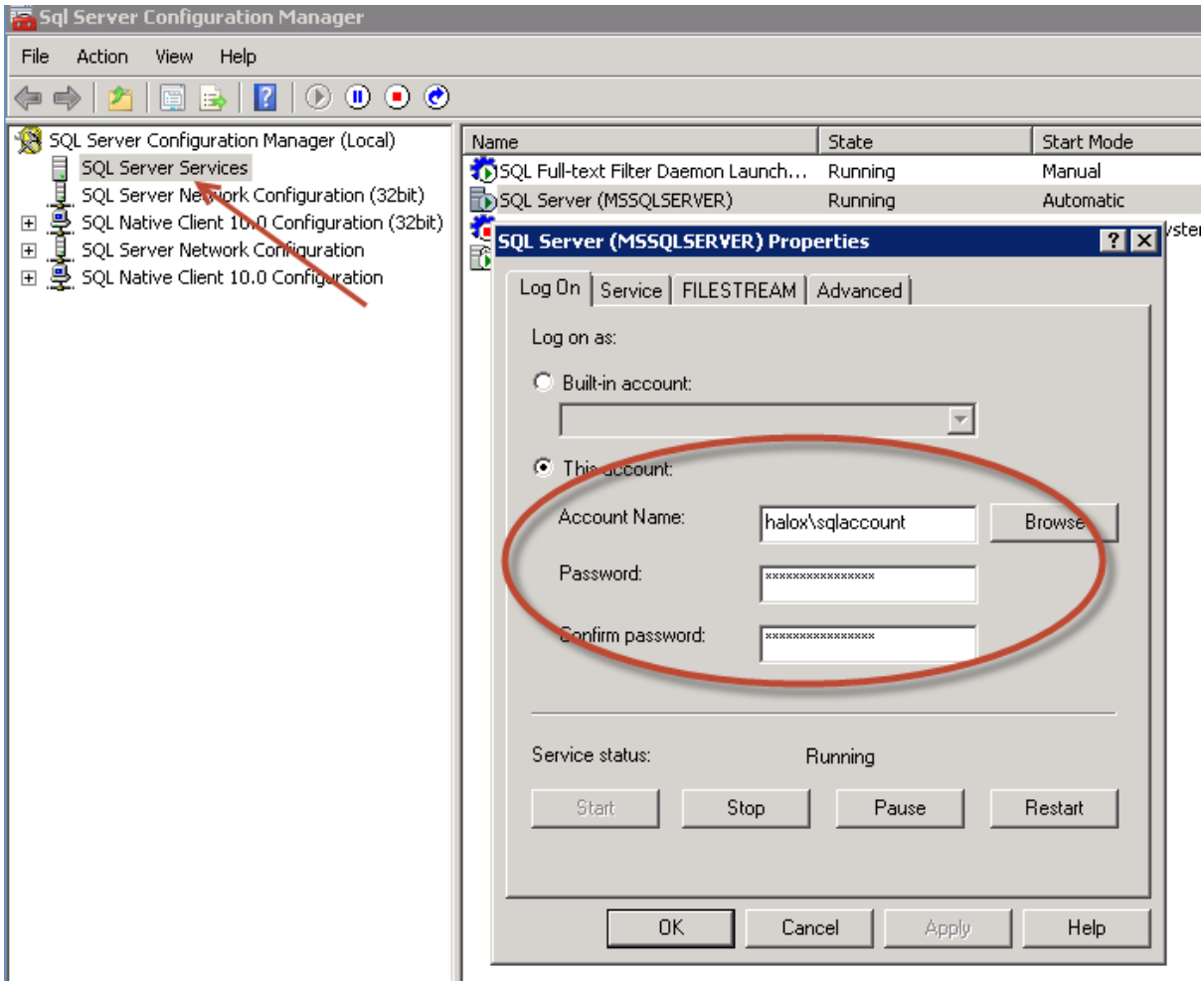
Backup Permissions

To allow backups to work through the Passwordstate web interface, you will need to specify an

account (domain or Windows account), which has the following permissions:

- Permissions to write to the Backup path you've specified
- Permissions to stop and start the Passwordstate Windows Service on the web server
- Permissions to write to the Passwordstate folder on your web server.

In addition to this, you must configure the SQL Server service to use a domain or Windows account which has permissions to also write to the Backup Path. To do this, you need to open the 'SQL Server Configuration Manager' utility on your database server, click on 'SQL Server Services', and the specify and account as per the next screenshot:



Note: Please ensure you test the upgrade by clicking on the 'Test Permissions' button - this will report any issues with permissions in performing a backup.

7 Bad Passwords

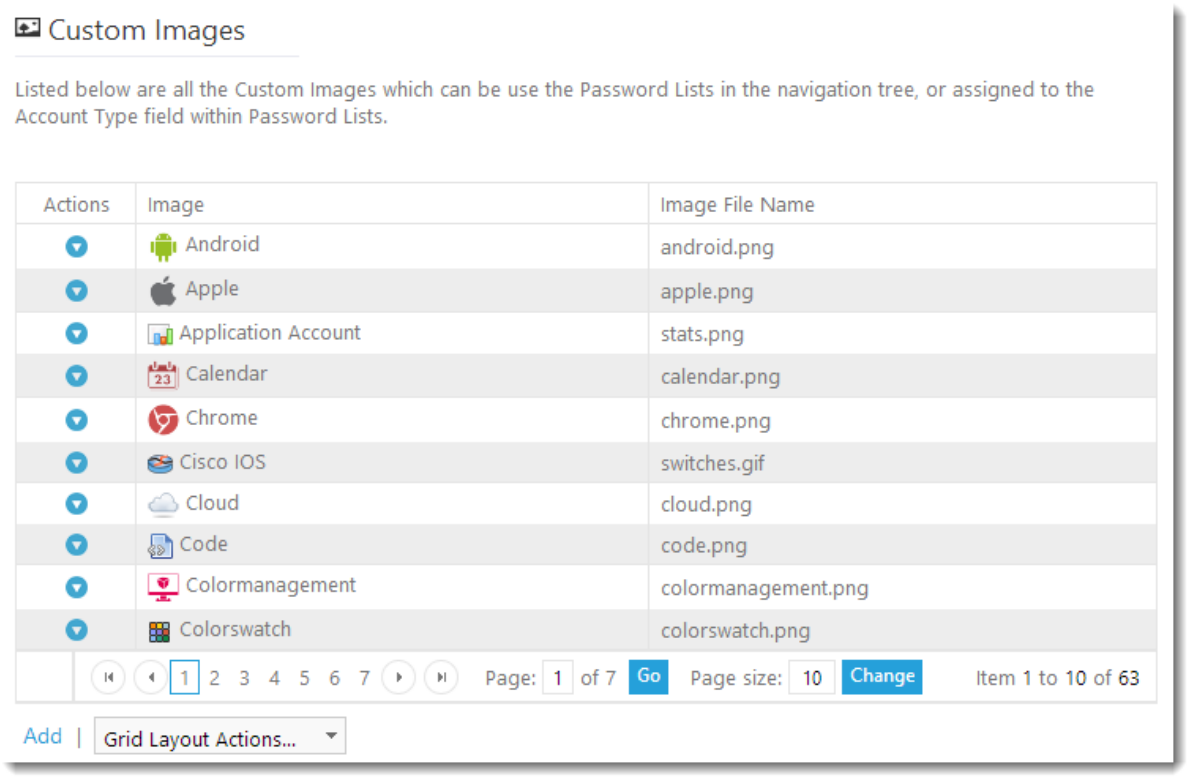
The Bad Passwords screen allows you to maintain a list of password which are deemed to be bad i.e. common passwords, easy to guess, etc. The intention is to educate your users to ensure they do not use 'Bad' passwords.

On this screen you can add or delete bad password records, and once you have a list you are happy with, there are options on the screen Administration -> System Settings -> Miscellaneous Tab, and Password Options Tab for notifying your users when bad passwords are detected.

8 Custom Images

The 'Custom Images' 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 once the Passwordstate Windows Service is next restarted.
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

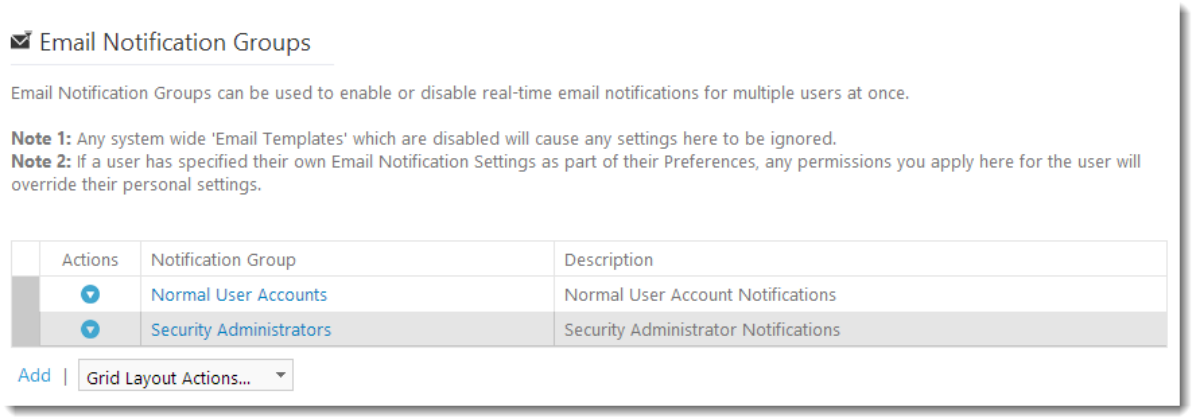


9 Email Notification Groups

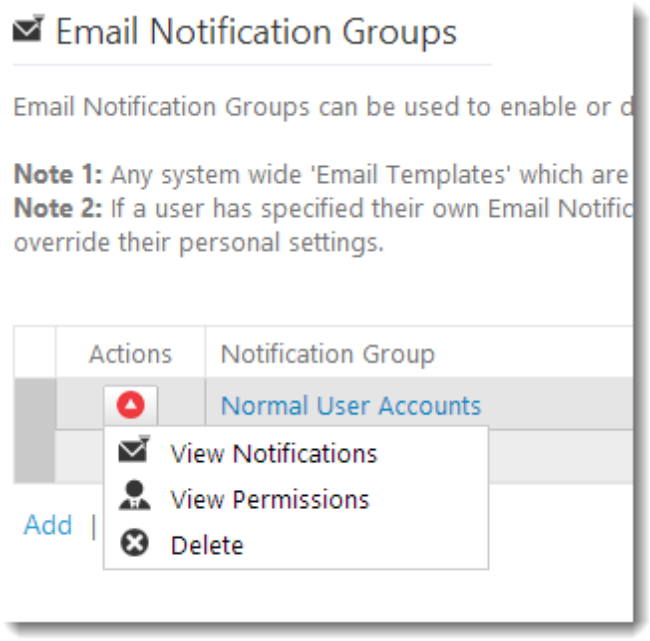
The Email Notification Groups screen is used to manage email notification settings for a group of individual users accounts, or members of security groups.

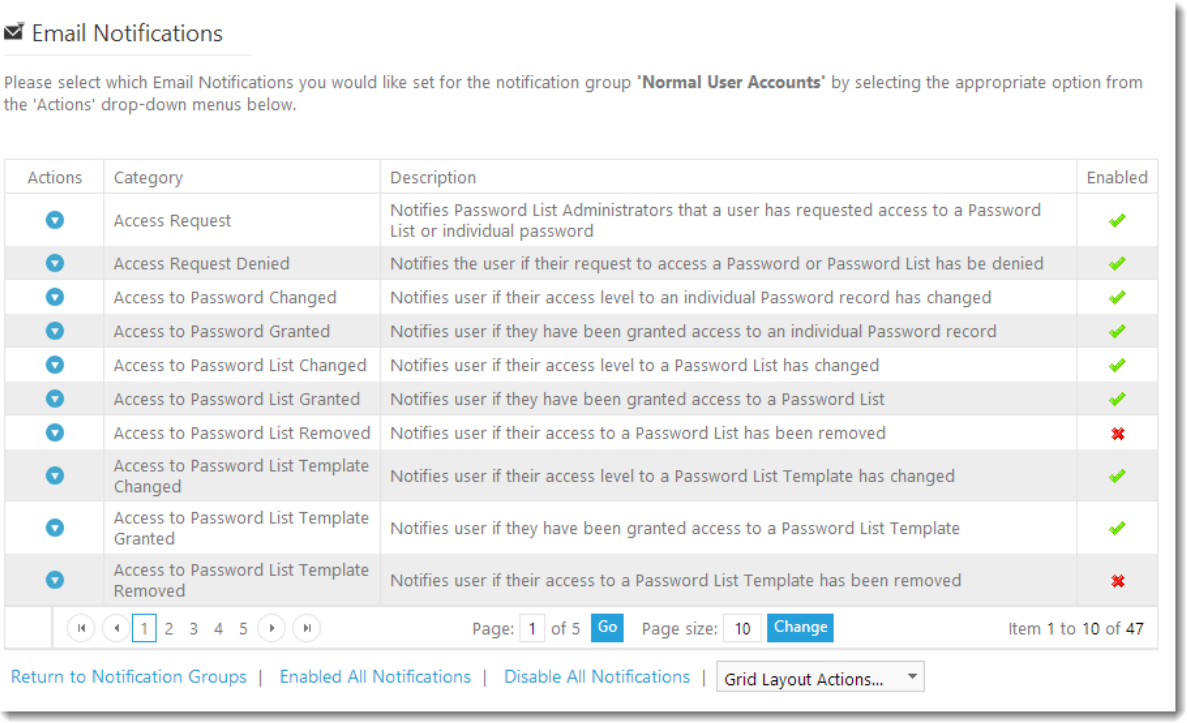
Using Email Notification Groups, you can specify which email notifications certain users receive, or don't receive i.e. you may wish to have certain notifications enabled for Security Administrators, but disabled for 'normal' user accounts in Passwordstate.

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



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.





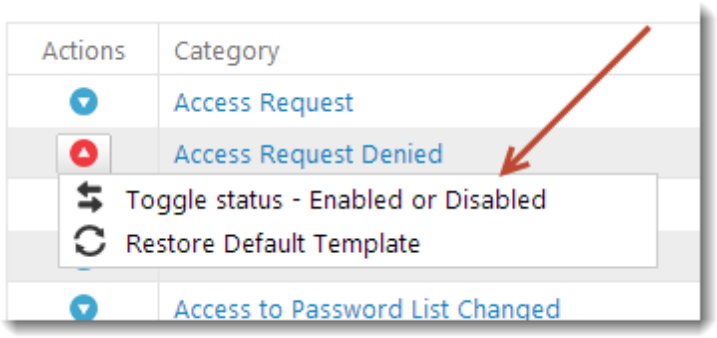
10 Email Templates

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

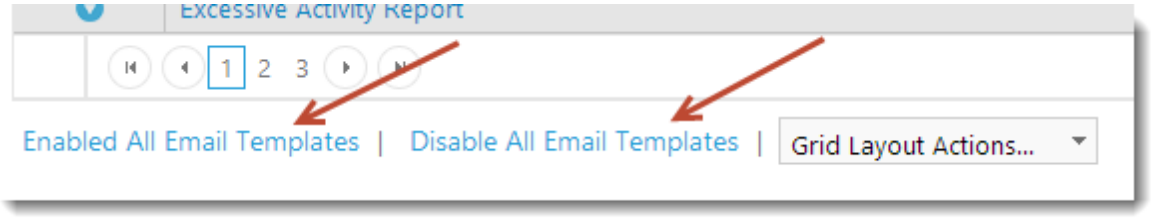
Enabling/Disabling Email Notifications

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 the appropriate 'Enable All' or 'Disable All' buttons at the bottom of the grid



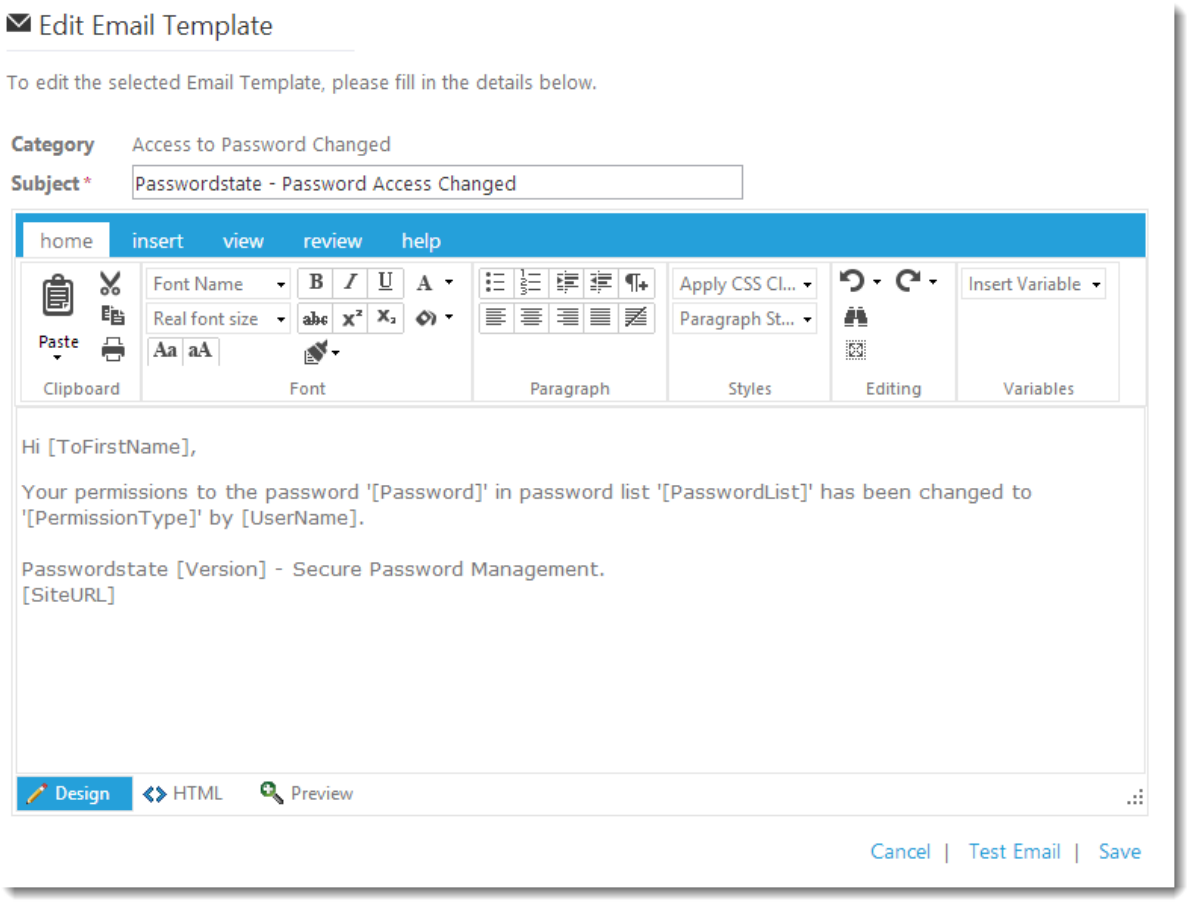
Editing Email Template Content

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.

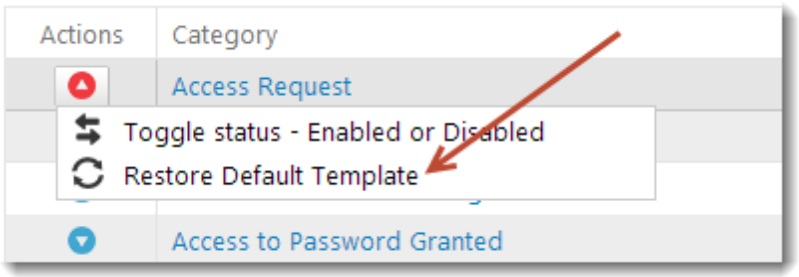
At the top right-hand side of the Editor you will notice the 'Variables' tab/ribbon bar. From this drop-down list, you can insert the following variables into your email templates:

- 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

- ExpiringPasswords - reserved for the Expiring Passwords report
- 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



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

11 Emergency Access

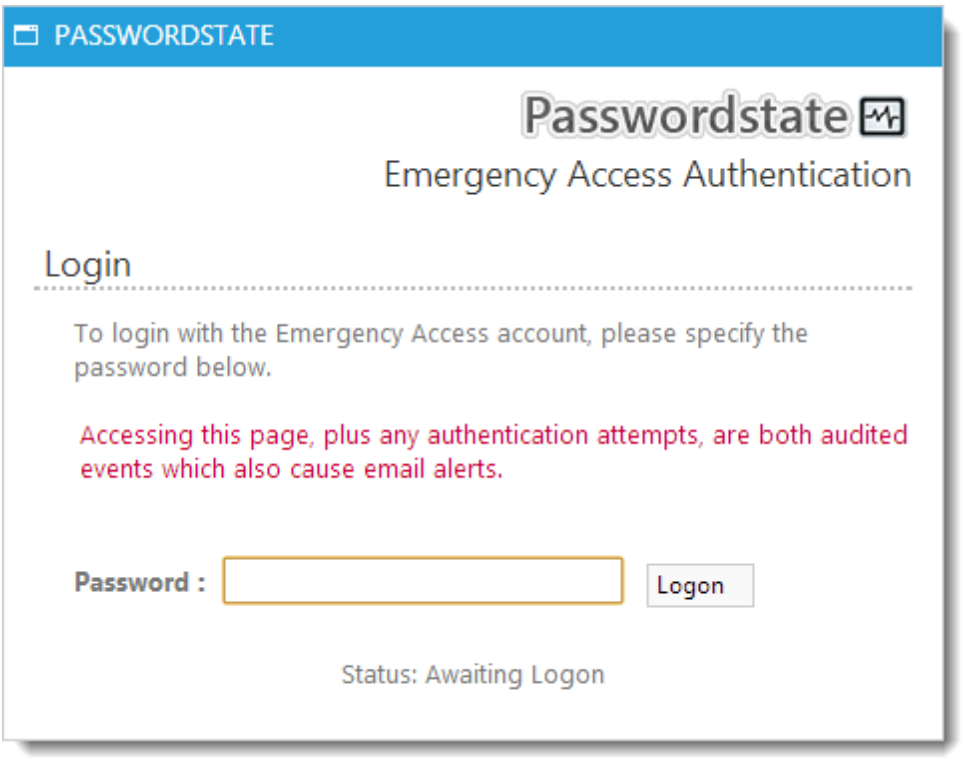
The Emergency Access screen allows you to specify a password for a separate 'Security Administrator' role login which can be used in the event other accounts are locked out, or inaccessible for any reason.

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



12 Export All Passwords

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

Note 1: 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
Note 2: In addition to the normal audit record added to indicate all Passwords have been exports, one 'Password Viewed' audit record will be added per password record - required for compliance reasons for some organizations

13 License Information

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

Note: 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.

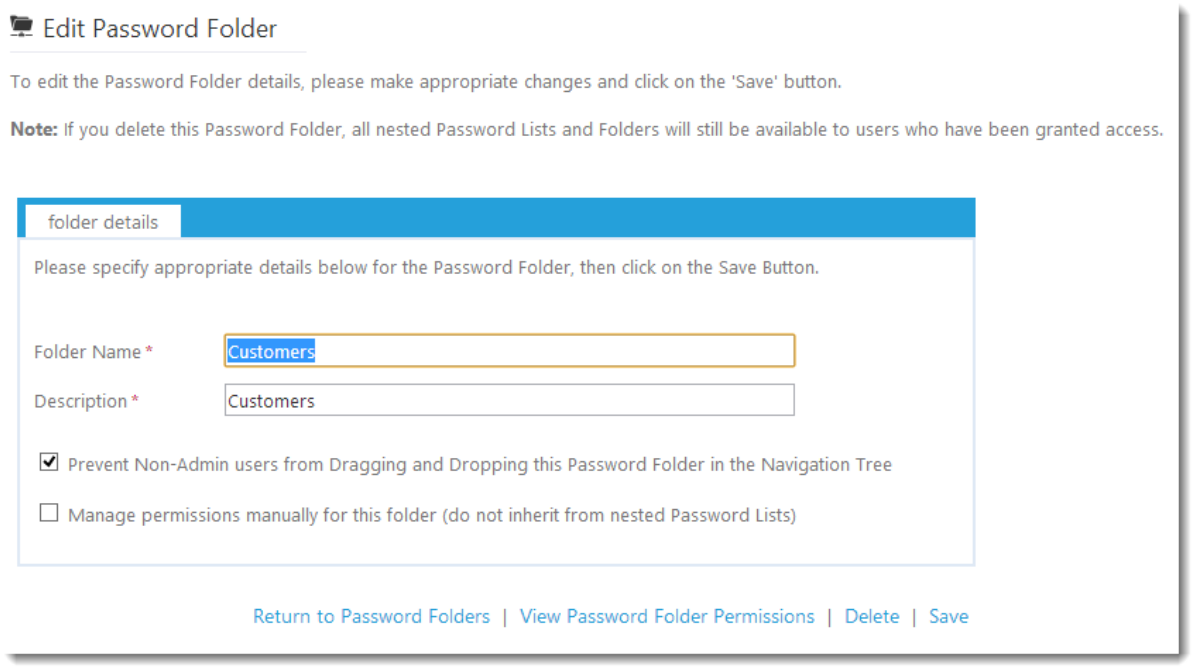
14 Password Folders

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, View Permissions & Delete the Folder

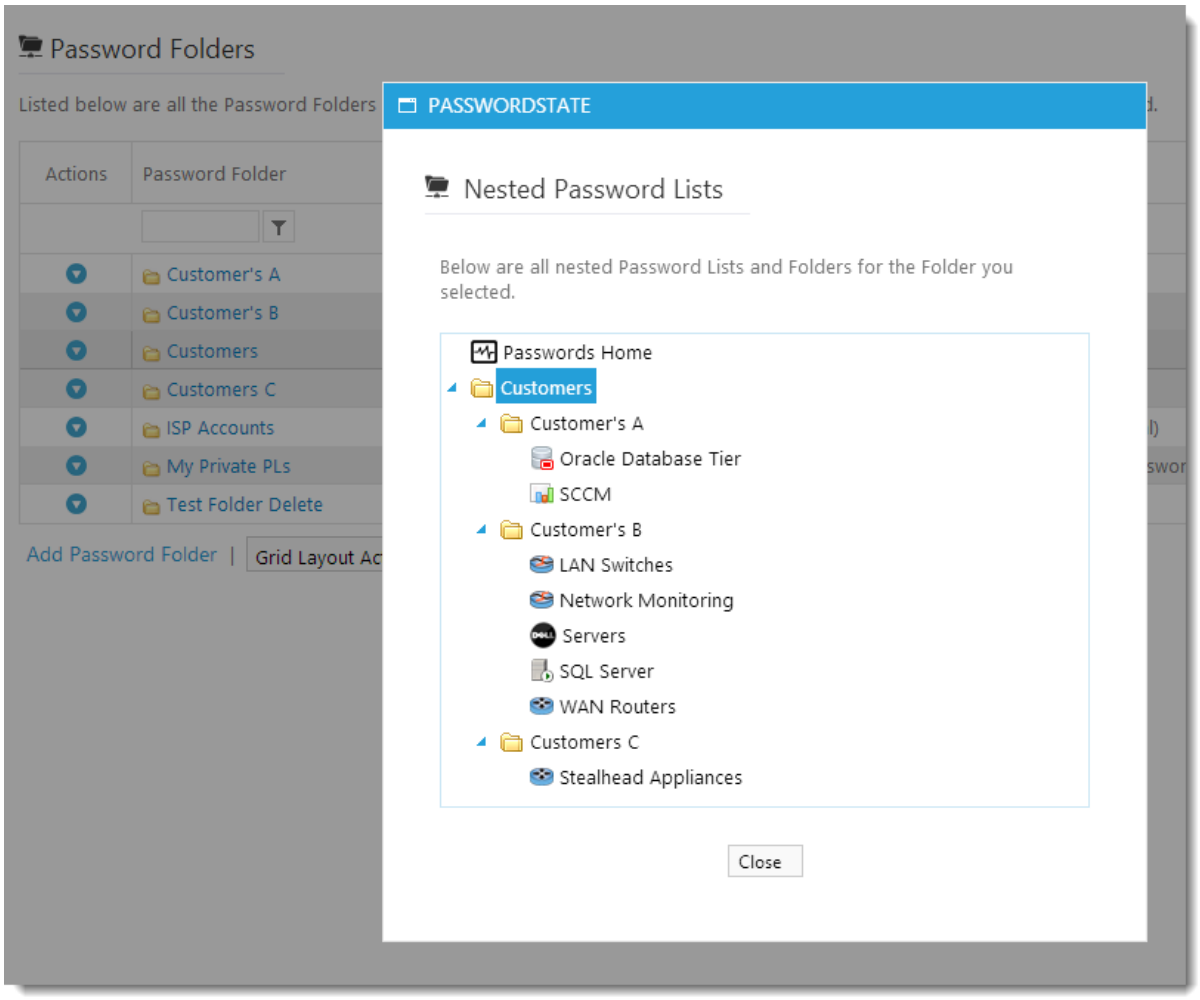
By clicking on the 'Password Folder' hyperlink you see in the grid, you will be taken to a screen where you can perform the following actions on the Folder:

- Edit name, description and settings
- View Permissions - by default, permissions are automatically applied to Folders. The permissions applied to Password Lists are propagated up through the Navigation Tree, and applied to any Folders above it. The only exception to this is when the 'Manager Permissions Manually' option is selected for a Folder
- 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.



15 Password Generator Policies

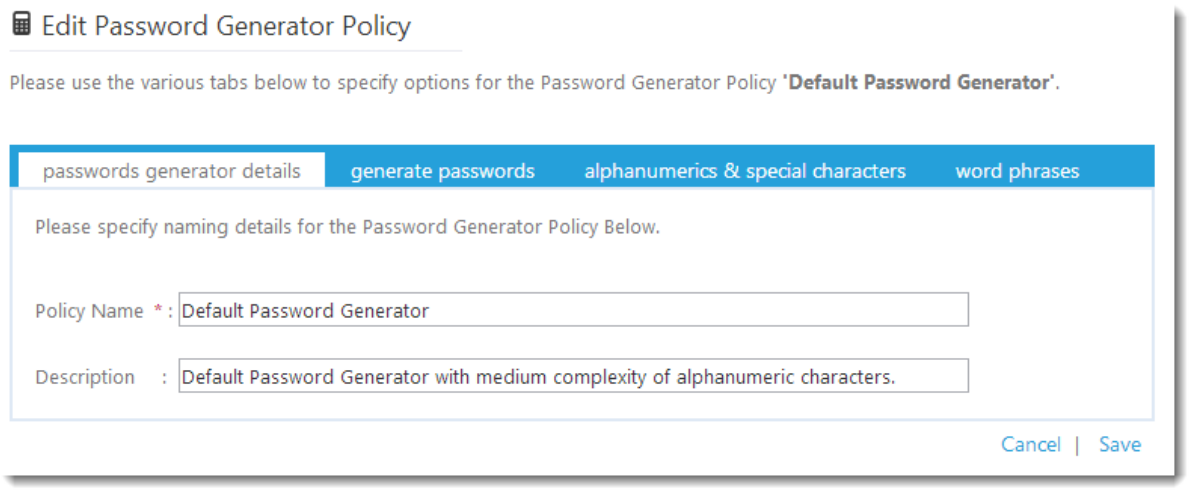
The Password Generator Policies screen allows you to create and manage multiple settings for the Password Generator, which can then be applied to one or more Password Lists.

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:

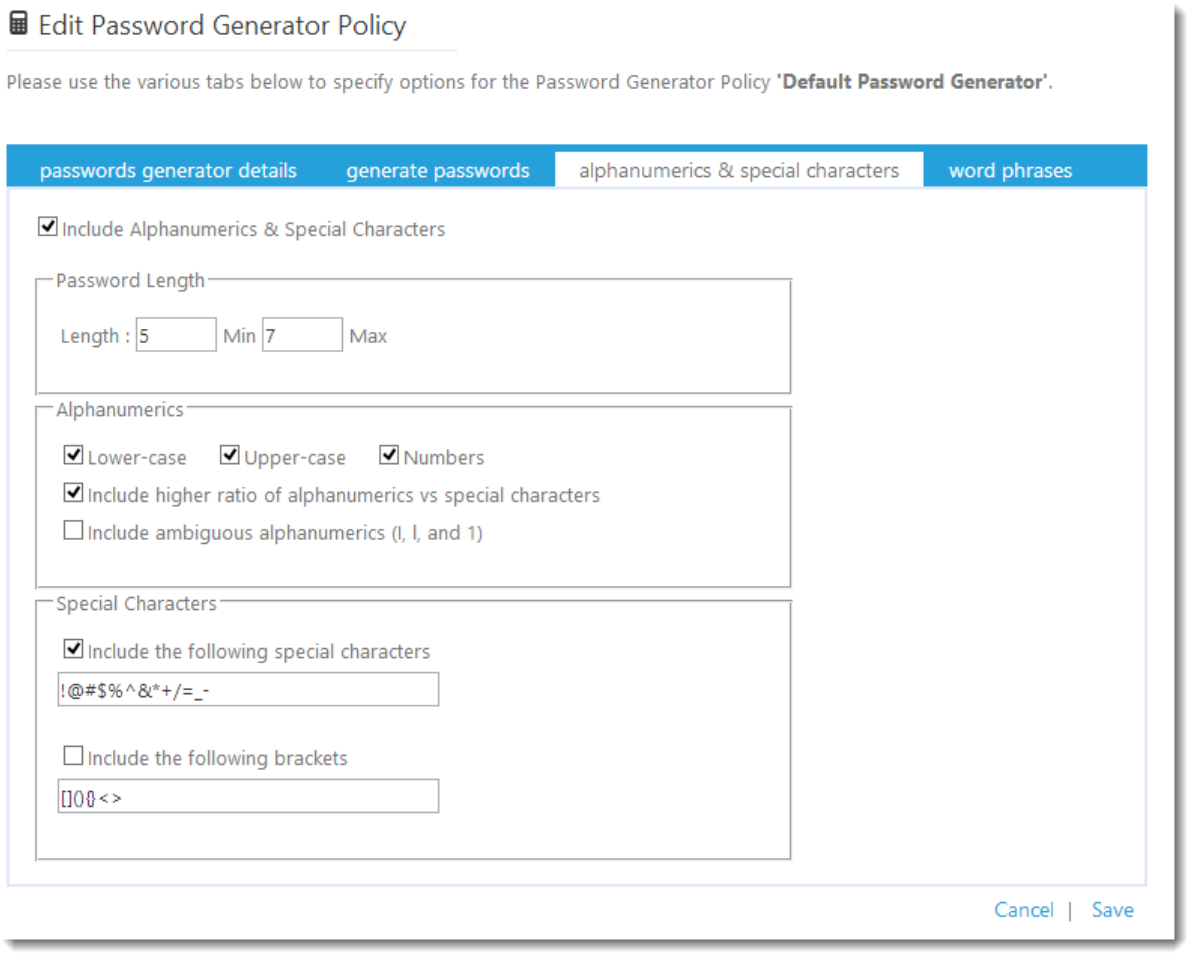
Password Generator Details

Edit the name and description for the Policy.



Alphanumerics & Special Characters

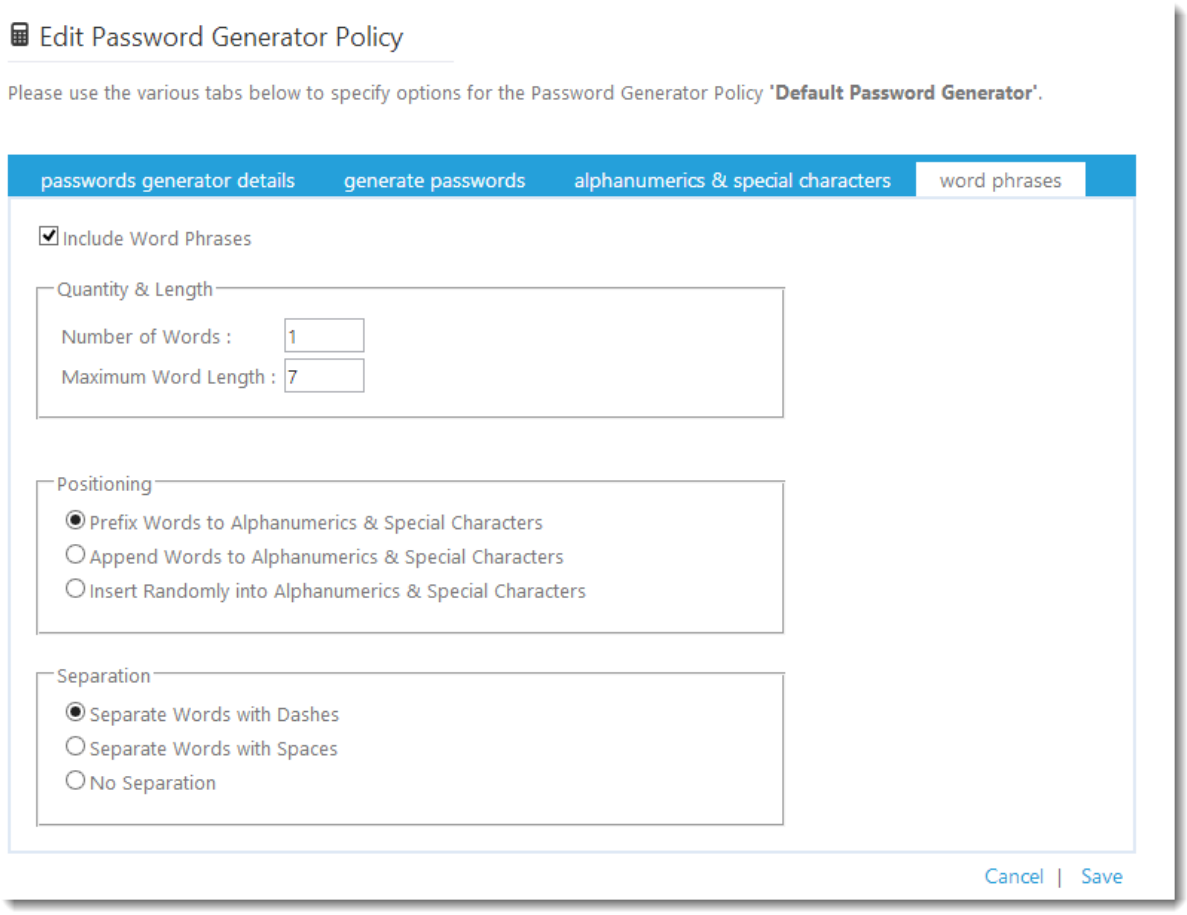
The Alphanumeric & Special Characters tab allows you to specify the desired length of the password you wish to generate, as well as settings for letters, numbers, special characters and various forms of brackets.



Word Phrases

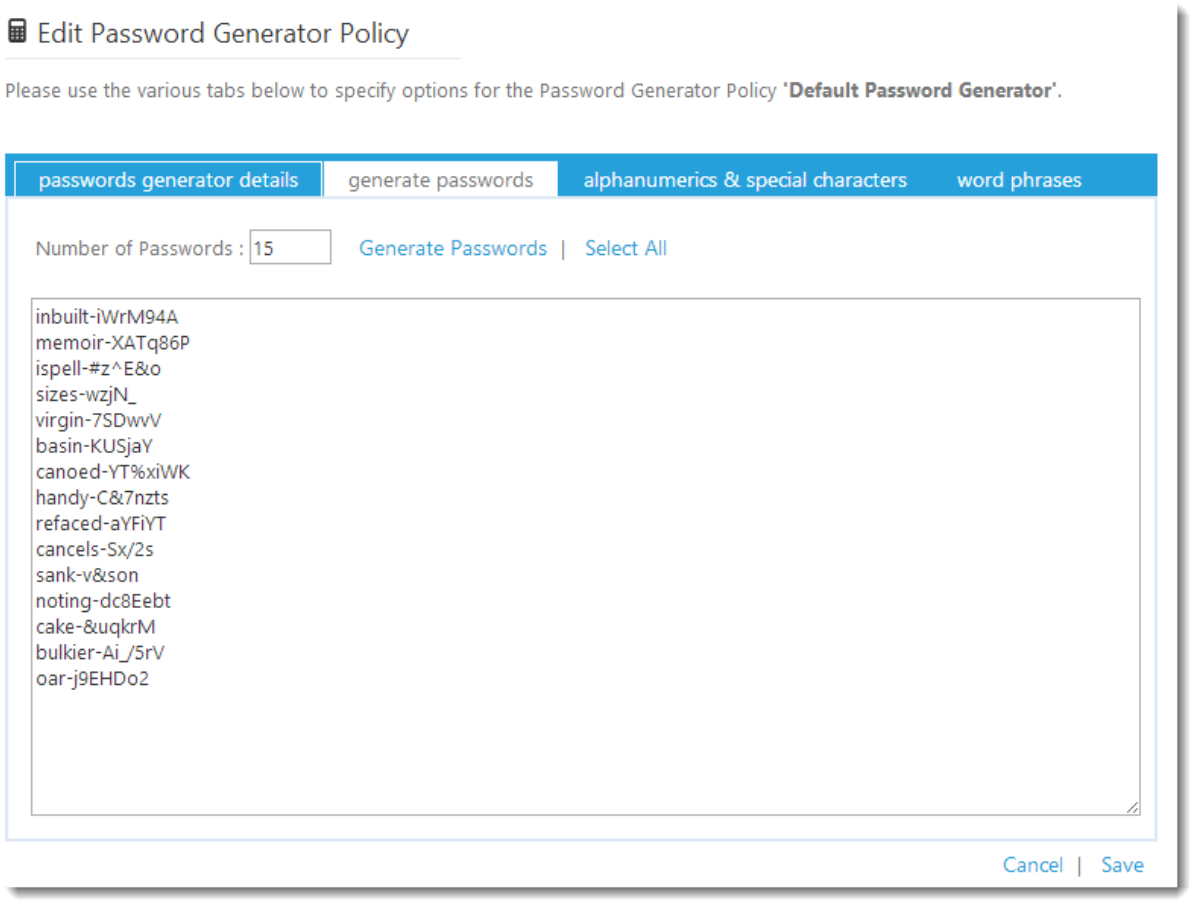
The Word Phrases tab allows you to insert a random word at the beginning of the password, somewhere in the middle, or at the end. You can specify how many words to create, what length, and what form of separation you would like between the word and the rest of the random password - either dashes, spaces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

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

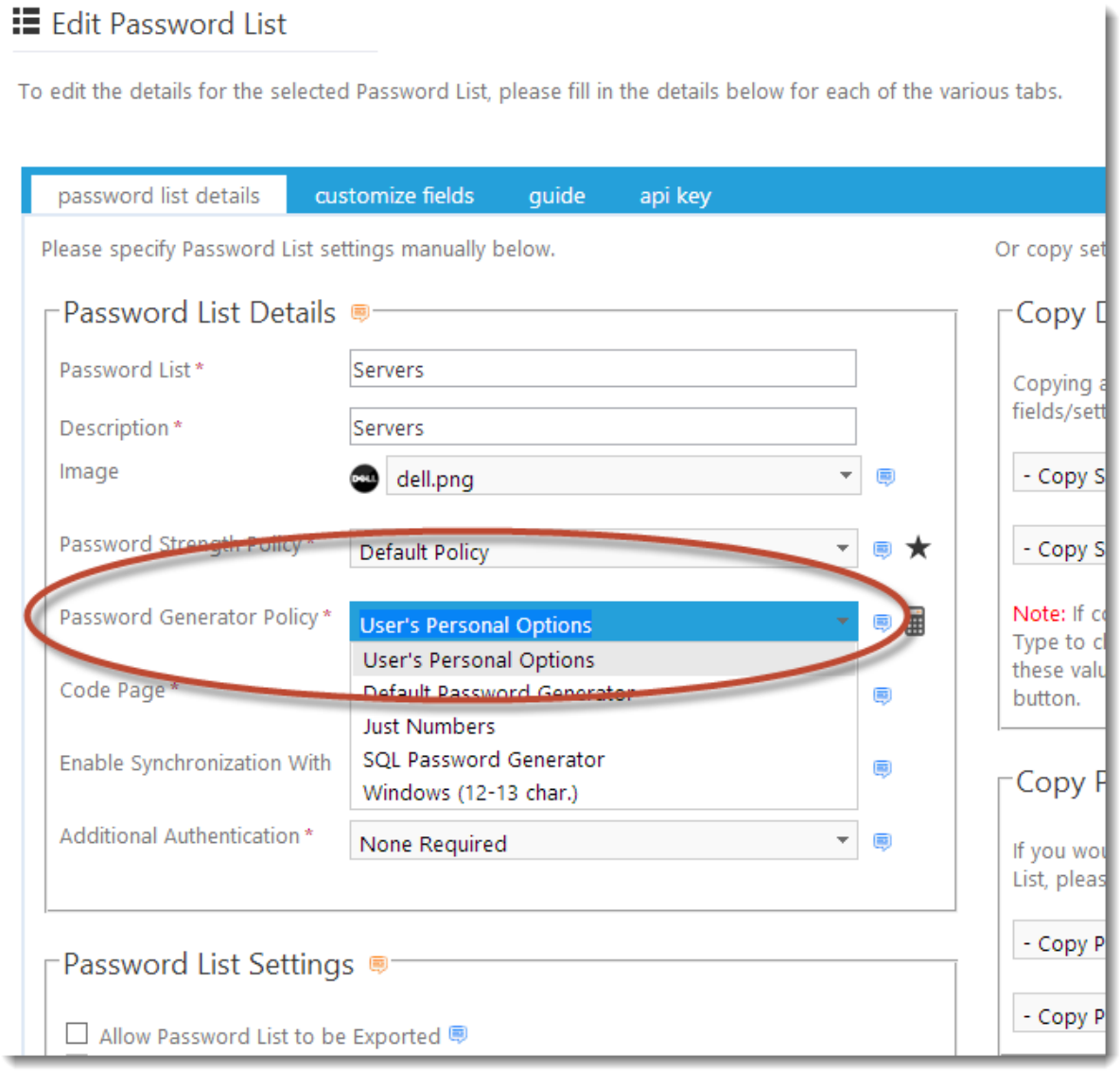


Generate Passwords

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.

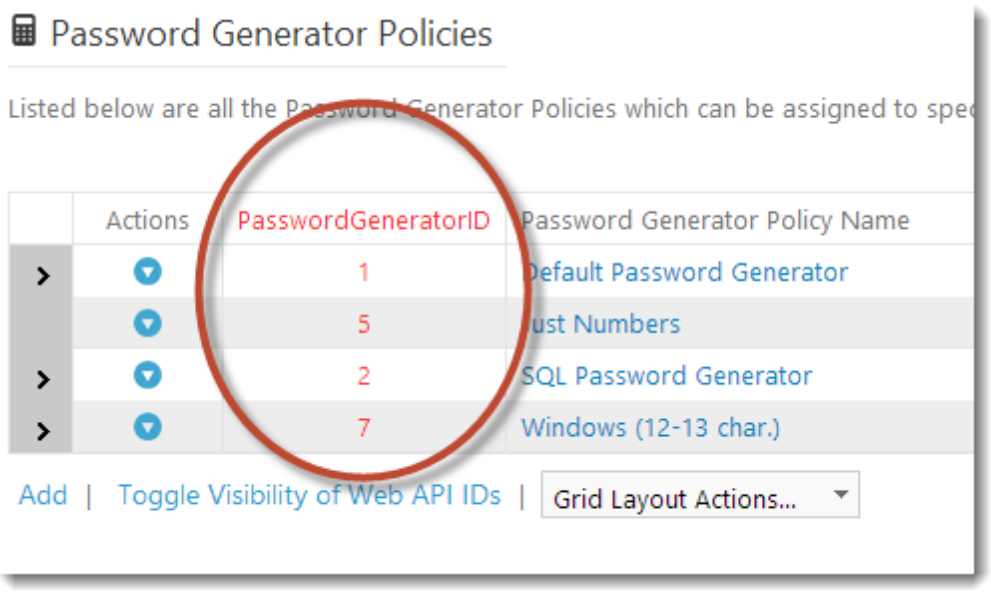


Once a Password Generator Policy has been created, it can be assigned to a Password List or Password List Template, by editing the appropriate settings, as per this screenshot below. When your users now click on the icon, the random password generated will be based on the selected Password Generator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



16 Password Lists

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

From this screen, the following features are available:

Navigating to, and viewing a Password List

By clicking on one of the 'Password List' hyperlinks in the grid, you will be redirected to the appropriate Password List screen.

Note: When you view the Password Lists screen via Administration -> Password Lists, the passwords themselves will be hidden, and most features will be disabled. The intention of navigating this way is to fix any permissions issues on the Password List, or correcting any possible settings issue. The following warning will be displayed on the screen when navigating to a Password List this way:

Note: As you have navigated to this page from the 'Administration' area, certain functions to view or modify passwords have been disabled.

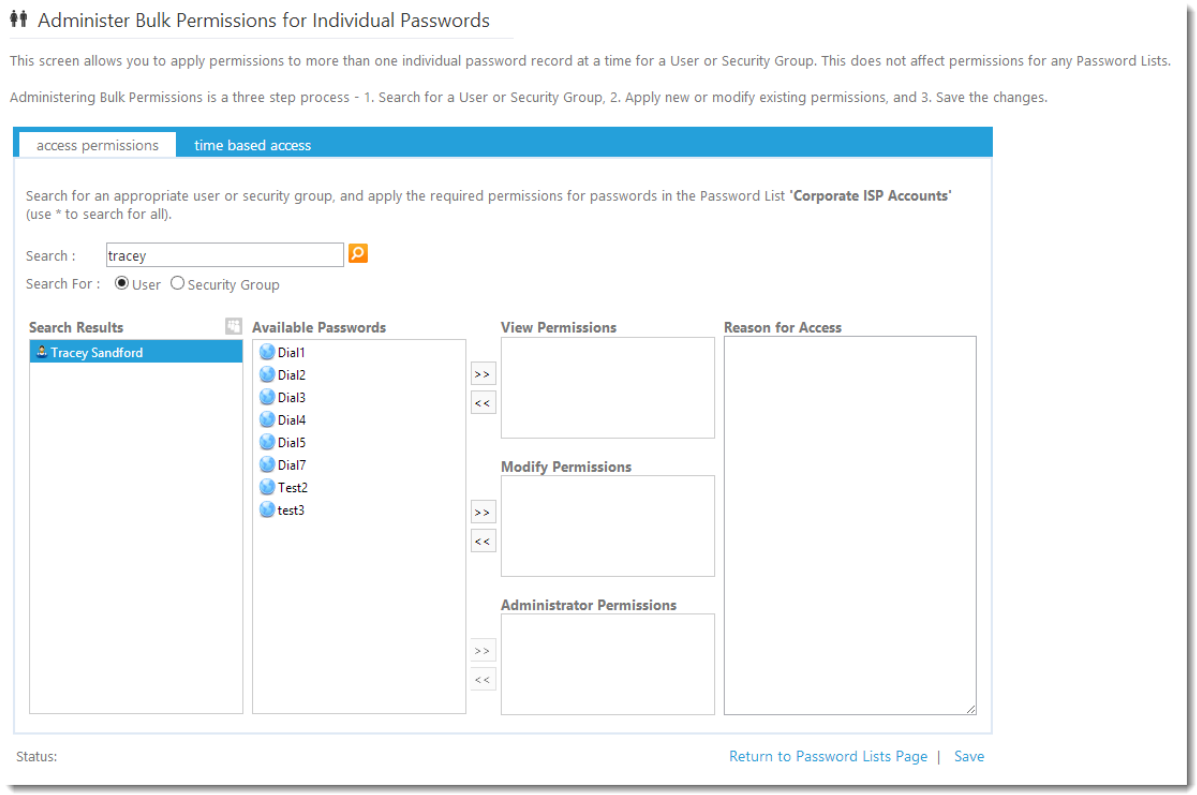
Edit Password List Details

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.

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.



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.

Warning: You are prompted twice to delete a Password List, or there is no Recycle Bin in the event you do delete one - so be sure you no longer require the passwords in this List. If you accidentally delete a Password List and still require it, you will need to ask your DBAs restored a copy of the database.

Add Password List

By clicking on the 'Add Password Lists' button, you will be able to add a new Password List to Passwordstate.

Note: Please refer to the Passwordstate User Manual for detailed instructions on settings which can be applied to new Password Lists or Templates.

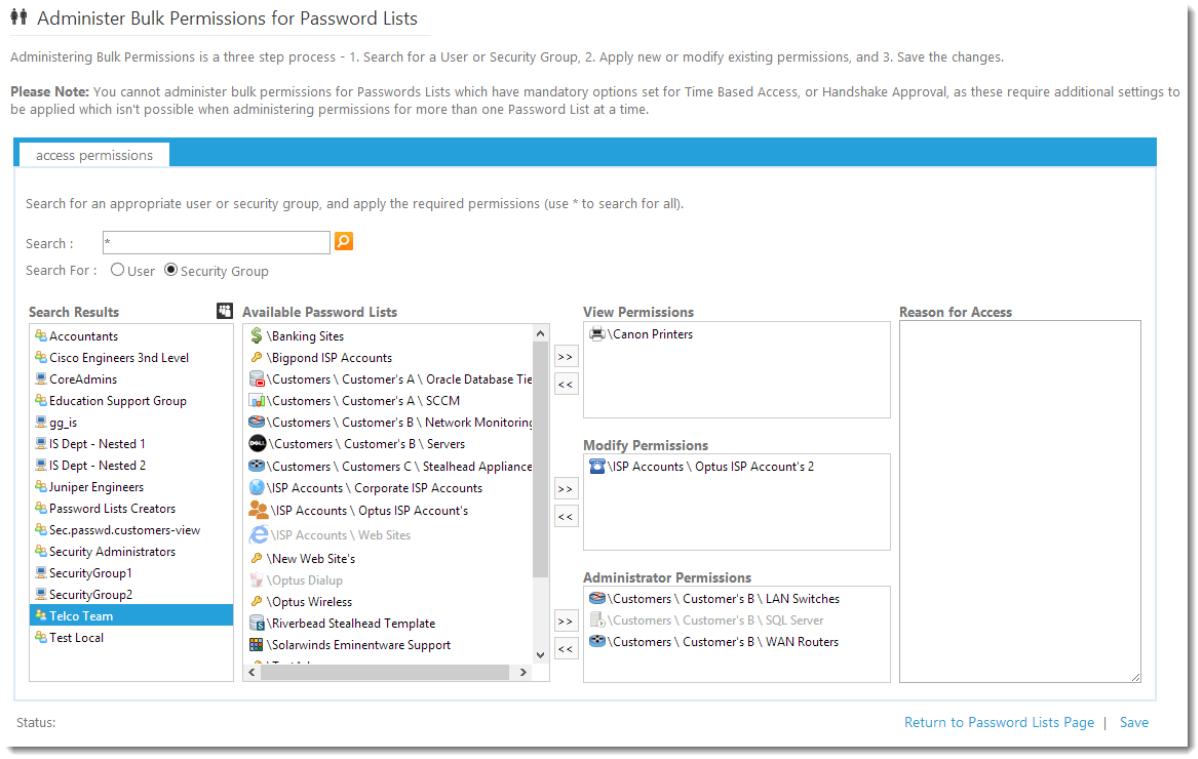
Administer Bulk Permissions

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, or Handshake approval.

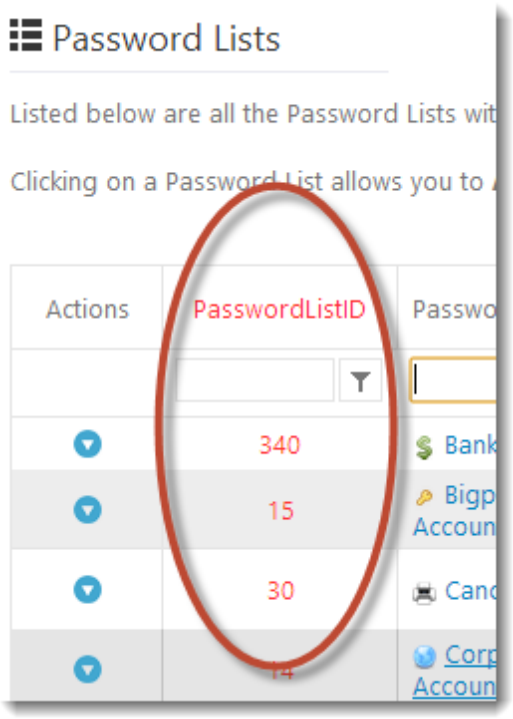


Export

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

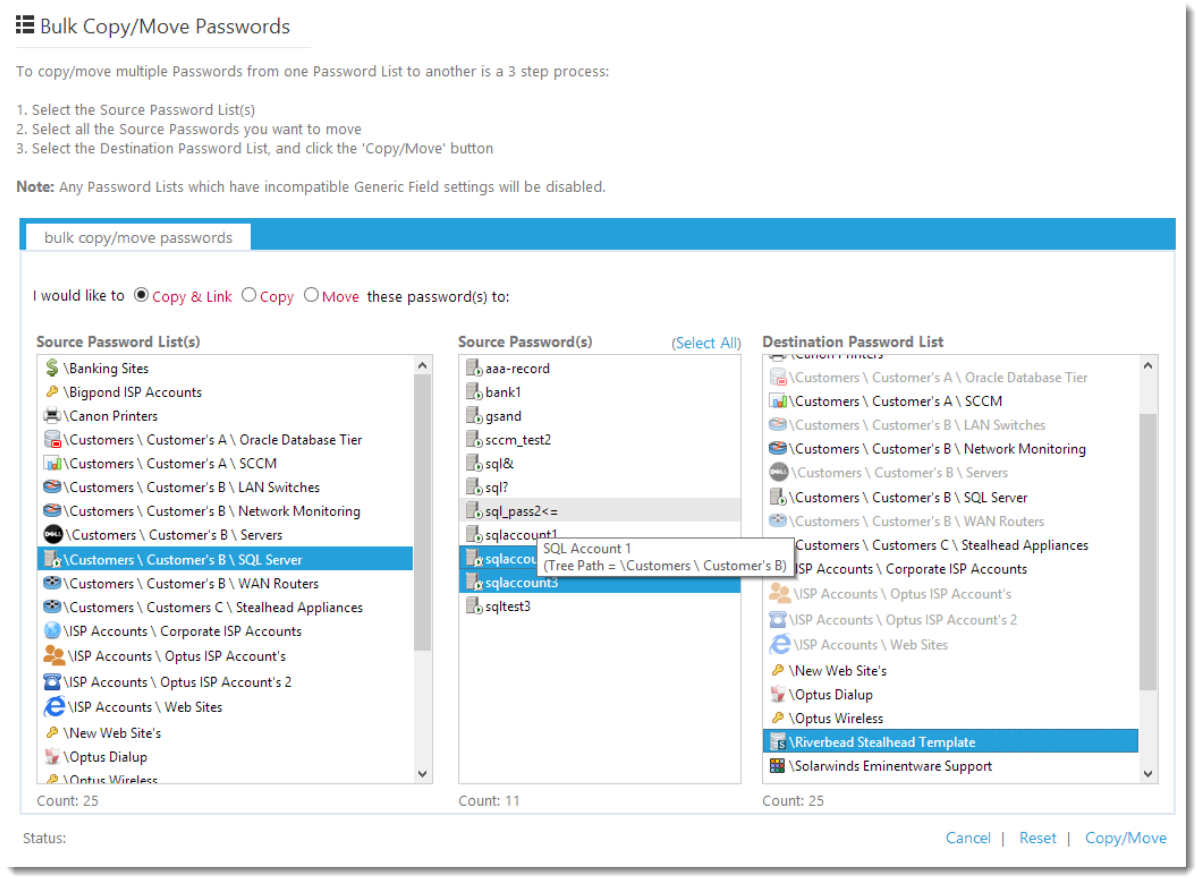
The Toggle ID Column Visibility button will either show or hide the PasswordListID value for each of the Password Lists. These PasswordListID values may be required if you are using the Passwordstate API, or the Bulk Password Import feature below.



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.

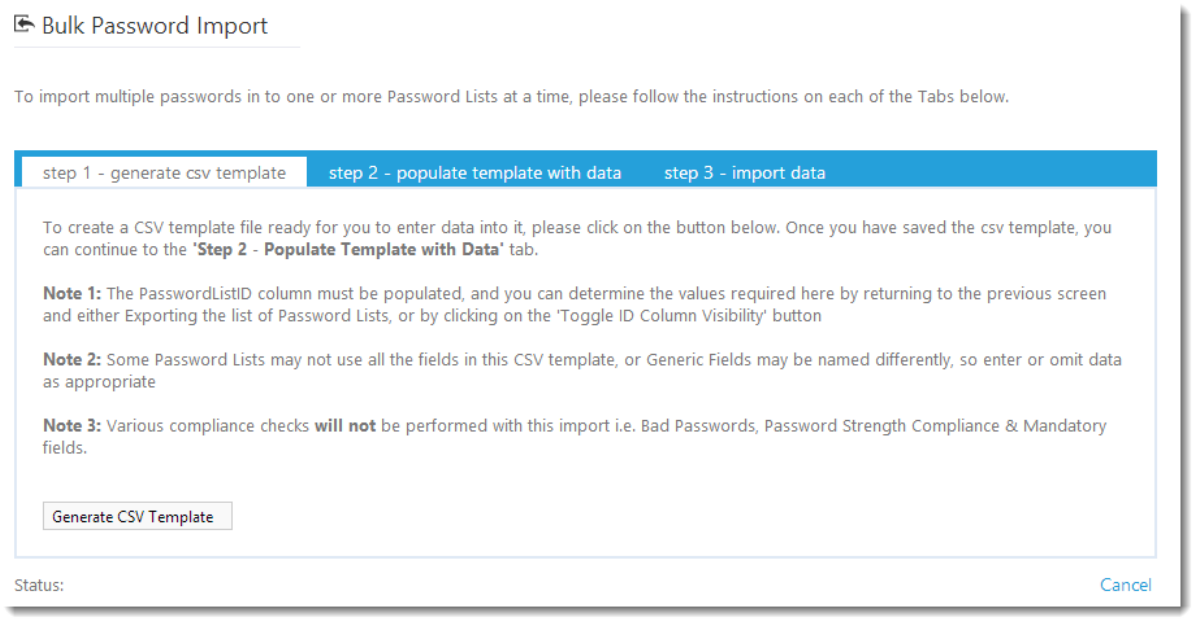


Bulk Password Import

The Bulk Password Import feature is useful when you are migrating data from another system, as it allows you to import multiple passwords records into multiple different Password Lists at once.

To import passwords in bulk is a 3 step process:

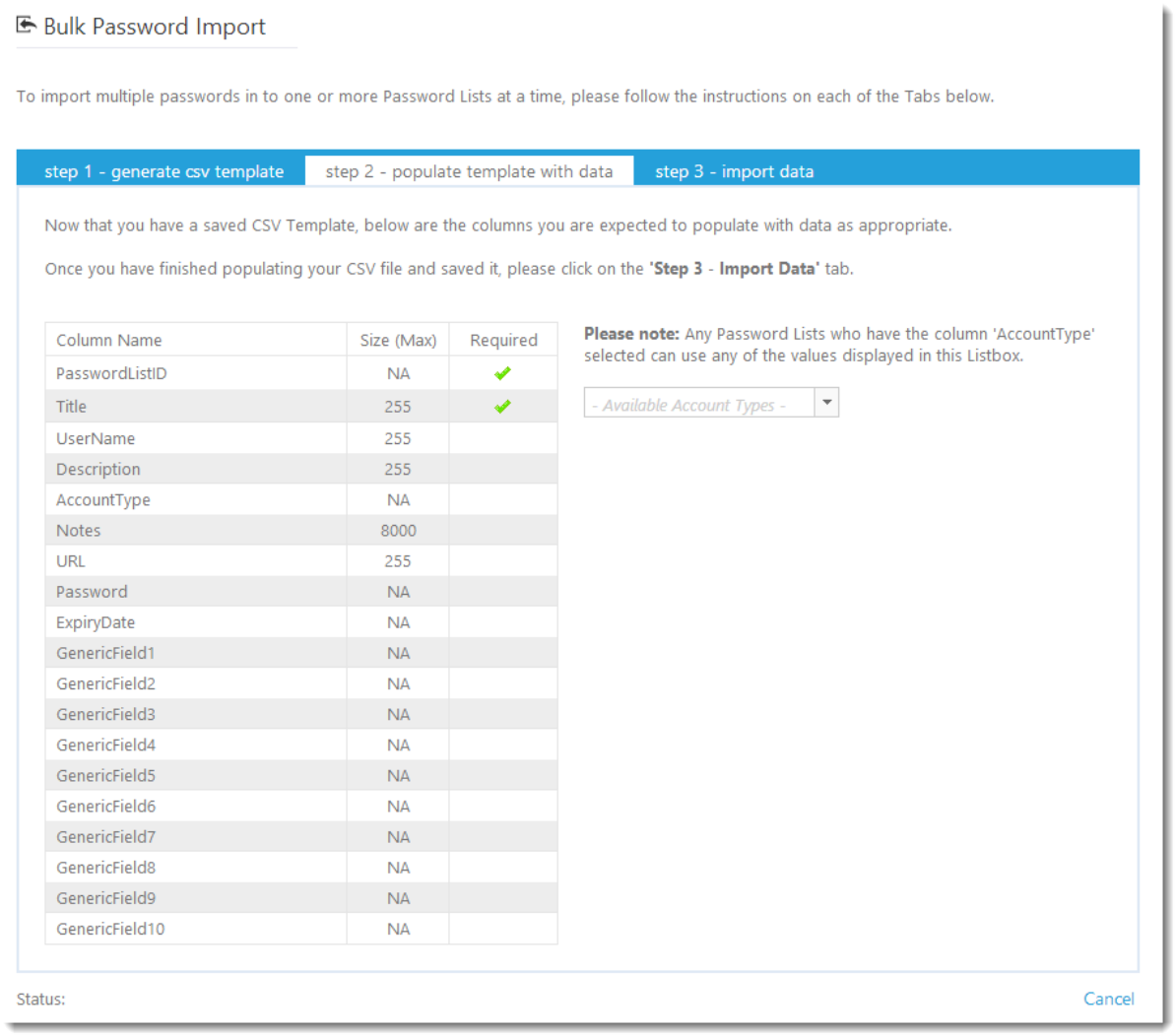
Step 1 - Generate CSV Template
By clicking on the 'Generate CSV Template' button you will be able to save an empty csv template file to your file system. It is this template you need to populate with data, ready for import.



Step 2 - Populate Template with Data
The screenshot below shows the fields which are populated in the csv template file, which fields are required, and the maximum size of any fields.

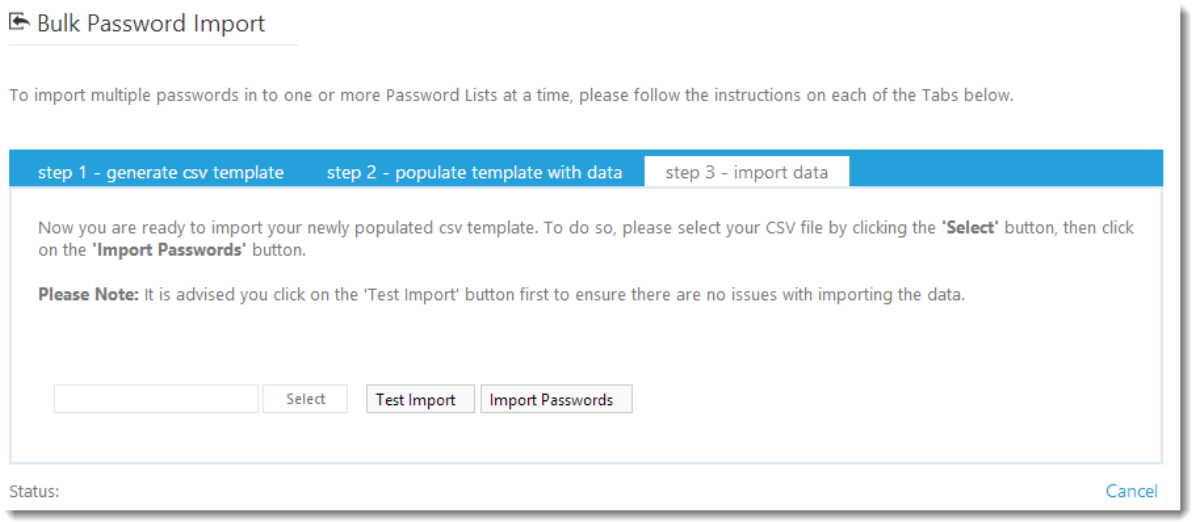
You will notice 10 Generic Fields in the csv template. By default, Password Lists are not configured to use any of the available Generic Fields, but it's possible they may have been configured to use them. Generally the Generic Fields are named differently, but those names cannot be shown in the csv template, as each Password List may have named them differently. You will need to ensure you populate the csv template file with the correct fields for each of the different Password Lists you are importing into.

Note 1: If a field is not 'Required', then you can leave it blank in the csv template
Note 2: The PasswordListID field is required so the import process knows which Password Lists to import the passwords into. The PasswordListID values can be determined by returning to the previous screen and either Exporting the list of Password Lists, or by clicking on the 'Toggle ID Column Visibility' button
Note 3: Various compliance checks will not be performed with this import i.e. Bad Passwords, Password Strength Compliance & Mandatory fields



Step 3 - Import Data

Once you have populated the csv file with the required data, the 'Step 3' tab allows you to either test the import process, or perform the actual import. It is recommended you test the import process first, and any errors will be reported back to you, including the line number in the csv file so you're able to correct the data.

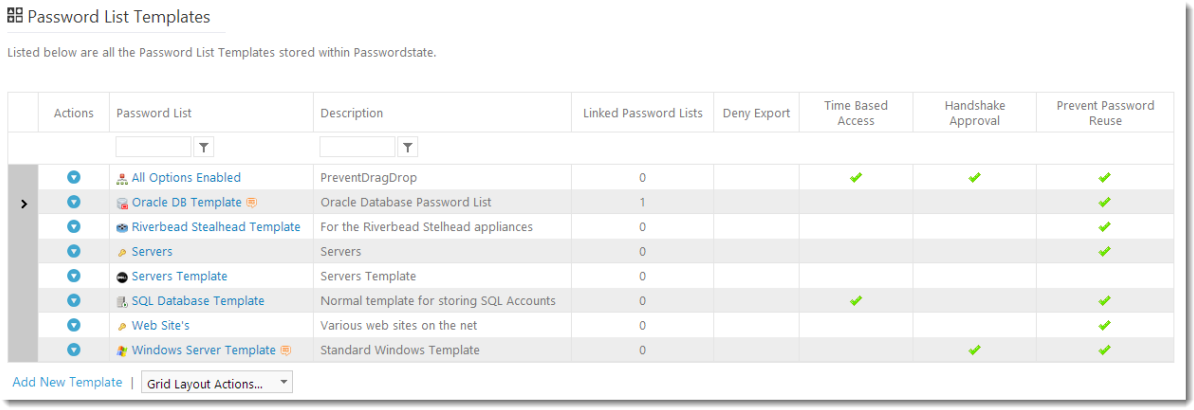


17 Password List Templates

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.

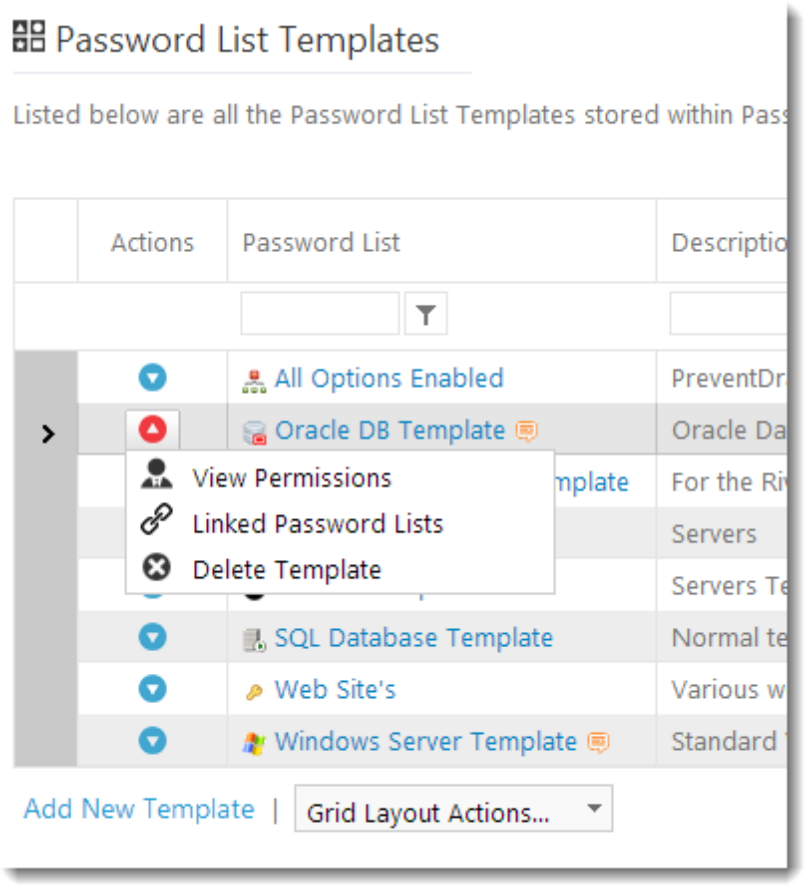
Caution: When editing a Template's settings when it is linked to other Password Lists, if you change any of the Field Types for any Generic Fields, these fields will have their data cleared/ blanked in the database when you click on the 'Save' button. This is because the different Generic Field Field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

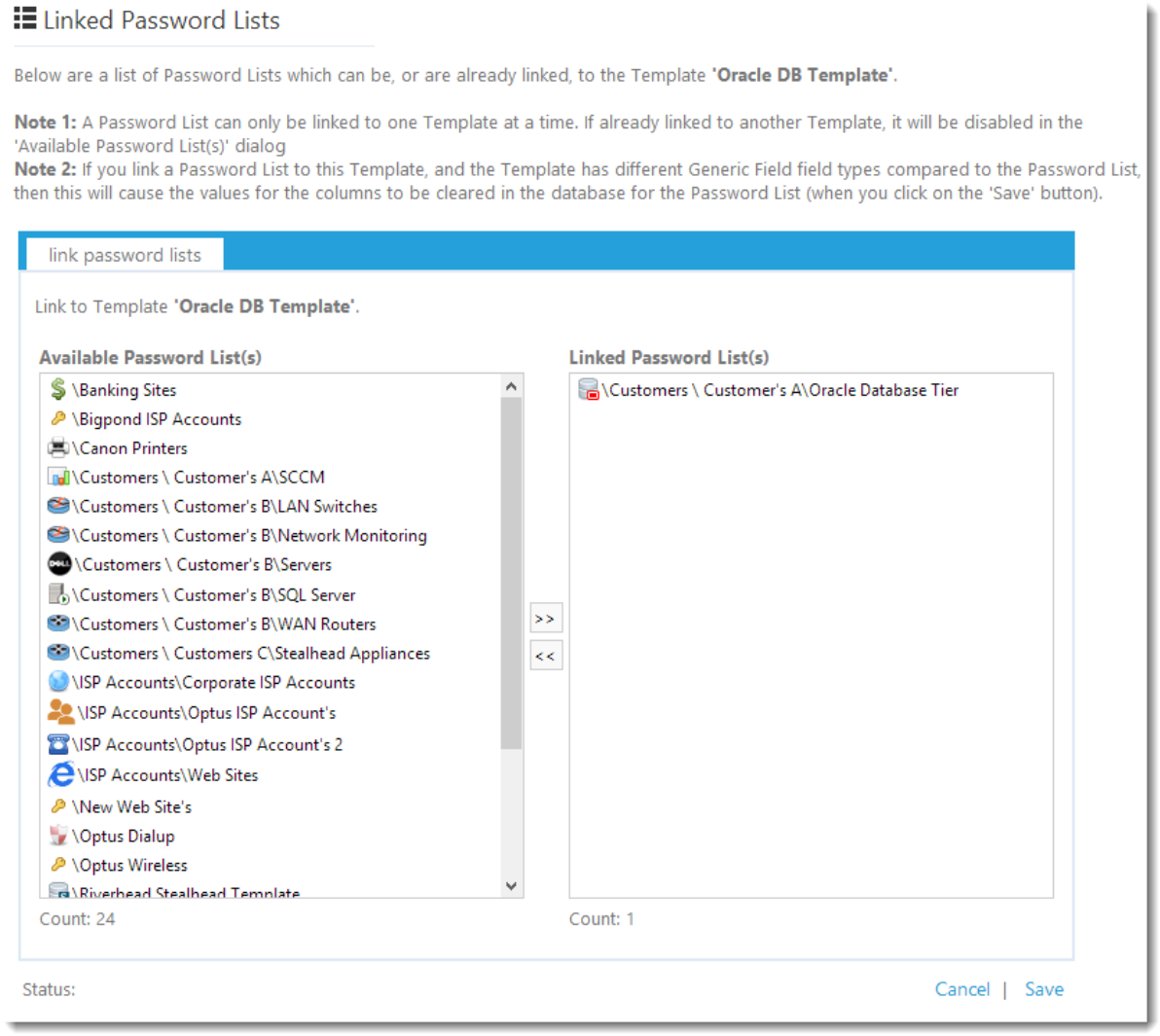


Linked Password Lists

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.



18 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.

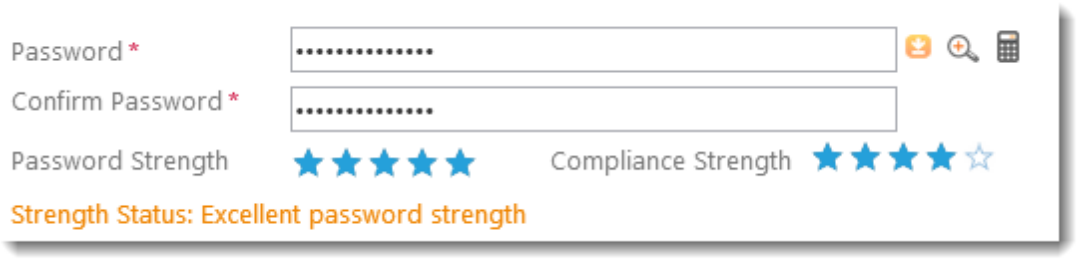
Policy Settings Tab

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

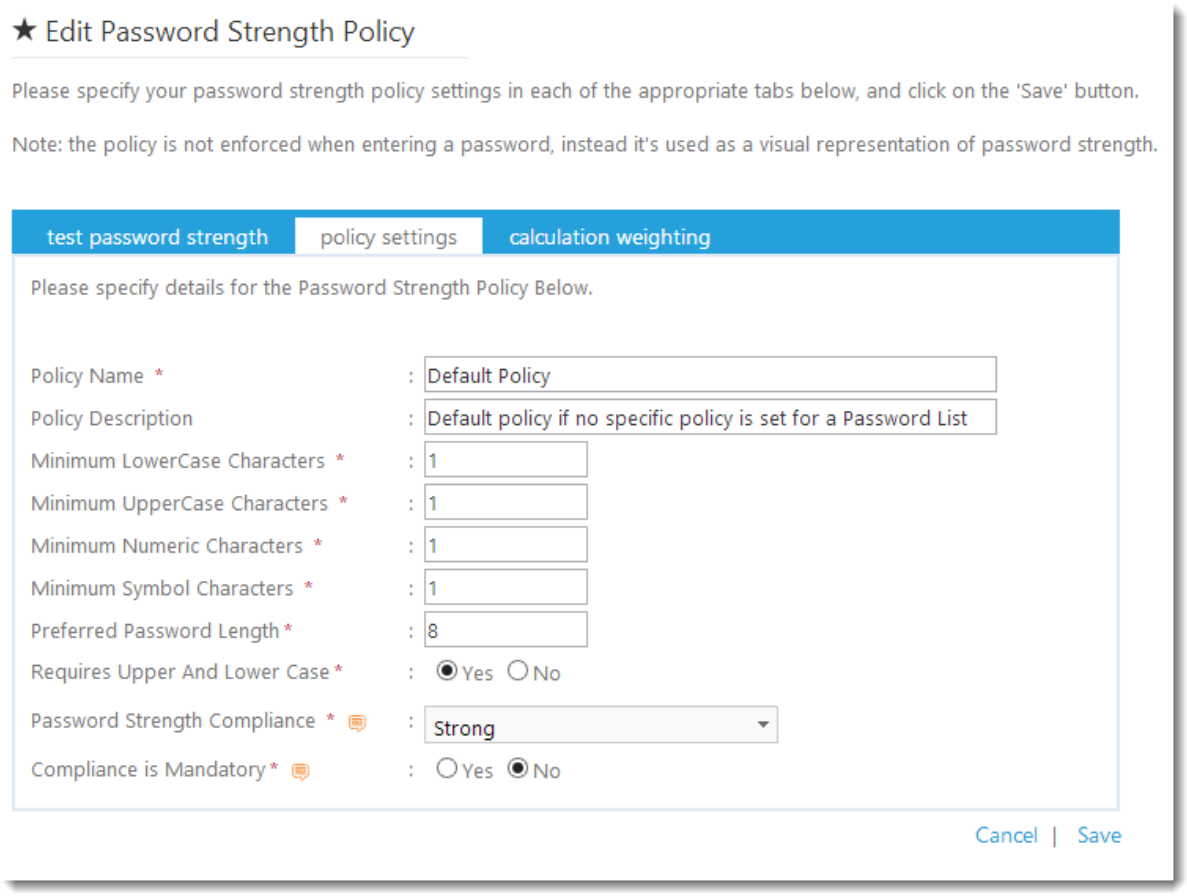
- Minimum LowerCase Characters - specifies how many lowercase characters are required as a minimum (abcd, etc)
- Minimum UpperCase Characters - specifies how many uppercase characters are required as a

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



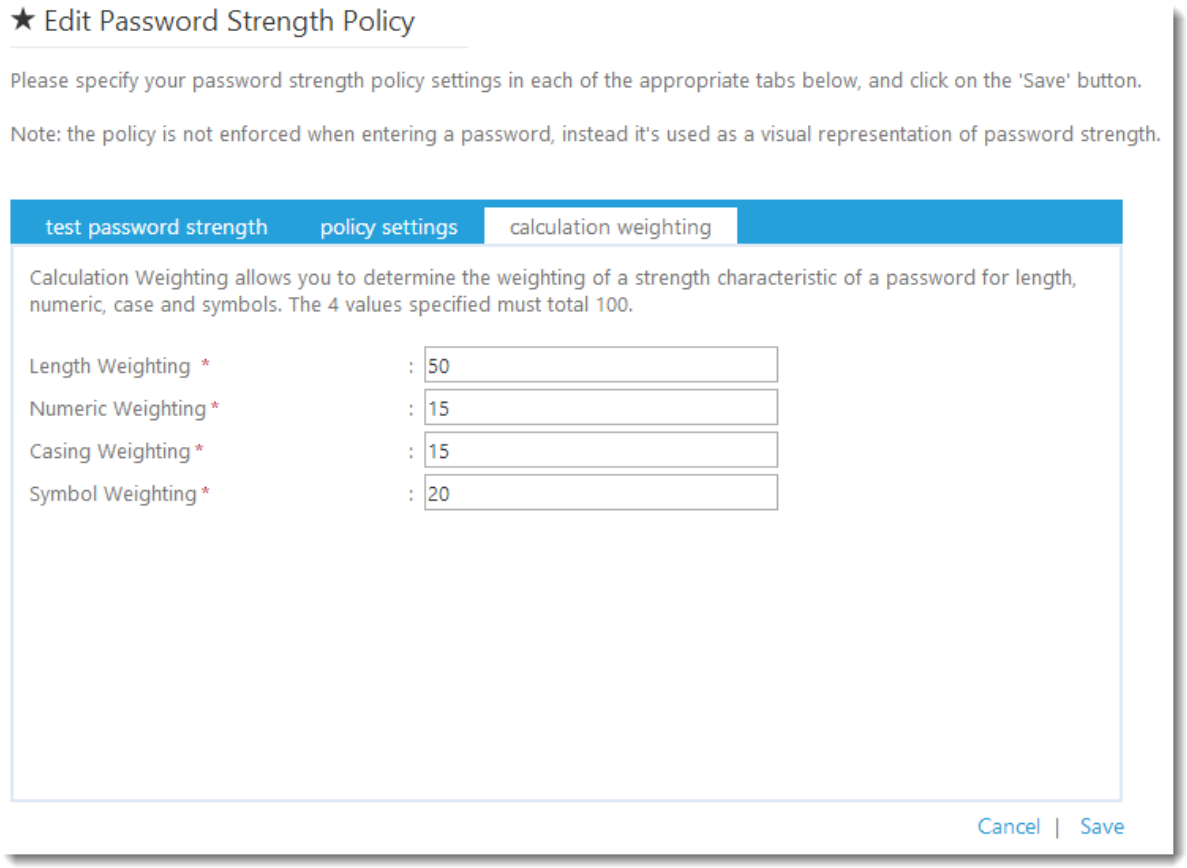
- Compliance is Mandatory - if this option is set to Yes, the user will not be able to save the password record if the strength of the password they're creating does not meet the 'Password Strength Compliance' setting above



Calculated Weighting Tab

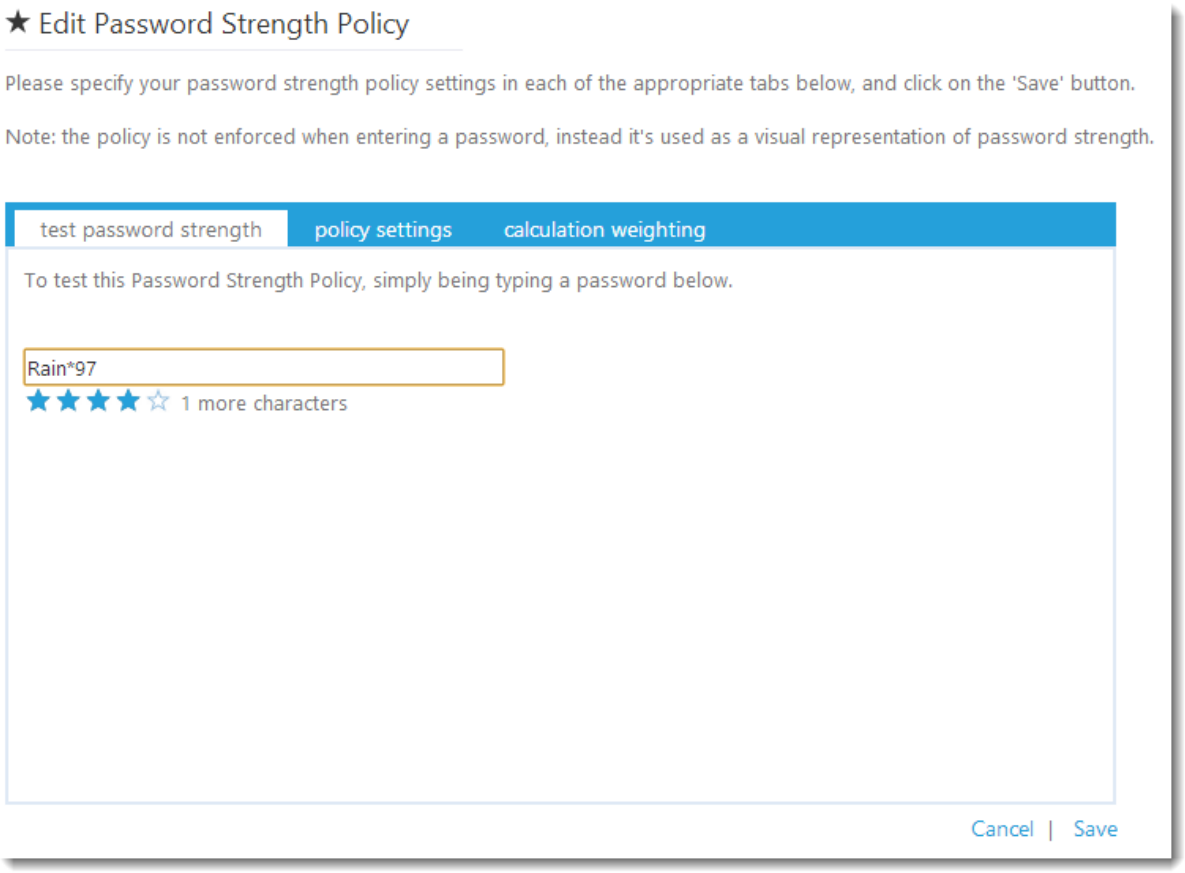
The Calculated Weighting Tab allows you to specify the weighting of a strength characteristic of a password for length, numeric, case and symbols. The higher the weighting, the more important the category is deemed to be.

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.



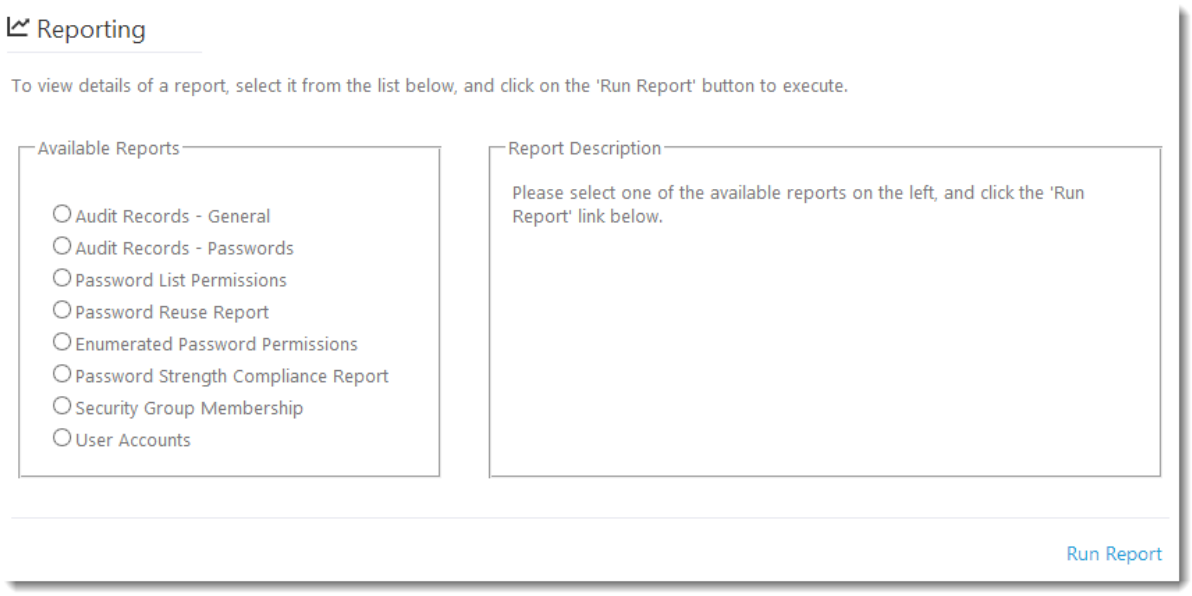
19 Reporting

The Reporting feature allows you to run the following reports, which will be exported to csv files for further analysis if required:

- Audit Records (General) - exports a sorted list of all general audit records, not specific to Passwords or Password Lists. Please note this could be a large CSV file, so may take some time to generate
- Audit Records (Passwords) - exports a sorted list of all audit records specific to Passwords and Password Lists. Please note this could be a large CSV file, so may take some time to generate
- Password List Permissions - exports a sorted list of permissions for all Password Lists, and any permissions applied to individual passwords. Note: if the Title field is populated in this report, then it means the permissions have been applied to the individual password record
- Password Reuse Report - exports a list of records where the same password have been used more than once.
- Enumerated Password Permissions - exports a sorted list of permissions for every individual password recorded in Passwordstate (excluding Private Password Lists). It will show permissions based on users, and will enumerate any Security Groups into User Account details
- Password Strength Compliance Report - exports a sorted list of all Password Lists, the strength

of each password, and whether or not the Password Strength is compliant or not
- Security Group Membership - exports a sorted list of Security Groups within Passwordstate, and their User Accounts membership
- User Accounts - exports a sorted list of User Accounts within Passwordstate

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



20 Security Administrators

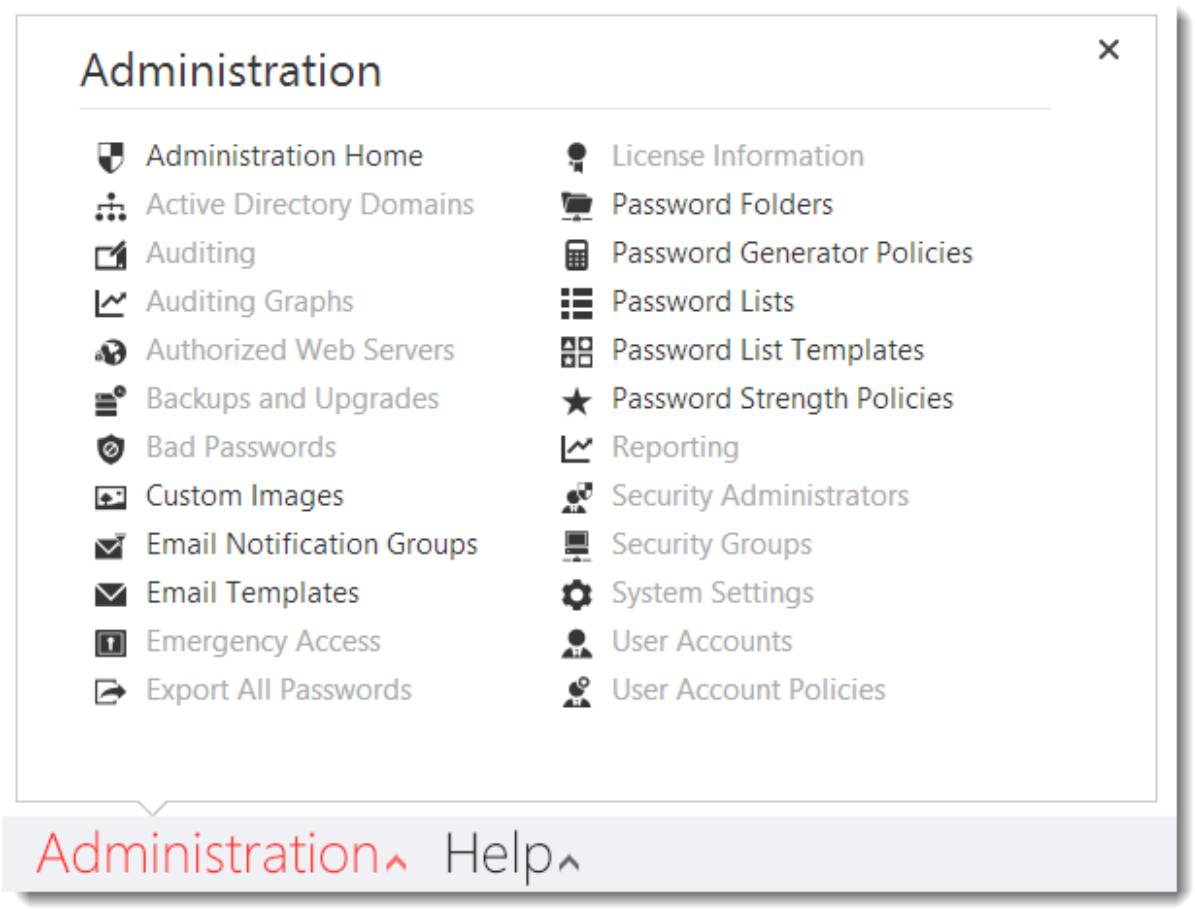
The 'Security Administrator' role in Passwordstate provides access to one or more features in the Administration area. If a user's account is not set up as a Security Administrator, the Administration menu on the bottom horizontal menu will not be visible to them.

There are 15 different types of roles a Security Administrator account can be configured for, with each role providing access to various screens/features in the Administration area. The roles are:

Role	Screen/Feature Access
Active Directory Domains	Active Directory Domains
Auditing	Auditing & Auditing Graphs
Bad Passwords	Bad Passwords
Email Templates	Email Notification Groups & Email Templates
Emergency Access	Emergency Access
Export All Passwords	Export All Passwords
Licensing	License Information
Password Generator	Password Generator Policies
Password Lists	Custom Images, Password Folders, Password Lists & Password List Templates
Password Strength Policy	Password Strength Policies
Reporting	Reporting

Security Administrators	Security Administrators
Security Groups	Security Groups
System Settings	Authorized Web Servers, Backups and Upgrades & System Settings
User Accounts	User Accounts & User Account Policies

If you deselect one or more of the Security Administrator roles for a user, the corresponding menu item will be disabled for the Administration menu, as per the following graphic.



21 Security Groups

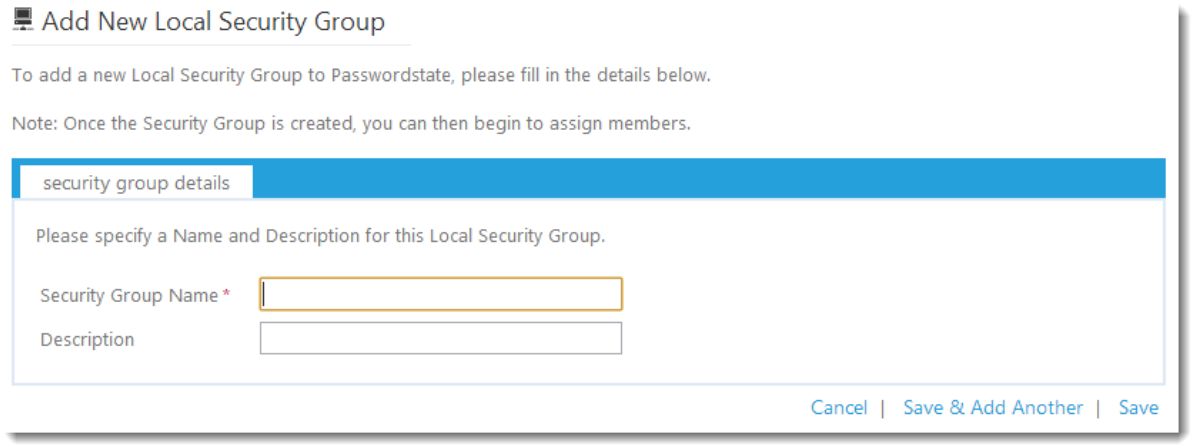
Security Groups allows you to manage either local security groups created within Passwordstate, or Active Directory security groups. These groups can then be used for applying permissions to Password Lists, or to give/deny access to various features.

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

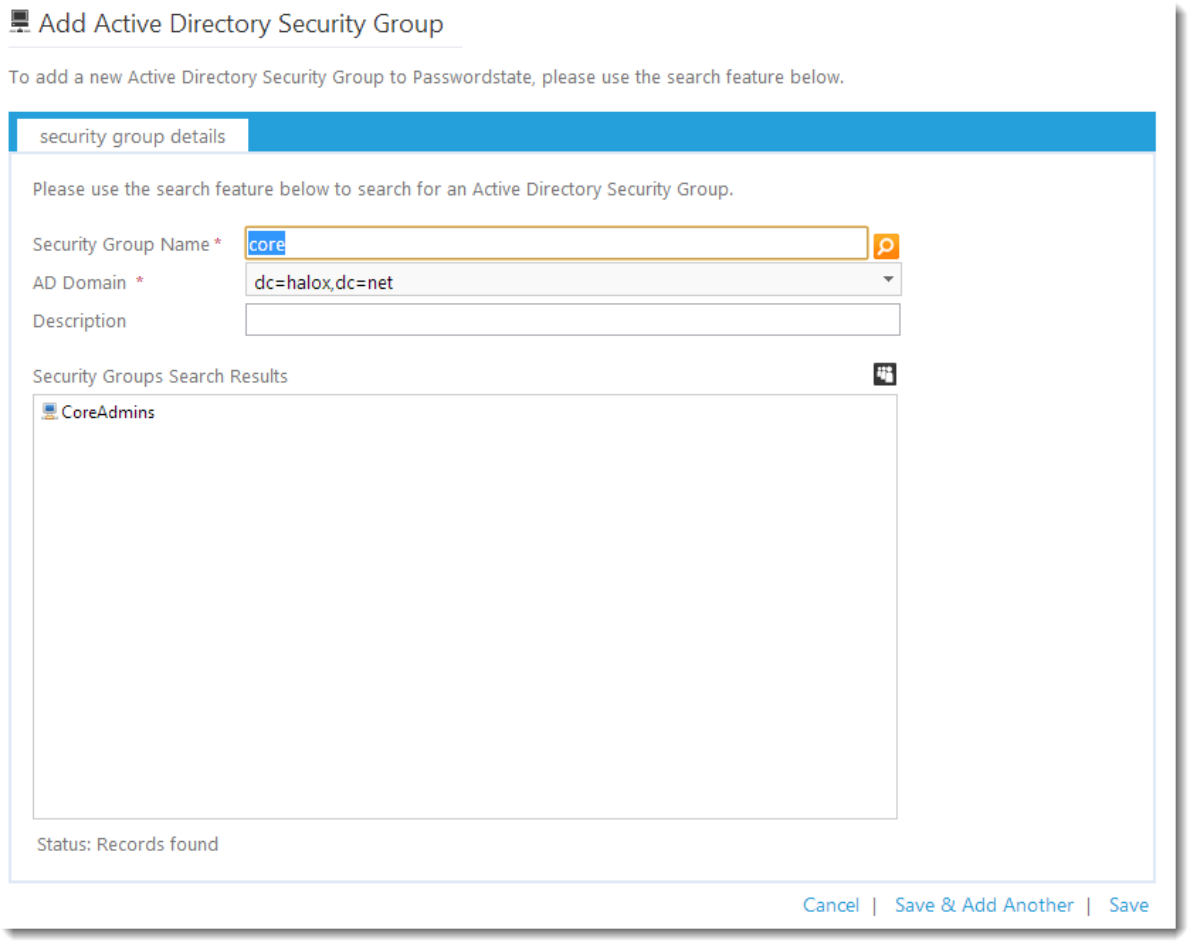


Add Active Directory Security Group

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

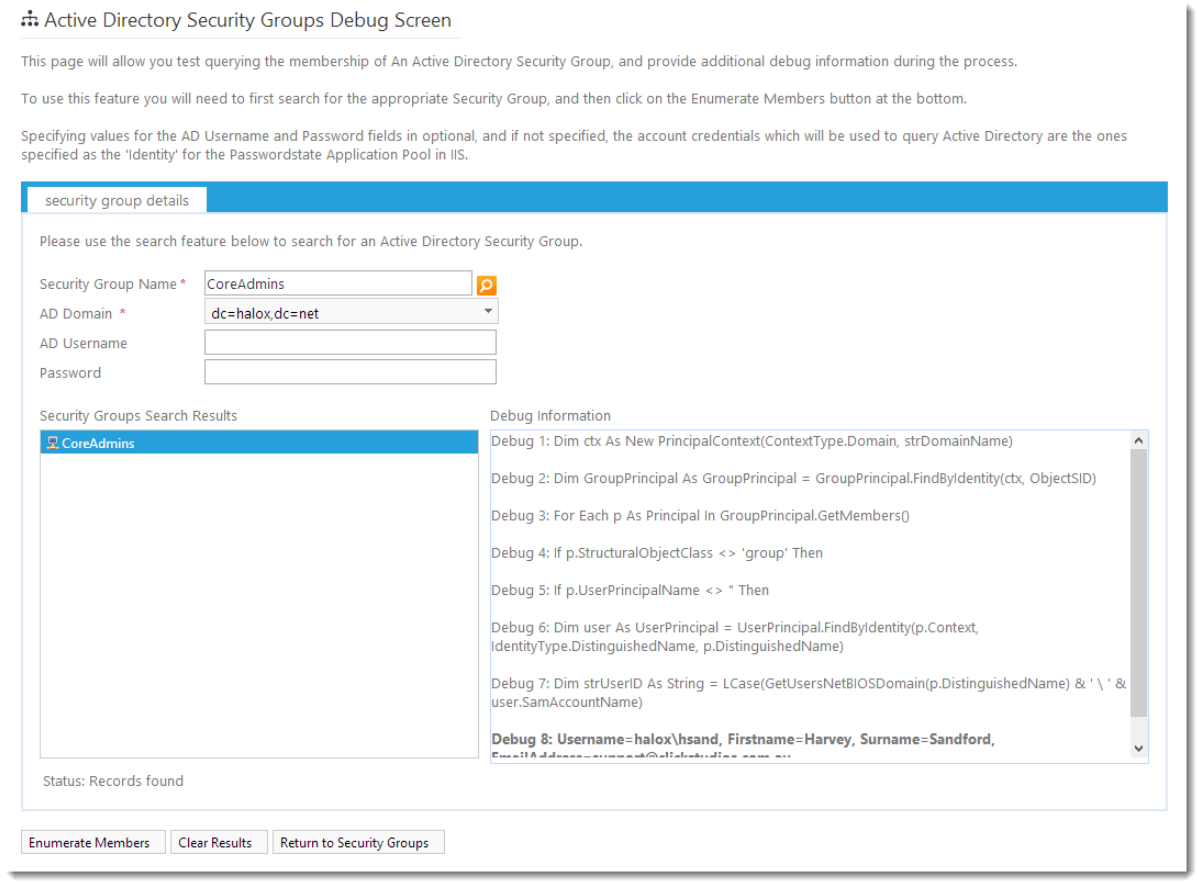
Note 1: When you add a security group, if the user account does not already exist in Passwordstate (on the User Accounts screen), there is on option on the screen Administration -> System Settings -> Active Directory Options Tab which allows you to also automatically add the user account

Note 2: If you have issues querying Active Directory, please see the section 'Active Directory Lookup Permissions' below



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.

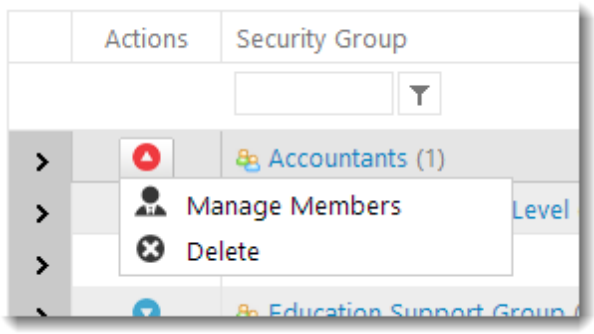


Local Security Group Actions Menu

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

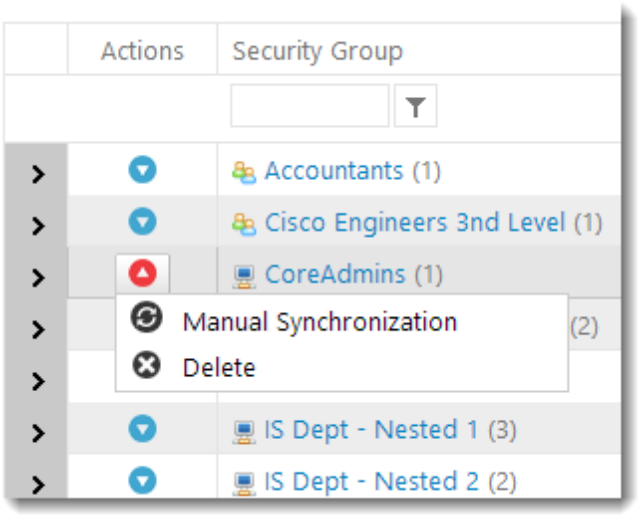
Note: If the Security Group has been used to apply permissions anywhere within Passwordstate, removing members from the security group, or deleting the Security Group itself, will removes one or more user's access



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



Active Directory Lookup Permissions

If you are having some issues querying the membership of an Active Directory Security Group,

then there may be a permission issue with the configuration of the Passwordstate Application Pool in Internet Information Services (IIS), or the account the Passwordstate Windows Service is configured to use. You may need to specify a domain account with sufficient privileges to query Active Directory, under the following circumstances:

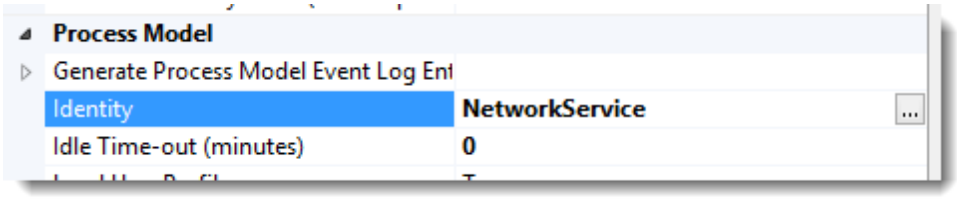
- Issues query AD through the web interface. If this is the case, then please refer to the instructions below titles 'Active Directory & IIS Application Pool'
- Issues with the scheduled synchronization the Passwordstate Windows Service performs, as evident by errors in the Event Log on your web server, or by security groups not updating as you would expect them to. If this is the case, then please refer to the instructions below titles 'Active Directory & Passwordstate Windows Service'

Active Directory & IIS Application Pool

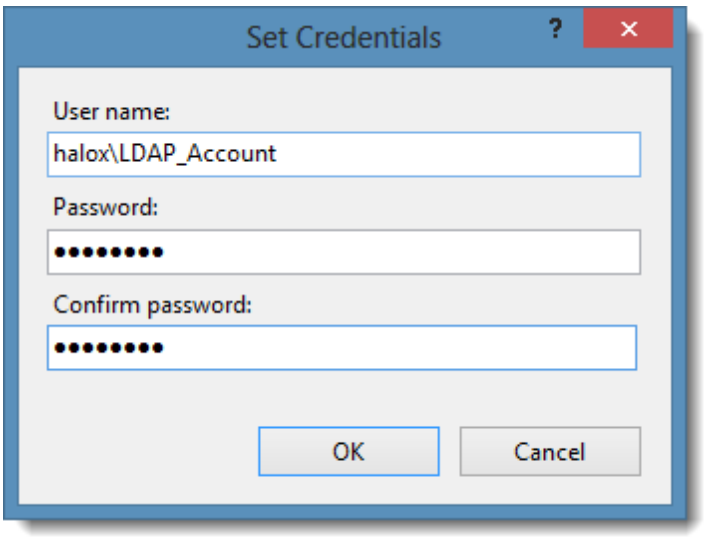
By default, the Passwordstate Application Pool in IIS uses the account 'NETWORK SERVICE', which is part of Internet Information Services (IIS).

If you experience any errors when try to add users via Active Directory or query Security Groups, then it's likely your Active Directory setup only allows certain accounts to query it. If this is the case, then you will need to modify the IIS configuration to specify a different account. To do this, you can follow these instructions.

1. Open Internet Information Services (IIS) Manager on your web server
2. Click on 'Application Pools' in the 'Connections' panel
3. Right click on the application pool 'Passwordstate', and select 'Advanced Settings'
4. Look for the setting 'Identity' click on **ApplicationPoolIdentity**, and then on the ellipses button as per this screenshot:



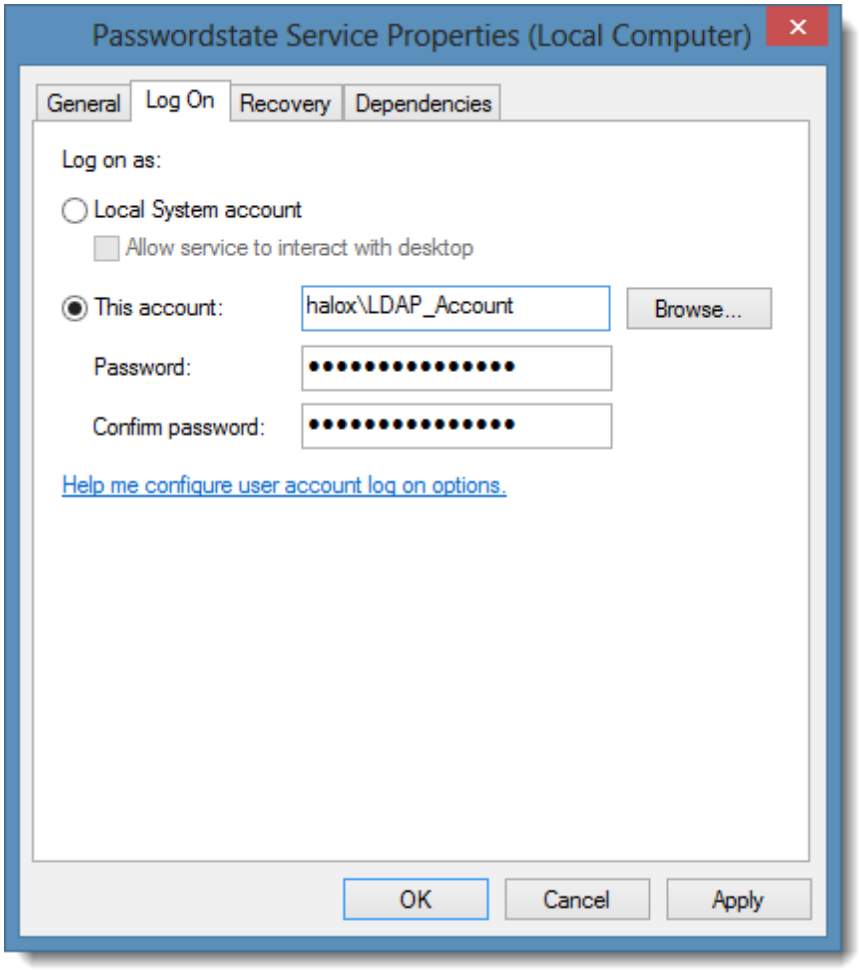
5. Select 'Custom account' and then specify the appropriate account details such as the example provided in the following screenshot:



6. Click on all the 'OK' buttons to close the windows, and then restart the Passwordstate site in IIS

Active Directory & Passwordstate Windows Service

If the scheduled synchronization of Security Group memberships does not appear to be working, or you are seeing Event Log Errors on your web server, you may need to also modify the 'Log On' rights for the Passwordstate Windows Service.



22 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.

Miscellaneous Tab	Various settings which don't fall into any other of the 'Tab' categories
Password List Options Tab	Settings which are specific to Password Lists
Password Options Tab	Settings which are specific to individual password records
Email Alerts & Options Tab	Email Server settings, and multiple options for various email notifications
Proxy & Syslog Servers Tab	Specify proxy settings or syslog settings for Passwordstate to use

Active Directory Options Tab	Various settings for synchronizing Active Directory user accounts, security groups, and password synchronization with Active Directory
Authentication Options Tab	Various options and settings for authenticating to the Passwordstate web site
User Acceptance Policy Tab	Specify a popop 'User Acceptance Policy' which users must read when they access the Passwordstate web site
Check for Updates Tab	Specify how frequently Passwordstate should check for new versions
Custom Logos Tab	Specify your own logos to use on various screens and dialogs
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
Allowed IP Ranges Tab	Specify which IP Addresses or IP Address Ranges are allowed to access the Passwordstate web site or API
API Key Tab	Specify a System Wide API Key which can be used for various API calls

22.1 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.

Execute Daily Tasks/Reports at

The following processes will occur at the time yet set this option:

- Emailing of the Expiring Passwords report
- Emailing of the Daily Audit report
- Querying for any audit data tamper detection

Specify the Base URL used in any emails generated by Passwordstate

This URL field is used as hyperlinks in any emails generated from Passwordstate.

Force the use of an SSL Certificate (HTTPS)

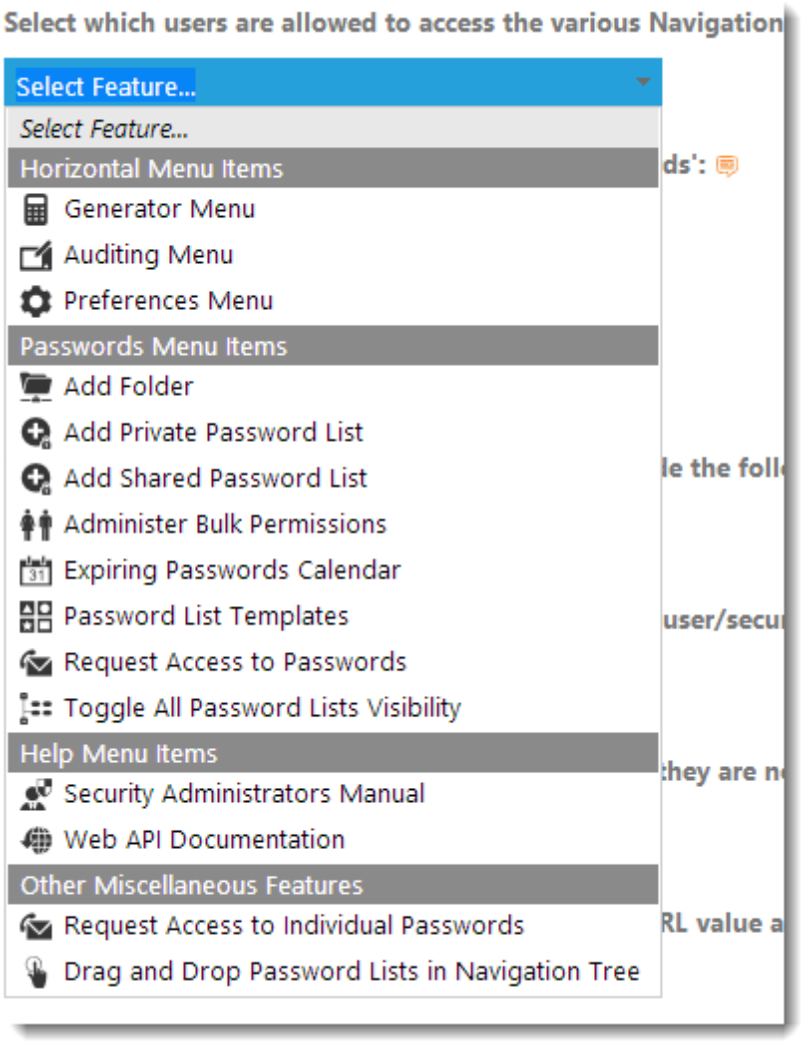
When set to Yes, if the user types HTTP into the browser address bar, they will be redirected to HTTPS - which securely encrypts all traffic between the user's browser and the web site. The API will return a 403 Forbidden message if HTTPS is not used.

Show Password List Auditing data 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 - this will also remove the Password List from the 'Auditing' section that users have access to.

Select which users are allowed to access the various Navigation Menu Items at the bottom of the screen, and various other Miscellaneous Features

By selecting one of the available options in this drop-down list, you can control who is allow to access the selected feature - you can choose either all users of Passwordstate, or just specific user accounts or security groups.



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.

Enable option for purging of Auditing records

If you don't want to give Security Administrators the ability to purge (delete) auditing records on the Auditing page, then you can hide the controls which allow the purging.

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

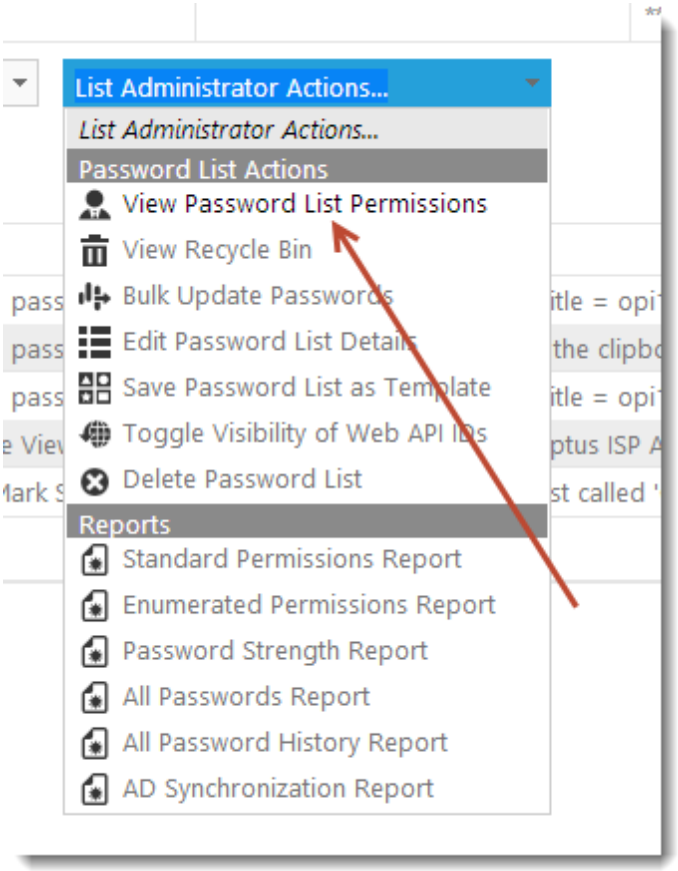
Password Lists or individual Passwords they don't already have access to - assuming you have enabled this feature for them. As viewing password related data can be sensitive by its very nature, you can choose to hide various fields on the screen from your users, either the Username, Description or Notes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

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

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

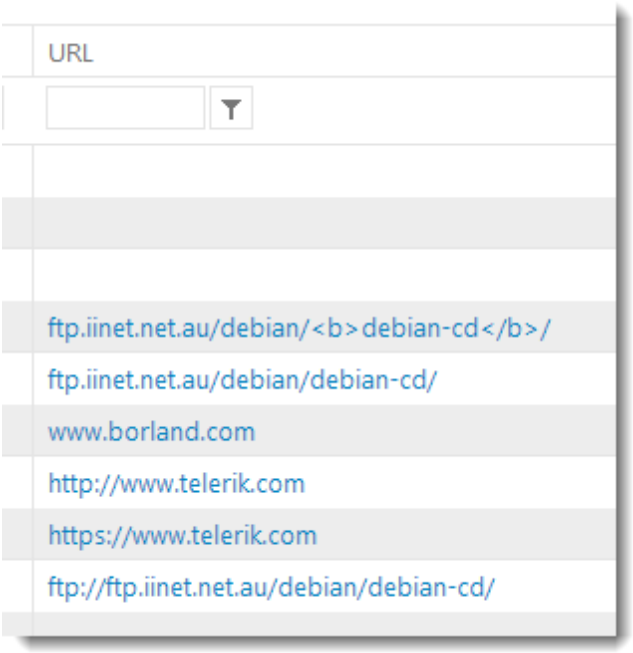
Allow users to view Password List permissions when they are not Administrators of the Password List

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.

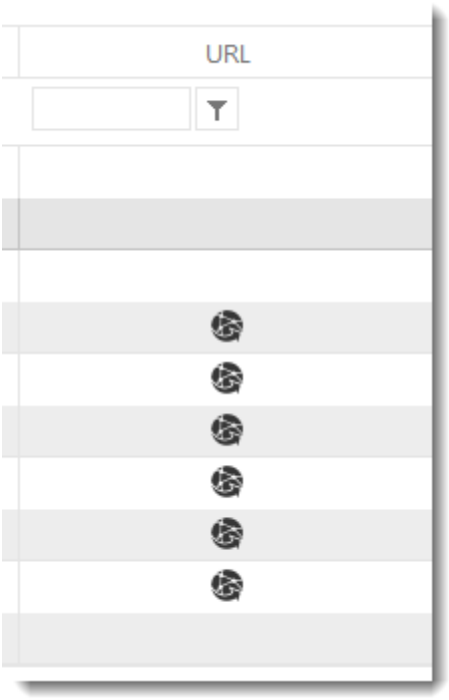


When displaying URL columns in grids, display the URL value as a

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



22.2 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.

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.

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.

When creating new Shared Password Lists, based the settings and permissions on the following Template

When your users create new Password Lists, you can specify a template here as a basis for the new Password List's settings. This allows you to provide some consistency across multiple Password Lists if required.

Note: This setting does not affect Private Password Lists.

Allow users to override the Template based settings above for new Shared Password Lists, with a Template they select in their 'Preferences' area

In addition to setting a Template above as the default settings for newly created Shared Password Lists, users can by default specify their own template to use in the 'Preferences' area. If you wish to enforce a single Template to be used by all users, you can do so with this option.

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 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 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.

22.3 Password Options Tab

The Password Options Tab has multiple settings applicable to Password values being visible on the screen, clearing the clipboard, 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.

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.

Automatically clear clipboard after the following specified number of seconds

When your users copy Passwords to the clipboard using the icon, you can specify how long before the clipboard is automatically cleared.

Note: This option is only applicable to Internet Explorer, as it's not possible to automatically clear the clipboard with Firefox or Chrome - a button will appear at the top right-hand side of the screen allowing you to clear the clipboard if required.

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

22.4 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

There are two different scenarios in which your users must authenticate when using Passwordstate:

1. When they first browse to the web site
2. If a Password List is configured to require an 'Additional Authenticate' step prior to the Password List being accessible

By selecting this option, Security Administrators who have the 'User Accounts' role will be alerted, via email, to any failed login attempts. Failed login attempts are also recorded and reportable on the Auditing screens.

Only send Failed Login Attempt email alerts to Security Administrators if the following conditions are met

If Security Administrators don't wish to be alerted to every single failed login attempt by individual users, you can set a threshold which must be met before an email is sent. Even if this option is used to not be notified every single time, auditing data is recorded for all failed login attempts.

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.

If there are no Password Lists Administrators assigned to a Password List when a user 'requests' new access, 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.

Send email alerts to Security Administrators (with the following role) if tampering of the Auditing table is detected

It's possible, but unlikely, that one of your users may try to edit/delete auditing data directly in the database, in attempt to conceal behavior they don't wish to be reported. By using this option, you can alert Security Administrators of any such activity. In the event tampering is detected, Security Administrators will be able to view which records have been affected, and also compare what data has been modified, facilitating an investigation if required.

Use the following settings to send emails from within Passwordstate

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

22.5 Proxy & Syslog Servers Tab

The Proxy & Syslog Servers Tab allows you to specify proxy server details to allow querying the Click Studios web site for new builds or Passwordstate, or Syslog server details to send all auditing data to.

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: If you are concerned about your Passwordstate web site accessing the Internet, the only file we access is http://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

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.

22.6 Active Directory Options Tab

The Active Directory Options tab allows you to specify various settings for how and when Active Directory User accounts are synchronized with Passwordstate, and what domain account to use to allow synchronizing of Passwords from Passwordstate into Active Directory.

Note: All the Synchronization features below will occur at the frequency you specify on the last option for this screen - they are not immediate. If you require to immediately disable/delete a user account in Passwordstate, you can do so via the User Accounts screen.

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 synchronizing passwords with Active Directory or Windows Server, validates the passwords match before allowing a password to be changed

By enabling this option, any time a user wishes to update a password in Passwordstate and synchronize the change with Active Directory or a Windows Server, the synchronization status of both accounts must first be validated - if the passwords aren't the same, then an update/ synchronization cannot occur. This feature can be useful in preventing a user from creating a Password List enabled for synchronization, and then changing domain/windows passwords when they shouldn't be. This feature also applies to the Automatic Password Rotation feature, and updating passwords with the API.

Allow the Password List setting of 'Show Active Directory & Windows Actions for Passwords which are enabled for Sync'

Disable this option on all Password List & Password List Templates Edit/Add screens by choosing No for this feature. This will prevent users from being able to use the features Enable/Disable/ Unlock/Change Password at next logon, for Active Directory and Windows Server accounts.

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, disabled the account, or simply do nothing.

Note: If you choose to delete the user account in Passwordstate, all access for the user's account will be removed, and any Private Password Lists they may have had will be deleted.

Specify account credentials to allow Windows Password Synchronization

In Passwordstate you can configure a Password List to synchronize the password records with Active Directory if required. This could be user accounts on the domain, or accounts you have created to act as "service accounts". In order to enable synchronization, you most likely will need

to specify a domain account with sufficient privileges to make changes to Active Directory, which you can specify here as part of this option.

For detailed instructions of how to configure permissions and use the Password Synchronization feature in Passwordstate, please see the Knowledge Base article '**Synchronize Passwords with Active Directory on Windows Servers**' in the User Manual.

Note 1: You can only synchronize passwords from Passwordstate into Active Directory, not the other way around - it's not possible to decrypt the values of AD passwords.
Note 2: You may also need to configure the Passwordstate Application Pool in Internet Information Services (IIS) to use an account to 'read' data from Active Directory - the account you specify above is only used to write data to Active Directory - although they can be the same account if you wish. Please refer to the Passwordstate Installation Instructions for how to configure the Application Pool in IIS.
Note 3: If you change the domain account used here, or modify the permissions for this account i.e. add to a new security group, then it is recommended you restart the Passwordstate Windows Service.

Synchronize Security Group Memberships, and User Account status at

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

22.7 Authentication Options Tab

The Authentication Options Tab provides various settings for when your users first authenticate to the Passwordstate web site.

Note 1: Options will be different on this screen, depending on if you have installed the Active Directory integrated version of Passwordstate, or the Forms-Based Authentication version.
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 authenticate.

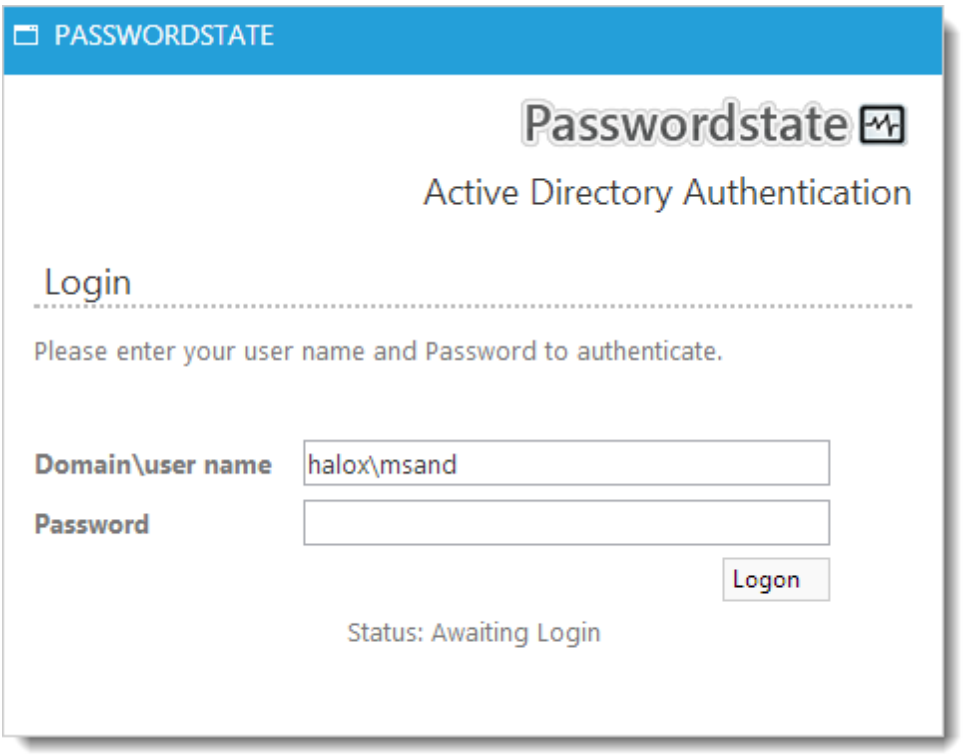
Authentication Option

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

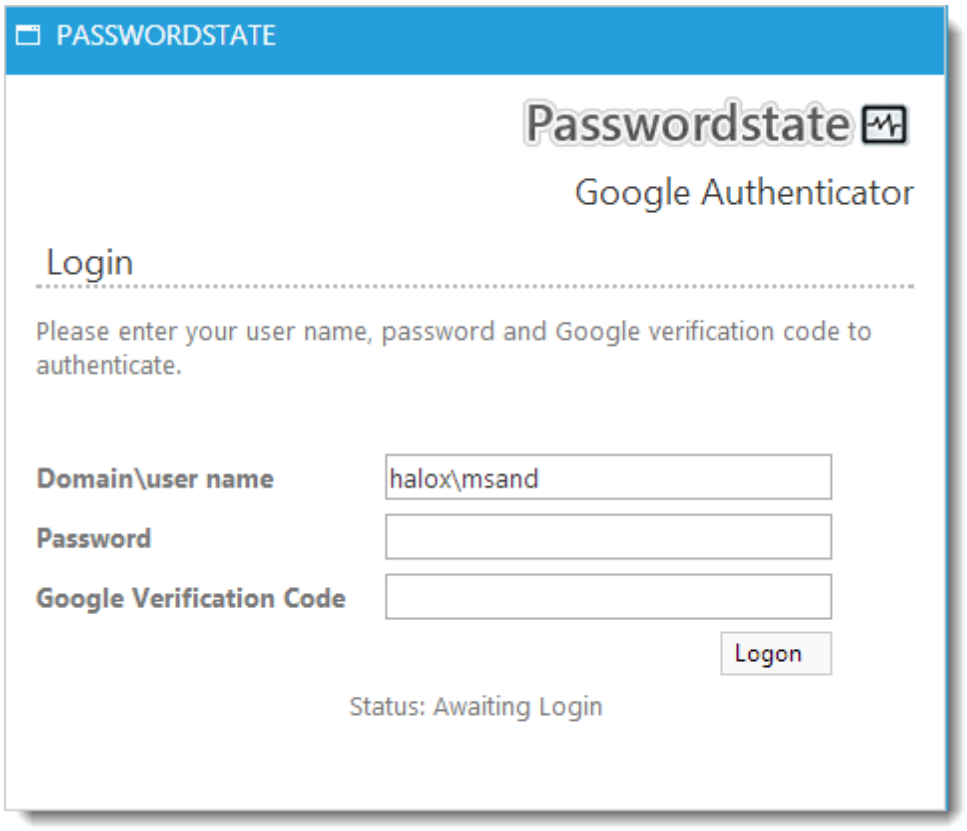
Passthrough AD Authentication
If DNS, your browser, and the site in IIS is configured correctly, your browser should not prompt you for your account details when using this authentication method, instead it should pass your account details to the Passwordstate web site in IIS, and IIS ensures your account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

Manual AD Authentication

Provides a dialog for users to manually specify their AD domain credentials.



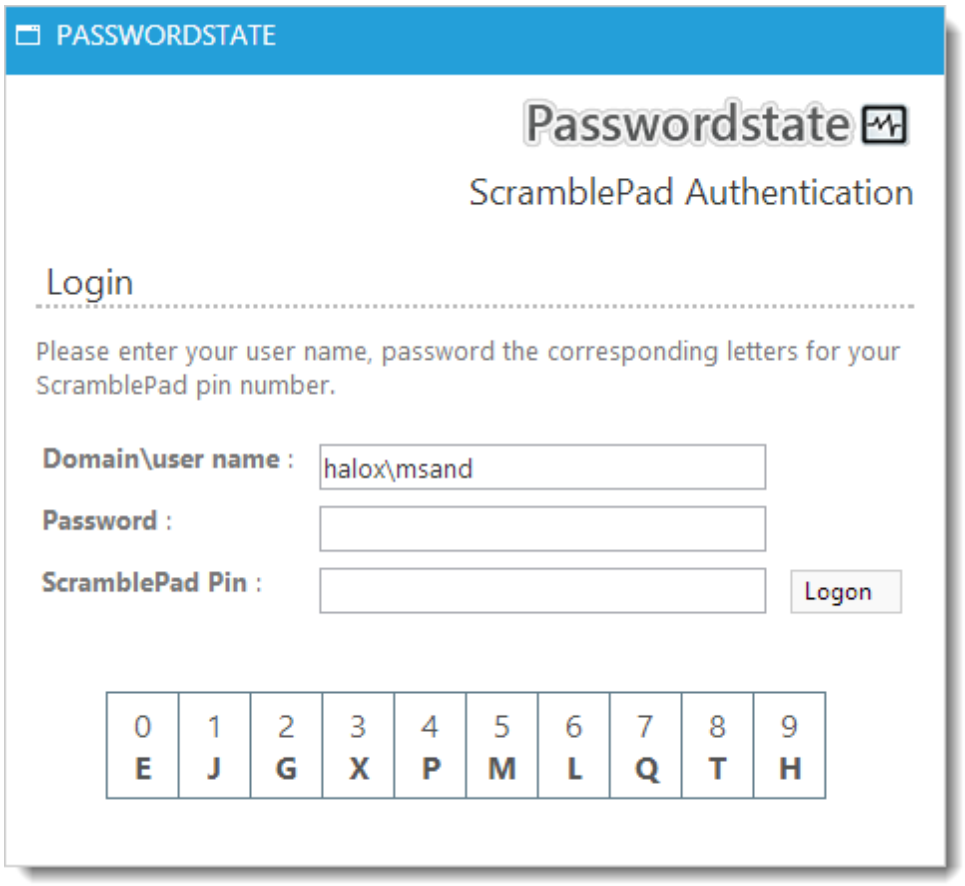
Manual AD and Google Authenticator
Provides a dialog for users to manually specify their AD domain credentials, and a Google Verification Code. To use this authentication method, the user must create a Google Authenticator Secret Key on the Preferences screen, or Security Administrators can do it for them on the User Accounts screen.



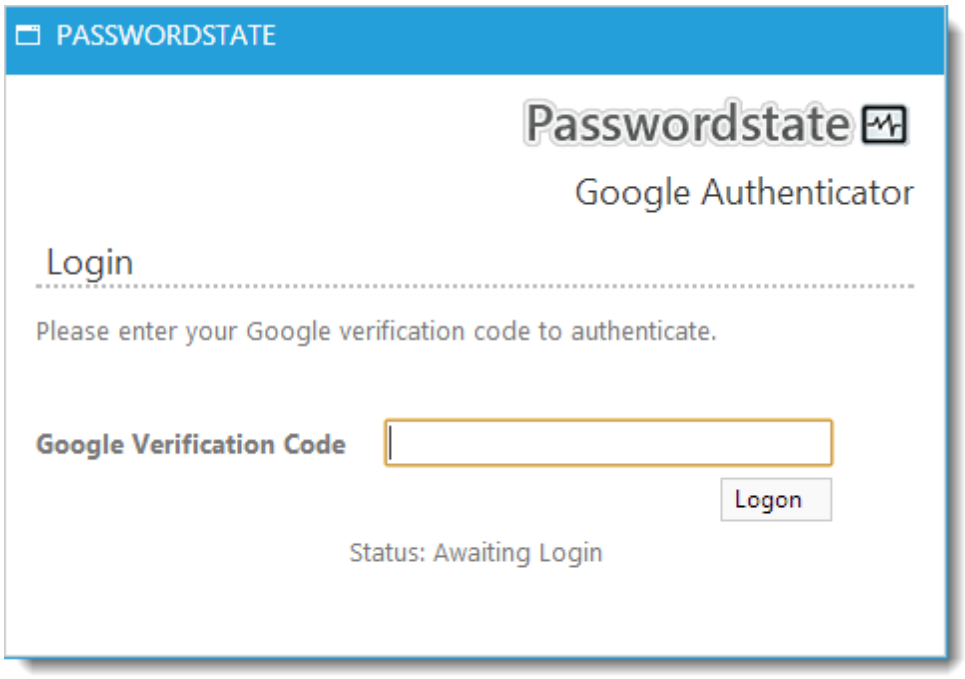
Manual AD and RSA SecurID Authentication
Provides a dialog for users to manually specify their AD domain credentials, and a SecurID Passcode. To use this authentication method, the user must have a valid SecurID account and token.

Manual AD and ScramblePad Authentication
Provides a dialog for users to manually specify their AD domain credentials, and a ScramblePad Pin. 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.

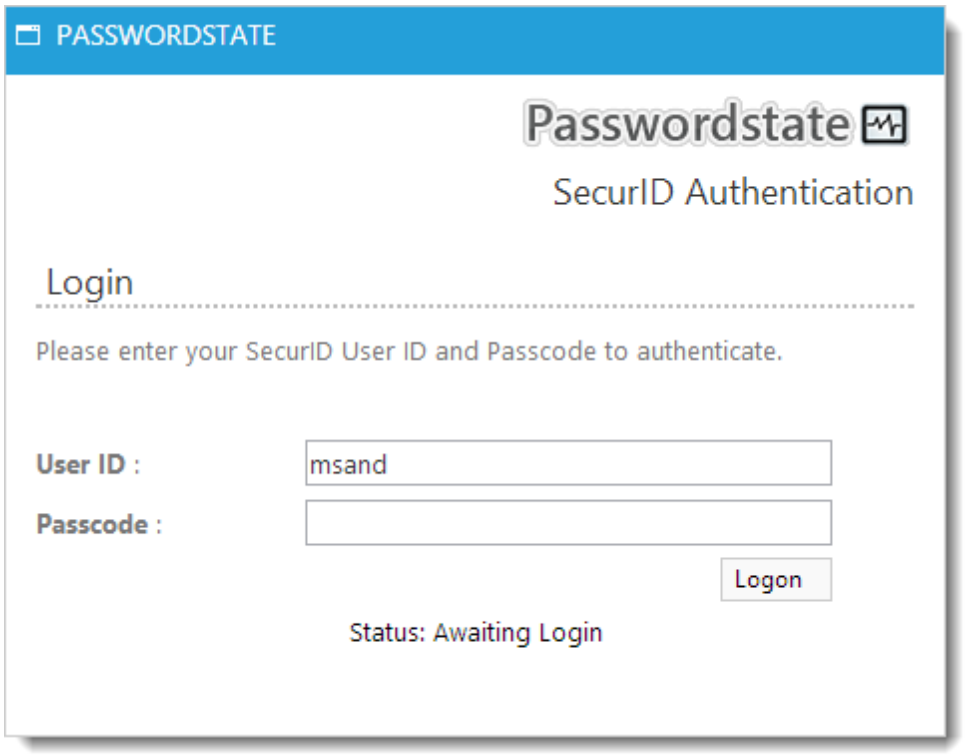
In the screenshot below, if the user's Pin Number was **0123**, then they would need to enter **ejgx** to authenticate correctly - the letters are rearranged every time the screen is accessed.



Google Authenticator
Provides a dialog for users to manually specify their Google Verification Code - this works in conjuction with Passthrough AD Authentication. To use this authentication method, the user must create a Google Authenticator Secret Key on the Preferences screen, or Security Administrators can do it for them on the User Accounts screen.

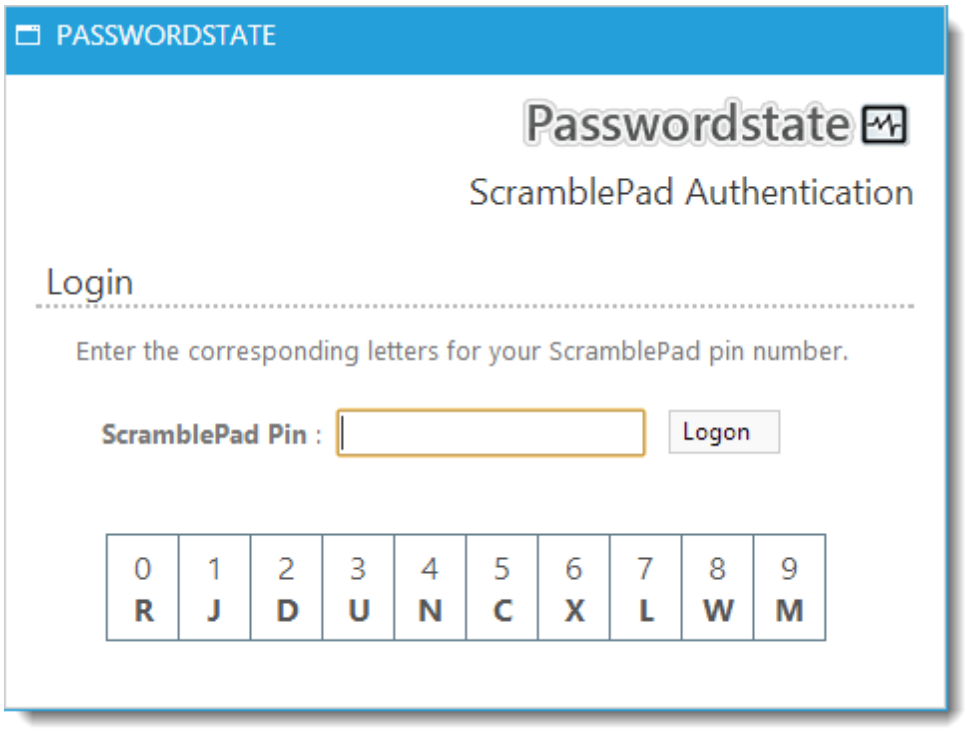


RSA SecurID Authentication
Provides a dialog for users to manually specify their SecurID Passcode - this works in conjuction with Passthrough AD Authentication. To use this authentication method, the user must have a valid SecurID account and token.

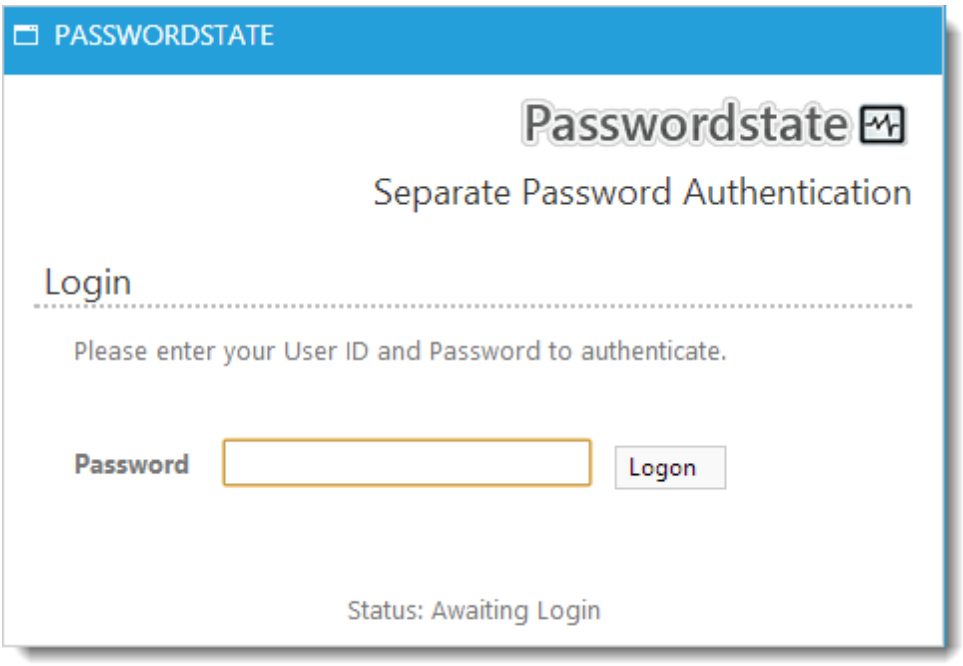


ScramblePad Authentication
Provides a dialog for users to manually specify their ScramblePad Pin code - this works in conjuction with Passthrough AD Authentication. To use this authentication method, the user must specify their ScramblePad Pin number on the Preferences screen, or Security Administrators can do it for them on the User Accounts screen.

In the screenshot below, if the user's Pin Number was **0123**, then they would need to enter **rjdu** to authenticate correctly - the letters are rearranged every time the screen is accessed.



Separate Password
Provides a dialog for users to specify a separate authentication password - this works in conjuction with Passthrough AD Authentication. To use this authentication method, the user must specify their separate password on the Preferences screen, or Security Administrators can create a random password for them on the User Accounts screen.



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

If one of the SecurID Authentication options are selected, auto-populate the UserID field based on the current logged in user - domain suffix will be dropped if using Active Directory version of Passwordstate

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

Minimum ScramblePad Pin Length

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

22.8 User Acceptance Policy Tab

The User Acceptance Policy Tab allows you to specify a popop '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)

22.9 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 - 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.

22.10 Custom Logos Tab

The Custom Logos Tab allows you to specify your own custom logo to use at the top left-hand side of the page, and on various Dialog windows.

If possible, it is recommended you make your logos of the following size, so that they appear symmetrically correct on the site:

- Title Logo - 192 pixels Wide x 28 pixels High
- Dialog Logo - 196 pixels Wide x 30 pixels High

Note 1: 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.
Note 2: Adobe Photoshop template files are also provided, allowing for easier creation of your own logos if required.

22.11 High Availability Options Tab

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

22.12 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, or make calls to the Passwordstate API.

Specifying IP Ranges can be done in the following format:

- 192.168.1.* (all addresses in the range of 192.168.1.1 to 192.168.1.254)
- 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

22.13 API Key Tab

The API Key Tab allows you to specify a System Wide API Key which can be used for various API Calls. Please refer to the API Documentation for further details.

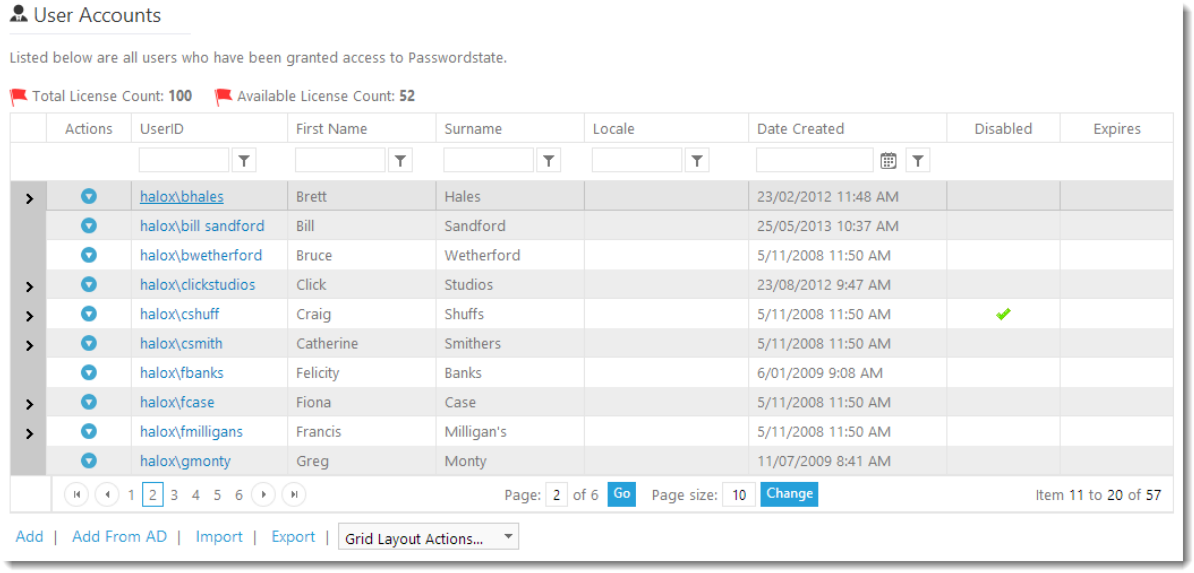
23 User Accounts

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

Note: 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.



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

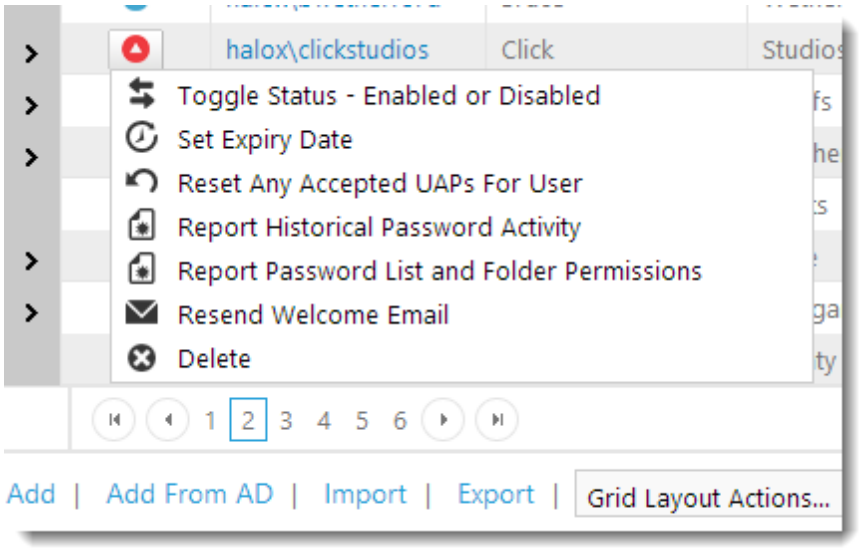
User Account Actions Menu

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

- Toggle Status (Enabled or Disabled) - this will either enable or disable the user's account, preventing them from accessing the Passwordstate web site
- 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
- 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
- Report Historical Password Activity - this reports shows all auditing data for the user's account as it relates to password records i.e. viewing passwords, copying to the clipboard, access permissions, etc
- Report Password List and Folder Permissions - this report will show all the Password Lists and Folders the user has access to, and what their permissions are. The permissions are either based on their own individual user account, or any security groups they may be members of
- 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
- Delete - deleting a user's account will remove all access for them, so please use with caution

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 : Disabling a user's account does not count towards the number of used licenses



Editing User Account Settings

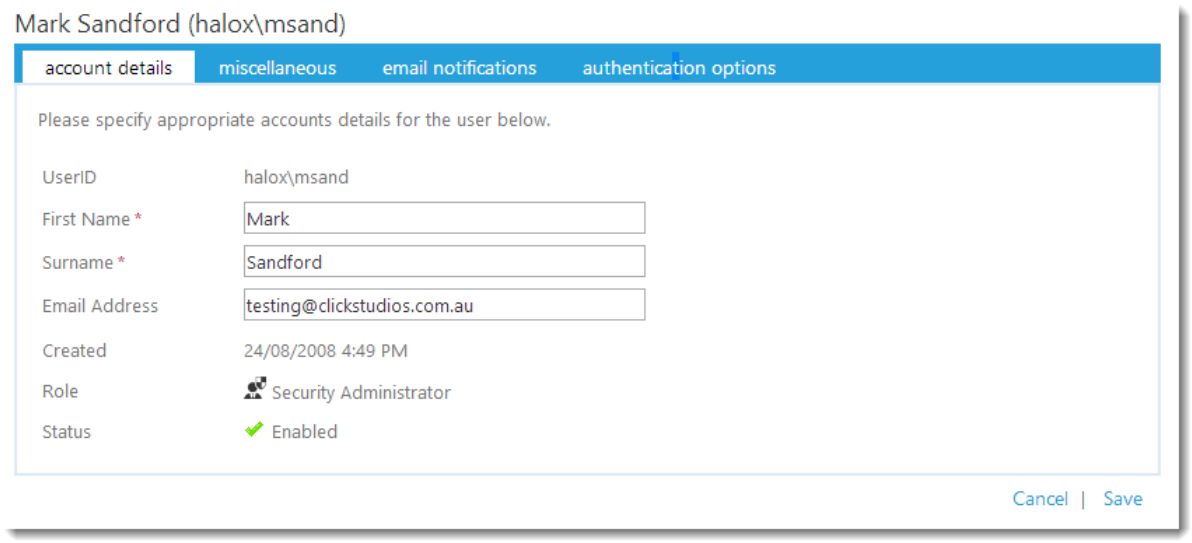
By clicking on the UserID hyperlink in the grid, you will be directed to a screen where you can edit multiple properties for the user's account.

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.

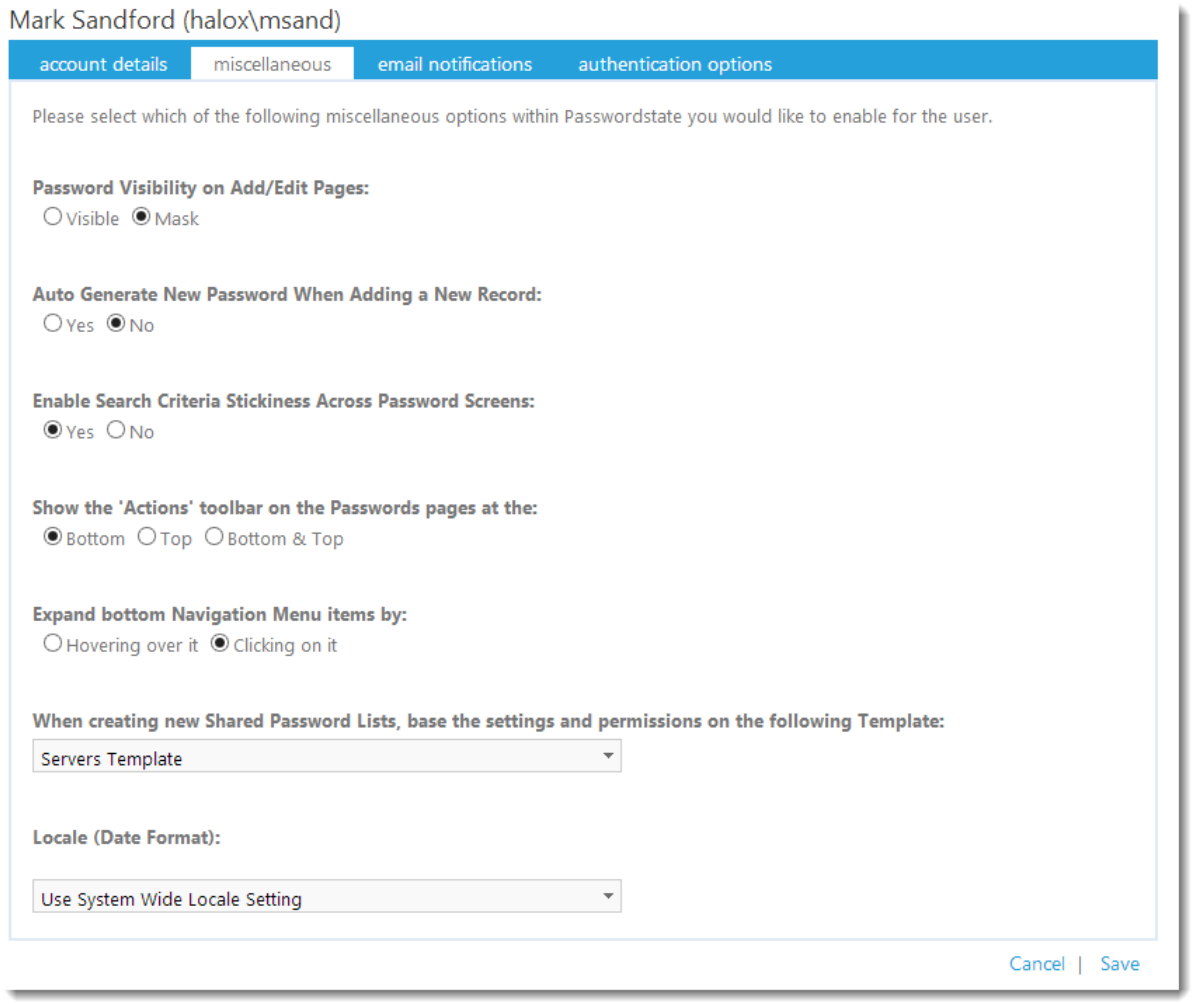


Miscellaneous Tab

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
Expand bottom Navigation Menu items by	The Navigation Menu at the bottom of the screen can expand certain menus vertically by simply hovering

	over them. If you choose, you can change this option so you must first click on the Menu item before it expands
When creating new Shared Password Lists, base the settings and permissions on the following Template	When creating new Password Lists, you can choose to automatically specify all the settings based 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



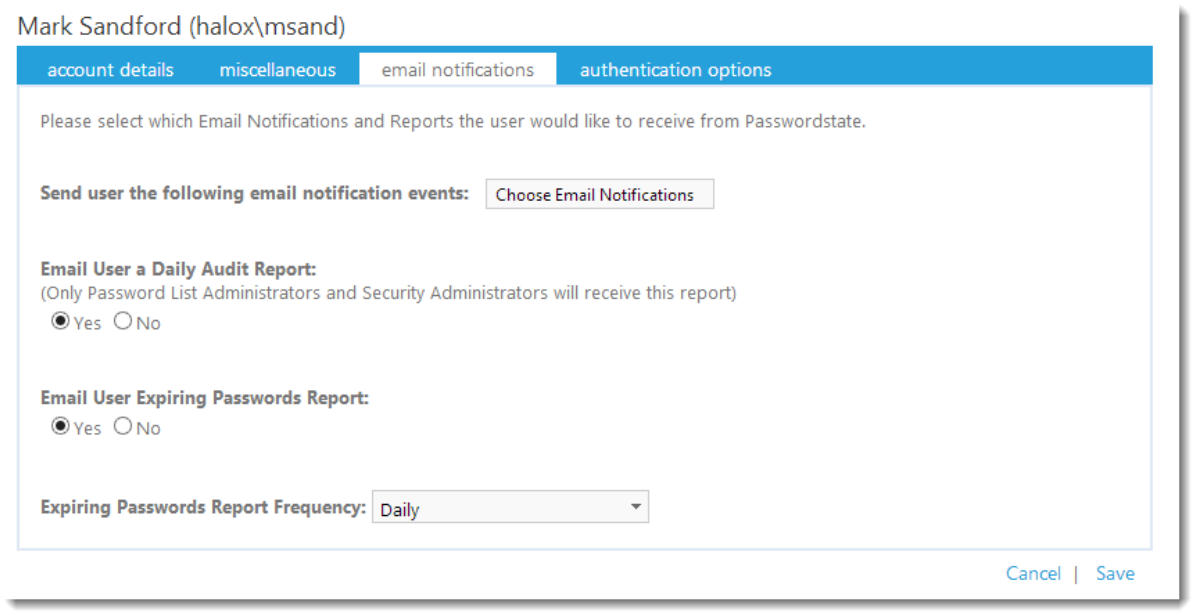
Email Notifications Tab

The Email Notifications Tab allows you to enabled/disabled one or more of the many different email notifications Passwordstate can send to the user, as well as different report options.

Note 1: The feature Email Notification Groups may cause the 'Choose Email Notifications'

button below to be disabled

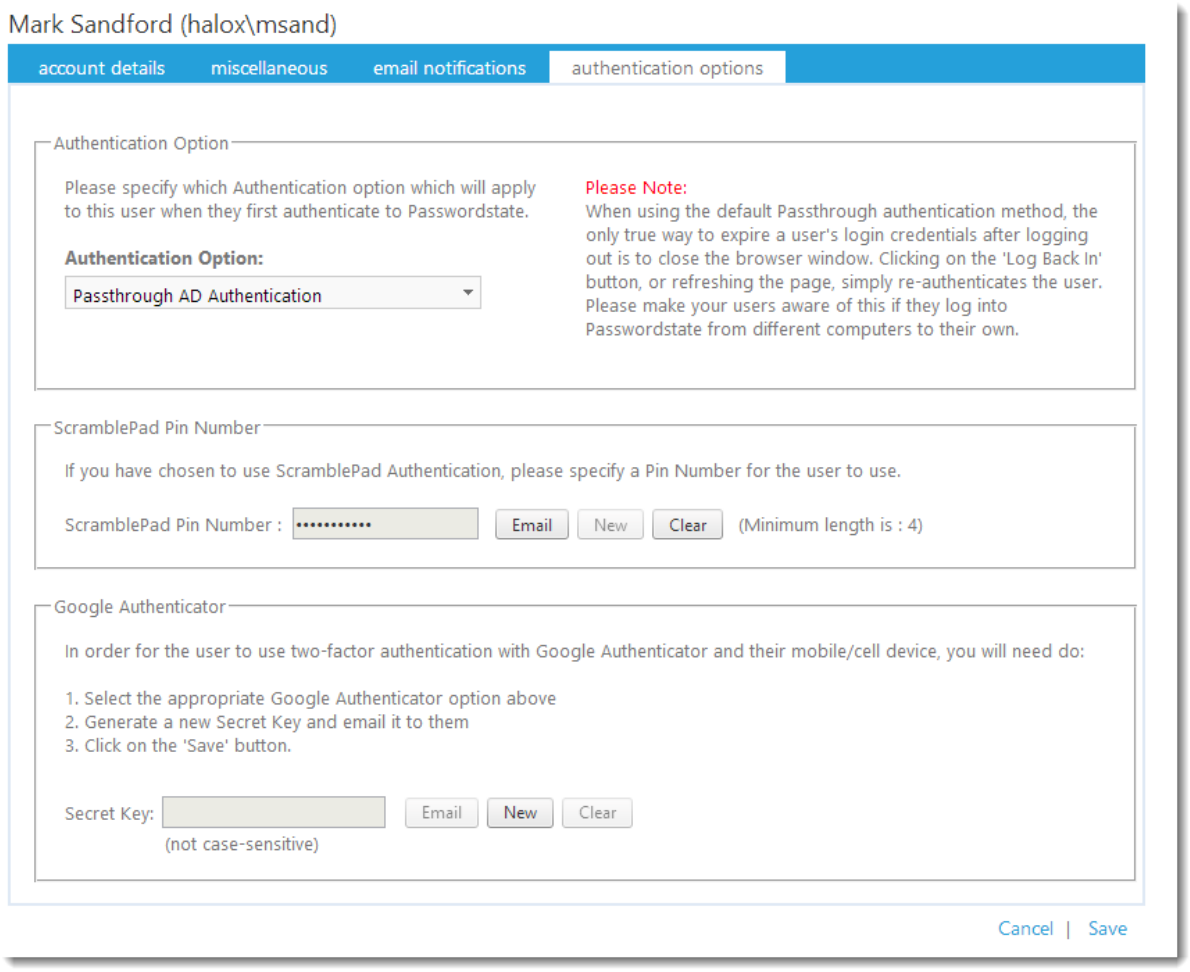
Note 2: One or more Email Templates may also be disabled, in which case the user will not receive email notifications for the disabled templates



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
- Create/clear/email the user their ScramblePad Pin number
- Create/clear/email the user their Google Authenticator Secret Key



24 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, Password Folders and 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
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


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:

- View Permissions - allows you to view, and make permission changes as to who the policy is in effect for
- Toggle Status - either enable or disable the policy
- Delete - delete the policy